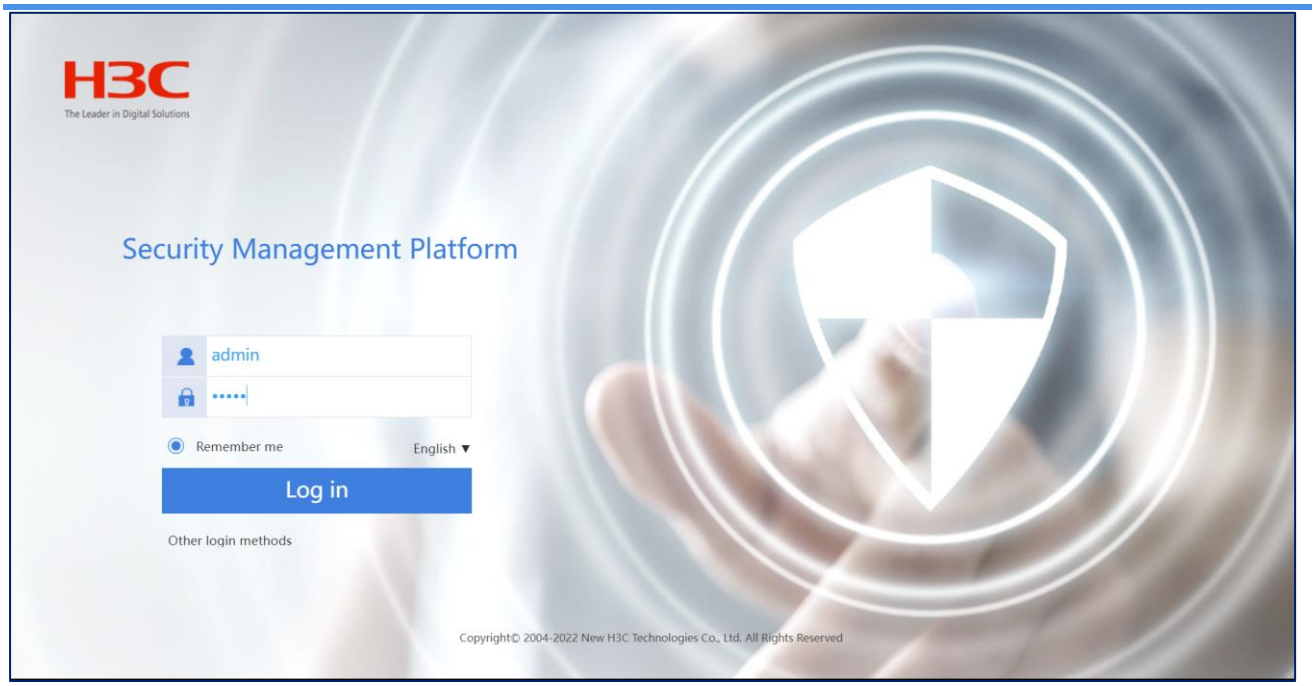
H3C SecPath ファイアウォール製品

GUI メニューヘルプ

文書バージョン:6W402-20220223

内容

Overview



Login to the Web interface

Web browser requirements

次の Web ブラウザを使用することをお勧めします。

- Google Chrome 40 以降。
- Mozilla Firefox 19 以降。
- Internet Explorer 10 以降。

Web インターフェースにアクセスするには、次のブラウザ設定を使用する必要があります。

- ファーストパーティクッキー(アクセスしているサイトのクッキー)を受け入れます。
- ソフトウェアのアップグレードまたはダウングレード後に Web ページが正しく表示されるようにするには、ログインする前にブラウザによってキャッシュされたデータをクリアします。
- Web ブラウザに応じて、アクティブスクリプトまたは JavaScript を有効にします。
- Microsoft Internet Explorer ブラウザを使用している場合は、次のセキュリティー設定を有効にする必要があります。
  - ActiveX コントロールとプラグインを実行します。
  - スクリプトを実行しても安全とマークされたスクリプト ActiveX コントロール。

Log in to the Web interface for the first time

セキュリティー上の理由から、最初のログイン成功後にログインパスワードを変更することをお勧めします。

デバイスは、HTTP および HTTPS によるユーザーログインをサポートします。デフォルトでは、HTTPS が有効になっています。

最初のログインには、次のデフォルト設定を使用します。

項目	設定
デバイス管理インターフェースの IP アドレス	192.168.0.1/24
Username	admin
Password	admin
User role	Network-admin

Web インターフェースにログインするには:

1. イーサネットケーブルを使用して、設定端末をデバイスのイーサネットポートに接続します。
2. ログインホストに、デバイスと同じサブネット内の IP アドレスを割り当てます。
3. ブラウザを開き、ログイン情報を入力します。
   a. アドレスバーで、デバイス **https://192.168.0.1** の IP アドレスを入力します。
   b. ログインページで、デフォルトのユーザー名(**admin**)とパスワード(**admin**)を入力します。
   c. **Login** をクリックします。
4. ログイン情報を変更します。

   Login をクリックすると、デフォルトパスワードの変更を強制するダイアログボックスが自動的に開きます。システムセキュリティーを確保するには、複雑な新規パスワードを構成します。次に、ダイアログボックスで OK をクリックして Web インターフェースにログインします。

   デバイスの IP アドレスを変更するには、**Network > Interface Configuration > Interfaces** ページに移動します。

   新しいユーザーカウントを追加し、別のユーザーにアクセス権限を割り当てるには、**System > Administrators > Administrators** ページに移動します。

Log out of the Web interface

- セキュリティー上の理由から、タスクを完了したらすぐに Web インターフェースからログアウトしてください。
- ブラウザを直接閉じてログアウトすることはできません。

- Web インターフェースからログアウトしても、デバイスは設定を自動的に保存しません。デバイスの再起動時に設定が失われないように、設定を保存する必要があります。

1. 現在の設定を保存するには、次のいずれかの方法を使用します。
   - Web インターフェースの右上隅にある **Save** アイコンをクリックします。
   - **System > Maintenance > Configuration Management** ページに移動して、設定を保存します。
2. Web インターフェースの右上隅にある **Logout** アイコンをクリックします。

Use the Web interface

Web interface layout

図 1 Web インターフェースのレイアウト

1)バナーと管理セクション	2)ナビゲーションペイン	3)作業ペイン

図 1 に示すように、Web インターフェースには以下の領域が含まれています。

面積	説明
(1) Banner and admin section	次のアイテムが含まれます。 • 会社のロゴ、デバイス名、現在のログインユーザーに関する情報などの基本情報。 • 基本的な管理アイコン: ○  **Admin** アイコン:ログインパスワードを変更するには、このアイコンをクリックします。 ○  **Save** アイコン:このアイコンをクリックして、設定を保存します。 ○  **Help** アイコン:オンラインヘルプにアクセスするには、このアイコンをクリックします。 ○  **Logout** アイコン:ログアウトするには、このアイコンをクリックします。
(2) Navigation pane	すべての機能のメニューが表示されます。
(3) Wok pane	情報を表示し、機能を設定するための領域を提供します。 このペインのコンテンツに応じて、Web ページには次のタイプがあります。 • **Table page**: テーブル内のエントリを表示します(「テーブルページの使用」を参照)。 • **Configuration page**: 機能を設定するためのパラメーターが含まれています(「設定ページを使用する」を参照)。

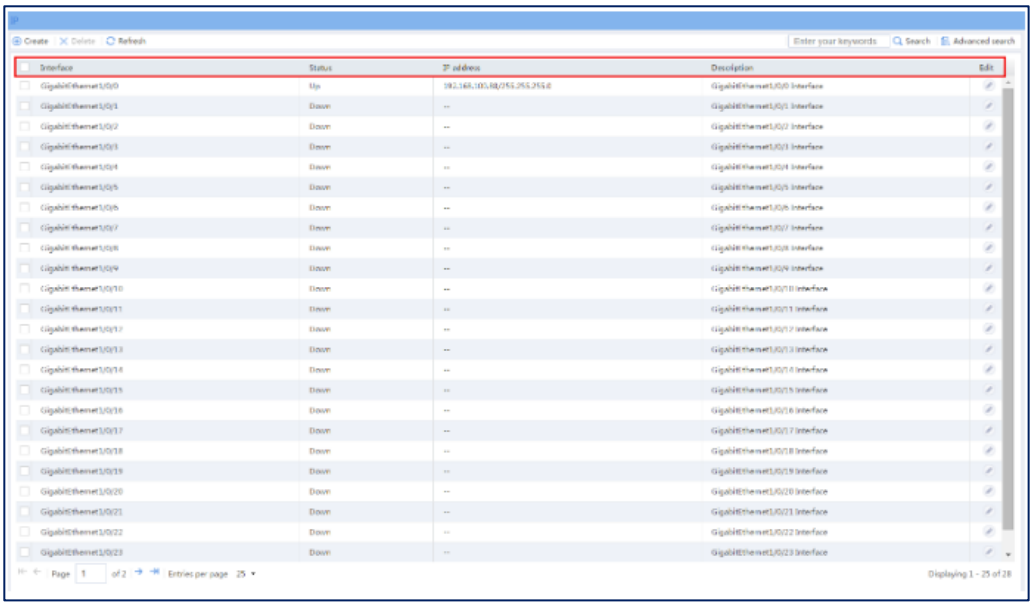
Types of webpages

Web ページには、表および構成ページがあります。この項では、これらのページの基本情報を説明します。

Use a table page

図 2 に示すように、テーブルページにはテーブル内のエントリが表示されます。エントリをフィールド別に昇順または降順でソートするには、フィールドをクリックします。たとえば、エントリをインターフェース別にソートするには、**Interface** をクリックします。

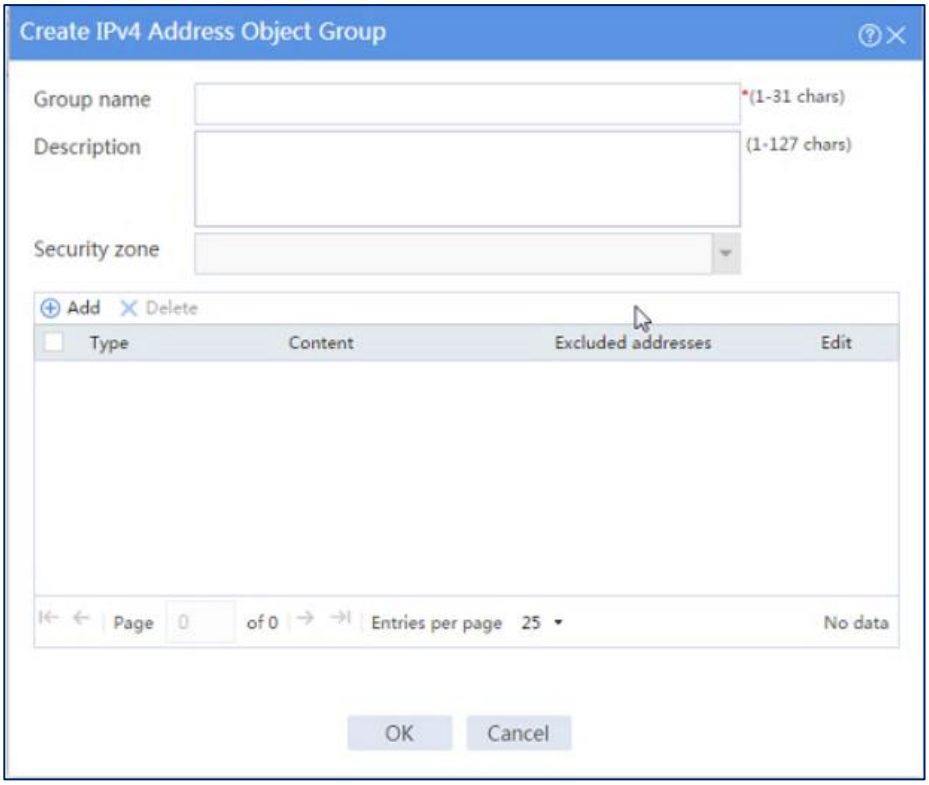
図 2 テーブルページの例



Use a configuration page

図 3 に示すように、1 つの構成ページには構成タスクのすべてのパラメーターが含まれています。パラメーターを別のページで構成する必要がある場合は、通常、構成ページにリンクが表示されます。宛先ページにナビゲートする必要はありません。

図 3 設定ページの例



Perform basic tasks

ここでは、デバイスを設定または管理するときに頻繁に実行する必要がある基本的なタスクについて説明します。

Save the configuration

通常、設定は作成後すぐに有効になります。ただし、システムは設定を構成ファイルに自動的に保存しません。設定はデバイスの再起動時に失われます。
設定が失われないようにするには、次のいずれかの方法を使用して設定を保存します。

- Web インターフェースの右上隅にある **Save** アイコン をクリックします。
- **System > Maintenance > Configuration Management** ページに移動し、**Save running configuration** をクリックします。

Reboot the device

一部の設定(IRF など)を有効にするには、再起動が必要です。
デバイスを再起動するには:

1. 設定を保存します。
2. **System** タブをクリックします。
3. ナビゲーションペインで、**Maintenance > Reboot** を選択します。

Reboot ページが開きます。

4. **Reboot the device** をクリックします。

Feature navigator

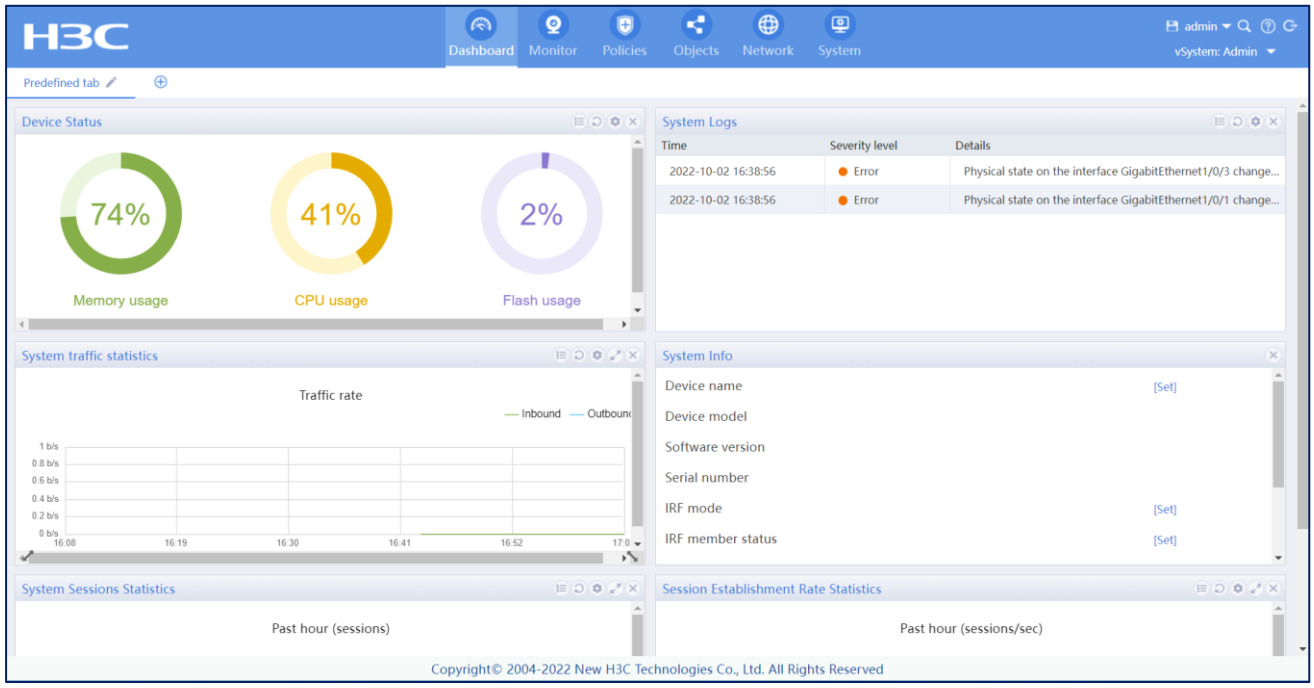
使用可能なメニューアイテムおよびアイコンは、ユーザーロールによって異なります。デフォルトでは、任意のユーザーロールを使用して情報を表示できます。機能を構成するには、**network-admin** または **context-admin** のユーザーロールが必要です。

network-admin または **context-admin** ユーザーロールでログインした後、バナーおよび admin セクションの各トップメニューをクリックしてナビゲータテーブルを開きます。ナビゲータテーブルを使用して、実行するタスクのページに移動します。

次に例を示します。

- デフォルトのデバイス名を変更するには、**System > Maintenance > Settings > Device Info** ページに移動します。
- IPv4 ACL を削除するには、**Objects > ACLs > IPv4 ACLs** ページに移動します。

Dashboard



このヘルプには、次のトピックが含まれています。

- Introduction
  - Operation monitor
  - Traffic monitor
  - Threat monitor
  - Load balancing monitor

Introduction

Dashboard ページには、キー情報、データおよびデバイスの様々な状態がグラフィカルウィジェットで明確に表示されます。このページには事前定義済のタブが用意されており、必要に応じてタブを定義することもできます。事前定義済のタブには基本モジュールに関する情報が表示され、必要に応じて他のモジュールを追加できます。操作モニター、トラフィックモニター、脅威モニターまたはフィルタリングモニターのモジュールなど、重要なモジュールに関する情報を簡単に表示するには、タブを定義し、そのタブにモジュールに関する情報を追加および表示できます。

モジュールのサポートは、デバイスモデルによって異なります。

Operation monitor

オペレーションモニターは、デバイスの動作状態情報を提供します。

Device status

Device status ウィジェットには、CPU 使用率、メモリー使用率および CF カード使用率が表示されます。詳細情報を表示してアラームしきい値を設定するには、**Details** アイコンをクリックします。
アラームしきい値には、CPU 使用率アラームしきい値と空きメモリーアラームしきい値があります。必要に応じてアラームしきい値を設定します。

System logs

System logs ウィジェットでは、エラーレベル以上のシステムログメッセージが表示されます。すべてのレベルのログメッセージに関する詳細情報を表示するには、**Details** アイコンをクリックします。この情報は、デバイスステータスの分析およびトラブルシューティングに使用できます。

System traffic statistics

System traffic statistics ウィジェットは、一定期間のインバウンドおよびアウトバウンドトラフィック統計を折れ線グラフで表示します。このグラフを使用して、ネットワーク上のトラフィック分布を時間の経過とともに分析できます。
インターフェースの詳細なトラフィック統計情報を表示するには、**Details** アイコンをクリックします。
トラフィック統計情報パラメーターを設定し、統計結果をフィルタリングするには、**Set** アイコンをクリックします。

System session statistics

System session ウィジェットには、過去 1 時間に確立されたセッション数に関する統計が表示されます。過去 1 時間、過去 1 日または過去 30 日間に確立されたセッションに関する統計を表示するには、**Details** アイコンをクリックします。
トップ 10 ランキングを有効にしてランキング結果を表示するには、次のボタンをクリックします。

- **Enable top 10 ranking**: デバイスがサービスに基づいて統計情報を収集し、送信元アドレスまたは宛先アドレスで統計情報をソートできるようにします。
- **View top 10 ranking**: 上位 10 位ランキング結果を表示します。期間(過去 1 時間、過去 1 日または過去 30 日間)とソート基準(送信元アドレスまたは宛先アドレス)を選択できます。

Session Establishment Rate Statistics

Session Establishment Rate Statistics ウィジェットは、過去 1 時間のセッション確立率統計を表示します。過去 1 時間、過去 1 日または過去 30 日間のセッション確立率統計を表示するには、**Details** アイコンをクリックします。

トップ 10 ランキングを有効にしてランキング結果を表示するには、次のボタンをクリックします。

- **Enable top 10 ranking**: デバイスがサービスに基づいて統計情報を収集し、送信元アドレスまたは宛先アドレスで統計情報をソートできるようにします。
- **view top 10 ranking**: 上位 10 位ランキング結果を表示します。期間(過去 1 時間、過去 1 日または過去 30 日間)とソート基準(送信元アドレスまたは宛先アドレス)を選択できます。

Deny session statistics

Deny session statistics ウィジェットには、拒否セッション数に関する統計が表示されます。過去 1 時間、過去 1 日または過去 30 日間の統計を表示するには、**Details** アイコンをクリックします。
トップ 10 ランキングを有効にしてランキング結果を表示するには、次のボタンをクリックします。

- **Enable top 10 ranking**: デバイスがサービスに基づいて統計情報を収集し、送信元アドレスまたは宛先アドレスで統計情報をソートできるようにします。
- **view top 10 ranking**: 上位 10 位ランキング結果を表示します。期間(過去 1 時間、過去 1 日または過去 30 日間)とソート基準(送信元アドレスまたは宛先アドレス)を選択できます。

System information

System info ウィジェットには、デバイス名、デバイスモデル、ソフトウェアバージョン、IRF モードなどのデバイス情報が表示されます。

Internet access monitoring

Internet access monitoring ウィジェットには、アプリケーションタイプ、Web サイトアドレスおよび転送されたファイルなどのインターネットアクセス情報が表示されます。詳細なインターネットアクセス情報および監査ユーザーの動作を表示するには、**Details** アイコンをクリックします。

License information

License info ウィジェットには、機能に関するライセンス情報が表示されます。ライセンスタイプ、ステータス、有効期間などの詳細なライセンス情報を表示するには、**Details** アイコンをクリックします。

Interface Information

Interface information ウィジェットは、デバイス上の各インターフェースの現在の状態と詳細情報を表示します。シミュレートされたデバイスパネルでインターフェース状態を表示するには、**View device panel** ボタンをクリックします。

Traffic monitor

トラフィックモニターには、最新のモニターリング間隔のトラフィックランキング統計情報が表示されます。デフォルトでは、上位 5 つが表示されます。

Real-time application ranking

デフォルトでは、リアルタイムアプリケーションランキングウィジェットは、リスト内の総トラフィックレートに対するアプリケーションのトラフィックレートの割合によって、上位 5 つのアプリケーションを表示します。
リアルタイムアプリケーションランキングリストには、次のフィールドが含まれます。

- application。
- downlink traffic rate。
- uplink traffic rate。
- total rate。
- percentage。

リアルタイムアプリケーションランキングリストを表示するようにウィジェットをカスタマイズするには、ウィジェットの右上隅にある **Set** アイコン をクリックし、次のいずれかの機能を設定します。

- **Auto refreshing**: **Auto refresh** オプションを選択し、**Refresh interval** フィールドに更新間隔を入力して、**OK** をクリックします。
- **real-time traffic data collection**: **Enable real-time traffic data collection** オプションを選択し、**OK** をクリックします。リアルタイムでトラフィックの詳細を表示するには、**Display real-time traffic details** オプションを選択します。異なるユーザーが使用しているアプリケーションのトラフィックデータをリアルタイムで表示するには、リアルタイムアプリケーションランキングリストの **Application** 列でアプリケーションをクリックします。

Threat monitor

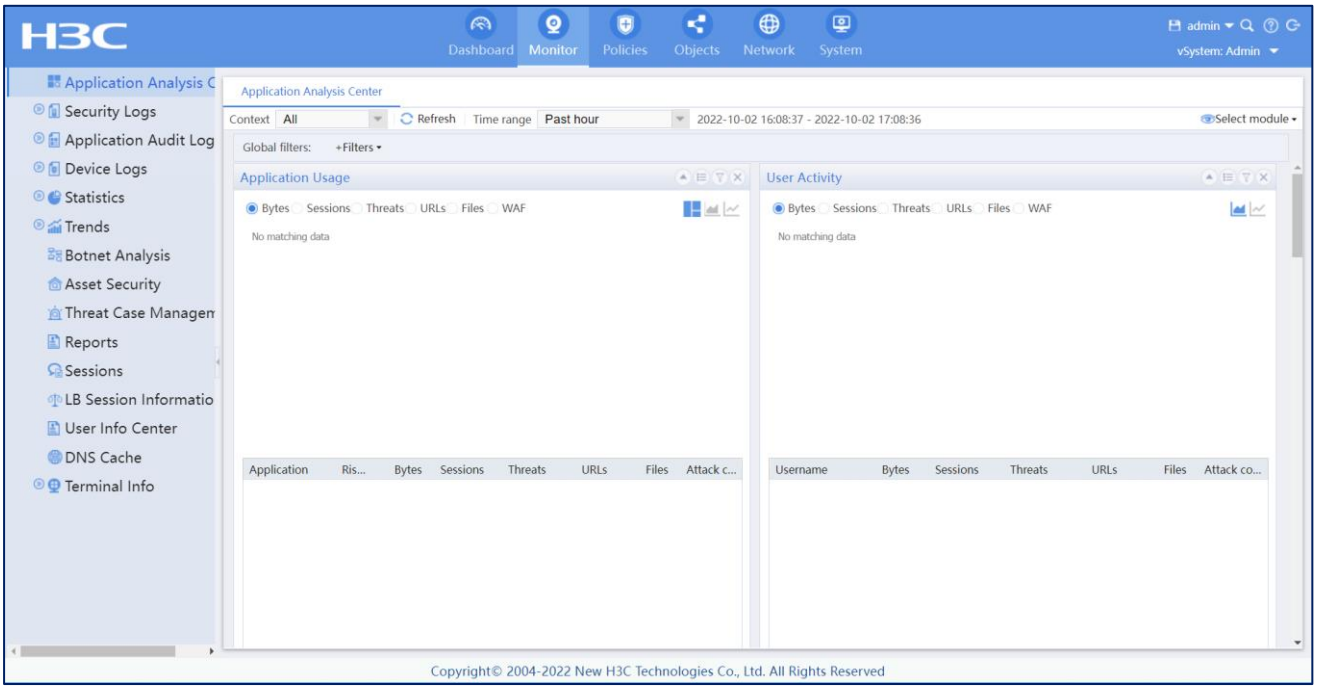
Security status

このウィジェットは、リスク要因とセキュリティーベントの分布を表示します。詳細な統計分析を表示するには、**Security Event Distribution** グラフのデータをクリックします。

Top 10 hosts at risk

このウィジェットは、ホスト名、リスクレベル、攻撃イベントなどのコンプロマイズドホスト情報を表示します。ホストの詳細なリスク分析を表示するには、ホスト名をクリックします。

Application analysis center



このヘルプには、次のトピックが含まれています。

- Introduction
- Restrictions and guidelines
- Configure the application analysis centerapplication security analysis
  - Configure global settings
  - Customize the settings for each widget
  - Application usage
  - User activity
  - Source IP activity
  - Destination IP activity
  - Source security zones
  - Destination security zones
  - Security policy usage
  - Threat activity
  - WAF activity

Introduction

アプリケーション分析センターには、次のウィジェットの統計情報が表示されます。

- **Application usage**。
- **User activity**。
- **Source IP activity**。
- **Destination IP activity**。
- **Security policy usage**。
- **Source security zones**。
- **Destination security zones**。
- **Threat activity**。

各ウィジェットは、次の側面に基づいて統計情報を表示します。

- **bytes**: トラフィック分布をバイト単位で表示します。
- **Sessions**: セッション統計を表示します。どのアプリケーション、ユーザーおよび IP アドレスが多数のセッションを確立または占有しているかに関する情報を取得できます。
- **Threats**: 脅威の統計情報を表示します。
- **URLs**: Web アクセス統計情報を表示します。
- **Files**: ファイルフィルタリングの統計情報を表示します。

Restrictions and guidelines

デバイスが、アプリケーション分析センター機能をサポートしないバージョンからサポートするバージョンに更新する場合、デバイスは、更新後のデータに対してのみアプリケーション分析を実行します。

Configure the application analysis center

Configure global settings

Application Analysis Center ページには、すべてのウィジェットに有効な統計収集に関する次のグローバル条件が表示されます。

Select a context

コンテキストベースの統計を表示するには、**Context** リストからコンテキストを選択します。すべてのコンテキストの統計を表示するには、リストから **All** を選択します。

Specify the time range

時間範囲の統計情報を表示するには、**Time range** リストから時間範囲を選択するか、リストから **Custom** をクリックして、必要に応じて時間範囲をカスタマイズします。

Select widgets

ページに表示されるウィジェットをカスタマイズするには、**select module** をクリックし、リストから目的のウィジェットを選択します。

Add global filters

統計情報をフィルタリングするフィルタを追加するには、**Global filters** フィールドで **Filters** をクリックし、フィルタタイプを選択して、必要に応じてフィルタを設定します。

フィルタを削除するには、フィルタの上にマウスを移動し、フィルタの右側にあるアイコンをクリックします。すべてのフィルタを削除するには、**global filters** フィールドの上にマウスを移動し、フィールドの右端にあるアイコンをクリックします。

Customize the settings for each widget

指定したウィジェットに対してのみ有効な次の設定を構成できます。

View more data

デフォルトでは、各ウィジェットには上位 10 項目のみが表示されます。詳細なデータを表示するには、各セクションの右上隅にあるアイコンをクリックします。

Add analyzer filters

ウィジェット専用のフィルタを追加するには、各セクションの右上隅にあるアイコンをクリックし、必要に応じてフィルタを設定します。

Switch between analysis aspects

分析アスペクトの統計を取得するには、各セクションの上部で分析アスペクトを選択します。現在のソフトウェアバージョンでは、**Bytes**、**Session**、**Threats**, **URLs**、そして **Files** の各アスペクトがサポートされています。分析アスペクトを選択すると、分析アスペクトに基づいて統計がランク付けされます。たとえば、**Bytes for Application Usage** に Bytes 選択した場合、**Application Usage** セクションでは、グラフおよび表のトラフィックに基づいてアプリケーションがランク付けされます。

Display data in graphs and tables

このページでは、各ウィジェットのデータをグラフや表で表示できます。

グラフの種類には、ツリーマップ()、エリアグラフ()、線グラフ()、ヒストグラム()があります。グラフの種類のサポートはウィジェットによって異なります。

グラフのタイプで統計を表示するには、各セクションの右上隅にあるグラフアイコンをクリックします。ドリルダウン機能をサポートしているのは面グラフのみです。ドリルダウンは、マウスをクリックして一般ビューから詳細ビューまで統計を表示できる機能です。たとえば、**application usage** ウィジェットでは、面グラフの電子メール領域をクリックできます。その後、面グラフには電子メールのサブカテゴリ(126 Mail、163 Mail など)に関する情報のみが表示されます。特定の電子メールサブカテゴリに関する情報を表示するには、サブカテゴリ領域(126 Mail 領域など)をクリックします。
デフォルトでは、表には上位 10 エントリのみが表示されます。詳細データを表示するには、**Miscellaneous** をクリックし、リストから **View more data** を選択します。

数値以外の列では、アプリケーション名をウィジェット固有のフィルタとして追加したり、グローバルフィルタとして追加するなど、より多くのアクションを行うことができます。数値以外の列のアイテムのアクションメニューを表示するには、アイテムの上にマウスを移動し、  アイコンをクリックします。

Application usage

Application Usage セクションには、様々な側面に基づいたアプリケーションの使用状況統計が表示されます。アプリケーションの設定は適宜カスタマイズできます。
エリアグラフは、帯域幅使用率の高いアプリケーションを可視化し、詳細なアプリケーション統計を表示するドリルダウン機能を提供します。

User activity

User Activity セクションには、様々な側面に基づいたユーザー統計が表示されます。ユーザーの設定は適宜カスタマイズできます。

Source IP activity

Source IP Activity セクションには、様々な側面に基づいたソース IP 統計が表示されます。ソース IP の設定は適宜カスタマイズできます。

Destination IP activity

Destination IP Activity セクションには、様々な側面に基づいた宛先 IP 統計が表示されます。宛先 IP の設定は、適宜カスタマイズできます。

Source security zones

Source Security Zones セクションには、様々な側面に基づいたソースセキュリティーゾーンの統計が表示されます。ソースセキュリティーゾーンの設定は、必要に応じてカスタマイズできます。

Destination security zones

Destination Security Zones セクションには、様々な側面に基づいた宛先セキュリティーゾーンの統計が表示されます。宛先セキュリティーゾーンの設定は、必要に応じてカスタマイズできます。

Security policy usage

Security Policy Usage セクションには、セキュリティーポリシーの一致数が表示されます。これに応じて、セキュリティーポリシーの設定をカスタマイズできます。

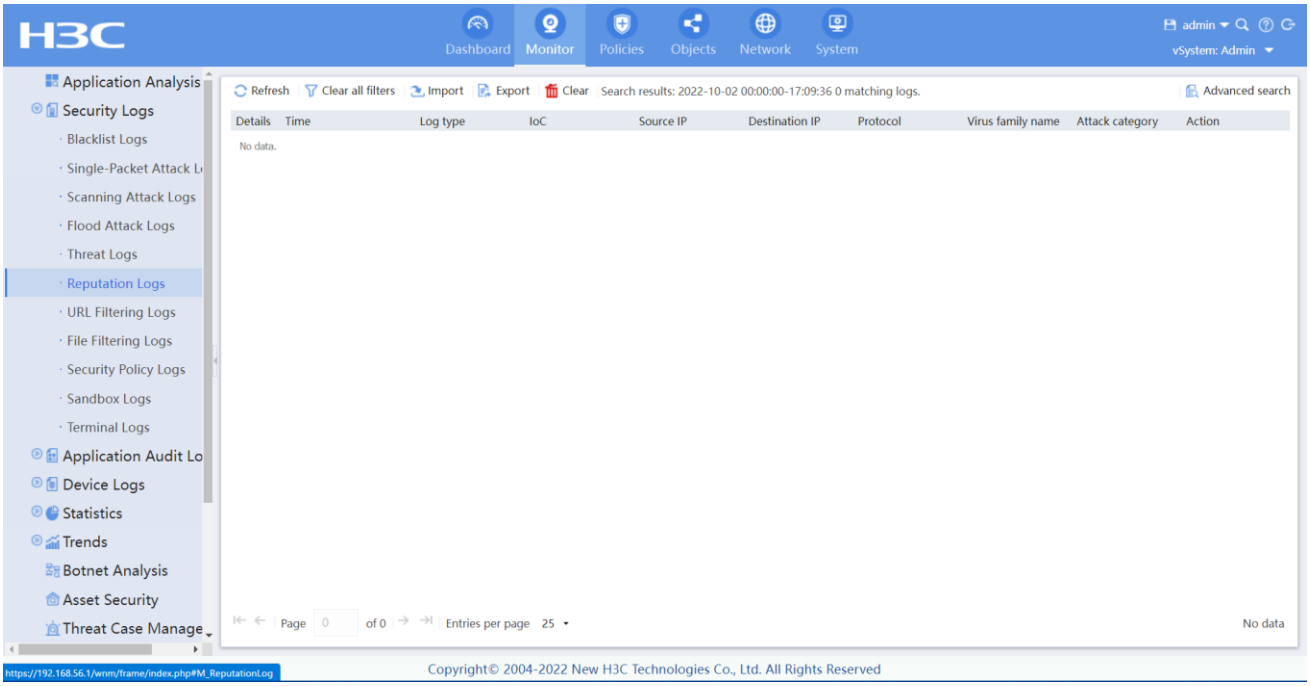
Threat activity

Threat Activity セクションには、脅威イベントの統計情報が表示されます。脅威防御の設定をカスタマイズできます。

WAF activity

WAF activity セクションには、WAF の攻撃イベントの統計情報が表示されます。WAF の防御設定をカスタマイズできます。

Reputation logs



このヘルプには、次のトピックが含まれています。

- Introduction
- Restrictions and guidelines
- Configuration guidelines
  - Import reputation logs
  - Export reputation logs

Introduction

Reputation Logs ページには、IP レピュテーション、URL レピュテーション、およびドメインレピュテーションの各モジュールによって生成されたログが表示されます。

IP レピュテーション、URL レピュテーション、およびドメインレピュテーションを設定する場合、必要に応じてロギング機能をイネーブルにできます。たとえば、ドメインレピュテーションモジュールで攻撃カテゴリのロギングをイネーブルにできます。次に、攻撃カテゴリに属するドメイン名を持つパケットを受信した場合、デバイスはログを生成します。

Restrictions and guidelines

- 一度に許可されるログ操作(インポート、エクスポート、または削除)は 1 つだけです。
- 一度に 1 人のユーザーのみがログ操作を実行できます。ログをインポート、エクスポートまたは削除するときは、他のユーザーがログ操作を実行していないことを確認してください。

Configuration guidelines

Import reputation logs

1. **Monitor** タブをクリックします。
2. ナビゲーションペインで、**Security Logs > Reputation Logs** を選択します。
3. **Import** をクリックします。
4. 表示されたダイアログボックスで、**Yes** をクリックします。
5. ログファイルを選択し、ログファイルのパスワードを入力します。パスワードは、ファイルがエクスポートされたときに設定されました。
6. **OK** をクリックします。

Export reputation logs

1. **Monitor** タブをクリックします。
2. ナビゲーションペインで、**Security Logs > Reputation Logs** を選択します。
3. **Advanced search** をクリックします。
4. 表示されたページで、エクスポートするログをフィルタするための検索基準を指定します。
5. **export** をクリックします。
6. 表示されたページで、ログエクスポートの設定を行います。

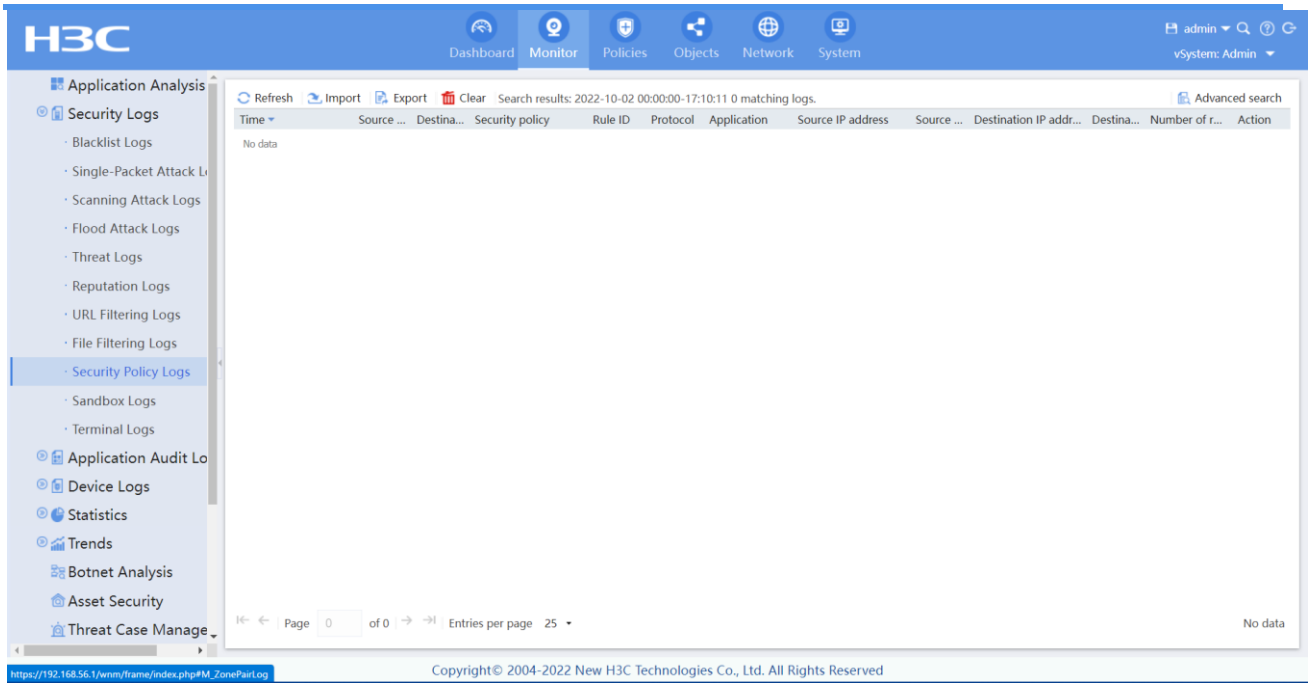
表 1 ログエクスポートの設定項目

項目	説明
Set password	ログファイルを暗号化するためのパスワードを入力します。このパスワードは、エクスポートされたログファイルを表示またはインポートするときに必要です。
Log range	エクスポートするログの範囲を指定します。オプションは次のとおりです: • **All result**: 検索基準を満たすすべてのログをエクスポートします。このページには、エクスポートされるログの合計数が表示されます。 • **Day on the current page**: カレントページの **Time** フィールドで示された日のログをエクスポートします。終了ページを定義して、エクスポートするログの数を減らすことができます。

7. 次のいずれかのエクスポート方法を選択します。
   - **Export to one file**: ログを 1 つのファイルにエクスポートします。エクスポートするログの数が少ない場合は、この方法を選択します。
   - **Export to files**: ログを複数のファイルにエクスポートします。エクスポートするログが 65000 個を超える場合は、この方法を選択します。
8. 必要に応じて、次のいずれかのタスクを実行します。
   - **Export to one file** を選択した場合は、表示されるダイアログボックスで **OK** をクリックします。
   - **Export to files** を選択した場合は、各ファイルにエクスポートするログの数を指定し、表示されたダイアログボックスで **OK** をクリックします。

     1 つのファイルへのログのエクスポートが完了すると、ダイアログボックスが開き、残りのログを新しいファイルにエクスポートし続けるかどうかを確認するメッセージが表示されます。
     - エクスポートを続行するには、**yes** をクリックします。
     - エクスポート処理を停止するには、**No** をクリックします。

Security policy logs



このヘルプには、次のトピックが含まれています。

- Introduction
- Restrictions and guidelines
- Manage security policy logs
  - Import logs
  - Export logs

Introduction

この機能を使用すると、システムはセキュリティーポリシー規則に一致する各パケットのセキュリティーポリシーログエントリを生成できます。これにより、管理者はユーザーの動作を監査し、ネットワークのトラブルシューティングを実行できます。

Restrictions and guidelines

- 一度に許可されるログ操作(インポート、エクスポート、または削除)は 1 つだけです。
- 一度に 1 人のユーザーのみがログ操作を実行できます。ログをインポート、エクスポートまたは削除するときは、他のユーザーがログ操作を実行していないことを確認してください。

Manage security policy logs

Import logs

1. クライアントの **Monitor** タブ。
2. ナビゲーションペインで、**Security Logs > Security Policy Logs** を選択します。
3. **Import** をクリックします。
4. 表示されたダイアログボックスで、**Yes** をクリックします。
5. ログファイルを選択し、ログファイルのパスワードを入力します。パスワードは、ファイルがエクスポートされたときに設定されました。

Export logs

1. クライアントの **Monitor** タブ。
2. ナビゲーションペインで、**Security Logs > Security Policy Logs** を選択します。
3. **Advanced search** をクリックします。
4. 表示されたページで、エクスポートするログを表示するための検索条件を指定します。
5. **export** をクリックします。
6. 表示されたページで、ログエクスポートの設定を行います。

表 1 ログエクスポートの設定項目

項目	説明
Set password	ログファイルを暗号化するためのパスワードを入力します。このパスワードは、エクスポートされたログファイルを表示またはインポートするときに必要です。
Log range	エクスポートするログの範囲を指定します。オプションは次のとおりです: • **All results**: 検索基準を満たすすべてのログをエクスポートします。このページには、エクスポートされるログの合計数が表示されます。 • **Day on the current page**: **Time** フィールドで示された日のログをエクスポートします。終了ページを定義して、エクスポートするログの数を減らすことができます。

7. 次のいずれかのエクスポート方法を選択します。

○ **Export to one file**: ログを 1 つのファイルにエクスポートします。エクスポートするログの数が少ない場合は、この方法を選択します。

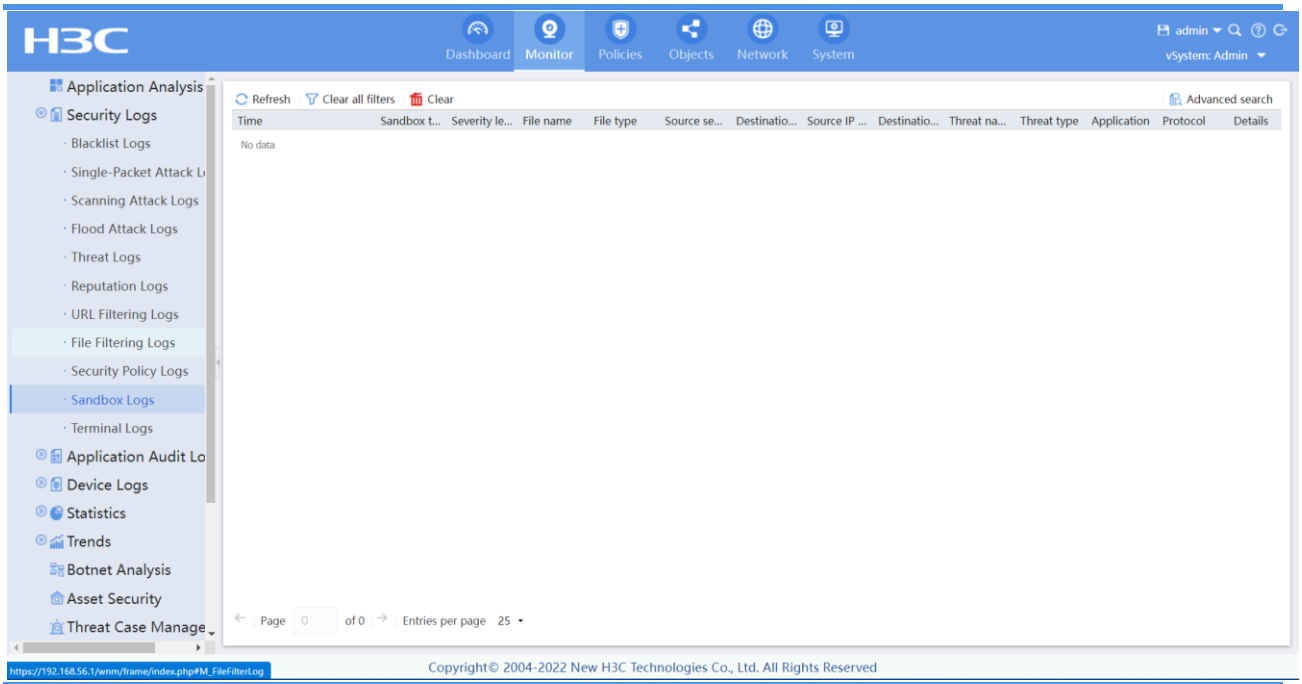
1 つのログファイルに最大 65000 個のログをエクスポートできます。

- **Export to files**: ログを複数のファイルにエクスポートします。エクスポートするログが 65000 個を超える場合は、この方法を選択します。

8. 必要に応じて、次のいずれかのタスクを実行します。
   - **Export to one file** を選択した場合は、表示されるダイアログボックスで **OK** をクリックします。
   - **Export to files** を選択した場合は、各ファイルにエクスポートするログの数を指定し、表示されたダイアログボックスで **OK** をクリックします。

     1 つのファイルへのログのエクスポートが完了すると、ダイアログボックスが開き、残りのログを新しいファイルにエクスポートし続けるかどうかを確認するメッセージが表示されます。
     - エクスポートを続行するには、**yes** をクリックします。
     - エクスポート処理を停止するには、**no** をクリックします。

Sandbox logs



Introduction

サンドボックスログには、パケットと検査されたファイルの基本情報、およびこれらのファイルで検出された脅威など、サンドボックス検査結果が記録されます。

脅威ファミリフィールドと脅威アクションフィールドの値の詳細については、「Appendix」を参照してください。

Restrictions and guidelines

サンドボックスログの詳細情報は、JSON 形式でのみ表示されます。

Appendix のフィールド値は、サンドボックスのソフトウェアバージョンによって異なります。

Appendix

表 1 脅威ファミリフィールドの値

識別番号	脅威ファミリ
0	その他

1	ウィルス
2.	トロイの木馬
3.	ワーム
4.	バックドア
5.	ランサムウェア
6.	ダウンローダ
7.	悪意のある広告
8.	悪意のあるスクリプト
9	マクロウィルス
10	脆弱性を持つ悪意のあるファイル
11.	フィッシング
12	リスクウェア
13.	シェルソフトウェア
14.	ヒューリスティックな動作
15.	電子貨幣
16	ボットネット
17.	APT 情報
18.	悪意のある DGA ドメイン名

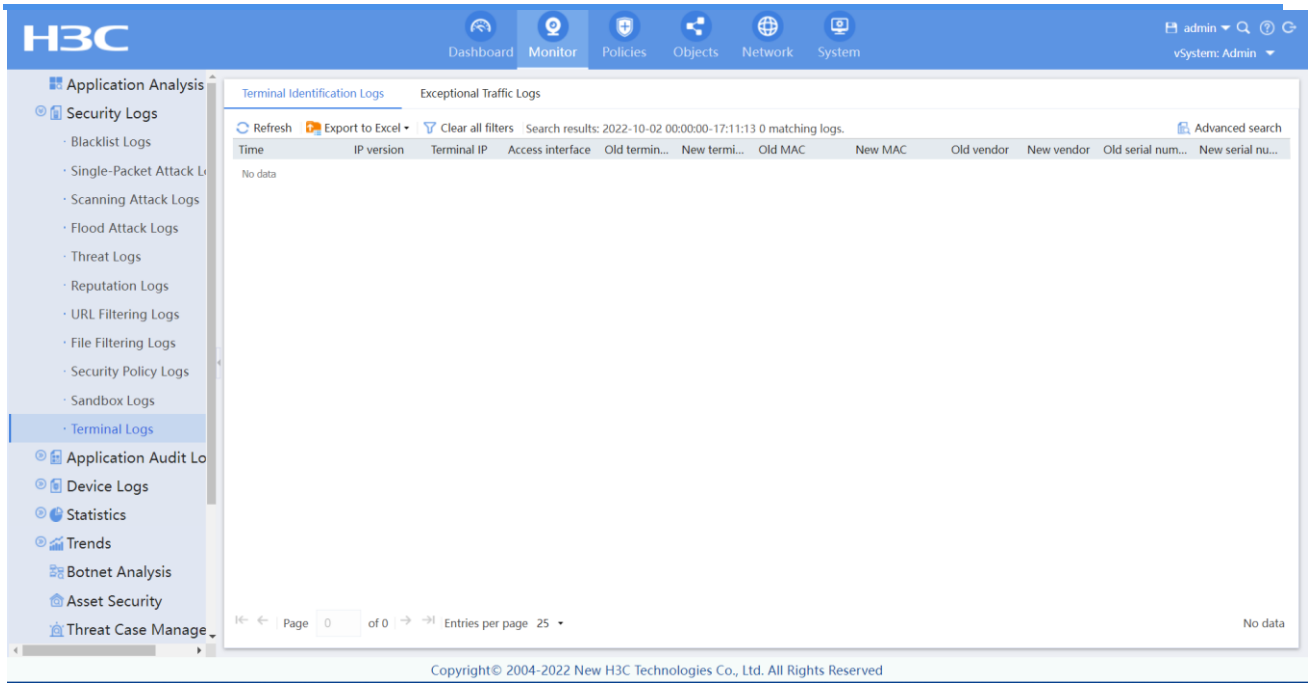
表 2:脅威行為フィールドの値

識別番号	脅威アクション
1	デバイスの起動後に自動実行を有効にします。
2.	他のプロセスにリモートでインジェクトする。
3.	ファイアウォールのセキュリティーレベルを下げるか、ホワイトリストエントリーを追加します。
4.	ユーザーカウント制御(UAC)をバイパスして、管理者特権を取得します。
5.	システム保護メカニズムを無効にします。
6.	アンチウィルスソフトウェアがシステムにインストールされているか実行されているかを検出します。
7.	ファイルがサンドボックス内で実行されるか、デバッガによってデバッグされるかを検出します。
8.	ローカルファイルを削除します。
9	DLL ハイジャックまたはイメージハイジャック。
10	ファイルを EXE ファイルまたは DLL ファイルに置き換えます。
11.	このファイルは、偽造のキープロセスに似た名前を使用しています。
12	既存の PE ファイルを感染させます。
13.	ドライバをロードします。
14.	IE ブラウザのセキュリティーポリシーを変更します。
15.	Windows アカウントを追加または変更します。
16	Windows サービスを追加または変更します。
17.	ネットワーク接続が疑わしい。
18.	疑わしいプロセスを作成し、疑わしいファイルをリリースします。

19	実行可能プログラムをリリースします。
20	自動シャットダウン、自動再起動、または自動ログアウト
21	PE ファイルの実行により、スクリプトファイルがリリースされます。
22	hosts ファイルを変更します。
23	プログラムの主要機能をフックします。
24	プログラムの権限を昇格します。
25	スクリプトファイルは PowerShell を使用します。
26	スクリプトファイルの不正なネットワーク動作。
27	ブラウザのユーザー名とパスワードが保存されているファイルなど、機密性の高いファイルにアクセスします。
28	Android ソフトを利用すると通話料金がかかります。
29	Android ソフトウェア上の悪意のある広告。
30	Android ソフトウェアはユーザーのプライバシーを盗みます。
31	ファイルの偽装
32	ファイルの隠し属性を変更します。
33	実行可能ファイルの悪意のあるネットワーク動作。
34	悪意のあるショートカットファイル
35.	疑わしいマクロウィルス
200	ウィルス
201	スパイウェア
202	ワーム

203	バックドア
204	ランサムウェア
205	ダウンローダ
206	悪意のある広告
207	悪意のあるスクリプト
208	脆弱性を持つ悪意のあるファイル
209	ウィルス発生器
210	シェルソフトウェア
211	ヒューリスティックな動作
212	リスクウェア
213	フィッシング
214	マクロウィルス
215	その他の脅威の種類

Terminal logs



Introduction

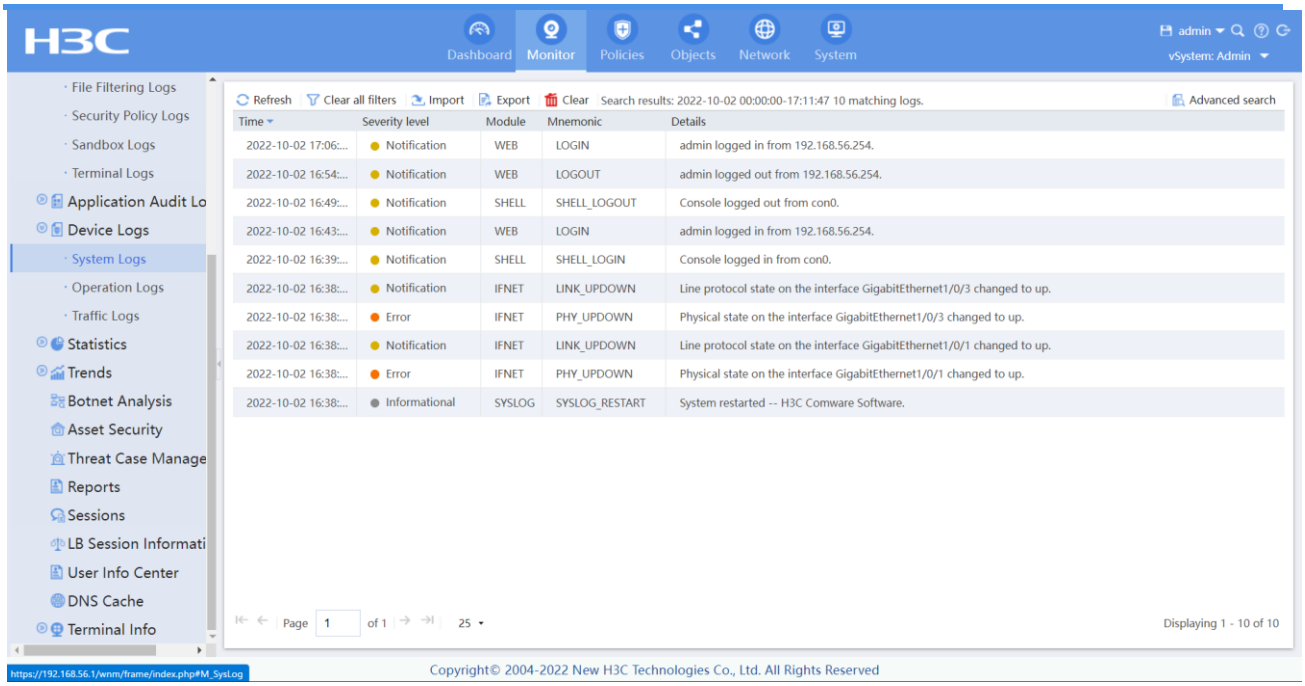
Terminal identification logs

端末識別ログには、端末 ID、IP アドレス、アクセスインターフェース、MAC アドレスなど、識別された端末に関する詳細情報が記録されます。

Traffic abnormality logs

トラフィック異常ログは、1 分間に端末の最高帯域幅が帯域幅上限を超えた場合、または最低帯域幅が帯域幅下限を下回った場合に記録されます。

System logs



このヘルプには、次のトピックが含まれています。

- Introduction
- Restrictions and guidelines
- Manage system logs
  - Import logs
  - Export logs

Introduction

System Logs ページには、デバイスシステムの実行中に生成されたログメッセージが記録されます。システムログメッセージは、システムのトラブルシューティングおよびメンテナンスに役立ちます。システムログメッセージを表示することで、デバイスの実行プロセスを把握し、ネットワーク条件を分析し、障害を特定できます。

Restrictions and guidelines

- 一度に許可されるログ操作(インポート、エクスポート、または削除)は 1 つだけです。
- 一度に 1 人のユーザーのみがログ操作を実行できます。ログをインポート、エクスポートまたは削除するときは、他のユーザーがログ操作を実行していないことを確認してください。

Manage system logs

Import logs

1. **monitor** タブをクリックします。
2. ナビゲーションペインで、**Device Logs > System Logs** を選択します。
3. **import** をクリックします。
4. 表示されたダイアログボックスで、**yes** をクリックします。
5. ログファイルを選択し、ログファイルのパスワードを入力します。パスワードは、ファイルがエクスポートされたときに設定されました。

Export logs

1. **Monitor** タブをクリックします。
2. ナビゲーションペインで、**Device Logs > System Logs** を選択します。
3. **Advanced search** をクリックします。
4. 表示されたページで、エクスポートするログを表示するための検索条件を指定します。
5. **export** をクリックします。
6. 表示されたページで、ログエクスポートの設定を行います。

表 1 ログエクスポートの設定項目

項目	説明
Set password	ログファイルを暗号化するためのパスワードを入力します。このパスワードは、エクスポートされたログファイルを表示またはインポートするときに必要です。
Log range	エクスポートするログの範囲を指定します。オプションは次のとおりです: • **All results**: 検索基準を満たすすべてのログをエクスポートします。このページには、エクスポートされるログの合計数が表示されます。 • **Day on the current page**: **Time** フィールドで示された日のログをエクスポートします。終了ページを定義して、エクスポートするログの数を減らすことができます。

7. 次のいずれかのエクスポート方法を選択します。
   - **Export to one file**: ログを 1 つのファイルにエクスポートします。エクスポートするログの数が少ない場合は、この方法を選択します。
     1 つのログファイルに最大 65000 個のログをエクスポートできます。
   - **Export to files**: ログを複数のファイルにエクスポートします。エクスポートするログが 65000 個を超える場合は、この方法を選択します。

8. 必要に応じて、次のいずれかのタスクを実行します。

- **Export to one file** を選択した場合は、表示されるダイアログボックスで **OK** をクリックします。
- **Export to files** を選択した場合は、各ファイルにエクスポートするログの数を指定し、表示されたダイアログボックスで **OK** をクリックします。

  1 つのファイルへのログのエクスポートが完了すると、ダイアログボックスが開き、残りのログを新しいファイルにエクスポートし続けるかどうかを確認するメッセージが表示されます。

  - エクスポートを続行するには、**yes** をクリックします。
  - エクスポート処理を停止するには、**no** をクリックします。

Configuration logs

このヘルプには、次のトピックが含まれています。

- Introduction
- Restrictions and guidelines
- Manage configuration logs
  - Import logs
  - Export logs

Introduction

このページには、デバイスで実行された構成操作が表示されます。この情報を使用して、管理者の操作の追跡、管理者の動作の監査およびデバイスのトラブルシューティングを行うことができます。

Restrictions and guidelines

- 一度に許可されるログ操作(インポート、エクスポート、または削除)は 1 つだけです。
- 一度に 1 人のユーザーのみがログ操作を実行できます。ログをインポート、エクスポートまたは削除するときは、他のユーザーがログ操作を実行していないことを確認してください。

Manage configuration logs

Import logs

1. **monitor** タブをクリックします。
2. ナビゲーションペインで、**Device Logs > Configuration Logs** を選択します。
3. **Import** をクリックします。
4. 表示されたダイアログボックスで、**Yes** をクリックします。
5. ログファイルを選択し、ログファイルのパスワードを入力します。パスワードは、ファイルがエクスポートされたときに設定されました。

Export logs

1. **monitor** タブをクリックします。
2. ナビゲーションペインで、**Device Logs > Configuration Logs** を選択します。

3. **Advanced search** をクリックします。
4. 表示されたページで、エクスポートするログを表示するための検索条件を指定します。
5. **export** をクリックします。
6. 表示されたページで、ログエクスポートの設定を行います。

表 1 ログエクスポートの設定項目

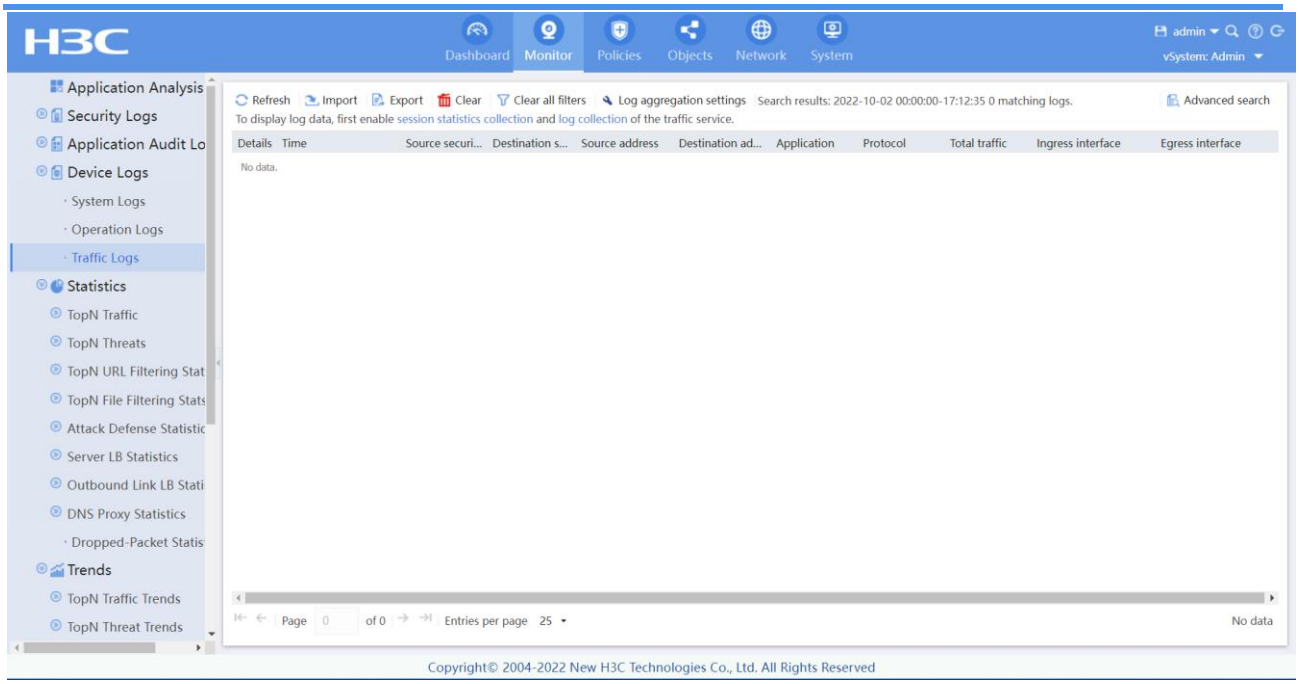
項目	説明
Set password	ログファイルを暗号化するためのパスワードを入力します。このパスワードは、エクスポートされたログファイルを表示またはインポートするときに必要です。
Log range	エクスポートするログの範囲を指定します。オプションは次のとおりです: • **All results**: 検索基準を満たすすべてのログをエクスポートします。このページには、エクスポートされるログの合計数が表示されます。 • **Day on the current page** の **Time** フィールドで示された日のログをエクスポートします。終了ページを定義して、エクスポートするログの数を減らすことができます。

7. 次のいずれかのエクスポート方法を選択します。
   - **Export to one file**: トログを 1 つのファイルにエクスポートします。エクスポートするログの数が少ない場合は、この方法を選択します。

     1 つのログファイルに最大 65000 個のログをエクスポートできます。
   - **Export to files**: トログを複数のファイルにエクスポートします。エクスポートするログが 65000 個を超える場合は、この方法を選択します。
8. 必要に応じて、次のいずれかのタスクを実行します。
   - **Export to one file** を選択した場合は、表示されるダイアログボックスで **OK** をクリックします。
   - **Export to files** を選択した場合は、各ファイルにエクスポートするログの数を指定し、表示されたダイアログボックスで **OK** をクリックします。

     1 つのファイルへのログのエクスポートが完了すると、ダイアログボックスが開き、残りのログを新しいファイルにエクスポートし続けるかどうかを確認するメッセージが表示されます。
     - エクスポートを続行するには、**yes** をクリックします。
     - エクスポート処理を停止するには、**no** クリックします。

Traffic logs



Introduction

このページには、フロー単位でトラフィック情報が表示されます。管理者は、トラフィックログに従って適切な帯域幅制限ポリシーを適用できます。

トラフィックログを表示するには、**System > Session Aging Time Settings > Advanced Setting** ページでセッション統計情報の収集をイネーブルにする必要があります。

Restrictions and guidelines

- 一度に許可されるログ操作(インポート、エクスポート、または削除)は 1 つだけです。
- 一度に 1 人のユーザーのみがログ操作を実行できます。ログをインポート、エクスポートまたは削除するときは、他のユーザーがログ操作を実行していないことを確認してください。

Manage traffic logs

Import logs

1. **monitor** タブをクリックします。
2. ナビゲーションペインで、**Device Logs > Traffic Logs** を選択します。
3. **Import** をクリックします。

4. 表示されたダイアログボックスで、**yes** をクリックします。
5. ログファイルを選択し、ログファイルのパスワードを入力します。パスワードは、ファイルがエクスポートされたときに設定されました。

Export logs

1. **monitor** タブをクリックします。
2. ナビゲーションペインで、**Device Logs > Traffic Logs** を選択します。
3. **Advanced search** をクリックします。
4. 表示されたページで、エクスポートするログを表示するための検索条件を指定します。
5. **export** をクリックします。
6. 表示されたページで、ログエクスポートの設定を行います。

表 1 ログエクスポートの設定項目

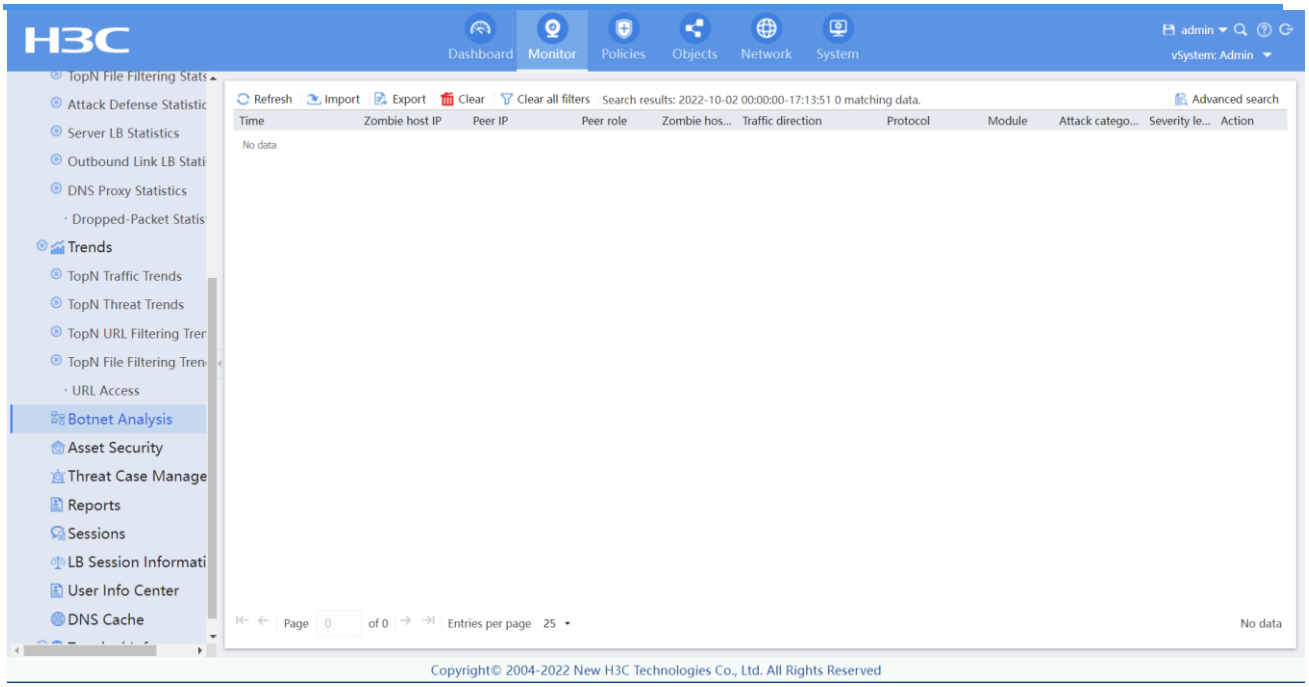
項目	説明
Set password	ログファイルを暗号化するためのパスワードを入力します。このパスワードは、エクスポートされたログファイルを表示またはインポートするときに必要です。
Log range	エクスポートするログの範囲を指定します。オプションは次のとおりです: • **All results**: 検索基準を満たすすべてのログをエクスポートします。このページには、エクスポートされるログの合計数が表示されます。 • **Day on the current page**: **Time** フィールドで示された日のログをエクスポートします。終了ページを定義して、エクスポートするログの数を減らすことができます。

7. 次のいずれかのエクスポート方法を選択します。
   - **Export to one file**: トログを 1 つのファイルにエクスポートします。エクスポートするログの数が少ない場合は、この方法を選択します。
     1 つのログファイルに最大 65000 個のログをエクスポートできます。
   - **Export to files**: ログを複数のファイルにエクスポートします。エクスポートするログが 65000 個を超える場合は、この方法を選択します。
8. 必要に応じて、次のいずれかのタスクを実行します。
   - **Export to one file** を選択した場合は、表示されるダイアログボックスで OK をクリックします。
   - **Export to files** を選択した場合は、各ファイルにエクスポートするログの数を指定し、表示されたダイアログボックスで **OK** をクリックします。

1 つのファイルへのログのエクスポートが完了すると、ダイアログボックスが開き、残りのログを新しいファイルにエクスポートし続けるかどうかを確認するメッセージが表示されます。

- エクスポートを続行するには、**yes** をクリックします。
- エクスポート処理を停止するには、**no** をクリックします。

Botnet analysis



このヘルプには、次のトピックが含まれています。

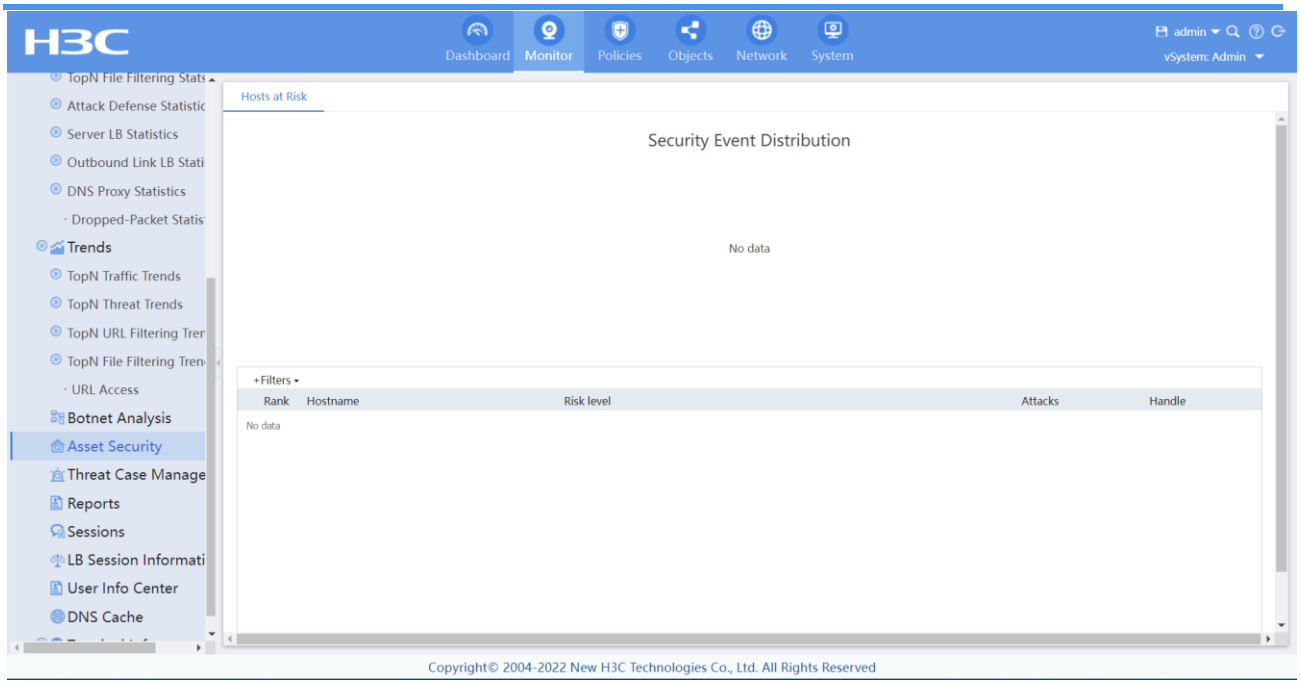
- Introduction

Introduction

デバイスは、ボットネットに関連するすべてのセキュリティーログを分析し、ゾンビホストである可能性のあるホストに関する情報(ホストおよびピアホストの IP など)の表示をサポートします。この機能は、ゾンビホストを識別して検出し、防止アクションを実行するのに役立ちます。

この機能のサポートは、デバイスモデルによって異なります。

Asset security



このヘルプには、次のトピックが含まれています。

- Introduction
- Restrictions and guidelines
- Configure asset security
- Appendix

Introduction

デバイスは、ダウンストリームホストのヘルスステータスを分析し、障害が発生したホストの数とセキュリティーイベントの分布をグラフおよび表に表示できます。ダウンストリームホストのセキュリティーステータスのサマリーと、単一ホストの詳細なセキュリティー分析レポートを表示できます。したがって、資産セキュリティー情報に基づいて防止アクションを実行できます。

Restrictions and guidelines

- この機能のサポートは、デバイスモデルによって異なります。
- 単一ホストの詳細セキュリティー分析レポートには、過去半年間の統計情報のみが表示されます。
- デバイスは、Controlled リスクレベル以上のホストについてのみ、詳細なセキュリティー分析レポートを生成します。

Configure asset security

1. **monitor** タブをクリックします。
2. ナビゲーションペインで、**Asset security** を選択します。

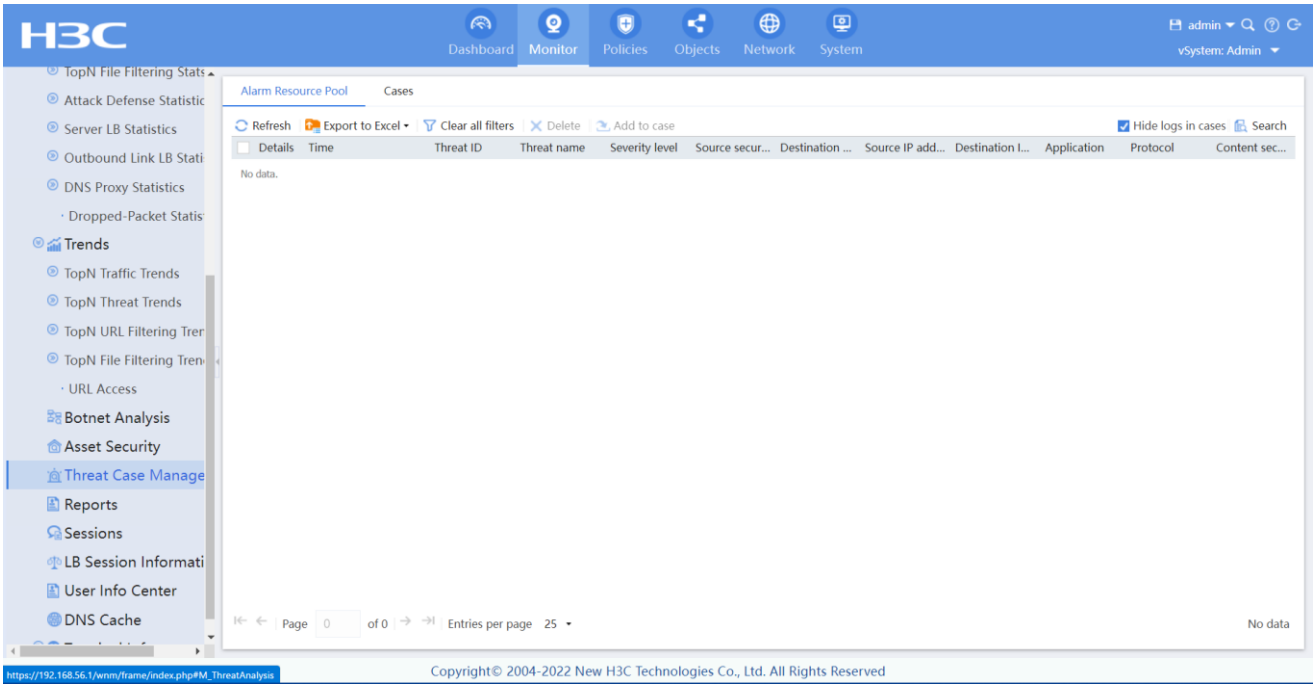
   このページには、**Hosts at risk** タブにホストのセキュリティーサマリーが表示されます。リスクレベルの詳細は、「Appendix」を参照してください。
3. 1 つのホストの詳細なセキュリティー分析レポートを表示するには、テーブルでホスト名をクリックします。

Appendix

表 1 リスクレベルの説明

リスクレベル	説明
Vulnerable	ホストで脆弱性が検出されました。ホストは攻撃されていません。たとえば、脆弱性スキャンによって、ホストで脆弱なポート 138 および 139 が開いていることが検出された可能性があります。
Attacked	ホストで悪意のある攻撃が検出されました。たとえば、ホストで DDoS 攻撃、SQL インジェクション攻撃、またはボットが発生する可能性があります。
Controlled	ホストで異常なアウトリーチ行動が検出されました。たとえば、ホストが C&C サーバーと通信したか、既知のマルウェアまたはワームに関連付けられた IP、URL、またはドメイン名と通信した可能性があります。
Spread	ホストから他のホストへの攻撃が検出されました。たとえば、ホストがポートスキャンや他のホストへのブルートフォース攻撃を開始した可能性があります。
Damaged	ホストでファイルリークが検出されたか、または他のホストやデータベースへの脅威が検出されました。例えば、マイニングやランサムウェアウィルスが存在する可能性があります。

Threat Case Management



Introduction

脅威ケース管理は、デバイスによって生成された脅威ログを管理および分類するために使用されます。デバイスは、脅威ログを保存するためのアラームリソースプールを提供し、ユーザーがログ管理を容易にするためにログをケースに追加できるようにします。

脅威事例を管理するには:

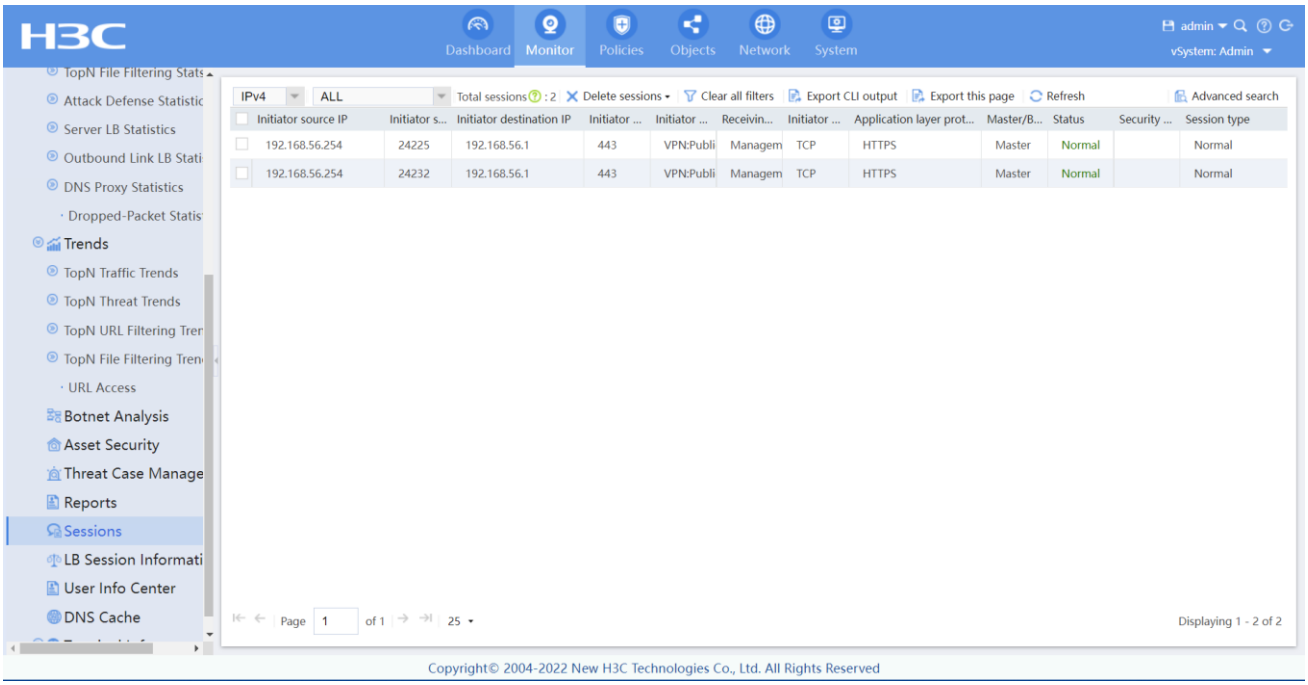
1. **Monitor** タブをクリックします。
2. ナビゲーションペインで、Security Logs > Threat Logs を選択します。ターゲットログを選択し、**Add to alarm resource pool** をクリックします。
3. ナビゲーションペインで、**Threat Case Management** を選択します。**Alarm Resource Pool** タブをクリックして、脅威分析のログを表示します。
4. ケースにログを追加するには、ターゲットログを選択し、**Add to case** をクリックして、選択したログをケースに追加します。

Cases タブでは、次の脅威ログ管理タスクを実行できます。

- ケースをアーカイブするには、次のいずれかのタスクを実行できます。
  - ケースを選択し、ケースエントリの **Edit** アイコン をクリックします。表示されるダイアログボックスで、**status** フィールドから **archived** を選択します。
  - ケースを選択し、ケースエントリの **logs** をクリックします。開いたダイアログボックスで、**archived** をクリックします。次に、**Yes** をクリックして操作を確認します。

- サポートリクエストの詳細を表示するには、サポートリクエストエントリの **Logs** をクリックします。表示されるダイアログボックスで、ログエントリの **Details** アイコンをクリックしてログの詳細を表示することもできます。
- ケースを編集するには、ケースエントリの **Edit** アイコン  をクリックします。表示されるダイアログボックスで、ケースのステータスを編集するか、必要に応じてケースからログを削除します。

Session list



このヘルプには、次のトピックが含まれています。

- Introduction

Introduction

Session List ページには、データフローの 5 タプル情報、一致するセキュリティーポリシーおよびアプリケーションなど、各データフローの詳細情報が記録されます。このページには、セッション停止機能もあります。セッションを停止するには、**Status** 列の **Normal** をクリックします。停止されたセッションのパケットはすべてドロップされます。

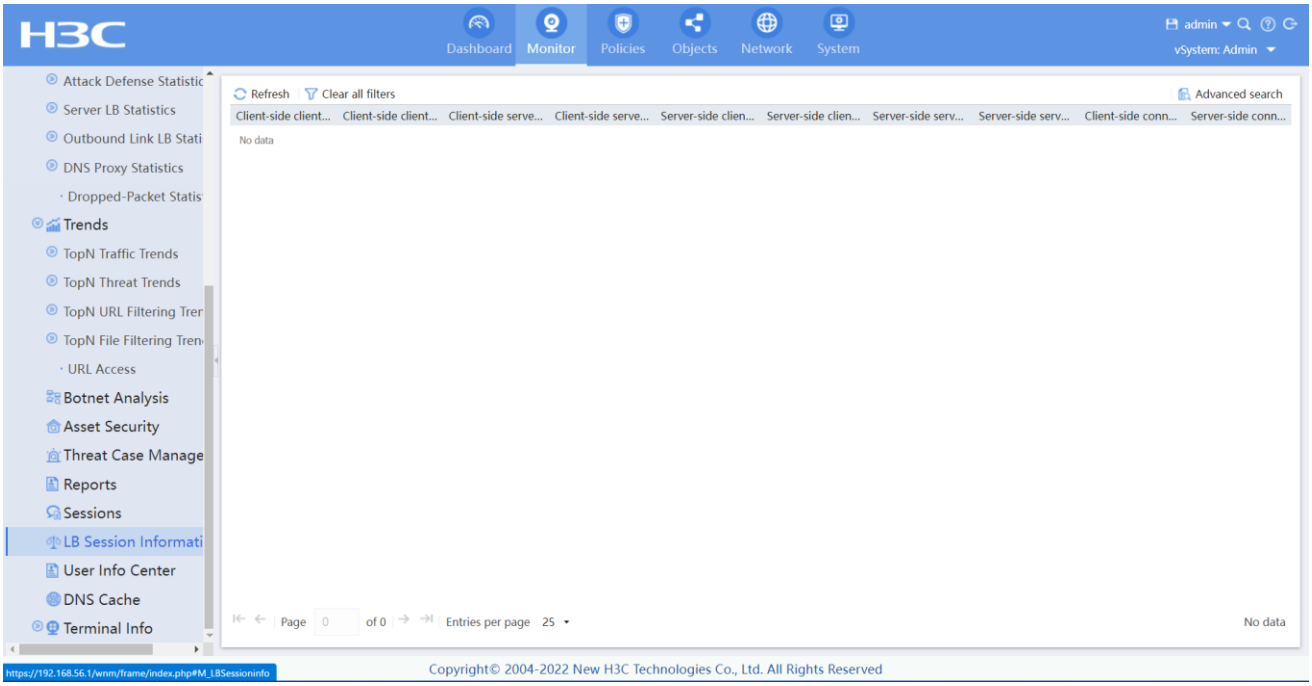
セッションのマスター/バックアップステータスの値には、以下が含まれます。

- **Master**: セッションは現在のデバイスで作成されます。
- **backup**: セッションは他のデバイスから同期化されます。

Restrictions and guidelines

Export CLI Output をクリックすると、最大 1000 セッションをエクスポートできます。

LB session information



Introduction

表 1 は、レイヤー7 サーバーロードバランシングの TCP 接続情報を示しています。

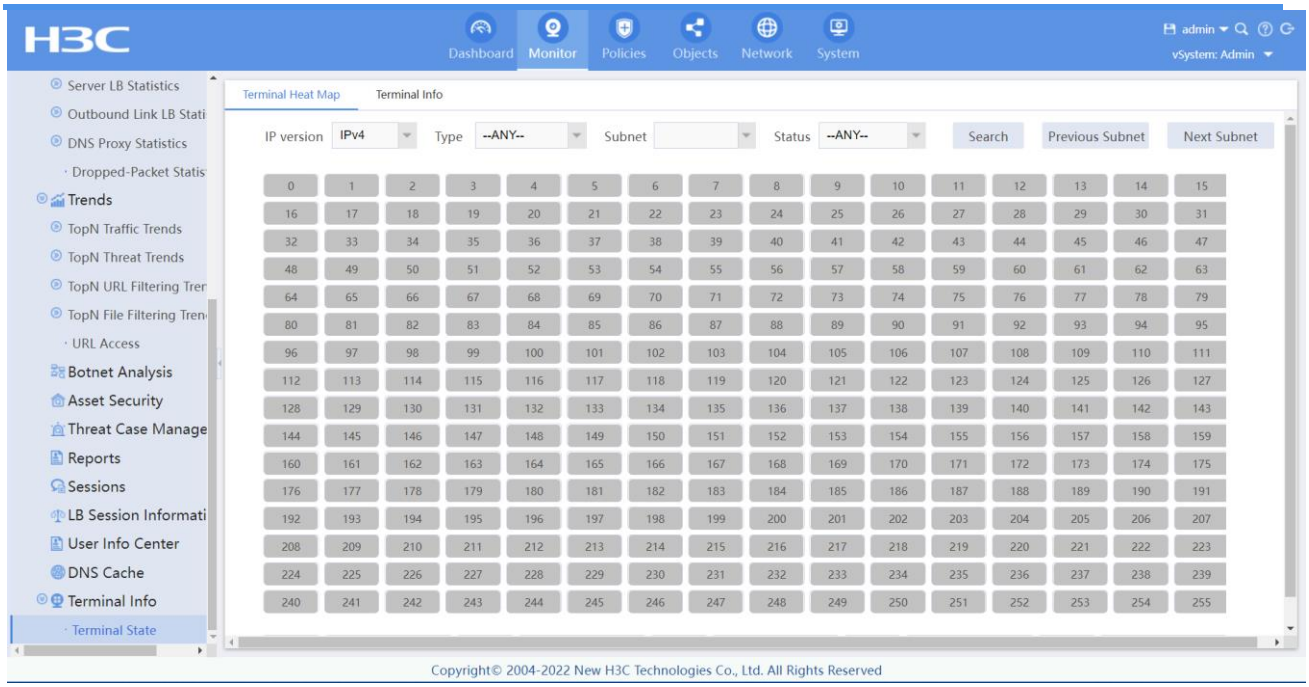
表 1 LB セッション情報

項目	説明
Client-side client IP	デバイスへの TCP 接続を確立するために使用されるクライアント側クライアント IP アドレス。
Client-side client port	デバイスへの TCP 接続を確立するために使用されるクライアント側のクライアントポート番号。
Client-side server IP	デバイスへの TCP 接続を確立するために使用するクライアント側サーバーの IP アドレス。
Client-side server port	デバイスへの TCP 接続を確立するために使用されるクライアント側サーバーのポート番号。
Server-side client IP	サーバーへの TCP 接続を確立するために使用されるサーバー側クライアントの IP アドレス。
Server-side client port	サーバーへの TCP 接続を確立するために使用されるサーバー側クライアントポート番号。

Sever-side server IP	サーバーへの TCP 接続を確立するために使用されるサーバー側サーバーの IP アドレス。
Sever-side server port	サーバーへの TCP 接続を確立するために使用されるサーバー側サーバーのポート番号。
Client-side connection state	クライアントとデバイス間の TCP 接続の状態。 • CLOSED • LISTENING • SYN_SENT • SYN_RECEIVED • ESTABLISHED • CLOSE_WAIT • FIN_WAIT_1 • CLOSING • LAST_ACK • FIN_WAIT_2 • TIME_WAIT
Server-side connection state	デバイスとサーバー間の TCP 接続の状態: • CLOSED • LISTENING • SYN_SENT • SYN_RECEIVED • ESTABLISHED • CLOSE_WAIT • FIN_WAIT_1 • CLOSING • LAST_ACK

	• FIN_WAIT_2 • TIME_WAIT

Terminal status



このヘルプには、次のトピックが含まれています。

- Introduction
  - Terminal heat map
  - Terminal information
- Restrictions and guidelines

Introduction

Terminal heat map

ターミナルヒートマップでは、各ネットワークセグメントの各ターミナルの状態が視覚的に表示されます。ターミナル状態には、正常、異常または到達不能があります。ターミナル状態またはブロック状態でターミナルを検索できます。ターミナルの IP アドレスをクリックして、ターミナルをブロックできます。ブロックされたターミナルは、ブロック期間が終了するかブロックを解除するまでネットワークにアクセスできません。

末端ヒートマップは、異なる状態を表現するために異なる色を使用する。

- **Unused(グレー)**: デバイスは、IP アドレスを使用する端末からのトラフィックを検出しません。
- **Normal(グリーン)**: デバイスは端末からのトラフィックを検出しました。トラフィックは帯域幅下限と帯域幅上限の間にあります。
- **Abnormal(オレンジ)**: 端末は異常な状態です。次のような状況が発生しています。

- **Poorly connected**: 端末からのトラフィックが帯域幅下限を下回っています。
- **Illegally used**: 端末の IP アドレスが別の不正な端末によって使用されています。デバイスは、端末情報が変化したときにこの状況を検出します。

- **Unreachable(赤)**: デバイスは端末からのトラフィックを検出しましたが、その後トラフィックを検出できません。この状態は 7 日間保持されると **Unused** 状態に移行します。
- **Blocked(紫)**: 端末の IP アドレスは管理上ブロックされています。

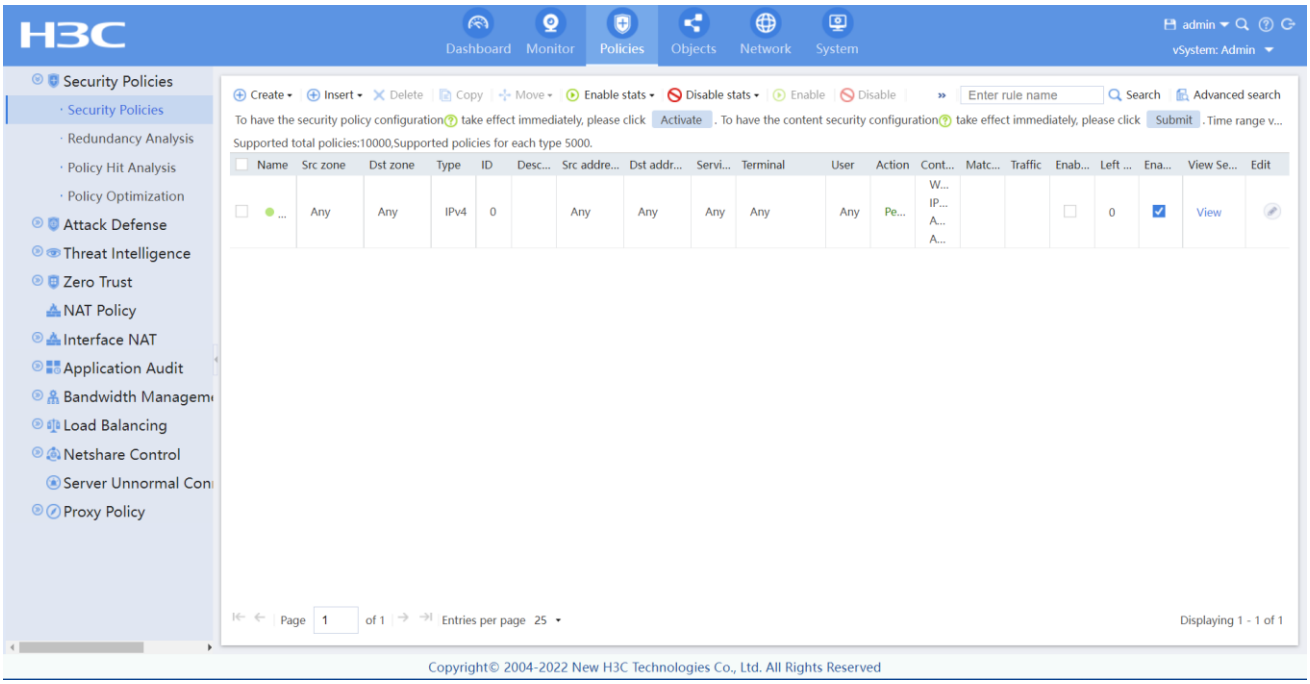
Terminal information

このセクションには、監視目的ですべての端末の情報と状態が表示されます。端末の MAC アドレス、製造元、およびモデル情報を監視することで、IP アドレスの不正使用や不正交換を防ぐことができます。**Unblocked** または **Blocked** をクリックして、端末をブロックまたはブロック解除することもできます。

Restrictions and guidelines

block 機能を使用できるのは、**Policies > Attack Defense > Blacklist** ページで **Enable globally** をクリックした場合だけです。

Security policy



このヘルプには、次のトピックが含まれています。

- Introduction
  - Security policy name
  - Security policy filtering criteria
  - Security policy matching order
  - Policy matching acceleration
  - Security policy group
  - Import and export
- Restrictions and guidelines
  - Restrictions and guidelines: Security policies
  - Restrictions and guidelines: Security policy groups
  - Restrictions and guidelines: Import and export
- Configure security policies
  - Create a security policy
  - Insert a security policy
  - Create a security policy group

Introduction

セキュリティーポリシーでは、トラフィックを識別するための一連のフィルタリング基準を定義します。フィルタリング基準には、送信元セキュリティーゾーン、宛先セキュリティーゾーン、送信元 IP アドレスと送信元 MAC アドレス、宛先 IP アドレス、ユーザー、アプリケーション、端末、サービス、VRF、および時間範囲のタイプが含まれます。デバイスはパケットをセキュリティーポリシーと照合し、一致したパケットに対してポリシーに記述されているアクションを実行します。セキュリティーポリシーと一致しないパケットは廃棄されます。ポリシーに基準が指定されていない場合、ポリシーはすべてのパケットと一致します。

Security policy name

複数のセキュリティーポリシーを設定できます。各ポリシーは、名前とタイプによって一意に識別される必要があります。

Security policy filtering criteria

フィルタリング基準には、送信元セキュリティーゾーン、宛先セキュリティーゾーン、送信元 IP アドレスと送信元 MAC アドレス、宛先 IP アドレス、ユーザー、アプリケーション、端末、サービス、VRF、および時間範囲のタイプが含まれます。
パケットは、ポリシー内のすべての基準タイプと一致する場合、一致したと見なされます。各基準タイプには 1 つ以上の基準が含まれ、パケットが基準タイプのいずれかと一致する場合、そのパケットは基準タイプと一致します。

Security policy matching order

デバイスは、ポリシーが作成された順序でパケットをセキュリティーポリシーと照合します。ポリシー作成時に深度優先の順序に従って、より厳密な一致基準を持つポリシーを最初に作成します。
Policies > Security Policies > Security Policies ページのセキュリティーポリシーは、ポリシー作成順序で表示されます。最初に作成されたポリシーがリストの最初に表示されます。ポリシーを移動して、ポリシーの一致順序を変更できます。

Policy matching acceleration

この機能は、セキュリティーポリシーマッチングを加速して、接続確立とパケット転送のパフォーマンスを向上させます。特に、複数のユーザーからのパケットを照合するために複数のポリシーを使用するデバイスでは、この機能が有効です。
オブジェクトポリシーから切り替えられたセキュリティーポリシーの一致は、デフォルトで加速されます。ポリシーが変更または新規追加された場合、または特定の理由で加速機能が非アクティブになった場

合は、ルールー致の加速をアクティブにする必要があります。ポリシーー致の加速をアクティブにするには、次の方法を使用できます。

- **Manual activation**: **activate** をクリックした直後に、セキュリティーポリシーマッチングアクセラレーションをアクティブ化します。ポリシーが変更された後、またはアクセラレーション機能が非アクティブ化された後に、手動アクティブ化を実行できます。
- **Automatic activation**: システムが特定の間隔でセキュリティーポリシーの変更を検出し、変更が行われた場合にセキュリティーポリシーマッチングアクセラレーションを自動的にアクティブにできるようにします。セキュリティーポリシーの数が 100 以下の場合、間隔は 2 秒です。セキュリティーポリシーの数が 100 を超える場合、間隔は 20 秒です。

Security policy group

セキュリティーポリシーグループ化により、ユーザーは同じセキュリティーポリシーグループ内のセキュリティーポリシーをバッチで有効化、無効化、削除および移動できます。各セキュリティーポリシーに対してセキュリティーポリシーグループを指定するか、各セキュリティーポリシーグループに対してセキュリティーポリシーの範囲を指定できます。
セキュリティーポリシーは、セキュリティーポリシーとそのセキュリティーポリシーグループの両方が有効になっている場合にのみ有効になります。

Import and export

この機能により、セキュリティーポリシー構成を迅速に移行できます。特定またはすべてのセキュリティーポリシー設定をエクスポートして、増分インポートを実行できます。
ファイルをインポートする場合は、次の制限とガイドラインに従ってください。

- インポートされたファイル内の構成アイテム(時間範囲など)が既存のアイテムと同じ名前である場合、インポートされたアイテムは既存のアイテムを上書きします。
- ポリシーのインポートに失敗した場合、インポートプロセスは終了しますが、インポートされたポリシーは影響を受けず、ロールバックできません。
- ファイルが CFG 形式であることを確認します。

Restrictions and guidelines

Restrictions and guidelines: Security policies

- セキュリティーポリシーを移動して、同じタイプのポリシー間で一致する順序を変更できます。
- 新しく追加されたセキュリティーポリシーは、同じ種類の既存のセキュリティーポリシーの下に一覧表示されます。

- セキュリティーポリシーでオブジェクトを持たないオブジェクトグループを使用する場合、セキュリティーポリシーはどのパケットにも一致しません。詳細は、オブジェクトグループのオンラインヘルプを参照してください。
- **Activate** をクリックしてもポリシーマッチングアクセラレーションをアクティブにできない場合、アクセラレーションされたポリシーのマッチングは影響を受けません。
- また、セキュリティーポリシーで使用されるオブジェクトグループ内のオブジェクトが変更された場合は、ポリシーマッチングアクセラレーションをアクティブにする必要があります。
- セキュリティーポリシーに設定されたエージングタイムは、**Session Aging Time Set** で設定されたエージングタイムよりも優先されます。
- VLAN 間ブリッジ転送が設定されている場合、統計情報収集機能は、セキュリティーポリシーによって廃棄されたパケットに関する統計情報だけを収集します。許可されたパケットに関する統計情報は収集されません。
- 送信元 MAC アドレスをフィルタリング基準として使用できるのは、IPv4 セキュリティーポリシーだけです。
- 既定以外のコンテキストのコンテンツセキュリティーを構成する前に、既定のコンテキストに対してコンテンツセキュリティー設定がアクティブになっていることを確認してください。コンテキストのコンテンツセキュリティー設定をアクティブにするには、コンテキストのセキュリティーポリシーページで **submit** をクリックします。

Restrictions and guidelines: Security policy groups

- セキュリティーポリシーのセキュリティーポリシーグループを指定した場合、そのポリシーは最後のポリシーとしてセキュリティーポリシーグループに追加されます。
- セキュリティーポリシーグループから最初のセキュリティーポリシーを削除すると、そのポリシーはポリシーグループの前に配置されます。他のセキュリティーポリシーをセキュリティーポリシーグループから削除すると、そのポリシーはポリシーグループの後に配置されます。
- ポリシーを含まないセキュリティーポリシーグループを移動したり、空のセキュリティーポリシーグループの前後にセキュリティーポリシーグループを移動したりすることはできません。
- セキュリティーポリシーグループを、別のセキュリティーポリシーグループ内のポリシー間に移動することはできません。
- セキュリティーポリシーグループの前後にセキュリティーポリシーを移動すると、そのポリシーは自動的にグループに参加します。

Restrictions and guidelines: Import and export

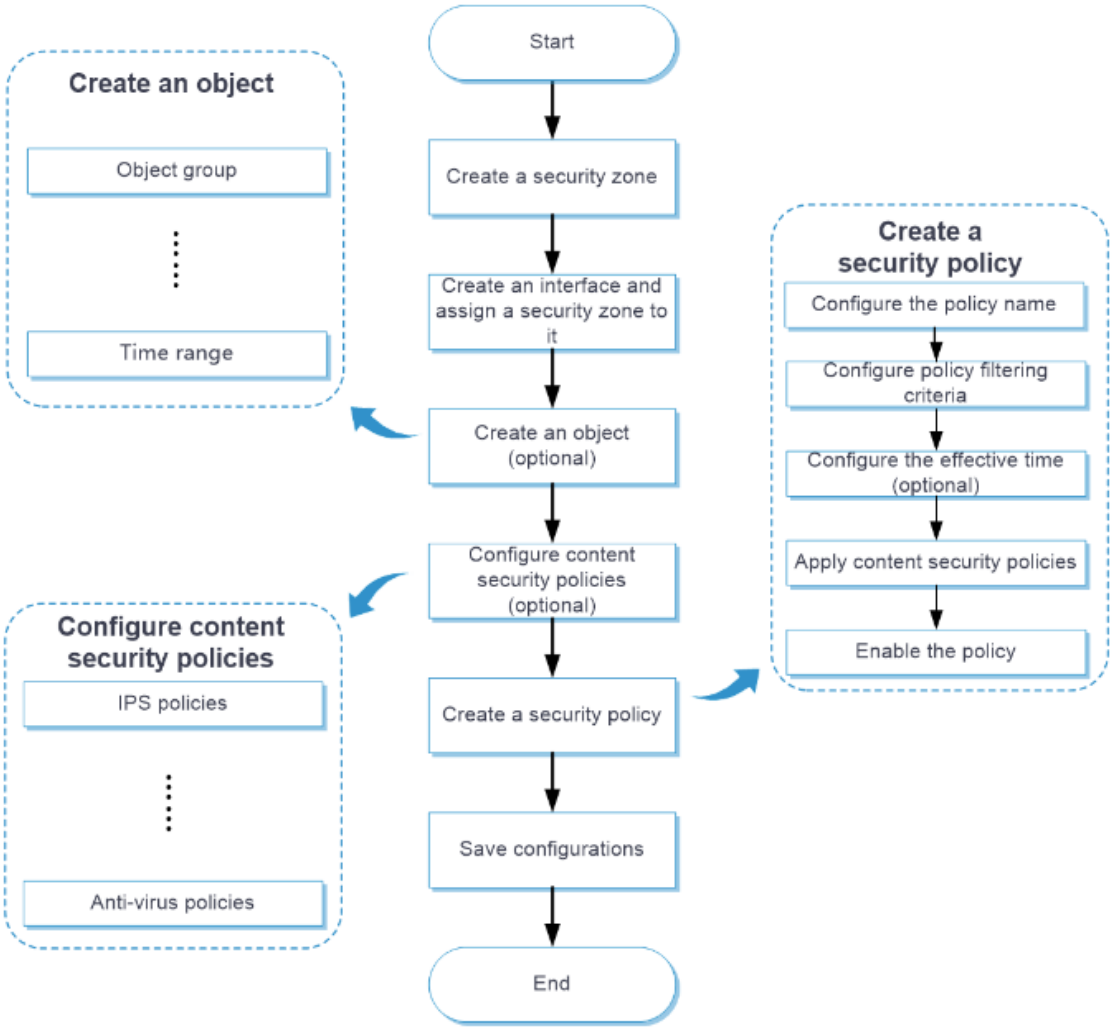
- エクスポートできるのは、ユーザー定義のアプリケーション、端末およびセキュリティーゾーンのみです。定義済みのアプリケーション、端末およびセキュリティーゾーンはエクスポートできません。

- インポートするファイルには、エクスポートに使用できるセキュリティー設定のみを含めることができます。
- セキュリティーゾーンおよび VRF 設定をエクスポートする場合、インターフェースとのバインディング関係はエクスポートされません。インポートされたセキュリティーゾーンおよび VRF に対してインターフェースバインディングを設定する必要があります。
- エクスポート操作では、セキュリティーポリシーの設定のみがエクスポートされ、セキュリティーポリシーで使用されるオブジェクトに関する設定はエクスポートされません。
- インポートまたはエクスポートを一度に実行できるユーザーは 1 人だけです。

Configure security policies

図 1 に示すように、セキュリティーポリシーを設定します。

図 1 セキュリティーポリシーの設定手順



Create a security policy

1. **Policies > Security Policies > Security Policies** を選択します。
2. **create** をクリックし、**create a policy** を選択します。
3. セキュリティーポリシーを作成します。

表 1 セキュリティーポリシーの構成項目

項目	説明
Name	セキュリティーポリシーの名前を入力してください。同じタイプのセキュリティーポリシーに同じ名前を付けることはできません。
Auto naming	セキュリティーポリシーに自動的に名前を付けるかどうかを選択します。この機能を有効にすると、ソースセキュリティーポリシーと宛先セキュリティーポリシーを 1 つずつのみ指定できます。
Source zone	フィルタリング基準として送信元セキュリティーゾーンを指定します。

Destination zone	フィルタリング基準として宛先セキュリティーゾーンを指定します。
Type	セキュリティーポリシータイプを指定します。オプションは次のとおりです。 • IPv4。 • IPv6。
Policy group	セキュリティーポリシーのセキュリティーポリシーグループを指定します。
Description	セキュリティーポリシーの説明を設定します。
Action	セキュリティーポリシーアクションを指定します。オプションは次のとおりです。 • **Permit** :一致したパケットの通過を許可します。 • **Deny**: 一致したパケットを廃棄します。
Source IP/MAC address	送信元 IP/MAC アドレスをフィルタリング基準として指定します。パケットフィルタリングに送信元 MAC アドレスを使用できるのは、IPv4 セキュリティーポリシーだけです。
Destination address	フィルタリング基準として宛先 IP アドレスを指定します。
Service	サービスをフィルタリング基準として指定します。
Application	フィルタリング基準としてアプリケーションまたはアプリケーショングループを指定します。
Terminal	フィルタリング基準として端末または端末グループを指定します。
User	フィルタリング基準としてユーザーまたはユーザーグループを指定します。
Time range	セキュリティーポリシールールが有効になる時間範囲を指定します。
VRF	指定された VRF のパケットで有効になるようにセキュリティーポリシールールを設定します。
Content security	一致するパケットに Deep Packet Inspection(DPI)サービスを設定します。
Logging	一致したパケットのロギングをイネーブルにします。
Match counting	一致したパケットの統計情報収集をイネーブルにします。
Statistics collection period	統計収集期間を指定します。オプションには、**permanent** と **Custom** があります。

Session aging	セキュリティーポリシーに一致するパケットに対して作成される安定セッションのエージングタイムを設定します。 エージングタイムが設定されていない場合、安定セッションでは、**System > Session Aging Time Set > Protocol Session Aging Set** ページで設定されたエージングタイムが使用されます。
Persistent session aging	セキュリティーポリシーに一致するパケットに対して作成された永続セッションのエージングタイムを設定します。 エージングタイムが設定されていない場合、安定セッションでは、**System > Session Aging Time Set > Protocol Session Aging Set** ページで設定されたエージングタイムが使用されます。
Policy status	このポリシーを有効にするかどうかを選択します。
Redundancy analysis	ポリシーの作成後に **Redundancy Analysis** ページにアクセスするかどうかを選択します。

4. **OK** をクリックします。
5. セキュリティーポリシーをすぐに有効にするには、**activate** をクリックします。

Insert a security policy

1. **Policies > Security Policies > Security Policies** を選択します。
2. 既存のすべてのセキュリティーポリシーの前または後にセキュリティーポリシーを挿入するには、**Insert** をクリックして **First** または **Last** を選択します。特定のポリシーの前または後にセキュリティーポリシーを挿入するには、ターゲットポリシーを選択して **Insert** をクリックし、**Before** または **After** を選択します。
3. 挿入するポリシーを構成し、**OK** をクリックします。詳細は、表 1 を参照してください。
   挿入されたポリシーが **security policies** ページに表示されます。
4. セキュリティーポリシーをすぐに有効にするには、**activate** をクリックします。

Create a security policy group

1. **Policies > Security Policies > Security Policies** を選択します。
2. **create** をクリックし、create a policy group を選択します。
3. セキュリティーポリシーグループを作成します。

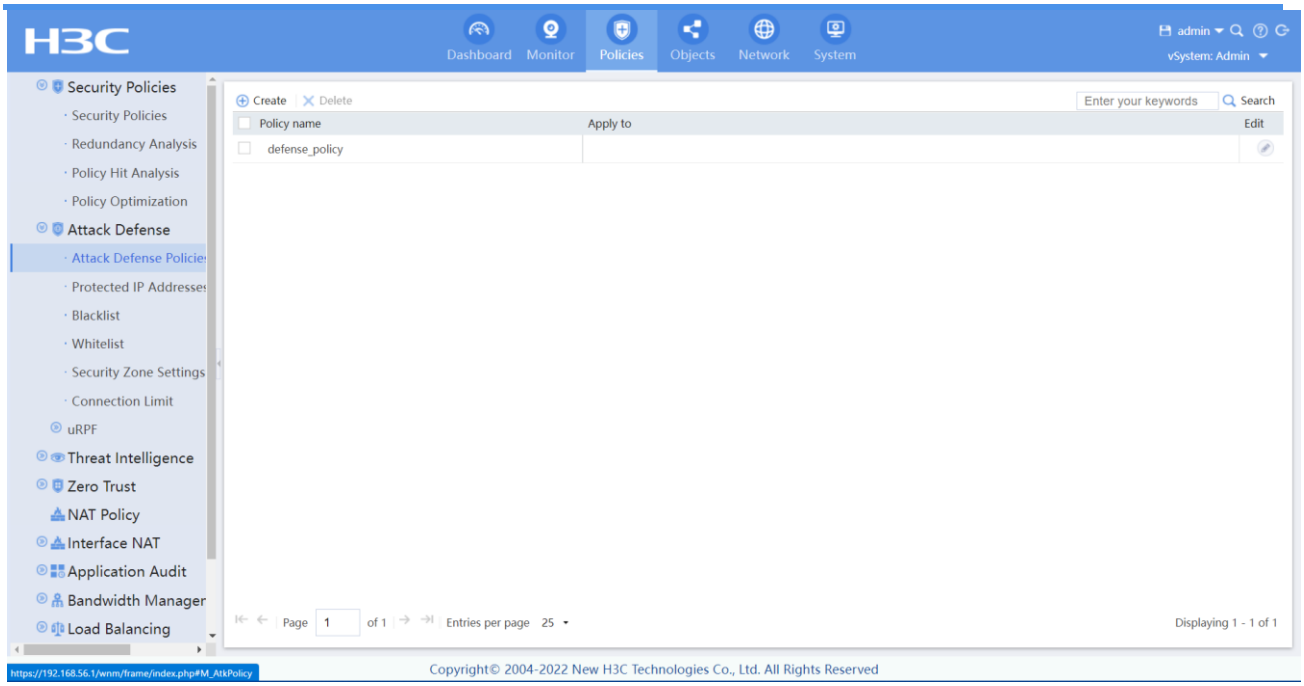
表 2 セキュリティーポリシーグループの構成項目

項目	説明
Name	セキュリティーポリシーグループの名前を入力します。

Description	セキュリティーポリシーグループの説明を構成します。
Type	セキュリティーポリシーグループタイプを指定します。オプションは次のとおりです。 • IPv4。 • IPv6。
Start policy	すべてのセキュリティーポリシーがグループに追加されるポリシー範囲の開始ポリシーの名前を指定します。
End policy	すべてのセキュリティーポリシーがグループに追加されるポリシー範囲の終了ポリシーの名前を指定します。 終了ポリシーが開始ポリシーの下にリストされていること、および指定したポリシー範囲内のポリシーが他のポリシーグループに属していないことを確認してください。

4. **OK** をクリックします。

Attack defense



このヘルプには、次のトピックが含まれています。

- Introduction
  - Attack defense policy
  - Client verification
  - Blacklist
  - Whitelist
- Restrictions and guidelines
- Configure attack defense and prevention
  - Configure an attack defense policy
  - Configure protected IP addresses
  - Configure the blacklist
  - Configure the whitelist
  - Configure security zone settings

Introduction

攻撃防御は、重要なネットワークセキュリティー機能として、着信パケットを検査することによって攻撃を検出し、防御アクションを実行します。

Attack defense policy

攻撃防御ポリシーには、一連の攻撃検出および防御アクション設定が含まれます。防御アクションには、ロギング、パケットドロップ、ブラックリスト、およびクライアント検証が含まれます。デバイスは、次の攻撃防御ポリシーをサポートします。

- Scanning attack defense policy。
- Flood attack defense policy。
- Single-attack defense policy。

セキュリティーゾーンに攻撃防御ポリシーを適用して、セキュリティーゾーンで受信に攻撃防御ポリシーを適用します。

Scanning attack detection and prevention

スキャンは、ネットワークへの侵入に備えるために使用される侵入前のアクティビティです。スキャンにより、攻撃者はターゲットネットワークに侵入する方法を見つけ、攻撃者の ID を偽装できます。
攻撃者は、スキャンツールを使用してネットワークを調査し、脆弱なホストを見つけ、ホスト上で実行されているサービスを発見します。攻撃者は、この情報を使用して攻撃を開始できます。
デバイスは、IP スイープ(アドレススキャン)およびポートスキャン攻撃を検出および防止できます。攻撃者が複数のホストからターゲットホストに対してポートスキャンを実行すると、分散ポートスキャン攻撃が発生します。
外部ネットワークに接続されているセキュリティーゾーンにスキャン攻撃防御ポリシーを適用します。スキャン攻撃検出では、ターゲットシステムへの接続の着信パケットレートが検査されます。送信元が事前に定義されたしきい値以上のレートで接続を開始した場合、デバイスは次のアクションを実行できます。

- 出力ログ。
- 攻撃者の IP アドレスから後続のパケットをドロップします。
- IP ブラックリストに攻撃者の IP アドレスを追加します。

スキャン攻撃防御ポリシーの検出感度レベルを指定できます。検出感度レベルは、**high**、**middle**、**low** のしきい値と検出期間が固定されています。しきい値と検出期間をカスタマイズするには、検出レベルを **user-defined** に設定します。
防御アクションが IP ブラックリストに攻撃者の IP アドレスを追加する場合は、スキャン攻撃防御ポリシーが適用されるセキュリティーゾーンでブラックリスト機能をイネーブルにする必要があります。

Flood attack detection and prevention

攻撃者は、短時間に多数の偽のリクエストを被害者に送信することにより、フラッディング攻撃を開始します。被害者は、これらの偽のリクエストへの応答に追われているため、合法的なユーザーにサービスを提供できず、DoS 攻撃が発生します。

外部ネットワークに接続されているセキュリティーゾーンにフラッド攻撃防御ポリシーを適用して、内部サーバーを保護します。フラッド攻撃検出は、内部サーバーへの接続が開始されるレートを監視します。フラッド攻撃検出がイネーブルの場合、デバイスは攻撃検出ステートになります。IP アドレスからのパケット受信レートまたは IP アドレスへのパケット送信レートが送信元または宛先の IP ベースのしきい値に達するか、それを超えると、デバイスは防御ステートになり、指定されたアクションを実行します。レートが無音しきい値(しきい値の 4 分の 3)を下回ると、デバイスは攻撃検出ステートに戻ります。
特定の IP アドレスに対してフラッド攻撃の検出と防御を設定できます。特定以外の IP アドレスの場合、デバイスはグローバルな攻撃防御設定を使用します。
適切なしきい値を設定すると、効果的に攻撃を防ぐことができます。システムは、グローバルしきい値を自動的に学習するしきい値学習機能を提供します。この機能により、デバイスはネットワーク内のトラフィックフローに基づいて次のようにグローバルしきい値を学習できます。

1. ネットワーク内のパケット送信速度を監視します。
2. しきい値学習時間内に学習されたピークレートに基づいて、グローバルしきい値を計算します。

しきい値学習機能には、次のモードが含まれます。

- **One-time learning**: デバイスはしきい値学習を 1 回だけ実行します。
- **Periodical learning**: デバイスは一定間隔でしきい値学習を実行します。最新の学習済みしきい値が常に有効になります。

しきい値学習では、すべてのタイプのフラッド攻撃のしきい値を学習します。学習したしきい値の自動適用をイネーブルにできます。
ネットワークトラフィック統計情報が不明な場合は、最初にフラッド攻撃防止パラメーターのデフォルト設定を使用してから、しきい値学習結果に基づいてしきい値を調整します。

Single-packet attack detection and prevention

単一パケット攻撃は、不正パケット攻撃とも呼ばれます。攻撃者は通常、次の方法を使用して単一パケット攻撃を開始します。

- 攻撃者が欠陥パケットをデバイスに送信すると、デバイスが誤動作またはクラッシュします。
- 攻撃者は通常のパケットをデバイスに送信し、デバイスが接続を中断したり、ネットワークトポロジを調査したりします。
- 攻撃者は、ターゲットデバイスに大量の偽造パケットを送信します。これにより、ネットワーク帯域幅が消費され、Denial of Service(DoS)が発生します。

単一パケット攻撃防御ポリシーを外部ネットワークに接続されているセキュリティーゾーンに適用します。単一パケット攻撃検出では、パケットシグニチャに基づいて着信パケットが検査されます。攻撃パケットが検出された場合、デバイスは次のアクションを実行できます。

- ログを出力。
- 攻撃パケットをドロップします。

デバイスは、既知の単一パケット攻撃と、ユーザー定義シグニチャを使用した攻撃パケットの両方の検出をサポートします。

Attack detection exemption

攻撃防御ポリシーでは、ACL を使用して免除されたパケットを識別します。ポリシーでは、ACL によって許可されたパケットはチェックされません。信頼できるサーバーからのパケットを識別するように ACL を設定できます。免除機能により、誤アラームレートが減少し、パケット処理効率が向上します。
攻撃検出の免除に ACL が使用されている場合、ACL 許可ルールの次の一致基準だけが有効になります。

- Source IP address.
- Destination IP address.
- Source port.
- Destination port.
- Protocol.
- VRF.
- Non-first fragments.

Client verification

クライアント検証機能は、TCP、DNS、DNS 応答、HTTP、および SIP フラッド攻撃からサーバーを保護します。クライアント検証が有効なデバイスは、クライアントと保護対象サーバーの間に配置され、クライアントによって開始された接続を検証します。
クライアント検証によって保護された IP アドレスは、手動で追加することも、自動的に学習することもできます。

- 保護 IP アドレスを手動で追加できます。デバイスは、保護 IP アドレス宛ての最初のパケットを受信したときにクライアント検証を実行します。
- クライアント検証では、フラッド攻撃検出と連携する際に、被害者の IP アドレスを保護 IP リストに自動的に追加できます。クライアント検証は、フラッド攻撃防御アクションとして指定されていることを確認してください。

デバイスは、信頼できる IP アドレスからのパケットを直接転送します。

TCP client verification

TCP クライアント検証機能は、次のフラッド攻撃から TCP サーバーを保護します。

- SYN.
- ACK.
- SYN-ACK.
- FIN.
- RST.

TCP クライアント検証は、次のモードで動作できます。

- **Safe reset**: TCP 接続発信側からのパケットに対してだけ単一方向 TCP プロキシをイネーブルにします。攻撃はクライアントから発生することが多いため、ほとんどのシナリオでは単一方向 TCP プロキシで十分です。
- **SYN cookie**: TCP クライアントおよびサーバーの双方向 TCP プロキシをイネーブルにします。

セーフリセットモードは次のように機能します。

1. 保護サーバー宛ての SYN パケットを受信した後、TCP プロキシは、無効なシーケンス番号を持つ SYN ACK パケットを送り返します。
2. TCP プロキシがクライアントから RST パケットを受信した場合、クライアントは正当であると検証されます。
3. TCP プロキシは、クライアントの IP アドレスを信頼できる IP リストに追加します。クライアントは再び接続を開始し、TCP プロキシは TCP パケットをサーバーに直接転送します。

セーフリセットモードでは、TCP クライアントが TCP プロトコルスイートに準拠している必要があります。TCP プロキシは、クライアントが TCP プロトコルスイートに準拠していない場合、正規のクライアントによるサーバーへのアクセスを拒否します。クライアント検証では、TCP 接続の確立に通常の TCP 接続の確立よりも時間がかかります。

SYN cookie モードでは、次のように 2 つの TCP 接続を確立する必要があります。

1. クライアントから保護サーバーへの SYN パケットを受信した後、TCP プロキシはウィンドウサイズ 0 の SYN ACK パケットを送り返します。クライアントが ACK パケットで応答した場合、クライアントは正当であると確認されます。プロキシデバイスはクライアントと TCP 接続を確立します。
2. TCP プロキシデバイスは、ウィンドウサイズが異なる新しい 3 ウェイハンドシェイクを通じてサーバーとの接続を確立します。この接続は、クライアントとプロキシデバイス間の接続とは異なるシーケンス番号を使用します。

SYN cookie モードでは、TCP プロキシはクライアントと通信するサーバープロキシであり、サーバーと通信するクライアントプロキシです。次の要件を満たす場合は、このモードを選択します。

- TCP プロキシデバイスは、保護サーバーの入力と出力を通過するキーパス上に配置されます。
- クライアントとサーバー間で交換されるすべてのパケットは、TCP プロキシデバイスを通過します。

DNS client verification

DNS クライアント検証機能は、DNS サーバーを DNS フラッド攻撃から保護します。この機能は、DNS クライアントから DNS サーバーへのパケットが通過するデバイスに設定されます。DNS クライアント検証機能が設定されているデバイスは、DNS クライアントオーセンティケータと呼ばれます。
DNS クライアントの検証は次のように機能します。

1. 保護サーバー宛ての UDP DNS クエリーを受信すると、DNS クライアントオーセンティケータは DNS Truncate(TC)パケットで応答します。DNS Truncate パケットでは、クライアントは TCP パケットでクエリーを開始する必要があります。
2. オーセンティケータがクライアントからポート 53 への TCP SYN パケットで DNS クエリーを受信すると、オーセンティケータは不正なシーケンス番号を含む SYN-ACK パケットで応答します。
3. オーセンティケータがクライアントから RST パケットを受信すると、オーセンティケータはクライアントが正当であることを確認します。
4. オーセンティケータは、クライアントの IP アドレスを信頼できる IP リストに追加し、信頼できるクライアントの後続パケットをサーバーに転送します。

DNS クライアント検証機能では、DNS クライアントが TCP/IP プロトコルスイートに準拠している必要があります。DNS クライアントオーセンティケータは、クライアントが TCP プロトコルスイートに準拠していない場合、正規のクライアントによるサーバーへのアクセスを拒否します。クライアント検証では、DNS 接続の確立に通常の TCP 接続の確立よりも時間がかかります。

DNS reply source verification

DNS 応答ソース検証機能は、DNS クライアントを DNS 応答フラッド攻撃から保護します。DNS 応答ソース検証機能が設定されているデバイスは、DNS 応答オーセンティケータと呼ばれます。
DNS 応答ソース検証は、次のように機能します。

1. 保護されたクライアント宛の UDP DNS 応答を受信すると、DNS 応答オーセンティケータは、ローカルで生成されたクエリーID とポート番号を持つ DNS クエリーパケットを返します。
2. DNS クエリーを受信した後、有効な DNS サーバーは、新しいクエリーID と宛先ポートを含む DNS 応答で応答します。
3. DNS 応答オーセンティケータは、応答内のクエリーID と宛先ポートを確認します。クエリーID と宛先ポートが、オーセンティケータが送信したクエリーID とポート番号と同じ場合、DNS サーバーは確認を通過します。オーセンティケータは、後続のパケットをサーバーから転送します。

HTTP client verification

HTTP クライアント検証機能は、HTTP フラッド攻撃から HTTP サーバーを保護します。これは、HTTP クライアントから HTTP サーバーへの HTTP GET または POST 要求パケットが通過するデバイスで設定されます。HTTP クライアント検証機能が設定されているデバイスは、HTTP クライアントオーセンティケータと呼ばれます。

HTTP クライアントオーセンティケータは、HTTP GET 要求を使用して HTTP クライアントを次のように確認します。

1. 保護された HTTP サーバー宛ての SYN パケットを受信すると、HTTP クライアントオーセンティケータは SYN cookie モードで TCP クライアント検証を実行します。クライアントが TCP クライアント検証に合格すると、クライアントとオーセンティケータの間に TCP 接続が確立されます。
2. オーセンティケータは、クライアントから HTTP GET パケットを受信すると、最初のリダイレクト検証を実行します。オーセンティケータはクライアント情報を記録し、HTTP リダイレクトパケットで応答します。HTTP リダイレクトパケットにはリダイレクト URI が含まれており、クライアントに TCP 接続の終了を要求します。
3. HTTP リダイレクトパケットを受信した後、クライアントは TCP 接続を終了し、オーセンティケータとの新しい TCP 接続を確立します。
4. オーセンティケータは HTTP GET パケットを受信すると、2 回目のリダイレクション検証を実行します。オーセンティケータは次の情報を検証します。
   - クライアントは最初のリダイレクト検証に合格しました。
   - HTTP GET パケット内の URI はリダイレクト URI です。
5. クライアントが 2 回目のリダイレクション検証にパスした場合、オーセンティケータはその IP アドレスを信頼できる IP リストに追加し、リダイレクトパケットに応答します。リダイレクトパケットには、クライアントが元々持っていた URI が含まれており、クライアントに TCP 接続の終了を要求します。
6. オーセンティケータは、信頼できるクライアントの後続のパケットをサーバーに直接転送します。

HTTP クライアントオーセンティケータは、HTTP POST 要求を使用して HTTP クライアントを次のように確認します。

1. 保護された HTTP サーバー宛ての SYN パケットを受信すると、HTTP クライアントオーセンティケータは SYN Cookie モードで TCP クライアント検証を実行します。クライアントが TCP クライアント検証に合格すると、クライアントとオーセンティケータの間に TCP 接続が確立されます。
2. オーセンティケータは、クライアントから HTTP POST 要求を受信すると、リダイレクト検証を実行します。オーセンティケータはクライアント情報を記録し、HTTP リダイレクトパケットで応答します。HTTP リダイレクトパケットには、リダイレクト URI と Set-Cookie ヘッダーが含まれており、クライアントに TCP 接続の終了を要求します。
3. HTTP リダイレクトパケットを受信した後、クライアントは TCP 接続を終了し、オーセンティケータとの新しい TCP 接続を確立します。
4. オーセンティケータは HTTP POST 要求を受信すると、タイムアウト検証を実行します。オーセンティケータは次の情報を検証します。
   - クライアントはリダイレクト検証に合格しました。
   - HTTP POST 要求に有効な cookie が含まれています。

5. クライアントがタイムアウト検証に合格すると、オーセンティケータは IP アドレスを信頼できる IP リストに追加し、HTTP Timeout パケットで応答します。Timeout パケットには、クライアントが最初に伝送した URI が含まれており、クライアントに TCP 接続の終了を要求します。
6. オーセンティケータは、信頼できるクライアントの後続のパケットをサーバーに直接転送します。

SIP client verification

SIP クライアント検証機能は、SIP フラッド攻撃から SIP サーバーを保護します。
SIP クライアント検証機能が設定されているデバイスは、SIP クライアントオーセンティケータと呼ばれます。SIP クライアント検証プロセスは次のとおりです。
1. 保護サーバー宛ての UDP INVITE パケットを受信すると、SIP クライアントオーセンティケータは、ブランチ値を含む OPTIONS パケットを返信します。
2. OPTIONS パケットを受信した後、クライアントは SIP クライアントオーセンティケータに応答を送信します。
3. 応答を受信すると、SIP クライアントオーセンティケータは応答内のブランチ値を確認します。応答パケット内のブランチ値が、SIP クライアントオーセンティケータが送信した OPTIONS パケット内のブランチ値と同じ場合、クライアントは確認に合格します。オーセンティケータは、後続のパケットをクライアントから転送します。
フラグメンテーションのために、SIP クライアントによって送信されたパケットに完全なヘッダー情報が含まれていない場合、正規の SIP クライアントはクライアント検証に合格しない可能性があります。

Blacklist

ブラックリスト機能は、IP アドレスまたはブラックリストエントリ内のアドレスオブジェクトグループによってパケットをフィルタリングする攻撃防御方法です。IP ブラックリストフィルタリングは、ACL ベースのパケットフィルタリングと比較して簡単で効果的なスクリーニングを高速に実行できます。
ブラックリストエントリは、手動で追加することも、動的に学習することもできます。

- IP ブラックリストエントリを手動で追加できます。これらのエントリはデフォルトではエージングアウトしません。エントリごとにエージングタイムを設定できます。
- デバイスは、スキャン攻撃検出と連携する場合、IP ブラックリストエントリを自動的に追加できます。動的に学習された各 IP ブラックリストエントリには、ユーザーが設定可能なエージングタイムがあります。IP ブラックリストへの攻撃者の IP アドレスの追加が、スキャン攻撃防御アクションとして指定されていることを確認してください。

Whitelist

この機能は、ホワイトリストに記載されたアドレスオブジェクトグループで指定されたサブネットから発信されたパケットを攻撃検出から除外します。ホワイトリストに記載されたアドレスからのパケットは、攻撃パケットであるかどうかに関係なく直接転送されます。
ホワイトリストに含めることができるアドレスオブジェクトグループは 1 つだけです。アドレスオブジェクトグループは、ホワイトリストに対して手動でのみ追加または削除できます。

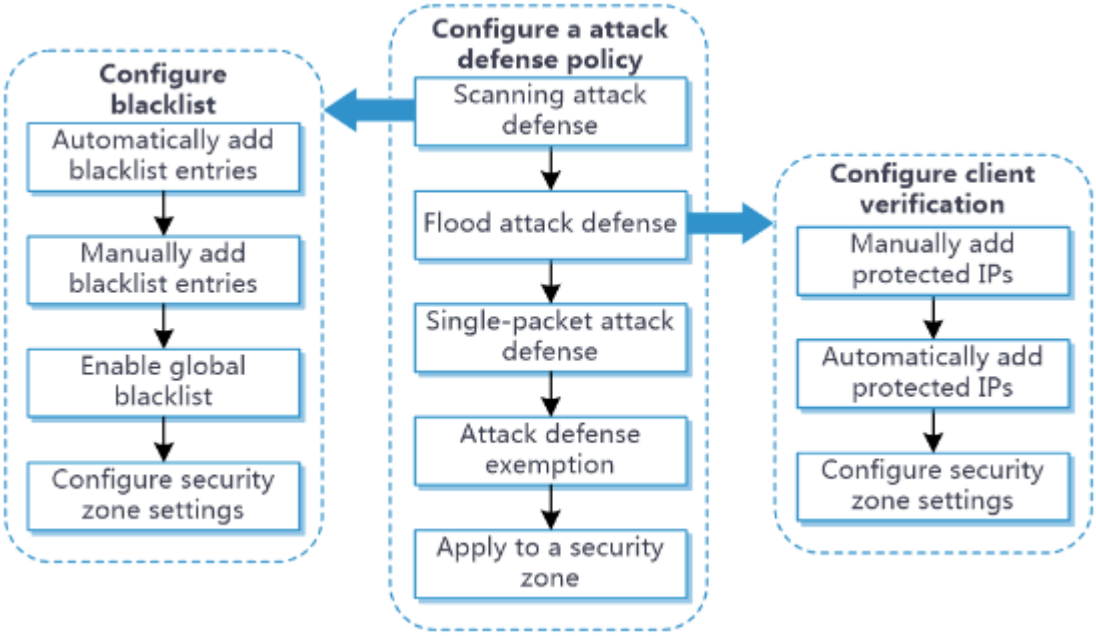
Restrictions and guidelines

- デバイスに複数のサービスカードがある場合、フラッド攻撃ポリシーのしきい値はカード固有です。デバイスのグローバルしきい値は、しきい値にサービスカード数量を乗算した積です。
- 攻撃防御ポリシーのクライアント検証アクションは、セキュリティーゾーンでクライアント検証がイネーブルになっている場合にだけ有効になります。
- アプリケーションシナリオに応じてしきい値を調整します。保護対象サーバーに送信されるパケット数が通常大きい場合は、大きいしきい値を設定します。小さいしきい値はサーバーサービスに影響を与える可能性があります。不安定なネットワークや攻撃を受けやすいネットワークの場合は、小さいしきい値を設定します。
- 指定された ACL が存在しない場合、またはルールが含まれていない場合、攻撃検出の免除は有効になりません。
- 攻撃検出の免除に ACL が使用されている場合、ACL 許可ルールの次の一致基準だけが有効になります。
  - Source IP address.
  - Destination IP address.
  - Source port.
  - Destination port.
  - Protocol.
  - VRF.
  - Non-first fragments
- しきい値学習機能は、デフォルトポートだけで次の攻撃のしきい値を学習します。
  - DNS flood attacks.
  - DNS response flood attacks.
  - SIP flood attacks.
  - HTTP flood attacks

- フラッド攻撃タイプに対して送信元 IP ベースのしきい値を 0 に設定すると、学習結果自動適用がイネーブルになっていても、デバイスは送信元 IP ベースの学習結果をこの攻撃タイプに適用しません。送信元 IP ベースの学習結果をこの攻撃タイプに手動で適用することもできません。宛先 IP ベースのしきい値を 0 に設定した場合も、同じ制限が適用されます。

Configure attack defense and prevention

図 1 攻撃防御と防御の設定手順



Configure an attack defense policy

攻撃防御および防御を設定する前に、攻撃防御ポリシーを作成します。ネットワークセキュリティー要件に基づいて、ポリシーに攻撃検出基準および防御アクションを指定します。

手順

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Attack Defense > Attack Defense Policies** を選択します。
3. **create** をクリックします。
4. 攻撃防御ポリシーを作成します。

表 1 攻撃防御ポリシーの設定項目

項目	説明
Policy name	攻撃防御ポリシーの名前を入力します。有効な文字は、英字、数字、下線(_)、およびハイフン(-)です。

Apply to	攻撃防御ポリシーが適用されるセキュリティーゾーンを選択します。セキュリティーゾーンに適用できる攻撃防御ポリシーは 1 つだけです。攻撃防御ポリシーは複数のセキュリティーゾーンに適用できます。 このリストには、デフォルトのセキュリティーゾーンと、**Network > Security Zones** ページで設定されたセキュリティーゾーンが含まれています。

スキャン攻撃防御ポリシーを作成するには、**Scanning Attack Defense** タブをクリックし、表 2 の説明に従ってポリシーを設定します。

表 2 スキャン攻撃防御ポリシーの設定項目

項目	説明
Detection sensitivity	スキャン攻撃検出レベル: • **Close**: スキャン攻撃防御をディセーブルにします。 • **Low**: 低レベルを指定します。このレベルは基本的なスキャン攻撃検出を提供し、誤アラーム率は低くなりますが、多くのスキャン攻撃は検出できません。 • **Medium**: 中レベルを指定します。高および低レベルと比較して、このレベルは中程度の誤アラーム率と攻撃検出精度を持ちます。 • **High**: 高レベルを指定します。このレベルでは、ほとんどのスキャン攻撃を検出できますが、誤アラーム率が高くなります。アクティブホストからの一部のパケットは、攻撃パケットと見なされる場合があります。 • **User-defined**: ユーザー定義レベルを指定します。スキャン攻撃防止のしきい値を設定できます。 必要に応じて、次のパラメーターを設定します。 • **Enable port scan attack prevention**: **detection sensibility** が **low**、**medium**、または **high** に設定されているときに有効になります。**Detection sensibility** が **user-defined** に設定されているときに有効にするかどうかを指定できます。 • **threshold**(**packets**):ポートスキャン攻撃防止をトリガーするしきい値。検出感度レベルが低い場合は 100000、検出感度レベルが中程度の場合は 40000、検出感度レベルが高い場合は 5000 です。検出感度が **User-defined** に設定されている場合は、しきい値を設定できます。検出感度が無効の場合は、表示されません。 • **enable port scan attack prevention**: **detection sensibility** が **low**、**medium**、または **high** に設定されているときに有効になります。**Detection sensibility** が **user-defined** に設定されているときに有効にするかどうかを指定できます。

	• **threshold(packets)**:アドレススキャン攻撃防止をトリガーするしきい値。検出感度レベルが低い場合は 100000、検出感度レベルが中程度の場合は 40000、検出感度レベルが高い場合は 5000 です。**Detection sensibility** が **user-defined** に設定されている場合は、しきい値を指定できます。**Detection sensibility** が無効の場合は表示されません。 • **detection period**: スキャン攻撃検出周期です。**Detection sensibility** が **Low**、**Medium**、**High** のとき検出周期は 10 秒です。**Detection sensibility** が **User-defined** のとき検出周期を設定できます。**Detection sensibility** が無効のときは表示されません。
Actions	スキャン攻撃に対する防御アクション。 • **Generate logs**。 • **Drop attack packets**。 • **Add attackers' IP addresses to blacklist**。 • **Age out after** *n* **minutes**: 動的に追加されたブラックリストエントリのエージングタイム。このパラメーターは、**Add attackers' IP addresses to blacklist** が選択されている場合にのみ使用できます。 **Detection sensitivity** が無効になっている場合、防止アクションは使用できません。

フラッド攻撃防御ポリシーを作成するには、**Flood Attack Defense Settings** タブをクリックします。攻撃防御ポリシーのグローバルパラメーターを構成するには、表 3 を参照してください。IP 固有のフラッド攻撃防御を構成するには、表 5 を参照してください。

表 3 フラッド攻撃防御グローバル設定の設定項目

項目	説明
Attack type	フラッド攻撃タイプ: • **ACK:** ACK フラッド攻撃タイプを指定します。ACK パケットは、ACK フラグのみが設定された TCP パケットです。クライアントから ACK パケットを受信すると、サーバーはハーフオープン接続を検索して一致するものを探す必要があります。ACK フラッド攻撃者は、多数の ACK パケットをサーバーに送信します。これにより、サーバーはハーフオープン接続の検索でビジー状態になり、通常のサービスのパケットを処理できなくなります。 • **DNS**: DNS フラッド攻撃タイプを指定します。DNS サーバーは、受信したすべての DNS クエリーを処理して応答します。DNS フラッド攻撃者は、偽造された多数の DNS クエリーを送信します。この攻撃により、DNS サーバーの帯域幅とリソースが消費され、正当な DNS クエリーを処理して応答することができなくなります。

	• **DNS reply**: DNS 応答フラッド攻撃タイプを指定します。DNS サーバーは、受信したすべての DNS 応答を処理して応答します。DNS 応答フラッド攻撃者は、偽造された大量の DNS 応答を送信します。この攻撃は DNS サーバーの帯域幅とリソースを消費し、サーバーが正規の DNS 応答を処理して応答することを妨げます。 • **FIN**: FIN フラッド攻撃タイプを指定します。FIN パケットは、TCP 接続をシャットダウンするために使用されます。FIN フラッド攻撃者は、偽造された大量の FIN パケットをサーバーに送信します。被害者は、正しい接続をシャットダウンするか、一致する接続を検索しているためにサービスを提供できない可能性があります。 • **HTTP**: HTTP フラッド攻撃タイプを指定します。HTTP GET リクエストまたは POST リクエストを受信すると、HTTP サーバーは文字列検索、データベース走査、データ再構成、フォーマット切替えなどの複雑な操作を実行します。これらの操作は大量のシステムリソースを消費します。HTTP フラッド攻撃者は、HTTP サーバーの処理能力を超える大量の HTTP GET リクエストまたは POST リクエストを送信します。これにより、サーバーがクラッシュします。 • **HTTP slow**: HTTP slow flood 攻撃タイプを指定します。攻撃者が HTTP サーバーへの多数の HTTP 同時接続を保持している場合、サーバーのシステムリソースがこれらの接続によって占有されます。その結果、サーバーは通常のサービスを処理できません。 • **ICMP**: ICMP フラッド攻撃タイプを指定します。ICMP フラッド攻撃者は、ping パケットなどの ICMP 要求パケットを高速でホストに送信します。ターゲットホストはこれらの要求への応答でビジー状態のため、サービスを提供できません。 • **ICMPv6**: ICMPv6 フラッド攻撃タイプを指定します。ICMPv6 フラッド攻撃者は、ping パケットなどの ICMPv6 要求パケットを高速でホストに送信します。ターゲットホストはこれらの要求に応答するためにビジー状態であるため、サービスを提供できません。 • **RST**: RST フラッド攻撃タイプを指定します。RST パケットは、TCP 接続エラーが発生したときに TCP 接続を中断するために使用されます。RST フラッド攻撃者は、偽造された大量の RST パケットをサーバーに送信します。被害者は、正しい接続をシャットダウンするか、一致する接続の検索でビジー状態のためサービスを提供できない可能性があります。 • **SIP**: SIP フラッド攻撃タイプを指定します。SIP クライアントから SIP INVITE パケットを受信した後、サーバーは SIP クライアントとのセッションを確立およびトレースするためにリソースを割り当てる必要があります。SIP フラッド攻撃者は、SIP サーバーの処理能力を超えるレートで大量の偽の

	INVITE 要求パケットを送信します。これにより、サーバーがクラッシュします。 • **SYN**: SYN フラッド攻撃タイプを指定します。SYN フラッド攻撃者は、TCP の 3 ウェイハンドシェイク特性を悪用し、被害者を正規ユーザーに応答させません。攻撃者は、偽造されたソースアドレスを持つ大量の SYN パケットをサーバーに送信します。これにより、サーバーは多数のハーフオープン接続を開き、要求に応答します。ただし、サーバーは予期された ACK パケットを受信できません。サーバーのすべてのリソースがハーフオープン接続にバインドされているため、サーバーは新しい着信接続要求を受け入れることができません。 • **SYN-ACK**: SYN-ACK フラッド攻撃タイプを指定します。SYN-ACK パケットを受信すると、サーバーは送信した SYN パケットに一致するものを検索する必要があります。SYN-ACK フラッド攻撃者は大量の SYN-ACK パケットをサーバーに送信します。これにより、サーバーは SYN パケットの検索でビジー状態になり、通常のサービスのパケットを処理できなくなります。 • **UDP**: UDP フラッド攻撃タイプを指定します。UDP フラッド攻撃者は UDP パケットを高速でホストに送信します。これらのパケットはターゲットホストの帯域幅を大量に消費するため、ホストは他のサービスを提供できません。
Src Threshold (pps)	フラッド攻撃防止をトリガーするグローバル送信元 IP ベースのしきい値を入力します。値の範囲は 0～1000000 です。ACK フラッド攻撃検出のデフォルト値は 40000 で、その他のタイプのフラッド攻撃検出のデフォルト値は 10000 です。 グローバルフラッド攻撃検出が設定されている場合、デバイスは攻撃検出ステートになります。IP アドレスから発信されたパケットの受信レートがしきい値に到達または超えた場合、デバイスは防止ステートになり、指定されたアクションを実行します。 このパラメーターを **0** に設定した場合、システムは送信元 IP ベースのフラッド攻撃検出を実行しません。
Dest Threshold (pps)	フラッド攻撃防止をトリガーするグローバル宛先 IP アドレスベースのしきい値を入力します。値の範囲は 0～1000000 です。ACK フラッド攻撃検出のデフォルト値は 40000 で、その他のタイプのフラッド攻撃検出のデフォルト値は 10000 です。 グローバルフラッド攻撃検出が設定されている場合、デバイスは攻撃検出ステートになります。IP アドレスへのパケットの送信レートがしきい値に到達または超えた場合、デバイスは防止ステートになり、指定されたアクションを実行します。

	グローバル宛先 IP ベースしきい値は、グローバルフラッド攻撃検出に適用されます。アプリケーションシナリオに従ってしきい値を調整します。保護されたサーバーに送信されるパケット数が通常大きい場合は、大きいしきい値を設定します。小さいしきい値は、サーバーサービスに影響を与える可能性があります。不安定なネットワークや攻撃を受けやすいネットワークの場合は、小さいしきい値を設定します。 このパラメーターを **0** に設定した場合、システムは宛先 IP ベースのフラッド攻撃検出を実行しません。
Logging	フラッド攻撃イベントのロギングをイネーブルにします。ログメッセージはログシステムに送信されます。
Detect All IPs	グローバルフラッド攻撃検出をイネーブルにします。
Client verification	クライアント検証をイネーブルにします。デバイスは自動的に犠牲 IP アドレスを保護 IP リストに追加し、保護 IP アドレス用のプロキシサービスを提供します。
Packet drop	防止アクションとしてパケットドロップを使用します。デバイスは、被害者の IP アドレス宛ての後続の攻撃パケットをドロップします。
Target ports	最大 32 個のポート番号項目のカンマ区切りリスト。たとえば、1-10,80。各項目は、ポート番号でポートを指定するか、start-port-number から end-port-number の形式でポート範囲を指定します。end-port-number は start-port-number より小さくできません。ポート番号の範囲は 1～65535 です。 デバイスは、ターゲットポート宛てのパケットに対してだけフラッディング攻撃検出を実行します。 ターゲットポート設定は、グローバルフラッド攻撃検出およびポートが指定されていない IP アドレス固有のフラッド攻撃検出に適用されます。IP アドレス固有のフラッド攻撃検出が特定のポートで設定されている場合、デバイスは、指定された IP アドレスのこれらのポートでフラッド攻撃を検出します。 このパラメーターを使用できるのは、DNS、DNS 応答、HTTP、HTTP 低速、および SIP フラッド攻撃タイプだけです。
Concurrent connections	許可される同時 HTTP 接続のしきい値を入力します。デフォルトは 5000 です。 HTTP 低速攻撃検出は、HTTP 同時接続の数がしきい値に達するとトリガーされます。 このパラメーターは、HTTP 低速攻撃タイプだけで使用できます。
Content-Length	HTTP パケットヘッダーの **Content-Length** フィールドの長さのしきい値を入力します。デフォルト値は 10000 です。 このパラメーターは、HTTP 低速攻撃タイプだけで使用できます。
Payload length	HTTP パケットペイロードのしきい値を入力します。デフォルトは 50 です。

	Content-Length フィールドの値が指定したしきい値より大きく、ペイロードが指定した長さより短い場合、HTTP パケットは異常パケットです。 このパラメーターは、HTTP 低速攻撃タイプだけで使用できます。
Abnormal packets	異常パケットのしきい値を入力します。デフォルトは 10 です。 このパラメーターは、HTTP slow flood 攻撃タイプだけで使用できます。
Detection cycle	攻撃検出期間を設定します。 デバイスは、検出期間内に受信した異常パケット数がしきい値を超えると、防止アクションを実行します。 このパラメーターは、HTTP slow flood 攻撃タイプだけで使用できます。
Blacklist	攻撃防御アクションとしてブラックリストを使用するかどうかを選択します。 攻撃防御ポリシーが適用されるセキュリティーゾーンでブラックリスト機能がイネーブルになっている場合、デバイスはブラックリストに記載された IP アドレスからのパケットをドロップします。 このパラメーターは、HTTP slow flood 攻撃タイプだけで使用できます。
Blacklist aging time	ダイナミックブラックリストエントリのエージングタイムを秒単位で設定します。デフォルトは 10 です。 このパラメーターを使用できるのは、ブラックリストが HTTP 低速フラッディング攻撃の防止アクションとして使用されている場合だけです。
Set threshold learning	表 4 に示すように、しきい値学習パラメーターを設定します。 **Edit** ページでしきい値ラーニング機能を設定する前に、まず攻撃防御ポリシーの設定を完了する必要があります。
Apply learned threshold	学習したしきい値を、フラッド攻撃防止のしきい値として使用します。 この設定は、**Detect All iPS** が有効になっており、学習結果がしきい値になっている攻撃タイプに対してだけ有効です。

表 4 しきい値学習の設定項目

項目	説明
Threshold learning	ベストプラクティスとして、しきい値ラーニングをイネーブルにして、しきい値設定のリファレンスを提供します。
Learning duration	しきい値学習の期間。システムは、しきい値学習期間内に学習されたピークレートに基づいて、さまざまな攻撃のしきい値を計算します。
Learning mode	次のモードを使用できます。 • **One-time learning**: デバイスはしきい値学習を 1 回だけ実行します。 • **Periodic learning**: デバイスは間隔を置いてしきい値学習を実行します。
Auto apply	デバイスが学習した最新のしきい値を自動的に適用します。

	このパラメーターは、**Detect All IPs** がイネーブルになっていて、学習結果がしきい値になっている攻撃タイプにだけ有効です。
Tolerance	しきい値学習許容値。しきい値が適用される前に、学習したしきい値をより大きな値に増加させます。これにより、しきい値学習機能はトラフィック変動に迅速に対応できます。

フラッド攻撃に対する保護 IP アドレスを追加するには、**Flood Attack Defense Settings** タブの **Protected IP** 領域で **Create** をクリックします。

表 5 IP 別フラッド攻撃防御の設定項目

項目	説明
IP version	IP バージョン(IPv4 または IPv6)を選択します。
IP address	保護する IP アドレスを入力します。 保護された IPv4 アドレスは 255.255.255.255 または 0.0.0.0 にできません。 保護された IPv6 アドレスはマルチキャストアドレスまたは::にできません。
Attack type	詳細は、表 3 を参照してください。
VRF	保護 IP アドレスが属する VRF。既存の VRF を選択するか、新しい VRF を作成できます。新しく作成された VRF は、**Network > VRF** ページに表示されます。
Dest Threshold (pps)	フラッド攻撃防止をトリガーする宛先 IP ベースのしきい値を設定します。デフォルト値は、ACK フラッド攻撃検出では 40000、その他のタイプのフラッド攻撃検出では 10000 です。
Threshold	HTTP 低速攻撃防御のしきい値を設定します。次の方法を使用できます。 • **Global settings**: **Global settings** 領域の設定を使用するには、このオプションを選択します。 • **User-defined**: このオプションを選択してしきい値を指定します。デフォルトのしきい値設定は次のとおりです: ○ 同時接続の数は 5000 です。 ○ **Content-Length** フィールドの値は 10000 です。 ○ ペイロード長は 50 です。 ○ 異常パケットの数は 10 です。 このパラメーターは、HTTP slow flood 攻撃タイプだけで使用できます。
Target ports	保護するポートを指定します。デバイスは、指定されたポート宛てのパケットを検出します。次の方法を使用できます。

	• **Global settings**: グローバル設定を使用するには、このオプションを選択します。デフォルトでは、グローバル設定はプロトコル固有の well-known ポートを保護します。たとえば、HTTP フラッド攻撃防止はポート 80 を保護します。 • **User-defined**: ポートまたはカンマで区切られたポート番号項目のリスト(1-10,80 など)を指定するには、このオプションを選択します。各項目は、ポート番号によってポートを指定するか、start-port-number～end-port-number の形式でポートの範囲を指定します。end-port-number は start-port-number より小さくできません。 このパラメーターを使用できるのは、DNS、DNS 応答、HTTP、HTTP 低速、および SIP フラッド攻撃タイプだけです。
Detection cycle	攻撃検出期間を設定します。次の方法を使用できます。 • **Global settings**: **Global settings** 領域で設定されたグローバル検出期間を使用するには、このオプションを選択します。 • **User defined**: このオプションを選択し、検出期間を設定します。検出期間が指定されていない場合は、グローバル検出期間が適用されます。 このパラメーターは、HTTP 低速攻撃タイプだけで使用できます。
Action	フラッド攻撃に対する予防措置を指定します。次の方法を使用できます。 • **Global settings**: Global settings 領域でグローバル防止アクションを使用するには、このオプションを選択します。 • **User-defined**: このオプションを選択し、防止アクションを指定します。 ○ **logging**: ロギングを防止アクションとして使用します。フラッド攻撃イベントが記録され、ログメッセージがログシステムに送信されます。 ○ **packet drop**: 防止アクションとしてパケットドロップを使用します。デバイスは、被害者の IP アドレス宛ての後続の攻撃パケットをドロップします。 ○ **client verification**: 防止アクションとして client verification を使用します。デバイスは自動的に犠牲 IP アドレスを保護 IP リストに追加し、保護 IP アドレスのプロキシサービスを提供します。
Blacklist	攻撃防御アクションとしてブラックリストを使用するかどうかを選択します。攻撃が検出されると、デバイスは自動的にパケットの送信元 IP アドレスをブラックリストに載せます。 セキュリティーゾーンでブラックリスト機能がイネーブルになっている場合、デバイスはブラックリストに記載された IP アドレスからのパケットをドロップします。 このパラメーターは、HTTP 低速攻撃タイプだけで使用できます。
Aging time	ダイナミックブラックリストエントリのエージングタイムを秒単位で設定します。デフォルトは 10 です。 このパラメーターを使用できるのは、ブラックリストアクションが HTTP 低速フラッディング攻撃に対して選択されている場合だけです。

表 6 よく知られた単一パケット攻撃防御の設定項目

項目	説明
Attack type	よく知られた単一パケット攻撃タイプを指定します。 • **IP fragment**: 攻撃者は、オフセットが 5 より小さい IP データグラムを被害者に送信します。これにより、被害者は誤動作またはクラッシュします。 • **IP impossible**: 攻撃者は、送信元 IP アドレスが宛先 IP アドレスと同じ IP パケットを送信します。これにより、被害者は誤動作します。 • **Teardrop**: 攻撃者は重複するフラグメントのストリームを送信します。被害者は重複するフラグメントを再構成しようとするとクラッシュします。 • **Tiny fragment**: 攻撃者はフラグメントサイズを小さくし、レイヤー4 ヘッダーフィールドを 2 番目のフラグメントに入れます。これらのフラグメントは一致しないため、パケットフィルタリングを通過できます。 • **IP option abnormal**: 攻撃者は、IP オプションが異常な IP データグラムを送信します。この攻撃は、ネットワークトポロジを探査することを目的としています。ターゲットシステムがエラーパケットを処理できない場合、ターゲットシステムは故障します。 • **Smurf**: 攻撃者は、ターゲットネットワークに ICMP エコー要求をブロードキャストします。これらの要求には、送信元 IP アドレスとして被害者の IP アドレスが含まれています。ターゲットネットワーク上のすべての受信者は、被害者に ICMP エコー応答を送信します。被害者は応答で溢れ、サービスを提供できなくなります。ネットワーク輻輳が発生する可能性があります。 • **traceroute**: 攻撃者は traceroute ツールを使用して、被害ネットワークのトポロジをプローブします。 • **ping of death**: 攻撃者は、IP プロトコルに違反する 65535 バイトを超える ICMP エコー要求を被害者に送信します。被害者がパケットを再構成すると、バッファオーバーフローが発生し、システムクラッシュが発生する可能性があります。 • **Large ICMP**: 攻撃者は大規模な ICMP パケットを送信して被害者をクラッシュさせます。大規模な ICMP パケットは、メモリー割り当てエラーを引き起こし、プロトコルスタックをクラッシュさせる可能性があります。 • **Large ICMPv6**: 攻撃者は大規模な ICMPv6 パケットを送信して被害者をクラッシュさせます。大規模な ICMPv6 パケットは、メモリー割り当てエラーを引き起こし、プロトコルスタックをクラッシュさせる可能性があります。 • **TCP invalid flags**: 攻撃者は無効な TCP フラグを持つパケットをターゲットホストに送信します。これにより、ターゲットシステムがクラッシュする可能性があります。

	• **CP null flag**: 攻撃者は、フラグのない TCP パケットをターゲットホストに送信します。これにより、ターゲットシステムがクラッシュする可能性があります。 • **TCP all flags**: 攻撃者は、すべてのフラグが設定された TCP パケットをターゲットホストに送信します。これは、ターゲットシステムをクラッシュさせる可能性があります。 • **TCP SYN-FIN**: 攻撃者は、SYN フラグと FIN フラグの両方をターゲットホストに設定した TCP パケットを送信します。これにより、ターゲットシステムがクラッシュする可能性があります。 • **TCP FIN only flag**: 攻撃者は、FIN フラグのみをターゲットホストに設定した TCP パケットを送信します。これにより、ターゲットシステムがクラッシュする可能性があります。 • **TCP land**: 攻撃者は、ターゲットの IP アドレスと同じソースおよび宛先 IP アドレスを持つ多数の TCP SYN パケットをターゲットに送信します。ターゲット上の接続リソースの半分が不足し、ターゲットは正常に動作できません。 • **WinNuke**: 攻撃者は、Windows システムを実行している被害者の TCP ポート 139(NetBIOS)にアウトオブバンド(OOB)データを送信します。悪意のあるパケットには、被害者のオペレーティングシステムをクラッシュさせる不正な緊急ポインタが含まれています。 • **UDP Bomb**: 攻撃者は不正な UDP パケットを送信します。IP ヘッダーの長さの値は、IP ヘッダーの長さに UDP ヘッダーの長さの値を加えた値よりも大きくなっています。ターゲットシステムがパケットを処理すると、バッファオーバーフローが発生し、システムクラッシュが発生する可能性があります。 • **UDP snork**: 攻撃者は、宛先ポート 135(Microsoft ロケーションサービス)および送信元ポート 135、7、または 19 で UDP パケットを送信します。この攻撃により、NT システムの CPU が消費されます。 • **UDP fraggle**: 攻撃者は、送信元 UDP ポート 7 および宛先 UDP ポート 19(UDP chargen ポート)を持つ大量のパケットをネットワークに送信します。これらのパケットは、送信元 IP アドレスとして被害者の IP アドレスを使用します。応答は被害者にフラッディングされ、DoS が発生します。 • **IPv6 ext header abnormal**: 攻撃者は、IPv6 拡張ヘッダーが無秩序または反復された IPv6 パケットをターゲットに送信します。 • **IPv6 ext header exceed**: 攻撃者は、IPv6 拡張ヘッダーが上限を超えている IPv6 パケットをターゲットに送信します。 異常 IPv6 拡張ヘッダーおよび IPv6 拡張ヘッダー超過攻撃検出では、ESP ヘッダーとそれより前のヘッダーを調べ、ESP ヘッダーより後のヘッダーは調べません。

Logging	単一パケット攻撃イベントのロギングをイネーブルにします。ログメッセージはログシステムに送信されます。
Packet drop	防止アクションとしてパケットドロップを使用します。デバイスは、被害者の IP アドレス宛ての後続の攻撃パケットをドロップします。
Threshold (bytes)	安全な ICMP または ICMPv6 パケットの最大長(バイト単位)。 • ICMP パケットの場合は 28～65534。 • ICMPv6 パケットの場合は 48～65534。

単一パケット攻撃防御ポリシーを作成して、ユーザー定義シグニチャを持つパケットを検出するには、**Custom Single-Packet Attack Defense** ページにアクセスし、**Create** をクリックします。

表 7 ユーザー定義パケットシグニチャを使用した単一パケット攻撃防御ポリシーの設定項目

項目	説明
Signature	パケットシグニチャ: • **IP option**: 特定の IP オプションを持つ攻撃パケットを指定します。 • **ICMP** : ICMP 攻撃パケットを指定します。 • **ICMPv6**: ICMPv6 攻撃パケットを指定します。 • **IPv6 extension header**: IPv6 拡張ヘッダーを含む攻撃パケットを指定します。
Value	0～255 の範囲のシグニチャ値。この値は、IP オプションコード、または ICMP パケット、ICMPv6 パケット、または IPv6 拡張ヘッダーのタイプ値を示します。
Logging	単一パケット攻撃イベントのロギングをイネーブルにします。ログメッセージはログシステムに送信されます。
Packet drop	防止アクションとしてパケットドロップを使用します。デバイスは、被害者の IP アドレス宛ての後続の攻撃パケットをドロップします。

表 8 攻撃検出免除設定項目

項目	説明
IPv4 exemption	攻撃検出免除用の IPv4 ACL。既存の IPv4 ACL を選択するか、新しい IPv4 ACL を作成できます。作成された ACL は、**Objects >ACL(ACLs) > IPv4 ACLs(IPv4 ACLs)**ページに表示されます。 指定された ACL が存在しない場合、またはルールが含まれていない場合、攻撃検出の免除は有効になりません。
IPv6 exemption	攻撃検出免除用の IPv6 ACL。既存の IPv6 ACL を選択するか、新しい IPv6 ACL を作成できます。作成された ACL は、**Objects> ACL(ACLs) > IPv6 ACLs(IPv6 ACLs)**ページに表示されます。

	指定された ACL が存在しない場合、またはルールが含まれていない場合、攻撃検出の免除は有効になりません。

5. **OK** をクリックします。

Configure protected IP addresses

クライアント検証で保護された IP アドレスは、手動で追加することも自動で学習することもできます。デバイスは、クライアント検証がフラッド攻撃検出と連携するときに、被害者の IP アドレスを保護された IP リストに自動的に追加できます。デバイスは、信頼できる IP アドレスからのパケットを直接転送します。クライアント検証がフラッド攻撃防止アクションとして指定されていることを確認してください。

Protected IP Addresses ページには、手動で追加され自動的に学習された保護された IP アドレスが表示されます。

手順

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Attack Defense > Protected IP Addresses** を選択します。
3. **create** をクリックします。
4. 保護された IP アドレスを設定します。

表 9 保護された IP アドレスの構成項目

項目	説明
Protocol	クライアント検証のプロトコルタイプ: • **TCP**: TCP クライアント検証を指定します。 • **DNS**: DNS クライアントの確認を指定します。 • **DNS reply**: DNS クライアント送信元検証を指定します。 • **HTTP**: HTTP クライアント検証を指定します。 • **SIP**: SIP クライアント検証を指定します。
VRF	保護 IP アドレスが属する VRF。既存の VRF を選択するか、新しい VRF を作成できます。新しく作成された VRF は、**Network > VRF(VRF)**ページに表示されます。
IP version	IP バージョン(IPv4 または IPv6)を選択します。
IP address	保護された IP アドレス。このアドレス宛てのすべての接続要求は、クライアント検証機能によって検証されます。攻撃者は、TCP 接続要求、DNS クエリー、DNS 応答、HTTP GET 要求、HTTP POST 要求、または SIP UDP INVITE 要求を保護された IP に送信します。

	保護された IPv4 アドレスは、255.255.255.255 または 0.0.0.0 にできません。 保護された IPv6 アドレスは、マルチキャストアドレスまたは::にできません。
Port number	保護ポートの番号。デフォルトでは、DNS クライアント検証はポート 53 を保護し、HTTP クライアント検証はポート 80 を保護し、SIP クライアント検証はポート 5060 を保護し、TCP クライアント検証はすべてのポートを保護します。

5. **OK** をクリックします。

Configure the blacklist feature

ブラックリスト機能は、ブラックリストエントリ内の IP アドレスまたはアドレスオブジェクトグループによってパケットをフィルタリングする攻撃防御方法です。
ブラックリストエントリは、手動で追加することも、動的に学習することもできます。デバイスは、ブラックリスト機能がスキャン攻撃検出と連携する場合、IP ブラックリストエントリを自動的に追加できます。IP ブラックリストへの攻撃者の IP アドレスの追加が、スキャン攻撃防御アクションとして指定されていることを確認してください。動的に学習された各 IP ブラックリストエントリには、エージングタイムがあります。エージングタイムは、**Policies>Attack Defense > Attack Defense Policies > Scanning Attack Defense** ページで設定します。

Configure the IP blacklist

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Attack Defense > Blacklist** を選択します。
3. **create** をクリックします。
4. IP ブラックリストエントリを追加します。

表 10 IP ブラックリストの設定項目

項目	説明
VRF	ブラックリストが属する VRF。既存の VRF を選択するか、新しい VRF を作成できます。新しく作成された VRF は、**Network > VRF(VRF)**ページに表示されます。
IP version	IP バージョン(IPv4 または IPv6)を選択します。
Match field	基準と比較するパケットフィールド: • Source IP address。 • Destination IP address。

IP address	ブラックリストエントリの IP アドレス。この IP アドレスを送信元または宛先とするパケットはドロップされます。
DS-Lite tunnel peer address	ブラックリストに記載された IPv4 アドレスからパケットを送信する DS-Lite トンネルの B4 要素の IPv6 アドレス。 このパラメーターは、**IP version** に **IPv4** が選択され、**match** フィールドに **Source IP** が選択されている場合に使用できます。
Aging time (sec)	ブラックリストエントリのエージングタイム。エージングタイムを設定しない場合、ブラックリストエントリはエージングアウトしません。手動で削除する必要があります。

5. **OK** をクリックします。**IP Blacklist** ページに、新しく追加された IP ブラックリストが表示されます。
6. **Enable** をグローバルにクリックします。IP ブラックリストは、すべてのセキュリティーゾーンで有効になります。

Configure the address object group blacklist

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Attack Defense > Blacklist** を選択します。
3. **Address Object Group Blacklist** タブをクリックします。
4. **Add** をクリックします。
5. アドレスオブジェクトグループブラックリストエントリを追加します。

表 11 アドレスオブジェクトグループブラックリストの設定項目

項目	説明
Object group type	アドレスオブジェクトグループのタイプ(IPv4 または IPv6)を選択します。
Object group name	アドレスオブジェクトグループの名前を入力します。

6. **OK** をクリックします。**Address Object Group Blacklist** ページに、新しく追加されたアドレスオブジェクトグループのブラックリストが表示されます。
7. **Enable globally** をクリックします。アドレスオブジェクトグループブラックリストは、すべてのセキュリティーゾーンで有効になります。

Configure the whitelist

ホワイトリスト機能では、ホワイトリストに記載されたアドレスオブジェクトグループで指定された IP アドレスを発信元とするパケットが攻撃検出から除外されます。
アドレスオブジェクトグループは、ホワイトリストに対して手動でのみ追加または削除できます。アドレスオブジェクトグループを設定するには、**Objects > Object Groups** ページにアクセスします。

手順

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Attack Defense > Whitelist** を選択します。
3. **create** をクリックします。
4. アドレスオブジェクトグループをホワイトリストに追加します。

表 12 ホワイトリストの設定項目

項目	説明
Object group type	IP バージョン(IPv4 または IPv6)を選択します。
Object group name	既存のアドレスオブジェクトグループを選択するか、新規に作成できます。新しく作成されたアドレスオブジェクトグループは、Objects: Object Groups ページに表示されます。

5. **OK** をクリックします。

Configure security zone settings

クライアント検証設定には、保護された IP アドレスの追加、およびセキュリティーゾーンでのクライアント検証の有効化が含まれます。
ブラックリスト設定には、ブラックリスト機能のイネーブル化とブラックリストエントリの追加が含まれます。ブラックリスト機能は、グローバルにイネーブル化することも、セキュリティーゾーン単位でイネーブル化することもできます。ブラックリスト機能がグローバルにイネーブル化されている場合、すべてのセキュリティーゾーンでブラックリスト機能がイネーブルになります。グローバルブラックリスト機能をイネーブルにするには **Policies > Attack Defense > Blacklist** ページにアクセスします。
ホワイトリスト設定には、ホワイトリスト機能のイネーブル化とホワイトリストエントリーの追加が含まれます。ホワイトリスト機能は、グローバルにイネーブルにすることも、セキュリティーゾーン単位でイネーブルにすることもできます。ホワイトリスト機能がグローバルにイネーブルになっている場合、すべてのセキュリティーゾーンでホワイトリスト機能がイネーブルになります。グローバルホワイトリスト機能をイネーブルにするには、**Policies > Attack Defense > Whitelist** ページにアクセスします。

手順

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Attack Defense > Security Zone Settings** を選択します。
3. セキュリティーゾーンで、クライアント検証、ブラックリスト、またはホワイトリスト機能をイネーブルにします。

表 13 セキュリティーゾーンの構成項目

項目	説明
Security zone	セキュリティーゾーンを選択します。**Network** > **Security Zones** ページで新しいセキュリティーゾーンを作成できます。
TCP verification	セキュリティーゾーンでの TCP クライアント検証設定: • **Disable**: TCP クライアント検証をディセーブルにします。 • **SYN Cookie**: TCP クライアント確認用の双方向 TCP プロキシをイネーブルにします。 • **Safe Reset**: TCP クライアント検証用の単一方向 TCP プロキシをイネーブルにします。
DNS verification	セキュリティーゾーンで DNS クライアントの検証を有効または無効にします。
DNS reply source verification	セキュリティーゾーンで DNS 応答ソースの検証を有効または無効にします。
HTTP verification	セキュリティーゾーンで HTTP クライアントの検証を有効または無効にします。
SIP verification	セキュリティーゾーンで SIP クライアント検証を有効または無効にします。
Blacklist	セキュリティーゾーンでブラックリスト機能を有効または無効にします。
Whitelist	セキュリティーゾーンでホワイトリスト機能を有効または無効にします。

4. **Apply** をクリックします。

Connection limit

このヘルプには、次のトピックが含まれています。

- Introduction
  - Connection limit policies
  - Connection limit rules
- Restrictions and guidelines
- Configure connection limit

Introduction

接続制限機能により、デバイスは統計情報を収集し、確立された接続の数を制限できます。これにより、内部ネットワークリソースを保護し、システムリソースをより適切に割り当てることができます。

Connection limit policies

デバイスは、IPv4 と IPv6 の両方の接続制限ポリシーをサポートしています。設定された接続制限ポリシーをグローバルに適用するか、インターフェースに適用してユーザー接続の数を制限できます。
インターフェースに適用された接続制限ポリシーは、インターフェース上の指定された接続だけで有効になります。グローバルに適用された接続制限ポリシーは、デバイス上の指定されたすべての接続で有効になります。
個々のインターフェースおよびデバイス上でグローバルに異なる接続制限ポリシーを適用できます。この場合、デバイスは、着信インターフェース上のポリシー、グローバルポリシー、発信インターフェース上のポリシーの順に、これらのポリシーに対して接続を照合します。新しい接続は、接続数がこれらのポリシーで定義されている最小の接続上限に達している限り、制限されます。

Connection limit rules

接続制限ポリシーを使用するには、制限ルールをポリシーに追加する必要があります。各ルールは、接続の範囲と接続を制限する基準を定義します。範囲内の接続は基準に基づいて制限されます。次の基準を使用できます。

- **Connection limits**: 一致する接続の数を制限します。一致する接続の数が上限に達すると、デバイスは構成したアクションに応じて新しい接続を許可または拒否します。アクションが新しい接続を拒否する場合、デバイスは接続のエージングにより接続の数が下限を下回るまで新しい接続を許可しません。接続の数が上限を超えると、デバイスはログを送信します。接続の数が下限を下回ると、アクションが新しい接続を拒否する場合にのみ、デバイスはログを送信します。

- **Connection establishment rate limit**: 1 秒あたりに確立される接続数を制限します。接続確立レートが上限に達すると、デバイスは設定したアクションに応じて新しい接続を許可または拒否し、ログを記録します。

どの制限ルールにも一致しない接続は制限されません。

各接続制限ルールでは、ACL を使用して接続範囲を定義します。ACL に一致するユーザー接続のみが制限されます。また、ルールは次のフィルタ方法も使用して接続をさらに制限します。

- **Source IP** :送信元 IP アドレスによってユーザー接続を制限します。
- **Destination IP**: 宛先 IP アドレスによってユーザー接続を制限します。
- **Service port**: サービス(トランスポート層プロトコルおよびサービスポート)ごとにユーザー接続を制限します。

複数のフィルタ方法を選択できます。選択した方法は同時に有効になります。たとえば、**Destination IP** と **Service port**,の両方を指定すると、同じサービスを使用し、同じ IP アドレスを宛先とするユーザー接続が制限されます。制限ルールでフィルタ方法を指定しない場合は、範囲内のすべてのユーザー接続が制限されます。

接続制限ポリシーが適用されると、デバイスは、ポリシー内のすべての制限ルールとの接続を、ルール ID の昇順で比較します。ID が小さいルールでは、範囲を小さくし、フィルタリング方法を多く指定することをお勧めします。

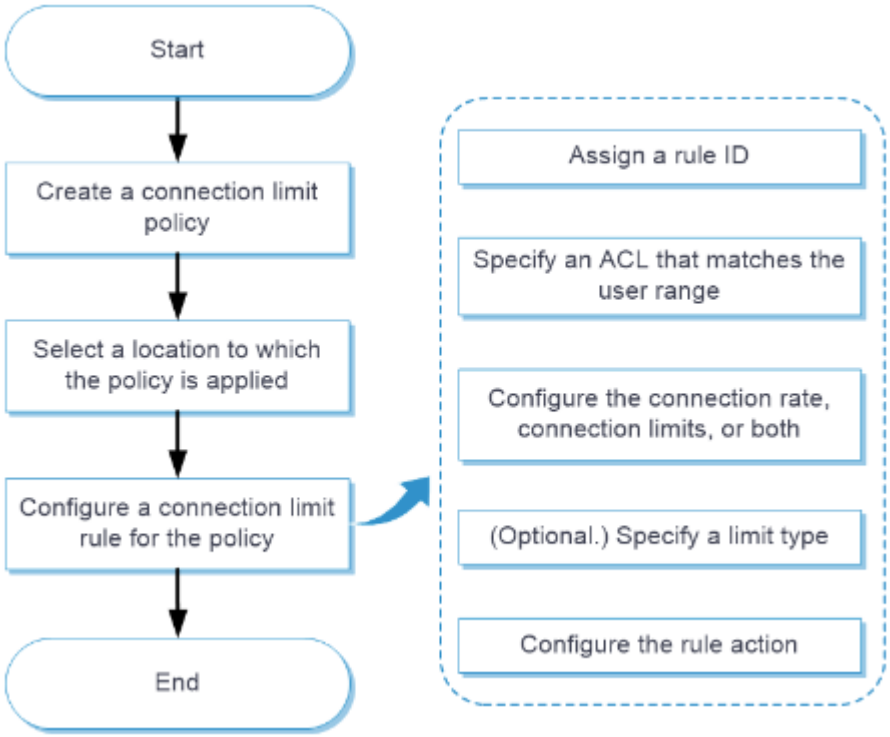
Restrictions and guidelines

- サービスモジュールをサポートするデバイスの場合、接続はサービスモジュール単位で制限されます。
- 接続制限ポリシーは、新規接続でのみ有効です。既存の接続では有効ではありません。
- セッション同期がイネーブルになっている IRF ファブリックでは、下位デバイスに適用された接続制限ポリシーは、マスターデバイスからスイッチされたセッションでは有効になりません。
- ACL は、接続制限ポリシーで一度だけ使用でき、複数の接続制限ポリシーで使用できます。

Configure connection limit

図 1 に示すように接続制限を設定します。

図 1 接続制限の設定手順



上限はデバイスの CPU コアの数より大きくなければなりません。上限は 32 より大きい値に設定することをお勧めします。

uRPF

このヘルプには、次のトピックが含まれています。

- Introduction
  - uRPF check modes
  - uRPF extended functions
  - uRPF operation
  - uRPF network application
- Restrictions and guidelines
- Configure uRPF
  - Configure IPv4 uRPF
  - Configure IPv6 uRPF

Introduction

Unicast Reverse Path Forwarding(uRPF)は、DoS 攻撃や DDoS 攻撃などの発信元アドレススプーフィング攻撃からネットワークを保護します。

攻撃者は、IP ベースの認証を使用するシステムにアクセスするために、認証されたユーザーまたは管理者の名前で、偽造された送信元アドレスを持つパケットを送信します。攻撃者または他のホストが応答パケットを受信できない場合でも、攻撃は攻撃されたターゲットを混乱させます。

図 1 送信元アドレススプーフィング攻撃

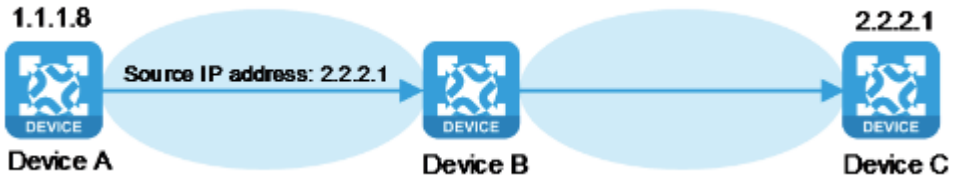


図 1 に示すように、攻撃者はデバイス A からサーバー(デバイス B)へのリクエストを送信します。送信元 IP アドレスは 2.2.2.1 です。デバイス B から IP アドレス 2.2.2.1(デバイス C)にレスポンスパケットが送信されます。その結果、デバイス B とデバイス C の両方が攻撃されます。管理者が誤ってデバイス C の接続を解除すると、ネットワークサービスが中断されます。

攻撃者は、偽造された異なるソースアドレスを持つパケットを送信したり、複数のサーバーを同時に攻撃して接続をブロックしたり、ネットワークを破壊したりすることもできます。

uRPF は、これらの送信元アドレススプーフィング攻撃を防ぐことができます。パケットを受信するインターフェースが、パケットの送信元アドレスと一致する FIB エントリの出力インターフェースであるかどう

かをチェックします。一致しない場合、uRPF はこれをスプーフィング攻撃と見なし、パケットを廃棄します。

uRPF check modes

uRPF は、strict モードと loose モードをサポートします。

Strict uRPF check

厳密な uRPF チェックに合格するには、パケットの送信元アドレスおよび受信インターフェースが、FIB エントリの宛先アドレスおよび出力インターフェースと一致する必要があります。一部のシナリオ(非対称ルーティングなど)では、厳密な uRPF が有効なパケットを廃棄する場合があります。
厳密な uRPF は、多くの場合、PE と CE の間に配置されます。

Loose uRPF check

loose uRPF チェックを通過させるには、パケットの送信元アドレスが FIB エントリの宛先アドレスと一致している必要があります。loose uRPF は有効なパケットの廃棄を回避できますが、攻撃パケットを解放する可能性があります。
Loose uRPF は、特に非対称ルーティングで、ISP 間に配置されることがよくあります。

uRPF extended functions

Using the default route in uRPF check

デフォルトルートが存在する場合、特定の FIB エントリと一致しないすべてのパケットは、uRPF チェック時にデフォルトルートと一致するため、通過が許可されます。この状況を回避するには、uRPF がデフォルトルートを使用してこのようなパケットを廃棄することをディセーブルにできます。デフォルトルートの使用を許可する場合、uRPF はデフォルトルートと一致するパケットだけを許可します。
デフォルトでは、uRPF はデフォルトルートとだけ一致するパケットを廃棄します。通常、PE デバイスには CE を指すデフォルトルートがないため、uRPF チェックにデフォルトルートを使用する必要はありません。CE インターフェースで uRPF をイネーブルにしていて、CE インターフェースに PE を指すデフォルトルートがある場合は、uRPF チェックにデフォルトルートを使用します。

Link layer check (only supported by IPv4 uRPF)

厳密な uRPF チェックでは、さらにパケットに対してリンク層チェックを実行できます。一致する FIB エントリ内のネクストホップアドレスを使用して、ARP テーブルで一致するエントリを検索します。パケットの

送信元 MAC アドレスが一致する ARP エントリ内の MAC アドレスと一致する場合、パケットは厳密な uRPF チェックを通過します。リンク層チェックは、レイヤー3 イーサネットインターフェースが多数の PC に接続されている ISP デバイスに適用されます。
Loose uRPF はリンク層チェックをサポートしません。

Using an ACL for uRPF check exemption

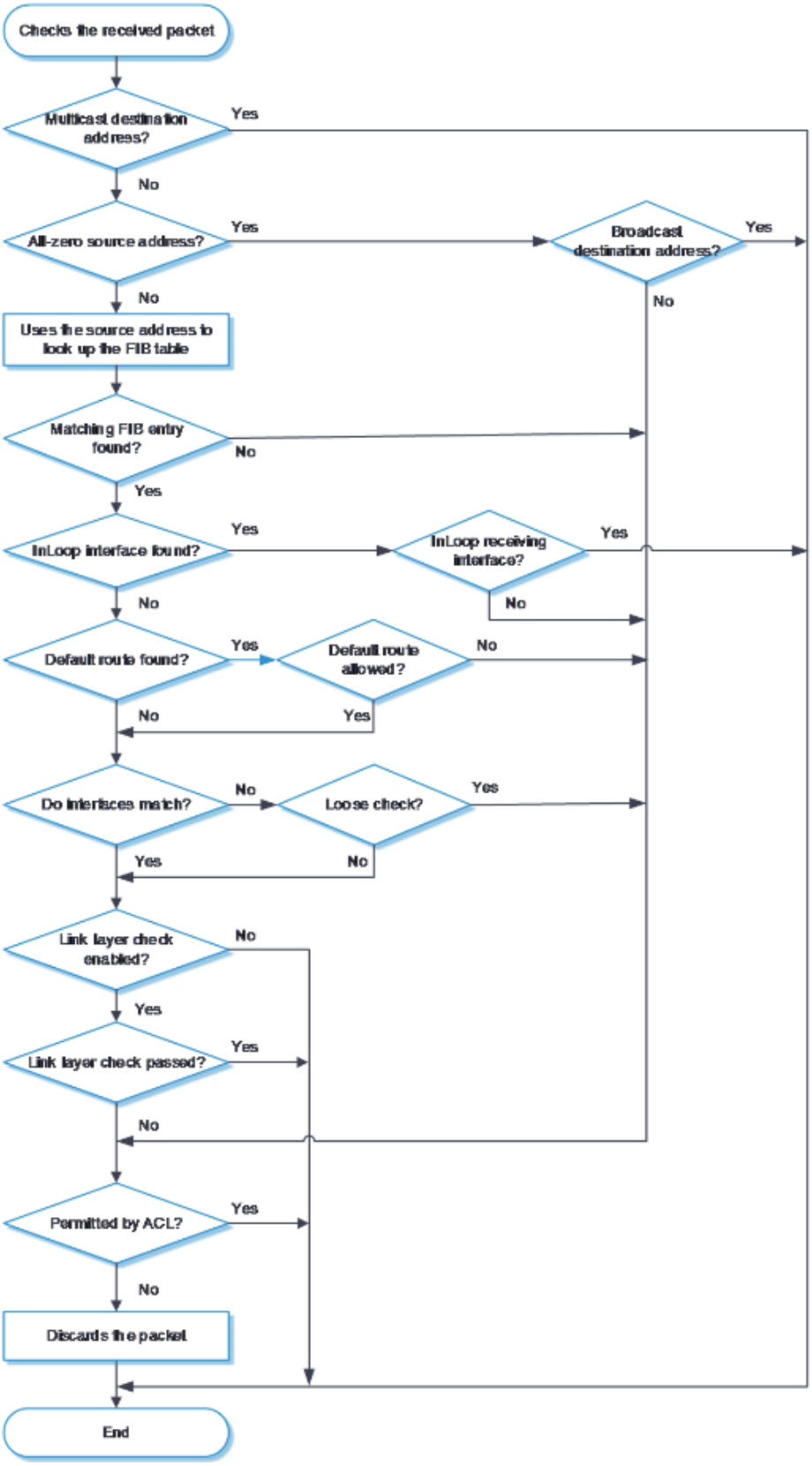
特定のパケットを有効なパケットとして識別するには、ACL を使用してこれらのパケットを照合します。パケットが uRPF チェックに合格しない場合でも、転送されます。

uRPF operation

IPv4 uRPF operation

次の図は、IPv4 uRPF の動作を示しています。

図 2 IPv4 uRPF のワークフロー



1. uRPF はアドレスの有効性をチェックします。
   - uRPF は、マルチキャスト宛先アドレスを持つパケットを許可します。

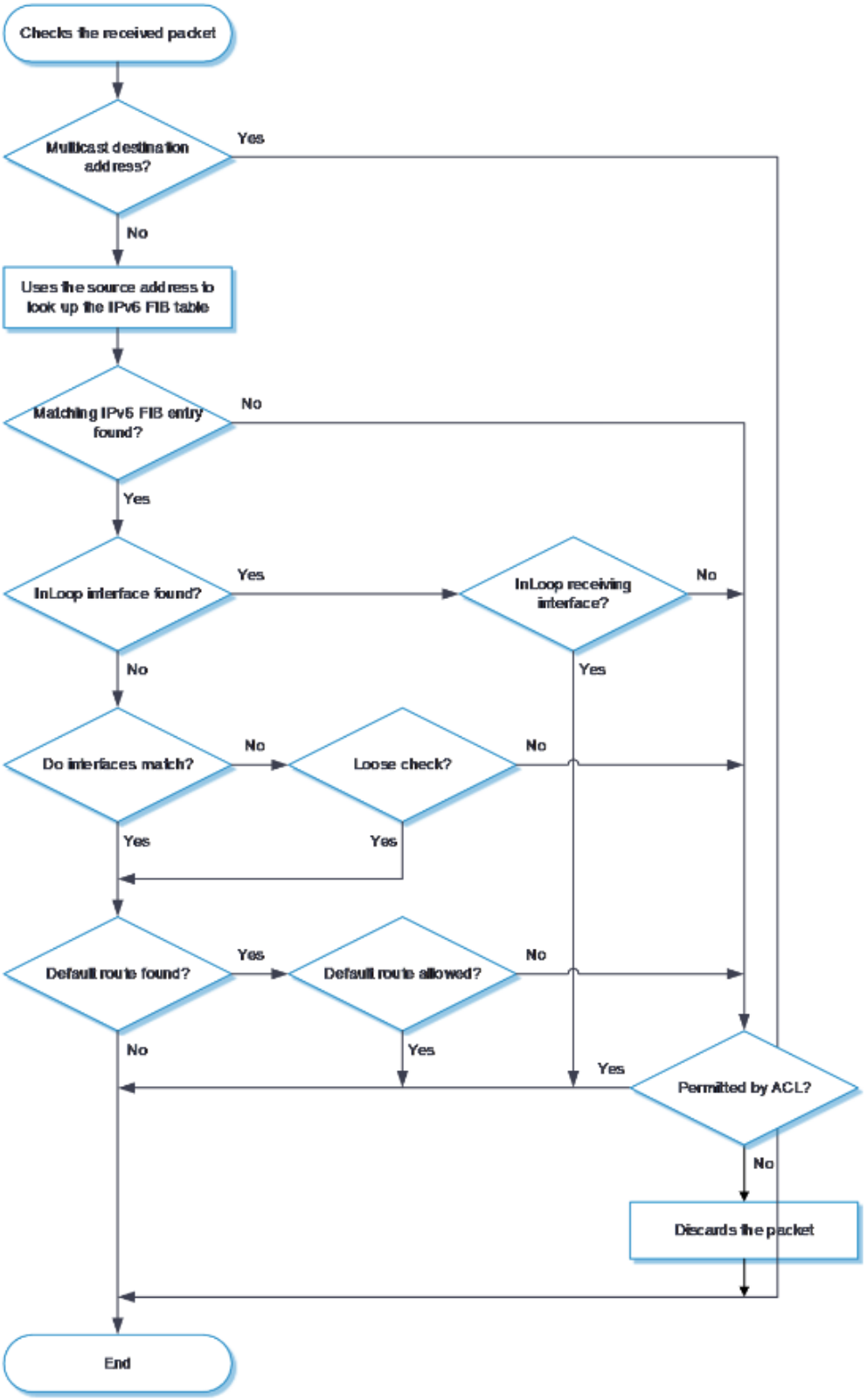
- 送信元アドレスがすべて 0 のパケットの場合、uRPF は、ブロードキャスト宛先アドレスを持つパケットを許可します(送信元アドレスが 0.0.0.0 で宛先アドレスが 255.255.255.255 のパケットは、DHCP または BOOTP パケットの場合があり、廃棄できません)。パケットに非ブロードキャスト宛先アドレスがある場合、uRPF はステップ 7 に進みます。
- 他のパケットについては、uRPF はステップ 2 に進みます。

2. uRPF は、送信元アドレスがユニキャストルートと一致するかどうかをチェックします。
   - そうであれば、uRPF はステップ 3 に進む。
   - No の場合、uRPF はステップ 7 に進む。非ユニキャスト送信元アドレスは非ユニキャストルートと一致します。
3. uRPF は、一致するルートがホスト自体へのものかどうかをチェックします。
   - yes の場合、一致するルートの出力インターフェースは InLoop インターフェースです。uRPF は、パケットの受信インターフェースが InLoop インターフェースであるかどうかをチェックします。yes の場合、パケットはチェックされません。no の場合、ステップ 7 に進みます。
   - そうでない場合、uRPF はステップ 4 に進む。
4. uRPF は、一致するルートがデフォルトルートであるかどうかをチェックします。
   - yes の場合、uRPF はデフォルトルートが許可されているかどうかをチェックします。yes の場合、ステップ 5 に進みます。no の場合、ステップ 7 に進みます。
   - そうでない場合、uRPF はステップ 5 に進む。
5. uRPF は、受信インターフェースが一致する FIB エントリの出力インターフェースと一致するかどうかをチェックします。
   - そうであれば、uRPF はステップ 6 に進む。
   - no の場合、uRPF はチェックモードが loose であるかどうかをチェックします。yes の場合、ステップ 7 に進みます。no の場合、ステップ 6 に進みます。
6. uRPF は、リンク層チェックが設定されているかどうかをチェックします。
   - no の場合、パケットはチェックを通過します。
   - yes の場合、uRPF は FIB エントリのネクストホップアドレスを使用して ARP テーブルを検索し、一致するエントリを探します。次に、一致する ARP エントリの MAC アドレスがパケットの送信元 MAC アドレスと同一であるかどうかをチェックします。yes の場合、パケットはチェックを通過します。no の場合、uRPF はステップ 7 に進みます。
7. uRPF は、パケットが ACL によって許可されているかどうかをチェックします。
   - Yes の場合、パケットは転送されます。このようなパケットはドロップされません。
   - no の場合、パケットは廃棄されます。

IPv6 uRPF operation

次の図は、IPv6 uRPF の動作を示しています。

図 3 IPv6 uRPF のワークフロー



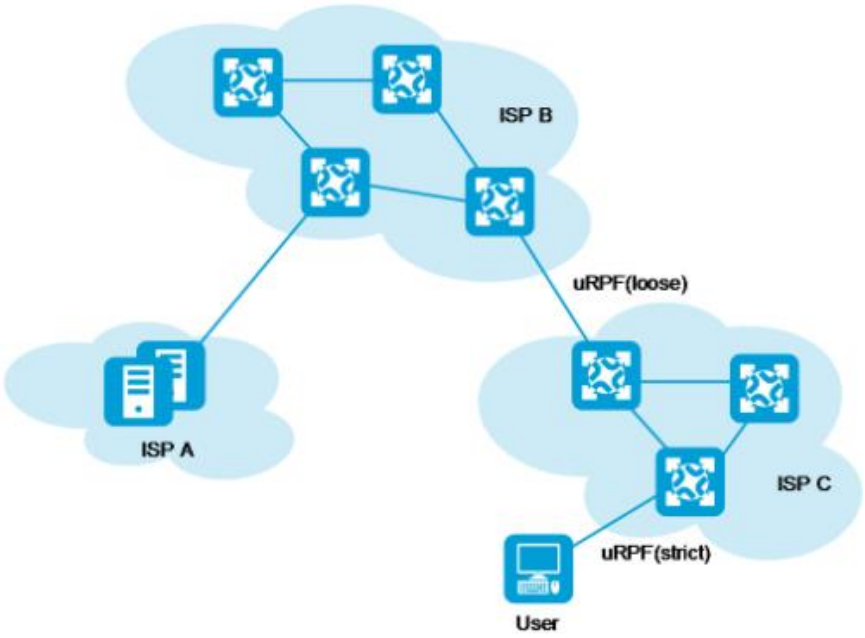
1. IPv6 uRPF は、受信したパケットにマルチキャスト宛先アドレスが含まれているかどうかをチェックします。
   - yes の場合、IPv6 uRPF はパケットを許可します。

- そうでない場合、IPv6 uRPF はステップ 2 に進みます。

2. IPv6 uRPF は、送信元アドレスがユニキャストルートと一致するかどうかをチェックします。
   - Yes の場合、IPv6 uRPF はステップ 3 に進みます。
   - no の場合、IPv6 uRPF はステップ 6 に進みます。非ユニキャスト送信元アドレスは非ユニキャストルートと一致します。
3. IPv6 uRPF は、一致するルートがホスト自体へのものかどうかをチェックします。
   - yes の場合、一致するルートの出力インターフェースは InLoop インターフェースです。IPv6 uRPF は、パケットの受信インターフェースが InLoop インターフェースであるかどうかをチェックします。yes の場合、IPv6 uRPF はパケットを許可します。no の場合、IPv6 uRPF はステップ 6 に進みます。送信元アドレスがリンクローカルアドレスであり、受信インターフェースアドレスである場合も、ステップ 6 に進みます。
   - そうでない場合、IPv6 uRPF はステップ 4 に進みます。
4. IPv6 uRPF は、受信インターフェースが一致する FIB エントリの出力インターフェースと一致するかどうかをチェックします。
   - Yes の場合、IPv6 uRPF はステップ 5 に進みます。
   - no の場合、IPv6 uRPF はチェックモードが loose であるかどうかをチェックします。yes の場合、ステップ 5 に進みます。no の場合、ステップ 6 に進みます。
5. IPv6 uRPF は、一致するルートがデフォルトルートであるかどうかをチェックします。
   - yes の場合、IPv6 uRPF はデフォルトルートが許可されているかどうかをチェックします。yes の場合、パケットは転送されます。no の場合、IPv6 uRPF はステップ 6 に進みます。
   - no の場合、パケットは転送されます。
6. IPv6 uRPF は、パケットが IPv6 ACL によって許可されているかどうかをチェックします。
   - Yes の場合、パケットは転送されます。このようなパケットはドロップされません。
   - no の場合、パケットは廃棄されます。

uRPF network application

図 4 ネットワーク図



ISP ネットワークとカスタマーネットワーク間では、厳格な uRPF チェックが設定されます。ISP 間では、緩やかな IPv6 uRPF チェックが設定されます。
特殊なパケットまたはユーザーに対して、ACL を設定できます。

Restrictions and guidelines

Allow using default route for uRPF check for loose uRPF check を選択しないでください。選択しないと、uRPF が動作しなくなる可能性があります。

Configure uRPF

Configure IPv4 uRPF

手順

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Attack defense > uRPF > IPv4 uRPF** を選択します。
3. **create** をクリックします。
4. IPv4 uRPF を設定します。

表 1 IPv4 uRPF 設定項目

項目	説明
Security zone	IPv4 uRPF が適用されるセキュリティーゾーンを選択します。 このリストには、デフォルトのセキュリティーゾーンと、**Network > Security Zones** ページで設定されたセキュリティーゾーンが含まれています。
Check mode	• **Strict**: 厳密な uRPF チェック。厳密な uRPF チェックに合格するには、パケットの送信元アドレスおよび受信インターフェースが、FIB エントリの宛先アドレスおよび出力インターフェースと一致する必要があります。 • **Loose**: 緩やかな uRPF チェック。緩やかな uRPF チェックを通過させるには、パケットの送信元アドレスが FIB エントリの宛先アドレスと一致する必要があります。
Check exemption	パケットドロップを抑制する ACL を選択します。 既存の IPv4 ACL を選択するか、新規に作成できます。作成された ACL は、≪オブジェクト **Objects > ACLs > IPv4 ACLs** ページに表示されます。
Allow using default route for uRPF check	uRPF チェックにデフォルトルートの使用を許可するかどうかを選択します。
Enable link layer check	リンク層チェックを有効にするかどうかを選択します。

5. **OK** をクリックします。

Configure IPv6 uRPF

手順

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Attack defense > uRPF > IPv6 uRPF** を選択します。
3. **create** をクリックします。
4. IPv6 uRPF を設定します。

表 2 IPv6 uRPF 設定項目

項目	説明
Security zone	IPv6 uRPF が適用されるセキュリティーゾーンを選択します。

	このリストには、デフォルトのセキュリティーゾーンと、**Network > Security Zones** ページで設定されたセキュリティーゾーンが含まれています。
Check mode	• **Strict**: 厳密な IPv6 uRPF チェック。厳密な IPv6 uRPF チェックに合格するには、パケットの送信元アドレスおよび受信インターフェースが、IPv6 FIB エントリの宛先アドレスおよび出力インターフェースと一致する必要があります。 • **Loose**: 緩やかな IPv6 uRPF チェック。緩やかな IPv6 uRPF チェックを通過させるには、パケットの送信元アドレスが IPv6 FIB エントリの宛先アドレスと一致する必要があります。
Check exemption	パケットドロップを抑制する ACL を選択します。 既存の IPv6 ACL を選択するか、新規に作成できます。作成された ACL は、≪オブジェクト **Objects > ACLs > IPv6 ACLs** ページに表示されます。
Allow using default route for uRPF check	uRPF チェックにデフォルトルートの使用を許可するかどうかを選択します。

5. **OK** をクリックします。

IP reputation

このヘルプには、次のトピックが含まれています。

- Introduction
  - IP reputation list
  - Attack category and action
  - Exception IP list
  - Blacklist operation
  - IP reputation workflow
- Restrictions and guidelines
- Configure IP reputation
  - Enable IP reputation
  - Enable top hit statistics collection
  - Configure the action for an attack category
  - Configure the exception IP list

Introduction

IP レピュテーションは、IP レピュテーションリストの IP アドレス情報を使用して、ネットワークトラフィックをフィルタリングします。

IP reputation list

IP レピュテーションリストには、攻撃カテゴリ、推奨処置、および DDoS、コマンドインジェクション攻撃、トロイの木馬ダウンロード攻撃、ポートスキャンなどの潜在的な攻撃リスクを持つ IP アドレスのロギング情報が含まれています。

Attack category and action

パケットの送信元 IP アドレスまたは宛先 IP アドレスが IP レピュテーションリストでヒットした場合、デバイスはアクション(**drop** または **permit**)を実行します。パケットのロギングもサポートされています。
IP レピュテーションリストでは、1 つの IP アドレスが複数の攻撃カテゴリに属する可能性があります。各攻撃カテゴリには、アクションが関連付けられています。
IP アドレスが 1 つの攻撃カテゴリにしか属していない場合、一致するパケットに対してデバイスが実行するアクションは、その攻撃カテゴリのアクションと一致します。IP アドレスが複数の攻撃カテゴリに属

する場合、デバイスは、その攻撃カテゴリのすべてのアクションの中で最も高いプライオリティを持つアクションを実行します。**drop** アクションは、**permit** アクションよりも高いプライオリティを持ちます。
IP アドレスが属する攻撃カテゴリのいずれかでロギングがイネーブルになっている場合、デバイスは一致するパケットのログを生成します。

Explicit IP list

送信元 IP アドレスまたは宛先 IP アドレスが例外 IP リストと一致する場合、パケットは転送されます。デバイスは、この送信元または宛先 IP アドレスを持つ後続の IP パケットに対して IP レピュテーションチェックを実行しません。

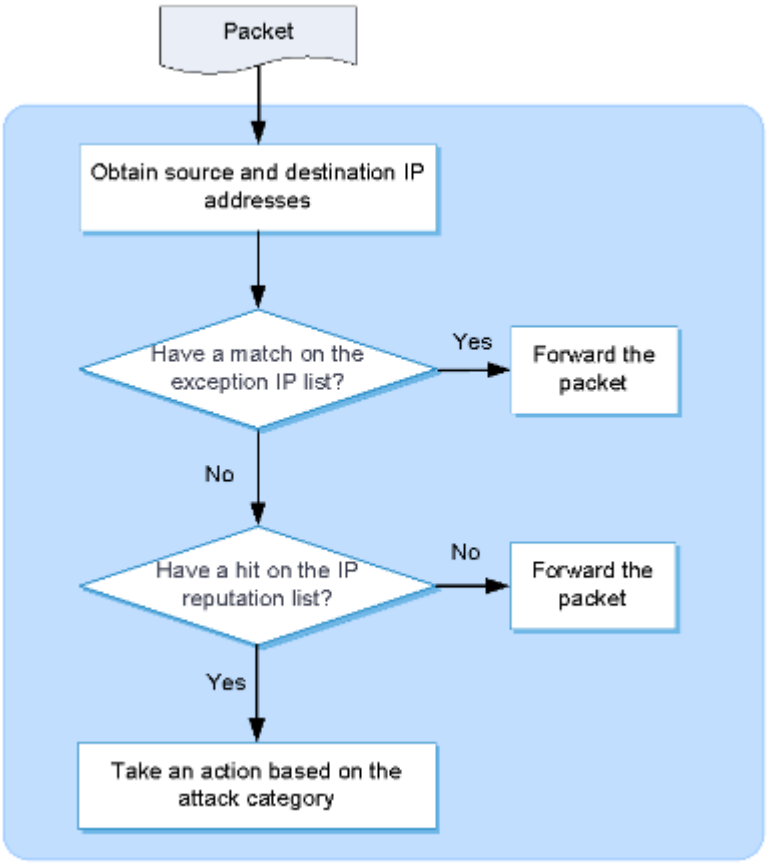
Blacklist operation

デバイスは、IP レピュテーションリスト上の IP アドレスのブラックリストへの追加またはブラックリストからの削除をサポートしています。IP レピュテーションリスト上の IP アドレスは、IP アドレスの方向アトリビュートに応じて、送信元アドレスのブラックリストまたは宛先アドレスのブラックリストに追加できます。
IP レピュテーションリストのすべての IP アドレスはパブリックアドレスです。VRF は、IP レピュテーションに基づいて追加されるブラックリストエントリ用のパブリックネットワークです。
ブラックリストエントリのデフォルトのエージングタイムは 7 日です。エージングタイムを変更するには、**Policies > Attack Defense > Blacklist** ページにアクセスします。
ブラックリストの詳細については、攻撃防御のヘルプを参照してください。

IP reputation workflow

図 1 に、IP レピュテーションのワークフローを示します。

図 1 IP レピュテーションのワークフロー



IP レピュテーションは、パケットを次のように処理します。

1. デバイスは、送信元 IP アドレスまたは宛先 IP アドレスが例外 IP リストに一致するかどうかを判断します。一致するものが見つかった場合、パケットはパススルーされます。一致するものがない場合、デバイスは次のステップに進みます。
2. デバイスは、送信元 IP アドレスまたは宛先 IP アドレスが IP レピュテーションリストで一致するかどうかを判断します。IP レピュテーションリストの IP アドレスには、送信元、宛先、双方向などの方向アトリビュートがあります。パケット内の IP アドレスがリスト上の IP アドレスと同じ方向アトリビュートを持っている場合にのみ、一致が成功します。IP アドレスの方向アトリビュートが双方向の場合、送信元または宛先 IP アドレスが IP レピュテーションリスト上の IP アドレスと同じであれば、一致が成功します。一致が検出されると、デバイスは IP アドレスの攻撃カテゴリに基づいてアクションを実行します。一致がない場合、デバイスはパケットを転送します。デバイスは次のアクションをサポートします。
   - **Permit**:パケットの通過を許可します。
   - **Drop**:パケットをドロップします。
   - **Logging**: IP レピュテーションログを生成します。

Restrictions and guidelines

- IP レピュテーション機能を使用するには、この機能のライセンスを購入して正しくインストールしてください。ライセンスの有効期限が切れると、既存の IP レピュテーションリストが使用可能になりますが、アップグレードできません。詳細については、ライセンスヘルプを参照してください。
- トップヒット統計情報をディセーブルにすると、トップヒット統計情報がクリアされます。
- IP レピュテーションによって追加された送信元 IP ブラックリストエントリには、DS-Lite ピアアドレス情報が含まれません。DS-Lite ピアアドレス情報を変更するには、**Policies > Attack Defense > Blacklist** ページにアクセスします。
- IP レピュテーションリストの更新が 7 日間連続して失敗した場合、デバイスは IP レピュテーションリストをクリアし、IP レピュテーションは使用できなくなります。
- システム時刻がネットワーク時刻と同じであることを確認します。

Configure IP reputation

Enable IP reputation

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > IP Reputation** の順に選択します。
3. **IP reputation** で **enable** を選択します。
4. IP アドレスを問い合せるには、**IP address search** をクリックし、IP アドレスを入力して Search をクリックします。IP アドレスに関する情報が表示されます。ブラックリストまたは例外 IP リストに IP アドレスを追加したり、リストから IP アドレスを削除したりできます。

Enable top hit statistics collection

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > IP Reputation** の順に選択します。
3. **IP reputation** で **enable** を選択します。
4. **IP address hit statistics** で **Enable** を選択します。
5. **Top Hit Statistics** ページを開くには、**Top hit statistics** をクリックします。上位ヒット統計ランキング情報を表示するには、統計条件を構成します。IP アドレスをブラックリストまたは例外 IP リストに追加したり、リストから削除することもできます。

Configure the action for an attack category

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > IP Reputation** の順に選択します。
3. **IP reputation** で **enable** を選択します。

4. アクション設定領域で、攻撃カテゴリのアクションを設定します。サポートされているアクションは次のとおりです。
    - **Permit:** パケットの通過を許可します。
    - **Drop**: パケットをドロップします。
5. 既定の設定に戻すには、**Restore default** をクリックします。
6. **Apply** をクリックします。

Configure the exception IP list

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > IP Reputation** の順に選択します。
3. **IP reputation** で **enable** を選択します。
4. **Exception IP list** 領域に IP アドレスを入力します。各 IP アドレスは 1 行に表示されます。
5. **Apply** をクリックします。

Domain reputation

このヘルプには、次のトピックが含まれています。

- Introduction
  - Domain reputation signature library
  - Attack category and action
  - Domain name exception list
  - Domain reputation workflow
- Restrictions and guidelines
- Configure domain reputation
  - Configure domain reputation
  - Enable top hit statistics collection
  - Configure the action for an attack category
  - Configure the domain name exception list

Introduction

ドメインレピュテーションは、ドメインレピュテーション署名ライブラリ内のドメイン名情報を使用してネットワークトラフィックをフィルタリングします。

Domain reputation signature library

ドメインレピュテーションシグニチャライブラリには、ゾンビホスト DDoS 攻撃、コマンドインジェクション攻撃、トロイの木馬ウィルスダウンロード攻撃、ポートスキャンなどのリスクを持つドメイン名が含まれています。シグニチャライブラリには、各ドメイン名の攻撃タイプ、推奨されるアクション、ログを記録するかどうかなどの情報が含まれています。詳細については、シグニチャのアップグレードヘルプを参照してください。

Attack category and action

DNS パケットのドメイン名がドメインレピュテーションシグニチャライブラリでヒットした場合、デバイスはアクション(**drop** または **permit**)を実行します。パケットのロギングもサポートされています。
ドメインレピュテーションシグニチャライブラリでは、ドメイン名は複数の攻撃カテゴリに属する可能性があります。各攻撃カテゴリには、関連付けられたアクションがあります。
ドメイン名が 1 つの攻撃カテゴリにしか属していない場合、デバイスはパケットに対して攻撃カテゴリのアクションを実行します。ドメイン名が複数の攻撃カテゴリに属する場合、デバイスは攻撃カテゴリのす

べてのアクションの中で最も高いプライオリティを持つアクションを実行します。**drop** アクションは、**permit** アクションよりも高いプライオリティを持ちます。
ドメイン名が属する攻撃カテゴリのいずれかでロギングがイネーブルになっている場合、デバイスは一致するパケットのログを生成します。

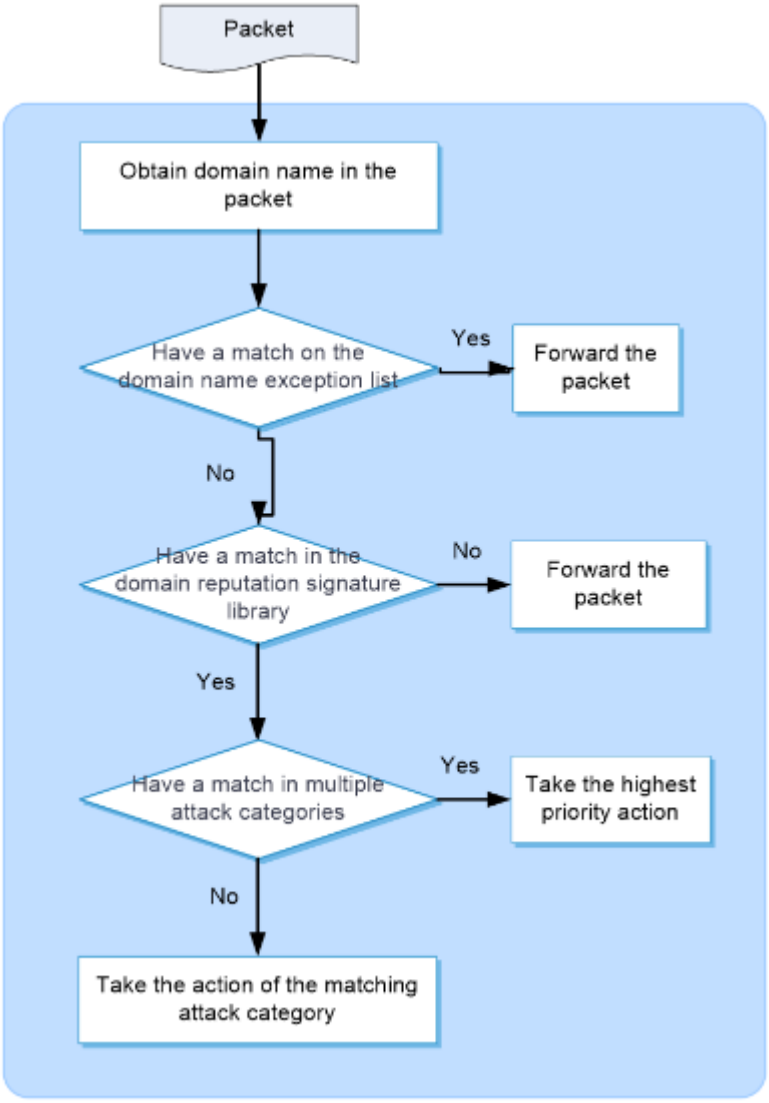
Domain name exception list

ドメイン名例外リストにドメイン名が含まれている場合、パケットは直接転送されます。デバイスはパケットに対してドメインレピュテーションチェックを実行しません。

Domain reputation workflow

図 1 に、ドメインレピュテーションのワークフローを示します。

図 1 ドメインレピュテーションワークフロー



ドメインレピュテーションは、パケットを次のように処理します。

2. デバイスは、パケット内のドメイン名がドメイン名例外リストと一致するかどうかを判断します。一致するものが見つかった場合、パケットは直接転送されます。一致するものがない場合、デバイスは次のステップに進みます。

3. デバイスは、ドメイン名がドメインレピュテーションシグニチャライブラリに一致するかどうかを判断し、対応するアクションを実行します。

○ 一致が見つかった場合、デバイスは一致する攻撃カテゴリのアクションを実行します。

○ 複数の一致が検出された場合、デバイスは、攻撃カテゴリのすべてのアクションの中で最も高いプライオリティを持つアクションを実行します。

○ 一致が見つからない場合、デバイスはパケットを転送します。

次のアクションがサポートされています。

- **Permit**: パケットの通過を許可します。
- **Drop**: パケットをドロップします。

- **Logging**: ドメインレピュテーションログを生成します。

Restrictions and guidelines

- ドメインレピュテーション機能を使用するには、この機能のライセンスを購入し、正しくインストールしてください。ライセンスの有効期限が切れると、既存のドメインレピュテーション署名ライブラリが使用可能になりますが、アップグレードできません。詳細については、ライセンスヘルプを参照してください。
- トップヒット統計情報をディセーブルにすると、トップヒット統計情報がクリアされます。
- システム時刻がネットワーク時刻と同じであることを確認します。

Configure domain reputation

Configure domain reputation

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > Domain Reputation** を選択します。
3. **Domain Reputation** で **enable** を選択します。
4. ドメイン名を検索するには、**domain name search** をクリックし、ドメイン名を入力して **search** をクリックします。一致するドメイン名に関する情報が表示されます。ドメイン名の例外リストにドメイン名を追加したり、ドメイン名の例外リストからドメイン名を削除したりできます。

Enable top hit statistics collection

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > Domain Reputation** を選択します。
3. **Domain Reputation** で **enable** を選択します。
4. **Domain name hit statistics** で **Enable** を選択します。
5. **Top Hit Statistics** ページを開くには、**Top hit statistics** をクリックします。上位ヒット統計ランキング情報を表示するには、統計条件を構成します。ドメイン名例外リストにドメイン名を追加したり、ドメイン名例外リストからドメイン名を削除したりすることもできます。
6. **policies** タブをクリックします。
7. ナビゲーションペインで、**Threat Intelligence > Domain Reputation** を選択します。
8. **Domain Reputation** で **enable** を選択します。
9. **Domain name hit statistics** で **Enable** を選択します。

10. **Top Hit Statistics** ページを開くには、**Top hit statistics** をクリックします。上位ヒット統計ランキング情報を表示するには、統計条件を構成します。ドメイン名例外リストにドメイン名を追加したり、ドメイン名例外リストからドメイン名を削除したりすることもできます。

Configure the action for an attack category

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > Domain Reputation** を選択します。
3. **Domain Reputation** で **enable** を選択します。
4. アクション設定領域で、攻撃カテゴリのアクションを設定します。サポートされているアクションは次のとおりです。
   - **Permit**: パケットの通過を許可します。
   - **Drop**: パケットをドロップします。
5. 既定の設定に戻すには、**restore default** をクリックします。
6. **Apply** をクリックします。

Configure the domain name exception list

1. **policies** タブをクリックします。
2. ナビゲーションペインで、**Threat Intelligence > Domain Reputation** を選択します。
3. **Domain Reputation** で **enable** を選択します。
4. **Domain name exception list** 領域で、ドメイン名を入力します。各ドメイン名は 1 行に表示されます。
5. **Apply** をクリックします。

URL filtering

このヘルプには、次のトピックが含まれています。

- Introduction
  - URL
  - URL filtering rule
  - URL category
  - URL filtering profile
  - URL filtering whitelist/blacklist rule
  - URL filtering cloud query
  - URL filtering action
  - HTTPS URL filtering
  - URL filtering mechanism
- Restrictions and guidelines
  - Restrictions and guidelines: Text-based URL filtering rule configuration
  - Restrictions and guidelines: Regular expression-based URL filtering rule configuration
  - Restrictions and guidelines: Whitelist
  - Restrictions and guidelines: URL filtering profile activation
  - Restrictions and guidelines: Licensing requirements
  - Restrictions and guidelines: HTTPS URL filtering
- Configure URL filtering
  - Configure a URL category
  - Configure the cloud query server
  - Configure a URL filtering profile

Introduction

URL フィルタリングは、ユーザーがアクセスする URL をフィルタリングすることによって、Web リソースへのアクセスを制御します。

URL

URL はリソースへの参照で、ネットワーク上のリソースの場所と、そのリソースを取得するためのメカニズムを指定します。URL の構文は protocol://hostname[:port]/path/[;parameters][?query]#fragment です。図 1 に URL の例を示します。

図 1 URL の構文

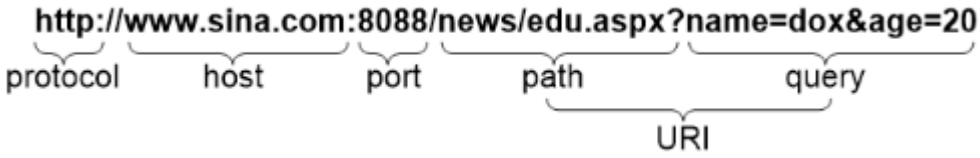


表 1 は、URL のフィールドについて説明しています。

表 1 URL フィールドの説明

フィールド	説明
protocol	伝送プロトコル(HTTP など)。
host	示されたリソースが存在するサーバーのドメイン名または IP アドレス。
[:port]	伝送プロトコルのポート番号を識別するオプションフィールド。このフィールドを省略すると、プロトコルのデフォルトのポート番号が使用されます。
/path/	示されたリソースが保管されているディレクトリーまたはファイルを識別するストリング。パスは、0 または複数のスラッシュで区切られた一連のセグメントです。
[parameters]	特殊パラメーターを含むオプションフィールド。
[?query]	動的 Web ページを照会するためにソフトウェアに渡されるパラメーターを含むオプションのフィールドです。各パラメーターは<key>=<value>のペアです。異なるパラメーターはアンパサンド(&)で区切られます。
URI	ネットワーク上のリソースを識別する統一リソース識別子。

URL filtering rule

URL フィルタリング規則は、URI またはホスト名フィールドの内容に基づいて URL を照合します。
URL フィルタリングでは、次のタイプの URL フィルタリング規則が提供されます。

- **Predefined URL filtering rules**: 署名ベースの URL フィルタリング規則。デバイスは、ローカルの URL フィルタリング署名に基づいて自動的に URL フィルタリング規則を生成します。ほとんどの場合、URL フィルタリングには事前定義された規則で十分です。
- **User-defined URL filtering rules**: 手動で設定された正規表現またはテキストベースの URL フィルタリング規則。

URL フィルタリング規則では、次の URL マッチング方法がサポートされます。

- **Text-based matching**: URL の hostname フィールドと URI フィールドをテキストパターンと照合します。

  URL のホスト名フィールドに対してテキストベースのマッチングを実行する場合、デバイスはまず、テキストパターンの先頭または末尾にアスタリスク(*)ワイルドカード文字が含まれているかどうかを判別します。

○ テキストパターンの先頭または末尾にアスタリスク(*)ワイルドカード文字が含まれていない場合、URL のホスト名がテキストパターンと一致すれば、ホスト名の照合は成功します。

○ テキストパターンの先頭にアスタリスク(*)ワイルドカード文字が含まれている場合、URL のホスト名がワイルドカード文字を含まないテキストパターンと一致するか、そのテキストパターンで終了すると、ホスト名の照合が成功します。

○ テキストパターンの末尾にアスタリスク(*)ワイルドカード文字が含まれている場合、URL のホスト名が、ワイルドカード文字を含まないテキストパターンと一致するか、そのテキストパターンで始まると、ホスト名の照合が成功します。

○ テキストパターンの先頭と末尾の両方にアスタリスク(*)ワイルドカード文字が含まれている場合、URL のホスト名がワイルドカード文字なしのテキストパターンと一致するか、含まれていれば、ホスト名の一致は成功します。

URI フィールドに対するテキストベースのマッチングは、hostname フィールドに対するテキストベースのマッチングと同じように機能します。

- **Regular expression-based matching**: URL のホスト名および URI フィールドを正規表現と照合します。たとえば、ホスト名照合用の正規表現を **sina.*cn** に設定すると、**news.sina.com.cn** ホスト名を含む URL が照合されます。

URL category

URL フィルタリングには、フィルタリング規則の管理を容易にするための URL カテゴリ化機能があります。

複数の URL フィルタルールを 1 つの URL カテゴリに分類し、そのカテゴリの処理を指定できます。一致するルールが複数の URL カテゴリにある場合は、重大度が最も高いカテゴリの処理が実行されます。

URL フィルタリングでは、次のタイプの URL カテゴリがサポートされています。

- Predefined URL categories。
  事前定義済の URL カテゴリには、事前定義済の URL フィルタルールが含まれています。事前定義済の各 URL カテゴリには、1 から 999 までの一意の重大度レベルがあり、
  Pre-.Predefined URL カテゴリで始まるカテゴリ名は変更できません。
- User-defined URL categories。
  URL カテゴリを手動で作成し、フィルタルールを構成できます。ユーザー定義 URL カテゴリの重大度レベルは 1000 から 65535 の範囲です。フィルタルールを編集し、ユーザー定義 URL カテゴリの重大度レベルを変更できます。

URL filtering profile

URL フィルタリングプロファイルには複数の URL カテゴリを含めることができます。各カテゴリには、カテゴリ内のフィルタリング規則に一致するパケットに対して定義されたアクションがあります。プロファイ

ル内のどのフィルタリング規則にも一致しないパケットに対してデフォルトアクションを指定することもできます。

URL filtering whitelist/blacklist rule

デバイスは、URL ベースのホワイトリストおよびブラックリストルールを使用しした HTTP パケットのフィルタリングがサポートされています。HTTP パケット内の URL がブラックリストルールと一致する場合、パケットはドロップされます。URL がホワイトリストルールと一致する場合、パケットの通過が許可されます。

URL filtering cloud query

URL フィルタリングプロファイルでクラウドクエリーをイネーブルにして、HTTP トラフィックの URL フィルタリング精度を向上させることができます。
クラウドクエリーを有効にすると、デバイスはローカル URL フィルタリング規則に一致しない URL をクラウドサーバーに送信してクエリーを実行します。デバイスは、クラウドサーバーから返されたクエリー結果に基づいて、適用するアクションを決定します。

- URL に一致するルールが検出された場合は、ルールが属する URL カテゴリに指定されたアクションが適用されます。ルールが複数の URL カテゴリに属する場合は、重大度が最も高いカテゴリに指定されたアクションが適用されます。
- 一致するルールが見つからない場合、デバイスはパケットに対して URL フィルタリングプロファイルのデフォルトアクションを実行します。デフォルトアクションが設定されていない場合、デバイスはパケットの通過を許可します。

URL filtering action

URL カテゴリには URL フィルタリングアクションを指定し、URL フィルタリングプロファイルにはデフォルトアクションを指定できます。
デバイスは、次の URL フィルタリングアクションをサポートしています。

- **Blacklist**: 一致するパケットをドロップし、パケットの送信元を IP ブラックリストに追加します。IP ブラックリスト機能がイネーブルになっている場合、ブラックリストに掲載された送信元からのパケットはブラックリスト期間中ブロックされます。IP ブラックリスト機能がイネーブルになっていない場合、ブラックリストに掲載された送信元からのパケットはブロックされません。
  IP ブラックリスト機能の詳細については、攻撃防御のオンラインヘルプを参照してください。
  blacklist アクションのブラックリスト期間を設定するには、**Objects** > **APPSecurity** > **Security Actions** > **Block** に移動します。
- **Drop**: 一致するパケットをドロップします。
- **Permit**: 一致するパケットの通過を許可します。

- **Redirect**:一致するパケットを Web ページにリダイレクトします。
- **Reset**: TCP リセットメッセージを送信して、一致するパケットの TCP 接続を閉じます。
- **Logging**: 一致するパケットをロギングします。このアクションは、URL フィルタリングプロファイルでロギング機能が有効になった後にのみ有効になります。

HTTPS URL filtering

デフォルトでは、デバイスは HTTP URL フィルタリングだけをサポートします。HTTPS トラフィックのフィルタリングをイネーブルにするには、次のいずれかの方法を使用します。

- SSL 復号化を使用して HTTPS トラフィックを復号化し、復号化されたトラフィックで HTTP URL フィルタリングを実行します。SSL 復号化の詳細は、アプリケーションプロキシのオンラインヘルプを参照してください。
- HTTPS URL フィルタリングをイネーブルにします。この機能は、復号化されていない HTTPS トラフィックに対して URL フィルタリングを実行します。デバイスはクライアントからの Client Hello メッセージを直接検出し、URL フィルタリング用の Sever Name Indication(SNI)拡張からサーバー名を抽出します。

SSL 復号化には大量の暗号化および復号化操作が含まれるため、デバイスの転送パフォーマンスが低下する可能性があります。ベストプラクティスとして、デバイスが HTTPS トラフィックに対してのみ URL フィルタリングを実行する必要がある場合は、HTTPS URL フィルタリングをイネーブルにして、HTTPS トラフィックに対して URL フィルタリングをイネーブルにします。

URL filtering mechanism

URL フィルタリングは、URL フィルタリングプロファイルをセキュリティーポリシー、URL フィルタリングが有効になります。

図 2 に示すように、デバイスは HTTP パケットを受信すると、以下の動作を行います。

1. デバイスは、パケットをセキュリティーポリシーと比較します。
   パケットが URL フィルタリングプロファイルに関連付けられたセキュリティーポリシーと一致する場合、デバイスはパケットから URL を抽出します。
2. デバイスは、抽出された URL を、URL フィルタリングプロファイル内のホワイトリストおよびブラックリストルールと比較します。
   - URL がホワイトリストルールと一致する場合、パケットの通過が許可されます。
   - URL がブラックリストルールと一致する場合、パケットはドロップされます。
   - URL がプロファイル内のホワイトリストルールまたはブラックリストルールと一致しない場合、デバイスはステップ 3 を実行します。
3. デバイスは、抽出された URL を、URL フィルタリングプロファイル内の URL フィルタリング規則と比較します。

○ URL がユーザー定義の URL カテゴリに属する URL フィルタリング規則と一致する場合、デバイスは URL カテゴリに指定されたアクションを実行します。

URL フィルタリング規則が複数のユーザー定義 URL カテゴリに属する場合、最も高い重大度を持つ URL カテゴリに指定されたアクションが適用されます。

○ URL レピュテーションがイネーブルの場合、デバイスは、一致する URL フィルタリング規則が URL レピュテーションシグニチャライブラリ内の攻撃カテゴリに属するかどうかを判断します。イネーブルの場合、デバイスはパケットの攻撃カテゴリに指定されたアクションを実行します。

○ URL が、定義済みの URL カテゴリに属する URL フィルタリング規則と一致する場合、デバイスは URL カテゴリに指定されたアクションを実行します。

URL フィルタリング規則が複数の定義済み URL カテゴリに属する場合、最も高い重大度を持つ URL カテゴリに指定されたアクションが適用されます。

4. URL がプロファイル内のどのルールとも一致せず、プロファイル内でクラウドクエリーがディセーブルになっている場合、プロファイルに指定されたデフォルトアクションが適用されます。デフォルトアクションが設定されていない場合、デバイスはパケットの通過を許可します。

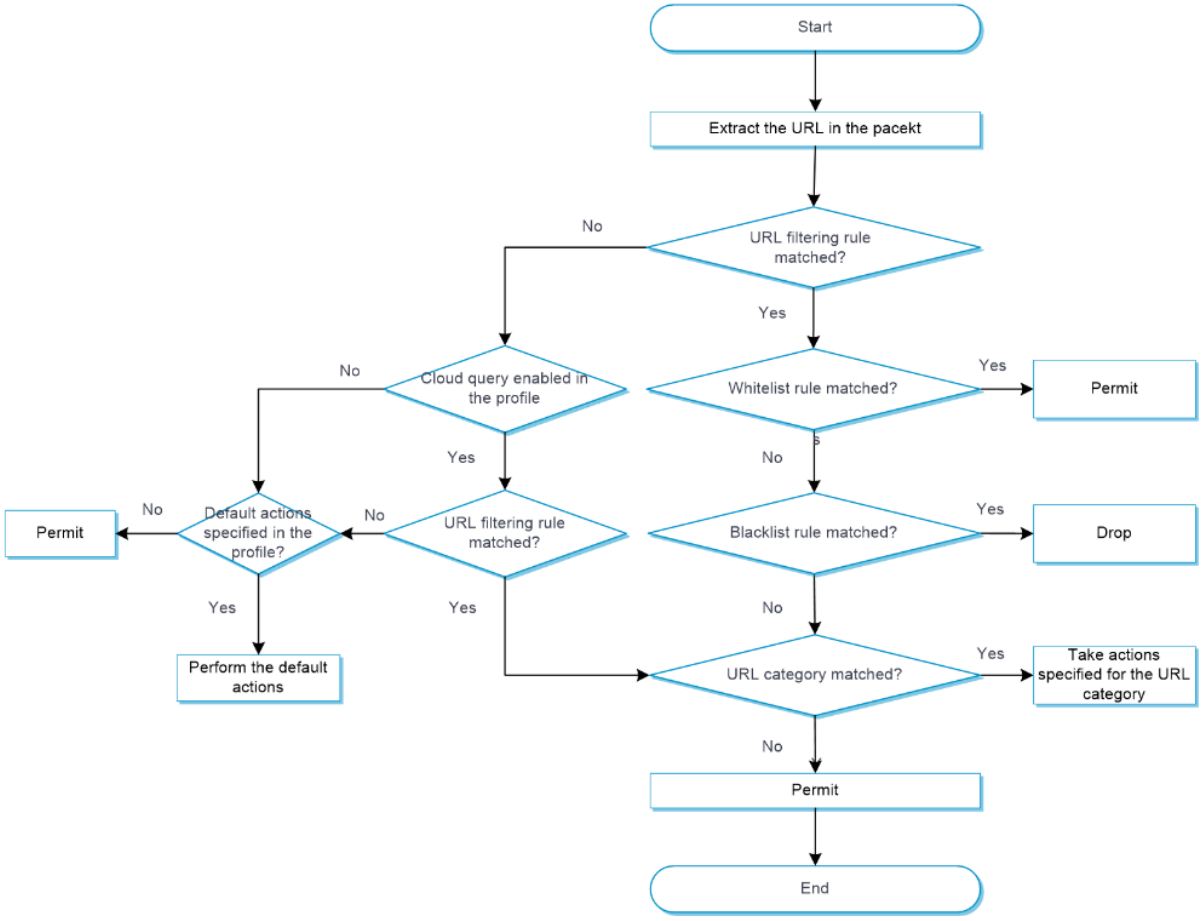
URL がプロファイル内のどのルールとも一致せず、プロファイル内でクラウドクエリーが有効になっている場合、デバイスはステップ 4 を実行します。

5. デバイスは URL をクラウドサーバーに転送して、さらにクエリーを実行します。

○ URL に一致するルールが見つかった場合、デバイスは、ステップ 3 で説明したようにパケットに対して実行するアクションを決定します。

○ 一致するルールが見つからない場合、デバイスはパケットに対してプロファイルのデフォルトアクションを実行します。デフォルトアクションが設定されていない場合、デバイスはパケットの通過を許可します。

図 2 URL フィルタリングメカニズム



Restrictions and guidelines

Restrictions and guidelines: Text-based URL filtering rule configuration

ホスト名または URI マッチングのテキストパターンでアスタリスク文字(*)を使用する場合は、次の注意事項に従ってください。

- ホスト名を照合する場合、アスタリスク(*)は、テキストパターンの先頭または末尾カード文字として、テキストパターンの先頭または末尾にだけ使用できます。0
- URI マッチングでは、アスタリスク(*)をワイルドカード文字としてテキストパターンの先頭または末尾に表示して 0 以上の文字と一致させるか、または中間に非ワイルドカード文字として表示できます。

Restrictions and guidelines: Regular expression-based URL filtering rule configuration

- 正規表現パターンには、最大 4 つの分岐を含めることができます。たとえば、**'abc(c d e¥x3D)'**は有効で、**'abc(c onreset onselect onchange style¥x3D)'**は無効です。
- 中かっこは使用できません。たとえば、**'ab((abcs*?))'**は無効です。
- 分岐を別の分岐の後に指定することはできません。たとえば、**'ab(a b)(c d)^¥¥r¥¥n]+?'**は無効です。
- アスタリスク(*)または疑問符(?) の前には、4 文字以上のワイルドカード以外の文字が必要です。たとえば、**'abc*'**は無効で、**'abcd*DoS¥x2d¥d{5}¥x20¥x2bxi¥¥r¥¥nJOIN'**は有効です。

Restrictions and guidelines: whitelist

- パケットがホワイトリストルールに一致する場合、URL フィルタリングログリストの **URL Category** カラムには **Whitelist** トが表示されます。
- HTTP 要求の referer ヘッダーが URL フィルタリングのホワイトリストと一致する場合、URL フィルタリングログリストの **URL Category** カラムには **Referer Whitelist** と表示されます。
- ホワイトリストモードがイネーブルの場合、パケットがいずれかのホワイトリスト規則に一致しないと、URL フィルタリングログリストの **URL Category** カラムに **Blacklist** と表示されます。

Restrictions and guidelines: URL filtering profile activation

URL フィルタプロファイルを作成、編集または削除した後、有効にするには構成をアクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化するか、デフォルトで 40 秒後に構成が自動的にアクティブ化されます。構成をアクティブ化すると、一時的な DPI サービスの中断が発生します。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。

Restrictions and guidelines: Licensing requirements

URL フィルタリングにはライセンスが必要です。ライセンスの期限が切れた場合、既存の URL フィルタリングシグニチャライブラリは引き続き使用できますが、デバイス上のライブラリをアップグレードしたり、クラウドクエリーを使用したりすることはできません。ライセンスの詳細については、ライセンスのオンラインヘルプを参照してください。

Restrictions and guidelines: HTTPS URL filtering

HTTPS URL フィルタリングでは、URL フィルタリング規則のホスト名一致基準のみが有効になります。URI 一致基準は有効になりません。
この機能は、URL のホスト名フィールドがサーバーのドメイン名である場合にのみ有効です。ホスト名フィールドが IP アドレスの場合、この機能は HTTPS トラフィックに適用されません。

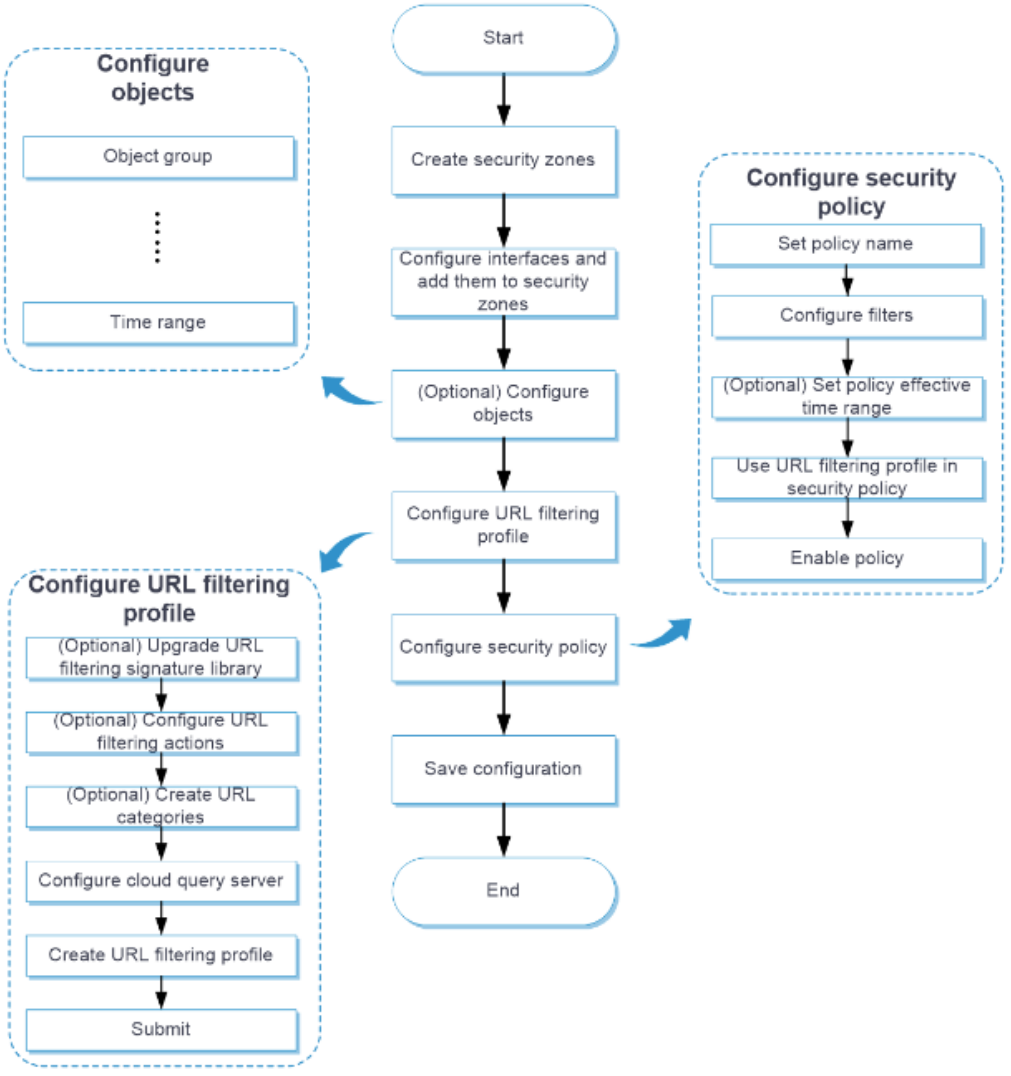
この機能は、次の状況では有効になりません。

- クライアントブラウザは、SNI 拡張が暗号化されるため、TLS 1.3 ダウングレード拡張メカニズムを有効にします。
- HTTPS パケットには SNI 拡張がありません。

Configure URL filtering

図 3 に示すように、URL フィルタリングを設定します。

図 3 URL フィルタリングの設定手順



Configure a URL category

ユーザー定義の URL カテゴリを作成し、特定の URL フィルタリング要件を満たすフィルタリング規則を設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **URL Filtering** > **URL Categories** を選択します。
3. **Create** をクリックします。
4. URL カテゴリを作成します。

表 2 URL カテゴリの設定項目

項目	説明
Name	URL カテゴリの名前を入力してください。カテゴリ名を **Pre-**で始めることはできません。
Description	URL カテゴリの説明を入力します。
Severity level	URL カテゴリに 1000～65535 の一意の重大度レベルを割り当てます。値が大きいほど、重大度レベルが高くなります。
Include predefined category	定義済みの URL カテゴリを選択して、そのすべての規則を URL カテゴリに追加します。

5. URL カテゴリに URL フィルタリング規則を追加します。

a. **Add** をクリックします。

b. **Match pattern** リストから、**host name** フィールドの一致パターンタイプを選択します。オプションは **Text** と **Regular expression** です。

c. ホスト名フィールド]フィールドに一致パターンを入力します。

d. **Match pattern** リストから、**URI** フィールドの一致パターンタイプを選択します。オプションは、**Text**、 **Regular expression**、および**–NONE—**です。

e. **URI** フィールドに一致パターンを入力します。**URI** フィールドの一致パターンに **–NONE—**オプションが選択されている場合は、この手順は不要です。

f. **OK** をクリックします。

g. 上記の手順を繰り返して、さらに URL フィルタリング規則を追加します。

6. **OK** をクリックします。

URL Categories ページに URL カテゴリが表示されます。

Configure the cloud query server

URL フィルタリング用のクラウドクエリーサーバーを設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **URL Filtering** > **URL Categories** を選択します。
3. **Cloud server connection status** フィールドの横にある **Configure** をクリックします。
4. クラウドクエリーサーバーを設定します。

表 3 クラウドクエリーサーバーの設定項目

項目	説明
Server address	クラウドクエリーサーバーの IP アドレスまたはホスト名を入力します。当社のクラウドクエリーサーバーのみがサポートされています。
Max cached URL entries	キャッシュできる URL エントリの最大数を指定します。 デバイスは、クラウドクエリーのためにクラウドクエリーサーバーに送信された一意の URL ごとに URL キャッシュエントリを作成します。クラウドクエリーの結果はキャッシュエントリに保存されます。
Min cache period	URL キャッシュエントリの最小キャッシュ期間を分単位で指定します。 URL キャッシュエントリの最小キャッシュ期間を設定すると、指定した期間中にエントリが削除されないようになります。 URL フィルタリングキャッシュがいっぱいになると、最も古い URL キャッシュエントリのキャッシュ期間が特定され、上書きするかどうかが決定されます。 • エントリのキャッシュ期間が最小キャッシュ期間以下の場合、システムはエントリを削除しません。新しいエントリはキャッシュされません。 • エントリのキャッシュ期間が最小キャッシュ期間より長い場合、システムはエントリを新しいエントリで上書きします。 ただし、設定された最大キャッシュ URL エントリが現在キャッシュされているエントリよりも少ない場合は、キャッシュ期間が最小キャッシュ期間以下であっても、最も古いキャッシュエントリが削除されます。

Configure a URL filtering profile

URL フィルタリングプロファイルでは、次の設定を行うことができます。

- クラウドクエリーを有効にします。
- どの URL フィルタリング規則にも一致しないパケットのデフォルトアクションを指定します。
- ホワイトリストおよびブラックリストルールを設定します。ホワイトリストルールは、ブラックリストルールよりも優先されます。

- URL カテゴリのアクションを指定します。

URL フィルタリングプロファイルには、デバイス上のすべての URL カテゴリが含まれています。URL フィルタリングプロファイルでは、個々の URL カテゴリに対してアクションを指定できます。HTTP パケットが URL カテゴリの URL フィルタリング規則と一致する場合、そのカテゴリに指定されたアクションがパケットに適用されます。一致規則が複数の URL カテゴリにある場合は、最も重大度の高いカテゴリに指定されたアクションが実行されます。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **URL Filtering** > **Profiles** を選択します。
3. **Create** をクリックします。
4. URL フィルタリングプロファイルを作成します。

表 4 URL フィルタリングプロファイルの構成項目

項目	説明
Name	URL フィルタリングプロファイルの名前を入力します。
Default action	URL フィルタリング規則に一致しないパケットに対して実行するデフォルトアクションを選択します。オプションは、**Permit**、**Drop**、**Reset**、**Redirect**、**Blacklist** です。
Cloud query	クラウドクエリーを有効にするには、ボックスを選択します。
Logging	URL フィルタリング規則に一致するパケットのロギングをイネーブルにするには、このボックスを選択します。 この項目を選択する前に、最初にデフォルトアクションを設定してください。
Enable HTTPS URL filtering	復号化されていない HTTPS トラフィックで URL フィルタリングを有効にするには、このボックスを選択します。 有効なプロキシポリシーで SSL 復号化アクションが選択されている場合、この機能は有効になりません。SSL 復号化の詳細は、アプリケーションプロキシのオンラインヘルプを参照してください。
Enable referer whitelist	このチェックボックスをオンにすると、HTTP 要求の referer ヘッダーが URL フィルタリングホワイトリストと一致した場合に、HTTP 要求を通過させることができます。
Whitelist mode	チェックボックスをオンにすると、URL フィルタリングのホワイトリストにある Web サイトにのみアクセスできます。

Whitelist	必要に応じて、URL フィルタリングプロファイルにホワイトリストルールを追加します。 URL フィルタリングプロファイルにホワイトリストルールを追加するには、次の手順を実行します。 1. **Whitelist** 領域で、**Add** をクリックします。 2. **Add Whitelist Rule** ウィンドウが開きます。 3. **Match pattern** リストから、**host name** フィールドの一致パターンタイプを選択します。オプションは **Text** と **Regular expression** です。 4. **Host name** フィールドに一致パターンを入力します。 5. **Match pattern** リストから、**URI** フィールドの一致パターンタイプを選択します。オプションは、**Text**,、**Regular expression**、および**–NONE—**です。 6. **URI** フィールドに一致パターンを入力します。**URI** フィールドの一致パターンに**–NONE—**オプションが選択されている場合は、この手順は不要です。
Blacklist	必要に応じて、URL フィルタリングプロファイルにブラックリストルールを追加します。
URL categories	**URL categories** 領域で、個々の URL カテゴリのアクションを選択します。サポートされているアクションは、**Permit**、**Drop**、**Reset**、**Redirect**、**Blacklist** および **Logging** です。 URL カテゴリのロギングアクションを選択する前に、まず、**Permit**、**Drop**、**Reset**、**Redirect**、および **Blacklist** アクションからアクションを選択します。
Enable URL reputation	悪意のある URL へのアクセスをブロックする URL レピュテーションを有効にするには、このボックスを選択します。この機能を有効にすると、デバイスはパケットから抽出された URL と URL レピュテーションシグニチャライブラリ内の URL を比較します。一致が検出された場合、その URL は悪意のある URL と見なされ、一致する URL が属する攻撃カテゴリに指定されたアクションが実行されます。一致が検出されない場合、デバイスはパケットの通過を許可します。
Action configuration	URL レピュテーションシグニチャライブラリ内の個々の攻撃カテゴリに対するアクションを設定します。

5. **OK** をクリックします。
   URL Filtering Profiles ページに URL フィルタリングプロファイルが表示されます。
6. セキュリティーポリシーで URL フィルタリングプロファイルを使用します。
   セキュリティーポリシーの詳細については、セキュリティーポリシーのオンラインヘルプを参照してください。

7. 構成をただちに有効にするには、**Submit** をクリックします。または、構成が自動的に有効になるまで 40 秒間待機します。

Trusted application proxies

このヘルプには、次のトピックがあります。

- Introduction
- Configure a trusted application proxy

Introduction

信頼できるアプリケーションプロキシは、アプリケーションにアクセスするためのユーザートラフィックのプロキシです。デバイスは、認証および認可のために、受信したユーザーリクエストを信頼できるアクセスコントローラに転送できます。信頼できるアクセスコントローラは、ユーザーアクセス権限を制御するために、関連する結果をデバイスに戻します。

Configure a trusted application proxy

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Zero Trust** > **Trusted App Proxies** を選択します。
3. **Create** をクリックします。
4. 信頼されたアプリケーションプロキシパラメーターを設定します。

表 1 トラステッドアプリケーションプロキシーの基本的な構成項目

項目	説明
Name	信頼されたアプリケーションプロキシの名前を入力します。大文字と小文字は区別されません。
IPv4 address	信頼できるアプリケーションプロキシサービスを提供するために使用される IPv4 アドレスを入力します。
Port number	信頼できるアプリケーションプロキシのポート番号を入力します。 トラステッドアプリケーションプロキシーが SSL ポリシーを使用する場合は、デフォルト以外のポート番号(典型的な例は 443)を指定する必要があります。
Proxy function	信頼できるアプリケーションプロキシを有効または無効にします。
Trusted access controller	信頼できるアプリケーションプロキシの信頼できるアクセスコントローラを指定します。デバイスは、信頼できるアプリケーションプロキシに一致するトラフィックを、認証および認可のために指定された信頼できるアクセスコントローラに

	送信します。認証および認可を通過したユーザーのみが、後続の手順を続行できます。 既存の信頼できるアクセスコントローラを選択することも、新しい信頼できるアクセスコントローラを作成することもできます。
SSL client policy	デバイス(SSL クライアント)と SSL サーバー間で交換されるトラフィックを暗号化するために、信頼できるアプリケーションプロキシによって使用される SSL クライアントポリシーを指定します。 既存の SSL クライアントポリシーを選択することも、新しい SSL クライアントポリシーを作成することもできます。
SSL server policy	デバイス(SSL サーバー)と SSL クライアント間で交換されるトラフィックを暗号化するために、信頼できるアプリケーションプロキシによって使用される SSL サーバーポリシーを指定します。 既存の SSL サーバーポリシーを選択することも、新しい SSL サーバーポリシーを作成することもできます。
Max connections	信頼されたアプリケーションプロキシが許可する最大接続数を設定します。0 は無制限を意味します。
Max connections per second	信頼されたアプリケーションプロキシが 1 秒間に許可する最大接続数を設定します。0 は無制限を意味します。

表 2 高度なトラステッドアプリケーションプロキシーの構成項目

項目	説明
LB policy	信頼できるアプリケーションプロキシの LB ポリシーを指定します。デバイスは、LB ポリシー規則に基づいて、信頼できるアプリケーションプロキシと一致するパケットについて、その内容に従ってロードバランシングを実行します。 既存の LB ポリシーを選択することも、新しい LB ポリシーを作成することもできます。 HTTP タイプの信頼できるアプリケーションプロキシは、汎用または HTTP タイプの LB ポリシーだけを使用できます。
Connection limit policy	信頼できるアプリケーションプロキシの接続制限ポリシーを指定します。信頼できるアプリケーションプロキシへの接続数は、指定したポリシーによって制限されます。 既存の接続制限ポリシーを選択することも、新しい接続制限ポリシーを作成することもできます。
TCP parameter profile (client)	信頼できるアプリケーションプロキシの TCP パラメータープロファイルを指定します。デバイスはパラメータープロファイルの設定を使用して、一致するトラフィックを処理します。クライアント側の TCP パラメータープロファイルは、デバイスとクライアント間の TCP 接続にのみ適用されます。

	既存の TCP パラメータープロファイルを選択することも、新しい TCP パラメータープロファイルを作成することもできます。
TCP parameter profile (server)	信頼できるアプリケーションプロキシの TCP パラメータープロファイルを指定します。デバイスはパラメータープロファイル設定を使用して、一致するトラフィックを処理します。サーバー側の TCP パラメータープロファイルは、デバイスとサーバー間の TCP 接続にのみ適用されます。 既存の TCP パラメータープロファイルを選択することも、新しい TCP パラメータープロファイルを作成することもできます。
HTTP parameter profile	信頼できるアプリケーションプロキシの HTTP パラメータープロファイルを指定します。デバイスはパラメータープロファイル設定を使用して、一致するトラフィックを処理します。 既存の HTTP パラメータープロファイルを選択することも、新しい HTTP パラメータープロファイルを作成することもできます。
HTTP protection policy	信頼できるアプリケーションプロキシの HTTP 保護ポリシーを指定します。デバイスは保護ポリシー設定を使用して、信頼できるアプリケーションプロキシと一致するトラフィックを保護します。 既存の HTTP 保護ポリシーを選択することも、新しい HTTP 保護ポリシーを作成することもできます。
Content security function	コンテンツセキュリティー機能を有効または無効にします。
Content security-WAF profile	コンテンツセキュリティーの WAF プロファイルを指定します。デバイスは、信頼できるアプリケーションプロキシと一致するトラフィックに対して Web アプリケーション保護を実行します。 WAF プロファイルの詳細については、WAF のヘルプを参照してください。
Content security-IPS profile	コンテンツセキュリティーの IPS プロファイルを指定します。デバイスは、信頼できるアプリケーションプロキシと一致するトラフィックに対して侵入防御を実行します。 IPS プロファイルの詳細については、IPS ヘルプを参照してください。
Content security-Anti-virus profile	コンテンツセキュリティーのウィルス対策プロファイルを指定します。デバイスは、信頼できるアプリケーションプロキシと一致するトラフィックに対してウィルス対策を実行します。 アンチウィルスプロファイルの詳細については、アンチウィルスのヘルプを参照してください。

5. **OK** をクリックします。

信頼できるアプリケーションプロキシは、信頼できるアプリケーションプロキシのページに表示されます。

Trusted API proxies

このヘルプには、次のトピックがあります。

- Introduction
- Configure a trusted API proxy

Introduction

信頼できる API プロキシは、API にアクセスするためのユーザートラフィックのプロキシです。デバイスは、受信したユーザーために、受信したユーザーリクエストを信頼できるアクセスコントローラに転送できます。信頼できるアクセスコントローラは、ユーザーアクセス権限を制御するために、関連する結果をデバイスに戻します。

Configure a trusted API proxy

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Zero Trust** > **Trusted API Proxies** を選択します。
3. **Create** をクリックします。
4. トラステッド API プロキシパラメーターを構成します。

表 1 トラステッド API プロキシの基本構成項目

項目	説明
Name	信頼できる API プロキシの名前を入力します。大文字と小文字は区別されません。
IPv4 address	信頼できる API プロキシサービスを提供するために使用する IPv4 アドレスを入力します。
Port number	トラステッド API プロキシのポート番号を入力します。 トラステッド API プロキシが SSL ポリシーを使用する場合は、デフォルト以外のポート番号(一般的な例は 443)を指定する必要があります。
Proxy function	信頼できる API プロキシを有効または無効にします。
Trusted access controller	信頼できる API プロキシの信頼できるアクセスコントローラを指定します。デバイスは、信頼できる API プロキシに一致するトラフィックを、認証および認可

	のために指定された信頼できるアクセスコントローラに送信します。認証および認可を通過したユーザーのみが、後続の手順に進むことができます。 既存の信頼できるアクセスコントローラを選択することも、新しい信頼できるアクセスコントローラを作成することもできます。
SSL client policy	デバイス(SSL クライアント)と SSL サーバー間で交換されるトラフィックを暗号化するために、信頼できる API プロキシが使用する SSL クライアントポリシーを指定します。 既存の SSL クライアントポリシーを選択することも、新しい SSL クライアントポリシーを作成することもできます。
SSL server policy	デバイス(SSL サーバー)と SSL クライアント間で交換されるトラフィックを暗号化するために、信頼できる API プロキシによって使用される SSL サーバーポリシーを指定します。 既存の SSL サーバーポリシーを選択することも、新しい SSL サーバーポリシーを作成することもできます。
Max connections	信頼できる API プロキシによって許可される最大接続数を設定します。0 は制限なしを意味します。
Max connections per second	信頼できる API プロキシが 1 秒間に許可する最大接続数を設定します。0 は制限なしを意味します。

表 2 高度なトラステッド API プロキシの構成項目

項目	説明
LB policy	信頼できる API プロキシの LB ポリシーを指定します。デバイスは、LB ポリシー規則に基づいて、信頼できる API プロキシと一致するパケットのロードバランシングを、その内容に従って実行します。 既存の LB ポリシーを選択することも、新しい LB ポリシーを作成することもできます。 HTTP タイプの信頼できる API プロキシは、汎用または HTTP タイプの LB ポリシーだけを使用できます。
Connection limit policy	信頼できる API プロキシの接続制限ポリシーを指定します。信頼できる API プロキシへの接続数は、指定したポリシーによって制限されます。 既存の接続制限ポリシーを選択することも、新しい接続制限ポリシーを作成することもできます。
TCP parameter profile (client)	信頼できる API プロキシの TCP パラメータープロファイルを指定します。デバイスはパラメータープロファイル設定を使用して、一致するトラフィックを処理します。クライアント側の TCP パラメータープロファイルは、デバイスとクライアント間の TCP 接続にのみ適用されます。

	既存の TCP パラメータープロファイルを選択することも、新しい TCP パラメータープロファイルを作成することもできます。
TCP parameter profile (server)	信頼できる API プロキシの TCP パラメータープロファイルを指定します。デバイスはパラメータープロファイル設定を使用して、一致するトラフィックを処理します。サーバー側の TCP パラメータープロファイルは、デバイスとサーバー間の TCP 接続にのみ適用されます。 既存の TCP パラメータープロファイルを選択することも、新しい TCP パラメータープロファイルを作成することもできます。
HTTP protection policy	信頼できる API プロキシの HTTP 保護ポリシーを指定します。デバイスは保護ポリシー設定を使用して、信頼できる API プロキシと一致するトラフィックを保護します。 既存の HTTP 保護ポリシーを選択することも、新しい HTTP 保護ポリシーを作成することもできます。
Content security function	コンテンツセキュリティー機能を有効または無効にします。
Content security-WAF profile	コンテンツセキュリティーの WAF プロファイルを指定します。デバイスは、信頼できる API プロキシに一致するトラフィックに対して Web アプリケーションの保護を実行します。 WAF プロファイルの詳細については、WAF のヘルプを参照してください。
Content security-IPS profile	コンテンツセキュリティーの IPS プロファイルを指定します。デバイスは、信頼できる API プロキシと一致するトラフィックに対して侵入防御を実行します。 IPS プロファイルの詳細については、IPS ヘルプを参照してください。
Content security-Anti-virus profile	コンテンツセキュリティーのアンチウィルスプロファイルを指定します。デバイスは、信頼できる API プロキシと一致するトラフィックに対してアンチウィルス防止を実行します。 アンチウィルスプロファイルの詳細については、アンチウィルスのヘルプを参照してください。

5. **OK** をクリックします。

トラステッド API プロキシは、トラステッド API プロキシページに表示されます。

Policy-based NAT

このヘルプには、次のトピックがあります。

- Introduction
- Restrictions and guidelines
- Configure policy-based NAT
  - Configuration flowchart
  - Configure a policy-based NAT44 rule
  - Configure a policy-based NAT64 rule
  - Configure a policy-based NAT66 rule

Introduction

ポリシーベース NAT には、一致するパケットを識別して変換するための一連の NAT 規則が含まれています。パケットの一致基準には、送信元セキュリティーゾーン、宛先セキュリティーゾーン、送信元 IP アドレス、宛先 IP アドレス、およびサービスが含まれます。

ポリシーベース NAT は、さまざまなシナリオに適用可能な次のタイプの規則をサポートしています。

- **NAT44 rule**: IPv4 ネットワーク間の NAT 変換に使用されます。
- **NAT64 rule**: IPv4 ネットワークと IPv6 ネットワーク間の NAT 変換に使用されます。
- **NAT66 rule**: IPv6 ネットワーク間の NAT 変換に使用されます。

ポリシーベース NAT は、次の変換モードをサポートしています。

- **Source address translation**: パケットの送信元 IP アドレスと送信元ポートを変換します。NO-PAT および PAT モードがサポートされています。NO-PAT および PAT の詳細については、「NAT」を参照してください。
- **Destination address translation**: パケットの宛先 IP アドレスと宛先ポートを変換します。ポリシーベース NAT は、一致するパケットの異なる宛先 IP アドレスと宛先ポートを同じ IP アドレスとポートに変換することをサポートします。
- **Bidirectional translation**: パケットの送信元 IP アドレス、送信元ポート、宛先 IP アドレス、および宛先ポートを変換します。送信元アドレス変換では、NO-PAT モードと PAT モードがサポートされます。宛先アドレス変換では、一致するパケットの異なる宛先 IP アドレスと宛先ポートを同じ IP アドレスとポートに変換できます。

Restrictions and guidelines

- ポリシーNAT はインターフェース NAT よりも優先順位が高く、パケットがポリシーNAT と一致すると、インターフェース NAT との一致が試行されます。
- デフォルトでは、ポリシーベース NAT の NAT 規則は、設定順の降順にソートされます。NAT 規則を再配置して、その優先順位を変更できます。規則の優先順位は、その後に表示される規則よりも高くなります。
- NAT アドレスグループは、PAT モードと NO-PAT モードの両方で使用できません。
- パケットがポリシーベースの NAT 規則とインターフェース NAT 規則の両方に一致する場合、パケットは次のように変換されます。
  - 送信元および宛先アドレス変換方式の場合:
    - ポリシーベース NAT 規則とインターフェース NAT 規則の変換方式が同じ場合、デバイスはポリシーベース NAT 規則を使用してパケットを変換します。
    - ポリシーベース NAT 規則とインターフェース NAT 規則の変換方式が異なる場合、デバイスは 2 つの規則を使用してパケットを変換します。
  - ポリシーベース NAT 規則の変換方式が双方向である場合、デバイスはポリシーベース NAT 規則を使用してパケットを変換し、インターフェース NAT 規則は有効になりません。
- NAT アドレスグループにアドレス範囲を追加する場合は、アドレス範囲が重複しないようにしてください。
- NAT 規則で使用されるアドレスオブジェクトグループには、ホスト名またはアドレスオブジェクトグループを含めることはできません。
- ポリシーベースの NAT 規則を作成またはコピーする場合:
  - **Automatically generate security policy** チェックボックスをオンにすると、デバイスは元のパケット設定に基づいてセキュリティーポリシーを自動的に生成します。
  - チェックボックスをオンにした後で元のパケット設定を変更する場合は、**Refresh** をクリックして、新しい設定に基づいてセキュリティーポリシーを生成します。

Configure policy-based NAT

NAT は、インバウンドまたはアウトバウンド方向で実行できます。

- **Inbound NAT**: 図 1 に示すように、セキュリティーゾーンで受信されたパケットのアドレス変換を実行します。
- **Outbound NAT**: 図 2 に示すように、セキュリティーゾーンから送信されたパケットのアドレス変換を実行します。

図 1 インバウンドセキュリティーゾーン上の NAT

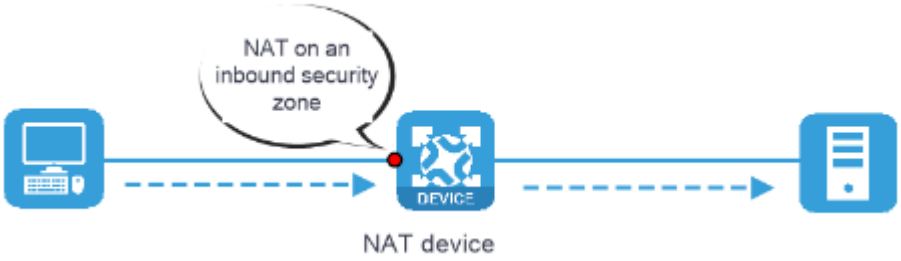
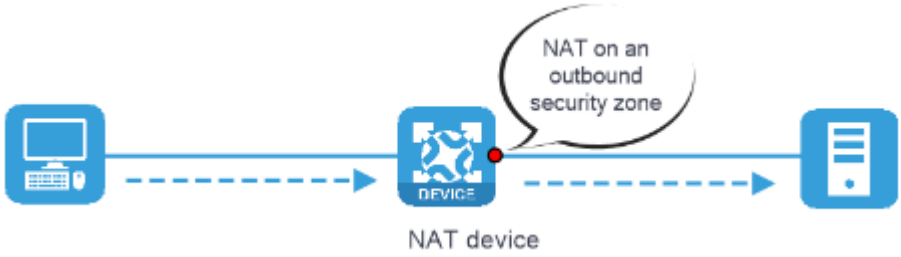


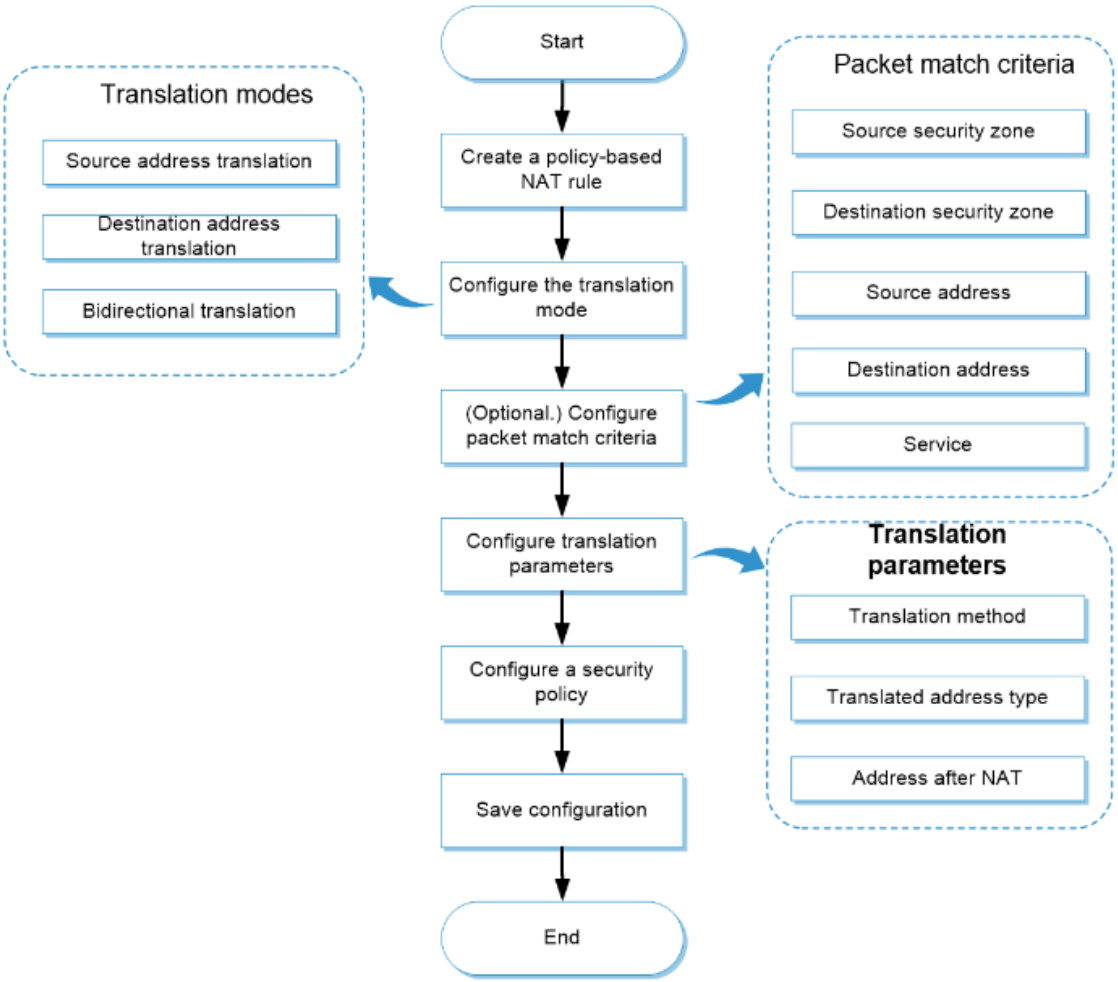
図 2:発信セキュリティーゾーンでの NAT



Configuration flowchart

ポリシーベース NAT は、セキュリティーゾーン、アドレスオブジェクトグループ、およびサービスオブジェクトグループを含むパケット一致基準をサポートします。ポリシーベース NAT は、送信元アドレス変換、宛先アドレス変換、および双方向変換をサポートします。図 3 に、設定のフローチャートを示します。

図 3 ポリシーベース NAT の設定フローチャート



Configure a policy-based NAT44 rule

手順

1. (オプション)セキュリティーゾーンを作成します。(詳細は表示されません。)
2. (任意)アドレスオブジェクトグループを作成します。(詳細は表示されません)。
3. (任意)サービスオブジェクトグループを作成します。(詳細は表示されません)。
4. (任意)NAT アドレスグループを作成します。
   a. **Objects** タブをクリックします。
   b. ナビゲーションペインで、**Object Groups** > **NAT Address Groups** を選択します。
   c. **Create** をクリックします。
   d. NAT アドレスグループを作成します。
   e. **OK** をクリックします。
5. ポリシーベースの NAT44 規則を作成します。
   a. **Policies** タブをクリックします。
   b. ナビゲーションペインで、**Policy-Based NAT** を選択します。

c. **Create** をクリックします。

d. ポリシーベースの NAT 規則を作成し、規則タイプとして NAT44 を選択します。

e. **OK** をクリックします。

表 1 ポリシーベースの NAT44 規則の設定項目

項目			説明
Rule name			ポリシーベースの NAT44 規則の名前を入力します。漢字がサポートされています。
Rule description			ポリシーベースの NAT44 規則の説明を入力します。
Original packets		Src zone	パケットの照合に使用する送信元セキュリティーゾーンを選択します。
		Dst zone	パケットを照合する宛先セキュリティーゾーンを選択します。
		Source IP	パケットを照合する送信元 IP アドレス、IP サブネット、またはアドレスオブジェクトグループを選択します。
		Destination IP	パケットを照合する宛先 IP アドレス、IP サブネット、またはアドレスオブジェクトグループを選択します。
		Service	パケットを一致させるサービスオブジェクトグループを選択します。
Source address translation	Translation method		送信元アドレス変換方式を選択します。 • **Dynamic IP+port**: PAT 方式を使用して、パケットの送信元 IP アドレスと送信元ポートの両方を変換します。 • **Dynamic IP**: NO-PAT 方式を使用して、パケットの送信元 IP アドレスだけを変換します。 • **Static IP**: パケットの送信元 IP アドレスを固定 IP アドレスに変換します。 • **No translation**: この規則およびこの規則よりも優先順位の低い規則は、送信元アドレスの変換には使用されません。
	Address		送信元アドレス変換の NAT アドレスタイプを選択します。 • **Address object group**: 送信元アドレス変換にアドレスオブジェクトグループ内の IP アドレスを使用します。 • **NAT address group**: 送信元アドレス変換に NAT アドレスグループ内の IP アドレスを使用します。

項目		説明
		• **IP address**: 送信元アドレス変換に固定 IP アドレスを使用します。 • **Network address**: ネットワーク上の IP アドレスを使用して送信元アドレスを変換します。 • **Easy IP**]: 送信元アドレス変換にデバイスの発信インターフェース IP アドレスを使用します。
	Source IP after NAT	送信元アドレス変換の NAT アドレスを選択します。
	Allow reverse NAT	逆アドレス変換をイネーブルにします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。 このオプションは、変換モードが **Dynamic IP** に設定されている場合にだけ使用できます。
	User original port preferentially	PAT には元のポートを優先的に使用します。元のポートが割り当てられている場合は、別のポートが使用されます。 このオプションは、変換モードが **Dynamic IP+port** に設定されている場合にだけ使用できます。
Destination address translation	Translation method	宛先アドレス変換方式を選択します。 • **Static IP**: パケットの宛先 IP アドレスを固定 IP アドレスに変換します。 • **Address object group**: パケットの宛先 IP アドレスをアドレスオブジェクトグループ内のアドレスに変換します。 • **No translation**: この規則およびこの規則よりも優先順位の低い規則は、送信元アドレスの変換には使用されません。
	Destination IP after NAT	変換後の宛先 IP アドレスを設定します。
	Port after NAT	変換後の宛先ポートを設定します。
VRF before NAT	パケットが属する VRF と照合するために使用する VRF を指定します。	
VRF after NAT	一致するパケットが属する VRF を置き換えるために使用する VRF を指定します。	
Enable this rule	このポリシーベースの NAT44 規則をイネーブルにします。	

項目		説明
Counting		ポリシーベースの NAT44 規則が一致する回数のカウントをイネーブルにします。

Configure a policy-based NAT64 rule

手順

1. (オプション)セキュリティーゾーンを作成します。(詳細は表示されません。)
2. (任意)アドレスオブジェクトグループを作成します。(詳細は表示されません)。
3. (任意)サービスオブジェクトグループを作成します。(詳細は表示されません)。
4. ポリシーベースの NAT64 規則を作成します。
   a. **Policies** タブをクリックします。
   b. ナビゲーションペインで、**Policy-Based NAT** を選択します。
   c. **Create** をクリックします。
   d. ポリシーベースの NAT 規則を作成し、規則タイプとして NAT64 を選択します。
   e. **OK** をクリックします。

表 2 ポリシーベースの NAT64 規則の設定項目

項目		説明
Rule name		ポリシーベースの NAT64 規則の名前を入力します。漢字がサポートされています。
Rule description		ポリシーベースの NAT64 規則の説明を入力します。
Original packets	Src zone	パケットの照合に使用する送信元セキュリティーゾーンを選択します。
	Source IP	パケットを照合する送信元 IP アドレス、IP サブネット、またはアドレスオブジェクトグループを選択します。
	Destination IP	パケットを照合する宛先 IP アドレス、IP サブネット、またはアドレスオブジェクトグループを選択します。
	サービス	パケットを一致させるサービスオブジェクトグループを選択します。
Source address translation	Translation method	送信元アドレス変換方式を選択します。

項目		説明
		• **Dynamic IP+port**: PAT 方式を使用して、パケットの送信元 IP アドレスと送信元ポートの両方を変換します。 • **Dynamic IP**: NO-PAT 方式を使用して、パケットの送信元 IP アドレスだけを変換します。 • **Static IP**: パケットの送信元 IP アドレスを固定 IP アドレスに変換します。 • **Prefix translation**: IPv6 プレフィクスを使用して、パケットの送信元 IP アドレスを変換します。
	Source IP after NAT	送信元アドレス変換の NAT アドレスを選択します。 このオプションは、変換方式が **Dynamic IP+port**, **Dynamic IP**、または **Static IP** の場合にだけ使用できます。
	Prefix translation	プレフィクス変換タイプを選択します。 • **General prefix**: 送信元アドレス変換に一般プレフィクスを使用します。 • **IVI prefix**: 送信元アドレス変換に IVI プレフィクスを使用します。 • **NAT64 prefix**: 送信元アドレス変換に NAT64 プレフィクスを使用します。 このオプションは、移動方法が **Prefix translation** である場合にのみ使用できます。
	IPv6 prefix	プレフィクス変換方式の IPv6 アドレスプレフィクスを設定します。 このオプションは、プレフィクス変換タイプが **General prefix** または **NAT64 prefix** の場合にだけ使用できます。
	Prefix length	IPv6 プレフィクス長を設定します。 このオプションは、プレフィクス変換タイプが **General prefix** または **NAT64 prefix** の場合にだけ使用できます。
Destination address translation	Translation method	宛先アドレス変換方式を選択します。 • **Prefix translation**: 宛先アドレス変換に IPv6 プレフィクスを使用します。 • **NAT server mapping**: パケットの宛先 IP アドレスと宛先ポート番号を、固定の宛先 IP アドレスと宛先ポート番号に変換します。

項目		説明
		• **Static translation**: パケットの宛先 IP アドレスを固定 IP アドレスに変換します。
	Prefix translation	プレフィクス変換タイプを選択します。 • **General prefix**: 送信元アドレス変換に一般プレフィクスを使用します。 • **IVI prefix**: 送信元アドレス変換に IVI プレフィクスを使用します。 • **NAT64 prefix**: 送信元アドレス変換に NAT64 プレフィクスを使用します。 このオプションは、移動方法が **Prefix translation** である場合にのみ使用できます。
	IPv6 prefix	プレフィクス変換方式の IPv6 アドレスプレフィクスを設定します。 このオプションは、接頭辞変換タイプが **General prefix** または **IVI prefix** の場合にのみ使用できます。
	Prefix length	IPv6 プレフィクス長を設定します。 このオプションは、接頭辞変換タイプが **General prefix** または **IVI prefix** の場合にのみ使用できます。
	Destination IP after NAT	変換後の宛先 IP アドレスを設定します。
	Port after NAT	変換後の宛先ポートを設定します。 このオプションは、変換方式が **NAT server mapping** の場合にだけ使用できます。
VRF before NAT	パケットが属する VRF と照合するために使用する VRF を指定します。VRF は入力ポートにバインドされます。	
VRF after NAT	一致するパケットが属する VRF を置き換えるために使用される VRF を指定します。VRF は出力ポートにバインドされます。	
Enable this rule	このポリシーベースの NAT64 規則をイネーブルにします。	
Counting	ポリシーベースの NAT64 規則が一致する回数のカウントをイネーブルにします。	

Configure a policy-based NAT66 rule

手順

1. (オプション)セキュリティーゾーンを作成します。(詳細は表示されません。)
2. (任意)アドレスオブジェクトグループを作成します。(詳細は表示されません)。
3. (任意)サービスオブジェクトグループを作成します。(詳細は表示されません)。
4. ポリシーベースの NAT66 規則を作成します。
   a. **Policies** タブをクリックします。
   b. ナビゲーションペインで、**Policy-Based NAT** を選択します。
   c. **Create** をクリックします。
   d. ポリシーベースの NAT 規則を作成し、規則タイプとして NAT66 を選択します。
   e. **OK** をクリックします。

表 3 ポリシーベースの NAT66 規則の設定項目

項目			説明
Rule name			ポリシーベースの NAT66 規則の名前を入力します。漢字がサポートされています。
Rule description			ポリシーベースの NAT66 規則の説明を入力します。
Original packets		Src zone	パケットの照合に使用する送信元セキュリティーゾーンを選択します。
		Dst zone	パケットを照合する宛先セキュリティーゾーンを選択します。
		Source IP	パケットを照合する送信元 IP アドレス、IP サブネット、またはアドレスオブジェクトグループを選択します。
		Destination IP	パケットを照合する宛先 IP アドレス、IP サブネット、またはアドレスオブジェクトグループを選択します。
		Service	パケットを一致させるサービスオブジェクトグループを選択します。
Source address translation	Translation method		送信元アドレス変換方式を選択します。 • **Dynamic IP+port**: PAT 方式を使用して、パケットの送信元 IP アドレスと送信元ポートの両方を変換します。 • **Dynamic IP**: NO-PAT 方式を使用して、パケットの送信元 IP アドレスだけを変換します。 • **Static IP**: パケットの送信元 IP アドレスを固定 IP アドレスに変換します。

項目		説明
		• **NPTV6**: NPTV6 方式を使用して、パケットの送信元 IPv6 アドレス内のプレフィクスを設定済みプレフィクスに変換します。この方式を使用するには、元のパケットに対してパケット一致規則を設定する必要があります。 • **No translation**: この規則およびこの規則よりも優先順位の低い規則は、送信元アドレスの変換には使用されません。
	Source IP after NAT	送信元アドレス変換の NAT アドレスを選択します。
	IPv6 prefix	プレフィクス変換方式の IPv6 アドレスプレフィクスを設定します。 このオプションは、プレフィクス変換方式が **NPTV6** の場合にだけ使用できます。
	Prefix length	IPv6 プレフィクス長を設定します。 このオプションは、プレフィクス変換方式が **NPTV6** の場合にだけ使用できます。
Destination address translation	Translation method	宛先アドレス変換方式を選択します。 • **Translation**: パケットの宛先 IP アドレスを固定 IP アドレスに変換します。 • **NPTV6**: NPTV6 方式を使用して、パケットの宛先 IPv6 アドレス内のプレフィクスを設定済みプレフィクスに変換します。 • **No translation**: この規則およびこの規則よりも優先順位の低い規則は、宛先アドレス変換には使用されません。
	Destination IP after NAT	変換後の宛先 IP アドレスを設定します。
	Port after NAT	変換後の宛先ポートを設定します。
	IPv6 prefix	プレフィクス変換方式の IPv6 アドレスプレフィクスを設定します。 このオプションは、変換方法が **NPTV6** の場合にのみ使用できます。
	Prefix length	IPv6 プレフィクス長を設定します。 このオプションは、変換方法が **NPTV6** の場合にのみ使用できます。

項目	説明
VRF before NAT	パケットが属する VRF と照合するために使用する VRF を指定します。VRF は入力ポートにバインドされます。
VRF after NAT	一致するパケットが属する VRF を置き換えるために使用される VRF を指定します。VRF は出力ポートにバインドされます。
Enable this rule	このポリシーベースの NAT66 規則をイネーブルにします。
Counting	ポリシーベースの NAT66 規則が一致する回数のカウントをイネーブルにします。

NAT

このヘルプには、次のトピックがあります。

Introduction

ネットワークアドレス変換(NAT)は、IP パケットヘッダー内の IP アドレスを別の IP アドレスに変換します。通常、NAT はゲートウェイ上で構成され、プライベートホストが外部ネットワークにアクセスし、外部ホストが Web サーバーなどのプライベートネットワークリソースにアクセスできるようにします。

Dynamic NAT

ダイナミック NAT は、アドレスプールを使用してアドレスを変換します。これは、多数の内部ユーザーが外部ネットワークにアクセスするシナリオに適用されます。

- **NO-PAT**

  Not Port Address Translation(NO-PAT)は、プライベート IP アドレスを IP パブリックアドレスに変換します。パブリック IP アドレスは、解放されるまで別の内部ホストで使用できません。

NO-PAT はすべての IP パケットをサポートします。

- **PAT**

  Port Address Translation(PAT)は、プライベート IP アドレスと送信元ポートをパブリック IP アドレスと一意のポートにマッピングすることによって、複数のプライベート IP アドレスを 1 つのパブリック IP アドレスに変換します。PAT は、TCP パケット、UDP パケット、および ICMP 要求パケットをサポートします。
  NAT アドレスグループは、アドレス範囲のセットです。外部ネットワーク宛てのパケット内の送信元アドレスは、いずれかのアドレス範囲内のアドレスに変換されます。

NAT Server

NAT サーバー機能は、パブリックアドレスとポート番号を内部サーバーのプライベート IP アドレスとポート番号にマップします。この機能により、プライベートネットワーク内のサーバーは外部ユーザーにサービスを提供できます。次の表に、NAT サーバーの外部ネットワークと内部ネットワーク間のアドレスとポートのマッピングを示します。

表 1 NAT サーバーのアドレスポートマッピング

外部ネットワーク	内部ネットワーク
One public address	1 つのプライベートアドレス
One public address and one public port number	1 つのプライベートアドレスと 1 つのプライベートポート番号
One public address and *N* consecutive public port numbers	• 1 つのプライベートアドレスと 1 つのプライベートポート番号 • N 個の連続したプライベートアドレスと 1 つのプライベートポート番号 • 1 つのプライベートアドレスと N 個の連続したプライベートポート番号
N consecutive public addresses	• 1 つのプライベートアドレス • N 個の連続するプライベートアドレス
N consecutive public addresses and one public port number	• 1 つのプライベートアドレスと 1 つのプライベートポート番号 • N 個の連続したプライベートアドレスと 1 つのプライベートポート番号

外部ネットワーク	内部ネットワーク
	• 1 つのプライベートアドレスと N 個の連続したプライベートポート番号
One public address and one public port number	1 つの内部サーバーグループ
One public address and *N* consecutive public port numbers	
N consecutive public addresses and one public port number	
Public addresses matching an ACL	1 つのプライベートアドレス
	1 つのプライベートアドレスと 1 つのプライベートポート
Public addresses in an address object group	1 つのプライベートアドレス
	1 つのプライベートアドレスと 1 つのプライベートポート

負荷分散のために複数の内部サーバーを内部サーバーグループに追加して、これらのサーバーが外部ホストに同じサービスを提供できるようにできます。NAT デバイスは、外部ホストから内部サーバーグループのパブリックアドレスへの要求に応答するために、サーバーの接続の重みと数に基づいて 1 つの内部サーバーを選択します。

Static NAT

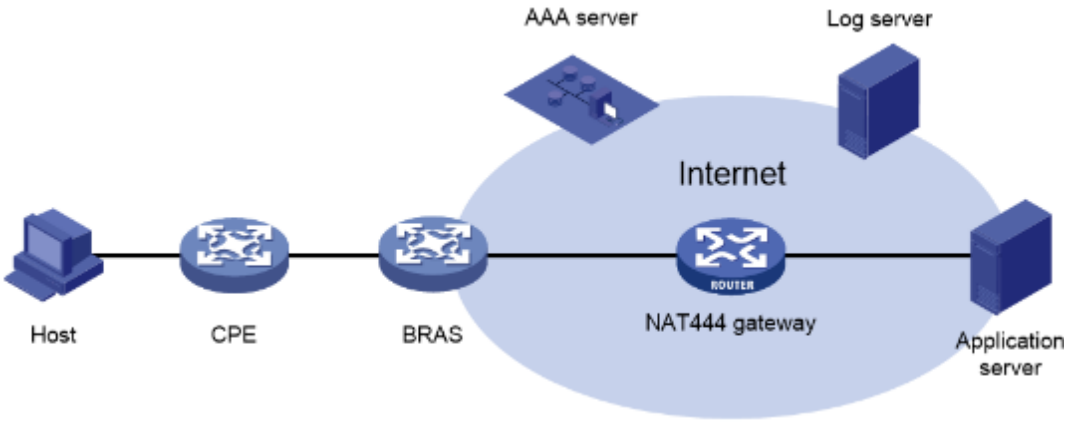
静的 NAT は、プライベートアドレスとパブリックアドレスの間に固定マッピングを作成します。静的 NAT は、内部ユーザーから外部ネットワークへの接続、および外部ユーザーから内部ネットワークへの接続をサポートします。静的 NAT は通常の通信に適用されます。

NAT444

NAT444 は、NAT444 ゲートウェイ、AAA サーバー、およびログサーバーを統合することによって、キャリアグレードの NAT を提供します。NAT444 では、キャリア側に NAT の第 2 レイヤーが導入されますが、カスタマー側とアプリケーションサーバー側での変更はほとんどありません。ポートブロックの割り当てにより、NAT444 はユーザートラッキングをサポートします。これは、IPv6 への移行において、キャリアにとって好ましいソリューションとなっています。

図 1 は、NAT444 ソリューションのアーキテクチャを示しています。

図 1:NAT444 ソリューションのアーキテクチャ



このアーキテクチャのデバイスは、次のようなサービスを提供します。

- **CPE**: カスタマー側のアドレス変換を実行します。
- **BRAS**: エンドポイントアクセスサービスを提供し、認証、認可、アカウンティングのために AAA サーバーと連動します。
- **NAT444 gateway** キャリアグレードのアドレス変換を実行します。
- **AAA Server**: 認証、認可、およびアカウンティングサービスを提供します。
- **Log Server**: ユーザークセス情報を記録し、ユーザー情報のクエリーに応答します。

NAT444 は、ポート範囲に基づく PAT 変換です。複数のプライベート IP アドレスを 1 つのパブリック IP アドレスにマッピングし、各プライベート IP アドレスに対して異なるポートブロックを使用します。たとえば、内部ホストのプライベート IP アドレス 10.1.1.1 はパブリック IP アドレス 202.1.1.1 にマッピングされ、ポートブロック 10001 は 10256 にマッピングされます。内部ホストがパブリックホストにアクセスすると、送信元 IP アドレス 10.1.1.1 は 202.1.1.1 に変換され、送信元ポートはポートブロック 10001～10256 のポートに変換されます。

Static NAT444

NAT ゲートウェイは、アドレス変換の前にスタティックポートブロックマッピングを計算します。マッピングは、プライベート IP アドレスとポートブロックを持つパブリック IP アドレスの間で行われます。

内部ユーザーが外部ネットワークへの接続を開始すると、システムは次の操作を実行します。

- ユーザーのプライベート IP アドレスに基づいてスタティックマッピングを検索し、マッピング内のパブリック IP アドレスとポートブロックを取得します。
- ポートブロック内のパブリックポート番号を選択します。
- プライベート IP アドレスをパブリック IP アドレスに変換し、選択したパブリックポート番号を割り当てます。

NAT ゲートウェイは、プライベート IP アドレス、パブリック IP アドレス、ポート範囲、およびポートブロック

サイズを使用して、スタティックマッピングを計算します。

1. ポート範囲をポートブロックサイズで除算して、各パブリック IP アドレスで使用可能なポートブロック数を取得します。

   この値はマッピングのベース番号です。

2. 各ブロックの開始ポート番号の昇順でポートブロックをソートします。
3. プライベート IP アドレスとパブリック IP アドレスを昇順にソートします。
4. プライベート IP アドレスの最初のベース番号を、最初のパブリック IP アドレスとそのポートブロックに昇順でマッピングします。

たとえば、各パブリック IP アドレスの使用可能なポートブロック数は m です。最初の m 個のプライベート IP アドレスは最初のパブリック IP アドレスにマッピングされ、m 個のポートブロックは昇順にマッピングされます。次の m 個のプライベート IP アドレスは 2 番目の IP アドレスにマッピングされ、m 個のポートブロックは昇順にマッピングされます。その他のスタティックポートブロックマッピングは、類推によって作成されます。

Dynamic NAT444

ダイナミック NAT444 は、ダイナミック NAT とスタティック NAT444 の機能を統合します。内部ユーザーが外部ネットワークへの接続を開始すると、ダイナミック NAT444 は次のように動作します。

1. ACL を使用して変換制御を実装します。ACL 許可ルールに一致するパケットだけを処理します。
2. 内部ユーザーのプライベート IP アドレスからパブリック IP アドレスおよびポートブロックへのマッピングを作成します。
3. プライベート IP アドレスをパブリック IP アドレスに変換し、送信元ポートを選択したポートブロック内のポートに変換して、プライベート IP アドレスからの後続の接続に使用します。
4. プライベート IP アドレスからのすべての接続が切断されたときに、ポートブロックを取り消し、ダイナミックポートブロックマッピングを削除します。

ダイナミックポートブロックマッピングは、ポートブロック拡張をサポートします。プライベートアドレスのポートブロック内のポートがすべて使用されている場合、ダイナミックポートブロックマッピングは送信元ポートを拡張ポートブロック内のポートに変換します。

NAT Advanced Settings

PAT mapping mode

次の PAT マッピングモードがサポートされています。

- **Endpoint-Independent Mapping(EIM)**: 同じ送信元 IP およびポートから任意の宛先へのパケットに対して、同じ IP およびポートマッピング(EIM エントリ)を使用します。EIM を使用すると、外部ホスト

は、内部ホストの変換された IP アドレスおよびポートへの接続を開始できます。また、異なる NAT ゲートウェイの背後にある内部ホストは、相互にアクセスできます。

- **Address and Port-Dependent Mapping(APDM)**: 同じ送信元 IP およびポートから異なる宛先 IP アドレスおよびポートへのパケットに対して、異なる IP およびポートマッピングを使用します。APDM では、内部ホストが以前に外部ホストにアクセスしたことがある場合にのみ、外部ホストが内部ホストへの接続を開始できます。これは安全ですが、異なる NAT ゲートウェイの背後にある内部ホストが相互にアクセスすることは許可されません。

NAT DNS Mappings

NAT DNS マッピングを使用すると、DNS サーバーがパブリックネットワーク上にある場合、内部ネットワークのユーザーは、ドメイン名を使用して内部サーバーにアクセスできます。NAT DNS マッピングは、NAT サーバーマッピングと連動して機能します。NAT DNS マッピングは、内部サーバーのドメイン名を、内部サーバーのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプにマッピングします。NAT サーバーマッピングは、パブリック IP およびポートを、内部サーバーのプライベート IP およびポートにマッピングします。
外部 DNS サーバーからの DNS 応答には、ペイロード内の内部サーバーのドメイン名とパブリック IP アドレスのみが含まれています。NAT インターフェースには、同じパブリック IP アドレスで異なるプライベート IP アドレスを持つ複数の NAT サーバーマッピングがある場合があります。DNS ALG は、パブリック IP アドレスのみを使用して不正な内部サーバーを検出する場合があります。NAT DNS マッピングが構成されている場合、DNS ALG は、ドメイン名を使用して内部サーバーのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプを取得できます。その後、DNS ALG は、内部サーバーのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプを使用して正しい内部サーバーを検出できます。

NAT hairpin

NAT ヘアピンを使用すると、内部ホストは NAT を介して相互にアクセスできます。パケットの送信元および宛先 IP アドレスは、内部ネットワークに接続されたインターフェース上で変換されます。NAT ヘアピンは、NAT サーバーおよび発信ダイナミックまたはスタティック NAT と連携して機能します。サービスを正しく提供するには、コラボレーティブ NAT 機能と同じインターフェースモジュール上で NAT ヘアピンを設定する必要があります。
NAT ヘアピンには、C/S モードと P2P モードがあります。

- **C/S**: 内部ホストが NAT アドレスを使用して内部サーバーにアクセスできるようにします。内部サーバーに送信されるパケットの宛先 IP アドレスは、NAT サーバーの設定と照合して変換されます。送信元 IP アドレスは、発信ダイナミック NAT エントリまたは発信スタティック NAT エントリと照合して変換されます。

- **P2P**: 内部ホストが NAT を介して相互にアクセスできるようにします。内部ホストは最初にパブリックアドレスを外部サーバーに登録します。次に、登録された IP アドレスを使用して相互に通信します。P2P モードを設定するには、外部ネットワークに接続されたインターフェース上で発信 PAT を設定し、EIM マッピングモードをイネーブルにする必要があります。

NAT global settings

NAT デバイスの 2 つの出力インターフェースが同じセキュリティーゾーンにある WAN ネットワークでは、一方のインターフェースのリンクに障害が発生すると、トラフィックはもう一方のインターフェースのリンクに切り替えられます。NAT デバイスは、リンクのスイッチオーバー後も古いセッションエントリを保持します。NAT デバイスは古いセッションエントリを使用してユーザートラフィックを照合するため、内部ユーザーは外部ネットワークにアクセスできません。この問題を回避するには、NAT セッションの再作成を有効にして、NAT サービスの可用性を確保します。ユーザートラフィックが到着すると、デバイスは NAT セッションを再作成します。

Restrictions and guidelines

General restrictions and guidelines

- **Policy NAT** はインターフェース NAT よりも優先順位が高く、パケットがポリシーNAT と一致すると、インターフェース NAT との一致が試行されます。
- **A-NAT** アドレスグループは、PAT モードと NO-PAT モードの両方で使用できません。
- ベストプラクティスとして、インバウンドスタティック NAT をアウトバウンドダイナミック NAT、NAT サーバー、またはアウトバウンドスタティック NAT とともに設定して、双方向 NAT を実装します。
- インターフェース上ですべての変換方式を実行する場合、NAT 規則は次の降順でソートされます。

a. NAT Server。
b. Static NAT。
c. NAT444 static port block mapping。
d. Dynamic NAT。

- NAT アドレスグループにアドレス範囲を追加する場合は、アドレス範囲が重複しないようにしてください。

Restrictions and guidelines: Dynamic NAT

1 つのインターフェースに複数の発信ダイナミック NAT 規則を設定できます。

- ACL を含む NAT 規則は、ACL を含まない規則よりも優先されます。
- 2 つの ACL ベースのダイナミック NAT 規則が設定されている場合、ACL 番号が大きい方の規則のプライオリティが高くなります。

Restrictions and guidelines: Static NAT

- スタティックマッピングにオブジェクトグループを指定する場合は、次の制約事項および注意事項に従ってください。
  - パブリックまたはプライベート IPv4 アドレスオブジェクトグループには、IPv4 アドレスオブジェクトを 1 つだけ含めることができます。
  - プライベート IPv4 アドレスオブジェクトグループ内の IPv4 アドレスの数は、パブリック IPv4 アドレスオブジェクトグループ内の数よりも多くすることはできません。
  - パブリック IPv4 アドレスオブジェクトグループ内のオブジェクトをアドレス範囲にすることはできません。
  - アドレスオブジェクトは除外されたアドレスを持つことはできません。そうでない場合、マッピングは有効になりません。
  - 住所オブジェクトの変更は、そのオブジェクトを使用するマッピングに直接影響します。住所オブジェクトの編集は慎重に行ってください。
- アウトバウンドスタティック NAT を VPN ネットワークに展開する場合は、VRF を指定する必要があります。指定する VRF は、NAT インターフェースが属する VRF である必要があります。
- ACL を指定する場合は、次の制約事項および注意事項に従ってください。
  - ACL を指定しない場合、すべての発信パケットの送信元アドレスとすべての着信パケットの宛先アドレスが変換されます。
  - ACL を指定し、逆アドレス変換を指定しない場合、ACL によって許可された発信パケットの送信元アドレスが変換されます。パケットの宛先アドレスは、外部ホストによって内部ホストにアクティブに開始された接続に対しては変換されません。
  - ACL と逆アドレス変換の両方を指定すると、ACL によって許可された発信パケットの送信元アドレスが変換されます。外部ホストによって内部ホストに対してアクティブに開始された接続のパケットが ACL 逆照合によって許可されると、宛先アドレスが変換されます。ACL 逆照合は次のように機能します。
    - パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
    - マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

Restrictions and guidelines: NAT Server

- 負荷共有 NAT サーバーマッピングを構成する場合は、ユーザーが同じパブリックアドレスとパブリックポートを使用して内部サーバー上の同じサービスにアクセスするようにする必要があります。このためには、次のマッピングの値 N が内部サーバーグループ内のサーバーの数以下であることを確認します。
  - 1 つのパブリックアドレスと N 個の連続するパブリックポート番号が、1 つの内部サーバーグループにマッピングされます。

○ N 個の連続するパブリックアドレスと 1 つのパブリックポート番号が、1 つの内部サーバーグループにマッピングされます。

- 重みが大きい内部サーバーは、内部サーバーグループ内で受信する接続の割合が大きくなります。
- VPN ネットワークで NAT サーバーマッピングを設定する場合は、VRF を指定する必要があります。指定する VRF は、NAT インターフェースが属する VRF である必要があります。
- オブジェクトグループベースの NAT サーバーマッピングを設定する場合、一致するパブリックアドレスのオブジェクトグループに指定できるのは、サブネット、IP アドレス範囲、またはホストアドレスで設定された IPv4 アドレスオブジェクトグループだけです。IPv4 アドレスオブジェクトグループは、除外 IPv4 アドレスを持つことはできません。

Configuring NAT

NAT は、インバウンドまたはアウトバウンド方向で実行できます。

- インバウンド NAT:図 2 に示すように、インターフェースで受信されたパケットのアドレス変換を実行します。
- アウトバウンド NAT:図 3 に示すように、インターフェースから送信されたパケットのアドレス変換を実行します。

図 2:インバウンド NAT

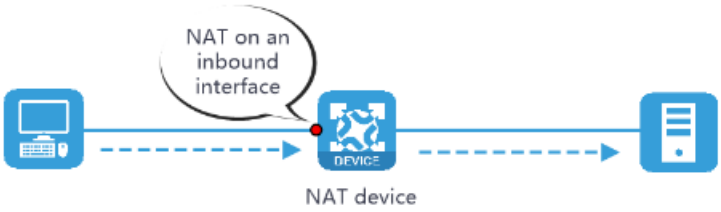
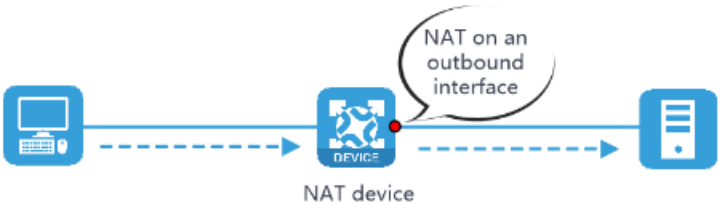


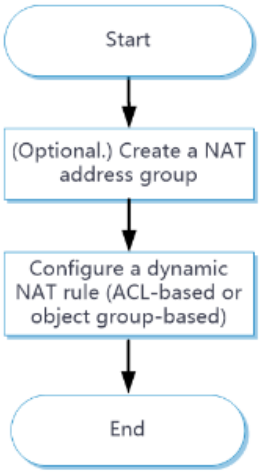
図 3:発信 NAT



Configure dynamic NAT

現在のソフトウェアバージョンでは、アウトバウンドダイナミック NAT だけがサポートされています。ACL ベースのアウトバウンドダイナミック NAT またはオブジェクトグループベースのアウトバウンドダイナミック NAT を設定できます。図 4 に、ダイナミック NAT の設定手順を示します。

図 4:ダイナミック NAT の設定手順



手順

1. (任意)NAT アドレスグループを作成します。
   a. **Objects** タブをクリックします。
   b. ナビゲーションペインで、**Object Groups** > **NAT Address Groups** を選択します。
   c. **Create** をクリックします。
   d. 表 2 に示すように、NAT アドレスグループを作成します。

表 2 NAT アドレスグループの構成項目

項目	説明
Address group ID	NAT アドレスグループの ID を入力します。
Address group name	NAT アドレスグループの名前を入力します。
VRRP group	ハイアベイラビリティの目的で VRRP グループを指定します。 VRRP グループ内のマスターデバイスは、仮想 IP アドレスと仮想 MAC アドレスを使用して ARP 要求に応答します。 VRRP グループ機能のサポートは、デバイスモデルによって異なります。
Port range	アドレス変換のポート範囲を指定します。
Address probe	NQA テンプレートを選択して、アウトバウンドアドレス変換用の NAT アドレスグループ内のアドレスの可用性をプローブします。
Address group members	NAT アドレスグループに IP アドレス範囲を追加します。 NAT アドレスグループは、これらの IP アドレス範囲を使用して、外部ネットワークに送信されるパケットの送信元 IP アドレスを変換します。

e. **OK** をクリックします。

2. ACL ベースのダイナミック NAT を設定します。
   a. **Policies** タブをクリックします。
   b. ナビゲーションペインで、**Interface NAT** > **IPv4** > **Dynamic NAT** を選択します。
   c. **Outbound Dynamic NAT (ACL-Based)**タブをクリックします。
   d. **Create** をクリックします。
   e. 表 3 に示すように、ACL ベースのアウトバウンドダイナミック NAT 規則を作成します。

表 3 ACL ベースのアウトバウンドダイナミック NAT の設定項目

項目	説明
Interface	NAT 規則が適用されるインターフェース。発信ダイナミック NAT は通常、外部ネットワークに接続されたインターフェースで設定されます。
ACL	パケットマッチング用の ACL。ACL を指定すると、NAT は ACL で許可された発信パケットの送信元 IP アドレスを変換します。ACL を指定しないと、NAT はすべてのパケットを変換します。
Source address after NAT	アドレス変換用の NAT アドレスを選択します。 • **NAT address group**: NAT アドレスグループ内の IP アドレスは、アドレス変換に使用されます。 • **Easy IP**: 指定したインターフェースの IP アドレスがアドレス変換に使用されます。 アドレスグループは、PAT モードと NO-PAT モードの両方で使用することはできません。
VRF	変換後に送信元アドレスが属する VRF。デフォルト設定は[Public network]です。 VPN にアウトバウンドダイナミック NAT を展開する場合は、このパラメーターを指定する必要があります。指定する VRF は、指定するインターフェースが属する VRF である必要があります。
Translation mode	ダイナミック NAT 変換モード: • **PAT**: アドレスグループ内の IP アドレスまたはインターフェースの IP アドレスを使用して、一致するパケットの IP アドレスを変換します。一致するパケット内の送信元ポートも変換されます。 • **NO-PAT**: アドレスグループ内の IP アドレスを使用して、一致するパケットの IP アドレスを変換します。一致するパケット内の送信元ポートは変換されません。
Port preservation	PAT のポート番号を保持するようにします。

項目	説明
	このオプションは、変換モードが PAT に設定されている場合にだけ使用できます。
Allow reverse NAT	逆アドレス変換をイネーブルにします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。 このオプションは、変換モードが NO-PAT に設定されている場合にだけ使用できます。
Enable this rule	この NAT 規則をイネーブルにします。

f. **OK** をクリックします。

3. オブジェクトグループベースのダイナミック NAT を設定します。

a. **Policies** タブをクリックします。

b. ナビゲーションペインで、**Interface NAT** > **IPv4** > **Dynamic NAT** を選択します。

c. **Outbound Dynamic NAT (Object Group-Based)**タブをクリックします。

d. **Create** をクリックします。

e. 表 4 に示すように、オブジェクトグループベースのアウトバウンドダイナミック NAT 規則を作成します。

表 4 オブジェクトグループベースのアウトバウンドダイナミック NAT の設定項目

項目	説明
Rule name	NAT 規則の名前を入力します。
Rule description	NAT 規則の説明を入力します。
Output interface	NAT 規則が適用されるインターフェース。発信ダイナミック NAT は通常、外部ネットワークに接続されたインターフェースで設定されます。
Source IP	NAT 規則の送信元 IP アドレスオブジェクトグループ。 1 つの NAT 規則に複数の送信元 IP アドレスオブジェクトグループを設定できます。各送信元 IP オブジェクトグループは、独立したパケット一致基準です。
Destination IP	NAT 規則の宛先 IP アドレスオブジェクトグループ。 1 つの NAT 規則に複数の宛先 IP アドレスオブジェクトグループを設定できます。各宛先 IP オブジェクトグループは、独立したパケット一致基準です。

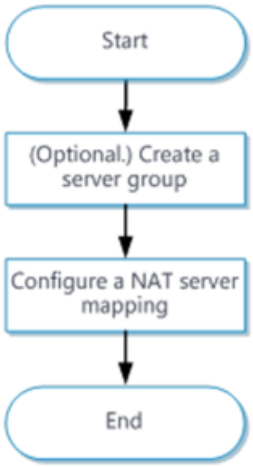
項目	説明
Service	NAT 規則のサービスオブジェクトグループ。 1 つの NAT 規則に複数のサービスオブジェクトグループを設定できます。各サービスオブジェクトグループは、独立したパケット一致基準です。 NAT 規則にサービスオブジェクトグループ、送信元 IP オブジェクトグループ、および宛先オブジェクトグループを設定すると、サービスタイプ、送信元 IP アドレス、および宛先 IP アドレスが一致するパケットだけが変換されます。
Action	ダイナミック NAT 変換モード: • **PAT**: アドレスグループ内の IP アドレスまたはインターフェースの IP アドレスを使用して、一致するパケットの IP アドレスを変換します。一致するパケット内の送信元ポートも変換されます。 • **NO-PAT**: アドレスグループ内の IP アドレスを使用して、一致するパケットの IP アドレスを変換します。一致するパケット内の送信元ポートは変換されません。 • **Easy IP**: 指定されたインターフェースの IP アドレスをアドレス変換に使用します。 • **No translation**: 一致するパケットを変換しません。
Source address after NAT	送信元アドレス変換用の NAT アドレスグループ。 アドレスグループは、PAT モードと NO-PAT モードの両方で使用することはできません。
Port reservation	PAT のポート番号を保持するようにします。 このオプションは、変換モードが PAT に設定されている場合にだけ使用できます。
Allow reverse NAT	逆アドレス変換をイネーブルにします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。 このオプションは、変換モードが NO-PAT に設定されている場合にだけ使用できます。
Enable this rule	この NAT 規則をイネーブルにします。

f. **OK** をクリックします。

Configure NAT Server

図 5 に示すように、NAT サーバー機能を設定します。

図 5 NAT サーバーの設定手順



手順

1. (任意)サーバーグループを作成します。
   a. **Policies** タブをクリックします。
   b. ナビゲーションペインで、**Interface NAT** > **IPv4** > **NAT Servers** > **NAT Server Groups** を選択します。
   c. **Create** をクリックします。
   d. サーバーグループを作成します。
   e. **OK** をクリックします。
2. NAT サーバー規則を設定します。
   a. **Policies** タブをクリックします。
   b. ナビゲーションペインで、**Interface NAT** > **IPv4** > **NAT Servers** > **Policy Configuration** を選択します。
   c. **Create** をクリックします。
   d. 表 5 に示すように、NAT サーバー規則を作成します。

表 5 NAT サーバーの構成項目

項目	説明
Rule name	NAT サーバー規則の名前を入力します。
Interface	NAT サーバー規則が適用されるインターフェース。NAT サーバー規則は通常、外部ネットワークに接続されたインターフェースで構成されます。
Protocol type	プロトコルタイプを指定します。プロトコルタイプを指定しない場合、構成はすべてのプロトコルのパケットに適用されます。

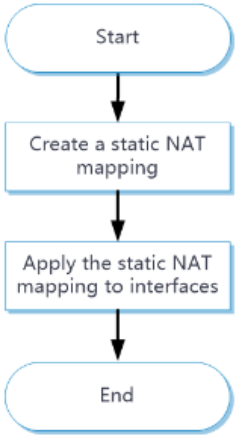
項目	説明
Mapping	アドレスとポートのマッピングを選択します。詳細については、表 1 を参照してください。
Mapping description	多数の NAT マッピングが存在する場合に識別するためのマッピング記述。
Public IP	サーバーが外部ネットワークにアドバタイズするパブリック IP アドレス。
Public port	マッピング方式に応じたパブリックポート番号またはポート範囲。ポート範囲を指定する場合は、終了ポートが開始ポートより大きいことを確認してください。
Public port VRF	アドバタイズされたパブリック IP アドレスが属する VRF。デフォルト設定は[Public network]です。
Server IP	マッピング方式に応じたプライベート IP アドレスまたはアドレス範囲。アドレス範囲では、終了アドレスは開始アドレスよりも大きい必要があります。範囲内のアドレスの数は、パブリックポート範囲内のポートの数と同じである必要があります。
Server port	マッピング方法に応じたプライベートポート番号またはポート範囲。ポート範囲を指定する場合は、終了ポートが開始ポートよりも高いことを確認してください。
Server VRF	NAT サーバーが属する VRF。デフォルト設定は[Public network]です。
ACL for packet matching	ACL を指定すると、NAT は ACL で許可されたパケットを変換します。 ACL を指定しないと、NAT はすべてのパケットを変換します。
VRRP group	ハイアベイラビリティの目的で VRRP グループを指定します。 VRRP グループ内のマスターデバイスは、仮想 IP アドレスと仮想 MAC アドレスを使用して ARP 要求に応答します。 VRRP グループ機能のサポートは、デバイスモデルによって異なります。
Allow reverse NAT	逆アドレス変換を許可します。逆アドレス変換は、内部サーバーによって外部ネットワークに対してアクティブに開始された接続に適用されます。内部サーバーのプライベート IP アドレスをパブリック IP アドレスに変換します。 このオプションは、マッピングタイプが[One single public address with one single public port]または[no public port]に設定されている場合にだけ使用できます。
Enable this rule	この NAT サーバー規則を有効にします。

e. **OK** をクリックします。

Configure Static NAT

現在のソフトウェアバージョンでは、アウトバウンドスタティック NAT だけがサポートされています。図 6 に示すように、スタティック NAT を設定します。

図 6:スタティック NAT の設定手順



手順

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Interface NAT** > **IPv4** > **Static NAT** > **Policy Configuration** を選択します。
3. **Create** をクリックします。
4. スタティック NAT マッピングを作成します。

表 6 静的 NAT 構成項目

項目	説明
Translation method	アドレス変換方式を選択します。 • **One-to-one**: プライベート IP アドレスからパブリック IP アドレスへのアドレス変換を実行します。 • **Net-to-net**: プライベートネットワークからパブリックネットワークへのアドレス変換を実行します。 • **Address object group**: アドレスオブジェクトグループベースのアドレス変換を実行します。

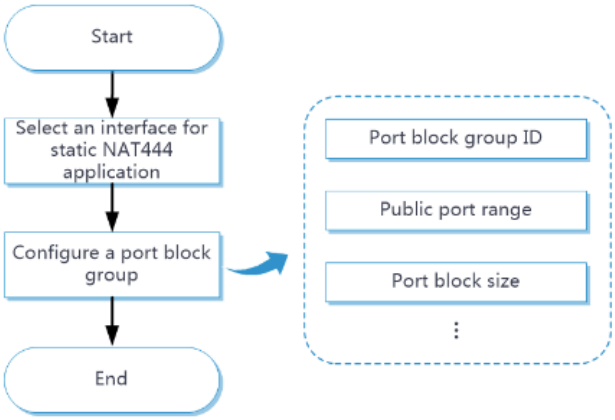
項目	説明
Private address	プライベート IP アドレス。パラメーター設定は変換方式によって異なります。アドレスオブジェクトグループベースの変換方式を選択した場合は、IPv4 アドレスオブジェクトグループを指定する必要があります。
Public VRF	パブリック IP アドレスが属する VRF。デフォルト設定は[Public network]です。
Private VRF	プライベート IP アドレスが属する VRF。デフォルト設定は[Public network]です。
Public address	パブリック IP アドレス。パラメーター設定は変換方式によって異なります。アドレスオブジェクトグループベースの変換方式を選択した場合は、IPv4 アドレスオブジェクトグループを指定する必要があります。
ACL	ACL を指定して、内部ホストがアクセスできる宛先 IP アドレスを定義します。
VRRP group	ハイアベイラビリティの目的で VRRP グループを指定します。 VRRP グループ内のマスターデバイスは、仮想 IP アドレスと仮想 MAC アドレスを使用して ARP 要求に応答します。 VRRP グループ機能のサポートは、デバイスモデルによって異なります。
Allow reverse NAT	逆アドレス変換を許可します。逆アドレス変換は、外部ホストによって内部ホストに対してアクティブに開始された接続に適用されます。パケットが ACL 逆照合によって許可されている場合は、マッピングを使用してこれらの接続のパケットの宛先アドレスが変換されます。
Enable this rule	このスタティック NAT 規則をイネーブルにします。

5. **OK** をクリックします。
6. **Policies** タブをクリックします。
7. ナビゲーションペインで、**nterface NAT** > **IPv4** > **Static NAT** > **Apply Policy** を選択します。
8. 1 つまたは複数のインターフェースを選択します。
9. **Enable** をクリックします。

Configure static NAT444

図 7 に示すように、スタティック NAT444 を設定します。

図 7:スタティック NAT444 の設定手順



手順

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Interface NAT** > **IPv4** > **Static NAT444** を選択します。
3. **Create** をクリックします。
4. インターフェースを選択します。
5. ポートブロックグループを選択または作成します。
6. **OK** をクリックします。

Configure Advanced NAT settings

Configure NAT DNS mappings

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Interface NAT** > **IPv4** を選択します。
3. **NAT DNS Mappings** タブをクリックします。
4. **Create** をクリックして、内部サーバーにドメイン名の新しいマッピングエントリーを追加します。

表 7 NAT DNS マッピング構成項目

項目	説明
Domain name	内部サーバーのドメイン名を指定します。
Internal server running protocol	内部サーバーの実行プロトコルを選択します。 • **TCP**。 • **UDP**。

項目	説明
Public IP	内部サーバーのパブリック IP アドレスを指定します。
Public port number	内部サーバーのパブリックポート番号を指定します。

5. **OK** をクリックします。

NAT hairpin settings

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Interface NAT** > **IPv4** を選択します。
3. **NAT Hairpin** タブをクリックします。
4. インターフェースを選択します。
5. **Enable** をクリックして、選択したインターフェースで NAT Hairpin をイネーブルにします。

Configure general settings

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Interface NAT** > **IPv4** を選択します。
3. **General Settings** タブをクリックします。
4. **Nat session reconstruction under double exists** を選択します。
5. **Apply** をクリックして、Double Exists での NAT セッション再構築をイネーブルにします。

Configure PAT mode

1. **Policies** タブをクリックします。
2. ナビゲーションペインで、**Interface NAT** > **IPv4** を選択します。
3. **General Settings** タブをクリックします。
4. PAT マッピングモードを選択します。オプションには **APDM** と **EIM** があります。
5. **Apply** をクリックします。

AFT

introduction

Address Family Translation(AFT)は、1 つのアドレスファミリの IP アドレスを他のアドレスファミリの IP アドレスに変換します。

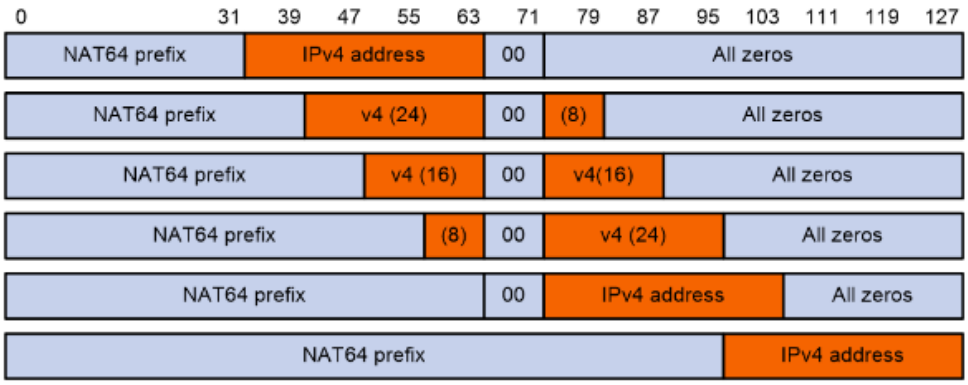
NAT64 prefix

NAT64 接頭辞は、IPv6 ネットワーク内の IPv4 ノードを表す IPv6 アドレスを構成するために使用される IPv6 アドレス接頭辞です。IPv6 ホストは、構成された IPv6 アドレスを実際の IP アドレスとして使用しません。NAT64 接頭辞の長さは、32、40、48、56、64 または 96 です。

図 1 に示すように、構築方法は NAT64 プレフィクス長によって異なります。構築された IPv6 アドレスのビット 64～71 は予約ビットです。

- プレフィクス長が 32、64、または 96 ビットの場合、IPv6 アドレスに含まれている IPv4 アドレスはそのまま残ります。
- プレフィクス長が 40、48、または 56 ビットの場合、IPv6 アドレスに含まれる IPv4 アドレスは、ビット 64～71 によって 2 つの部分に分割されます。

図 1:NAT64 プレフィクスと IPv4 アドレスを使用した IPv6 アドレス構成



AFT translation methods

ダイナミック AFT が IPv 6 から IPv 4 への送信元アドレス変換を実行する場合、Not Port Address Translation(NO-PAT;ポートアドレス変換なし)モードと Port Address Translation(PAT;ポートアドレス変換)モードが使用できます。

NO-PAT

NO-PAT は、1 つの IPv6 アドレスを 1 つの IPv4 アドレスに変換します。1 つの IPv6 ホストに割り当てられた IPv4 アドレスは、解放されるまで他の IPv6 ホストで使用できません。
NO-PAT はすべての IP パケットをサポートします。

PAT

PAT は、各 IPv6 アドレスおよびポートを IPv4 アドレスおよび一意のポートにマッピングすることによって、複数の IPv6 アドレスを単一の IPv4 アドレスに変換します。PAT は次のパケットタイプをサポートします。

- TCP パケット。
- UDP パケット。
- ICMPv6 エコー要求およびエコー応答メッセージ。

PAT は、接続制限およびユーザートレースのためのポートブロックをサポートします。ポートブロックは、ポート範囲(1024～65535)をポートブロックサイズで除算することによって生成されます。ポートブロックベースの PAT は、複数の IPv6 アドレスを 1 つの IPv4 アドレスにマッピングし、各 IPv6 アドレスにポートブロックを使用します。
ポートブロックベースの PAT は次のように機能します。

1. IPv6 ホストが最初に IPv4 ネットワークへの接続を開始すると、ホストの IPv6 アドレスから IPv4 アドレスとポートブロックへのマッピングが作成されます。
2. ポートブロック内のポートがすべて使用されるまで、IPv6 ホストからの後続の接続のために、IPv6 アドレスを IPv4 アドレスに変換し、送信元ポートをポートブロック内のポートに変換します。

AFT translation process

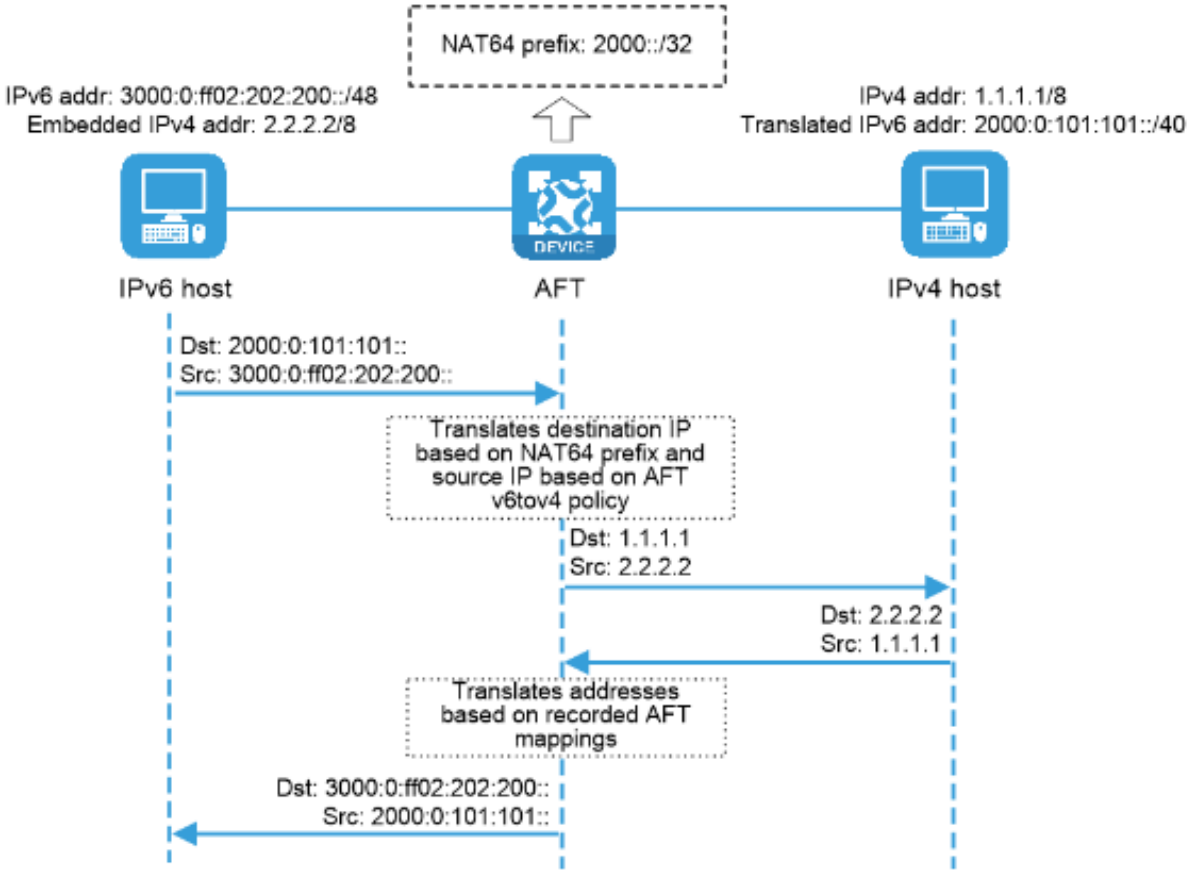
図 2 に示すように、IPv6 ホストが IPv4 ホストへのアクセスを開始すると、AFT は次のように動作します。

1. IPv6 ホストからパケットを受信すると、AFT はそのパケットを IPv6 から IPv 4 への宛先アドレス変換ポリシーと比較します。
    - 一致するポリシーが見つかると、AFT はそのポリシーに従って宛先 IPv6 アドレスを変換します。
    - 一致するポリシーが見つからない場合、AFT はパケットを処理しません。
2. AFT は事前検索を実行して、変換されたパケットの出力インターフェースを決定します。PBR は事前検索には使用されません。
    - 一致するルートが見つかった場合、プロセスはステップ 3 に進みます。
    - 一致するルートが見つからない場合、AFT はパケットを廃棄します。
3. AFT は、パケットの送信元 IPv6 アドレスを IPv6 から IPv 4 への送信元アドレス変換ポリシーと比較します。

- 一致するポリシーが見つかると、AFT はそのポリシーに従って送信元 IPv6 アドレスを変換します。
- 一致するポリシーが見つからない場合、AFT はパケットを廃棄します。

4. AFT は変換されたパケットを転送し、IPv6 アドレスと IPv4 アドレス間のマッピングを記録します。
5. AFT は、パケット転送前に、アドレスマッピングに基づいて、応答パケットヘッダー内の IPv4 アドレスを IPv6 アドレスに変換します。

図 2:IPv 6 で開始される通信の AFT プロセス



Application audit

このヘルプには、次のトピックがあります。

- Introduction
  - Basic concepts
  - Application audit process
  - Application audit policy
  - Match criteria
  - Audit rule
- Restrictions and guidelines
- Configure application audit
  - Configure a keyword group
  - Configure an application audit policy

Introduction

> この機能はユーザーパケットの個人情報を解析するため、正当な目的で使用する必要があります。

アプリケーション監査は,アプリケーション認識(APR:Application Recognition)に基づいて,アプリケーションの動作や動作内容を識別し,ユーザーのインターネットアクセス動作を監査して記録する。

Basic concepts

Application behaviors

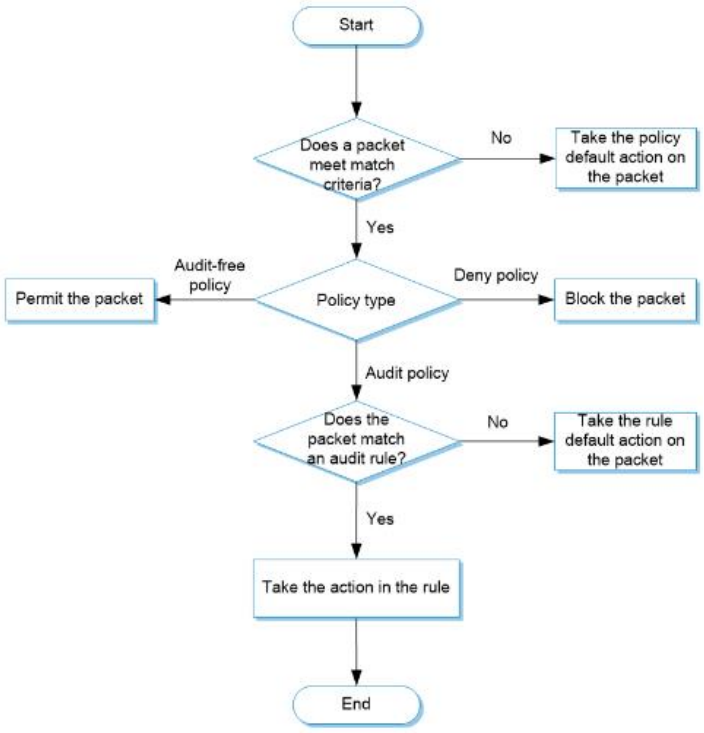
アプリケーションとプログラムは、異なる動作によって特徴付けられます。たとえば、IM アプリケーションはログインとメッセージ送信によって特徴付けられます。FTP はファイルのアップロードとダウンロードによって特徴付けられます。

Behavior contents

動作コンテンツは、動作のコンテンツです。たとえば、ログイン動作のコンテンツはアカウント情報です。FTP ファイルアップロード動作のコンテンツはファイル名です。文字列または数値を使用して動作コンテンツを照合できます。

Application audit process

図 1:アプリケーション監査プロセス



Application audit policy

監査ポリシーが異なると、一致するパケットの処理も異なります。

Policy types

アプリケーション監査ポリシーには、次のタイプがあります。

- **Audit policy**: ポリシーの一致基準を満たすパケットを監査します。
- **Audit-free policy**: ポリシーの一致基準を満たすパケットを監査しません。
- **Deny policy**: ポリシーの一致基準を満たすパケットをドロップします。

Policy matching

1 つのデバイスに複数のアプリケーション監査ポリシーを設定できます。デバイスはパケットとポリシーを設定順に比較します。一致するものが見つかると、照合プロセスは終了します。一致するものが見つからない場合、デバイスはパケットにデフォルトのアクションを適用します。

ポリシーの構成順序は、Audit Policy ページで確認できます。構成順序は、ポリシーが移動されない場合の作成順序です。ポリシーの構成順序は、ポリシーを移動することで変更できます。パケットをより正確に

監査するためのベストプラクティスとして、ポリシーの作成時には深さ優先の原則に従ってください。常に、監査スコープが小さいポリシーを作成してから、監査スコープが大きいポリシーを作成してください。

Match criteria

1 つのアプリケーション監査ポリシーで複数の一致基準を構成できます。ポリシーは、ポリシー内のすべての一致基準が一致する場合に一致します。
次の一致基準を使用できます。

- ソースおよびターゲットのセキュリティーゾーン。
- 送信元および宛先の IP アドレス。
- ユーザー/ユーザーグループ。
- アプリケーション/アプリケーショングループ。
- サービス。
- 時間範囲。

1 つの一致基準に複数の一致値を含めることができます。たとえば、送信元 IP アドレスの一致基準に複数のアドレスオブジェクトグループを設定できます。一致基準は、その一致値のいずれかが一致した場合に一致します。

Audit rule

監査規則の監査規則を設定して、ユーザーの動作をより詳細に制御し、監査ログを生成できます。
次のルール一致モードを使用できます。

- **in-order**: デバイスは、規則 ID の昇順でパケットを監査規則と比較します。パケットが規則と一致すると、デバイスは一致プロセスを停止し、規則で定義されたアクションを実行します。
- **all**: デバイスは、規則 ID の昇順でパケットを監査規則と比較します。
    - パケットが permit アクションを規則と一致する場合、以降のすべての規則は引き続き一致します。
      デバイスは、一致するパケットに対してより高いプライオリティでアクションを実行します。deny アクションは、permit アクションよりも高いプライオリティを持ちます。
    - パケットが deny アクションを含むルールと一致する場合、デバイスは一致プロセスを停止し、deny アクションを実行します。

パケットがどの監査規則とも一致しない場合、デバイスはパケットの監査規則に対するデフォルトのアクションを実行します。
電子メール保護はルールで構成できます。デバイスは受信電子メールを検出し、受信者に基づいて電子メールをカウントし、受信者を攻撃から保護します。具体的には、次の機能を構成できます。

- **Limit email sending**: ユーザーが別のドメインのユーザーに電子メールを送信できないようにします。たとえば、user1@abc.com のユーザーは、user2@123.com のユーザーからの電子メールを受信できません。
- **Prevent email bombing**: 受信者が同じ送信者からの大量の電子メールに短時間で圧倒されないように保護します。

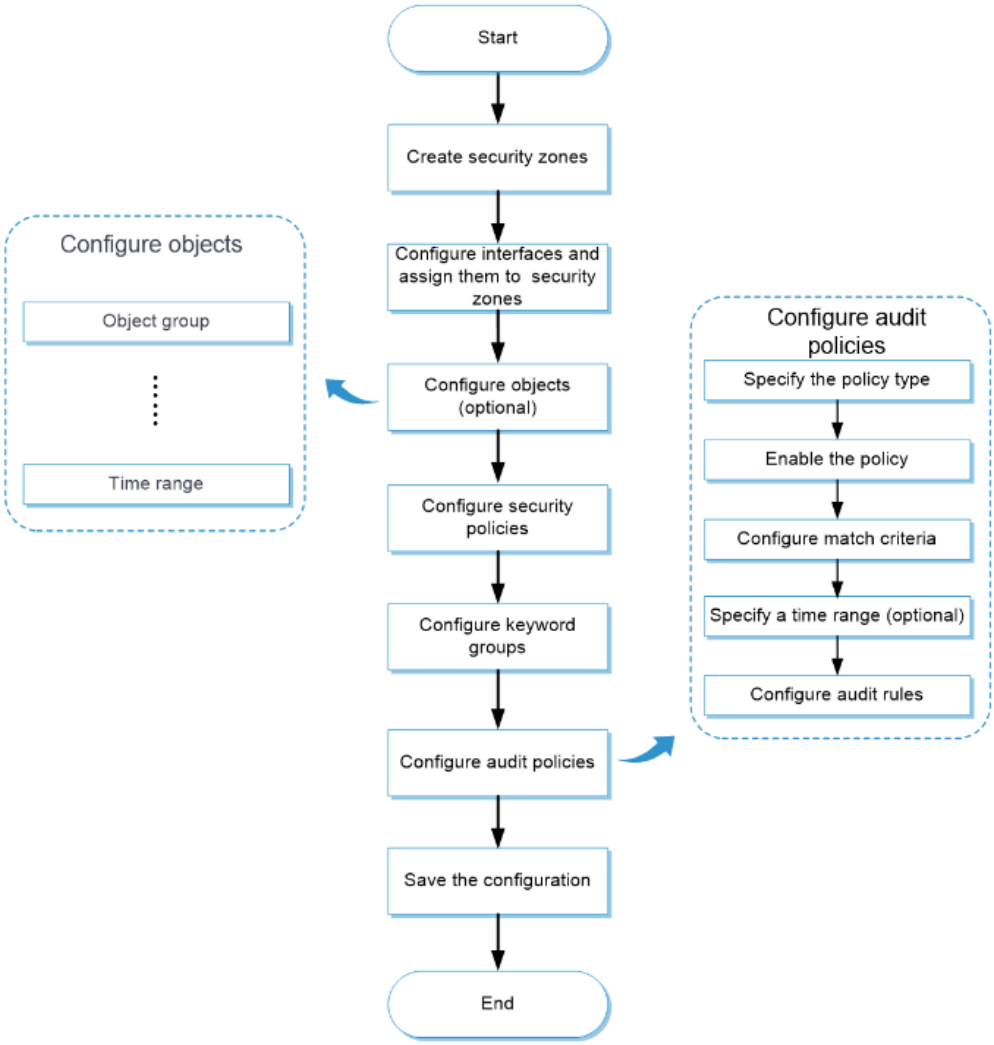
Restrictions and guidelines

デフォルトでは、監査ポリシー構成の変更は、変更が実行されてから 40 秒後に有効になります。変更をすぐに有効にするには、Submit ボタンをクリックします。構成の変更は、監査ポリシーの作成、編集、削除、有効化または無効化を示します。構成をアクティブ化すると、一時的な DPI サービスの中断が発生します。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。

Configure application audit

図 2 は、アプリケーション監査の構成手順を示しています。

図 2:アプリケーション監査設定手順



アプリケーション監査を構成する前に、セキュリティーポリシーを構成して、トラフィックがデバイスを通過できるようにします。セキュリティーポリシーの構成の詳細は、「セキュリティーポリシーのヘルプ」を参照してください。

Configure a keyword group

1. **Policies** > **Application Audit** > **Keyword Groups** を選択します。
2. **Keyword Group** ページで **Create** をクリックします。
3. キーワードグループを作成します。

表 1 キーワードグループの構成項目

項目	説明
Name	キーワードグループの名前を入力します。

Description	キーワードグループの説明を入力します。これは、管理者がキーワードグループを識別するのに役立ちます。
Keyword	監査するキーワードを入力します。キーワードは改行で区切ります。

4. **OK** をクリックします。新しいキーワードグループが **Keyword Group** ページに表示されます。

Configure an application audit policy

1. **Policies** > **Application Audit** > **Audit Policies** を選択します。
2. **Audit Policy** ページで **Create** をクリックします。
3. アプリケーション監査ポリシーを作成します。

表 2 アプリケーション監査ポリシーの構成項目

項目	説明
Name	アプリケーション監査ポリシーの名前を入力します。
Type	アプリケーション監査ポリシータイプ([監査]、[監査なし]、および[拒否])を選択します。
Enable	ポリシーを有効にして有効にします。
Source security zone	送信元セキュリティーゾーンを一致基準として指定します。
Destination security zone	宛先セキュリティーゾーンを一致基準として指定します。
Source IP address	送信元 IP アドレスオブジェクトグループを一致基準として指定します。
Destination IP address	一致基準として宛先 IP アドレスオブジェクトグループを指定します。
Service	一致基準としてサービスオブジェクトグループを指定します。
User	一致基準としてユーザーを指定します。
Application	アプリケーションまたはアプリケーショングループを一致基準として指定します。
Time range	ポリシーが有効な時間範囲を指定します。

Audit rule	監査規則を構成して、アプリケーションの動作および動作内容に対して詳細な監査を実行します。この項目は、監査タイプのポリシーに対してのみ構成できます。
Rule ID	ルール ID を入力します。
Application	監査するアプリケーションを選択します。
Behavior	監査する動作を選択します。
Behavior content	監査する動作内容を選択します。
Match type	動作のコンテンツタイプを指定します。 • **Keyword**。 • **Number**。
Keyword	動作の内容が一致する場合に使用される演算子: • キーワードタイプの動作コンテンツの場合: **Include**, **Exclude**, **Equal**, **Unequal**。 • 数値タイプの動作内容の場合: **Equal**, **Unequal**, **Greater**, **Less**, **Greater-equal**, **Less-equal**。
Email protection	**Enable** を選択して、**Limit email sending** および **Prevent email bombing** 機能を設定します。
Limit email sending	**Enable** を選択して、ユーザーが別のドメインのユーザーに電子メールを送信できないようにします。
Prevent email bombing	この機能を設定すると、同じ送信者からの大量の電子メールが短時間に受信者を圧倒することを防ぐことができます。 • **Detection time**: この期間中に同じユーザーから受信できる E メールの最大数を指定します。 • **Email count**: 検出時間内に同じユーザーから受信できる電子メールの最大数。
Action	監査規則と一致するパケットに対して実行するアクション **Permit** または **Deny** を選択します。
Logging	**Enabled** または **Disabled** を選択して、ログの生成を有効または無効にします。

4. **OK** をクリックします。新しいアプリケーション監査ポリシーが **Audit Policy** ページに表示されます。

5. 新しいアプリケーション監査ポリシーをすぐに有効にするには、**Submit** ボタンをクリックします。デフォルトでは、新しい監査ポリシーは作成されてから 40 秒後に有効になります。

Bandwidth management

このヘルプには、次のトピックがあります。

- Introduction
  - Bandwidth management process
  - Traffic rule
  - Traffic profile
- Restrictions and guidelines
- Configure bandwidth management
  - Configure a traffic profile
  - Configure a traffic policy
  - Configure interface bandwidth

Introduction

帯域幅管理は、送信元および宛先の IP アドレスやユーザー名などの情報を使用して、デバイスを通過するトラフィックをきめ細かく制御します。
帯域幅管理は、次のシナリオで使用されます。

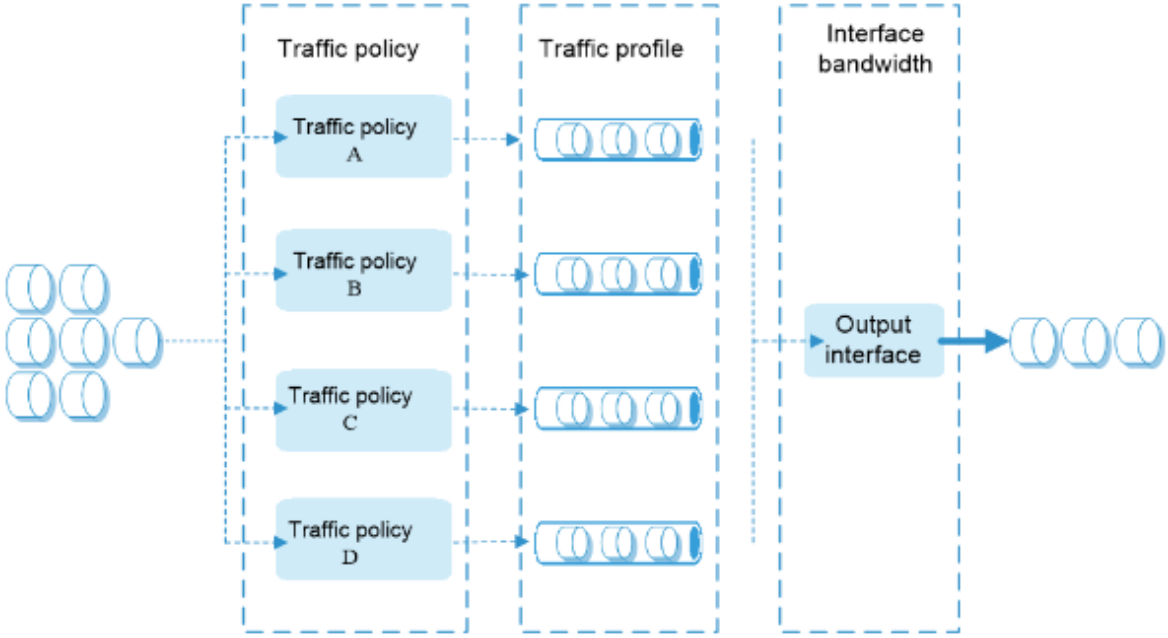
- 企業のイントラネットユーザーは、ISP からリースされた帯域幅の量よりもはるかに多くの帯域幅を必要とします。これにより、イントラネット出力で帯域幅のボトルネックが発生します。
- イントラネット出力上の P2P トラフィックは、帯域幅リソースの大部分を消費します。その結果、主要サービスの帯域幅は保証されません。

帯域幅管理を使用すると、さまざまなトラフィックタイプのネットワーク出力にトラフィックポリシーを導入できます。帯域幅管理により、帯域幅効率が向上し、輻輳が発生した場合に主要なサービスの帯域幅が保証されます。

Bandwidth management process

帯域幅管理は、トラフィックポリシーを通じて実装されます。トラフィックポリシーでは、トラフィックプロファイルとトラフィックポリシーを設定できます。トラフィックプロファイルは、保証帯域幅と最大帯域幅を指定します。トラフィックポリシーは、パケットを照合するための一致基準と、一致するパケットに適用するトラフィックプロファイルを指定します。

図 1:帯域幅管理プロセス



帯域幅管理プロセスは次のとおりです。

2. パケットがトラフィックポリシーと一致する場合、インターフェースは、トラフィックポリシーに指定されたトラフィックプロファイル(存在する場合)に従ってパケットを処理します。
   トラフィックポリシーにトラフィックプロファイルが指定されていない場合、パケットは帯域幅管理なしで転送されます。
3. トラフィックプロファイルは、その設定に従ってパケットを処理します。
4. パケットは、出力インターフェースのインターフェース帯域幅によって制限されます。

Traffic rule

複数のトラフィックポリシーを設定できます。トラフィックポリシーでは、パケットを一致させる一致基準を定義し、一致するパケットに適用するトラフィックプロファイルを指定できます。デバイスは、デバイス上での出現順にトラフィックポリシーを一致させます。トラフィックポリシーが一致すると、一致プロセスが終了し、デバイスはトラフィックポリシーのトラフィックプロファイルをトラフィックに適用します。トラフィックポリシーが一致しない場合、デバイスはトラフィックを転送します。

トラフィックポリシーでは、次の一致基準を設定できます。

- ソースおよびターゲットのセキュリティーゾーン。
- 送信元および宛先の IP アドレス。
- ユーザー。

1 つの一致基準に複数の一致値を含めることができます。たとえば、送信元 IP アドレスの一致基準に複

数のアドレスオブジェクトグループを設定できます。一致基準は、その一致値のいずれかが一致した場合に一致します。

トラフィックポリシーは、ポリシーのネストをサポートします。これにより、トラフィックポリシーは親トラフィックポリシーを持つことができます。最大 4 つのネストレベルがサポートされます。デバイスがトラフィックポリシーを親トラフィックポリシーと一致させる場合、次の規則が適用されます。

- 親トラフィックポリシーが最初に照合されます。親トラフィックポリシーが照合された後、子トラフィックポリシーが照合されます。親トラフィックポリシーが照合されない場合、子トラフィックポリシーは無視され、照合プロセスは失敗します。
- 親と子の両方のトラフィックポリシーが一致する場合、親のトラフィックポリシーのトラフィックプロファイルが実行される前に、子のトラフィックポリシーのトラフィックプロファイルが実行されます。親と子の両方のトラフィックポリシーがほぼ同じパラメーターである場合、上限パラメーターには小さい値が適用され、下限パラメーターには大きい値が適用されます。親のトラフィックポリシーだけが一致する場合、親のトラフィックポリシーのトラフィックプロファイルが適用されます。

Traffic profile

トラフィックプロファイルは、トラフィックタイプで使用できる帯域幅リソースを定義します。インターフェース帯域幅は、複数のトラフィックプロファイル間で割り当てることができます。トラフィックプロファイルでは、次のパラメーターを設定できます。

表 1 トラフィックプロファイルのパラメーター

項目	説明
Rate limit mode	トラフィックレートは、次のいずれかの方法で制限できます。 • アップストリーム帯域幅とダウンストリーム帯域幅を別々に制限します。 • アップストリーム帯域幅とダウンストリーム帯域幅全体を制限します。
Reference mode	トラフィックプロファイルは、次のいずれかの方法で複数のトラフィックポリシーによって参照できます。 • **Exclusive**: プロファイルを使用する各ルールは、プロファイルで指定された帯域幅制限および接続制限に到達できます。 • **Shared**: プロファイルを使用するすべてのルールは、プロファイルで指定された帯域幅制限と接続制限を共有します。
Total guaranteed bandwidth	輻輳が発生した場合に、キーサービスの合計最小帯域幅を保証します。
Total maximum bandwidth	非キーサービスが大量の帯域幅を消費しないように、非キーサービスの合計最大帯域幅を制御します。

Bandwidth allocation among IP addresses	最大帯域幅の合計を、オンライン IP アドレス間で動的かつ均等に割り当てます。
Per-IP or per-user guaranteed bandwidth	IP アドレス単位またはユーザー単位の最小帯域幅を保証して、より細かい粒度での帯域幅管理を実現します。
Per-IP or per-user maximum bandwidth	IP アドレス単位またはユーザー単位で許可される最大帯域幅を制御して、より細かい単位で帯域幅を管理します。
Connection limits	合計接続数、合計接続率、ユーザーごと/IP ごとの接続数、およびユーザーごと/IP ごとの接続率を制限します。
Per-IP traffic quota	IP アドレスごとの月間トラフィッククォータを制限します。 この機能を設定すると、**Per-IP traffic statistics** タブでトラフィック統計情報を表示できます。
Monthly traffic quota	IP 単位の月間トラフィッククォータ。
Forwarding priority	インターフェースが複数のトラフィックプロファイルのパケットで輻輳している場合、プライオリティの高いパケットが最初に送信されます。プライオリティが同じパケットは、転送される可能性が同じです。
DSCP marking	パケット内の DSCP 値を変更します。ネットワークデバイスは、DSCP 値を使用してトラフィックを分類し、変更された DSCP 値に従ってパケットに異なる処理を提供できます。
TCP MSS	TCP 最大セグメントサイズを指定します。
Bandwidth check	送信元 IP アドレス別にトラフィックによって消費される帯域幅の量をデバイスがリアルタイムで検出できるようにします。
Static thresholds	最大帯域幅しきい値および最小帯域幅しきい値を指定します。 デバイスは、トラフィックレートが最大帯域幅しきい値を超えるか、最小帯域幅しきい値を下回ることを検出すると、高速ログ出力機能を使用してログホストにログを出力します。
Dynamic threshold learning	デバイスが帯域幅しきい値を動的に学習できるようにします。 ネットワーク内のトラフィックレートが不明な場合は、このオプションをイネーブルにします。デバイスは、学習した帯域幅しきい値に最大許容値と最小許容値を乗算して、最大帯域幅しきい値と最小帯域幅しきい値を導出します。導出された最大帯域幅しきい値と最小帯域幅しきい値は、スタティックしきい値よりも高いプライオリティを持ちます。
Learning duration	学習時間を分単位で指定します。 ダイナミックしきい値学習がイネーブルになると、デバイスは指定された期間のトラフィックレートを学習し、学習した帯域幅しきい値とし

	て平均値を計算します。デバイスが 1 日のトラフィックを学習できるようにするためのベストプラクティスとして、学習期間を 1440 分(24 時間)よりも長く設定します。デバイスの学習中に学習期間が変更された場合、デバイスは新しい学習期間に基づいて再度トラフィックを学習します。
Bandwidth tolerance	帯域幅の許容値を指定します。 デバイスは、学習した帯域幅しきい値に最大および最小帯域幅許容値を乗算することによって、最大および最小帯域幅しきい値を導出します。 最小帯域幅しきい値を考慮しない場合は、最大帯域幅許容値だけを指定できます。最大帯域幅しきい値を考慮しない場合は、最小帯域幅許容値だけを指定できます。

Restrictions and guidelines

- 子トラフィックポリシーの最大帯域幅は、親トラフィックポリシーの最大帯域幅以下である必要があります。
- 子トラフィックポリシーの保証帯域幅は、親トラフィックポリシーの保証帯域幅以下である必要があります。
- トラフィックプロファイルは、子と親のトラフィックポリシーで同じにすることはできません。
- トラフィックポリシーに子トラフィックポリシーがある場合、デバイスは子トラフィックポリシーに対してだけ帯域幅チェックとダイナミックしきい値学習を実行します。
- デフォルトの予想帯域幅が小さいインターフェースでは、次の条件が存在する場合にトラフィック損失が発生する可能性があります。
    - インターフェース上に大量のトラフィックがあります。
    - インターフェースは、デフォルトの予想帯域幅を使用します。

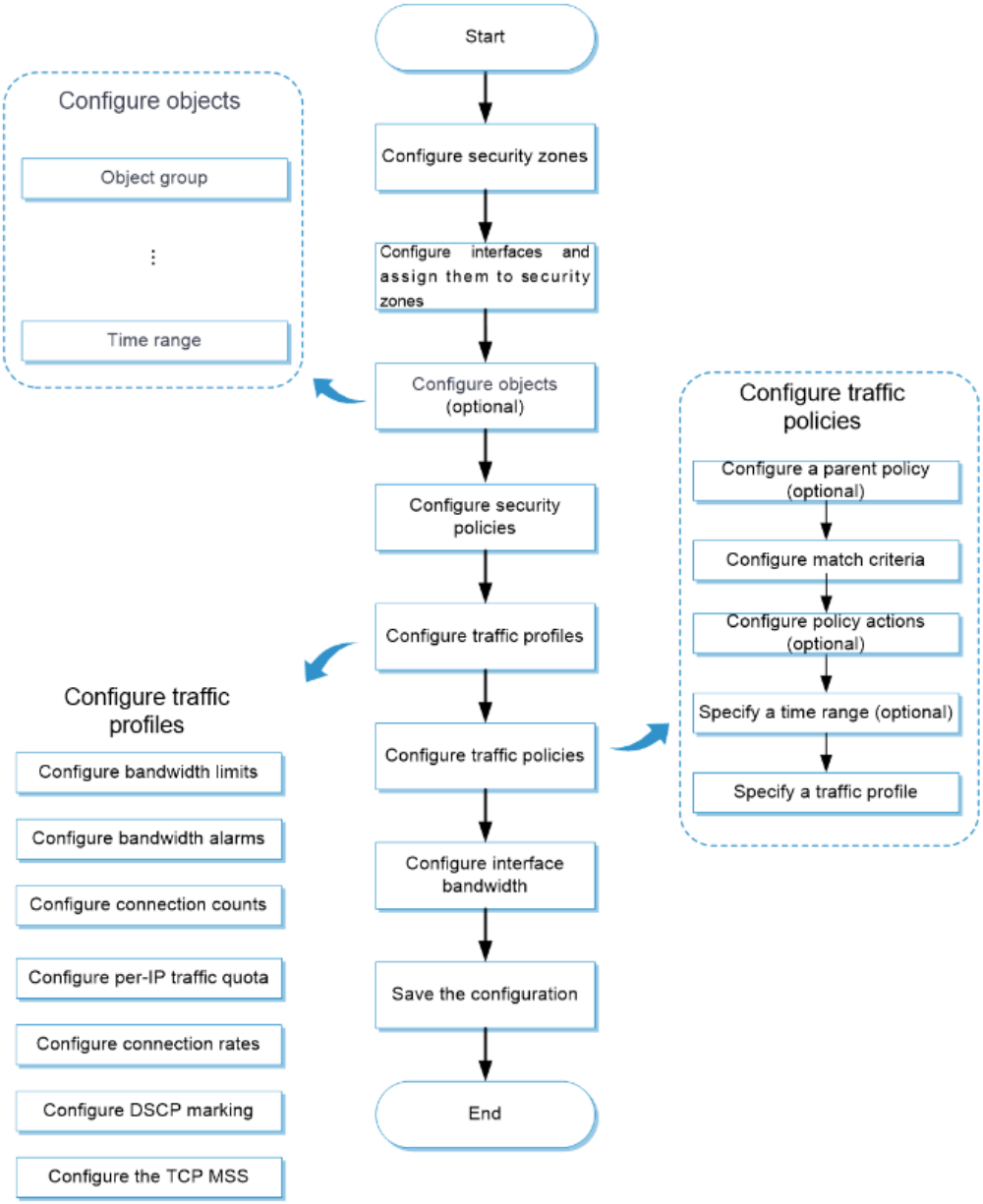
  トラフィック損失を回避するには、このようなインターフェースの予想帯域幅を暗黙的に大きな値に設定します。たとえば、インターフェース上に大量のトラフィックが存在する場合、トンネルインターフェースの予想帯域幅を 64 kbps(デフォルト)より大きい値に設定できます。
- コピーするトラフィックポリシーに子トラフィックポリシーがある場合は、親トラフィックポリシーだけがコピーされます。
- トラフィックポリシーのコピーによって作成されたトラフィックポリシーは、コピーされたトラフィックポリシーの横に配置されます。
- 親トラフィックポリシーは、トラフィックポリシーの作成時にのみ指定できます。既存のトラフィックポリシーに対して親トラフィックポリシーを追加または変更することはできません。
- 子と親のトラフィックポリシーのレート制限モードは同じである必要があります。
- 親トラフィックポリシーでは、最大帯域幅の動的割り当ておよび均等割り当てはサポートされません。

- 全 OSI レイヤープロトコルフロー制御機能は、IPv6 パケットに対してだけ有効です。
- 全 OSI レイヤープロトコルフロー制御機能がディセーブルになると、レイヤー4 プロトコルおよび上位レイヤープロトコルのトラフィックに対して帯域幅管理が実行されます。

Configure bandwidth management

図 2 は、帯域幅管理の設定手順を示しています。

図 2:帯域幅管理の設定手順



帯域幅管理を構成する前に、トラフィックがデバイスを通過できるようにセキュリティーポリシーを構成します。セキュリティーポリシーの構成の詳細は、「セキュリティーポリシーのヘルプ」を参照してください。

Configure a traffic profile

1. **Policies** > **Bandwidth Management** > **Traffic Profiles** を選択します。
2. **Traffic Profile** タブで **Create** をクリックします。
3. トラフィックプロファイルを作成します。

表 2 トラフィックプロファイルの設定項目

項目	説明
Name	トラフィックプロファイルの名前を入力します。
Rate limit mode	**Limit uplink and downlink separately** または **Limit uplink and downlink** を選択します。
Reference mode	**Exclusive** または **Shared** を選択します。
Total uplink maximum bandwidth	合計アップリンク最大帯域幅を設定します。
Total uplink guaranteed bandwidth	アップリンク保証帯域幅の合計を設定します。
Total downlink maximum bandwidth	合計ダウンリンク最大帯域幅を設定します。
Total downlink guaranteed bandwidth	ダウンリンク保証帯域幅の合計を設定します。
Forwarding priority	転送の優先順位を設定します。優先順位の値が大きいほど、優先順位が高くなります。
Bandwidth allocation among IP addresses	最大帯域幅の合計をオンライン IP アドレス間で動的かつ均等に割り当てるには、このオプションを選択します。
Per-IP uplink maximum bandwidth	IP 単位のアップリンク最大帯域幅を設定します。
Per-IP downlink maximum bandwidth	IP 単位のダウンリンク最大帯域幅を設定します。
Per-user uplink maximum bandwidth	ユーザー単位のアップリンク最大帯域幅を設定します。
Per-user downlink maximum bandwidth	ユーザー単位のダウンリンク最大帯域幅を設定します。
Enable bandwidth check	送信元 IP アドレスごとにトラフィックによって消費される帯域幅の量をリアルタイムで検出するようにデバイスをイネーブルにします。
Static threshold-Maximum	最大静的しきい値を設定します。

Static threshold-Minimum	最小静的しきい値を設定します。
Enable dynamic threshold learning	デバイスが帯域幅しきい値を動的に学習できるようにします。
Learning duration	学習時間を設定します。
Learning tolerance-Maximum	最大帯域幅許容値を設定します。 デバイスは、学習した帯域幅しきい値に最大帯域幅許容値を乗算して、最大帯域幅しきい値を導出します。
Learning tolerance-Minimum	最小帯域幅許容値を設定します。 デバイスは、学習した帯域幅しきい値に最小帯域幅許容値を乗算して、最小帯域幅しきい値を導出します。
Total connection count	合計接続数を設定します。
Per-IP/Per-user connection count	IP 単位/ユーザー単位の接続数を設定します。
Total connection rate	合計接続レートを設定します。
Per-IP/Per-user connection rate	IP 単位/ユーザー単位の接続レートを設定します。
Monthly traffic quota	IP 単位の月間トラフィッククォータを設定します。
Mark DSCP priority	パケットにマークされる DSCP プライオリティを設定します。
TCP MSS	TCP MSS を設定します。

4. **OK** をクリックします。**Traffic Profile** ページに新しいトラフィックプロファイルが表示されます。

Configure a traffic policy

1. **Policies** > **Bandwidth Management** > **Traffic Policies** を選択します。
2. **Traffic Policy** ページで **Create** をクリックします。
3. トラフィックポリシーを作成します。

表 3 トラフィックポリシーの構成項目

項目	説明
Name	トラフィックポリシーの名前を入力します。

Parent policy	親ポリシーを指定します。
Source security zone	送信元セキュリティーゾーンを一致基準として指定します。
Destination security zone	宛先セキュリティーゾーンを一致基準として指定します。
Source IP address	送信元 IP アドレスオブジェクトグループを一致基準として指定します。
Destination IP address	一致基準として宛先 IP アドレスオブジェクトグループを指定します。
User	アイデンティティユーザーまたはユーザーグループを一致基準として指定します。
Application	アプリケーションまたはアプリケーショングループを一致基準として指定します。
Service	一致基準としてサービスオブジェクトグループを指定します。
Time range	ポリシーが有効な時間範囲を指定します。
DSCP priority	一致基準として DSCP プライオリティを指定します。
IPv6 flow label	一致基準として IPv6 フローラベルを指定します。
IPv6 extension header	IPv6 拡張ヘッダーを一致基準として指定します。
Terminal	端末または端末グループを一致基準として指定します。
Action	ポリシーのアクションを指定します。 • **Rate limit**: トラフィックプロファイルを参照することによって、一致するパケットのレートを制限します。 • **Not rate limit**: 一致するパケットのレートを制限しません。 • **Block**: 一致するパケットをブロックします。
Traffic profile	トラフィックプロファイルを指定します。

4. **OK** をクリックします。新しいトラフィックポリシーが **Traffic Policy** ページに表示されます。

5. レイヤー3 プロトコルおよび上位層プロトコルのトラフィックに対して帯域幅管理を実行するには、ページの右上隅で **All-OSI-layer protocol flow control** をイネーブルにします。デフォルトでは、帯域幅管理はレイヤー4 プロトコルおよび上位層プロトコルのトラフィックに対して実行されます。

Configure interface bandwidth

1. **Policies** > **Bandwidth Management** > **Interface Bandwidth** を選択します。
2. **Interface Bandwidth List** ページで **Create** をクリックします。
3. インターフェースの帯域幅エントリを作成します。

表 4 インターフェースの帯域幅設定項目

項目	説明
Interface name	インターフェースを選択します。
Expected bandwidth	予想される帯域幅値を指定します。

4. **OK** をクリックします。新しいインターフェース帯域幅エントリが **Interface Bandwidth List** ページに表示されます。

Load balancing common configuration

このヘルプには、次のトピックがあります。

Configure common settings
Configure a link
Configure a sticky group
Configure an SNAT address pool
Configure proximity
Configure ISP information
Configure a region
Advanced configuration

Configure common settings

Configure a link

リンクは、ISP によって提供される物理リンクです。リンクは、アウトバウンドリンクロードバランシング、インバウンドリンクロードバランシング、および透過的な DNS プロキシで使用できます。

手順

Policies > **Load Balancing** > **Common Configuration** > **Links** を選択します。
Link ページで **Create** をクリックします。
リンクを作成します。

表 1 リンク構成項目

項目	説明
Link name	リンク名を入力します。大文字と小文字は区別されません。
Next hop config method	ネクストホップの設定方法を選択します。 Manual Automatic
Next hop IPv4 address	発信ネクストホップ IPv4 アドレスを指定します。 IPv4 アドレスには、デバイス上のインターフェースの IPv4 アドレス、ループバックアドレス、マルチキャストアドレス、ブロードキャストアドレス、または 0.X.X.X の形式のアドレスは使用できません。

Next hop IPv6 address	発信ネクストホップ IPv6 アドレスを指定します。 IPv6 アドレスは、デバイス上の任意のインターフェースの IPv6 アドレス、ループバックアドレス、マルチキャストアドレス、リンクローカルアドレス、またはすべて 0 のアドレスにはできません。
Outgoing interface	リンクの発信インターフェースを指定します。発信インターフェースは、IP アドレスを動的に取得できるインターフェースである必要があります。
Link cost for proximity calculation	近接計算のリンクコストを指定します。
Link feature	リンク機能を有効または無効にします。
VRF	リンクが属する VPN インスタンスを指定します。
VRF inheritance	VRF 継承をイネーブルまたはディセーブルにします。VRF 継承がイネーブルの場合、VPN インスタンスが指定されていないリンクは、仮想サーバーの VPN インスタンスを継承します。VRF 継承がディセーブルの場合、VPN インスタンスが指定されていないリンクは、パブリックネットワークに属します。
Description	リンクの説明を入力します。

表 2 高度なリンク構成項目

項目	説明
Weight	リンクの重みを指定します。加重ラウンドロビンおよび加重最小接続アルゴリズムでは、値が大きいほど、参照される優先度が高くなります。
Priority	リンクグループ内のリンクのプライオリティを指定します。 最高の優先順位を持つリンクの数が最小数よりも少ない場合は、最小数を満たすか、使用可能なリンクがなくなるまで、優先順位の低いリンクが選択されます。 最大数と最小数は、**Policies** > **Load Balancing** > **Link Load Balancing** > **Outbound Link Load Balancing** > **Link Group** から設定できます。
Link group	既存のリンクグループを選択するか、リンクグループを作成します。
Probe method	リンクの状態および可用性の検出に使用するプローブテンプレートを指定します。このパラメーターは、**Link Group** ページでリンクグループに対して構成することもできます。リンクに対して構成されたプローブテンプレートは、リンクグループに対して構成されたプローブテンプレートよりも優先度が高くなります。

	既存のプローブテンプレートを選択することも、プローブテンプレートを作成することもできます。
Success criteria	リンクのヘルスモニタリング成功基準を指定します。 **All probes succeed**: ヘルスモニタリングは、指定されたすべてのヘルスモニタリング方式が成功した場合にのみ成功します。 **At least n probes succeed**: ヘルスモニタリングは、指定された数以上のヘルスモニタリング方式が成功した場合に成功します。指定された数のヘルスモニタリング方式がデバイス上のヘルスモニタリング方式の数よりも多い場合は、すべてのヘルスモニタリング方式が成功した場合にヘルスモニタリングが成功します。
Total bandwidth-Bandwidth ratio	帯域幅比を指定します。帯域幅比は、合計最大帯域幅に対する現在の帯域幅の割合です。トラフィックが最大予測帯域幅にリンクの帯域幅比を乗算した値を超えた場合、新しいトラフィック(スティッキエントリと一致しないトラフィック)はリンクに配信されません。 このパラメーターを設定しない場合は、設定可能な最大値が適用されます。
Total bandwidth-Bandwidth recovery ratio	帯域幅回復率を指定します。トラフィックが最大予測帯域幅にリンクの帯域幅回復率を乗算した値を下回ると、リンクは再びスケジューリングに参加します。 リンクの帯域幅回復率は、リンクの帯域幅率以下である必要があります。
Inbound bandwidth-Bandwidth ratio	インバウンド帯域幅比率を指定します。インバウンド帯域幅比率は、最大インバウンド帯域幅に対する現在のインバウンド帯域幅の割合です。トラフィックが最大予測帯域幅にリンクの帯域幅比率を乗算した値を超えると、新しいトラフィック(スティッキエントリと一致しないトラフィック)はリンクに配信されません。 このパラメーターを設定しない場合は、設定可能な最大値が適用されます。
Inbound bandwidth-Bandwidth recovery ratio	インバウンド帯域幅回復率を指定します。トラフィックが最大予測帯域幅にリンクの帯域幅回復率を乗算した値を下回ると、リンクは再びスケジューリングに参加します。 リンクの帯域幅回復率は、リンクの帯域幅率以下である必要があります。
Outbound bandwidth-Bandwidth ratio	アウトバウンド帯域幅比率を指定します。インバウンド帯域幅比率は、最大インバウンド帯域幅に対する現在のインバウンド帯域幅の割合です。トラフィックが最大予測帯域幅にリンクの帯域幅比率を乗算した値を超えると、新しいトラフィック(スティッキエントリと一致しないトラフィック)はリンクに配信されません。 このパラメーターを設定しない場合は、設定可能な最大値が適用されます。
Outbound bandwidth-Bandwidth recovery ratio	アウトバウンド帯域幅回復率を指定します。トラフィックが最大予測帯域幅にリンクの帯域幅回復率を乗算した値を下回ると、リンクは再びスケジューリングに参加します。 リンクの帯域幅回復率は、リンクの帯域幅率以下である必要があります。

Maximum bandwidth-Expected bandwidth	予想される合計最大帯域幅を指定します。値 0 は、予想される合計最大帯域幅が制限されないことを意味します。予想される合計最大帯域幅は、リンク保護に使用されるだけでなく、帯域幅アルゴリズム、最大帯域幅アルゴリズム、および動的近接アルゴリズムでの残りの帯域幅の計算にも使用されます。
Maximum bandwidth-Expected inbound bandwidth	インバウンド最大予測帯域幅を指定します。値 0 は、インバウンド最大予測帯域幅が制限されないことを意味します。インバウンド最大予測帯域幅は、リンク保護に使用されるだけでなく、帯域幅アルゴリズム、最大帯域幅アルゴリズムおよび動的近接アルゴリズムでの残りの帯域幅計算にも使用されます。
Maximum bandwidth-Expected outbound bandwidth	アウトバウンド最大予測帯域幅を指定します。値 0 は、アウトバウンド最大予測帯域幅が制限されないことを意味します。アウトバウンド最大予測帯域幅は、リンク保護に使用されるだけでなく、帯域幅アルゴリズム、最大帯域幅アルゴリズム、および動的近接アルゴリズムでの残りの帯域幅計算にも使用されます。
QoS-Connections	リンクで許可される最大接続数を指定します。値 0 は、リンクで許可される接続数が制限されないことを意味します。
QoS-Connections per second	リンクで許可される 1 秒当たりの最大接続数を指定します。値 0 は、リンクで許可される 1 秒当たりの接続数が制限されないことを意味します。
QoS-Bandwidth	リンクで許可される最大帯域幅の合計を指定します。値 0 は、リンクで許可される合計帯域幅が制限されないことを意味します。
QoS-Inbound bandwidth	リンクで許容されるインバウンド最大帯域幅を指定します。値 0 は、リンクで許容されるインバウンド帯域幅が制限されないことを意味します。
QoS-Outbound bandwidth	リンクで許可されるアウトバウンド最大帯域幅を指定します。値 0 は、リンクで許可されるアウトバウンド帯域幅が制限されないことを意味します。

OK をクリックします。**Link** ページに新しいリンクが表示されます。

Configure a sticky group

スティッキグループは、スティッキ方式を使用して、スティッキエントリに従って同じ実サーバーまたはリンクに類似したセッションを配信します。スティッキ方式は、セッションの最初のパケットに適用されます。セッションの他のパケットは、同じ実サーバーまたはリンクに配信されます。

手順

Policies > **Load Balancing** > **Common Configuration** > **Sticky Groups** を選択します。
Sticky Group ページで **Create** をクリックします。
スティッキグループを作成します。

表 3 スティッキグループの設定項目

項目	説明
Stick group name	スティッキグループの名前を入力します。大文字と小文字は区別されません。
Type	グループタイプを選択します。 Address and port Payload HTTP-Content HTTP-Cookie HTTP-Header SSL RADIUS SIP HTTP-Passive UDP-Passive TCP-Payload
Aging	スティッキエントリを期限切れにするかどうかを **Yes** または **No** で指定します。
Aging time	スティッキエントリのタイムアウト時間を指定します。HTTP cookie タイプのスティッキグループには、次の規則が適用されます。 スティッキ方式が cookie 挿入または cookie 書き換えの場合、タイムアウトタイマー0 はセッションの持続性を示します。 スティッキ方式が cookie get の場合、タイムアウトタイマー0 は、スティッキエントリのタイムアウト時間が 0 秒であることを示します。
Override limits	スティッキエントリと一致するセッションの制限を無視する機能をイネーブルまたはディセーブルにします。この機能をイネーブルにすると、デバイスはスティッキエントリと一致するセッションの次の制限を無視します。 実サーバーまたはリンクの帯域幅および接続パラメーター。 仮想サーバー上の LB 接続制限ポリシー。
Stickiness-over-busyness	スティッキオーバービジー機能をイネーブルまたはディセーブルにします。この機能を使用すると、実サーバーがビジー状態かどうかに関係なく、デバイスはスティッキエントリに基づいてクライアント要求を実サーバーに割り当てることができます。この機能をディセーブルにすると、デバイスはクライアント要求を通常状態の実サーバーだけに割り当てます。
Match Across Virtual Servers	仮想サーバー間でのスティッキエントリの照合をイネーブルまたはディセーブルにします。この機能をイネーブルにすると、仮想サーバー上のスティッキエ

	ントリと一致しないトラフィックは、別の仮想サーバー上のスティッキエントリと照合されます。 このパラメーターは、アドレスおよびポートと RADIUS スティッキ方式だけでサポートされます。
Match Across Services	サービス間でのスティッキエントリの照合をイネーブルまたはディセーブルにします。この機能をイネーブルにすると、仮想サーバー上のスティッキエントリと一致しないトラフィックは、同じ IP アドレスを持つ別の仮想サーバー上のスティッキエントリと照合されます。 このパラメーターは、アドレスおよびポートと RADIUS スティッキ方式だけでサポートされます。
Description	スティッキグループの説明を入力します。

表 4 アドレスおよびポートスティッキ方式の設定項目

項目	説明
IPv4(IPv4	IPv4 アドレス/ポートスティッキ方式を選択します。 送信元アドレス 送信元アドレス/ポート 宛先アドレス 宛先アドレス/ポート 送信元アドレス/宛先アドレス 送信元/宛先アドレス/ポート
IPv6(IPv6	IPv6 アドレス/ポートスティッキ方式を選択します。 送信元アドレス 送信元アドレス/ポート 宛先アドレス 宛先アドレス/ポート 送信元アドレス/宛先アドレス 送信元/宛先アドレス/ポート

表 5 ペイロードスティッキ方式の設定項目

項目	説明
Offset	HTTP パケットの開始に基づいて、HTTP ペイロードのオフセット値を指定します。
Start string	HTTP ペイロードの開始を示す正規表現を指定します。文字列に疑問符(?)を含めることはできません。

Length/End string	HTTP ペイロードの長さと終了文字列を指定します。 **Length**: HTTP ペイロードの長さを指定します。値 0 は任意の長さを示します。 **End string**: HTTP ペイロードの終了を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。

表 6 HTTP エンティティスティッキ方式の設定項目

項目	説明
Offset	HTTP パケットの開始に基づいて、エンティティのオフセット値を指定します。
Start string	エンティティの開始を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。
Length/End string	HTTP エンティティの長さと終了文字列を指定します。 **Length**: HTTP エンティティの長さを指定します。値 0 は任意の長さを示します。 **End string**: HTTP エンティティの終了を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。

表 7 HTTP cookie スティッキ方式の設定項目

項目	説明
Cookie stickiness	Cookie のスティッキ方式を選択します。 **Cookie insert**: サーバーから送信される HTTP 応答パケットに **Set-Cookie** フィールドを挿入します。 **Cookie rewrite**: サーバーから送信された HTTP 応答パケットの **Set-Cookie** フィールドを書き換えます。 **Cookie get**: サーバーから送信された HTTP 応答パケットの **Set-Cookie** フィールドを取得します。
Cookie name	HTTP Cookie を名前で指定します。大文字と小文字は区別されます。
Cookie domain name	Cookie の送信先となるホストを示すドメイン名を指定します。このオプションを指定しないと、Cookie は作成されたホストにのみ送信されます。 クライアントが hosts **example.com**、**www.example.com** および **www.corp.example.com** にアクセスできるとします。**example.com** を指定すると、クライアントは 3 つのホストのいずれかに HTTP リクエストを送信するときに Cookie を含めます。**www.corp.example.com** を指定すると、クライアントは **www.corp.example.com** に HTTP リクエストを送信するときにのみ Cookie を含めます。 このパラメーターは、cookie 挿入スティッキ方式でのみサポートされます。

Cookie path	Cookie を送信するパスを指定します。パスを指定しない場合、Cookie は指定したドメイン名のすべてのパス(ルートディレクトリ/applys)に送信されます。 このパラメーターは、Cookie の範囲を指定されたパスに制限します。クライアントが **www.example.com/a** および **www.example.com/b** フォルダにアクセスできるとします。ドメイン名 **www.example.com** および path**/a** を指定すると、クライアントは www.example.com/a に HTTP 要求を送信するときにのみ Cookie を含めます。 このパラメーターは、cookie 挿入スティッキ方式でのみサポートされます。
HTTPOnly	このオプションを有効にすると、スクリプトから Cookie にアクセスできなくなります。このオプションを無効にした場合、スクリプトから Cookie にアクセスできます。 このオプションは、攻撃者がスクリプトを使用して cookie 情報を取得することを防止します。 このオプションは、cookie insert および cookie rewrite sticky メソッドでのみサポートされます。
Secure	このオプションを有効にすると、を送信するには、このオプションを有効にします。このオプションを無効にすると、Cookie は任意の接続で送信できます。 このオプションは、cookie insert および cookie rewrite sticky メソッドでのみサポートされます。
Check all packets	すべてのパケットのチェックを有効または無効にします。 スティッキ方式が cookie get の場合は、このパラメーターを使用してすべての HTTP 応答パケットから cookie を取得します。このパラメーターが設定されていない場合、デバイスは接続の最初の応答パケットから Set-Cookie のみを取得します。 スティッキ方式が cookie rewrite の場合は、このパラメーターを使用してすべての HTTP 応答パケットの cookie を書き換えます。このパラメーターが設定されていない場合、デバイスは接続の最初の応答パケットの Set-Cookie だけを書き換えます。 スティッキ方式が cookie 挿入の場合は、このパラメーターを使用してすべての HTTP 応答パケットに cookie を挿入します。このパラメーターが設定されていない場合、デバイスは接続の最初の応答パケットに Set-Cookie だけを挿入します。
Secondary cookie	セカンダリ Cookie の名前を指定します。大文字と小文字が区別されます。名前には、大カッコ({}、()、[]、<>)、アットマーク(@)、カンマ(,)、セミコロン(;)、コロン(:)、バックスラッシュ(¥)、引用符(")、スラッシュ(/)、疑問符(?) 、等号 (=) 、スペース文字 (SP)、水平タブ (HT)は使用できません。また、文字列には、31 以下および 127 以上の ASCII コードは含まれません。このパラメーターをサポートしているのは、cookie の get sticky メソッドのみです。 デバイスは、HTTP 要求パケットヘッダー内の指定された cookie を検出できなかった場合に、URI 内のセカンダリ cookie を検出します。
Offset	HTTP パケットの開始に基づく Cookie のオフセット値を指定します。このパラメーターをサポートしているのは、cookie の get sticky メソッドのみです。

Start string	Cookie の開始を示す正規表現を指定します。文字列には疑問符(?) を含めることはできません。このパラメーターをサポートしているのは、cookie の get sticky メソッドのみです。
Length/End string	cookie の長さおよび終了ストリングを指定します。 **Length**: Cookie の長さを指定します。値 0 は任意の長さを示します。 **End string**: HTTP Cookie の終了を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。 このパラメーターをサポートしているのは、cookie get sticky メソッドだけです。

表 8 HTTP ヘッダースティッキ方式の設定項目

項目	説明
Header stickiness	ヘッダーのスティッキ方式を選択します。 **URL**: HTTP URL ベースのスティッキ方式。 **Host**: HTTP ホストベースのスティッキ方式。 **Method** : HTTP Request:スティッキ方式に基づく方式。 **Version**: HTTP バージョンベースのスティッキ方式。 **Name**: HTTP ヘッダー名ベースのスティッキ方式。
Header name	HTTP ヘッダー名を指定します。このパラメーターは、HTTP ヘッダー名ベースのスティッキ方式を選択した場合にのみ表示されます。
Offset	HTTP パケットの開始に基づいて、HTTP ヘッダーのオフセット値を指定します。
Start string	HTTP ヘッダーの開始を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。
Length/End string	HTTP ヘッダーの長さと終了文字列を指定します。 **Length**: HTTP ヘッダーの長さを指定します。値 0 は任意の長さを示します。 **End string**: HTTP ヘッダーの終了を示す正規表現を指定します。文字列には疑問符(?) を含めることはできません。

表 9 SSL スティッキ方式の設定項目

項目	説明
SSL stickiness	SSL セッション ID に基づいて SSL スティッキ方式を指定します。このスティッキ方式は HTTPS 要求パケットにのみ適用され、仮想サーバーの SSL サーバーポリシーを指定する必要があります。

表 10 RADIUS スティッキ方式の設定項目

項目	説明

RADIUS attribute	RADIUS アトリビュートスティッキ方式を指定します。このスティッキ方式は、RADIUS パケットだけに適用されます。値 1 は User-Name アトリビュートを示します。値 8 は Framed-IP-Address アトリビュートを示します。

表 11 SIP スティッキ方式の設定項目

項目	説明
SIP stickiness	SIP メッセージのヘッダー内のコール ID に基づいて SIP スティッキ方式を指定します。同じコール ID を持つすべての SIP メッセージは、同じ実サーバーに割り当てられます。

表 12 HTTP-passive スティッキ方式の設定項目

項目	説明
Check all packets	すべてのパケットのチェックを有効または無効にします。 このパラメーターは、すべての HTTP 応答パケットからスティッキエントリを生成するかどうかを決定します。このパラメーターが設定されていない場合、デバイスは接続の最初の応答パケットからのみスティッキエントリを生成します。
Request configuration	HTTP パッシブスティッキエントリを照合するために、デバイスが HTTP 要求から指定された文字列を取得できるようにします。 HTTP パッシブスティッキ方式では、スティッキエントリを生成するために要求と応答の両方の設定が必要です。HTTP パッシブスティッキ方式が設定されている場合、デバイスは応答設定に基づいて HTTP 応答内の指定された文字列を取得し、スティッキエントリを生成します。後続のすべての HTTP 要求では、デバイスは要求設定に基づいて指定された文字列を取得します。文字列がスティッキエントリと一致する場合、デバイスはスティッキエントリに従って HTTP 要求を転送します。 要求および応答を設定する場合は、次の注意事項に従ってください。 HTTP-passive スティッキグループを使用すると、デバイスは HTTP 応答パケットから最大 4 つの取得し、HTTP 要求パケットから最大 4 つのストリングを取得できます。 デバイスが HTTP レスポンスパケットから n 個の文字列を取得するとします。これらの文字列は、レスポンス構成でメソッド ID を組み合せることにより、さらに 2n-1 個の文字列を生成できます。2n-1 個の文字列のいずれかを使用して、リクエスト構成を使用して取得した文字列と一致させることができます。 デバイスが HTTP 要求パケットから n 個の文字列を取得したとします。これらの文字列は、メソッド ID の構成順に従って 1 つの文字列として結合されます。 次の例を使用して、HTTP 要求および応答パケットに基づいてスティッキエントリを生成する方法を示します。

	応答設定でメソッド ID 1、2、および 3 を設定します。デバイスが設定に基づいて文字列 a、b、および c を取得した場合、文字列はさらに 7 つの文字列 a、b、c、ab、ac、bc、および abc を生成できます。 要求設定でメソッド ID 2、3、および 4 を設定します。 HTTP 要求を受信した後、次の条件が満たされると、デバイスはスティッキエントリを生成します。 デバイスは、要求の設定に基づいて文字列 a、b、および c を取得します。 結合文字列 abc は、応答設定に基づいて取得された文字列と一致します。 文字列 abc に基づいて生成されたスティッキエントリと一致する後続の HTTP 要求については、デバイスはスティッキエントリに従って要求を転送します。 要求を構成する手順は、次のとおりです。 **Create** をクリックして、HTTP パッシブスティッキ方式を作成します。 **ID**:方式 ID を入力します。 **Search position** : HTTP リクエストから文字列を取得する位置を選択します。オプションは **Header** および **Content** です。 **Header type**: HTTP リクエストから取得する文字列のタイプを指定します。オプションは **Name** および **URL** です。このパラメーターは、**Search position** が **Header** に設定されている場合にのみ使用できます。 **Header name**: HTTP ヘッダー名を入力します。大文字と小文字は区別されません。このパラメーターは、**Header type** が **Name** に設定されている場合にのみ使用できます。 **Start string**: HTTP ヘッダー、URL、または HTTP エンティティの開始を示す正規表現を指定します。 **Length/End string**: HTTP ヘッダー、URL、または HTTP エンティティの長さと終了文字列を指定します。 **OK** をクリックします。HTTP-passive スティッキ方式が要求設定リストに表示されます。
Response configuration	HTTP パッシブスティッキエントリを生成するために、デバイスが HTTP 応答から指定された文字列を取得できるようにします。 HTTP パッシブスティッキ方式では、スティッキエントリを生成するために要求と応答の両方の設定が必要です。 応答を設定するには、次の手順を実行します **Create** をクリックして、HTTP パッシブスティッキ方式を作成します。 **ID**: 方式 ID を入力します。 **Search position** : HTTP レスポンスから文字列を取得する位置を選択します。オプションは **Header** および **Content** です。

	Header type: HTTP レスポンスから取得する文字列のタイプを指定します。このパラメーターは、**Search position** が **Header** に設定されている場合にのみ使用できます。 **Header name**: HTTP ヘッダー名を入力します。大文字と小文字は区別されません。このパラメーターは、**Header type** が **Name** に設定されている場合にのみ使用できます。 **Start string**: HTTP ヘッダーまたは HTTP エンティティの開始を示す正規表現を指定します。 **Length/End string**:　HTTP ヘッダーまたは HTTP エンティティの長さと終了文字列を指定します。**Length** には、HTTP ヘッダーまたは HTTP エンティティの長さを指定します。値 0 は任意の長さを示します。**End string** には、HTTP ヘッダーまたは HTTP エンティティの終了を示す正規表現を指定します。文字列に疑問符(?)を含めることはできません。 **OK** をクリックします。HTTP-passive スティッキ方式が応答設定リストに表示されます。

表 13 UDP-passive スティッキ方式の設定項目

項目	説明
Request configuration	UDP-passive スティッキエントリを照合するために、デバイスが UDP 要求から指定された文字列を取得できるようにします。 UDP-passive スティッキ方式では、スティッキエントリを生成するために要求と応答の両方の設定が必要です。 デバイスは UDP 要求を受信すると、要求設定に基づいて指定されたペイロードを取得します。ペイロードが、応答設定を使用して取得された UDP 応答ペイロードと一致する場合、デバイスは応答内のペイロードに基づいてスティッキエントリを生成します。後続の UDP 要求パケットがスティッキエントリと一致する場合、デバイスはスティッキエントリに従ってパケットを転送します。 **UDP-Passive sticky method** を選択して、次のパラメーターを設定します。 **Offset**: UDP 要求パケットの開始に基づいて、UDP ペイロードのオフセット値を指定します。 **Start string**: UDP ペイロードの開始を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。 **Length/End string**: UDP ペイロードの長さと終了文字列を指定します。**Length** は UDP ペイロードの長さを指定します。値 0 は任意の長さを示します。**End string** は UDP ペイロードの終了を示す正規表現を指定します。文字列には疑問符(?) を含めることはできません。

Response configuration	UDP パッシブスティッキエントリを生成するために、デバイスが UDP 応答から指定された文字列を取得できるようにします。 UDP-passive スティッキ方式では、スティッキエントリを生成するために要求と応答の両方の設定が必要です。 **UDP-Passive sticky method** を選択して、次のパラメーターを設定します。 **Offset**: UDP 応答パケットの開始に基づいて、UDP ペイロードのオフセット値を指定します。 **Start string**: UDP ペイロードの開始を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。 **Length/End string**: UDP ペイロードの長さと終了文字列を指定します。**Length** は UDP ペイロードの長さを指定します。値 0 は任意の長さを示します。**End string** は UDP ペイロードの終了を示す正規表現を指定します。文字列には疑問符(?) を含めることはできません。

表 14 TCP-payload スティッキ方式の設定項目

項目	説明
Offset	TCP パケットの開始に基づいて、TCP ペイロードのオフセット値を指定します。
Start string	TCP ペイロードの開始を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。
Length/End string	TCP ペイロードの長さと終了文字列を指定します。 **Length**: TCP ペイロードの長さを指定します。値 0 は任意の長さを示します。 **End string**: TCP ペイロードの終了を示す正規表現を指定します。文字列に疑問符(?) を含めることはできません。

OK をクリックします。新しいスティッキグループが **Sticky Group** ページに表示されます。

Configure an SNAT address pool

サーバーファームまたはリンクグループが SNAT アドレスプールを参照すると、LB デバイスは受信したパケットの送信元アドレスを SNAT アドレスに置き換えてから、パケットを転送します。

手順

Policies > **Load Balancing** > **Common Configuration** > **SNAT Address Pools** を選択します。
SNAT Address Pool ページで **Create** をクリックします。
SNAT アドレスプールを作成します。

表 15 SNAT アドレスプールの構成項目

項目	説明
SNAT pool name	SNAT アドレスプールの名前を入力します。大文字と小文字は区別されません。
VRF	SNAT アドレスプールが属する VPN インスタンスを指定します。 2 つのアドレスプールに重複するアドレスが含まれている場合は、アドレスプールごとに VPN インスタンスを指定して、デバイスでの設定の競合を回避します。 SNAT アドレスプールに基づくトラフィック転送の場合、ベストプラクティスとして、関連付けられた実サーバーの VPN インスタンスを SNAT アドレスプールの VPN インスタンスとして指定します。
Address range list	アドレス範囲を追加するには: **Add** をクリックします。 **Start IP address**: 開始 IP アドレスを入力します。 **End IP address**: 終了 IP アドレスを入力します。開始 IP アドレスより小さい値は指定できません。 **OK** をクリックします。新しいアドレス範囲がアドレス範囲リストに表示されます。
Interfaces for sending gratuitous ARP/ND packets	余計な ARP パケットおよび ND パケットを送信するためのインターフェースを指定します。 サーバーに接続されているインターフェースの IP アドレスが SNAT アドレスプールと同じネットワークセグメント内にある場合は、そのインターフェースを gratuitous ARP/ND パケットを送信するインターフェースとして指定する必要があります。
Description	SNAT アドレスプールの説明を入力します。

OK をクリックします。新しい SNAT アドレスプールが **SNAT Address Pool SNAT Address Pool** ページに表示されます。

Configure proximity

近接機能は、宛先への最適なリンクを選択するためにリンク検出を実行します。宛先の近接情報が使用できない場合、ロードバランシングモジュールはスケジューリングアルゴリズムに基づいてリンクを選択します。次に、近接検出を実行して、後続のトラフィックを転送するための近接エントリを生成します。
近接機能を使用するには、近接プローブテンプレートと近接パラメーターを設定してから、リンクグループ内で近接機能をイネーブルにします。

手順

Policies > **Load Balancing** > **Common Configuration** > **Proximity** を選択します。
Proximity Parameter ページで **Create** をクリックします。
近接パラメーターを作成します。

表 16 近接パラメーターの構成項目

項目	説明
VRF	近接エントリが属する VPN インスタンスを指定します。 既存の VPN インスタンスを選択することも、VPN インスタンスを作成することもできます。
Default probe method	デフォルトのプローブ方式を指定します。 既存のプローブ方式を選択することも、プローブ方式を作成することもできます。
Mask length	IPv4 近接エントリのマスク長を指定します。値 0 は自然マスクを示します。
Aging time	近接エントリのタイムアウトタイマーを設定します。
TTL weight	近接計算用の TTL の重みを設定します。値が大きいほど、重みが高くなります。
RTT weight	近接計算のネットワーク遅延の重みを設定します。値が大きいほど、重みが高くなります。
Cost weight	近接計算のコスト加重を設定します。値が大きいほどコスト加重が高くなります。
Bandwidth weight	近接計算の帯域幅の重みを設定します。 **Inbound**: 近接性計算のインバウンド帯域幅の重みを設定します。値が大きいほど、帯域幅の重みが高くなります。 **Outbound**: 近接性計算のアウトバウンド帯域幅の重みを設定します。値が大きいほど、帯域幅の重みが高くなります。
Max entries	近接エントリの最大数を設定します。値 0 は、近接エントリの最大数が制限されていないことを示します。
Packet loss ratio weight	近接計算のためのパケット損失率の重みを設定します。 このパラメーターは、複合リンクコストを計算する際のパケット損失率の重みを指定します。これは、近接機能をイネーブルにするか、リンク品質アルゴリズムを設定する場合にだけ適用されます。 近接機能とリンク品質アルゴリズムの設定は相互に排他的です。

OK をクリックします。新しい近接パラメーターが **Proximity Parameter** ページに表示されます。
Proximity Probe Template ページで **Create** をクリックします。

近接プローブテンプレートを作成します。

表 17 近接プローブテンプレートの構成項目

項目	説明
Probe template name	プローブテンプレート名の名前を入力します。大文字と小文字は区別されません。
Probe interval	プローブ間隔を設定します。
Timeout time	プローブ応答のタイムアウト時間を設定します。

OK をクリックします。新しい近接プローブテンプレートが **Proximity Probe Template** ページに表示されます。

Configure ISP information

ICANN によって割り当てられた IP アドレスを使用して、ISP の IP アドレスを設定します。パケットの宛先 IP アドレスが LB クラスの ISP 一致規則と一致する場合、LB デバイスはリンクグループ設定に基づいて、パケットを転送するリンクを選択します。
ISP 情報は、手動で構成することも、ISP ファイルをインポートすることも、自動更新することもできます。また、これらの方法を組み合わせて構成することもできます。
次の問題が検出された場合、インポートされた情報はそのまま保持されます。

The file does not exist。
The file name is invalid。
File decryption fails。

IP アドレスの解析に失敗したためにインポート操作が終了した場合、システムは次の操作を実行します。

最後にインポートされた情報をクリアします。
今回インポートした情報を保存します。

インポートされた ISP またはその IPv4 または IPv6 アドレスは削除できません。手動で構成された ISP 情報とインポートされた ISP 情報が重複している場合は、手動で構成された ISP 情報を削除できます。
複数の ISP ファイルを読み込む場合は、新しく読み込まれたファイルが以前に読み込まれたファイルを上書きします。

手順

Policies > **Load Balancing** > **Common Configuration** > **ISP** を選択します。

ISP ページで ISP ファイルをインポートします。

Select をクリックして、インポートするファイルを選択します。

Import をクリックします。インポートされたファイルが ISP リストに表示されます。

ISP 情報を手動で設定します。

Create をクリックします。

表 18 ISP の手動構成項目

項目	説明
ISP name	ISP の名前を入力します。大文字と小文字は区別されません。
Description	ISP の説明を入力します。
Whois maintainer object	ISP を識別する whois メンテナーオブジェクトを設定します。 whois メンテナーオブジェクトの名前を入力し、**Add** をクリックします。 **Object name**: whois maintainer オブジェクトの名前を 1～63 文字の文字列で入力します。1 つの ISP に対して最大 10 個の whois maintainer オブジェクトを設定できます。 **Source**: whois メンテナーオブジェクトを追加する方法。**Manually configured**, **Imported from file** と **Manually configured and Imported from file**.が可能です。
ISP list	**Create** をクリックして、ISP アドレスを構成します。 **Address type**: アドレスタイプ(IPv4 または IPv6)を選択します。 **IP address**: IPv4 アドレスとマスク長(1～32)または IPv6 アドレスとプレフィクス長(1～128)を入力します。 **OK** をクリックします。ISP アドレスが ISP リストに表示されます。 :**Source** : ISP アドレスを取得する方法。**Manually configured**, **Imported from file** と **Auto update** が可能です。

OK をクリックします。ISP リストに ISP 情報が表示されます。

Auto update ページで ISP 自動更新を設定します。

ISP 自動更新を有効にし、ISP 自動更新パラメーターを設定します。

表 19 構成アイテムの自動更新

項目	説明

ISP auto update	ISP の自動アップデートを有効または無効にします。
Whois server	デバイスが ISP 情報を照会する whois サーバーを指定します。whois サーバーは、ドメイン名または IP アドレスを指定することによって指定できます。 **Domain name**: whois サーバーのドメイン名を指定します。大文字と小文字は区別され、1～253 文字のドット区切り文字列です。ドメイン名の各ドット区切りラベルには、最大 63 文字を使用できます。ドメイン名には、文字、数字、ハイフン(-)、アンダースコア(_)、およびピリオド(.)を使用できます。 **IPv4 address**: whois サーバーの IPv4 アドレスを指定します。
ISP update frequency	ISP の自動更新の間隔を指定します。オプションには、**Per day**, **Per week**、および **Per month** があります。特定の更新時間は午前 4:02:00 です。
Last successfully updated	最後に正常に更新された時刻。
Last updated	最新の更新の時刻。
Updated ISPs	最新の更新内の ISP アドレスの数。
Update result	最新の更新の結果。値には、**Success**, **Connection error**, **Connection abort**, **DNS error** と **No update** があります。

Apply をクリックして、設定を保存して適用します。

Configure a region

リージョンには、さまざまな ISP に対応するネットワークセグメントが含まれます。

手順

Policies > **Load Balancing** > **Common Configuration** > **Regions** を選択します。
Region ページで **Create** をクリックします。
リージョンを作成します。

表 20 リージョン構成アイテム

項目	説明
Region name	リージョンの名前を入力します。大文字と小文字は区別されません。

ISP	ISP を追加します。 既存の ISP を選択するか、ISP を作成します。 **Add** をクリックします。追加した ISP がテキストボックスの下のボックスに表示されます。

OK をクリックします。**Region** ページに新規リージョンが表示されます。

Advanced configuration

DNS キャッシュエントリのエージングタイムを設定できます。DNS キャッシュエントリは、**Monitor** > **DNS Cache** から表示できます。

Server load balancing

このヘルプには、次のトピックがあります。

Introduction

サーバーロードバランシングは、複数のサーバーまたはファイアウォール間でサービスを分散するクラスタテクノロジーです。
サーバーロードバランシングは、レイヤー4 サーバーロードバランシングとレイヤー7 サーバーロードバランシングに分類されます。

Layer 4 server load balancing: ネットワーク層およびトランスポート層の情報を識別し、ストリームに基づいて実装されます。同じストリーム内のパケットを同じサーバーに配信します。レイヤー4 サーバーのロードバランシングでは、コンテンツに基づいてレイヤー7 サービスを配信できません。AFT 機能は、レイヤー4 サーバーのロードバランシングとだけ連携できます。

Layer 7 server load balancing: ネットワーク層、トランスポート層、およびアプリケーション層の情報を識別し、コンテンツに基づいて実装されます。パケットの内容を分析し、その内容に基づいてパケットを 1 つずつ配信し、事前定義されたポリシーに従って指定されたサーバーへの接続を配信します。レイヤー7 サーバーロードバランシングは、ロードバランシングサービスを広範囲に適用します。

サーバーロードバランシングは IPv4 および IPv6 をサポートしますが、レイヤー4 サーバーロードバランシングは IPv4-to-IPv6 または IPv6-to-IPv4 変換をサポートしません。

Deployment modes

サーバーロードバランシングでは、Network Address Translation(NAT)および間接展開モードが使用されます。

NAT-mode server load balancing

図 1 ネットワーク図

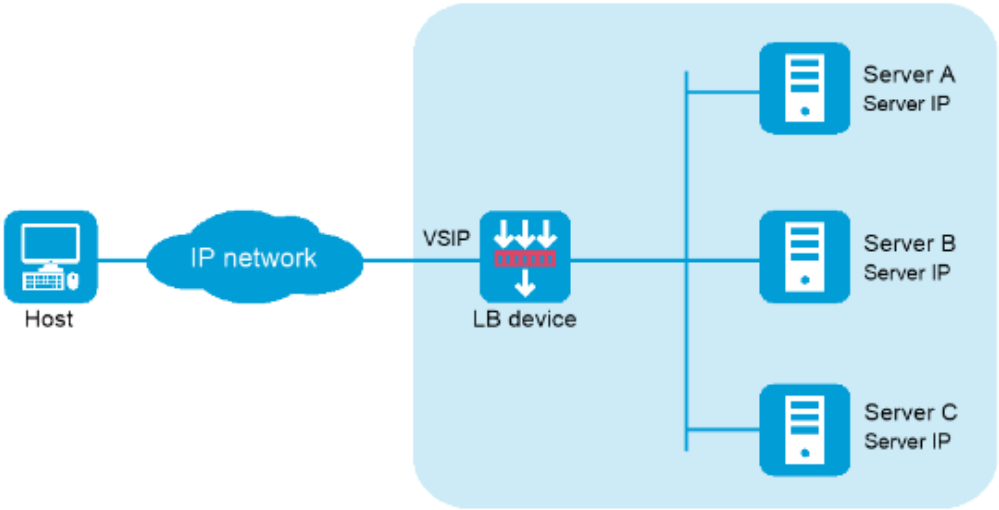


図 1 に示すように、NAT モードのサーバーロードバランシングには次の要素があります。

LB device: さまざまなサービス要求を複数のサーバーに配信します。
Server: さまざまなサービス要求に応答して処理します。
VSIP: クラスタの仮想サービス IP アドレス。ユーザーがサービスを要求するために使用されます。
Server IP: サーバーの IP アドレス。LB デバイスが要求の配信に使用します。

Indirect-mode server load balancing

図 2:ネットワーク図

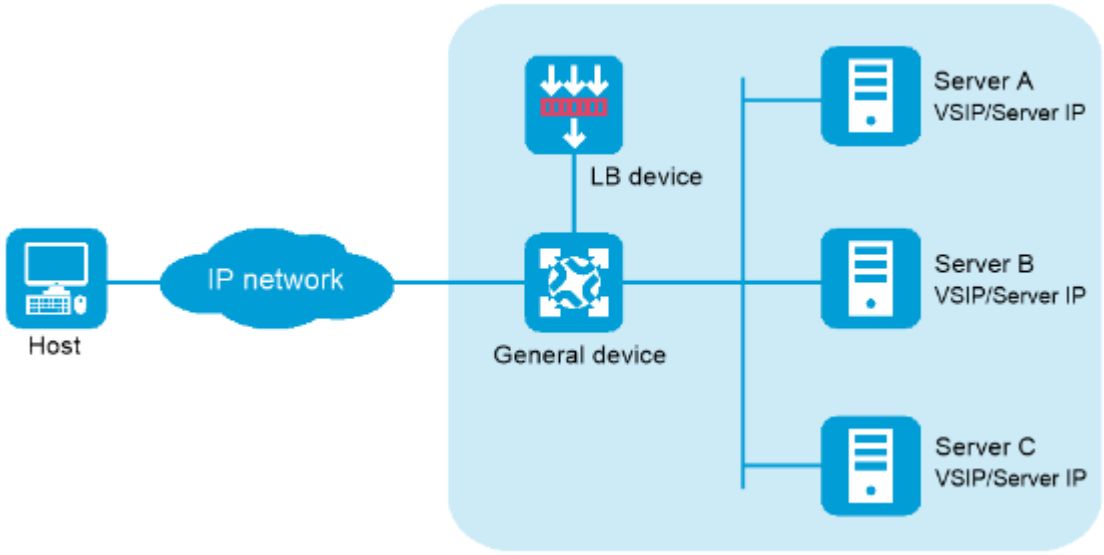


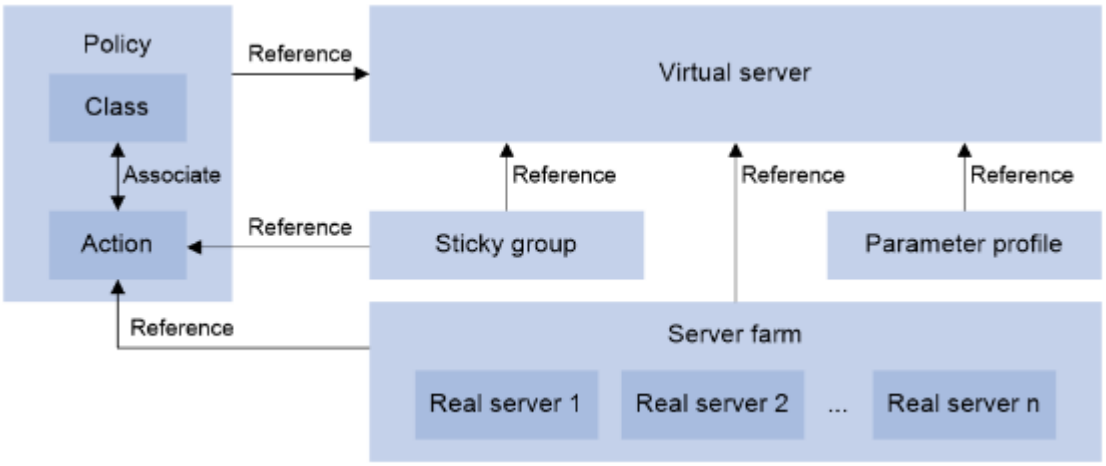
図 2 に示すように、間接モードのサーバー負荷分散には次の要素が含まれます。

LB device: さまざまなサービス要求を複数のサーバーに配信します。
General device: 一般的な転送ルールに従ってデータを転送します。
Server: さまざまなサービス要求に応答して処理します。
VSIP: クラスタの仮想サービス IP アドレス。ユーザーがサービスを要求するために使用されます。
Server IP: サーバーの IP アドレス。LB デバイスが要求の配信に使用します。

間接モードのサーバーロードバランシングでは、LB デバイスとサーバーの両方で VSIP を設定する必要があります。サーバー上の VSIP は ARP 要求および応答に含めることができないため、ループバックインターフェース上で VSIP を設定できます。

Relationship between the main configuration items

図 3 主要な構成項目間の関係



Restrictions and guidelines

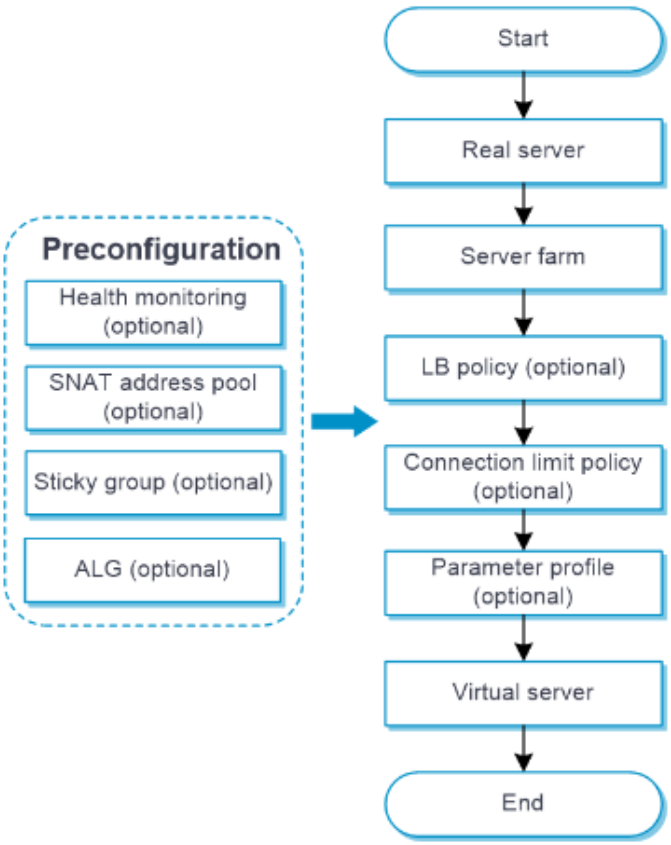
デバイスは、MySQL データベース 5.0、5.1、5.5、5.6、および 5.7 のみをサポートします。
デバイスは、MySQL データベースのネイティブパスワード認証プラグインのみをサポートします。
MySQL 仮想サーバーの読み取り/書き込みスプリットを有効にした後、読み取り/書き込みサーバーファーム間のデータ同期を確保する必要があります。
デバイスは、暗号スーツ **exp_rsa_des_cbc_sha**、**exp_rsa_rc2_md5**、**exp_rsa_rc4_md5**、または **rsa_des_cbc_sha** を使用する SSL サーバーポリシーをサポートしません。
サーバーロードバランシングの NAT 機能は、一般的な NAT 機能と一緒に使用することはできません。
複数のサーバーファームに同じ実サーバーを指定する場合は、すべてのサーバーファームに対して NAT をイネーブルまたはディセーブルにする必要があります。

Configure server load balancing

サーバーの負荷分散を構成する前に、ライセンスを正しくインストールしてください。詳細については、ライセンス管理のヘルプを参照してください。

図 4 に示すように、サーバーロードバランシングを構成します。

図 4 サーバーロードバランシングの設定手順



Configure health monitoring (optional)

ヘルスモニタリングプローブテンプレートは、実サーバーまたはサーバーファームで使用できます。
ヘルスモニタリングの設定の詳細については、ヘルスモニタリングのヘルプを参照してください。
ヘルスモニタリングの設定の詳細については、ロードバランシング共通設定のヘルプを参照してください。

Configure an SNAT address pool (optional)

SNAT アドレスプールは、サーバーファームで使用できます。
SNAT アドレスプールの設定の詳細については、ロードバランシングの共通設定に関するヘルプを参照してください。

Configure ALG (optional)

ALG の設定の詳細については、ロードバランシング共通設定のヘルプを参照してください。

Configure a server farm

同様のコンテンツを含む実サーバーをサーバーファームに追加して、管理を容易にすることができます。

サーバーファームは、仮想サーバーまたはアクションで使用できます。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Server Farms** を選択します。
Create をクリックします。
サーバーファームを作成します。

表 1 基本構成項目

項目	説明
Server farm name	サーバーファームの名前を入力します。大文字と小文字は区別されません。
Scheduling algorithm	サーバーファームのスケジューリングアルゴリズムを選択します。 **Round robin**: 実サーバーの重みに基づいて、ユーザー要求を実サーバーに割り当てます。重みが大きいほど、多くのユーザー要求が割り当てられます。 **Random**: ユーザー要求を実サーバーにランダムに割り当てます。 **Weighted least connections**: 常に、加重アクティブ接続数(アクティブ接続数を加重で除算した数)が最も少ない実サーバーにユーザー要求を割り当てます。このアルゴリズムで使用される加重は、**Create Real Server** ページで構成されます。 **Bandwidth**: 実サーバーの重みと残りの帯域幅に従って、ユーザー要求を実サーバーに配信します。 **Maximum bandwidth**: ユーザー要求を、最大の残り帯域幅を持つアイドル状態の実サーバーに常に配信します。 **Dynamic feedback**: 実サーバーのメモリー、CPU およびディスク使用量を使用して計算された負荷加重値に基づいて、新しい接続を実サーバーに割り当てます。負荷が少ないほど、加重値は大きくなります。加重値が大きい実サーバーには、より多くの接続が割り当てられます。 **Least time**: 実サーバーのレスポンス時間を使用して計算された負荷加重値に基づいて、新しい接続を実サーバーに割り当てます。レスポンス時間が短いほど、加重値は大きくなります。加重値が大きい実サーバーほど、より多くの接続が割り当てられます。 **Source IP address hash**: ユーザー要求の送信元 IP アドレスをハッシュし、ハッシュ値に従ってユーザー要求を異なる実サーバーに配布します。このアルゴリズムは、同じ送信元 IP アドレスを持つユーザー要求を同じ実サーバーに配布する必要がある場合に適用されます。

	Source IP address CARP hash: ユーザー要求の送信元 IP アドレスをハッシュし、CARP ハッシュ値に従ってユーザー要求を異なる実サーバーに配布します。このアルゴリズムは、同じ送信元 IP アドレスを持つユーザー要求を同じ実サーバーに配布する必要がある場合に適用されます。使用可能な実サーバーの数が変化すると、このアルゴリズムにより、すべての使用可能な実サーバーの負荷変化が最小になります。 **Source IP address and port number hash**: ユーザー要求の送信元 IP アドレスおよびポート番号をハッシュし、ハッシュ値に従ってユーザー要求を異なる実サーバーに配布します。このアルゴリズムは、同じ送信元 IP アドレスおよびポート番号を持つユーザー要求を同じ実サーバーに配布する必要がある場合に適用されます。 **Source IP address and port number CARP hash**: ユーザーリクエストの送信元 IP アドレスおよびポート番号をハッシュし、CARP ハッシュ値に従ってユーザーリクエストを異なる実サーバーに配布します。このアルゴリズムは、送信元 IP アドレスおよびポート番号が同じユーザーリクエストを同じ実サーバーに配布する必要がある場合に適用されます。使用可能な実サーバーの数が変化すると、このアルゴリズムにより、すべての使用可能な実サーバーの負荷変化が最小になります。 **Destination IP address hash**: ユーザー要求の宛先 IP アドレスをハッシュし、ハッシュ値に従ってユーザー要求を異なる実サーバーに配布します。このアルゴリズムは、クライアントが実サーバーと繰り返し通信する必要がある場合に適用されます。 **Destination IP address CARP hash**: ユーザー要求の宛先 IP アドレスをハッシュし、CARP ハッシュ値に従ってユーザー要求を異なる実サーバーに配布します。このアルゴリズムは、クライアントが実サーバーと繰り返し通信する必要がある場合に適用されます。使用可能な実サーバーの数が変化すると、このアルゴリズムにより、すべての使用可能な実サーバーの負荷変化が最小になります。 **HTTP hash**: ユーザー要求の内容をハッシュし、ハッシュ値に従ってユーザー要求を異なる実サーバーに配信します。このスケジューリングアルゴリズムは、HTTP 仮想サーバーに対してのみ有効です。 **HTTP CARP hash**: ユーザー要求の内容をハッシュし、ユーザー要求を CARP ハッシュ値に従って異なる実サーバーに配布します。使用可能な実サーバーの数が変化すると、このアルゴリズムにより、すべての使用可能な実サーバーの負荷変化が最小になります。このスケジューリングアルゴリズムは、HTTP 仮想サーバーに対してのみ有効です。 **Weighted least connections (member)**: 常に、加重アクティブ接続数(アクティブ接続数を加重で除算した数)が最も少ない実サーバーにユーザ

	ーリクエストを割り当てます。このアルゴリズムで使用される加重は、**Real Server** ページで構成されます。 **Least time (member)**: 常に、実サーバーのレスポンス時間を使用して計算された負荷加重値に基づいて、ユーザー要求を実サーバーに割り当てます。レスポンス時間が短いほど、加重値は大きくなります。加重値が大きい実サーバーほど、多くの接続が割り当てられます。 デフォルトでは、送信元 IP アドレスハッシュアルゴリズムが使用されます。
Offset	HTTP コンテンツの開始に基づいてオフセット値を指定します。 このパラメーターは、スケジューリングアルゴリズムが HTTP ハッシュまたは HTTP CARP ハッシュである場合にだけサポートされます。
Start string	HTTP コンテンツの開始を示す正規表現(オフセット値から始まる文字列)を指定します。文字列には疑問符(?) を含めることはできません。 このパラメーターは、スケジューリングアルゴリズムが HTTP ハッシュまたは HTTP CARP ハッシュである場合にだけサポートされます。
Length/End string	**Length** は、HTTP コンテンツの長さを指定します。 **End string** は、HTTP コンテンツの終了を示す正規表現(開始文字列値から始まる文字列)を指定します。この文字列には疑問符(?)を含めることはできません。 このパラメーターは、スケジューリングアルゴリズムが HTTP ハッシュまたは HTTP CARP ハッシュである場合にだけサポートされます。
Priority scheduling	スケジュール可能なサーバーファーム内の実サーバーの上限と下限を指定します。デフォルトでは、サーバーファーム内で最も高い優先順位を持つすべての実サーバーがスケジュールされます。 プライオリティが最も高い実サーバーの数が、設定された最大数よりも大きい場合は、最大数が適用されます。 このような実サーバーの数が最小数よりも少ない場合は、最小数を満たすように、または使用可能な実サーバーがなくなるまで、優先順位の低い実サーバーが選択されます。 実サーバーのプライオリティは、**Real Servers** ページで設定できます。

Real server	次のいずれかの方法で、実サーバーをサーバーファームに追加できます。 実サーバーを作成し、サーバーファームに追加します。 **Add** をクリックし **Create real server** を選択します。 実サーバーのパラメーターを設定します(「実サーバーの設定」を参照)。 **OK** をクリックします。新しい実サーバーが実サーバーリストに表示されます。 既存の実サーバーを選択します。 **Add** をクリックし、**Add existing real server** を選択します。 リストから実サーバーを選択し、実サーバーのパラメーターを設定します(「実サーバーの設定」を参照)。 **OK** をクリックします。実サーバーが実サーバーリストに表示されます。
Probe method	実サーバーの稼働状態と可用性を検出するためにサーバーファームで使用されるプローブテンプレートを指定します。このパラメーターは、**Real Servers** ページで単一の実サーバーに対して構成することもできます。**Real Servers** ページで実行される構成は **Server Farms** ページで実行される構成よりも優先度が高くなります。既存のプローブテンプレートを選択することも、プローブテンプレートを作成することもできます。 プローブテンプレートを作成するには: **Add** をクリックします。 **Template name**: プローブテンプレートの名前を入力します。 **Use template's port number for detection**: このオプションを選択すると、テンプレートで指定された宛先ポート番号が検出に使用されます。このオプションを選択しないと、実サーバーのポート番号が検出に使用されます。 **OK** をクリックします。新しいプローブテンプレートが **Health Monitoring** ページに表示されます。
Description	サーバーファームの説明を入力します。

表 2 高度な構成項目

項目	説明
Success criteria	実サーバーのヘルスモニタリング成功基準を指定します。 **All probes succeed**: 指定したすべてのヘルスモニタリング方式が成功した場合にだけ、ヘルスモニタリングが成功します。 **At least n probes succeed**: ヘルスモニタリングは、指定された数以上のヘルスモニタリング方式が成功した場合に成功します。指定された数のヘルスモニタリング方式がデバイス上のヘルスモニタリング

	方式の数よりも多い場合は、すべてのヘルスモニタリング方式が成功した場合にヘルスモニタリングが成功します。
SNAT mode	サーバーファームの SNAT モードを指定します。 **SNAT pool**: 送信元 IP アドレスを指定された SNAT アドレスプールの IP アドレスに変換します。 **Auto mapping**: 送信元 IP アドレスを、実サーバーに接続しているインターフェースの IP アドレスに変換します。 **TCP option**: 送信元 IP アドレスを、パケットの TCP オプションフィールドで伝送される IP アドレスに変換します。 サーバーファームに SNAT が設定されていない場合、サーバーファームはアドレス変換にグローバル SNAT ポリシーを使用します。
SNAT pool name	既存の SNAT プールを選択するか、サーバーファーム用の SNAT プールを作成します。 このパラメーターは、SNAT モードが SNAT プールである場合にだけサポートされます。
NAT	間接モード NAT コンフィギュレーションでサーバーファームの NAT をディセーブルにするか、または NAT モードコンフィギュレーションでサーバーファームの NAT をイネーブルにします。
RST packet monitoring	既存の RST プローブテンプレートを選択するか、サーバーファーム用の RST プローブテンプレートを作成します。
Zero-window packet monitoring	既存の 0 ウィンドウプローブテンプレートを選択するか、サーバーファーム用の 0 ウィンドウプローブテンプレートを作成します。
HTTP passive probe	既存の HTTP パッシブプローブテンプレートを選択するか、サーバーファーム用の HTTP パッシブプローブテンプレートを作成します。
Custom monitoring	既存のカスタムプローブテンプレートを選択するか、サーバーファーム用のカスタムプローブテンプレートを作成します。
Auto recovery	自動回復を有効または無効にします。この関数は、自動回復タイマーの期限が切れたときに、インテリジェントプローブテンプレートによってシャットダウンされた実サーバーの自動回復を有効にします。 ヘルスモニタリングが設定されていない場合、実サーバーは未知の状態に回復されます。 ヘルスモニタリングが設定されていて成功した場合、実サーバーは使用可能な状態に回復されます。ヘルスモニタリングが失敗した場合、実サーバーは health-monitoring-failed 状態に回復されます。 この機能は、サーバーファームに HTTP パッシブ、RST、または 0 ウィンドウプローブテンプレートが指定されている場合にだけ使用できます。

Recovery time	自動リカバリ時間を入力します。値 0 は、実サーバーが自動的にリカバリできないことを意味します。 このパラメーターは、自動リカバリが有効になっている場合にのみ使用できます。
Fault processing method	実サーバーの障害処理方法を指定します。 **Keep existing connections**: 障害が発生した実サーバーとの接続を維持します。接続の維持または終了は、プロトコルのタイムアウトメカニズムによって異なります。 **Redirect connections**: 接続をサーバーファーム内の別の使用可能な実サーバーにリダイレクトします。 **Terminate existing connections**: RST パケット(TCP パケットの場合)または ICMP 到達不能パケット(その他のタイプのパケットの場合)を送信して、障害が発生した実サーバーとの接続を終了します。
低速なオンライン	サーバーファームに新たに追加された実サーバーは、LB デバイスによって割り当てられた大量のサービスをすぐには処理できない場合があります。この問題を解決するには、サーバーファームの低速オンライン機能をイネーブルにします。この機能では、スタンバイタイマーとランプアップタイマーが使用されます。実サーバーがオンラインになると、LB デバイスはスタンバイタイマーが期限切れになるまで、実サーバーにサービスを割り当てません。スタンバイタイマーが期限切れになると、ランプアップタイマーが開始されます。ランプアップ時間中、LB デバイスは、ランプアップタイマーが期限切れになるまで、実サーバーの処理能力に応じてサービス量を増やします。 **Standby time**: 指定できる値の範囲は 0～600 秒です。 **Ramp-up time**: 値の範囲は 3～600 秒です。
忙しさへの対応	サーバーファームがビジー状態の場合に実行するアクションを指定します。すべての実サーバーがビジー状態の場合、サーバーファームはビジー状態とみなされます。次のいずれかのアクションを構成できます。 **Schedule**: クライアント要求をサーバーファーム内のすべての実サーバーに強制的に割り当てます。 **Queue and wait**: クライアント要求のサーバーファームへの割り当てを停止し、新しい接続要求を待機キューに割り当てます。 **Queue length**: キューの長さが設定された長さを超えると、新しい接続要求はドロップされます。 **Timeout time**: キューにすでに存在する接続要求は、設定されたタイムアウト時間が経過すると期限切れになります。 レンダリングのスケジュールに失敗しましたサーバーファームへのクライアント要求の割り当てを停止します。サーバーファームの LB ポリシーに次のルールと一致するアクションが含まれている場合、デバイスはクライアント

	要求を次のルールと比較します。それ以外の場合、デバイスはクライアント要求をドロップします。 デバイスは、次の要因に基づいて、実サーバーがビジー状態かどうかを判断します。 最大接続数。 1 秒あたりの最大接続数。 1 秒あたりの HTTP 要求の最大数。 最大帯域幅、最大インバウンド帯域幅、および最大アウトバウンド帯域幅。 SNMP-DCA プローブの結果。
可用性の基準	サーバーファームが使用可能かどうかを判断する基準(パーセンテージの下限と上限)を設定します。これにより、マスターサーバーファームとバックアップサーバーファーム間のトラフィックスイッチオーバーが実装されます。 **Lower percentage**: プライマリサーバーファーム内の実サーバーの合計数に対する使用可能な実サーバーの数が低いパーセンテージよりも少ない場合、トラフィックはバックアップサーバーファームに切り替えられます。 **Upper percentage**: プライマリサーバーファーム内の実サーバーの合計数に対する使用可能な実サーバーの数が上限パーセンテージよりも大きい場合、トラフィックはマスターサーバーファームに戻されます。
すべてのサーバーファームメンバーが利用できない場合のアクション	すべてのサーバーファームメンバーが使用できない場合に実行するアクションを指定します。 **Drop**。 **Forward**: 最後に選択したサーバーファームメンバーに要求を転送します。

OK をクリックします。**Server Farm** ページに新しいサーバーファームが表示されます。

Configure a real server

実サーバーは、ユーザーサービスを処理するための LB デバイス上のエンティティです。実サーバーは複数のサーバーファームに属することができます。サーバーファームは複数の実サーバーを持つことができます。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Real Servers** を選択します。
Create をクリックします。
実サーバーを作成します。

表 3 基本構成項目

項目	説明
Real server name	実サーバーの名前を入力します。大文字と小文字は区別されません。
IPv4 address	実サーバーの IPv4 アドレスを指定します。 IPv4 アドレスは、ループバックアドレス、マルチキャストアドレス、ブロードキャストアドレス、または 0.X.X.X の形式のアドレスにはできません。
IPv6 address	実サーバーの IPv6 アドレスを指定します。 IPv6 アドレスは、ループバックアドレス、マルチキャストアドレス、リンクローカルアドレス、またはすべて 0 のアドレスにはできません。
Port number	実サーバーのポート番号を指定します。ポート番号が 0 の場合、パケットにはそれぞれのポート番号が使用されます。
VPN instance	実サーバーの VPN インスタンスを指定します。
VPN instance inheritance	VPN インスタンスの継承をイネーブルまたはディセーブルにします。 VPN インスタンスの継承がイネーブルの場合、VPN インスタンスが指定されていない実サーバーは、仮想サーバーの VPN インスタンスを継承します。
Probe logging	ヘルスモニタリングのロギングを有効または無効にします。 この機能は、実サーバーのヘルスステータスの変更をログに記録します。
Real server feature	実サーバー機能をイネーブルまたはディセーブルにします。
Description	実サーバーの説明を入力します。

表 4 高度な構成項目

項目	説明
Weight	実サーバーの重みを入力します。加重ラウンドロビンアルゴリズムおよび加重最小接続アルゴリズムでは、値が大きいほど高い優先度が選択されます。
Priority	サーバーファーム内の実サーバーのプライオリティを入力します。値が大きいほど、高いプライオリティが選択されます。 最も高いプライオリティを持つ実サーバーの数が、設定された最小数よりも少ない場合、最小数を満たすために、より低いプライオリティを持つ実サーバーが選択されます。 最大数と最小数は、**Server Farms** ページで設定できます。

Server farm	既存のサーバーファームを選択するか、実サーバー用のサーバーファームを作成します。
Probe-Probe method	ヘルスおよびアベイラビリティを検出するために実サーバーで使用されるプローブテンプレートを指定します。このパラメーターは、**Server Farms** ページでサーバーファームに対して設定することもできます。**Real Servers** ページで実行される設定は、**Server Farms** ページで実行される設定よりも優先順位が高くなります。 既存のプローブテンプレートを選択することも、プローブテンプレートを作成することもできます。 プローブテンプレートを作成するには: **Add** をクリックします。 **Template name**: プローブテンプレートの名前を入力します。 **Use template's port number for detection**: このオプションを選択すると、テンプレートで指定された宛先ポート番号が検出に使用されます。このオプションを選択しないと、実サーバーのポート番号が検出に使用されます。 **OK** をクリックします。新しいプローブテンプレートが **Health Monitoring** ページに表示されます。
Probe-Success criteria	実サーバーのヘルスモニタリング成功基準を指定します。 **All probes succeed**: 指定したすべてのヘルスモニタリング方式が成功した場合にだけ、ヘルスモニタリングが成功します。 **At least n probes succeed**: ヘルスモニタリングは、指定された数以上のヘルスモニタリング方式が成功した場合に成功します。指定された数のヘルスモニタリング方式がデバイス上のヘルスモニタリング方式の数よりも多い場合は、すべてのヘルスモニタリング方式が成功した場合にヘルスモニタリングが成功します。
Custom monitoring	既存のカスタムプローブテンプレートを選択するか、実サーバー用のカスタムプローブテンプレートを作成します。
Variables	サーバーファームメンバーの変数を設定します。 変数を構成するには: **Add** をクリックします。 **Name**: 変数名を入力します。大文字と小文字は区別されます。 **Value**: 変数値を入力します。大文字と小文字は区別されます。 **OK** をクリックします。**Variables** リストに新しい変数が表示されます。 この変数は、一般的な LB アクションで TCP ペイロードを書き換えるために使用されます。TCP ペイロード内の特定のコンテンツは、サーバーファームメンバーに関連付けられた変数値で置換されます。たとえば、**var1** および value_**1** という名前の変数を構成し、**QMGR.S01** を **QMGR.S01%[var1]**として書き換えるアクション

	を構成すると、TCP ペイロード内の **QMGR.S01** 文字列は **QMGR.S01_1** として書き換えられます。
QoS-Max connections	実サーバーの最大接続数を指定します。0 は無制限を意味します。
QoS-Max connections per second	実サーバーの 1 秒あたりの最大接続数を指定します。0 は無制限を意味します。
QoS-HTTP requests per second	実サーバーの 1 秒あたりの HTTP 要求の最大数を指定します。0 は無制限を意味します。
QoS-Total max bandwidth	実サーバーの最大帯域幅を指定します。0 は制限なしを意味します。
QoS-Max inbound bandwidth	実サーバーの最大インバウンド帯域幅を指定します。0 は制限なしを意味します。
QoS-Max outbound bandwidth	実サーバーの最大アウトバウンド帯域幅を指定します。0 は無制限を意味します。

OK をクリックします。新しい実サーバーが **Real Server** ページに表示されます。

Configure a sticky group (optional)

スティッキグループは、仮想サーバーまたはアクションで使用できます。
スティッキグループの設定の詳細については、ロードバランシングの共通設定に関するヘルプを参照してください。

Configure an LB policy (optional)

LB ポリシーは、クラスをアクションに関連付けて、パケット転送をガイドします。LB ポリシーでは、指定したクラスに一致するパケットのアクションを設定し、クラスに一致しないパケットのデフォルトアクションを設定できます。
1 つの LB ポリシーに複数のクラスを指定できます。パケットは、クラスが設定されている順序でクラスを照合します。クラスが照合されると、指定されたアクションが実行されます。クラスが照合されない場合は、デフォルトのアクションが実行されます。
LB ポリシーは仮想サーバーで使用できます。

Configure a class

Policies > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Class** を選択します。
Create をクリックします。
クラスを作成します。

表 5 クラス構成項目

項目	説明
Class name	クラスの名前を入力します。大文字と小文字は区別されません。
Type	クラスのタイプを指定します。 **Generic**: レイヤー4 サーバーロードバランシングに適用されます。 **HTTP**: レイヤー7 サーバーロードバランシングに適用されます。 **RADIUS**: レイヤー7 サーバーロードバランシングに適用されます。 **MySQL**: レイヤー7 サーバーのロードバランシングに適用されます。
Match type	クラスの照合タイプを指定します。 **Match any**: LB クラスの任意のルールを照合する必要があります。 **Match all**: LB クラスのすべてのルールを一致させる必要があります。
Match rule	クラスは、パケットを特定のルールと比較することによってパケットを分類します。一致するパケットはアクションによってさらに処理されます。1 つのクラスには最大 65535 のルールを作成できます。 **Create** をクリックして、一致ルールを作成します。 **Rule ID**: ルール ID を指定します。ルールはルール ID の昇順で照合されます。 **Type**: ルールタイプを指定します。ルールタイプには、ソース IPv4 アドレス、ソース IPv6 アドレス、クラス、IPv4 ACL、IPv6 ACL、Cookie、HTTP ヘッダー、メソッド、URL、コンテンツ、ユーザー、RADIUS 属性、入力インターフェース、HTTP バージョン、ISP、TCP ペイロードおよび MySQL が含まれます。 **IPv4 address**: IPv4 アドレスを指定します。このパラメーターは、ルールタイプがソース IPv4 アドレスの場合にのみ使用可能です。 **Mask length**: マスク長を指定します。このパラメーターは、ルールタイプがソース IPv4 アドレスの場合にのみ使用可能です。 **IPv6 address**: IPv6 アドレスを指定します。このパラメーターは、ルールタイプがソース IPv6 アドレスの場合にのみ使用可能です。 **Prefix length**: 接頭辞の長さを指定します。このパラメーターは、ルールタイプがソース IPv6 アドレスの場合にのみ使用可能です。 **Class**: クラスを指定します。このパラメーターは、ルールタイプがクラスの場合にのみ使用できます。

	ACL: ACL を指定します。既存の ACL を選択することも、ACL を作成することもできます。このパラメーターは、ルールタイプが IPv4 ACL または IPv6 ACL の場合にのみ使用できます。 **Cookie name**: HTTP パケットの Cookie 名を指定します。Cookie 名は、大文字と小文字が区別される文字列です。ただし、スペース、水平タブ、31 以下の ASCII 文字、127 以上の ASCII 文字、または()<>@、;:¥"/[]?={}を除きます。このパラメーターは、ルールタイプが Cookie の場合にのみ使用可能です。 **Cookie value**: Cookie 値の正規表現を指定します。文字列には疑問符 (?) を含めることはできません。このパラメーターは、ルールタイプが Cookie の場合にのみ使用可能です。 **Header name**: HTTP パケットのヘッダー名を指定します。ヘッダー名は、大/小文字を区別しない文字列です。ただし、スペース、水平タブ、31 以下の ASCII 文字、127 以上の ASCII 文字、または()<>@、;:¥"/[]?={}を除きます。このパラメーターは、ルールタイプが HTTP ヘッダーの場合にのみ使用できます。 **Header value**: ヘッダー値の正規表現を指定します。文字列に疑問符(?)を含めることはできません。このパラメーターは、ルールタイプが HTTP ヘッダーの場合にのみ使用できます。 **Extension type**: 拡張タイプは Predefined または Custom です。このパラメーターは、ルールタイプが Method の場合にのみ使用できます。 **Method**: 事前定義されたメソッドには、GET、CONNECT、DELETE、HEAD、OPTIONS、POST、PUT および TRACE があります。カスタムメソッドでは、大文字と小文字が区別されます。ただし、スペース、水平タブ、31 以下の ASCII 文字、127 以上の ASCII 文字または()<>@、;:¥"/[]?={}を除きます。このパラメーターは、ルールタイプがメソッドの場合にのみ使用できます。 **URL**: URL の正規表現を指定します。文字列には疑問符(?) を含めることはできません。このパラメーターは、ルールタイプが URL の場合にのみ使用できます。 **Content offset**: HTTP パケットの開始に基づく HTTP エンティティのオフセット値を指定します。このパラメーターは、ルールタイプがコンテンツの場合にのみ使用できます。 **Content value**: HTTP エンティティの正規表現を指定します。文字列に疑問符(?) を含めることはできません。このパラメーターは、ルールタイプが内容の場合にのみ使用できます。

	User: アイデンティティードメイン内の既存のユーザーまたはユーザーグループを選択するか、ユーザーまたはユーザーグループを作成します。このパラメーターは、ルールタイプがユーザーの場合にのみ使用できます。 **Attribute type**: 属性タイプの値を入力します。このパラメーターは、ルールタイプが RADIUS 属性の場合にのみ使用可能です。 **Attribute value**: RADIUS 属性の正規表現を指定します。このパラメーターは、ルールタイプが RADIUS 属性の場合にのみ使用可能です。 **Input interface**: 入力インターフェースを指定します。このパラメーターは、ルールタイプが入力インターフェースの場合にのみ使用できます。 **HTTP version**: HTTP バージョンを指定します。このパラメーターは、ルールタイプが HTTP バージョンの場合にのみ使用できます。 **ISP**: 既存の ISP を選択するか、ISP を作成します。このパラメーターは、ルールの種類が ISP の場合にのみ使用できます。 **TCP payload**: TCP ペイロードの照合に使用する正規表現を入力します。このパラメーターは、ルールタイプが TCP ペイロードの場合にのみ使用可能です。 **Case insensitive**: 照合時の大/小文字の区別を使用可能にします。このパラメーターは、ルールタイプが TCP ペイロードまたは MySQL の場合にのみ使用できます。 **Negate the match rule**: このオプションを選択しない場合、TCP パケットが正規表現と一致したときに LB アクションが実行されます。このオプションを選択すると、TCP パケットが正規表現と一致しないときに LB アクションが実行されます。このパラメーターは、ルールタイプが TCP ペイロードまたは MySQL である場合にだけ使用できます。 **Regular expression**: MySQL 文の照合に使用する正規表現を入力します。このパラメーターは、ルールタイプが MySQL の場合にのみ使用可能です。 **OK** をクリックします。
Description	クラスの説明を入力します。

OK.をクリックします。**Class** ページに新しいクラスが表示されます。

Configure an action

Policies > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Action** を選択します。

Create をクリックします。

アクションを作成します。

表 6 基本構成項目

項目	説明
Action name	アクションの名前を入力します。大文字と小文字は区別されません。
Type	アクションタイプを指定します。 Generic HTTP HTTP redirection RADIUS
Forwarding mode	転送モードを指定します。 Load balance Drop Forward(汎用タイプおよび RADIUS タイプだけでサポート) Respond by using a file (HTTP タイプでのみサポート)
Uncompressed file	クライアント要求内の URL パスが指定された URL パスと一致する場合、デバイスは非圧縮ファイルを使用して要求に応答します。 **Create** をクリックして、圧縮されていない応答ファイルを作成します。 **URL Path**: HTTP リクエストの照合に使用する URL パスを指定します。大文字と小文字が区別される文字列です。指定する URL パスは、スラッシュ(/)で始まる必要があります。 **Uncompressed file**: 非圧縮ファイルを絶対パスとファイル名で指定します。flash:/file.html のように、大文字と小文字は区別されません。1 つの URL には 1 つの非圧縮ファイルのみを使用でき、複数の URL には 1 つの非圧縮ファイルを使用できます。 **OK** をクリックします。 このパラメーターは、転送モードが **Respond by using a file** の場合にのみ使用できます。
Compressed file	クライアント要求内の URL パスが、指定された作業パスおよび zip ファイル内の相対パスと一致する場合、デバイスは zip ファイル内のファイルを使用して要求に応答します。たとえば、作業パスを**/index** に、圧縮ファイルを **flash:/za/zb/test.zip** に構成し、**test.zip** 内に相対パス**/css/col.css** が存在する場合、一致する URL は**/index/css/col.css** で、応答ファイルは **col.css** です。

	Working Path: 作業パスと、HTTP リクエスト内の URL と一致する zip ファイル内の相対パス(大文字と小文字を区別する文字列)を指定します。作業パスは、スラッシュで始まる必要があります。 **Compressed file**: 圧縮ファイルは絶対パスとファイル名で指定します。ファイル名の大文字と小文字は区別されません。ファイルは zip ファイル(flash:/file.zip など)である必要があります。 このパラメーターは、転送モードが **Respond by using a file** の場合にのみ使用できます。
Fallback action	フォールバックアクションを指定します。 **Match next rule**: 使用可能な実サーバーが見つからない場合に、次のルールを照合します。 **Respond by using another file**: 使用可能な実サーバーが見つからなかった場合に、指定されたデフォルトの応答ファイルを使用してクライアント要求に応答します。 **Default response file**: 非圧縮ファイルを絶対パスとファイル名で指定します。flash:/file.html のように、大文字と小文字は区別されません。 **Fin close**: TCP 接続を閉じるために FIN パケットを送信します。 **Rst close**: TCP 接続を閉じるために RST パケットを送信します。 このパラメーターは、転送モードが **Load balance** の場合にのみ使用できます。
Action taken upon failure to find the response file	応答ファイルが見つからなかった場合に実行するアクションを指定します。 **Match next rule**: レスポンスファイルの検索に失敗した場合に次のルールと一致します。 **Respond by using a file**: 応答ファイルが見つからなかった場合に、指定されたデフォルトの応答ファイルを使用してクライアント要求に応答します。 **Default response file**: 非圧縮ファイルを絶対パスとファイル名で指定します。flash:/file.html のように、大文字と小文字は区別されません。 **Fin close**: TCP 接続を閉じるために FIN パケットを送信します。 **Rst close**: TCP 接続を閉じるために RST パケットを送信します。

	このパラメーターは、転送モードが **Respond by using a file** の場合にのみ使用できます。
TCP connection close mode	TCP 接続クローズモードを指定します。 **By sending FIN:** TCP 接続を閉じるために FIN パケットを送信します。 **By sending RST**: TCP 接続を閉じるために RST パケットを送信します。 このパラメーターは、転送モードが **Drop** の場合にだけ使用できます。
ToS	サーバーに送信される IP パケットの ToS フィールド値を設定します。
Description	アクションの説明を入力します。
Server farms-Primary server farm	既存のサーバーファームを選択するか、プライマリサーバーファームとしてサーバーファームを作成します。 プライマリサーバーファームが使用可能な場合(実サーバーが含まれている場合)、パケットはプライマリサーバーファームを経由して転送されます。プライマリサーバーファームが使用できない場合、パケットはバックアップサーバーファームを経由して転送されます。 このパラメーターは、転送モードが **Load balance** の場合にのみ使用できます。
Server farms-Backup server farm	既存のサーバーファームを選択するか、バックアップサーバーファームとしてサーバーファームを作成します。 このパラメーターは、転送モードが **Load balance** の場合にのみ使用できます。
Server farms-Sticky group	既存のスティッキグループを選択するか、またはスティッキグループを作成します。 このパラメーターは、転送モードが **Load balance** の場合にのみ使用できます。
HTTP redirection configuration-Redirection URL	この設定は、アクションに一致するすべての HTTP 要求パケットを、指定された URL にリダイレクトします。 リダイレクト URL を指定します。大文字と小文字が区別される文字列です。リダイレクト URL として疑問符(?)または次の文字列を指定することもできます。 **%h**: クライアント要求パケット内のホスト名を指定します。 **%p**: クライアント要求パケット内の URL を指定します。 **%%**: パーセント記号(%)を指定します。 このパラメーターは、アクションタイプが HTTP リダイレクションである場合にだけ使用できます。

HTTP redirection configuration -Redirection mode	リダイレクションモードを指定します。 **Temporary**: 302 **Temporary**: 307 **Permanent**: 301 このパラメーターは、アクションタイプが HTTP リダイレクションである場合にだけ使用できます。

表 7 高度な構成項目(action type が HTTP で、forwarding mode が Load balance または Respond by using a file の場合にのみ使用可能)

項目	説明
TCP payload rewrite	**Create** をクリックします。 **Direction:** 方向を指定します。**Both**, **Request1** または **Response** を指定できます。 **Content before rewrite**: 書き直す TCP メッセージ本文。大文字と小文字が区別される正規表現文字列です。 **Content after rewrite**: 書き換え後の TCP メッセージ本文。次の置換文字列も指定できます。 **%[*variable*]**: 指定した値をサーバーファームメンバーに関連付けられた変数に置き換えます。variable は変数名です。 **%[1-9]**: 指定した値を、対応するカッコ内の内容に置換します。たとえば、書き換え前の内容を**(Wel)(co)(me)**に設定し、書き換え後の内容を**%2** に設定した場合、2 番目のカッコ内の文字列 **Welcome** は **co** に置換されます。 **OK** をクリックします。 このパラメーターは、汎用 LB アクションでのみサポートされています。 レイヤー7 で動作する TCP 仮想サーバーだけが、TCP ペイロード書き換え設定を含む LB ポリシーをサポートします。
Insert X-Forwarded-For	X-Forwarded-For ヘッダーを挿入します。
Response content rewrite-Content before rewrite	書き直す HTTP パケットの内容を指定します。
Response content rewrite-Content after rewrite	書き換え後の HTTP パケットの内容を指定します。 **%is** :送信元 IPv4 または IPv6 アドレス。 **%ps**: 送信元ポート番号。 **%id**: 宛先 IPv4 または IPv6 アドレス。 **%pd**: 宛先ポート番号。

項目	説明
	%%: パーセント記号(%)。 **%[1-9]**: 括弧で囲まれたヘッダー値。
Header deletion	**Create** をクリックします。 **Direction**: 方向を指定します。**Both**, **Request**, または **Response** を指定できます。 **Header name**: ヘッダー名を指定します。大文字と小文字は区別されず、事前定義またはカスタマイズできます。ヘッダー名には、スペース、水平タブ、31 以下の ASCII 文字、127 以上の ASCII 文字、または ()<>@、;:¥"/[]?={}の文字は使用できません。 **OK** をクリックします。
Header insertion	**Create** をクリックします。 **Direction**: HTTP パケットの方向を指定します。**Both**, **Request**, または **Response** を指定できます。 **Header name**: ヘッダー名を指定します。大文字と小文字は区別されず、事前定義またはカスタマイズできます。ヘッダー名には、スペース、水平タブ、31 以下の ASCII 文字、127 以上の ASCII 文字、または ()<>@、;:¥"/[]?={}の文字は使用できません。 **Header value**: HTTP パケットに挿入するヘッダーコンテンツを指定します。文字列には疑問符(?) は使用できません。次の置換文字列も指定できます。 **%is**: HTTP 要求の送信元 IP アドレス。 **%ps**: HTTP 要求の送信元ポート番号。 **%id**: HTTP 要求の宛先 IP アドレス。 **%pd**: HTTP 要求の宛先ポート番号。 **%sps**: HTTP 応答の送信元ポート番号。 **%spd**: HTTP 応答の宛先ポート番号。 **%sis**: HTTP 応答内の送信元 IP アドレス。 **%sid**: HTTP 応答の宛先 IP アドレス。 **%{x509v}**: 証明書のバージョン。 **%{x509snum}**: 証明書のシリアル番号。 **%{x509sigalgo}**: Certificate Signature Algorithm(CA)。 **%{x509issuer}**: 証明書の発行者。 **%{x509before}**: 証明書の有効時間。 **%{x509after}**: 証明書の有効期限です。 **%{x509sub}**: 証明書のサブジェクト。 **%{x509spktype}**: 証明のサブジェクトの公開キーの種類です。

項目	説明
	%{x509spk}: 証明書のサブジェクトの公開キー。 **%{x509spkRSA}**: 認証サブジェクトの RSA 公開キーの長さ(RSA 公開キーの場合だけ使用可能)。 **%{x509hash}**: クライアント証明書の MD5 ハッシュ値。 **%{dncn}**: 問題。 **%{dne}**: 電子メール。 **%{dno}**: 会社/組織。 **%{dnou}**: 部門。 **%{dnc}** :国。 **%{dns}**: 州/県。 **%{dnl}:** 市。 **Encoding method**: 置換文字列のエンコード方法を指定します。エンコード方法には **Not encoded**, **URL**, または **Base64**.を指定できます。URL エンコードでは、スペースと、置換文字列内の/?:@&=+${}、¥^[]`<>#%の特殊文字のみがエンコードされます。Base64 エンコードでは、置換文字列全体がエンコードされます。 **OK** をクリックします。
Header rewrite	**Create** をクリックします。 **Direction**: HTTP パケットの方向を指定します。**Both**, **Request**, または **Response** を指定できます。 **Header name**: ヘッダー名を指定します。大文字と小文字は区別されず、事前定義またはカスタマイズできます。ヘッダー名には、スペース、水平タブ、31 以下の ASCII 文字、127 以上の ASCII 文字、または ()<>@、;:¥"/[]?={}の文字は使用できません。 **Header value**: 書き換え後のヘッダーコンテンツを指定します。文字列には疑問符(?) を含めることはできません。次の置換文字列も指定できます: **%is**: HTTP 要求の送信元 IP アドレス。 **%ps**: HTTP 要求の送信元ポート番号。 **%id**: HTTP 要求の宛先 IP アドレス。 **%pd**: HTTP 要求の宛先ポート番号。 **%sps**: HTTP 応答の送信元ポート番号。 **%spd**: HTTP 応答の宛先ポート番号。 **%sis**: HTTP 応答内の送信元 IP アドレス。 **%sid**: HTTP 応答の宛先 IP アドレス。 **%1-9**: 置換に使用される指定された文字列。最大 9 つの項目がサポートされています。

項目	説明
	%{x509v}: 証明書のバージョン。 **%{x509snum}**: 証明書のシリアル番号。 **%{x509sigalgo}**: Certificate Signature Algorithm(CA;認証局署名アルゴリズム)。 **%{x509issuer}**: 証明書の発行者。 **%{x509before}**: 証明書の有効時間。 **%{x509after}**: 証明書の有効期限です。 **%{x509sub}**: 証明書のサブジェクト。 **%{x509spktype}**: 証明のサブジェクトの公開キーの種類です。 **%{x509spk}**: 証明書のサブジェクトの公開キー。 **%{x509spkRSA}**: 認証サブジェクトの RSA 公開キーの長さ(RSA 公開キーの場合だけ使用可能)。 **%{x509hash}**: クライアント証明書の MD5 ハッシュ値。 **%{dncn}**: 問題。 **%{dne}**: 電子メール。 **%{dno}**:会社/組織。 **%{dnou}**: 部門。 **%{dnc}**: 国。 **%{dns}**: 州/県。 **%{dnl}**: 市。 **Encoding method**: 置換文字列のエンコード方法を指定します。エンコード方法には、**Not encoded**, **URL**,または **Base64** を指定できます。URL エンコードでは、スペースと、置換文字列内の/?:@&=+${}、¥^[]`<>#%の特殊文字のみがエンコードされます。Base64 エンコードでは、置換文字列全体がエンコードされます。 **OK** をクリックします。
URL rewrite	**Create** をクリックします。 **URL to be rewritten**: URL コンテンツに疑問符(?)を含めることはできません。 **URL Url after rewriten**: 再書込み後の URL コンテンツを指定します。次の置換文字列も指定できます。 **%is**: HTTP 要求の送信元 IP アドレス。 **%ps**: HTTP 要求の送信元ポート番号。 **%id**: HTTP 要求の宛先 IP アドレス。 **%pd**: HTTP 要求の宛先ポート番号。 **%sps**: HTTP 応答の送信元ポート番号。

項目	説明
	%spd: HTTP 応答の宛先ポート番号。 **%sis**: HTTP 応答内の送信元 IP アドレス。 **%sid**: HTTP 応答の宛先 IP アドレス。 **%1-9**: 置換に使用される指定された文字列。最大 9 つの項目がサポートされています。 **%{x509v}**: 証明書のバージョン。 **%{x509snum}**: 証明書のシリアル番号。 **%{x509sigalgo}**: Certificate Signature Algorithm(CA;認証局署名アルゴリズム)。 **%{x509issuer}**: 証明書の発行者。 **%{x509before}**: 証明書の有効時間。 **%{x509after}**: 証明書の有効期限です。 **%{x509sub}**: 証明書のサブジェクト。 **%{x509spktype}**: 証明のサブジェクトの公開キーの種類です。 **%{x509spk}**: 証明書のサブジェクトの公開キー。 **%{x509spkRSA}**: 認証サブジェクトの RSA 公開キーの長さ(RSA 公開キーの場合だけ使用可能)。 **%{x509hash}**: クライアント証明書の MD5 ハッシュ値。 **%{dncn}**: 問題。 **%{dne}**: 電子メール。 **%{dno}**: 会社/組織。 **%{dnou}**: 部門。 **%{dnc}**: 国。 **%{dns}**: 州/県。 **%{dnl}**: 市。 **Encoding method**: 置換文字列のエンコード方法を指定します。エンコード方法には、**Not encoded**, **URL**, または **Base64** を指定できます。URL エンコードでは、スペースと、置換文字列内の/?:@&=+$\{\}、¥^[]`<>#%の特殊文字のみがエンコードされます。Base64 エンコードでは、置換文字列全体がエンコードされます。 **OK** をクリックします。
SSL security-SSL client policy	既存の SSL クライアントポリシーを選択するか、または SSL クライアントポリシーを作成します。
SSL security-SSL redirection URL list	**Create** をクリックします。 **URL**: Location ヘッダーの URL 正規表現を指定します。 **HTTP port**: 書き直す HTTP ポート番号を指定します。

項目	説明
	SSL Port: 書き換え後の SSL ポート番号を指定します。 **OK** をクリックします。

OK をクリックします。**Action** ページに新規アクションが表示されます。

Configure an LB policy

Policies > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Load Balancing Policy** を選択します。
Create をクリックします。
LB ポリシーを作成します。

表 8 LB ポリシーの構成項目

項目	説明
Name	LB ポリシーの名前を入力します。大文字と小文字は区別されません。
Type	LB ポリシーのタイプを指定します。 **Generic**: レイヤー4 サーバーロードバランシングに適用されます。 **HTTP**: レイヤー7 サーバーロードバランシングに適用されます。 **RADIUS**: レイヤー7 サーバーロードバランシングに適用されます。 **MySQL**: レイヤー7 サーバーのロードバランシングに適用されます。
Default action	汎用 LB ポリシーには汎用アクションを指定し、HTTP LB ポリシーには任意のタイプのアクションを指定します。 既存のアクションを選択することも、アクションを作成することもできます。
Rule	指定したクラスに一致するパケットのアクションを指定します。 **Create** をクリックします。 **Class**: 既存のクラスを選択するか、クラスを作成します。 **Action**: 既存のアクションを選択するか、アクションを作成します。 **Insert before**: ターゲットクラスをクラスの前に挿入します。 **OK** をクリックします。
Description	LB ポリシーの説明を入力します。

OK をクリックします。新しい LB ポリシーが **Load Balancing Policy** ページに表示されます。

Configure a connection limit policy (optional)

接続制限ポリシーを使用すると、デバイス上の接続数を制限できます。これにより、多数の接続がデバイスシステムリソースおよびサーバーリソースを大量に消費するのを防ぐことができます。このようにして、内部ネットワークリソース(ホストまたはサーバー)が保護され、デバイスシステムリソースをより適切に使用できます。

接続制限ポリシーは、複数の規則を持つことができます。各規則は、ユーザーの範囲とユーザー接続の制限を指定します。接続制限ポリシーは、規則と一致するユーザー接続にのみ適用されます。特定の種類の接続数が上限に達すると、デバイスはその種類の新しい接続要求を受け付けません。接続数が下限を下回った場合にのみ、新しい接続要求を受け付けます。

ルール内のユーザー範囲は、ACL を使用して設定します。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Connection Limit Policy** を選択します。

Create をクリックします。

接続制限ポリシーを作成します。

表 9 接続制限ポリシーの構成項目

項目	説明
名前	接続制限ポリシーの名前を入力します。大文字と小文字は区別されません。
制約条件	ルールを作成します。 **Create** をクリックします。 **Rule ID**: 接続制限ルールの ID を指定します。 **Type**: 接続制限規則のタイプを指定します。IPv4 ACL または IPv6 ACL を指定できます。 **ACL**: ACL を指定します。既存の ACL を選択することも、ACL を作成することもできます。 **Limit by**: 送信元 IP アドレス、宛先 IP アドレスまたはサービスを選択します。送信元 IP アドレスは、送信元 IP アドレスによってユーザー接続を制限します。宛先 IP アドレスは、宛先 IP アドレスによってユーザー接続を制限します。サービスは、サービスによってユーザー接続を制限します。サービスは、トランスポート層プロトコルおよびサービスポート番号によって分類されます。

	Connection limits-Upper limit: 接続の上限を指定します。指定した範囲または特定のタイプの接続数が上限に達すると、デバイスは新しい接続リクエストを受け入れません。 **Connection limits Lower limit**: 接続の下限を指定します。下限は、上限以下である必要があります。デバイスは、接続数が下限を下回った場合にのみ新規接続リクエストを受け入れます。 **OK** をクリックします。
説明	接続制限ポリシーの説明を入力します。

OK をクリックします。新しい接続制限ポリシーが **Connection Limit Policy** ページに表示されます。

Configure a protection policy (optional)

保護ポリシーは、LB デバイスおよび内部サーバーが攻撃されるのを防ぐことができます。保護ポリシーでは、保護ルールおよび保護アクションを指定できます。保護ルールは、保護する URL および保護期間を定義します。保護期間中に保護された URL にユーザーがアクセスする回数が、構成された保護しきい値を超えると、保護アクションが実行されます。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Advanced Policies** > **Protection Policy** を選択します。
Create をクリックします。
保護ポリシーを作成します。

表 10 保護ポリシーの構成項目

項目	説明
Name	保護ポリシーの名前を入力します。大文字と小文字は区別されません。
Type	保護ポリシーのタイプを指定します。 デバイスは HTTP タイプだけをサポートします。
Protction action	保護アクションを選択します。保護された URL へのユーザーのアクセス回数が、構成された保護しきい値を超えると、保護アクションが実行されます。次の保護アクションを指定できます。 **Warning**: ログメッセージを生成し、Information Center に送信します。 **Drop**: 要求をドロップします。

	Verify client: Cookie 値を含むレスポンスをクライアントに戻します。後続のリクエストに戻された Cookie 値が含まれている場合は、検証に合格します。後続のリクエストに Cookie 値が含まれていない場合、または異なる Cookie 値が含まれている場合は、検証に合格せず、ドロップされます。デバイスは、HTTP ヘッダーまたは JS スクリプトを挿入して Cookie 値を戻すことをサポートします。
Protection rule	保護ポリシーには、複数の保護ルールを含めることができます。各保護ルールでは、保護する URL および保護期間が定義されます。保護期間中に、保護された URL へのユーザーのアクセス回数が、構成された保護しきい値を超えると、保護アクションが実行されます。デバイスでは、送信元 IP ベースおよび Cookie ベースの基準を使用して、要求が同じユーザーに属するかどうかが判別されます。Cookie ベースの要求しきい値と送信元 IP ベースの要求しきい値の両方を構成すると、いずれかのしきい値を超えたときに保護アクションが実行されます。 **Create** をクリックして、保護規則を作成します。 **Rule ID**: ルール ID を指定します。 **Protected URL**: URL と一致する正規表現を指定します。大文字と小文字が区別される文字列です。正規表現には疑問符(?)を含めることはできません。 **Statistics period**: 保護期間を設定します。保護期間中にユーザーが保護された URL にアクセスする回数がリクエストのしきい値を超えると、保護アクションが実行されます。 **Source-IP-based threshold**: 送信元 IP ベースの要求しきい値を設定します。 **Cookie name**: HTTP Cookie を名前で指定します。大文字と小文字が区別されます。Cookie 名には、大カッコ({}、()、[]、<>)、アットマーク(@)、カンマ(,)、セミコロン(;)、コロン(:)、バックスラッシュ(¥)、引用符(")、スラッシュ(/)、疑問符(?) 、等号(=)、スペース文字(SP)および水平タブ(HT)を含めることはできません。また、Cookie 名には、31 以下および 127 以上の ASCII コードを含めることはできません。 **Cookie-based threshold**: Cookie ベースの保護しきい値を設定します。 **OK** をクリックします。
Description	保護ポリシーの説明を入力します。

OK をクリックします。新しい保護ポリシーが **Protection Policy** ページに表示されます。

Configure a parameter profile (optional)

パラメータープロファイルを使用して拡張パラメーターを構成できます。仮想サーバーは、サービストラフィックを分析、処理および最適化するためにパラメータープロファイルを参照します。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Parameter Profiles** を選択します。
Create をクリックします。
パラメータープロファイルを作成します。

表 11 パラメータープロファイルの構成項目

項目	説明
Parameter profile name	パラメータープロファイルの名前を入力します。大文字と小文字は区別されません。
Type	パラメータープロファイルのタイプを指定します。 **IP**: レイヤー4 サーバーのロードバランシングに適用されます。IP パラメーター構成の詳細は、表 14 を参照してください。 **TCP**: レイヤー7 サーバーのロードバランシングに適用されます。TCP パラメーター構成の詳細は、表 15 を参照してください。 **HTTP**: レイヤー7 サーバーのロードバランシングに適用されます。HTTP パラメーター設定の詳細については、表 16 を参照してください。 **HTTP-Compression**: レイヤー7 サーバーのロードバランシングに適用されます。HTTP 圧縮パラメーター構成の詳細は、表 17 を参照してください。 **HTTP-Statistics**: レイヤー7 サーバーのロードバランシングに適用されます。HTTP 統計情報パラメーター設定の詳細については、表 18 を参照してください。 **OneConnect**: レイヤー7 サーバーのロードバランシングに適用されます。OneConnect パラメーター構成の詳細は、表 19 を参照してください。 **TCP-Application**: レイヤー7 サーバーのロードバランシングに適用されます。TCP アプリケーションパラメーター構成の詳細は、表 20 を参照してください。 **MySQL**: レイヤー7 サーバーのロードバランシングに適用されます。MySQL アプリケーションパラメーター構成の詳細は、表 21 を参照してください。
Description	パラメータープロファイルの説明を入力します。

表 12 IP パラメーターの構成項目

項目	説明
ToS sent to client	クライアントに送信される IP パケットの ToS フィールド値を設定します。

表 13 TCP パラメーター構成項目

項目	説明
Option operation list	この機能を使用すると、LB デバイスはクライアントの実際の IP アドレスを、サーバーに送信される TCP パケットのヘッダー内の指定されたオプションに挿入したり、指定されたオプションを削除したりできます。 オプション操作を作成するには、**Create** をクリックします。 **Insert**: クライアントの実際の IP アドレスを、サーバーに送信される TCP パケットのヘッダー内の指定されたオプションに挿入します。 **Remove**: サーバーに送信される TCP パケットのヘッダーから、指定したオプションを削除します。 **Option number**: 操作されるオプションの番号。 **Encoding type**: TCP オプションの符号化モードとして、バイナリまたは文字列を選択します。 **OK** をクリックします。**Option operation list** に新しいオプション操作が表示されます。
Max local window size	TCP 接続の最大ローカルウィンドウサイズを設定します。
Action on MSS-exceeded packets	クライアントが送信した HTTP 要求で MSS を超えるセグメントに対して実行するアクションを指定します。 **Permit**: セグメントが MSS を超えることを許可します。 **Drop**: MSS を超過するセグメントを廃棄します。
Idle timeout time	TCP 接続のアイドルタイムアウト時間を指定します。 アイドルタイムアウト時間が経過する前にデータが送信されない場合、LB デバイスはクライアントまたはサーバーとの TCP 接続を切断します。
TCP MSS	LB デバイスの MSS を指定します。
TIME-WAIT timeout time	TCP 接続の TIME_WAIT 状態タイムアウト時間を設定します。 TCP の TIME_WAIT タイマーが長いため、TCP 接続は切断された後にゆっくりと解放されます。TIME_WAIT 状態のタイムアウト時間は調整できます。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。

SYN timeout time	TCP 接続のザシンパケットタイムアウト時間を設定します。タイマーの期限が切れたときに SYN-ACK パケットが受信されない場合、TCP 接続は閉じられます。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。
Keepalive timeout time	アイドル状態の TCP 接続に対する TCP キープアライブパケットの送信間隔を設定します。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。
Keepalive retransmission interval	TCP キープアライブパケットの再送信間隔を設定します。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。
Keepalive retransmission times	TCP キープアライブパケットの再送信回数を設定します。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。
FIN-WAIT-1 timeout time	TCP 接続の FIN-WAIT-1 状態タイムアウトタイマーを設定します。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。
FIN-WAIT-2 timeout time	TCP 接続の FIN-WAIT-2 状態タイムアウトタイマーを設定します。 このパラメーターは、TCP パラメータープロファイルが HTTP または HTTPS 仮想サーバーで使用されている場合にだけ有効です。
TCP option number for SNAT	SNAT に使用する TCP オプションの番号を指定します。 LB デバイスは、パケットの送信元 IP アドレスを、指定された TCP オプションの IP アドレスに変換します。
Encoding type	TCP オプションのバイナリまたは文字列のエンコードモードを選択します。

表 14 HTTP パラメーターの構成項目

項目	説明
Max header parse length	解析可能な HTTP ヘッダーの最大長を設定します。
Max content parse length	解析可能な HTTP エンティティの最大長を設定します。
Max content length	HTTP 要求の最大コンテンツ長を設定します。HTTP 要求のコンテンツ長が最大長を超えた場合、デバイスは HTTP 要求をドロップします。
Secondary cookie delimiter	! " # ; < > ? [¥] ^ ` | : @ & $ + * ' ( ) , /,/など、URL 内のセカンダリ Cookie を区切る区切り文字を指定します。

Secondary cookie start delimiter	! " # ; < > ? [¥] ^ ` | など、URL 内のセカンダリ Cookie の開始デリミタを指定します。
Cookie name	暗号化する cookie を名前で指定します(大文字と小文字を区別するストリング)。
Cookie encryption key	平文または暗号文形式でキーを指定します。
Key	キーを指定します。大文字と小文字を区別するストリングです。
Action on max-header-length exceeded packets	パケットヘッダーが最大長を超えた場合に HTTP 要求に対して実行するアクションを指定します。 [Permit]:HTTP 要求の通過を許可します。 [Drop]:HTTP 要求を廃棄します。 HTTP パケットヘッダーの長さがロードバランシングの処理能力を超えると、**drop** アクションが適用されます。
Per-packet load balancing	HTTP 要求に対するパケット単位のロードバランシングをイネーブルまたはディセーブルにします。
Connection reuse	LB デバイスとサーバー間の接続の再利用を有効または無効にします。 接続の再利用により、LB デバイスはクライアントが再利用できるサーバーへの接続を確立できます。複数のクライアントが同じ接続を使用できるため、クライアントとサーバー間の接続数が減少します。
Case sensitivity	文字列の照合で大文字と小文字の区別を有効または無効にします。この設定は次の内容に影響します: HTTP ヘッダー値、HTTP cookie の名前と値、および一致するクラスの URL。 HTTP ヘッダースティッキ方式のスティッキエントリの生成に使用されるヘッダー値、URL、およびキー値。 cookie get sticky メソッドのスティッキエントリの生成に使用される cookie の名前、値、およびキー値。
Load balance each request	HTTP 要求に対する要求単位のロードバランシングを有効または無効にします。

表 15 HTTP 圧縮パラメーターの構成項目

項目	説明
Level	応答パケットの圧縮レベルを設定します。値が大きいほど、圧縮速度が遅く、圧縮率が高くなります。

Preferred compression algorithm	優先する圧縮アルゴリズムを指定します。クライアント要求が構成済圧縮アルゴリズムをサポートしている場合は、構成済圧縮アルゴリズムが適用されます。クライアント要求が構成済圧縮アルゴリズムをサポートしていない場合は、要求に含まれている圧縮アルゴリズムが適用されます。 **gzip**: GNU zip 圧縮アルゴリズムを指定します。 **deflate**: Deflate 圧縮アルゴリズムを指定します。
Min content length	圧縮する HTTP レスポンスコンテンツの最小長を設定します。値 0 は、コンテンツ長に関係なく、パケットコンテンツが常に圧縮されることを示します。 HTTP 応答パケットに Content-Length ヘッダーが含まれている場合、パケットの内容は、圧縮する HTTP 応答コンテンツの最小長に達した場合にのみ圧縮されます。HTTP 応答パケットに Content-Length ヘッダーが含まれていない場合、設定は有効になりません。パケットの内容は、その長さに関係なく圧縮されます。
Insert Vary header	HTTP 応答への Vary ヘッダーの挿入を有効または無効にします。 この機能を有効にすると、HTTP 応答に Vary ヘッダーが挿入され、クライアントに送信する前にヘッダーの内容が Accept-Encoding に設定されます。この設定は、応答パケットに Vary ヘッダーが含まれているかどうか、またはパケットが圧縮されているかどうかに関係なく有効です。
Compression for HTTP 1.0	HTTP 1.0 要求への応答の圧縮を有効または無効にします。
Delete Accept-Encoding header	HTTP 要求からの Accept-Encoding ヘッダーの削除を有効または無効にします。 この機能をイネーブルにすると、LB デバイスはサーバーに送信する前に HTTP 要求から Accept-Encoding ヘッダーを削除できます。サーバーから送信された応答パケットが指定された一致規則と一致する場合、LB デバイスはパケットを圧縮してから要求元クライアントに送信します。クライアントから送信された HTTP 要求に Accept-Encoding ヘッダーが含まれていない場合、この機能がイネーブルかどうかに関係なく、LB デバイスは応答パケットを圧縮しません。
Memory size	圧縮に使用するメモリーサイズを KB 単位で指定します。値は 1、2、4、8、16、32 または 64 のみです。
Window size	圧縮に使用するウィンドウサイズを KB 単位で指定します。値は 1、2、4、8、16 または 32 のみです。
Filtering rule for compression	**Create** をクリックします。 **Rule ID**: ルール ID を指定します。 **Action**: 一致するパケットを圧縮するには permit を指定し、一致するパケットを圧縮しないには deny を指定します。 **Type**: パケット内の URL と照合する場合は URL を指定し、パケットの Content-Type ヘッダー内のコンテンツタイプと照合する場合はコンテンツを指定します。

	URL: 照合する URL の正規表現を指定します。大文字と小文字が区別される文字列です。文字列に疑問符(?)を含めることはできません。このパラメーターは、URL タイプでのみ使用できます。 **Content-Type**: コンテンツタイプを照合する正規表現を指定します。大文字と小文字が区別される文字列です。文字列に疑問符(?)を含めることはできません。このパラメーターは、コンテンツタイプに対してのみ使用できます。 **OK** をクリックします。

表 16 HTTP 統計パラメーターの構成項目

項目	説明
Address オブジェクトグループ	HTTP パケットが指定された URL および送信元 IP アドレスオブジェクトグループと一致する場合、送信元 IP アドレスオブジェクトグループに基づいてカウントされます。HTTP パケットが指定された URL と一致するが、指定された送信元 IP アドレスオブジェクトグループと一致しない場合、送信元 IP アドレスに基づいてカウントされます。 1 つの HTTP 統計情報パラメータープロファイルには、最大 1024 の送信元 IP アドレスオブジェクトグループを指定できます。
HTTP 統計ノードリスト	**Create** をクリックします。 **Node name**: 統計ノード名を指定します。大文字と小文字は区別されません。1 つの HTTP 統計パラメータープロファイルには、最大 256 の統計ノードを構成できます。 **Description**: 統計ノードの説明を入力します。大文字と小文字は区別されます。 **Statistics rule list**: URL 一致ルールのリスト。1 つの統計情報ノードに対して最大 256 の URL 一致ルールを設定できます。 **ID**: 一致ルール ID を指定します。 **URL**: URL の正規表現を指定します。文字列に疑問符(?)を含めることはできません。 **OK** をクリックします。

表 17 OneConnect パラメーターの構成項目

項目	説明
Max reuse number	TCP 接続を再利用できる最大回数を設定します。

	接続の再利用が有効になると、再利用の最大回数に達するまで TCP 接続は切断されません。TCP 接続が切断されると、新しい接続要求によって新しい TCP 接続の確立がトリガーされます。
Idle timeout time	LB デバイスとサーバー間の TCP 接続のアイドルタイムアウト時間を設定します。アイドルタイムアウト時間は、TCP 接続が切断されるまでアイドル状態を維持できる時間です。TCP 接続が切断された後、新しい接続要求によって新しい TCP 接続の確立がトリガーされます。
IPv4 mask length	接続再利用のための IPv4 マスク長を指定します。 この設定は、LB デバイスとサーバー間の接続を再利用できるクライアントのネットワークセグメントを制限します。接続要求を開始したクライアントがアイドル状態の TCP 接続と同じネットワークセグメントにある場合は、アイドル状態の TCP 接続が再利用されます。クライアントがこの要件を満たさない場合は、新しい TCP 接続が確立されます。
IPv6 prefix length	接続再利用のための IPv6 プレフィクス長を指定します。 この設定は、LB デバイスとサーバー間の接続を再利用できるクライアントのネットワークセグメントを制限します。接続要求を開始したクライアントがアイドル状態の TCP 接続と同じネットワークセグメントにある場合は、アイドル状態の TCP 接続が再利用されます。クライアントがこの要件を満たさない場合は、新しい TCP 接続が確立されます。

表 18 TCP アプリケーションパラメーターの構成項目

項目	説明
TCP buffering period	TCP ペイロードマッチングのバッファリング期間を指定します。
TCP maximum buffering size	最大バッファリングサイズを指定します。 最大バッファリングサイズに達すると、デバイスはトラフィックのバッファリングを停止します。
TCP buffering end string	TCP バッファリング終了文字列を設定します。 バッファリング終了文字列を受信すると、デバイスはトラフィックのバッファリングを停止します。

表 19 MySQL パラメーターの構成項目

項目	説明
Connection pool size	接続プールに格納できる TCP 接続の最大数を指定します。

	MySQL データ転送が完了すると、TCP 接続は閉じられるのではなく、接続プールに格納されます。新しい接続要求の場合、デバイスは新しい接続を開く前に、接続プールから使用可能な接続を選択します。
Connection reuse	接続の再利用を有効または無効にします。 この機能を使用すると、LB デバイスは、複数のクライアントが再利用できるサーバーへの接続を確立できます。 この機能は、クライアントとサーバーの間で開かれる接続を減らすのに役立ちます。
Max reuse number	TCP 接続を再利用できる最大回数を設定します。 接続の再利用が有効になると、再利用の最大回数に達するまで TCP 接続は切断されません。TCP 接続が切断されると、新しい接続要求によって新しい TCP 接続の確立がトリガーされます。
Idle timeout time	LB デバイスとサーバー間の TCP 接続のアイドルタイムアウト時間を設定します。アイドルタイムアウト時間は、TCP 接続が切断されるまでアイドル状態を維持できる時間です。TCP 接続が切断された後、新しい接続要求によって新しい TCP 接続の確立がトリガーされます。
IPv4 mask length	接続再利用のための IPv4 マスク長を指定します。 この設定により、LB デバイスとサーバー間の接続を再利用できるクライアントのネットワークセグメントが制限されます。接続要求を開始したクライアントがアイドル状態の TCP 接続と同じネットワークセグメントにある場合、クライアントはアイドル状態の TCP 接続を再利用します。クライアントがこの要件を満たさない場合は、新しい TCP 接続が確立されます。
IPv6 prefix length	接続再利用のための IPv6 プレフィクス長を指定します。 この設定により、LB デバイスとサーバー間の接続を再利用できるクライアントのネットワークセグメントが制限されます。接続要求を開始したクライアントがアイドル状態の TCP 接続と同じネットワークセグメントにある場合、クライアントはアイドル状態の TCP 接続を再利用します。クライアントがこの要件を満たさない場合は、新しい TCP 接続が確立されます。

OK をクリックします。**Parameter Profile** ページに新しいパラメータープロファイルが表示されます。

Configure an intelligent probe template (optional)

HTTP パッシブ、RST、0 ウィンドウ、またはカスタムインテリジェントプローブテンプレートを設定して、単一のサーバーファームメンバーまたはサーバーファーム内のすべてのメンバーを監視できます。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Probe Templates** を選択します。
Create をクリックします。
インテリジェントプローブテンプレートを作成します。

表 20 インテリジェントプローブテンプレートの設定項目

項目	説明
プローブテンプレート名	プローブテンプレートの名前を入力します。大文字と小文字は区別されません。
[タイプ]	インテリジェントプローブテンプレートのタイプを指定します。 **RST**: 実サーバーによって送信される RST パケットの数を監視します。RST プローブテンプレートの設定については、表 23 を参照してください。 **Zero-window**: 実サーバーから送信される 0 ウィンドウパケットの数を監視します。0 ウィンドウプローブテンプレートの設定については、表 23 を参照してください。 **HTTP Passive**: HTTP 応答パケット内の異常な URL の数を監視します。HTTP パッシブプローブテンプレートの構成については、表 24 を参照してください。 **Custom**: カスタムスクリプトファイルを使用して実サーバーの状態を監視します。カスタムプローブテンプレートの構成の詳細は、表 25 を参照してください。
説明	インテリジェントプローブテンプレートの説明を入力します。

表 21 RST および Zero-window プローブテンプレートの設定項目

項目	説明
Monitoring time	監視時間を指定します。監視時間中に、RST または 0 ウィンドウプローブテンプレートが指定されている場合、システムはサーバーファーム内の各サーバーファームメンバーによって送信された RST パケットまたは zero-window パケットの数をカウントします。
Threshold	アクションが実行される前に実サーバーが送信できる RST パケットまたは zero-window パケットの最大数を指定します。
Action	RST または zero-window パケットしきい値に達したときに実行するアクションを指定します。 **Shutdown**: 実サーバーをシャットダウンします。 **Set to busy**: 実サーバーをビジー状態にします。システムは、プローブ間隔で実サーバーのプローブを続行します。送信された RST ま

	たは zero-window パケットの数がプローブ間隔中にしきい値に達しない場合、実サーバーは通常の状態に戻されます。パケット数がしきい値に達すると、システムは最大プローブ時間に達するまで実サーバーをプローブします。すべてのプローブの結果がしきい値に達すると、システムは自動的に実サーバーをシャットダウンします。 パケットしきい値違反またはプローブ時間の超過が原因でシャットダウンされた実サーバーは、インテリジェントプローブテンプレートが削除されるとすぐに通常の状態に復元されます。
Probe interval	ビジー状態の実サーバーをプローブする間隔を指定します。
Probe times	ビジー状態の実サーバーをプローブする最大回数を指定します。値 0 は、プローブ回数に制限がないことを意味します。

表 22 HTTP パッシブプローブテンプレートの設定項目

項目	説明
Monitoring time	監視時間を指定します。監視時間中に、HTTP パッシブプローブテンプレートが指定されている場合、システムは一致する HTTP 要求の応答を監視します。
Threshold	HTTP 応答パケット内の異常な URL の最大数を指定します。異常な URL の数が最大数を超えると、実サーバーはシャットダウンされます。
Timeout time	HTTP パッシブプローブテンプレートのタイムアウト時間を指定します。 デバイスは、指定された URL を持つ HTTP 要求の応答を監視します。HTTP 要求の応答時間がタイムアウト時間を超えると、URL エラーが記録されます。
URLs to check	チェックする URL を構成します。URL に疑問符(?)を含めることはできません。 デバイスは、指定された URL のいずれかを含む HTTP 要求を受信すると、HTTP 要求の応答を監視します。 HTTP パッシブプローブテンプレートには、最大 10 個の URL を設定できます。
Response status code	チェックする応答状況コードを構成します。 HTTP 応答に指定された応答状況コードのいずれかが含まれている場合、URL エラーが記録されます。 HTTP パッシブプローブテンプレートには、最大 10 個の応答ステータスコードを設定できます。

表 23 カスタムプローブテンプレートの設定項目

項目	説明
Monitoring time	監視間隔を指定します。監視間隔になると、指定したスクリプトファイルが実行されます。

Timeout time	応答待ちのタイムアウト時間を指定します。 タイムアウト時間は、監視間隔よりも短く設定することをお勧めします。
Script parameters	スクリプトパラメーターを設定します。 スクリプトファイルを実行すると、デバイスはスクリプトパラメーターをスクリプトファイルに転送します。 スペースで区切られた複数のスクリプトパラメーターがサポートされています。
Script file	スクリプトファイルを選択してインポートします。 デバイスは、スクリプトファイルの検出内容に従って実サーバーの状態を検出します。 デバイスは、**.py** サフィックスを持つスクリプトファイルだけをサポートします。
Environment variable	環境変数を設定します。 環境変数を設定することにより、カスタムスクリプトファイルを実行する環境を指定できます。

OK をクリックします。新しいインテリジェントプローブテンプレートが **Probe Templates** ページに表示されます。

Configure a global SNAT policy (optional)

グローバル SNAT ポリシーは、パケットの送信元 IP アドレスを指定された IP アドレスに変換するために使用されます。SNAT を実装するには、Global SNAT Policy ページでグローバル SNAT ポリシーを設定するか、または Server Farm ページで SNAT を設定します。Server Farm ページの SNAT 設定の方が優先度が高くなります。SNAT 設定のないサーバーファームでは、アドレス変換にグローバル SNAT ポリシーが使用されます。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Global SNAT Policies** を選択します。
Create をクリックします。
グローバル SNAT ポリシーを作成します。

表 24 グローバル SNAT ポリシーの設定項目

項目	説明
Global SNAT policy name	グローバル SNAT ポリシーの名前を入力します。大文字と小文字は区別されません。
SNAT mode	SNAT モードを選択します。

	SNAT Pool: 送信元 IP アドレスを指定された SNAT アドレスプールの IP アドレスに変換します。 **Auto mapping**: 送信元 IP アドレスを、実サーバーに接続しているインターフェースの IP アドレスに変換します。
SNAT pool name	既存の SNAT プールを選択するか、SNAT プールを作成します。 このパラメーターは、SNAT モードが SNAT プールである場合にだけサポートされます。
VRF	グローバル SNAT ポリシーが属する VPN インスタンスを指定します。
Priority	グローバル SNAT ポリシーのプライオリティを設定します。 異なるプライオリティを持つ複数のグローバル SNAT ポリシーを設定できます。これらはプライオリティ値の降順で照合されます。
Source IP address object group	アドレス変換の送信元 IP アドレスオブジェクトグループを指定します。デバイスは、送信元 IP アドレスが一致するパケットに対してだけ SNAT を実行します。
Destination IP address object group	アドレス変換の宛先 IP アドレスオブジェクトグループを指定します。デバイスは、宛先 IP アドレスが一致するパケットに対してだけ SNAT を実行します。
Service object group	アドレス変換のサービスオブジェクトグループを指定します。デバイスは、サービスが一致するパケットに対してだけ SNAT を実行します。
Policy status	グローバル SNAT ポリシーをイネーブルまたはディセーブルにします。
Description	グローバル SNAT ポリシーの説明を入力します。

OK をクリックします。新しいグローバル SNAT ポリシーが **Global SNAT Policy** ページに表示されます。

Configure a virtual server

仮想サーバーは、LB デバイスで受信されたパケットのロードバランシングを実行するかどうかを決定するために LB デバイスによって提供される仮想サービスです。仮想サーバーと一致するパケットだけがロードバランシングされます。

サーバーロードバランシングでサポートされる仮想サーバータイプには、IP、TCP、UDP、SIP-TCP、SIP-UDP、HTTP、Performance(HTTP)、HTTPS、HTTP リダイレクション、RADIUS、および MySQL があります。UDP および SIP-UDP タイプの仮想サーバーには同じ VSIP およびポート番号を指定しないでください。TCP、SIP-TCP、HTTP、Performance(HTTP)、HTTPS、HTTP リダイレクション、RADIUS、および MySQL タイプの仮想サーバーには同じ VSIP およびポート番号を指定しないでください。LB デバイ

スでパケットを正しく処理するには、Performance(HTTP)仮想サーバーと TCP クライアント検証機能を同時に設定しないでください。TCP クライアント検証機能の詳細については、**Policies** > **Attack Defense** > **Protected IP Addresses** を選択して、ジアタック防御のヘルプを参照してください。

手順

Policies > **Load Balancing** > **Server Load Balancing** > **Virtual Servers** を選択します。
Create をクリックします。
仮想サーバーを作成します。

表 25 基本構成項目

項目	説明
Virtual server name	仮想サーバーの名前を入力します。大文字と小文字は区別されません。
Type	仮想サーバーのタイプを指定します。指定できるタイプは、IP、TCP、UDP、SIP-TCP、SIP-UDP、HTTP、Performance(HTTP)、HTTPS、HTTP リダイレクション、RADIUS、または MySQL です。
IPv4 address	仮想サーバーの IPv4 アドレス/マスク長(0～32)を設定します。 レイヤー4 サーバーロードバランシングで AFT を使用する場合、仮想サーバーIP アドレスとしてサブネットアドレスを指定できません。仮想サーバーIP アドレスのマスク長が 32 ビットであることを確認してください。
IPv6 address	仮想サーバーの IPv6 アドレス/プレフィクス長(0～128)を設定します。 レイヤー4 サーバーロードバランシングで AFT を使用する場合、仮想サーバーの IPv6 アドレスとしてサブネットアドレスを指定できません。仮想サーバーの IPv6 アドレスのプレフィクス長が 128 ビットであることを確認してください。
Port number	仮想サーバーのポート番号を構成します。0 は任意のポートを示します。 IP、TCP、UDP および RADIUS 仮想サーバータイプの場合は、最大 32 個のポート番号アイテムのカンマ区切りリストを入力できます。各アイテムには、ポート番号またはポート番号の範囲(5,10,20-28 など)を指定します。
UDP per-packet load balancing	仮想サーバーの UDP トラフィックに対するパケット単位のロードバランシングを有効または無効にします。 UDP トラフィックのパケット単位のロードバランシングがディセーブルの場合、LB デバイスは、アプリケーションタイプに従って仮想サーバーに一致するトラフィックを分散します。同じアプリケーションタイプのトラフィックは 1 つの実サーバーに分散されます。UDP トラフィックのパケット単位のロードバランシングがイネーブルの場合、LB デバイスは、仮想サーバーに一致するトラフィックをパケット単位で分散します。

	このパラメーターは、UDP タイプ、SIP-UDP タイプ、および RADIUS タイプの仮想サーバーだけでサポートされます。
SSL server policy	LB デバイス(SSL サーバー)と SSL クライアント間のトラフィックを暗号化するための仮想サーバーの SSL サーバーポリシーを指定します。 既存の SSL サーバーポリシーを選択することも、SSL サーバーポリシーを作成することもできます。 このパラメーターは、TCP および HTTPS タイプの仮想サーバーでのみサポートされます。
Redirection URL	仮想サーバーのリダイレクト URL を指定します。大文字と小文字は区別されます。リダイレクト機能は、仮想サーバーに一致するすべての要求パケットを URL にリダイレクトします。 リダイレクト URL として疑問符(?) または次の文字列を指定することもできます。 **%h**: クライアント要求パケット内のホスト名を指定します。 **%p**: クライアント要求パケット内の URL を指定します。 **%%**: パーセント記号(%)を指定します。 このパラメーターは、HTTP リダイレクトタイプの仮想サーバーでのみサポートされます。
Redirection mode	仮想サーバーのリダイレクションモードを指定します。 Temporary-302 Temporary-307 Permanent-301 このパラメーターは、HTTP リダイレクトタイプの仮想サーバーでのみサポートされます。
Server farm	既存のサーバーファームを選択するか、仮想サーバー用のサーバーファームを作成します。 このパラメーターは、HTTP リダイレクトタイプの仮想サーバーではサポートされません。
Sticky group of the server farm	既存のスティッキグループを選択するか、またはサーバーファームのプライマリスティッキグループとしてスティッキグループを作成します。 このパラメーターは、HTTP リダイレクトタイプの仮想サーバーではサポートされません。
VRRP-group-associated interface	VRRP グループに関連付けるインターフェースを指定します。 このパラメーターを設定する場合は、VRRP グループ番号を仮想サーバーにバインドする必要があります。
VRRP group number	仮想サーバーにバインドする VRRP グループの番号を指定します。

	High Availability(HA;ハイアベイラビリティ)グループのデュアルアクティブモードでは、両方のデバイスが相互にバックアップし、サービスを処理します。VRRP グループ番号を仮想サーバーにバインドしない場合、両方のデバイスがサービスを処理し、SNAT アドレスプールを使用します。VRRP グループ番号を仮想サーバーにバインドした場合、プライマリデバイスだけがサービスを処理し、SNAT アドレスプールを使用します。HA グループの詳細については、オンラインヘルプを参照してください。 この設定は、IPv4 アドレスを持つ仮想サーバーだけに適用されます。 このパラメーターを設定できるのは、VRRP グループ関連インターフェースを指定した後だけです。
IPv6 VRRP-group-associated interface	IPv6 VRRP グループに関連付けるインターフェースを指定します。 このパラメーターを設定する場合は、IPv6 VRRP グループ番号を仮想サーバーにバインドする必要があります。
IPv6 VRRP group number	仮想サーバーにバインドする IPv6 VRRP グループの数を指定します。 デュアルアクティブ HA ネットワークでは、両方のデバイスが相互にバックアップし、サービスを処理します。仮想サーバーに IPv6 VRRP グループ番号をバインドしない場合、両方のデバイスがサービスを処理し、SNAT アドレスプールを使用します。仮想サーバーに IPv6 VRRP グループ番号をバインドする場合、プライマリデバイスだけがサービスを処理し、SNAT アドレスプールを使用します。HA の詳細については、オンラインヘルプを参照してください。 この設定は、IPv6 アドレスを持つ仮想サーバーだけに適用されます。 このパラメーターを設定できるのは、IPv 6-VRRP グループ関連インターフェースを指定した後だけです。
MySQL version	MySQL データベースのバージョンを指定します。 LB デバイスは、MySQL サーバーに代わってクライアントへの認証を開始し、指定された MySQL バージョンのデータベース初期化パケットをクライアントに送信します。
Read/Write splitting	読み取り/書き込みスプリットを有効または無効にします。 この機能を使用すると、読み取りコマンドと書き込みコマンドをそれぞれ読み取りサーバーファームと書き込みサーバーファームで実行できます。 この機能は、同時読み取り/書き込み要求がデータベースパフォーマンスに与える影響を軽減するのに役立ちます。 この機能をイネーブルにした後は、読み取りサーバーファームと書き込みサーバーファームの両方を設定する必要があります。
Read server farm	既存のサーバーファームを選択するか、仮想サーバーの読み取りサーバーファームとしてサーバーファームを作成します。

	このパラメーターは、読み取り/書き込みスプリットが有効な場合にのみ使用できます。
Read sticky group	既存のスティッキグループを選択するか、または仮想サーバーの読み取りスティッキグループとしてスティッキグループを作成します。 このパラメーターは、読み取り/書き込みスプリットが有効な場合にのみ使用できます。
Write server farm	既存のサーバーファームを選択するか、仮想サーバーの書き込みサーバーファームとしてサーバーファームを作成します。 このパラメーターは、書き込み/書き込みスプリットが有効な場合にのみ使用できます。
Write sticky group	仮想サーバーの書き込みスティッキグループとして、既存のスティッキグループを選択するか、またはスティッキグループを作成します。 このパラメーターは、書き込み/書き込みスプリットが有効な場合にのみ使用できます。
Interfaces for sending gratuitous ARP/ND packets	余計な ARP パケットおよび ND パケットを送信するためのインターフェースを指定します。 クライアントに接続されているインターフェースの IP アドレスが、仮想サーバーの IP アドレスと同じネットワークセグメントにある場合は、次の作業を実行する必要があります。 対応するクライアントに接続されているインターフェースを、余計な ARP/ND パケットを送信するためのインターフェースとして指定します。 IP アドレスアドバタイズメントをイネーブルにします。
Operation mode	仮想サーバーの動作モード: Layer 4。 Layer 7。 このパラメーターは、TCP 仮想サーバーでのみサポートされます。
IP address advertisement	仮想サーバーの IP アドレスアドバタイズメントを有効または無効にします。この機能が設定されると、デバイスはルート計算のために仮想サーバーの IP アドレスを OSPF にアドバタイズします。データセンターのサービスが別のデータセンターに切り替わると、仮想サーバーへのトラフィックもそのデータセンターに切り替えられます。
Redundancy group traffic distribution	既存の冗長グループを選択するか、冗長グループを作成します。仮想サーバーと一致するトラフィックは、指定した冗長グループに転送されます。 冗長グループが存在しないか、有効なフェールオーバーグループが含まれていない場合、この機能は有効になりません。 この機能のサポートは、デバイスモデルによって異なります。

Session extension information synchronization	仮想サーバーのセッション拡張情報の同期を有効または無効にします。 このパラメーターは、IP、TCP、UDP、SIP-TCP、SIP-UDP、および RADIUS タイプの仮想サーバーでのみサポートされます。
Sticky entry synchronization	仮想サーバーのスティッキエントリの同期をイネーブルまたはディセーブルにします。 次の設定変更により、デバイスは既存のスティッキエントリを削除し、後続のトラフィックに基づいて新しいスティッキエントリを生成します。 スティッキエントリの同期化をディセーブルにします。 スティッキエントリの同期タイプを変更します。 このパラメーターは、HTTP リダイレクトタイプの仮想サーバーではサポートされません。
Sticky entry synchronization type	スティッキエントリの同期タイプを選択します。 **Intra-group synchronization**: 同じフェールオーバーグループ内のデバイスにスティッキエントリを同期します。 **Global synchronization**: すべてのフェールオーバーグループ内のデバイスにスティッキエントリを同期します。 この機能は、スティッキエントリの同期化がイネーブルになっている場合にだけ使用できます。 HTTP リダイレクションタイプの仮想サーバーは、この機能をサポートしていません。 この機能のサポートは、デバイスモデルによって異なります。
Virtual server feature	仮想サーバーを有効または無効にします。 仮想サーバーを設定したら、仮想サーバーを有効にして動作させる必要があります。
Fast log output	高速ログ出力機能を使用して、出力する内容を設定します。 複数のセミコロンで区切られた変数がサポートされています。デバイスは次の変数をサポートしています: **%{is}**: HTTP 要求内の送信元 IP アドレス。 **%{ps}**: HTTP 要求内の送信元ポート番号。 **%{id}**: HTTP 要求の宛先 IP アドレス。 **%{pd}**: HTTP 要求の宛先ポート番号。 **%{sis}**: HTTP 応答の送信元 IP アドレス。 **%{sps}**: HTTP 応答の送信元ポート番号。 **%{sid}**: HTTP 応答の宛先 IP アドレス。 **%{spd}**: HTTP 応答の宛先ポート番号。 **%{vsn}**: 仮想サーバー名。 **%{sfn}**: サーバーファーム名。 **%{reqtmstamp}**: HTTP 要求のタイムスタンプ。

	%{uri}: HTTP URI。 **%{ver}**: HTTP バージョン番号。 **%{args}**: HTTP アクセスパラメーター。 **%{method}**: HTTP 要求方式。 **%{xff}**: XFF(X-Forwarded-For)の IP アドレス。 **%{ctype}**: HTTP 要求の Content-Type フィールド。 **%{clen}**: HTTP 要求の Content-Length フィールド。 **%{ref}**: HTTP 要求内の Referer ヘッダーフィールド。 **%{ua}**: HTTP 要求内の User-Agent ヘッダーフィールド。 **%{host}**: HTTP 要求のホストヘッダーフィールド。 **%{path}**: HTTP 要求内のパス。 **%{reqsz}**: HTTP 要求のサイズ(バイト単位)。 **%{reqtm}**: HTTP 要求の期間(ミリ秒単位)。期間は、デバイスが HTTP 要求を受信してから HTTP 応答を受信するまでの時間です。 **%{rspclen}**: HTTP 応答の Content-Type フィールド。 **%{reqsz}**: HTTP 応答のサイズ(バイト単位)。 **%{rsptm}**: HTTP 応答時間(ミリ秒単位)。時間は、デバイスが HTTP 応答を受信してから、デバイスが HTTP 応答の送信を終了するまでの時間です。 **%{stscode}**: HTTP 応答ステータスコード。 **%{reqbsz}**: HTTP 要求の本文のサイズ(バイト単位)。 **%{rspbsz}**: デバイスがサーバーから受信した HTTP 応答の本文サイズ(バイト単位)。 **%{rspsntbsz}**: デバイスからクライアントに送信される HTTP 応答の本文のサイズ(バイト単位)。 **%{cookie_cookie-name}**: HTTP Cookie 名。大文字と小文字が区別されます。Cookie 名には、大カッコ({}、()、[]、<>)、アットマーク(@)、カンマ(,)、セミコロン(;)、コロン(:)、バックスラッシュ(¥)、引用符(")、スラッシュ(/)、疑問符(?) 、等号 (=) 、スペース文字 (SP)、水平タブ (HT)は使用できません。また、Cookie 名には、31 以下または 127 以上の ASCII コードは使用できません。複数の Cookie を指定できます。 このパラメーターは、HTTP および HTTPS 仮想サーバーでのみサポートされます。
Description	仮想サーバーの説明を入力します。
User list	MySQL サーバーへのログインに使用するユーザー名とパスワードを設定します。

	Create をクリックしてユーザーを作成します。 ユーザー名:ユーザー名を入力します。 パスワード:パスワードを入力します。 **OK** をクリックします。新しいユーザーがユーザーリストに表示されます。 デバイスは最大 100 人のログインユーザーをサポートします。
External link domain name rewrite	外部リンクプロキシを有効または無効にします。 外部リンクプロキシ機能を使用すると、LB デバイスは外部リンクプロキシとして動作し、IPv6 クライアントに代わって IPv4 リソースを要求できます。この機能により、IPv4 から IPv6 へのネットワーク移行が円滑に行われます。 LB デバイスは、サーバーからの HTTP 応答で外部リンクを検出すると、外部リンクを書き直すためのスクリプトファイルを戻します。クライアントはスクリプトファイルを実行し、指定されたパラメーターを外部リンクのドメイン名に追加します。パラメーターには、URI、ドメイン名接尾辞および仮想サーバーポート番号が含まれます。変更されたドメイン名を含む DNS 要求を受信すると、LB デバイスは IPv6 クライアントに代わって関連する IPv4 リソースを要求します。 書き換え後のドメイン名の形式は、プロトコル type://original ドメイン名+URI+ドメイン名サフィックス+:仮想サーバーポート番号です。プロトコルタイプは HTTP または HTTPS です。 プロトコルタイプが HTTP、元の外部リンクのドメイン名が **www.aaa.com**、URI が **proxy**、ドメイン名サフィックスが **bbb.com**、仮想サーバーポート番号が **8080** であり、書き換え後の外部リンクドメイン名が **http://www.aaa.com.proxy.bbb.com:8080** であるとします。
URI	外部リンクのドメイン名を書き直すための URI を指定します。URI は大文字と小文字を区別しない文字列で、文字、数字、ハイフン(-)およびアンダースコア(_)のみを使用できます。 LB デバイスは、IPv6 サイトサーバーからの応答を受信すると、関連付けられたドメイン名に指定されたパラメーターを追加して、応答内の IPv4 外部リンクを書き換えます。パラメーターには、URI、ドメイン名サフィックス、および仮想サーバーポート番号が含まれます。元の外部リンクのドメイン名が **http://www.aaa.com**,URI は **proxy**、ドメイン名サフィックスが **bbb.com**、および仮想サーバーポート番号が **8080** であるとします。書き換え後の外部リンクドメイン名は **http://www.aaa.com.proxy.bbb.com:8080** です。この変更されたドメイン名を含む DNS 要求を受信すると、LB デバイスは次の操作を実行します。 元のドメイン名を抽出します。 IPv6 クライアントに代わって、関連する IPv4 リソースを要求します。

	取得した IPv4 リソースを IPv6 クライアントに返します。
Domain name suffix	外部リンクのドメイン名を書き直すためのドメイン名サフィックスを指定します。 ドメイン名の接尾辞は、大文字と小文字を区別するドット区切りの文字列です。ドメイン名の各ドット区切りのラベルには、最大 63 文字を使用できます。ドメイン名には、文字、数字、ハイフン(-)、アンダースコア(_)およびドット(.)を使用できます。
SNAT address pool	外部リンクプロキシ用の SNAT アドレスプールを指定します。 外部リンクプロキシとして IPv4 リソースを要求する場合、LB デバイスは指定された SNAT プールから IP アドレスを選択します。LB デバイスはこの IP アドレスをクライアント IP アドレスとして使用して、IPv6 クライアントの代わりに要求を開始します。 SNAT アドレスプールを指定しない場合、LB デバイスはサーバーへの出力インターフェースの IP アドレスをクライアント IP アドレスとして使用します。
SNAT address pool	外部リンクプロキシ用の SNAT アドレスプールを指定します。 外部リンクプロキシとして IPv4 リソースを要求する場合、LB デバイスは指定された SNAT プールから IP アドレスを選択します。LB デバイスはこの IP アドレスをクライアント IP アドレスとして使用して、IPv6 クライアントの代わりに要求を開始します。 トラフィック分散モードを設定する場合は、SNAT アドレスプールを指定する必要があります。トラフィック分散をディセーブルにする場合は、SNAT アドレスプールを指定するかどうかを選択できます。 SNAT アドレスプールを指定しない場合、LB デバイスはサーバーへの出力インターフェースの IP アドレスをクライアント IP アドレスとして使用します。
Allowlists	外部リンクプロキシの許可リストにドメイン名を追加します。 ドメイン名を入力します。大文字と小文字は区別され、ドットで区切られた文字列です。ドメイン名のドットで区切られた各ラベルには、最大 63 文字を使用できます。ドメイン名には、文字、数字、ハイフン(-)、アンダースコア(_)およびドット(.)を使用できます。 **Add** をクリックします。ドメイン名が **Allowlists** に表示されます。 LB デバイスは、許可リスト内のドメイン名を含む外部リンクを書き換えません。

表 26 高度な構成項目

項目	説明

Scheduling resources-Backup server farm	仮想サーバーのバックアップサーバーファームを指定します。 プライマリサーバーファームが使用可能な場合(実サーバーが含まれている場合)、仮想サーバーはプライマリサーバーファームを介してパケットを転送します。プライマリサーバーファームが使用できない場合、仮想サーバーはバックアップサーバーファームを介してパケットを転送します。 既存のサーバーファームを選択することも、サーバーファームを作成することもできます。
Scheduling resources-Backup sticky group of the server farm	サーバーファームのバックアップスティッキグループを指定します。 プライマリスティッキグループとバックアップスティッキグループの両方を指定すると、プライマリスティッキエントリとバックアップスティッキエントリの両方が生成されます。パケットがプライマリスティッキエントリと一致しない場合は、バックアップスティッキエントリを使用してパケットが照合されます。 このパラメーターは、HTTP、HTTPS、および RADIUS タイプの仮想サーバーでのみサポートされます。
Scheduling resources-Load balancing policy	仮想サーバーの LB ポリシーを指定します。 LB ポリシーを使用することにより、仮想サーバーはパケットの内容に基づいてパケットを照合するロードバランシングを実装します。 既存の LB ポリシーを選択することも、LB ポリシーを作成することもできます。 仮想サーバーは、指定したタイプのポリシーテンプレートを使用できます。たとえば、Performance(HTTP)または HTTP タイプの仮想サーバーは、汎用タイプまたは HTTP タイプのポリシーテンプレートを使用できます。IP、TCP、UDP、SIP-TCP または SIP-UDP タイプの仮想サーバーは、汎用タイプのポリシーテンプレートのみを使用できます。RADIUS タイプの仮想サーバーは、汎用タイプまたは RADIUS タイプのポリシーテンプレートのみを使用できます。
Scheduling resources-Connection limit policy	仮想サーバーの接続数を制限するために、仮想サーバーの接続制限ポリシーを指定します。 既存の接続制限ポリシーを選択することも、接続制限ポリシーを作成することもできます。
Scheduling resources-SSL client policy	LB デバイス(SSL クライアント)と SSL サーバー間のトラフィックを暗号化するための仮想サーバーの SSL クライアントポリシーを指定します。 既存の SSL クライアントポリシーを選択することも、SSL クライアントポリシーを作成することもできます。 このパラメーターは、HTTPS タイプの仮想サーバーでのみサポートされます。
Scheduling resources-SSL server policy with SNI	仮想サーバーの SNI を使用して SSL サーバーポリシーを設定します。

	Add をクリックして、SNI を使用する SSL サーバーポリシーを作成します。 ポリシー名:ポリシー名を入力します。大文字と小文字は区別されません。 Server name indication(SNI):SNI を入力します。大文字と小文字は区別されません。 **OK** をクリックします。新しい SSL サーバーポリシーがポリシーリストに表示されます。 SNI のない SSL サーバーポリシーと SNI のある SSL サーバーポリシーの両方を設定した場合、SNI のない SSL サーバーポリシーが有効になります。 仮想サーバーに同じ SNI を使用して複数の SSL サーバーポリシーを設定することはできません。 このパラメーターは、HTTPS タイプの仮想サーバーでのみサポートされます。
Scheduling resources-Cookie sticky group	仮想サーバーの cookie スティッキグループを指定します。 また、**Create Virtual Server** ページまたは≪アクションの作成 **Create Action** ページで、サーバーファームに関連付けるスティッキグループを指定することもできます。仮想サーバーに指定された Cookie スティッキグループの優先度が最も高くなります。このグループは、スティッキエントリの生成に優先的に使用されます。 このパラメーターに指定できるのは、cookie スティッキグループだけです。
Scheduling resources-VPN instance	仮想サーバーの VPN インスタンスを指定します。 既存の VPN インスタンスを選択することも、VPN インスタンスを作成することもできます。
Protection policy-HTTP protection policy	仮想サーバーの HTTP 保護ポリシーを指定して、保護ポリシーに一致する攻撃トラフィックから保護します。 既存の HTTP 保護ポリシーを選択することも、HTTP 保護ポリシーを作成することもできます。
Parameter profile-IP parameter profile	仮想サーバーがパラメータープロファイルに基づいて一致するトラフィックを処理するための IP パラメータープロファイルを指定します。 既存の IP パラメータープロファイルを選択するか、または IP パラメータープロファイルを作成できます。
Parameter profile-TCP parameter profile (client side)	仮想サーバーがパラメータープロファイルに基づいて一致するトラフィックを処理するための TCP パラメータープロファイルを指定します。仮想サーバーが使用する TCP パラメータープロファイル(クライアント)は、デバイスとクライアント間の TCP 接続を処理し、最適化します。

	既存の TCP パラメータープロファイルを選択するか、、TCP パラメータープロファイルを作成することもできます。 このパラメーターは、TCP、Performance(HTTP)、HTTP、HTTPS、または MySQL タイプの仮想サーバーでのみサポートされます。
Parameter profile-TCP parameter profile (server side)	仮想サーバーがパラメータープロファイルに基づいて一致するトラフィックを処理するための TCP パラメータープロファイルを指定します。仮想サーバーが使用する TCP パラメータープロファイル(サーバー)は、デバイスとサーバー間の TCP 接続を処理し、最適化します。 既存の TCP パラメータープロファイルを選択するか、TCP パラメータープロファイルを作成することもできます。 このパラメーターは、TCP、Performance(HTTP)、HTTP、HTTPS、または MySQL タイプの仮想サーバーでのみサポートされます。
Parameter profile-TCP-application parameter profile	仮想サーバーがパラメータープロファイルに基づいて一致するトラフィックを処理するための TCP アプリケーションパラメータープロファイルを指定します。 既存の TCP アプリケーションパラメータープロファイルを選択するか、または TCP アプリケーションパラメータープロファイルを作成できます。 このパラメーターは、レイヤー7 で動作する TCP 仮想サーバーだけでサポートされます。
Parameter profile-HTTP parameter profile	仮想サーバーがパラメータープロファイルに基づいて一致するトラフィックを処理するための HTTP パラメータープロファイルを指定します。 既存の HTTP パラメータープロファイルを選択することも、HTTP パラメータープロファイルを作成することもできます。 このパラメーターは、Performance(HTTP)、HTTP、または HTTPS タイプの仮想サーバーでのみサポートされます。
Parameter profile-HTTP statistics parameter profile	仮想サーバーがパラメータープロファイルに基づいて一致するトラフィックを処理するための HTTP 統計情報パラメータープロファイルを指定します。 既存の HTTP 統計情報パラメータープロファイルを選択するか、または HTTP 統計情報パラメータープロファイルを作成できます。 このパラメーターは、HTTP タイプの仮想サーバーでのみサポートされます。
OneConnect parameter profile	パラメータープロファイルに基づいて一致するトラフィックを処理するために、仮想サーバーの OneConnect パラメータープロファイルを指定します。 既存の OneConnect パラメータープロファイルを選択するか、OneConnect パラメータープロファイルを作成できます。 このパラメーターは、HTTP または HTTPS タイプの仮想サーバーでのみサポートされます。
MySQL parameter profile	パラメータープロファイルに基づいて一致するトラフィックを処理するために、仮想サーバーの MySQL パラメータープロファイルを指定します。

	既存の MySQL パラメータープロファイルを選択するか、MySQL パラメータープロファイルを作成できます。 このパラメーターは、MySQL タイプの仮想サーバーでのみサポートされます。
QoS-Maximum connections	仮想サーバーの最大接続数を指定します。0 は制限なしを意味します。
QoS-Maximum connections per second	仮想サーバーの 1 秒あたりの最大接続数を指定します。0 は無制限を意味します。
QoS-Maximum bandwidth	仮想サーバーの最大帯域幅を指定します。0 は制限なしを意味します。
QoS-Maximum inbound bandwidth	仮想サーバーの最大インバウンド帯域幅を指定します。0 は制限なしを意味します。
QoS-Maximum outbound bandwidth	仮想サーバーの最大アウトバウンド帯域幅を指定します。0 は制限なしを意味します。
Content security-Content security function	コンテンツセキュリティを有効または無効にします。
Content security-WAF profile	仮想サーバーと一致する Web アプリケーションのトラフィック保護に使用する WAF プロファイルを指定します。 WAF プロファイルの詳細については、WAF のオンラインヘルプを参照してください。
Content security-IPS profile	仮想サーバーと一致するトラフィックの侵入保護に使用する IPS プロファイルを指定します。 IPS プロファイルの詳細については、IPS のオンラインヘルプを参照してください。
Content security-Anti-virus profile	仮想サーバーと一致するトラフィックのアンチウイルス保護に使用するアンチウイルス保護コンフィギュレーションファイルを指定します。 アンチウイルスプロファイルの詳細については、アンチウイルスのオンラインヘルプを参照してください。

OK をクリックします。**Virtual Server** ページに新しい仮想サーバーが表示されます。

NetShare control

このヘルプには、次のトピックがあります。

Introduction

NetShare コントロールを使用すると、ネットワーク共有動作を識別して制御できます。

Basic concepts

Max terminals per IP

IP アドレスを共有できる端末の最大数を指定します。
NetShare コントロールは、パケットの送信元 IP アドレスを共有する端末の数に基づいて、パケットのアクションを決定します。

IP アドレスを共有する端末の数が制限を超えると、NetShare ポリシーで指定されたアクションが実行されます。
IP アドレスを共有する端末の数が制限を下回る場合は、パケットの通過が許可されます。

Freeze and unfreeze

IP アドレスが凍結されると、その IP アドレスから送信されたすべてのパケットがドロップされます。
デバイスは、次の条件が満たされると、凍結時間の間、IP アドレスを自動的に凍結します。
IP アドレスを共有する端末数が、**Max terminals per IP** の制限を超えています。

Freeze アクションは、**Max terminals per IP** の制限を超える端末によって共有される IP アドレスに対して設定されます。

NetShare Control > **NetShare List** ページで、IP アドレスを手動でフリーズまたはフリーズ解除するこ

ともできます。

NetShare list

NetShare リストには、端末間で共有されていることが検出されたすべての IP アドレスとその関連情報が表示されます。次のような情報があります。

Position:
User name。
VRF。
Number of terminals sharing the IP address。
NetShare policy name。

IP アドレスが凍結されているかどうか。凍結されている場合は、凍結時間が経過するまでの残り時間。

NetShare リストにアクセスするには、ナビゲーションペインで **NetShare Control** > **NetShare List** を選択します。

NetShare detection methods

端末のネットワーク共有動作を検出するには、次の方法があります。

APR-based detection: デバイスは、Application Recognition(APR)に基づいてパケット内のアプリケーション情報を抽出し、NetShare の動作を検出します。

IPID trail tracking: デバイスはパケット内の IPID フィールドの値を追跡して、NetShare 動作を検出します。

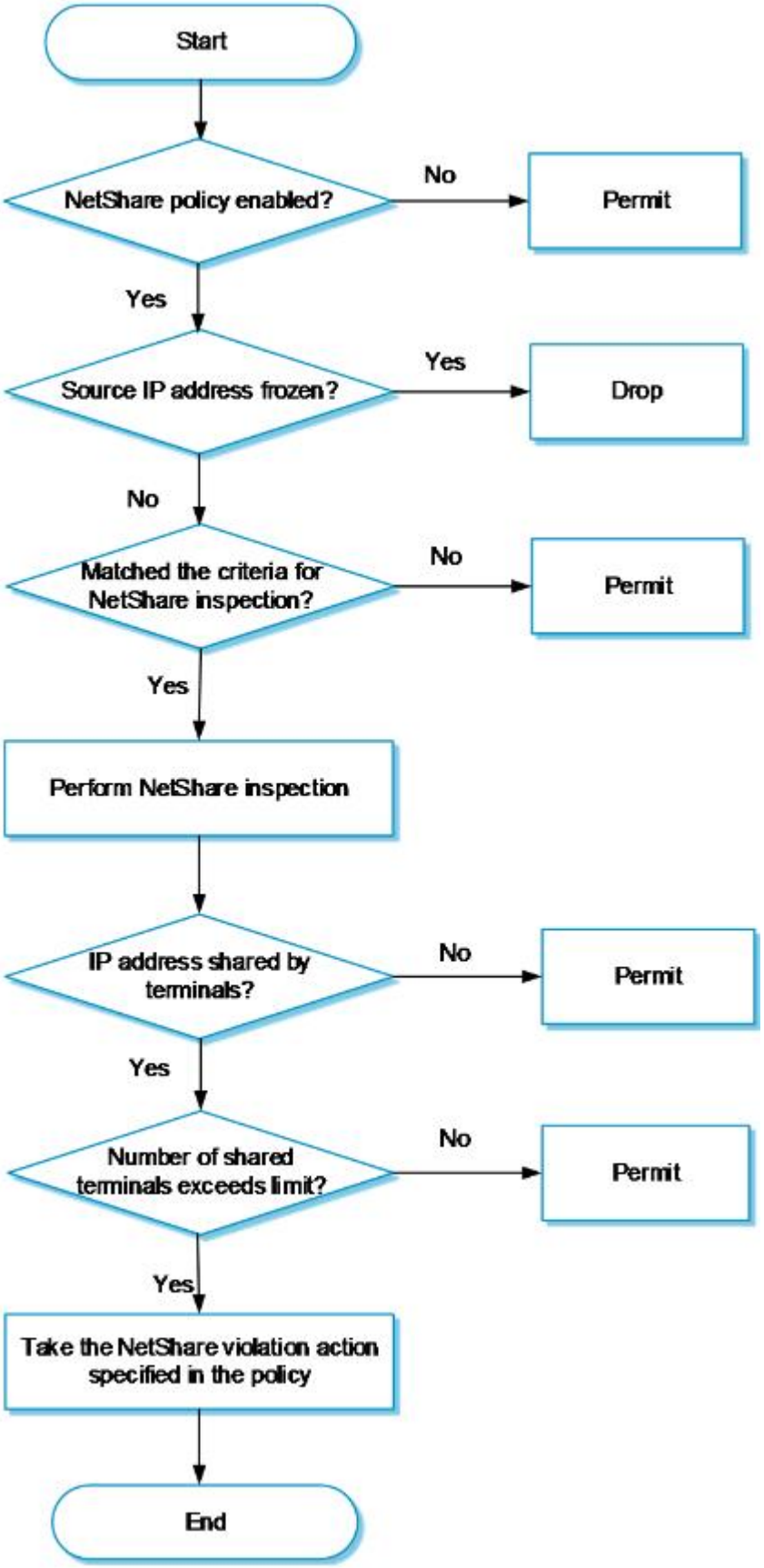
同じホストから送信されたパケットには、ランダムな番号で始まる一意の連続パターンの増分 IPID 値が含まれています。NetShare コントロールは、同じ IP アドレスから送信されたパケットの IPID 値を追跡します。期間内のパケットの IPID 値が同じ一意の連続パターンに属している場合、1 つの端末のみがその IP アドレスを使用します。IPID 値が異なる連続パターンに属している場合、送信元 IP アドレスは複数の端末で共有されます。

NetShare control mechanism

図 1 に示すように、NetShare 制御モジュールはパケットを次のように処理します。
NetShare ポリシーを有効にするかどうかを指定します。
ポリシーが無効になっている場合、NetShare コントロールはパケットの通過を許可します。
ポリシーが有効な場合、NetShare の制御は手順 2 に進みます。

パケットの送信元 IP アドレスが凍結されているかどうかを確認します。
「はい」の場合、NetShare 制御はパケットをドロップします。
そうでない場合、NetShare 制御はステップ 3 に進みます。
パケットを NetShare ポリシーのフィルタと比較して、パケットがポリシーに一致するかどうかを判断します。
パケットがポリシーに一致しない場合、NetShare コントロールはパケットの通過を許可します。
パケットがポリシーに一致する場合、NetShare 制御はステップ 4 に進みます。
パケットの送信元 IP アドレスが複数の端末で共有されているかどうかを確認します。
そうでない場合、NetShare コントロールはパケットのパススルーを許可します。
yes の場合、NetShare コントロールはさらに、IP アドレスを共有する端末の数が **Max terminals per IP** の制限を超えているかどうかを判断します。
制限を超えると、NetShare コントロールは NetShare ポリシーで指定されたアクションを実行します。
制限を超えていない場合、NetShare コントロールはパケットの通過を許可します。

図 1 NetShare の制御メカニズム

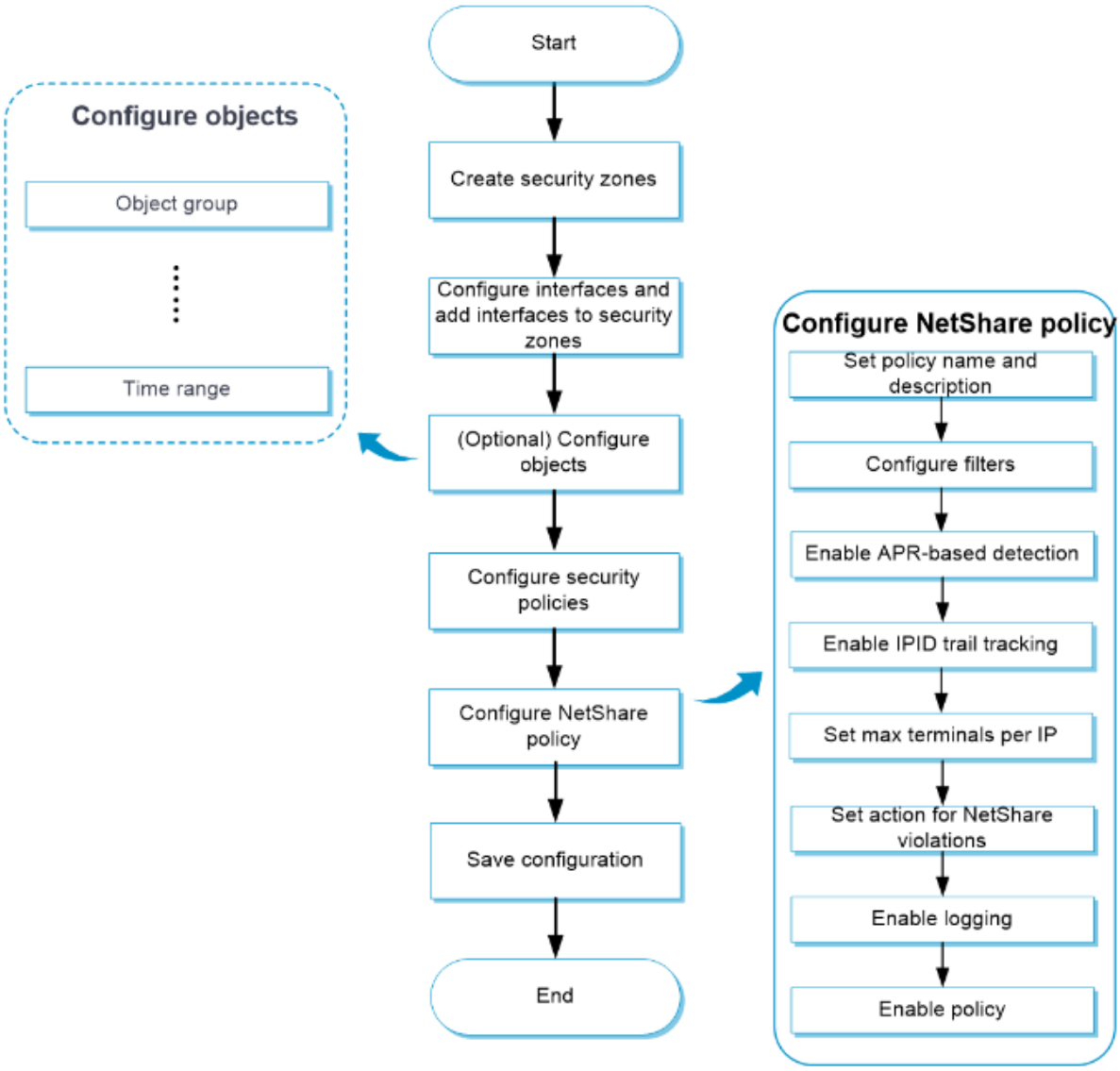

Start
NetShare policy enabled?
No
Permit
Yes
Source IP address frozen?
Yes
Drop
No
Matched the criteria for NetShare inspection?
No
Permit
Yes
Perform NetShare inspection
IP address shared by terminals?
No
Permit
Yes
Number of shared terminals exceeds limit?
No
Permit
Yes
Take the NetShare violation action specified in the policy
End

Restrictions and guidelines

NetShare ポリシーを作成または削除した後は、NetShare ポリシーを有効にするためにアクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化することも、既定で 40 秒後に構成が自動的にアクティブ化されるようにすることもできます。**Submit** をクリックすると、DPI サービスの処理が一時的に中断され、その結果、他の DPI ベースのサービスが中断されることがあります。たとえば、セキュリティーポリシーではアプリケーションのアクセス制御を実装できません。
NetShare 制御は、セキュリティーポリシーによって許可されたトラフィックにのみ適用されます。セキュリティーポリシーの詳細については、セキュリティーポリシーのヘルプを参照してください。
この機能を使用する前に、APR シグニチャライブラリを最新バージョンにアップグレードしてください。
デバイスがサポートする NetShare 制御ポリシーは 1 つだけです。これは手動で作成する必要があります。
APR ベースの検出を使用して NetShare の動作を検出する場合は、次の規則に従います。
この検出方法では、QQ や WeChat などの特定のアプリケーションだけを検査します。
アプリケーションが暗号化されている場合、この検出方式ではアプリケーションを検査できません。
IPID 追跡を使用して NetShare の動作を検出する場合は、次の規則に従います。
この機能は、Windows システムを実行している端末の検出と、IPID フィールドの値が定期的に変化するパケットの検出をサポートします。モバイル端末はサポートされません。
この検出方式は、IPv4 パケットの検査をサポートします。

Configure NetShare control

NetShare コントロールを図 2 のように設定します。
図 2 NetShare コントロールの設定手順



Configure a NetShare policy

手順

Policies タブをクリックします。

ナビゲーションペインで、**NetShare Control** > **NetShare Policy** を選択します。

NetShare ポリシーを作成します。

表 1 NetShare ポリシーの構成項目

項目	説明
Name	NetShare ポリシーの名前を入力します。
Description	NetShare ポリシーの説明を入力します。

Src security zones	ポリシーが適用されるソースセキュリティゾーンを指定します。
Dst security zones	ポリシーを適用する宛先セキュリティゾーンを指定します。
Src IP addresses	ポリシーを適用する送信元 IP アドレスを指定します。
Dst IP addresses	ポリシーを適用する宛先 IP アドレスを指定します。
User	ポリシーを適用するユーザーを指定します。
APR-based detection	APR ベースの検出を有効にするかどうかを選択します。この機能は、APR に基づく NetShare の動作を検出します。
IPID trail tracking	IPID 追跡を有効にするかどうかを選択します。この機能は、パケットの IPID フィールドの値を追跡して、NetShare の動作を検出します。
Max terminals per IP	同じ IP アドレスを共有できる端末の最大数を入力します。
Action	IP アドレスを共有する端末の数が制限を超えたときの動作を選択します。 オプションは次のとおりです。 **Permit**: パケットの通過を許可します。 **Freeze**: IP アドレスをフリーズして、その IP アドレスを発信元とするすべてのパケットがドロップされるようにします。
Freezing time	この項目は、**Freeze** アクションが選択されている場合にのみ必要です。 IP アドレスが固定される時間(分)を入力します。
Logging	NetShare 制御ログを有効にするかどうかを選択します。 IP アドレスが過剰な数の端末によって共有されていることが検出されると(**Max terminals per IP** の制限を超える)、デバイスはログメッセージを生成し、IP アドレスと NetShare ポリシー情報を記録します。
Status	NetShare ポリシーを有効または無効にします。ポリシーは、有効にした後にのみ有効になります。

OK をクリックします。

新しい NetShare ポリシーを有効にするには、アクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化することも、デフォルトで 40 秒後に構成が自動的にアクティブ化されるようにすることもできます。

Server connection detection

このヘルプには、次のトピックがあります。

Introduction
Configure SCD
Configure SCD learning
Configure an SCD policy

Introduction

サーバー接続検出(SCD)を使用すると、デバイスはユーザー定義のルールに基づいて、特定のサーバーによって開始された正当な接続と不正な接続を識別して分類できます。これにより、管理者は内部サーバーを監視して、内部サーバーがボットネットの一部になったり、攻撃を開始したり、内部ネットワークに侵入したりするのを防ぐことができます。

Configure SCD

SCD の構成には、次のタスクが含まれます。

SCD 学習の構成指定したサーバーによって開始された接続を学習するようにデバイスを構成します。学習結果は、管理者が SCD ポリシーを作成して、サーバーによって開始された不正な接続を監視および記録するための基礎となります。
SCD ポリシーの構成サーバーの SCD ポリシーを作成し、SCD ルールを構成して、サーバーによって開始される有効な接続を定義します。デバイスは、SCD ルールに一致しないサーバーによって開始された接続をログに記録できます。

Configure SCD learning

デバイスが特定のサーバーによって開始された接続を学習できるようにするには、次の作業を実行します。

手順

Policies タブをクリックします。

ナビゲーションペインで、**Server Connection Detection** を選択します。
SCD Learning タブをクリックします。

サーバー起動接続の学習に使用するサーバーの IP アドレスを入力し、学習期間を設定します。
Start をクリックします。

デバイスは、指定された学習期間に指定されたサーバーによって開始された接続の学習を開始し、学習結果をリストに表示します。
サーバー起動接続を有効な接続として設定するには、接続を選択して **Create SCD rule** をクリックします。
デバイスによって、サーバーの SCD ポリシーが自動的に作成され、ポリシーで選択したサーバー接続の SCD ルールが作成されます。

Configure an SCD policy

SCD ポリシーを作成するには、次のタスクを実行します。

手順

Policies タブをクリックします。
ナビゲーションペインで、**Server Connection Detection** を選択します。
SCD Policy タブをクリックします。
Create をクリックします。
SCD ポリシーを作成します。

表 1:SCD ポリシーの構成項目

項目	説明
Policy name	SCD ポリシーの名前を入力します。
Server address	サーバーの IP アドレスを入力します。SCD ポリシーは、サーバーによって開始された接続を監視します。
Enable policy	SCD ポリシーを有効にするかどうかを選択します。
Logging	どの SCD ルールにも一致しないサーバーによって開始された接続をログに記録するかどうかを選択します。
SCD rules	各 SCD ルールは、サーバーによって開始される有効な接続のセットを定義します。どの SCD ルールにも一致しないサーバーによって開始された接続は、無効とみなされます。

	SCD ルールを作成する手順は、次のとおりです。 **Create** をクリックします。 接続の宛先 IP アドレスを入力します。 接続のプロトコルとポート番号を設定します。 SCD ルールには、少なくとも 1 つのプロトコルを構成する必要があります。 **OK** をクリックします。

Health monitoring

Introduction

ヘルスモニタリングは、Network Quality Analyzer(NQA)を介して実装されます。
NQA を使用すると、ネットワークパフォーマンスの測定、IP サービスおよびアプリケーションのサービスレベルの検証、およびネットワーク問題のトラブルシューティングを行うことができます。

NQA operating mechanism

NQA 操作には、操作の実行方法を定義する操作タイプ、宛先 IP アドレス、ポート番号などの一連のパラメーターが含まれています。ヘルスモニタリングでは、プローブテンプレートで NQA 操作のパラメーターを設定できます。

図 1 に示すように、NQA ソースデバイス(NQA クライアント)は、IP サービスとアプリケーションをシミュレートしてネットワークパフォーマンスを測定することによって、NQA ターゲットデバイスにデータを送信します。
すべてのタイプの NQA 操作には NQA クライアントが必要ですが、NQA サーバーが必要なのは TCP 操作のみです。FTP などの宛先デバイスによってすでに提供されているサービスの NQA 操作には、NQA サーバーは必要ありません。NQA サーバーを構成して、特定の IP アドレスおよびポートをリスニングして応答し、様々なテストニーズを満たすことができます。

図 1 ネットワーク図

Configuration items for probe templates

次の表では、さまざまなプローブテンプレートの設定項目について説明します。
表 1 すべてのプローブテンプレートの基本設定項目
表 2 ICMP テンプレートの基本的な構成項目
表 3 UDP/TCP テンプレートの基本構成項目
表 4 FTP テンプレートの基本構成項目
表 5 DNS テンプレートの基本的な構成項目

表 1 すべてのプローブテンプレートの基本設定項目

項目	説明
Type	テンプレートの名前を入力します。テンプレート名の大文字と小文字は区別されません。
Probe interval	リストから操作タイプを選択します。オプションは次のとおりです。 **ICMP**。 **UDP**。 **TCP**。 **FTP**。 **DNS**。 **HTTP**。 **RADIUS**。 **SSL**。 **HTTPS**。 **TCP half open**。 **SNMP-DCA**。 **RADIUS-ACCOUNT**。
Probe timeout	NQA 操作を繰り返す間隔をミリ秒単位で入力します。間隔を 0 に設定すると、NQA は操作を 1 回だけ実行し、統計情報は生成しません。
Description	応答を待機するタイムアウト時間をミリ秒単位で入力します。
Type	テンプレートの説明を入力します。

表 2 ICMP テンプレートの基本的な構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。

Data to pad	プローブパケットのペイロード充てん文字列を入力します。大文字と小文字が区別されます。ペイロード充てん文字列は、プローブパケットのペイロードサイズに適合するように、最後で切り捨てられるか、周期的に繰り返されます。
Length of data to pad	各プローブパケットのペイロードサイズをバイト単位で入力します。
Next hop IP address	プローブパケットのネクストホップ IPv4 または IPv6 アドレスを入力します。ネクストホップアドレスが設定されていない場合、デバイスはルーティングテーブルを検索して、プローブパケットのネクストホップアドレスを決定します。
Outgoing interface	プローブパケットの発信インターフェースを入力します。正常に動作するには、指定した発信インターフェースがアップ状態である必要があります。

表 3 UDP/TCP テンプレートの基本構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
Data to pad	プローブパケットのペイロード充てん文字列を入力します。大文字と小文字が区別されます。ペイロード充てん文字列は、プローブパケットのペイロードサイズに適合するように、最後で切り捨てられるか、周期的に繰り返されます。
Length of data to pad	各プローブパケットのペイロードサイズをバイト単位で入力します。 この項目は TCP 操作では使用できません。
Next hop IP address	プローブパケットのネクストホップ IPv4 または IPv6 アドレスを入力します。ネクストホップアドレスが設定されていない場合、デバイスはネクストホップアドレスのルーティングテーブルを検索します。 この項目は UDP 操作では使用できません。
Expected data offset	予想される応答データに対する最初の一致操作が開始されるまでのオフセットをバイト単位で入力します。 応答パケットを受信すると、NQA クライアントはパケットペイロードで期待されるデータを検索します。 オフセットが設定されていない場合、NQA クライアントはペイロードの先頭バイトから最初の一致操作を開始します。一致が見つからない場合は、ペイロードの 2 番目のバイトから別の一致操作を開始します。一致が見つかるか、最後のペイロードバイトが試行されるまで、プロセスは続行されます。

	オフセットが設定されている場合、NQA クライアントは指定されたオフセットバイトの後に最初の一致操作を開始します。一致が見つからない場合は、オフセットが設定されていないかのように一致操作を続行します。 いずれの場合も、NQA クライアントは、一致するものが見つかると NQA 操作を成功とマークします。一致するものが見つからない場合は、NQA 操作を失敗とマークします。
Expected data	大文字と小文字を区別して、予想される応答データを入力します。

表 4 FTP テンプレートの基本構成項目

項目	説明
URL	FTP 操作のターゲットリソースの URL を入力します。1～255 文字のストリング(大文字と小文字が区別されます)。 有効な URL 形式: ftp://host/filename です。 ftp://host:port/filename です。 host パラメーターは、リソースをホストするサーバーのホスト名を表します。このサーバーは、次の要件を満たす必要があります。 大文字と小文字が区別されます。 有効な文字は、文字、数字、ハイフン(-)、アンダースコア(_)、およびドット(.)ですが、連続したドット(.)は使用できません。 ドットで区切られた一連のラベルである必要があります。各ラベルには 1～63 文字を使用できます。
Username	FTP ログインユーザー名を入力します。ユーザー名では、大文字と小文字が区別されます。
Password	FTP ログインパスワードを暗号化形式で入力します。
Operation type	リストから FTP 操作タイプを選択します。オプションは次のとおりです。 **Download**: FTP サーバーからファイルを取得します。 **Upload**: ファイルを FTP サーバーにアップロードします。
Local file name	この項目は、**Operation type** で **Upload** が選択されている場合にのみ使用できます。 FTP サーバーにアップロードするファイルの名前を入力します。ファイル名は 1～200 文字の文字列で、大文字と小文字が区別されます。スラッシュ(/)は使用できません。

Mode	FTP 操作のデータ伝送モードを選択します。オプションは次のとおりです。 **Active**: アクティブモードでは、FTP サーバーが接続要求を開始します。 **Passive**: パッシブモードでは、FTP クライアントが接続要求を開始します。

表 5 DNS テンプレートの基本的な構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IP アドレスとして、DNS サーバーの IP アドレスを入力します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
Domain to resolve	解決するドメイン名を入力します。 ドメイン名は、次の要件を満たす必要があります。 1～255 文字の長さ。 大文字と小文字が区別されます。 有効な文字は、文字、数字、ハイフン(-)、アンダースコア(_)、およびドット(.)ですが、連続したドット(.)は使用できません。 ドットで区切られた一連のラベルである必要があります。各ラベルには 1～63 文字を使用できます。
Resolving type	ドメイン名解決のタイプを選択します。オプションは次のとおりです。 **A**: A タイプ A クエリーは、ドメイン名をマップされた IPv4 アドレスに解決します。 **AAA**: A タイプの AAAA クエリーは、ドメイン名をマッピングされた IPv6 アドレスに解決します。
Expected IPv4 address	この項目は、**Resolving type** で **A** が選択されている場合にのみ使用できます。 予想される IPv4 アドレスを入力します。 DNS 操作中に、NQA クライアントは予想される IPv4 アドレスと DNS サーバーによって解決された IPv4 アドレスを比較します。それらが同じである場合、NQA クライアントは DNS サーバーが正当であると見なします。
Expected IPv6 address	この項目は、**Resolving type** で **AAA** が選択されている場合にのみ使用できます。 予想される IPv6 アドレスを入力します。 DNS 操作中に、NQA クライアントは予想される IPv6 アドレスと DNS サーバーによって解決された IPv6 アドレスを比較します。それらが同じである場合、NQA クライアントは DNS サーバーが正当であると見なします。
Outgoing interface	プローブパケットの発信インターフェースを入力します。

表 6 HTTP/HTTPS テンプレートの基本構成項目

項目	説明
URL	ターゲットリソースの URL を入力します。URL は 1～255 文字のストリングで、大文字と小文字が区別されます。疑問符(?)は使用できません。 有効な URL 形式: HTTP: http://host/resource です。 http://host:port/resource です。 HTTPS: https://host/resource です。 https://host:port/resource です。 host パラメーターは、リソースをホストするサーバーのホスト名を表します。このサーバーは、次の要件を満たす必要があります。 大文字と小文字が区別されます。 有効な文字は、文字、数字、ハイフン(-)、アンダースコア(_)、およびドット(.)ですが、連続したドット(.)は使用できません。 ドットで区切られた一連のラベルである必要があります。各ラベルには 1～63 文字を使用できます。
Username	ログインユーザー名を入力します。ユーザー名では大文字と小文字が区別されます。
Password	ログインパスワードは暗号化された形式で入力します。パスワードでは大文字と小文字が区別されます。
Operation type	リストから操作タイプを選択します。オプションは次のとおりです。 **Get**: HTTP または HTTPS サーバーからデータを取得します。 **Post**: HTTP または HTTPS サーバーHTTPS サーバーにデータを転送します。 **Raw**: RAW 要求を HTTP サーバーまたは HTTPS サーバーに送信します。
Version	HTTP または HTTPS 操作で使用するバージョンを選択します。オプションは次のとおりです。 **V1.0**。 **V1.1**。
SSL client policy	この項目は、HTTPS テンプレートでのみ使用できます。 既存の SSL クライアントポリシーを選択するか、**Create SSL client policy** を選択して HTTPS テンプレートの SSL クライアントポリシーを作成します。作成された SSL クライアントポリシーは、**Create SSL client policy** ページに表示されます。

	HTTPS 操作では、NQA クライアントは指定された SSL クライアントポリシーを使用して、サーバーへの SSL 接続を確立します。
Expected status code	ステータコードアイテムのカンマ区切りリストを入力します。各アイテムは、ステータスコードまたは status-num1-status-num2 の形式のステータスコードの範囲を指定します。status-num1 および status-num2 引数の値の範囲は、どちらも 0 から 999 です。status-num2 引数の値は、status-num1 引数の値以上である必要があります。 例:1-4、6、8-10。
Expected data offset	予想される応答データに対する最初の一致操作が開始されるまでのオフセットをバイト単位で入力します。 応答パケットを受信すると、NQA クライアントはパケットペイロードで期待されるデータを検索します。 オフセットが設定されていない場合、NQA クライアントはペイロードの先頭バイトから最初の一致操作を開始します。一致が見つからない場合は、ペイロードの 2 番目のバイトから別の一致操作を開始します。一致が見つかるか、最後のペイロードバイトが試行されるまで、プロセスは続行されます。 オフセットが設定されている場合、NQA クライアントは指定されたオフセットバイトの後に最初の一致操作を開始します。一致が見つからない場合は、オフセットが設定されていないかのように一致操作を続行します。 いずれの場合も、NQA クライアントは、一致するものが見つかると NQA 操作を成功とマークします。一致するものが見つからない場合は、NQA 操作を失敗とマークします。
Expected data	大文字と小文字を区別して、予想される応答データを入力します。

表 7 RADIUS テンプレートの基本的な構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
Username	RADIUS 操作のログインユーザー名を入力します。ユーザー名では、大文字と小文字が区別されます。
Password	暗号化された形式でログインパスワードを入力します。パスワードでは大文字と小文字が区別されます。

Shared key	共有キーをプレーンテキスト形式で入力します。共有キーでは大文字と小文字が区別されます。

表 8 SSL テンプレートの基本構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
SSL client policy	既存の SSL クライアントポリシーを選択するか、**Create SSL client policy** を選択して SSL テンプレートの SSL クライアントポリシーを作成します。作成された SSL クライアントポリシーは、**Objects** > **SSL** > **SSL Client Policies** ページに表示されます。 SSL 操作では、NQA クライアントは指定された SSL クライアントポリシーを使用してサーバーへの SSL 接続を確立します。

表 9 TCP ハーフオープンテンプレートの基本構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。
Next hop IP address	プローブパケットのネクストホップ IPv4 または IPv6 アドレスを入力します。 ネクストホップアドレスが設定されていない場合、デバイスはルーティングテーブルを検索して、プローブパケットのネクストホップアドレスを決定します。
Port detection	TCP ハーフオープンテンプレートのポート検出をイネーブルにします。 TCP ハーフオープン動作では、ポート検出は、宛先デバイス上の TCP サービスのリスニングポートが使用可能かどうかをプローブします。NQA クライアントが、SYN パケットを送信してからプローブタイムアウト時間内に宛先デバイスからザシン-ACK パケットを受信すると、TCP ハーフオープン動作は成功します。プローブタイムアウト時間内に SYN-ACK パケットを受信しないと、TCP ハーフオープン動作は失敗します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
Outgoing interface	プローブパケットの発信インターフェースを入力します。正常に動作するには、指定した発信インターフェースがアップ状態である必要があります。

表 10 SNMP-DCA テンプレートの基本設定項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
SNMP community	SNMP コミュニティ名を入力します。 この項目は、SNMP エージェントがコミュニティ名で設定されている場合に必要です。 指定したコミュニティ名が、SNMP エージェントに設定されているコミュニティ名と同じであることを確認します。
SNMP version	SNMP DCA 操作で使用する SNMP バージョンを選択します。 SNMP DCA 操作が正しく動作するためには、選択した SNMP バージョンが、監視対象の SNMP エージェントのバージョンと一致している必要があります。
Agent type	SNMP エージェントのタイプを選択します。オプションは次のとおりです。 **Net-SNMP**。 **Windows**。 **Customize**。 SNMP DCA 操作は、SNMP エージェントを実行しているデバイスのパフォーマンスを監視します。SNMP エージェントから CPU、メモリー、およびディスクの使用状況を収集し、収集したオブジェクト値とそれに関連するしきい値および重みに基づいてデバイスのパフォーマンスを判断します。 SNMP エージェントタイプが異なると、CPU、メモリー、およびディスク使用オブジェクトに異なる OID が使用されます。SNMP DCA テンプレートで指定された SNMP エージェントタイプが、監視対象の SNMP エージェントのタイプと一致することを確認してください。 Net-SNMP または Windows SNMP エージェントの場合、NQA クライアントには、CPU、メモリーおよびディスク使用オブジェクトを収集するための組込み OID があります。これらのオブジェクトのしきい値および重みを設定できます。また、**OID settings** で、関連する SNMP オブジェクトを追加することもできます。 ユーザー定義タイプの SNMP エージェントの場合、NQA クライアントには収集する事前定義済の SNMP オブジェクトがありません。関連する SNMP オブジェクトおよび関連するしきい値と重みを構成する必要があります。
CPU usage threshold	この項目は、**Agent type** として **Net-SNMP** または **Windows** が選択されている場合にのみ使用できます。 CPU 使用率のしきい値を入力します。 しきい値 0 は、CPU 使用率が SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。

CPU weight	この項目は、**Agent type** として **Net-SNMP** または **Windows** が選択されている場合にのみ使用できます。 CPU 使用率オブジェクトの重みを入力します。 重み 0 は、CPU 使用率が SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。
Memory usage threshold	この項目は、**Agent type** として **Net-SNMP** または **Windows** が選択されている場合にのみ使用できます。 メモリー使用量のしきい値を入力します。 しきい値 0 は、メモリー使用量が SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。
Memory weight	この項目は、**Agent type** として **Net-SNMP** または **Windows** が選択されている場合にのみ使用できます。 メモリー使用量オブジェクトの重みを入力します。 重み 0 は、メモリー使用量が SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。
Disk usage threshold	この項目は、**Agent type** として **Net-SNMP** または **Windows** が選択されている場合にのみ使用できます。 ディスク使用率のしきい値を入力します。しきい値 0 は、ディスク使用率が SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。
Disk weight	この項目は、**Agent type** として **Net-SNMP** または **Windows** が選択されている場合にのみ使用できます。 ディスク使用量オブジェクトの重量を入力します。 重み 0 は、ディスク使用量が SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。
OID settings	監視する SNMP オブジェクトを設定するには、次の手順を実行します。 **OID settings** 領域で **Create** をクリックします。 開いた **Create OID** ウィンドウで、次の項目を構成します。 **OID**: 監視する SNMP オブジェクトの OID を入力します。 **OID usage threshold**: オブジェクトのしきい値を入力します。しきい値 0 は、オブジェクトが SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。 **OID weight** を入力します。重み 0 は、オブジェクトが SNMP エージェントのパフォーマンスを測定するためのメトリックとして使用されないことを意味します。 **OK** をクリックします。OID が OID リストに表示されます。 **Customize** エージェントタイプを使用する場合は、OID 構成が必要です。最大 8 つの OID を追加できます。

表 11 RADIUS-ACCOUNT テンプレートの基本構成項目

項目	説明
Destination IP address	プローブパケットの宛先 IPv4 または IPv6 アドレスを入力します。
Destination port number	プローブパケットの宛先ポート番号を入力します。
Username	ログインユーザー名を入力します。ユーザー名では大文字と小文字が区別されます。
Shared key	共有キーをプレーンテキスト形式で入力します。共有キーでは大文字と小文字が区別されます。

表 12 プローブテンプレートの高度な設定項目

項目	説明
VPN instance	操作を適用する VPN インスタンスを指定します。 **Public network** で既存の VPN インスタンスを選択するか、または **Create VPN instance policy** を選択して VPN インスタンスを作成できます。作成された VPN インスタンスは、**Network** > **VPN** ページに表示されます。 VPN インスタンスを指定すると、NQA 操作により、指定した VPN インスタンスの接続がテストされます。
TTL	プローブパケットが通過できる最大ホップカウントを入力します。
ToS	プローブパケットの IP ヘッダーに ToS 値を入力します。
Source IP address	プローブパケットの送信元 IPv4 または IPv6 アドレスを入力します。 送信元アドレスはローカルインターフェースのアドレスである必要があり、インターフェースはアップ状態である必要があります。そうでないと、プローブパケットを送信できません。 テンプレートを NAT アドレスグループで使用する場合は、この項目を設定しないでください。
Probe result frequency	プローブ結果の送信基準を選択します。オプションは次のとおりです。 **Consecutive probes**：指定した回数だけ連続して失敗または成功したプローブの後で、テンプレートを使用する機能にプローブ結果を送信します。 **Consecutive successful probes**：プローブ結果の送信をトリガーする連続成功プローブの数を入力します。

	Consecutive failed probes: プローブ結果の送信をトリガーする、連続して失敗したプローブの数を入力します。 **Per probe**:プローブが完了するたびに、NQA テンプレートを使用する機能にプローブ結果を送信します。このオプションは、ICMP および TCP ハーフオープンテンプレートでのみ使用できます。

User management

このヘルプには、次のトピックがあります。

Introduction

Local users

Users

ローカルユーザーは、ネットワークアクセス用にデバイス上のローカルユーザーデータベースに格納されるユーザートリビュートのセットです。ローカルユーザーは、ユーザー名によって一意に識別されます。ローカル認証、認可、アカウンティングを実装するには、デバイス上でローカルユーザーを作成し、ユーザートリビュートを設定します。

User groups

ユーザーグループを使用すると、ローカルユーザーの構成および管理が簡略化されます。ユーザーグループには、ローカルユーザーのグループが含まれ、ローカルユーザー属性のセットがあります。ユーザーグループのローカルユーザー属性を構成して、グループ内のローカルユーザーの集中ユーザー属性管理を実装できます。ユーザーグループを使用して管理可能なローカルユーザー属性は、認可属性です。

新しく作成された各ローカルユーザーは、**system** という名前のシステム定義ユーザーグループに属し、そのグループのすべての属性を持ちます。

Password control

ユーザーのパスワードセキュリティを強化するために、パスワード制御機能を設定できます。

Minimum password length

ユーザーパスワードの最小長を定義できます。システムは、構成された最小長より短いパスワードを拒否します。デフォルトでは、最小パスワード長は 10 文字です。

Password composition check

パスワードには、次の種類の文字を組み合わせて使用できます。
大文字の A～Z。
小文字の a～z。
数字の 0～9。
特殊文字。表 1 を参照してください。

表 1 特殊文字

キャラクタ名	記号	キャラクタ名	記号
Ampersand sign	&	アポストロフィ	'
Asterisk	*	アット記号	@
Back quote	`	バックスラッシュ	¥
Blank space	N/A	キャレット	^
Colon	:	カンマ	,
Dollar sign	$	ドット	.
Equal sign	=	感嘆符	!
Left angle bracket	<	左中括弧	{
Left bracket	[	左括弧	(
Minus sign	-	パーセント記号	%
Plus sign	+	ポンド記号	#
Quotation marks	"	右山括弧	>
Right brace	}	右ブラケット	]
Right parenthesis	)	セミコロン	;
Slash	/	ティルダ	～
Underscore	_	縦棒	|

システムのセキュリティ要件に応じて、表 2 に示すように、パスワードに含める必要がある文字タイプの

最小数と、各タイプの最小文字数を設定できます。

表 2 パスワード構成チェック

パスワードの組み合わせレベル	文字タイプの最小数	各タイプの最小文字数
レベル 1	1	1
レベル 2	2	1
レベル 3	3	1
レベル 4	4	1

ユーザーがパスワードを設定または変更すると、システムは、パスワードが組合せ要件を満たしているかどうかを調べます。パスワードが要件を満たしていない場合、操作は失敗します。
デフォルトでは、文字タイプの最小数は 1 であり、各タイプの最小文字数は 1 です。

Password complexity check

パスワードの強度は、その複雑さが増すにつれて増加します。あまり複雑でないパスワードは、解読される可能性が高くなります。たとえば、ユーザー名または繰り返される文字を含むパスワードは、そうでないパスワードよりも解読される可能性が高くなります。システムセキュリティーを強化するには、パスワードの複雑さチェックポリシーを構成して、ユーザーが構成したパスワードがほとんどのパスワード攻撃に対して十分に複雑であることを確認します。
次のパスワード複雑度要件を適用できます。

パスワードには、ユーザー名または逆スペルのユーザー名を含めることはできません。たとえば、ユーザー名が **abc** の場合、パスワードを **abc982** または **2cba** にすることはできません。
パスワードには、連続する同じ文字を 2 つ以上含めることはできません。たとえば、パスワード **a111** は許可されません。

Password history

この機能により、システムはユーザーが使用したパスワードを格納できます。ユーザーがパスワードを変更すると、システムは新規パスワードを現行パスワードおよびパスワード履歴レコードに格納されているパスワードと比較します。新規パスワードは、現行パスワードおよび履歴レコードに格納されているパスワードと 4 文字以上異なる必要があります。新規パスワードがこの要件を満たしていない場合は、エラーメッセージが表示され、パスワード変更操作が拒否されます。

各ユーザーに対してシステムが保持する履歴パスワードレコードの最大数を設定できます。履歴パスワードレコードの数が設定を超えると、最新のレコードが最も古いレコードを上書きします。

Password updating

この機能を使用すると、ユーザーがパスワードを変更できる最小間隔を設定できます。ユーザーは、指定した間隔内に 1 回のみパスワードを変更できます。
最小間隔は、次の状況には適用されません。

ユーザーは、最初のログイン時にパスワードの変更を求められます。
パスワードの有効期限が切れます。

Identity users

ユーザー識別機能は、他のセキュリティー機能とともに使用して、ユーザーベースのネットワークアクセス制御およびネットワーク特権管理を実行できます。
ユーザー識別機能には、次の利点があります。

ユーザー単位でのセキュリティーポリシーの導入を容易にします。
ユーザーベースのネットワーク攻撃/アクセストラフィック統計情報を提供することにより、ユーザーに対するネットワークアクセス動作の監査を実装します。
ポリシー制御を実装するために、デバイスがダイナミック IP アドレスではなく固定ユーザー名を使用できるようにします。

Identity users

アイデンティティーユーザーは、異なるソースからのネットワークアクセスユーザーの識別情報を記録するために使用されます。識別情報には、ユーザーのユーザー名、ユーザーグループ名およびアイデンティティードメイン名が含まれます。ユーザー識別モジュールは、異なるソースからのアイデンティティーユーザーを一様に管理します。
デバイスは、アイデンティティーユーザーを作成するために次の方法をサポートしています。

Learning from the local user database: ユーザー識別モジュールは、ローカルユーザーデータベースからローカルユーザー情報を学習し、そのユーザー情報をアイデンティティーユーザーとして保存します。

Importing from a .csv file: ネットワーク管理者は.csv ファイルからデバイスにユーザー情報をインポートします。デバイスはインポートされた情報に基づいて自動的にアイデンティティーユーザーを作成します。

Importing from third-party servers: デバイスはサードパーティサーバーへのユーザー情報要求を開始し、ネットワークアクセスユーザー情報をインポートして、インポートされた情報に基づいてアイデンティティーユーザーを作成します。この方法により、ユーザー情報がサードパーティサーバー上にある場合、ネットワーク管理者はアイデンティティーユーザーを管理できます。サポートされているサードパーティサーバーには、LDAP サーバーおよび IMC RESTful サーバーが含まれます。

ID ユーザーは、次のいずれかの理由で削除されます。

ネットワーク管理者は、ID ユーザーを手動で削除します。
ユーザー識別モジュールは、対応するネットワークアクセスユーザーがローカルユーザーデータベースから削除された後に、アイデンティティーユーザーを自動的に削除する。

Identity groups

アイデンティティーユーザーは、バッチ構成および階層ユーザー管理のために異なるグループに追加できます。これらのグループはアイデンティティーグループと呼ばれます。ユーザー識別モジュールは、異なるソースからのアイデンティティーグループを一様に管理します。
デバイスは、ID グループを作成するために次の方法をサポートします。

Learning from the local user database: ローカルユーザーグループが作成されると、デバイスはユーザー識別モジュールに対して、同じグループ名で ID グループを作成するように指示します。
Importing from a .csv file: デバイスは.csv ファイルから ID ユーザーカウント情報をインポートし、インポートされた情報に基づいて ID グループを自動的に作成します。
Importing from third-party servers: デバイスは、IMC RESTful サーバーまたは LDAP サーバーからアイデンティティーユーザーカウント情報をインポートし、アカウント内のグループ情報に基づいてアイデンティティーグループを作成できます。また、デバイスは、LDAP サーバーからユーザーグループ情報を直接取得して、アイデンティティーグループを作成することもできます。

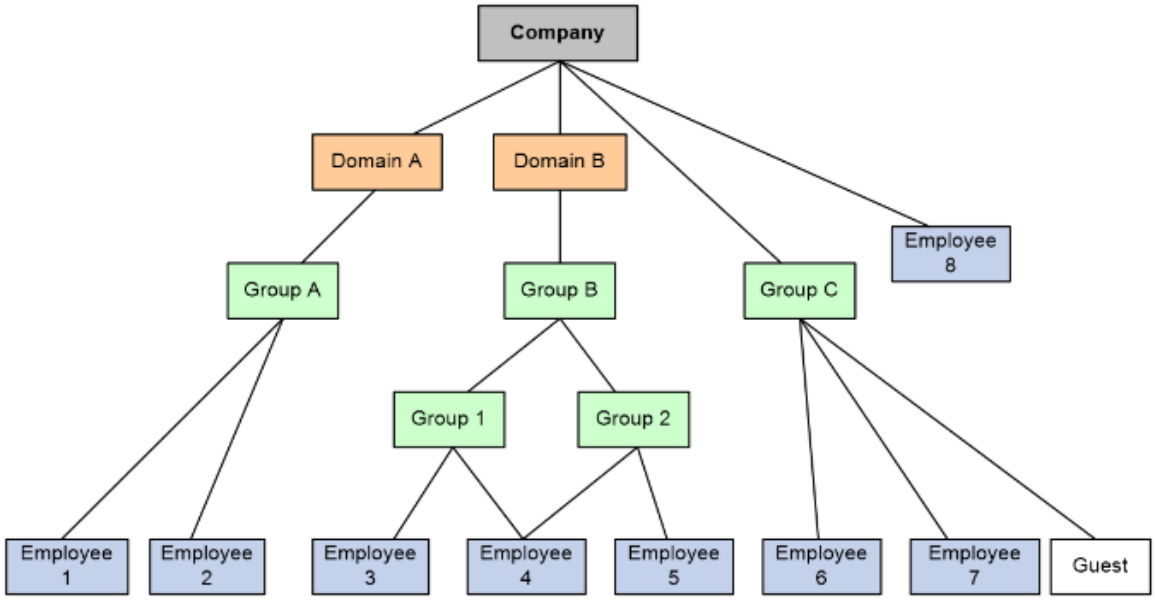
ID グループは、アプリケーションモジュールによって使用されるとアクティブになり、ID グループに基づくすべてのサービスが有効になります。アプリケーションモジュールが ID グループの使用を停止すると、ID グループは非アクティブになります。
ID グループは、次のいずれかの理由で削除されます。

ネットワーク管理者は ID グループを削除します。
ユーザー識別モジュールは、対応するローカルユーザーグループがローカルユーザーデータベースから削除されると、ID グループを自動的に削除します。

Identity user management

すべてのアイデンティティーユーザーは、ツリー構造で編成されます。アイデンティティーユーザーは、1 つ以上のアイデンティティーグループに属することができます。アイデンティティーグループは、1 つ以上の上位レイヤーイデンティティグループに属することができます。ツリー構造により、ユーザーの検索と問合せが容易になります。図 1 に示すように、デバイスは、アイデンティティードメインとユーザー名の組合せ、またはアイデンティティードメインとアイデンティティーグループの組合せによって、管理対象オブジェクトを一意に識別します。

図 1:ID ユーザー管理アーキテクチャ



Identity-based user access control

次に、ID ベースのユーザーアクセスコントロールのプロセスを示します。

ID 認証。ネットワークアクセスユーザーは ID 認証を通過し、オンラインになります。
ユーザーID。デバイスはオンラインユーザーのユーザー名と IP アドレスを取得し、その情報をローカル ID ユーザーカウントとローカル ID グループに関連付けます。次に、ネットワークアクセスユーザーのユーザー名と IP のマッピングが作成されます。管理者は、スタティックなユーザー名と IP のマッピングを追加して、ID 認証なしでネットワークアクセスを許可することもできます。
ID ベースのアクセスコントロール。デバイスは、ネットワーク宛てのトラフィックの送信元 IP アドレスを識別し、マッピングに基づいて IP アドレスをユーザー名およびユーザーグループに解決します。デバイスは、ブラックリストやオブジェクトポリシーなどの他のセキュリティー機能の設定に基づいて、ユーザーまたはユーザーグループのネットワークアクセスコントロールを実行します。

Online users

オンラインユーザーは、ユーザー識別モジュールによって管理されるオンラインネットワークアクセスユーザー(ポータル、PPP、および IPoE ユーザーを含む)です。デバイスは、オンラインユーザーのユーザー名、アイデンティティードメイン名、IP アドレス、および MAC アドレスを記録します。
オンラインユーザーには、動的オンラインユーザーと静的オンラインユーザーがあります。

動的な構成。

Online network access users that access the network through the device: ユーザーがローカルまたはリモート認証を通過してオンラインになると、ユーザー識別モジュールはローカル ID ユーザー内のユーザーのユーザー名とドメイン名を検索します。一致するエントリが見つかると、デバイスはユーザーのオンラインユーザーエントリを作成します。

Online network access users obtained from third-party servers: デバイスがサードパーティサーバーからオンラインユーザーに関する情報を取得した後、ユーザー識別モジュールはローカルアイデンティティーユーザー内のユーザーのユーザー名およびドメイン名を検索します。一致するエントリが見つかった場合、デバイスはそのユーザーのオンラインユーザーエントリを作成します。デバイスは、サードパーティサーバーのすべてのオンラインユーザー(他のデバイス上のオンラインユーザーを含む)に関する情報を取得して、管理と監視を統合できます。サポートされているサードパーティサーバーには、IMC RESTful サーバーが含まれます。

静的構成。

ネットワーク管理者は、オンラインユーザーを手動で作成します。各静的アイデンティティーユーザーには、ユーザー名とユーザーの IP アドレス間のマッピングが含まれています。静的アイデンティティーユーザーが作成されると、ユーザー識別モジュールはローカルアイデンティティーユーザー内のユーザーのユーザー名とドメイン名を検索します。一致するエントリが検出されると、デバイスは静的アイデンティティーユーザーの静的オンラインユーザーエントリを作成します。静的オンラインユーザーは、アイデンティティー認証なしでネットワークにアクセスできますが、ネットワークへのアクセスはセキュリティー機能によって制御されます。ネットワーク管理者は、一時的にネットワークにアクセスする必要があるユーザーが少ない場合に、静的アイデンティティーユーザーを構成できます。

アプリケーションモジュールは、オンラインユーザーにセキュリティーポリシーを課すことができます。オンラインユーザーエントリが削除されると、ユーザー識別モジュールはアプリケーションモジュールに対して、ユーザーのサービスの処理を停止するように指示します。
オンラインユーザーは、次のいずれかの理由で削除されます:

ネットワーク管理者は、オンラインユーザーを手動で削除します。
アクセスモジュールは、関連するネットワークアクセスユーザーがオフラインになった後にオンラインユーザーを削除するようにユーザー識別モジュールに指示する。
すべてのダイナミックオンラインユーザーは、デバイスの再起動後に削除されます。
ユーザーID 機能をディセーブルにすると、すべてのダイナミックオンラインユーザーが削除されます。
サードパーティ製サーバーは、関連付けられたユーザーがオフラインになった後にオンラインユーザーを削除するようにデバイスに指示します。

User import policies

ユーザーインポートポリシーは、RESTful サーバーまたは LDAP サーバーからアイデンティティーユーザー、オンラインユーザー、またはアイデンティティーグループをインポートするために使用されます。
ユーザーインポートポリシーでは、次のインポート方法がサポートされています。

Automatic import: デバイスは最初にポリシーで指定されたサーバーからすべての ID ユーザーとオンラインユーザーをインポートし、次にサーバーから定期的に ID ユーザーを自動的にインポートします。
Manual import: デバイスは、ポリシーで指定されたサーバーへの接続要求を開始し、すべてのアイデンティティーユーザーとオンラインユーザーをサーバーからインポートします。

Restrictions and guidelines

Restrictions and guidelines for users

パスワードで保護されていないローカルユーザーは、正しいユーザー名を指定して属性チェックに合格すると、認証に合格します。セキュリティを強化するには、各ローカルユーザーのパスワードを構成します。
ポータルユーザーの場合は、認可 ACL およびアイドルタイムアウトアトリビュートだけが有効です。
SSL VPN ユーザーの場合、SSL VPN ポリシーグループアトリビュートだけが有効になります。
ID ユーザーを削除しても、対応するネットワークアクセスユーザーはローカルユーザーデータベースから削除されません。

Restrictions and guidelines for user import policy configuration

CSV テンプレートからユーザーをインポートする場合は、ファイルが標準の.CSV ファイルであることを確認し、テンプレートの注釈ヘッダーを変更しないでください。違反すると、データが失われる可能性があります。
IMC RESTful サーバーを使用するには、サーバーが SSM コンポーネントとともにインストールされ、IMC PLAT 7.0(E0201)またはそのパッチバージョンで実行されていることを確認します。
デバイスが RESTful サーバーとの接続を確立すると、RESTful サーバーはデバイスのリアルタイムユー

ザーログインおよびログアウト情報を送信して、オンラインユーザーを更新します。

Restrictions and guidelines for email server configuration

受信者の電子メールアドレスを設定する前に、電子メールサーバーを設定する必要があります。

Restrictions and guidelines for password control

User Password Control ページで設定したパスワード制御設定は、すべてのローカルユーザーに有効になります。**User Password Control** ページを開くには、**User** > **User Management** > **Local Users** > **Users** ページにアクセスし、メニューの **Password control** ボタンをクリックします。
User Password Control ページと **Create User** ページまたは **Edit User** ページの両方で、最小パスワード長、パスワード複雑性チェックおよびパスワード構成チェックを構成できます。**Create User** ページまたは **Edit User** ページで構成された設定は、**User Password Control** ページで構成された設定より優先されます。

Administrator Password Control ページと **User Password Control** ページでは、パスワード制御の設定が共有されます。一方のページでパスワード制御の設定を変更すると、新しい設定がもう一方のページに自動的に同期化されます。
パスワード制御を有効にした後、ローカルユーザーのパスワードセットには、少なくとも 4 つの異なる文字が必要です。
ユーザーに構成されたパスワード制御設定を有効にするには、パスワード制御を有効にする必要があります。パスワード制御を有効にするには、**Users** ページの **Password control** をクリックして **User Password Control** ページを表示し、**Enable password control** を選択します。

Configure user management

Configure local users

ローカルユーザーは手動で作成することも、一括してインポートすることもできます。

Create a local user

Objects タブをクリックします。
ナビゲーションペインで、**User** > **User Management** > **Local Users** を選択します。
Users タブをクリックし、**Create** をクリックします。**Create User** ページが開きます。
ローカルユーザーを作成します。

表 3 ローカルユーザー構成項目

項目	説明
Username	ネットワークアクセスユーザーの名前を入力します。 ユーザーはデバイスを介してネットワークリソースにアクセスします。 ローカル認証を実装するには、デバイス上でローカルユーザーを設定する必要があります。
Set random password	ユーザーのランダムなパスワードを生成する場合に選択します。
Receiver email	ランダムパスワードを受信する受信者の電子メールアドレスを入力します。 このフィールドを設定する前に、[Email Server]ページして電子メールサーバーを設定してください。
Password	ユーザーのパスワードを入力します。
Confirm	ユーザーのパスワードをもう一度入力します。
Validity period	ユーザーの有効期間を設定します。 有効期限が切れたユーザーカウントは認証に使用できません。 開始時刻と終了時刻の両方を指定する場合は、終了時刻を開始時刻よりも後にする必要があります。 開始時刻だけが指定された場合、ユーザーは指定された時刻以降有効です。 終了時刻だけを指定した場合、ユーザーは指定した時刻まで有効です。
Authorization user group	認可ユーザーグループを選択します。 各ローカルユーザーはユーザーグループに属し、グループのすべての属性を持ちます。属性には、パスワード制御属性と認可属性が含まれます。
Identity group	ID グループを選択します。 ユーザー識別モジュールは、ユーザーが属する ID グループに基づいてローカルユーザーのネットワークアクセスを制御する。
Available services	ユーザーが使用できるサービスを選択します。 ローカル認証では、ローカルユーザーのサービスタイプがチェックされます。使用可能なサービスタイプがない場合、ユーザーは認証を通過できません。
Max number of concurrent logins	同じユーザー名を使用してデバイスに同時にアクセスできるユーザーの最大数を入力します。 ユーザー名を使用したログイン数が制限に達すると、そのユーザー名を使用してデバイスにアクセスできるローカルユーザーはなくなります。
Description	ユーザーの説明情報を入力します。

(任意) authorization attributes を設定します。

表 4 許可属性の構成項目

項目	説明
Authorization ACL	認可 ACL を選択します。 デバイスは、認証されたユーザーが ACL によって許可されたネットワークリソースだけにアクセスするように制限します。
Idle timeout	アイドルカットのタイムアウト時間を入力します。 指定された方向のアイドルタイムアウト時間内のユーザーの合計トラフィックが、指定された最小トラフィックよりも少ない場合、デバイスはユーザーをログアウトします。
Authorization VLAN	VLAN ID を入力します。 デバイスは、認証されたユーザーが VLAN 内のネットワークリソースだけにアクセスするように制限します。
SSL VPN policy group	SSL VPN ポリシーグループを入力します。 デバイスは、認証されたユーザーが SSL VPN ポリシーグループで指定されたネットワークリソースだけにアクセスするように制限します。

(任意) binding attributes を設定します。

表 5 バインド属性の構成項目

項目	説明
Access interface	アクセスインターフェースを選択します。 ユーザーの実際のアクセスインターフェースがバインディングインターフェースと同じでない場合、ユーザーは認証に失敗します。
IPv4 address	IPv4 アドレスを入力します。 ユーザーの IP アドレスがバインディング IPv4 アドレスと異なる場合、ユーザーは認証に失敗します。
MAC address	MAC アドレスを入力します。 ユーザーの MAC アドレスがバインディング MAC アドレスと異なる場合、ユーザーは認証に失敗します。
VLAN	VLAN ID を入力します。 ユーザーがバインディング VLAN とは異なる VLAN に所属している場合、ユーザーは認証に失敗します。

(任意) password settings を行います。

表 6 パスワード設定の構成項目

項目	説明

Min password length	パスワードの最小長を入力します。 ユーザーが入力したパスワードがこの値より短い場合、システムはパスワード設定を拒否します。
Min character types	パスワードの文字タイプの最小数を入力します。 ユーザーが入力したパスワードの文字タイプの数がこの値より少ない場合、システムはパスワード設定を拒否します。
Min number of characters for each type	パスワードの各タイプの最小文字数を入力します。 ユーザーが入力したパスワードの各タイプの文字数がこの値より少ない場合、システムはパスワード設定を拒否します。
No username or reversed username in password	ユーザー名またはその逆のパスワードを拒否するには、この項目を選択します。
No more than two consecutive identical characters in password	連続した同じ文字が 2 つ以上あるパスワードを拒否するには、この項目を選択します。

OK をクリックします。ユーザーが **Users** ページに表示されます。

Import local users in bulk

Objects タブをクリックします。
ナビゲーションペインで、**User** > **User Management** > **Local Users** を選択します。
Users タブをクリックし **Import** をクリックします。**Import Users** ページが開きます。
ローカルユーザーをインポートします。

表 7 ローカルユーザーをインポートするための構成項目

項目	説明
Import file	ローカルユーザーをインポートするデバイスの.CSV ファイルを指定します。 CSV ファイルが標準の.csv ファイルであることを確認し、テンプレートの注釈ヘッダーを変更しないでください。違反すると、データが失われる可能性があります。
Automatically create groups	ユーザーが属する ID グループがデバイス上に存在しない場合に、デバイスがユーザーの ID グループを自動的に作成できるようにするには、この項目を選択します。 この項目を選択しない場合、デバイスは存在しないユーザーグループを作成せず、ユーザーをシステム定義のユーザーグループシステムに割り当てます。

Overriding existing user accounts	インポートする ID ユーザーカウントと同じ名前の既存の ID ユーザーカウントをデバイスが上書きできるようにするには、この項目を選択します。 この項目を選択しない場合、デバイスは既存のアイデンティティーユーザーカウントを保持します。
Import from line	アカウントのインポートを開始する行の番号を入力します。 行番号を指定しない場合、デバイスはアイデンティティーユーザーカウント情報を最初の行からインポートします。

OK をクリックします。インポートされたローカルユーザーが **Users** ページに表示されます。

Configure password control

Objects タブをクリックします。
ナビゲーションペインで、**User** > **User Management** > **Local Users** を選択します。
Users タブをクリックし、**Password Control** をクリックします。**User Password Control** ページが開きます。
パスワード制御設定を構成します。

表 8 パスワード制御の構成項目

項目	説明
Enable password control	パスワード制御を有効にするには、この項目を選択します。
Enable password length check	パスワード長のチェックを有効にするには、この項目を選択します。
Min password length	パスワードの最小長を入力します。 ユーザーが入力したパスワードがこの値より短い場合、システムはパスワード設定を拒否します。
Enable password composition check	パスワード構成チェックを有効にするには、この項目を選択します。
Min number of character types	パスワードの文字タイプの最小数を入力します。 ユーザーが入力したパスワードの文字タイプの数がこの値より少ない場合、システムはパスワード設定を拒否します。
Min number of characters for each type	パスワードの各タイプの最小文字数を入力します。 ユーザーが入力したパスワードの各タイプの文字数がこの値より少ない場合、システムはパスワード設定を拒否します。

No more than two same consecutive characters in password	連続した同じ文字が 2 つ以上あるパスワードを拒否するには、この項目を選択します。
No username or reversed username in password	ユーザー名またはその逆のパスワードを拒否するには、この項目を選択します。
Enable password history recording	この項目を選択すると、パスワード履歴の記録が有効になります。
Max number of history password records	履歴パスワードレコードの最大数を入力します。 履歴パスワードレコードの数がこの値を超えると、最も新しいレコードが最も古いレコードを上書きします。
Min password update interval	パスワードの最小更新間隔を入力します。 ユーザーがパスワードを変更できるのは、指定した時間内に一度だけです。

OK をクリックします。

Manage online users

オンラインユーザーを管理するには、次の作業を実行します。

Objects タブをクリックします。
ナビゲーションペインで、**User** > **User Management** > **Online Users** を選択します。
オンラインユーザーを管理します。

表 9 オンラインユーザーを管理するための構成項目

項目	説明
Enable user identification	ユーザー識別機能を有効にするには、このボタンをクリックします。
Username match mode	ユーザー名の一致モードを選択します。 次のモードを使用できます。 **Keep-original**: ユーザーが入力したユーザー名を使用して、ユーザー名の照合を実行します。 **with-domain**: ユーザーの認証ドメイン名を含むユーザー名を使用して、ユーザー名の照合を実行します。たとえば、認証ドメインが **abc** で、入力されたユーザー名が **test@123** の場合、デバイスはローカルユーザーカウントのユーザー名 **test@abc** を検索します。

	Without-domain: ユーザーのドメイン名を除外したユーザー名を使用して、ユーザー名の照合を実行します。たとえば、認証ドメインが **abc** で、入力されたユーザー名が **test@123** の場合、デバイスはどのアイデンティティードメインにも参加していないローカルユーザーカウントのユーザー名 **test** を検索します。

Configure a user import policy

Create a user import policy

Objects タブをクリックします。
ナビゲーションペインで、**User** > **User Management** > **User Import Policies** を選択します。
Create をクリックします。**Create User Import Policy** ページが開きます。
ユーザーインポートポリシーを作成します。

表 10 ユーザーインポートポリシーの構成項目

項目	説明
Name	ユーザーインポートポリシーの名前を入力します。 この名前は、ユーザーインポートポリシーを一意に識別します。
RESTful server	RESTful サーバーを選択します。 デバイスは RESTful サーバーから ID ユーザーとオンラインユーザーをインポートします。
LDAP schemes	LDAP スキームを選択します。 デバイスは、LDAP スキームで指定された LDAP サーバーからアイデンティティーユーザーをインポートします。
Import types	インポートする情報のタイプを選択します。 このパラメーターは、LDAP スキームにのみ適用できます。
Enable auto import	ユーザーの自動インポートを有効にするには、この項目を選択します。 この機能をイネーブルにすると、デバイスは最初にユーザーインポートポリシーで指定されたサーバーから ID ユーザーとオンラインユーザーをインポートし、次にサーバーから ID ユーザーを定期的にインポートします。
Import interval	自動インポートの間隔を入力します。 デバイスは、ユーザーインポートポリシーで指定されたサーバーから、指定された間隔でアイデンティティーユーザーを自動的にインポートします。

OK をクリックします。**OK** ページにユーザーインポートポリシーが表示されます。

Manually import users

ユーザーインポートポリシーを設定したら、ユーザーインポートポリシーで指定されたサーバーから ID ユーザーおよびオンラインユーザーを手動でインポートできます。
ユーザーを手動でインポートするには、次の作業を実行します。

Manually import identity users: デバイスはサーバーへのユーザー情報要求を開始し、サーバーからユーザーアカウント情報をインポートしてから、対応するアイデンティティーユーザーを作成します。デバイスがアカウントのインポートに失敗すると、デバイスはそのアカウントをスキップし、次のアカウントのインポートを続行します。

Manually import online users: デバイスは、サーバーへのリアルタイムオンラインユーザー情報要求を開始し、すべてのオンラインユーザー情報をインポートします。デバイスは、IMC RESTful サーバーからのみオンラインアイデンティティーユーザーをインポートできます。

Configure the email server

デバイスは、ランダムなパスワードを電子メール通知でユーザーに送信します。受信者の電子メールアドレスを設定する前に、電子メールサーバーを設定する必要があります。
電子メールサーバーを設定するには、次の作業を実行します。

Objects タブをクリックします。
ナビゲーションペインで、**User** > **User Management** > **Email Server** を選択します。
電子メールサーバーを設定します。

表 11 電子メールサーバーの構成項目

項目	説明
Email subject	電子メール通知の件名を入力します。
Email body	電子メール通知の本文を入力します。
Sender address	メール送信元のアドレスを設定します。
Server address	電子メールサーバーの URL(smtp://で始まる)を入力します。
Username	電子メールサーバーへのログインに使用するユーザー名を入力します。
Password	電子メールサーバーへのログインに使用するパスワードを入力します。

Authentication

このヘルプには、次のトピックがあります。

Introduction

ISP domains

AAA は、ユーザーの ISP ドメインに基づいてユーザーを管理します。各 ISP ドメインは、ISP ドメイン内のユーザーの AAA 動作を制御するために、一連の認証、承認、およびアカウンティング方式を維持します。管理者は、ドメイン内のユーザーアクセスの種類とセキュリティー要件に基づいて、ISP ドメインの認証、承認、およびアカウンティング方式を構成できます。
デバイスは次の認証方式をサポートしています。

No authentication: このメソッドはすべてのユーザーを信頼し、認証を実行しません。セキュリティー上の理由から、このメソッドは使用しないでください。

Local authentication: NAS は、ユーザー名、パスワード、ユーザートリビュートなど、ローカルに設定されたユーザー情報に基づいて、ユーザーを独自に認証します。ローカル認証は、高速で低コストの認証サービスを提供しますが、NAS に保存できる情報量は、ストレージスペースのサイズによって制限されます。

RADIUS authentication: RADIUS 認証はリモート認証の一種です。NAS は RADIUS プロトコルを介してリモートサーバーと通信してユーザーを認証します。サーバーはユーザー情報を集中管理します。リモート認証は、複数の NAS に対して大容量で信頼性の高い集中認証サービスを提供します。高可用性を実現するために、ユーザー認証用に複数の RADIUS サーバーを指定できます。また、サーバーが使用できない場合に使用するバックアップ方法を構成できます。

LDAP authentication: LDAP 認証はリモート認証の一種です。NAS は LDAP プロトコルを介してリモートサーバーと通信し、ユーザーを認証します。LDAP は、その機能を実装するための一連の操作を定義します。認証の主な操作は、バインド操作と検索操作です。LDAP 認証では、クライアントは次のタスクを実行します。

LDAP サーバー管理者 DN を使用して、LDAP サーバーとバインドします。バインドが作成されると、クライアントはサーバーへの接続を確立し、検索権限を取得します。

ユーザーの認証情報に含まれるユーザー名を使用して検索条件を構成します。指定したサーバーのルートディレクトリが検索され、ユーザーDN リストが生成されます。

各ユーザーDN およびパスワードを使用して LDAP サーバーとバインドします。バインドが作成されると、ユーザーは正当であるとみなされます。

Single sign-on: NAS はリモートサーバーと連携してユーザーを認証します。サーバーは、ユーザーが認証を通過した後、ユーザーID で構成されたデバイスにユーザーID 情報を送信します。デバイスはこの情報を使用してユーザーの識別を実行し、認証を完了します。

デバイスは次の認可方式をサポートしています。

No authorization: NAS は認可交換を実行しません。ユーザーが認証を通過すると、次のデフォルト認可情報が適用されます。

ログインユーザーはデフォルトのユーザーロールを取得します。FTP、SFTP および SCP ログイユーザーの作業ディレクトリーは、NAS のルートディレクトリです。ただし、ユーザーにはルートディレクトリへのアクセス権限はありません。

ログインしていないユーザーはネットワークにアクセスできます。

Local authorization: NAS は、ユーザーに対してローカルに設定されたユーザートリビュートに従って認可を実行します。

RADIUS authorization: RADIUS 認可はリモート認可の一種です。NAS はリモートサーバーと連携してユーザーを認可します。RADIUS 認可は RADIUS 認証とバインドされます。RADIUS 認可は RADIUS 認証が成功した後にのみ機能し、認可情報は Access-Accept パケットに含まれます。リモートサーバーが使用できない場合に使用するバックアップ方法を構成できます。

LDAP authorization: LDAP 認証はリモート認証の一種です。NAS はリモートサーバーと連携してユーザーを認証します。LDAP 認証では、クライアントは LDAP 認証と同じタスクを実行しますが、検索条件を作成するときに認証情報とユーザーDN リストの両方を取得する点が異なります。

デバイスは、次のアカウンティング方式をサポートします。

No accounting: NAS はユーザーのアカウンティングを実行しません。
Local accounting: ローカルアカウンティングは NAS に実装されます。ローカルアカウンティングは、同じローカルユーザーカウントを使用する同時ユーザー数をカウントおよび制御しますが、課金に関する統計情報は提供しません。
RADIUS accounting: RADIUS アカウンティングはリモートアカウンティングの一種です。NAS はリモートサーバーと連動してアカウンティングを行います。高可用性を実現するために、ユーザーカウンティングに複数の RADIUS サーバーを指定できます。また、リモートサーバーが使用できない場合に使用するバックアップ方式を設定できます。

NAS では、各ユーザーは 1 つの ISP ドメインに属します。NAS は、ログイン時にユーザーが入力したユーザー名に基づいて、ユーザーが属する ISP ドメインを決定します。AAA は、ユーザーのアクセスタイプに基づいて、同じ ISP ドメイン内のユーザーを管理します。デバイスは、次のユーザークセスタイプをサポートします。

Login: ログインユーザーには、デバイスにログインする Telnet、FTP、および端末ユーザーが含まれます。端末ユーザーは、コンソールポートを介してにアクセスできます。
LAN access。
Portal ポータルユーザーがネットワークにアクセスするには、ポータル認証を通過する必要があります。
ADVPN。
SSL VPN。
PPP。

複数の ISP があるネットワークシナリオでは、デバイスは異なる ISP のユーザーに接続できます。デバイスは、システム定義の ISP ドメイン **syst** を含む複数の ISP ドメインをサポートします。デバイスでは、各ユーザーは ISP ドメインに属します。ユーザーがログイン時に ISP ドメイン名を提供しない場合、デバイスはユーザーが既定の ISP ドメインに属していると見なします。ISP ドメインを既定のドメインとして指定できます。

デバイスは、次の順序で各ユーザーの認証ドメインを選択します。

アクセスモジュールに指定された認証ドメイン。

ユーザー名の ISP ドメイン。
デバイスのデフォルトの ISP ドメイン。

RADIUS

Overview

Remote Authentication Dial-In User Service(RADIUS)は、クライアント/サーバーモデルを使用する分散情報対話プロトコルです。このプロトコルは、不正アクセスからネットワークを保護でき、高度なセキュリティーとリモートユーザーアクセスの両方を必要とするネットワーク環境でよく使用されます。

RADIUS client: RADIUS クライアントは、ネットワーク全体に配置された NAS 上で実行されます。RADIUS クライアントは、ユーザー情報を RADIUS サーバーに渡し、ユーザーアクセス要求の拒否や受け入れなどの応答に基づいて動作します。

RADIUS server: RADIUS サーバーはネットワークセンターのコンピュータまたはワークステーション上で実行され、ユーザー認証およびネットワークサービスアクセスに関連する情報を保持します。RADIUS サーバーは次のプロセスを使用して動作します。
RADIUS クライアントからの認証、認可、アカウンティング要求を受信します。
ユーザー認証、認可、またはアカウンティングを実行します。
ユーザーアクセス制御情報(ユーザーアクセス要求の拒否または受け入れなど)をクライアントに戻します。

RADIUS は UDP を使用してパケットを送信します。RADIUS クライアントとサーバーは、クライアントとサーバーで事前に設定された共有キーを使用して、相互に情報を交換します。
ユーザーに AAA サービスを提供するには、アクセスデバイス上で RADIUS サーバーパラメーターを設定する必要があります。

Enhanced RADIUS features

アカウンティングオン機能

この機能を使用すると、デバイス全体のリブート後に、デバイスから RADIUS サーバーにアカウンティングオンパケットが自動的に送信されます。アカウンティングオンパケットを受信すると、RADIUS サーバーはデバイスを介してオンラインになったすべてのオンラインユーザーをログアウトします。この機能がないと、ユーザーはリブート後に再びログインできません。これは、RADIUS サーバーがこれらのユーザーがまだオンラインであると判断するためです。
デバイスがアカウンティングオンパケットの再送信を待機する間隔と最大再試行回数を設定できます。

セッション制御機能

RADIUS サーバーは、セッション制御パケットを使用して、ユーザー認可情報を動的に変更したり、ユーザーを強制的に切断したりします。デバイスが UDP ポート 1812 で RADIUS セッション制御パケットを受信できるように、デバイスのセッション制御機能をイネーブルにします。
RADIUS セッション制御機能は、IMC 上で実行されている RADIUS サーバーだけで動作します。

オンラインユーザーパスワードの変更

この機能を使用すると、デバイスは RADIUS サーバーと連携して、ユーザーが自分のパスワードをオンラインで変更できるようになります。この機能を有効にすると、デバイスはオンラインユーザーからパスワード変更要求を受信すると、RADIUS サーバーに RADIUS 認証要求を送信します。認証要求では、デバイスは RADIUS 属性 2 の古いユーザーパスワードと RADIUS 属性 17 の新しいユーザーパスワードを伝送します。デバイスが RADIUS サーバーから応答を受信すると、オンラインユーザーのパスワードは正常に変更されます。

LDAP

Overview

Lightweight Directory Access Protocol(LDAP)は、標準のマルチプラットフォームディレクトリサービスを提供します。LDAP はクライアント/サーバーモデルを使用し、すべてのディレクトリー情報は LDAP サーバーに格納されます。
LDAP は、頻繁に変更されないデータの格納に適しています。このプロトコルは、ユーザー情報の格納に使用されます。たとえば、LDAP サーバーソフトウェア Active Directory サーバーは、Microsoft Windows オペレーティングシステムで使用されます。ソフトウェアは、ユーザーログインの認証および認可のためにユーザー情報およびユーザーグループ情報を格納します。
LDAP では、ディレクトリーを使用して組織情報、人事情報およびリソース情報が保守されます。ディレクトリーはツリー構造で編成され、エントリが含まれます。エントリは、識別名(DN)を持つ属性のセットです。属性は、ユーザー名、パスワード、電子メール、コンピュータ名および電話番号などの情報を格納するために使用されます。

LDAP attribute map

LDAP アトリビュートマップ機能を使用すると、デバイスは LDAP 認可サーバーから取得した LDAP アトリビュートを、マッピングエントリーに基づいてデバイスが認識できる AAA アトリビュートに変換できます。デバイスは認識できない LDAP アトリビュートを無視するため、無視できない重要な LDAP アトリビュートを含めるようにマッピングエントリーを設定します。
LDAP 属性は、1 つの AAA 属性にのみマッピングできます。異なる LDAP 属性は、同じ AAA 属性にマッピングできます。LDAP 属性マップは、LDAP-AAA 属性マッピングエントリーのリストを定義します。LDAP 属性マップを適用するには、認可に使用される LDAP スキームの LDAP 属性マップの名前を指定します。

RESTful server

RESTful サーバー構成は、デバイスが RESTful サーバーと通信するための関連パラメーター設定を定義します。パラメーターには、ログインアカウントおよび RESTful サーバーの URI が含まれます。RESTful サーバーとの接続が確立されると、デバイスはサーバーからアイデンティティーユーザーおよびオンラインユーザーをインポートできます。

Security management server set

セキュリティー管理サーバーセットの設定では、サーバーの IP アドレス、サーバーポート、サービスポート番号など、サードパーティ製サーバーと通信するためのデバイスの関連パラメーターが定義されます。サーバーとの接続が確立されると、デバイスはサーバーからユーザーログインおよびログアウト情報を受信して、オンラインユーザーを更新できます。

Restrictions and guidelines

Restrictions and guidelines: ISP domains

FTP ユーザーのアカウンティングはサポートされていません。
ISP ドメイン内の SSL VPN ユーザーに対して RADIUS およびその他の方式を使用する場合は、すべての方式の認証と認可の順序が同じであることを確認してください。
ISP ドメインで RADIUS 承認を成功させるには、認証と承認に同じ RADIUS スキームが使用されていることを確認します。
ISP ドメイン内の SSL VPN ユーザーに対して複数の認証方式を指定した場合、SSL VPN ユーザーのパスワードは、デバイスでオンラインになった後は変更できません。
ISP ドメイン内の SSL VPN ユーザーに対して LDAP スキームを指定した場合、SSL VPN ユーザーのパスワードは、デバイスでオンラインになった後は変更できません。
サーバーまたは NAS が認証されたユーザーに対して属性のタイプを許可しない場合、デバイスは ISP ドメイン内の属性をユーザーに許可します。
system という名前のシステム定義の ISP ドメインは削除できません。
ISP ドメインをブロックすると、ドメインのオフラインユーザーがネットワークサービスを要求できなくなります。ただし、オンラインユーザーは影響を受けません。

Restrictions and guidelines: RADIUS configuration

デバイスに設定されている共有キーが、RADIUS サーバーに設定されている共有キーと同じであることを確認します。

アクティブに使用されているアカウンティングサーバーを削除すると、デバイスはユーザーのリアルタイムアカウンティング要求およびアカウンティング停止要求を送信しなくなります。また、アカウンティング停止要求もバッファに格納されません。アカウンティングの結果が不正確になる可能性があります。
デバイスが送信する RADIUS パケットの送信元 IP アドレスが、RADIUS サーバー上で設定されている NAS の IP アドレスと一致していることを確認します。
アカウンティングを正確に行うために、デバイスと RADIUS アカウンティングサーバーに設定されているトラフィック統計情報の単位が同じであることを確認します。
2 つ以上の ISP ドメインが同じ RADIUS スキームを使用している場合は、ドメイン識別用のユーザー名に ISP ドメイン名を保持するように RADIUS スキームを設定します。
デバイスは、次の規則に基づいてサーバーを選択します。
プライマリサーバーがアクティブ状態の場合、デバイスは最初にプライマリサーバーとの通信を試行します。プライマリサーバーに到達できない場合、デバイスはサーバーが設定されている順序でアクティブなセカンダリサーバーを検索します。
1 つまたは複数のサーバーがアクティブ状態にある場合、デバイスは、サーバーが使用できない場合でも、これらのアクティブサーバーだけと通信しようとします。
すべてのサーバーがブロック状態にある場合、デバイスはプライマリサーバーとの通信だけを試行します。
サーバーに到達できない場合、デバイスはサーバーステータスをブロックに変更し、サーバーのクワイエットタイマーを開始します。次に、プライオリティが最も高いアクティブ状態の次のセカンダリサーバーとの通信を試行します。
サーバーの待機タイマーが期限切れになるか、サーバーを手動でアクティブ状態に設定すると、サーバーのステータスはアクティブに戻ります。デバイスは、認証またはアカウンティングプロセス中にサーバーを再チェックしません。
検索プロセスは、デバイスが使用可能なセカンダリサーバーを検出するか、アクティブ状態のすべてのセカンダリサーバーをチェックするまで続行されます。到達可能なサーバーがない場合、デバイスは認証またはアカウンティングの試行が失敗したと判断します。
RADIUS パケット送信試行の最大数および RADIUS サーバー応答タイムアウトタイマーを設定する場合は、セカンダリサーバーの数を考慮してください。RADIUS スキームに多数のセカンダリサーバーが含まれている場合は、再送信プロセスが長すぎる可能性があり、Telnet などのアクセスモジュールのクライアント接続がタイムアウトすることがあります。
サーバーの待機タイマーが正しく設定されていることを確認します。タイマーが短すぎると、認証またはアカウンティングの失敗が頻繁に発生する可能性があります。これは、デバイスがアクティブな状態にある到達不能なサーバーとの通信を試行し続けるためです。タイマーが長すぎると、障害から回復した到達可能なサーバーが一時的にブロックされる可能性があります。これは、サーバーがタイマーの期限が切れるまでブロックされた状態のままになるためです。
Reply-Message アトリビュート解析規則とともにオンラインユーザーパスワード変更機能を設定すると、オンラインユーザーパスワード変更機能は有効になりません。

Restrictions and guidelines: LDAP configuration

デバイスが LDAP 認可サーバーと連携する必要がある場合は、CLI でデバイスに関連する LDAP 設定を行う必要があります。

Configure authentication

異なる ISP のユーザーを管理するには、各 ISP ドメインに対して異なるアクセスの種類の認証、承認、およびアカウンティングの方法を指定し、必要に応じてドメイン属性を構成します。ドメイン属性には、ISP ドメインの状態と、ISP ドメイン内のユーザーの承認属性が含まれます。

ローカル認証を実行するには、ローカルユーザーと関連アトリビュートを設定します。
リモート認証を実行するには、必要な RADIUS スキームを設定します。

Configure an ISP domain

Objects タブをクリックします。
ナビゲーションペインで、**User** > **Authentication** > **ISP Domains** を選択します。
Create をクリックします。
ISP ドメインを作成します。

表 1 ISP ドメインの構成項目

項目	説明
Domain name	ISP ドメインの名前を入力します。 ISP ドメイン名は、大文字と小文字を区別しない 1～255 文字の文字列で、ISP ドメインを一意に識別します。名前は次の要件を満たす必要があります。 スラッシュ(/)、バックスラッシュ(¥)、縦棒(|)、引用符(")、コロン(:)、アスタリスク(*)、疑問符(?)、左山カッコ(<)、右山カッコ(>)、アットマーク(@)は使用できません。 **d**、**de**、**def**、**defa**、**defau**、**default**、**default**、**i**、**if**、**if-**、**if-u**、**if-un**、**if-unk**、**if-unkn**、**if-unkno**、**if-unknow**、または **if-unknown** は使用できません。
Status	ISP ドメインの状態を選択します。 **Active**: ISP ドメインをアクティブ状態にして、ISP ドメイン内のユーザーがネットワークサービスを要求できるようにします。 **Blocked**: ISP ドメインをブロック状態にして、ISP ドメイン内のユーザーがネットワークサービスを要求できないようにします。

Access types	ISP ドメイン内のユーザーのアクセスタイプを選択します。 ユーザーのアクセス認証要件に基づいて、ユーザーのアクセスタイプを選択します。たとえば、管理者の場合は **Login** を選択します。

(オプション) advanced settings を構成します。

表 2 詳細設定の構成項目

項目	説明
Idle timeout	アイドルタイムアウト時間を設定します。 アイドルタイムアウト期間中のユーザーの合計トラフィックが、指定された最小トラフィックよりも少ない場合、デバイスはユーザーをログアウトします。
Min traffic in an idle timeout	アイドルタイムアウト期間に生成する必要がある最小トラフィックを設定します。
IP address pool	IP アドレスプールの名前を入力します。 デバイスは、認証された各 PPP ユーザーまたはポータルユーザーに IP アドレスプールの IP アドレスを割り当てます。

OK をクリックします。新しい ISP ドメインが **ISP Domains** ページに表示されます。

Configure RADIUS

Objects タブをクリックします。

ナビゲーションペインで、**User** > **Authentication** > **RADIUS** の順に選択します。

Create をクリックします。

RADIUS スキームを作成します。

表 3 RADIUS スキームの構成項目

項目	説明
Authentication servers	認証サーバーを作成、編集、または削除します。 構成項目には、IP アドレス、ポート番号、および共有キーが含まれます。
Accounting servers	アカウンティングサーバーを作成、編集、または削除します。 構成項目には、IP アドレス、ポート番号、および共有キーが含まれます。
Advanced settings	必要に応じて、スキームの詳細設定を行います。

OK をクリックします。新しい RADIUS スキームが **RADIUS** ページに表示されます。

Configure LDAP

LDAP スキームを設定するには:

Objects タブをクリックします。
ナビゲーションペインで、**User** > **Authentication** > **LDAP** > **LDAP Schemes** を選択します。
Create をクリックします。
LDAP スキームを作成します。

表 4 LDAP スキームの構成項目

項目	説明
Name	LDAP スキームの名前を入力します。 スキーム名は、LDAP スキームを一意に識別します。
LDAP attribute map	LDAP 認可用の LDAP アトリビュートマップを選択します。 デバイスは、LDAP 認可サーバーから取得した LDAP アトリビュートをデバイスで認識可能な AAA アトリビュートに変換します。
Authentication server	LDAP 認証サーバーの名前を入力します。 デバイスとサーバーが確実に接続を確立できるように、LDAP 認証サーバーのパラメーターを設定できます。
Authorization server	LDAP 許可サーバーの名前を入力します。 デバイスとサーバーが接続を確立できるように、LDAP 認可サーバーのパラメーターを設定できます。

OK をクリックします。新しい LDAP スキームが **LDAP Schemes** ページに表示されます。

LDAP サーバーを構成するには:

Objects タブをクリックします。
ナビゲーションペインで、**User** > **Authentication** > **LDAP** > **LDAP Servers** を選択します。
Create をクリックします。
LDAP サーバーを作成します。

表 5 LDAP サーバーの構成項目

項目	説明
Name	LDAP サーバーの名前を入力します。 サーバー名は、LDAP サーバーを一意に識別します。
VRF	LDAP サーバーが属する VRF を選択します。

	LDAP サーバーがパブリックネットワークに属している場合は、この項目を設定しないでください。
IP address type	LDAP サーバーの IP アドレスタイプを選択します。 使用可能な IP アドレスの種類には、IPv4 と IPv6 があります。
Server IP address	LDAP サーバーの IP アドレスを入力します。
Port	LDAP サーバーのサービスポート番号を入力します。
Source address type	LDAP サーバーに送信される LDAP パケットの送信元アドレスタイプを選択します。 オプションは、送信元 IP アドレスと送信元インターフェースです。
Source IPv4 address	LDAP サーバーに送信される LDAP パケットの送信元 IP アドレスとして IPv4 アドレスを指定します。
Source IPv6 address	LDAP サーバーに送信される LDAP パケットの送信元 IP アドレスとして IPv6 アドレスを指定します。
Source interface	LDAP サーバーに送信される LDAP パケットの送信元 IP アドレスを提供するインターフェースを選択します。 このパラメーターは、送信元アドレスタイプが送信元インターフェースの場合にだけ使用できます。
Administrator DN	管理者 DN を入力します。 デバイスの管理者 DN は、LDAP サーバーで設定されている管理者 DN と同じである必要があります。
Administrator password	管理者パスワードを入力します。
LDAP version	LDAP バージョンを選択します。 使用可能な LDAP バージョンには、LDAPv2 および LDAPv3 があります。 デバイスが使用する LDAP バージョンは、LDAP サーバーが使用するバージョンと一致している必要があります。
Server timeout period	LDAP サーバーのタイムアウト時間を設定します。 デバイスがサーバーのタイムアウト時間内にサーバーの応答を受信せずに LDAP サーバーにバインド要求または検索要求を送信すると、認証要求または認可要求はタイムアウトになります。
Base DN for user search	ユーザー検索のベース DN を入力します。 LDAP サーバーに多くのディレクトリレベルが含まれている場合、ルートディレクトリから開始するユーザーDN 検索には時間がかかることがあります。効率を向上させるために、検索ベース DN を指定して開始点を変更できます。
User search scope	ユーザー検索範囲を選択します。 **All-level**: ユーザー検索はベース DN のすべてのサブディレクトリを通過します。

	Single-level: ユーザー検索は、ベース DN の下の 1 つ下のレベルのサブディレクトリだけを検索します。
Username attribute	ユーザー名属性の値を入力します。デフォルト値は **cn** です。
Username format	LDAP サーバーに送信するユーザー名の形式を選択します。 **With-domain** :LDAP サーバーに送信されるユーザー名に ISP ドメイン名を含めます。 **Without-domain**: LDAP サーバーに送信されるユーザー名から ISP ドメイン名を除外します。
User object class	ユーザー検索用のユーザーオブジェクトクラスを入力します。
User group filter	ユーザーグループフィルタを入力します。 デバイスが LDAP サーバーからのユーザーグループ情報のインポートを要求すると、LDAP サーバーはユーザーグループフィルタに一致するユーザーグループだけをデバイスに送信します。

OK をクリックします。新しい LDAP サーバーが **LDAP Servers** ページに表示されます。

Configure a RESTful server

Objects タブをクリックします。
ナビゲーションペインで、**User** > **Authentication** > **RESTful Server** を選択します。
Create をクリックします。
RESTful サーバーを作成します。

表 6 RESTful なサーバー構成項目

項目	説明
Name	RESTful サーバーの名前を入力します。 この名前は RESTful サーバーを一意に識別します。
Username	RESTful サーバーにログインするためのユーザー名を入力します。
Password	RESTful サーバーにログインするためのパスワードを入力します。
Get-user-account URI	RESTful サーバーからユーザーカウント情報を要求するために使用する URI を入力します。
Get-online-user URI	RESTful サーバーからオンラインユーザー情報を要求するために使用する URI を入力します。
Get-user-group URI	RESTful サーバーからユーザーグループ情報を要求するために使用する URI を入力します。
Put-online-user URI	オンラインユーザー情報を RESTful サーバーにアップロードするために使用する URI を入力します。

	デバイスが RESTful サーバーからインポートされていないアイデンティティーユーザーを追加すると、デバイスはオンラインユーザー情報を RESTful サーバーにアップロードします。
Put-offline-user URI	オフラインユーザー情報を RESTful サーバーにアップロードするために使用する URI を入力します。 デバイスは、RESTful サーバーからインポートされていないアイデンティティーユーザーを削除すると、オフラインユーザー情報を RESTful サーバーにアップロードします。
VRF	RESTful サーバーが属する VRF を選択します。 RESTful サーバーがパブリックネットワークに属している場合は、この項目を構成しないでください。
Enable server detection	RESTful サーバーの到達可能性検出を有効にするには、この項目を選択します。 この機能がイネーブルの場合、デバイスは RESTful サーバーの到達可能性を検出します。

OK をクリックします。**RESTful Server** ページに新しい RESTful サーバーが表示されます。

Configure a security management server set

Objects タブをクリックします。

ナビゲーションペインで、**User** > **Authentication** > **Sec Mgt Server Set** を選択します。

Create をクリックします。

セキュリティー管理サーバーセットを作成します。

表 7 セキュリティー管理サーバーセットの構成項目

項目	説明
Name	セキュリティー管理サーバーセットの名前を入力します。 この名前は、セキュリティー管理サーバーセットを一意に識別します。
Server addresses	TSM サーバーの IP アドレスを入力します。
Listening port	TSM サーバーからのパケットをリスンするポートを入力します。
Encryption algorithm	TSM サーバーからのパケットを復号化するための暗号化アルゴリズムを選択します。
Shared key	TSM サーバーからのパケットを復号化するための共有キーを入力します。

OK をクリックします。新しく作成されたセキュリティー管理サーバーセットが **Security Management Server Set** ページに表示されます。

Portal

このヘルプには、次のトピックがあります。

Introduction
Portal authentication server
Portal Web server
Local portal Web server
Portal-free rule
Interface portal policies
Restrictions and guidelines

Introduction

ポータル認証は、ネットワークへのユーザーアクセスを制御します。ポータルは、ユーザーがポータル認証ページで入力したユーザー名とパスワードでユーザーを認証します。したがって、ポータル認証は Web 認証とも呼ばれます。
ポータル認証は、アクセスレイヤーおよび重要なデータエントリに対してアクセス制御を柔軟に適用します。ポータル認証には次の利点があります:

クライアントソフトウェアをインストールしなくても、Web ページを通じて認証を実行できます。
ISP に多様な管理オプションと拡張機能を提供します。たとえば、ISP は広告を掲載したり、コミュニティサービスを提供したり、認証ページに情報を公開したりできます。
複数の認証モードをサポートします。たとえば、再 DHCP 認証では、柔軟なアドレス割り当てスキームが実装され、パブリック IP アドレスが保存されます。クロスサブネット認証では、アクセスデバイスとは異なるサブネットに存在するユーザーを認証できます。

一般的なポータルシステムは、次のコンポーネントで構成されます。

Authentication client: 認証クライアントは、HTTP/HTTPS を実行する Web ブラウザ、またはポータルクライアントアプリケーションを実行するユーザーホストです。

Access device: アクセスデバイスとは、スイッチ、ルータ、ファイアウォールデバイスなどのブロードバンドアクセスデバイスを指します。

Portal authentication server: ポータル認証サーバーは、認証クライアントから認証要求を受信し、アクセスデバイスと対話してユーザーを認証します。

Portal Web server: ポータル Web サーバーは、Web 認証ページを認証クライアントにプッシュし、ユーザー認証情報(ユーザー名とパスワード)をポータル認証サーバーに転送します。ポータル Web サーバーは、ポータル認証サーバーまたは独立したサーバーと統合できます。

AAA server: AAA サーバーはアクセスデバイスと対話して、ポータルユーザーの認証、認可、アカウンティングを実行します。

Portal authentication server

Portal authentication server detection

ポータル認証中に、アクセスデバイスとポータル認証サーバー間の通信が切断されると、新規ポータルユーザーはログインできず、オンラインポータルユーザーは正常にログアウトできません。この問題に対処するには、アクセスデバイスがポータルサーバーの到達可能性の変更を迅速に検出し、変更に対応するアクションを実行できる必要があります。
ポータル認証サーバー検出機能を使用すると、デバイスは定期的にポータル認証サーバーからのポータルパケットを検出して、サーバーの到達可能性を判断できます。デバイスが検出タイムアウト内にポータルパケットを受信し、そのパケットが有効である場合、デバイスはポータル認証サーバーが到達可能であると判断します。有効でない場合、デバイスはポータル認証サーバーが到達不能であると判断します。ポータルパケットには、ユーザーログインパケット、ユーザーログアウトパケット、およびハートビートパケットが含まれます。サーバーの到達可能性ステータスが変化したときに、次の 1 つ以上のアクションを実行するようにデバイスを設定できます。

NMS へのトラップメッセージの送信。トラップメッセージには、ポータル認証サーバーの名前と現在の状態が含まれています。
ポータル認証サーバーの名前、現在の状態、および元の状態を含むログメッセージを送信する。

Portal user synchronization

アクセスデバイスがポータル認証サーバーとの通信を失うと、通信が再開された後に、アクセスデバイス上のポータルユーザー情報とポータル認証サーバー上のポータルユーザー情報が一致しなくなる可能性があります。この問題に対処するために、デバイスはポータルユーザー同期機能を提供します。この機能は、次のように、ポータル同期パケットを送信および検出することによって実装されます。

ポータル認証サーバーは、ユーザーハートビート間隔で、オンラインユーザー情報を同期パケットでアクセスデバイスに送信します。ユーザーハートビート間隔は、ポータル認証サーバーで設定されます。
同期パケットを受信すると、アクセスデバイスは、パケットに含まれるユーザーを自身のユーザーリストと比較し、次の操作を実行します。
パケットに含まれるユーザーがアクセスデバイス上に存在しない場合、アクセスデバイスはポータル認証サーバーにユーザーを削除するように通知します。アクセスデバイスは、ユーザーがログインするとすぐに同期検出タイマーを開始します。
同期検出期間内にユーザーがどの同期パケットにも現れない場合、アクセスデバイスは、ユーザーがポータル認証サーバー上に存在しないと見なし、ユーザーをログアウトさせます。

Portal Web server

Parameters carried in the portal Web server URL

ユーザーIP アドレス、ユーザーMAC アドレス、最初に要求された URL などのパラメーターを構成して、ポータル Web サーバーURL に追加できます。URL パラメーターを構成すると、デバイスはこれらのパラメーターとともにポータル Web サーバーURL をポータルユーザーに送信します。たとえば、ポータル Web サーバーの URL が **http://www.test.com/portal**,であり、ユーザーIP アドレスと元の URL **http://www.abc.com/welcome** をサーバーURL に追加するとします。次に、アクセスデバイスは 1.1.1.1 のユーザーに URL **http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome** を送信します。

Portal Web server detection

アクセスデバイスとポータル Web サーバー間の通信が切断されている場合、ポータル認証プロセスは完了できません。この問題に対処するには、アクセスデバイスでポータル Web サーバーの検出を有効にします。
ポータル Web サーバー検出機能を使用すると、アクセスデバイスは Web アクセスプロセスをシミュレートして、ポータル Web サーバーへの TCP 接続を開始します。TCP 接続が正常に確立された場合、アクセスデバイスは検出が成功したと見なし、ポータル Web サーバーは到達可能です。それ以外の場合は、検出が失敗したと見なします。アクセスデバイスのインターフェースのポータル認証ステータスは、ポータル Web サーバー検出機能に影響しません。

検出パラメーター
Detection interval: デバイスがサーバーの到達可能性を検出する間隔。
Max detection attempts: 連続して検出に失敗した回数がこの値に達すると、アクセスデバイスは、ポータル Web サーバーが到達不能であると見なします。

サーバーの到達可能性ステータスが変更されたときに実行するアクション

Log: NMS にトラップメッセージを送信します。トラップメッセージには、ポータル Web サーバーの名前と現在の状態が含まれます。

Trap: ポータル Web サーバーの名前、現在の状態、および元の状態を含むログメッセージを送信します。

Local portal Web server

System components

アクセスデバイスは、ポータルユーザーにローカルポータルサービスを提供するローカルポータル Web サーバー機能をサポートします。この機能により、アクセスデバイスはポータル Web サーバーおよびポータル認証サーバーとしても機能します。この場合、ポータルシステムは、認証クライアント、アクセスデバイスおよび認証/アカウンティングサーバーの 3 つのコンポーネントのみで構成されます。

Client and local portal Web server interaction protocols

HTTP および HTTPS は、認証クライアントとローカルポータル Web サーバー間の対話に使用できます。HTTP を使用すると、HTTP パケットがプレーンテキストで転送されるため、セキュリティー上の問題が発生する可能性があります。HTTPS を使用すると、HTTP パケットが SSL によって保護されるため、安全なデータ伝送が保証されます。

Portal page customization

ローカルポータル Web サーバーは、カスタムポータル認証ページをサポートしています。複数の認証ページセットをカスタマイズし、各ページセットを.zip ファイルに圧縮し、圧縮したファイルをデバイスの記憶域メディアにアップロードできます。

ローカルポータル Web サーバーがポータル認証中に認証ページをユーザーにプッシュするには、カスタム認証ページファイルをデフォルトの認証ページファイルとして指定する必要があります。デフォルトの認証ページファイルとして認証ページファイルが指定されていない場合、ローカルポータル Web サーバー機能は実装できません。

Custom authentication pages

認証ページは HTML ファイルです。ローカルポータル認証には、ログオンページ、ログオン成功ページ、ログオン失敗ページ、オンラインページ、システムビジーページおよびログオフ成功ページの各認証ページが必要です。認証ページをカスタマイズする必要があります。これには、認証ページが使用するページ要素(たとえば、認証ページ **Logon.htm** 用の **back.jpg**)も含まれます。

認証ページファイルを編集するときは、認証ページのカスタマイズ規則に従ってください。

File name rules

メイン認証ページファイルの名前は固定されています(表 1 を参照)。

表 1 メイン認証ページのファイル名

メイン認証ページ	[ファイル名]
Logon page	ログオン.htm
Logon success page	logonSuccess.htm
Logon failure page	logonFail.htm
Online page Pushed after the user gets online for online notification	オンライン.htm
System busy page Pushed when the system is busy or the user is in the logon process	busy.htm(ビジー)
Logoff success page	logoffSuccess.htm

メイン認証ページファイル以外のファイルの名前を定義できます。ファイル名およびディレクトリー名では、大文字と小文字は区別されません。

Page request rules

ローカルポータル Web サーバーは、Get 要求と Post 要求のみをサポートします。

Get requests: 認証ページの静的ファイルを取得し、再帰を許可しない場合に使用します。たとえば、ファイル Logon.htm にファイル **ca.htm** に対する Get アクションを実行するコンテンツが含まれている場合、ファイル **ca.htm** にはファイル Logon.htm への参照を含めることはできません。

Post requests: ユーザーがユーザー名とパスワードのペアを送信し、ログインおよびログアウトするときに使用されます。

Post request attribute rules

認証ページのフォームを編集する場合は、次の要件に従ってください。
認証ページは複数のフォームを持つことができますが、アクションが **logon.cgi** であるフォームは 1 つだけである必要があります。そうでない場合、ユーザー情報はローカルポータル Web サーバーに送信できません。
ユーザー名属性は **PtUser** に固定されています。パスワード属性は **PtPwd** に固定されています。
PtButton 属性の値は **Logon** または **Logoff** であり、ユーザーが要求するアクションを示します。
ログオン Post 要求には、**PtUser**、**PtPwd**、および **PtButton** の属性が含まれている必要があります。
ログオフ Post 要求には **PtButton** 属性が含まれている必要があります。
認証ページ **logon.htm** および **logonFail.htm** には、ログオン Post 要求が含まれている必要があります。
次の例は、**logon.htm** ページ内のスクリプトの一部を示しています。

```
<form action=logon.cgi method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px"
maxlength=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px"
maxlength=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;”>
</form>
```

認証ページ **logonSuccess.htm** および **online.htm** には、ログオフ Post 要求が含まれている必要があります。
次の例は、ページ内の **online.htm** スクリプトの一部を示しています。

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

Page file compression and saving rules
認証ページとそのページ要素は、標準 zip ファイルに圧縮する必要があります。zip ファイルの名前に使用できるのは、文字、数字およびアンダースコアのみです。
認証ページは、zip ファイルのルートディレクトリに配置する必要があります。

Redirecting authenticated users to a specific webpage

デバイスが認証されたユーザーを特定の Web ページに自動的にリダイレクトするようにするには、logon.htm および logonSuccess.htm で次の操作を行います。
logon.htm で、Form の target 属性を**_blank** に設定します。

内容はグレーで表示されます。

<form method=post action=logon.cgi target="_blank">
pt_init()をロードするページの関数を logonSuccess.htm に追加します。

内容はグレーで表示されます。

```
<html>
<head>
<title>LogonSuccessed</title>
<script type="text/javascript" language="javascript" src="pt_private.js"></script>
</head>
<body onload="pt_init();" onbeforeunload="return pt_unload();">
... ...
</body>
</html>
```

Portal-free rule

ポータルフリー規則を使用すると、指定されたユーザーは、ポータル認証なしで指定された外部 Web サイト(規則の送信元および宛先情報によって決定されます)にアクセスできます。
ポータルフリールールの一致項目には、送信元/宛先 IP アドレス、TCP/UDP ポート番号、送信元 MAC アドレス、アクセスインターフェース、および VLAN が含まれます。ポータルフリールールに一致するパケットはポータル認証をトリガーしないため、パケットを送信するユーザーは指定された外部 Web サイトに直接アクセスできます。

Interface portal policies

Portal fail-permit

ポータルの fail-permit 機能は、ポータル認証サーバーまたはポータル Web サーバーが到達不能である場合に有効になります。アクセスデバイスは、ポータル認証サーバーまたはポータル Web サーバーが到達不能であることを検出すると、インターフェース上のユーザーがポータル認証なしでネットワークにアクセスできるようにします。

BAS-IP or BAS-IPv6 attribute

デバイスは、設定された BAS-IP または BAS-IPv6 アドレスを、ポータル認証サーバーに送信されるポータル通知の送信元 IP アドレスとして使用します。
BAS-IP または BAS-IPv6 アトリビュートを設定しない場合、デバイスは、ポータル認証サーバーに送信さ

れるポータルパケットの送信元 IP アドレスを次のように選択します。

ポータル認証サーバーに送信される IPv4 ポータル応答パケットの BAS-IP 属性は、パケットの送信元 IPv4 アドレスです。ポータル認証サーバーに送信される IPv6 ポータル応答パケットの BAS-IPv6 属性は、パケットの送信元 IPv6 アドレスです。
ポータル認証サーバーに送信される IPv4 ポータル通知パケットの BAS-IP 属性は、パケットの発信インターフェースの IPv4 アドレスです。ポータル認証サーバーに送信される IPv6 ポータル通知パケットの BAS-IPv6 属性は、パケットの発信インターフェースの IPv6 アドレスです。

Online user detection

この機能は、ポータルユーザーの異常なログアウトを迅速に検出します。ARP または ICMP 検出は IPv4 ポータルユーザーに適用され、ND または ICMPv6 検出は IPv6 ポータルユーザーに適用されます。
ARP および ND 検出は、直接および再 DHCP ポータル認証にだけ適用されます。ICMP 検出は、すべてのポータル認証モードに適用されます。
アイドル時間内にデバイスがポータルユーザーからパケットを受信しない場合、デバイスは次のようにユーザーのオンラインステータスを検出します。

ICMP or ICMPv6 detection: 設定可能な間隔で ICMP または ICMPv6 要求をユーザーに送信して、ユーザーステータスを検出します。
デバイスが最大検出試行回数内に応答を受信した場合、デバイスはユーザーがオンラインであると見なし、検出パケットの送信を停止します。その後、デバイスはアイドルタイマーをリセットし、タイマーの期限が切れると検出プロセスを繰り返します。
最大回数の検出試行後にデバイスが応答を受信しない場合、デバイスはユーザーをログアウトします。

ARP or ND detection: ARP または ND 要求をユーザーに送信し、設定可能な間隔でユーザーの ARP または ND エントリステータスを検出します。
ユーザーの ARP または ND エントリが検出試行の ND エントリが更新された場合、デバイスはユーザーがオンラインであると見なし、ユーザーの ARP または ND エントリの検出を停止します。その後、デバイスはアイドルタイマーをリセットし、タイマーの期限が切れると検出プロセスを繰り返します。
最大回数の検出試行後にユーザーの ARP または ND エントリがリフレッシュされない場合、デバイスはユーザーをログアウトします。

Restrictions and guidelines

Restrictions and guidelines: Portal authentication server detection

ハートビートパケットの送信をサポートしているのは、IMC ポータル認証サーバーだけです。ハートビートパケットを検出してサーバーの到達可能性をテストするには、IMC ポータル認証サーバーでサーバーハートビート機能をイネーブルにする必要があります。
ポータル認証サーバーの到達可能性ステータスが変化したときに、1 つ以上のアクションを実行するようにデバイスを設定できます。

Restrictions and guidelines: Portal user synchronization

ポータルユーザー同期では、ポータル認証サーバーがポータルユーザーハートビート機能をサポートしている必要があります。ポータルユーザーハートビート機能をサポートしているのは、IMC ポータル認証サーバーのみです。ポータルユーザー同期機能を実装するには、ポータル認証サーバーでユーザーハートビート機能も構成する必要があります。ポータル認証サーバーで構成されたユーザーハートビート間隔が、アクセスデバイスで構成された同期検出タイムアウトよりも大きくないことを確認してください。

Restrictions and guidelines: The local portal Web server feature

ローカルポータル Web サーバー機能は、いくつかの単純なポータルサーバー機能のみを実装します。ユーザーが Web インターフェースを介してログインおよびログアウトできるのは、この機能のみです。独立したポータル Web および認証サーバーのかわりにはなりません。
構成できるのは、1 つの HTTP ベースのローカルポータル Web サーバーと 1 つの HTTPS ベースのローカルポータル Web サーバーのみです。
SSL サーバーポリシーが HTTPS ベースのローカルポータル Web サーバーに指定されている場合、サーバーのサービスポート番号としてポート 443 を指定することはできません。

Restrictions and guidelines: Portal-free rules

VLAN とインターフェースの両方を指定する場合、インターフェースは VLAN に属している必要があります。そうでない場合、ポータルフリールールは有効になりません。
同じフィルタリング基準で複数のポータルフリールールを設定することはできません。設定しないと、ルールがすでに存在することを示すプロンプトが表示されます。
ポータル認証が有効かどうかにかかわらず、ポータルフリールールは追加または削除のみ可能です。変更はできません。

Restrictions and guidelines: The BAS-IP or BAS-IPv6 attribute

デバイスで Portal 2.0 が実行されている場合、ポータル認証サーバーに送信される非送信請求パケットは BAS-IP アトリビュートを伝送する必要があります。デバイスで Portal 3.0 が実行されている場合、

ポータル認証サーバーに送信される非送信請求パケットは BAS-IP または BAS-IPv6 アトリビュートを伝送する必要があります。
re-DHCP ポータル認証中に、デバイスはポータル通知パケットをポータル認証サーバーに送信します。認証を完了するには、BAS-IP/BAS-IPv6 属性が、ポータル認証サーバーで指定されたデバイス IP または IPv6 アドレスと同じであることを確認します。
次の条件が満たされる場合は、ポータル認証がイネーブルになっているインターフェースで BAS-IP または BAS-IPv6 アトリビュートを設定する必要があります。
ポータル認証サーバーは IMC サーバーです。
ポータル認証サーバーで指定されたポータルデバイスの IP アドレスが、ポータルパケット出力インターフェースの IP アドレスではありません。

IPS

このヘルプには、次のトピックが含まれています。

- Introduction
  - IPS functions
  - IPS profiles
  - IPS actions
  - IPS mechanism
- Restrictions and guidelines
- Configure IPS
  - Configure an IPS profile
  - Import or delete Snort signatures
  - Create and delete user-defined IPS signatures
  - Export all signatures in the signature library
  - Configure IPS whitelist

Introduction

Intrusion Prevention System(IPS)機能を使用すると、デバイスはネットワークトラフィックを監視して悪意のあるアクティビティを検出し、予防的なアクションを事前に実行できます。

IPS functions

IPS には次の機能があります。

- **In-depth protection**: IPS は、パケットのアプリケーション層データを検査し、ネットワークトラフィックフローのプロトコル分析と再構成を実行し、分析結果に従ってアクションを実行します。

- **Real-time protection**: IPS はネットワークトラフィックをリアルタイムで監視し、検出された攻撃に対してアクションを実行できます。

- **All-Around Protection** : IPS は、次のタイプの攻撃を検出して防止できます。
  - ワーム、ウィルス、トロイの木馬、ボット、スパイウェア、アドウェア、スキャナ、バックドアなどの悪意のあるソフトウェア。
  - Common Gateway Interface(CGI)攻撃、クロスサイトスクリプティング攻撃、インジェクション攻撃、ディレクトリートラバーサル攻撃、情報漏えい攻撃、リモートファイルインクルージョン攻撃、バッファオーバーフロー攻撃、コード実行攻撃、DoS 攻撃などの悪意のある攻撃。

- **Bidirectional protection**: IPS は着信トラフィックと発信トラフィックの両方を監視して、内部ネットワークと外部ネットワークから発生する攻撃を防止します。

IPS profiles

IPS は IPS プロファイルに基づいて実装されます。IPS プロファイルには、パケットを照合するための一連の IPS シグニチャと、一致するパケットに対するアクションが含まれています.

IPS signatures

デバイスはパケットを IPS シグニチャと比較して、ネットワーク攻撃を検出、分類、および防止します。各 IPS シグニチャには、攻撃カテゴリ、アクション、保護ターゲット、重大度、および方向などのさまざまなアトリビュートが含まれています。デフォルトでは、IPS プロファイルはデバイス上でイネーブルになっているすべての IPS シグニチャを使用します。シグニチャアトリビュートに基づいて、IPS プロファイルが使用する IPS シグニチャをフィルタリングする基準を設定できます。
デバイスは、次のタイプの IPS シグニチャをサポートしています。

- **Predefined IPS signatures**: ローカルシグニチャライブラリに基づいてデバイスによって自動的に生成されます。定義済み IPS シグニチャを追加、変更、または削除することはできません。

- **User-defined IPS signatures**: 事前定義のシグニチャでは検出できない攻撃については、ユーザー定義の IPS シグニチャを作成できます。ユーザー定義のシグニチャを変更および削除することもできます。

- **Snort signatures**: Snort ファイルからインポートされます。Snort シグニチャをインポートおよび削除できます。

定義済み、ユーザー定義、および Snort IPS シグニチャには、デフォルトのシグニチャアクションとイネーブルステータスがあります。
IPS プロファイル内の IPS 署名のアクションを変更するには、IPS 署名を選択し、IPS 署名の設定をカスタマイズします。IPS プロファイル内の署名が有効な状態でない場合は、署名の状態を有効に変更できます。IPS 署名用にカスタマイズされたアクションは、IPS プロファイル内のデフォルトの署名アクションより優先されます。IPS アクションの詳細は、「IPS アクション」を参照してください。非アクティブな IPS 署名を IPS プロファイルに追加することもできます。非アクティブな IPS 署名を追加する方法の詳細は、「IPS プロファイルの設定」を参照してください。

IPS actions

デバイスは、IPS シグニチャに一致するパケットを検出すると、そのパケットのシグニチャに指定されたアクションを実行します。

デバイスは、次の IPS アクションをサポートします。

- **Blacklist**: 一致するパケットをドロップし、パケットの送信元を IP ブラックリストに追加します。IP ブラックリスト機能がイネーブルになっている場合、ブラックリストに掲載された送信元からのパケットはブラックリスト期間中ブロックされます。IP ブラックリスト機能がイネーブルになっていない場合、ブラックリストに掲載された送信元からのパケットはブロックされません。

  IP ブラックリスト機能の詳細については、攻撃防御のオンラインヘルプを参照してください。
- **drop**: 一致するパケットをドロップします。
- **Permit** 一致するパケットの通過を許可します。
- **Reset**: TCP リセットメッセージまたは ICMP ポート到達不能メッセージを送信して、一致するパケットの TCP 接続または UDP 接続を閉じます。
- **redirect**: 一致するパケットを Web ページにリダイレクトします。
- **Predefined action**: シグニチャライブラリ内の定義済みシグニチャアクションを使用して、一致するパケットを処理します。
- **Capture**: 一致するパケットをキャプチャします。
- **Logging**: 一致するパケットを記録します。

IPS mechanism

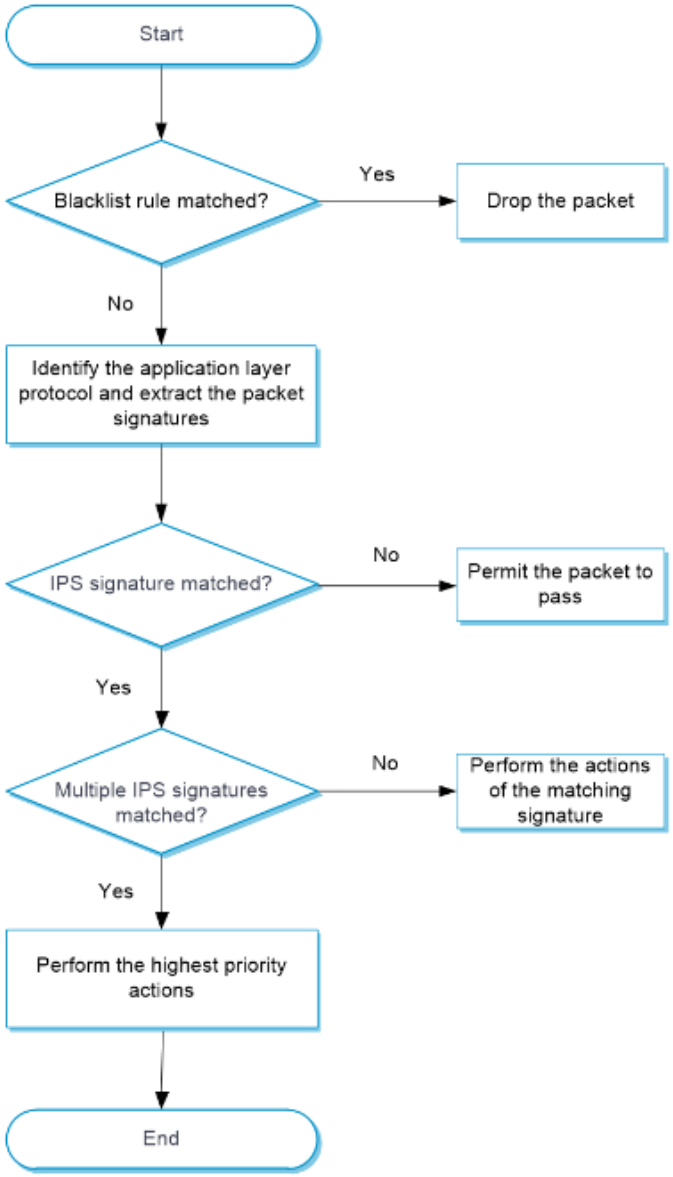
図 1 に示すように、デバイスはパケットを受信すると、以下の動作を行います。

1. デバイスはパケットを IP ブラックリストルールと比較します。
   - 一致するルールが見つかった場合、デバイスはパケットをドロップします。
   - 一致するルールが見つからない場合、デバイスはステップ 2 に進みます。
2. デバイスは、パケットをセキュリティーポリシーと比較します。

   パケットが IPS プロファイルに関連付けられたセキュリティーポリシーと一致する場合、デバイスはパケットアプリケーション層プロトコルを識別し、パケットシグニチャを抽出します。
3. デバイスは、抽出されたパケットシグニチャを IPS プロファイル内の IPS シグニチャと比較することによって、パケットに対するアクションを決定します。
   - パケットがどの IPS シグニチャとも一致しない場合、デバイスはパケットの通過を許可します。
   - パケットが 1 つの IPS シグニチャだけと一致する場合、デバイスはシグニチャアクションを実行します。
   - パケットが複数の IPS シグニチャと一致する場合、デバイスは次の規則を使用してアクションを選択します。

- 一致する IPS シグニチャに **redirect**, **drop, permit**、**reset** トなどの 2 つ以上のアクションがある場合、デバイスは最も高い優先順位のアクションを実行します。優先順位の高いアクションは、**reset**, **redirect**, **drop**, **permit** の順です。
- デバイスは、**blacklist**, **capture**,および **logging** アクションが一致する IPS シグニチャに含まれている場合、それらのアクションを実行します。

図 1 IPS メカニズム



Restrictions and guidelines

- IPS プロファイルを作成、編集、または削除した後、設定を有効にするには、設定をアクティブにする必要があります。**Submit** をクリックして設定をすぐにアクティブにするか、デフォルトで設定が 40 秒後に自動的にアクティブになります。設定をアクティブにすると、DPI サービスが一時的に中断されます。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。

- IPS モジュールをデバイスで実行するには、ライセンスが必要です。ライセンスの有効期限が切れた場合でも、IPS 機能を使用できますが、デバイスの IPS シグニチャライブラリをアップグレードできません。ライセンスの詳細については、ライセンスのオンラインヘルプを参照してください。

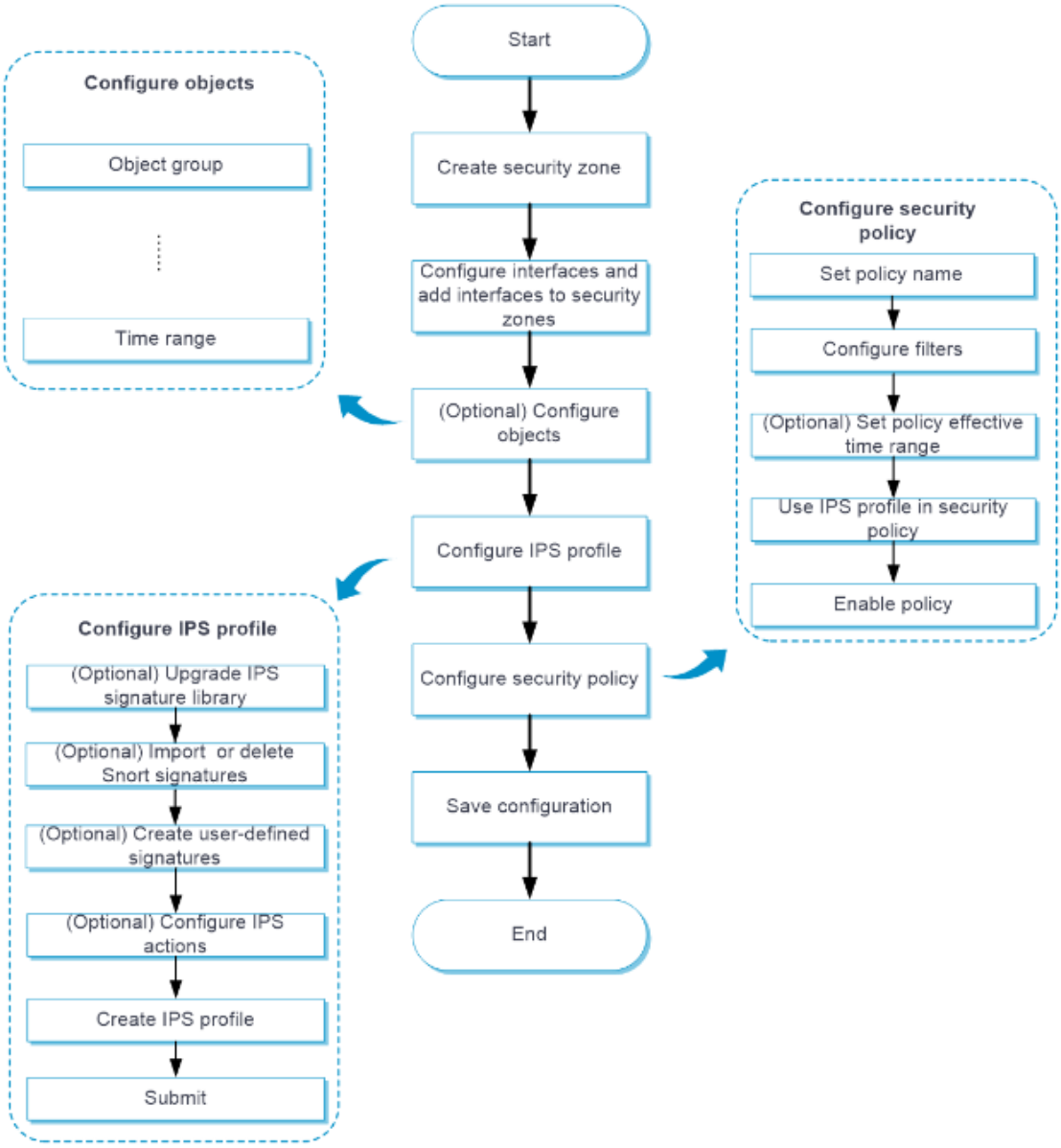
- ホワイトリストエントリーを設定する場合は、脅威 ID、URL、または IP アドレス、あるいはそれらの 2 つまたはすべてを入力する必要があります。

- スノットファイルから Snort シグニチャをインポートする場合、Snort ファイルは UTF-8 形式でエンコードする必要があります。

Configure IPS

図 2 に示すように、IPS を設定します。

図 2:IPS 設定手順



Configure an IPS profile

デバイスには、**default** という名前の定義済みの IPS プロファイルが用意されています。デフォルトの IPS プロファイルでは、デバイス上でイネーブルになっているすべての IPS シグニチャが使用され、変更や削除はできません。

デバイスに IPS プロファイルを作成することもできます。デフォルトでは、新しく作成された IPS プロファイルは、イネーブルになっているすべての IPS シグニチャを使用し、シグニチャと一致するパケットにデフォルトのシグニチャアクションを適用します。IPS プロファイルで使用される IPS シグニチャをフィルタリングし、シグニチャアクションを変更できます。

IPS プロファイルのグローバルアクションを設定したり、プロファイル内の個々の IPS シグニチャのアク

ションを変更したりできます。

IPS シグニチャに一致するパケットのアクションは、次の順序で選択されます。

1. IPS プロファイルのシグニチャ例外として IPS シグニチャに対して設定されたアクション。
2. IPS プロファイルに設定されたグローバルアクション。
3. IPS シグニチャのデフォルトアクション。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Profiles** を選択します。
   IPS Profiles ページが開きます。
3. **Create** をクリックします。
   Create IPS Profile ページが開きます。
4. IPS プロファイルの基本設定を行います。

表 1 IPS プロファイルの基本設定項目

項目	説明
Name	IPS プロファイル名を指定します。ベストプラクティスとして、IPS プロファイル名に特殊文字<>¥/*?":,;を入力しないでください。 これらの特殊文字を含む名前の IPS プロファイルをエクスポートする場合、IPS プロファイル名のこれらの特殊文字はアンダースコア(_)に置き換えられます。
Action	IPS プロファイルのグローバルアクションを選択します。 オプションは、**Predefined action**、**Blacklist**、**Drop**、**Permit**、**Reset**、および **Redirect** です。 グローバルアクションは、IPS プロファイル内のシグニチャに一致するすべてのパケットに適用されます。

5. IPS プロファイル内の IPS シグニチャをフィルタリングする基準を設定します。
   フィルタリング基準を設定しない場合、デフォルトステータスが **Enabled** のすべての IPS シグニチャが IPS プロファイルに追加されます。

表 2 IPS シグニチャフィルタリングの設定項目

項目	説明
Protected	保護ターゲット基準の保護ターゲットを選択します。

Attack	攻撃カテゴリ基準の攻撃カテゴリを選択します。
Direction	方向基準のトラフィック方向を選択します。オプションは次のとおりです。 • **To-server**: クライアントからサーバーへの方向。 • **To-client**: サーバーからクライアントへの方向。
Predefined action	IPS シグニチャアクション基準の定義済みアクションを選択します。 オプションは、**Drop**, **Permit**, **Reset**、および **Blacklist** です。
Severity level	重大度レベル基準の重大度レベルを選択します。 オプションは、**Critical**, **High**, **Medium**、**Low** です。
Predefined status	定義済み IPS シグニチャステータス基準の定義済みステータスを選択します。オプションは、**Enabled** と **Disabled** です。

6. **Search** をクリックします。**Viewing matching signatures** セクションで IPS シグニチャを表示します。
   - IPS プロファイルで使用されている IPS シグニチャを表示するには、**Active Signatures** タブをクリックします。
   - IPS プロファイルで使用されていない IPS シグニチャを表示するには、**Inactive Signatures** タブをクリックします。
7. アクティブまたは非アクティブの IPS シグニチャのステータスまたはアクションを変更するには、次の手順を実行します。
   a. **Active Signatures** タブまたは **Inactive Signatures** タブで IPS シグニチャを選択します。
   b. **Custom** をクリックします。
   c. 表示されるダイアログボックスで、必要に応じて設定を行い、**OK** をクリックします。
8. 非アクティブな IPS シグニチャを IPS プロファイルに追加するには、次の手順を実行します。
   a. **Inactive Signatures** タブで IPS シグニチャを選択し、**Custom** をクリックします。
   b. 表示されたダイアログボックスで、**Status** フィールドで **Enable** を選択し、**OK** をクリックします。
      IPS シグニチャが **Active Signatures** タブに表示されます。
9. IPS プロファイルから IPS シグニチャを削除するには、次の手順を実行します。
   a. **Active Signatures** タブで IPS シグニチャを選択し、**Custom** をクリックします。
   b. 表示されたダイアログボックスで、**Status** フィールドで **Disable** を選択し、**OK** をクリックします。
      IPS シグニチャが **Inactive Signatures** タブに表示されます。
10. **Advanced settings** をクリックします。
11. 表示されたダイアログボックスで、IPS プロファイルの詳細設定を行います。

表 3 IPS プロファイルの詳細設定項目

項目	説明
Count policy matches	IPS プロファイルの一致カウントをイネーブルにするかどうかをイネーブルにします。
Log settings	ロギング設定を構成する方法を選択します。オプションは次のとおりです: • **Global**: **System** タブの **Log Settings** > **Threat Log Settings** > **IPS Logs** ページでグローバル設定を表示または編集します。 • **User-defined**: このページのロギング設定を続行します。
Log output	このフィールドは、**Log settings** フィールドで **User-defined** を選択した場合にのみ使用できます。 オプションは、**Output system logs** と **Output through email** です。両方のオプションを同時に選択できます。
Sig. library baseline version	シグニチャライブラリのベースラインバージョンを選択して、IPS が現在アクティブなシグニチャライブラリのシグニチャに加えて、ベースラインバージョンのシグニチャを使用してパケットを照合できるようにします。 シグニチャライブラリのベースラインバージョンが選択されている場合、新しく追加されたシグニチャは非アクティブな状態であり、パケットの照合に使用できません。これらのシグニチャのステータスを変更するには、次のタスクを実行します。 1. 新たにシグニチャが追加された現在のバージョンがベースラインバージョンよりも高い場合は、現在のバージョン番号をベースラインバージョン番号として設定します。 2. 新しく追加されたシグニチャを含む現在のバージョンがベースラインバージョンよりも古い場合は、シグニチャを選択し、**Custom** をクリックしてシグニチャをイネーブルにします。
Email server	**Log output** フィールドで **Output through email** を選択した後は、電子メールサーバーを構成する必要があります。新規電子メールサーバーを構成するか、既存の電子メールサーバーを選択できます。既存の電子メールサーバーを表示または編集するには、**System** タブの **Log Settings** > **Email Server** ページに移動します。
Email output condition	電子メールでログ出力するために、一致する IPS シグニチャのフィルタリング基準を設定します。
Min. signature severity level	電子メールでログ出力するために、一致する IPS シグニチャの最も低い重大度を指定します。

	システムは、一致するシグニチャの重大度レベルが指定された重大度レベル以上である場合にのみ、電子メールでログを出力します。

12. **OK** をクリックします。
    IPS プロファイルが **IPS Profiles** ページに表示されます。
13. セキュリティーポリシーで IPS プロファイルを使用します。セキュリティーポリシーの詳細については、セキュリティーポリシーのオンラインヘルプを参照してください。
14. **Submit** をクリックしてすぐに設定をアクティブにするか、設定が自動的にアクティブになるまで 40 秒待ちます。
    IPS プロファイルを作成した後、有効にするには、設定をアクティブにする必要があります。デフォルトでは、設定は 40 秒後に自動的にアクティブになります。
15. IPS プロファイルで使用されている IPS シグニチャをエクスポートするには、**IPS Profiles** ページの IPS プロファイルエントリの **Export signatures** カラムにあるアイコン をクリックします。
    シグニチャライブラリ内のすべての IPS シグニチャは.csv ファイルにエクスポートされますが、この IPS プロファイルで使用される IPS シグニチャは、エクスポートファイルの **Active** カラムで **Y** とマークされます。

Import or delete Snort signature

Import Snort signatures

Snort シグニチャを追加するには、Snort 形式の IPS シグニチャファイルを作成し、ファイルからデバイスにシグニチャをインポートします。
IPS シグニチャファイルに、使用するユーザー定義シグニチャがすべて含まれていることを確認します。デバイス上の既存のすべての Snort シグニチャは、インポートされた Snort シグニチャによって上書きされます。
Snort ルールで定義されたシグニチャを IPS シグニチャファイルから正しくインポートするには、Snort ルールが有効であることを確認します。
Snort シグニチャをインポートするには:

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Signatures** を選択します。
   IPS Signatures ページには、デバイス上のすべての IPS シグニチャが表示されます。
3. ページの左上隅にある **Import Snort signatures** をクリックします。
   Import Snort Signatures ウィンドウが開きます。
4. インポートする IPS シグニチャファイルを選択します。
5. **Import Snort Signatures** をクリックします。

Delete all Snort signatures

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Signatures** を選択します。
   IPS Signatures ページが開きます。
3. **Delete signatures** をクリックし、ページの左上隅にある **Delete all Snort signatures** を選択します。
4. 表示された確認ダイアログボックスで **Yes** をクリックします。

Create and delete user-defined IPS signature

現在のシグニチャライブラリに存在しないユーザー定義シグニチャを作成できます。
ユーザー定義の IPS シグニチャには、基本的な設定と規則が含まれています。
ユーザー定義シグネチャには、複数のルールを含めることができます。ルール間の論理演算子は次のとおりです:

- **Logical AND**: パケットが IPS シグニチャと一致するのは、シグニチャ内のすべてのルールとパケットが一致する場合だけです。

- **Logical OR**: パケットがシグニチャ内のいずれかのルールと一致する場合、そのパケットは IPS シグニチャと一致します。

ユーザー定義シグニチャ規則では、送信元 IPv4 アドレス、宛先 IPv4 アドレス、送信元ポート、宛先ポート、および要求方式の一致基準、検出項目、および検出トリガー条件を設定できます。
ユーザー定義シグニチャは、次のいずれかのタイプになります。

- **Keyword**: キーワードタイプでは、1 つまたは複数の検出項目と 1 つの検出トリガー条件だけを設定する必要があります。デバイスは、パケットが検出トリガー条件に一致した後にだけ、パケットと検出項目の比較を継続します。パケットがルールに一致するのは、ルール内のすべての検出項目に一致した場合だけです。

- **Number**: 番号タイプでは、検出項目を 1 つだけ設定する必要があります。パケットがルールと一致するのは、パケットがルール内の検出項目と一致する場合だけです。

Create a user-defined IPS signature

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Signatures** を選択します。
   IPS Signatures ページには、デバイス上のすべての IPS シグニチャが表示されます。
3. **Create user-defined signature** をクリックします。

4. 表示されたページで、ユーザー定義の IPS シグニチャの基本設定を行います。

表 4 IPS シグニチャの基本的な設定項目

項目	説明
Name	IPS シグニチャ名を入力します。
Description	識別しやすいように説明を入力します。
Severity level	一致パケットがネットワークにもたらすリスクインパクトの重大度レベルを選択します。 オプションは、**Critical**, **High**, **Medium**、**Low** です。
Direction	方向基準のトラフィック方向を選択します。オプションは次のとおりです。 • **To-server**: クライアントからサーバーへの方向。 • **To-client**: サーバーからクライアントへの方向。 • **o-server, To-client**: クライアントからサーバーへの方向とサーバーからクライアントへの方向の両方。
Action	IPS シグニチャに一致するパケットのアクションを選択します。 オプションは、**Blacklist**, **Drop**, **Permit**、および **Reset** です。
Logging	一致するパケットのロギングを有効にするかどうかを選択します。オプションは **Enable** および **Disable** です。
Capture	一致するパケットのキャプチャを有効にするかどうかを選択します。オプションは **Enable** と **Disable** です。 キャプチャアクションを使用すると、デバイスはパケットをキャプチャし、スケジュールされたエクスポート時間に指定された URL にキャプチャされたパケットをエクスポートできます。キャプチャアクションの設定の詳細については、セキュリティーアクションのオンラインヘルプを参照してください。

5. **Rules** 領域で、シグニチャの規則を設定する前に論理演算子を選択します。
6. **Create** をクリックします。
7. 開いたページで、規則の基本設定を構成します。

表 5 ルールの基本構成項目

項目	説明

ID	ルール ID を入力します。
Match pattern type	シグネチャー致パターンタイプを選択します。オプションは **Keyword** と **Number** です。
Application layer protocol	フィルタリング基準としてアプリケーション層プロトコルを選択します。
Transport layer protocol	フィルタリング基準としてトランスポート層プロトコルを選択します。
Request method	GET や POST などの HTTP 要求メソッドを選択します。
Source IPv4 address	フィルタリング基準として送信元 IPv4 アドレスを入力します。
Source port range	送信元ポート範囲をフィルタリング基準として指定します。
Destination IPv4 address	フィルタリング基準として宛先 IPv4 アドレスを入力します。
Destination port range	フィルタリング基準として宛先ポートの範囲を指定します。

8. **Detection trigger conditions** 領域で、**Create** をクリックします。
この領域は、一致パターンタイプとして **Keyword** が選択されている場合にのみ使用できます。
9. 検出トリガー条件を作成します。

表 6 検出トリガー条件の設定項目

項目	説明
Protocol field	検査するプロトコルフィールドを選択します。
Match pattern type	マッチパターンの種類を選択します。オプションは **Text** と **Hex** です。
Match pattern	一致パターンの内容を入力します。
Depth	検査するバイト数を指定します
Offset	検査開始後のオフセットをバイト単位で入力します。オフセットは、プロトコルフィールドの先頭からカウントされます。

10. **OK** をクリックします。
Detection trigger conditions リストに検出トリガー条件が表示されます。

11. **Detection items** 領域で、**Create** をクリックします。
12. 検出項目を作成します。

表 7 検出項目構成項目

項目	説明
ID	検出項目 ID を入力します。
Protocol field	プロトコルフィールドを選択します。
Operator	検出項目で一致操作を定義する演算子を選択します。 オプションは、**Create Rule** ページで選択した一致パターンタイプによって異なります。 • **Keyword** が選択されている場合、オプションは **Contain** と **Not contain** です。 • **Number** を選択した場合、オプションは **Greater than**, **Equal to**, **Not equal to**, **Less than**, **Greater than or equal to**、**Less than or equal to** です。
Match pattern type	一致パターンのタイプを選択します。オプションは、**Text**、**Regular expression** および **Hex** です。
Match pattern	一致パターンの内容を入力します。
Depth	検査するバイト数を指定します。
Offset	検査開始後のオフセットをバイト単位で入力します。オフセットは、プロトコルフィールドの先頭からカウントされます。
Relative depth	検査するバイト数を指定します。
Relative offset	検査を開始するオフセットを入力します。オフセットは、前の検出項目の末尾からカウントされます。

13. **OK** をクリックします。
    Detection items リストに検出項目が表示されます。
14. **OK** をクリックします。
    ルールが **Rules** リストに表示されます。
15. **OK** をクリックします。
    シグニチャは **IPS Signatures** ページに表示されます。
16. 設定を有効にするには、**Submit** をクリックします。

ユーザー定義の IPS シグニチャの削除

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Signatures** を選択します。
   IPS Signatures ページが開きます。
3. 削除するユーザー定義シグニチャを選択します。
4. **Delete signatures** をクリックし、**Delete user-defined signatures** を選択します。
5. 表示された確認ダイアログボックスで **Yes** をクリックします。

Export all signatures in the signature library

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Signatures** を選択します。
   IPS Signatures ページが開きます。
3. **Export all signatures** をクリックします。
   シグニチャライブラリ内のすべての IPS シグニチャは、.csv ファイルにエクスポートされます。

Configure IPS whitelist

脅威ログに誤アラームが存在する場合は、ホワイトリスト機能を有効にし、検出された脅威 ID(IPS シグニチャ ID)、URL、および IP アドレスをホワイトリストに追加できます。デバイスは、ホワイトリスト上の IPS シグニチャまたは URL に一致するパケットの通過を許可し、誤アラームを減少させます。
ホワイトリストを有効にすると、デバイスは各ホワイトリストエントリーのヒットカウントを記録します。**Whitelist** ページで統計情報を確認できます。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **IPS** > **Whitelist** を選択します。
   Whitelist ページには、デバイス上のすべてのホワイトリストエントリーが表示されます。
3. ホワイトリストエントリーを作成します。

表 8 ホワイトリストエントリーの構成項目

項目	説明
Entry ID	ホワイトリストエントリーID を入力します。
Description	ホワイトリストエントリーの説明を入力します。

Threat ID	脅威 ID を入力します。脅威 ID は脅威ログから取得できます。
URL	URL を入力します。URL は脅威ログから取得できます。URL にはパケットヘッダーフィールドとパケットの最初の行が含まれています(例:111.15.93.166/wnm/get.j)。 URL を作成、編集、または削除した後、**Activate** をクリックして設定を有効にする必要があります。
Match type	照合タイプを選択します。オプションは次のとおりです。 • **Exact match**: パケット内で検出された URL が、設定された URL とまったく同じである場合、一致と見なされます。 • **Substring match**: パケット内で検出された URL に設定された URL が含まれている場合、一致と見なされます。
IP type	脅威ログから取得できる IP アドレスのタイプを選択します。オプションは **IPv4** と **IPv6** です。
IP address	IP アドレスを入力します。IP アドレスは脅威ログから取得できます。

4. **OK** をクリックします。
5. **Enable whitelist** をクリックします。

Anti-virus

このヘルプには、次のトピックが含まれています。

- Introduction
  - Application scenario
  - Basic concepts
  - Virus detection methods
  - Cloud query
  - Anti-virus mechanism
- Restrictions and guidelines
- Configure anti-virus
  - Configure an anti-virus profile
  - Configure the cloud query server

Introduction

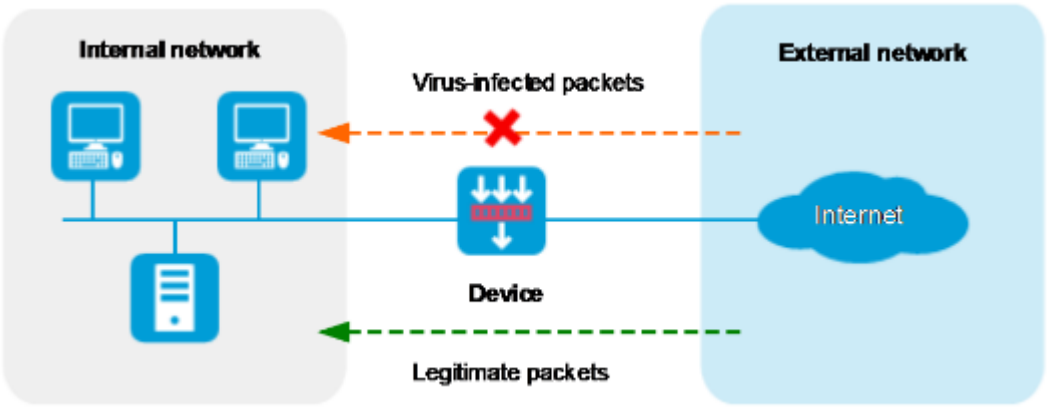
アンチウィルスは、最新のウィルスシグニチャライブラリに基づいてパケットのアプリケーション層でウィルスを識別し、ネットワークの感染を防止するアクションを実行します。この機能は通常、内部ネットワークをウィルスから隔離し、内部データを保護するためにゲートウェイに配置されます。

Application scenario

図 1 に示すように、デバイスは内部ネットワークのゲートウェイであり、内部ユーザーは外部ネットワークにアクセスし、外部ネットワークからデータをダウンロードします。内部サーバーは外部ユーザーがアップロードしたデータを受け入れます。

このシナリオでは、ゲートウェイでアンチウィルスを設定して内部ネットワークを保護できます。アンチウィルスは着信パケットを検査し、正規のパケットの通過を許可し、ウィルスを含むパケットに対してアラート、ブロック、リダイレクトなどのアクションを実行します。

図 1 アンチウィルスアプリケーションのシナリオ



Basic concepts

Virus signature

ウィルスシグニチャは、特定のウィルスを一意に識別する文字列です。ウィルスシグニチャライブラリには、事前定義されたウィルスシグニチャが含まれています。

MD5 rules

MD5 ルールは、ウィルスシグニチャライブラリ内のウィルスシグニチャに基づいてシステムによって生成され、ウィルスに感染したファイルを識別します。

Virus exception

通常、アンチウィルスは、ウィルスシグニチャに一致するパケットに対してアンチウィルスアクションを実行します。ウィルスが誤ったアラームであることが判明した場合は、ウィルスシグニチャをウィルス例外として設定できます。ウィルス例外に一致するパケットは通過が許可されます。

Application exception

通常、アンチウィルスアクションはプロトコル固有であり、プロトコルによって実行されるすべてのアプリケーションに適用されます。アプリケーションに別のアクションを実行するには、アプリケーションを例外として設定し、アプリケーションに別のアンチウィルスアクションを指定します。アプリケーション例外はアプリケーション固有のアクションを使用し、他のアプリケーションはプロトコル固有のアクションを使用します。たとえば、HTTP のアンチウィルスアクションは permit です。HTTP によって実行されるゲームをブロックするには、ゲームをアプリケーション例外として設定し、ブロックアクションを指定します。

MD5 value exception

パケットにウィルスが含まれていることが検出されたが、実際にはパケットが安全である場合、ウィルス

の MD5 値を MD5 値例外として設定できます。デバイスは、MD5 値例外に一致する後続のパケットの通過を許可します。
ウィルスの MD5 値は、脅威ログから取得できます。

Anti-virus action

ウィルス対策アクションは、ウィルスシグニチャと一致するパケットに適用されます。アクションには次のタイプがあります。

- **Alarm**: 一致するパケットを許可し、ログを生成します。
- **Block**: 一致するパケットをブロックし、ログを生成します。
- **Redirect**: 一致する HTTP 接続を URL にリダイレクトし、ログを生成します。
- **Permit**: 一致するパケットを許可します。

Virus detection methods

デバイスは、次のウィルス検出方法をサポートしています。

- **Virus signature-based detection**: デバイスは、パケットをウィルスシグニチャライブラリ内のウィルスシグニチャと照合し、一致が検出された場合にパケットにウィルスが含まれていると判断します。
- **MD5 rule-based detection** デバイスは検査対象ファイルの MD5 ハッシュ値を生成し、その値をシステム定義の MD5 ルールと比較します。一致が検出された場合、そのファイルはウィルス感染であると識別されます。

Cloud query

アンチウィルスプロファイルでクラウドクエリーを有効にできます。パケット内のファイルがローカルのウィルスシグニチャまたは MD5 ルールと一致しない場合、デバイスはファイルの MD5 値をクラウドサーバーに送信してクラウドクエリーを実行します。デバイスは、クラウドサーバーから返されたクエリー結果に基づいて適用するアクションを決定します。

- ファイルの MD5 値が MD5 ルールと一致する場合、ファイルはウィルスに感染していると見なされ、ウィルス対策アクションが適用されます。
- MD5 値に一致するルールが見つからない場合、またはファイルがウィルスフリーであることが確認された場合、パケットは通過を許可されます。

Anti-virus mechanism

図 2 に示すように、アンチウィルスデバイスはパケットを受信すると、次の動作を行います。

1. デバイスは、パケットをセキュリティーポリシーと比較します。

パケットがアンチウィルスポリシーに関連付けられたセキュリティーポリシーと一致する場合、デバイスはパケットのアプリケーション層プロトコルの識別を継続します。

2. デバイスは、アンチウィルスがパケットのアプリケーション層プロトコルをサポートしているかどうかを識別します。
   - ○ そうでない場合、デバイスはアンチウィルス検査なしでパケットの通過を許可します。
   - ○ Yes の場合、デバイスはパケットをウィルスシグニチャおよび MD5 ルールと比較します。

3. 一致するシグニチャまたは MD5 ルールが見つかった場合、デバイスは次の動作を実行します。

   a. 一致するシグニチャが例外かどうかを判断します。Yes の場合、デバイスはパケットの通過を許可します。No の場合、デバイスはアプリケーションが例外かどうかを調べます。

   b. アプリケーションが例外の場合、デバイスはアプリケーション固有のアクション(alert、block、または permit)を実行します。アプリケーションが例外でない場合、デバイスはプロトコル固有のアクション(alert、block、または redirect)を実行します。

4. 一致するシグニチャまたは MD5 ルールが見つからない場合、デバイスは次の処理を実行します。

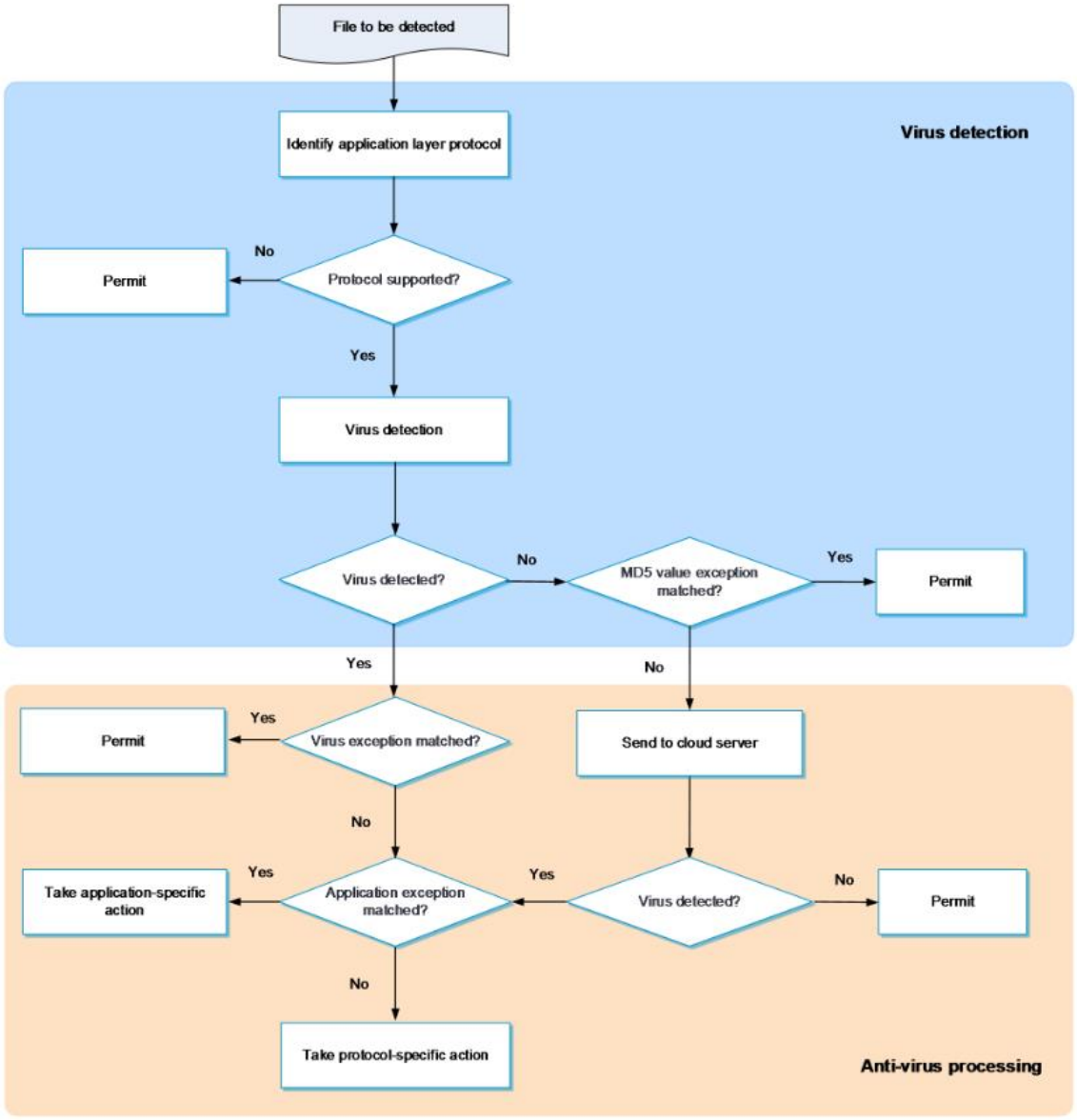
   a. パケット内のファイルの MD5 値が MD5 値例外かどうかを判別します。
      - Yes の場合、デバイスはパケットの通過を許可します。
      - そうでない場合、デバイスはパケット内のファイルの MD5 値をクラウドサーバーに送信します。

   b. クラウドクエリーがアンチウィルスポリシーで無効になっている場合、デバイスはパケットの通過を許可します。

   c. クラウドクエリーがアンチウィルスポリシーで有効になっていても、クラウドサーバーがウィルスを検出しない場合、デバイスはパケットの通過を許可します。

   d. クラウドクエリーがアンチウィルスポリシーで有効になっていて、クラウドサーバーがウィルスを検出した場合、デバイスはアプリケーションが例外かどうかを判断します。
      - Yes の場合、デバイスはアプリケーション固有のアクション(alert、block、または permit)を実行します。
      - そうでない場合、デバイスはプロトコル固有のアクション(alert、block、または redirect)を実行します。

図 2:アンチウィルスメカニズム



Restrictions and guidelines

- アンチウィルスイルスプロファイルを作成、編集または削除した後、有効にするには構成をアクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化するか、デフォルトで構成が 40 秒後に自動的にアクティブ化されます。構成をアクティブ化すると、一時的な DPI サービスの中断が発生します。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。
- アンチウィルス機能をデバイスで実行するには、ライセンスが必要です。ライセンスの有効期限が切れた場合、アンチウィルス機能は引き続き使用できますが、デバイス上のウィルスシグニチャ

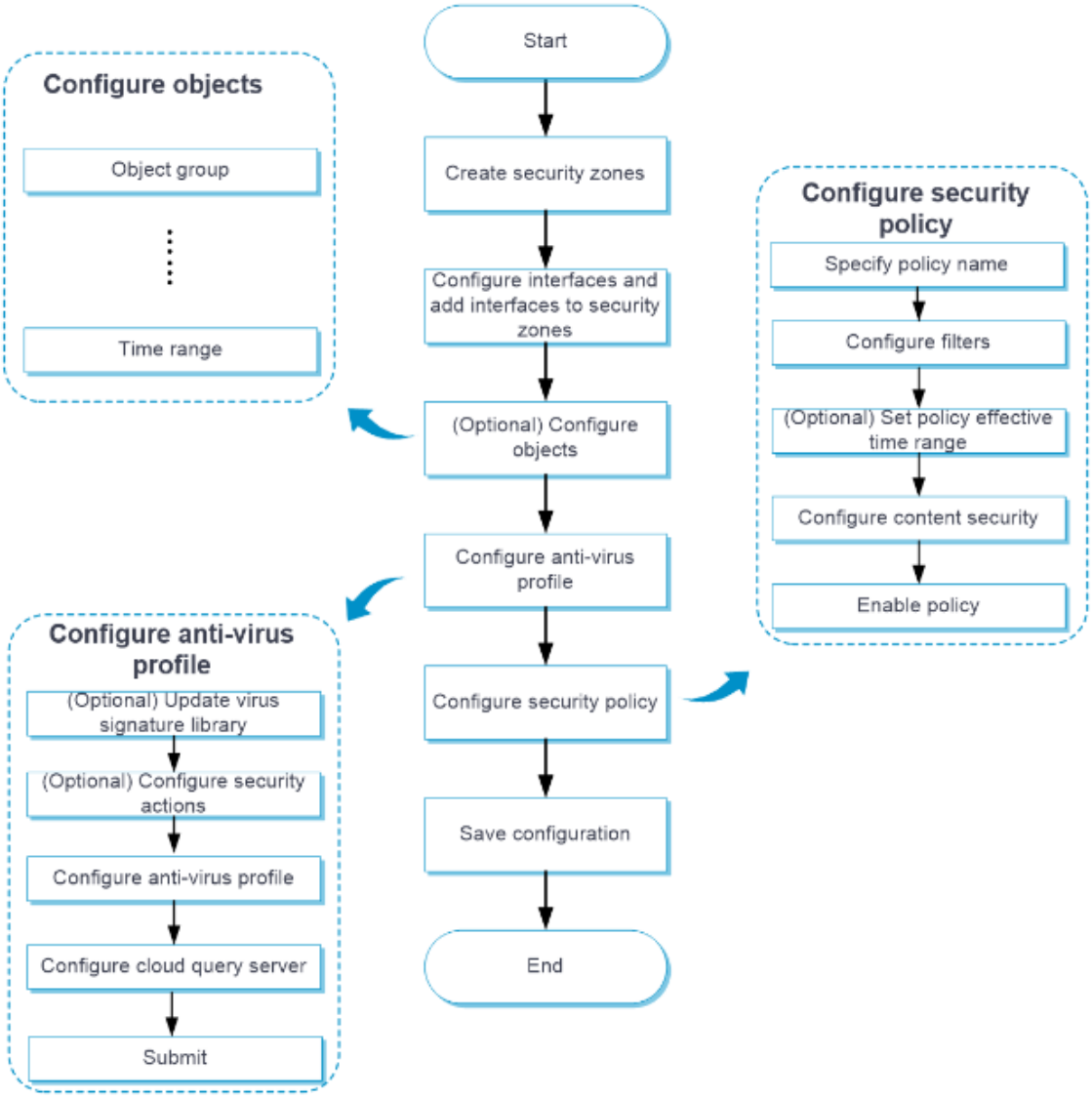
ライブラリを更新したり、クラウドクエリーやサンドボックスコラボレーションを使用することはできません。ライセンスの詳細については、ライセンス管理のオンラインヘルプを参照してください。

- クラウドクエリー機能は、HTTP、IMAP、NFS(読み取り操作のみ)、POP3、および SMTP トラフィックでのみ使用できます。
- アンチウィルスプロファイルでアラームテンプレートを選択すると、IPS シグニチャと一致する HTTP プロトコルパケットに対して IPS の **capture** アクションが有効になりません。

Configure anti-virus

アンチウィルスを設定します(図 3)。

図 3:アンチウィルスの設定手順



Configure an anti-virus profile

デフォルトでは、デバイスに **default** という名前の定義済みアンチウィルスプロファイルが用意されています。このプロファイルは変更または削除できません。
必要に応じて、アンチウィルスプロファイルをカスタマイズできます。
アンチウィルスがサポートするすべてのプロトコルでは、接続要求は常にクライアントによって開始されます。アンチウィルスが正しく動作するためには、アンチウィルスプロファイルを使用するセキュリティーポリシーが次の要件を満たしていることを確認してください。

- クライアントが存在するセキュリティーゾーンは、ソースセキュリティーゾーンとして設定されます。
- サーバーが存在するセキュリティーゾーンは、宛先セキュリティーゾーンとして設定されます。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security > Anti-Virus > Profiles** を選択します。
3. **Create** をクリックします。
4. アンチウィルスプロファイルを作成します。

表 1 アンチウィルスプロファイルの設定項目

項目	説明
Name	アンチウィルスプロファイルの名前を入力します。
Description	アンチウィルスプロファイルの説明を入力します。
Enable cloud query	クラウドクエリーを有効にするには、この項目を選択します。
Alarm message template	アラームテンプレートを選択します。このテンプレートを使用すると、ウィルスが検出されたときにデバイスからクライアントにアラームメッセージを送信できます。 この項目は、アップロードおよびダウンロード HTTP トラフィックに **Block** アクションを定義した場合にだけサポートされます。 アラームメッセージテンプレートを作成または適用した後、**Edit** をクリックしてアラームメッセージをインポートできます。 TXT または HTML ファイルのみがサポートされています。 アラームテンプレートを選択すると、**capture** IPS アクションは、IPS シグニチャと一致する HTTP プロトコルパケットアクションが有効になりません。

	この項目のサポートは、デバイスモデルによって異なります。
Upload	プロトコルのアップロードトラフィックにプロファイルを適用するには、この項目を選択します。 この項目は、POP3 プロトコルでは使用できません。
Download	プロトコルのダウンロードトラフィックにプロファイルを適用するには、この項目を選択します。 この項目は SMTP プロトコルでは使用できません。
Action	プロトコルの **Action** リストから、パケットを一致させるアクションを選択します。 サポートされているアクションは、**Alarm**, **Block**、**Redirect** です。 IMAP プロトコルは、**Alarm** アクションのみをサポートします。
Application exceptions	アプリケーションをアプリケーション例外として設定するには、アプリケーションを選択し、**Add** をクリックしてアプリケーション例外リストに追加します。アプリケーション例外リストで、**Action** リストからアプリケーション例外の処理を選択します。
Virus exceptions	ウィルスをウィルス例外として設定するには、ウィルス ID を入力し、**Add** をクリックしてウィルス例外リストに追加します。
MD5 value exceptions	ウィルスの MD5 値を MD5 値例外として設定するには、MD5 値を入力し、**Add** をクリックして MD5 値例外リストに追加します。

5. **OK** をクリックします。
6. セキュリティーポリシーでアンチウィルスプロファイルを使用します。セキュリティーポリシーの詳細は、セキュリティーポリシーのオンラインヘルプを参照してください。
7. **Submit** をクリックしてすぐに設定をアクティブにするか、設定が自動的にアクティブになるまで 40 秒待ちます。

   アンチウィルスプロファイルを作成した後、有効にするには構成をアクティブ化する必要があります。デフォルトでは、構成は 40 秒後に自動的にアクティブ化されます。

Configure the cloud query server

クラウドクエリーサーバーをアンチウィルス用に設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APP Security** > **Anti-Virus** > **Profiles** を選択します。
3. **Cloud server connectivity** フィールドの横にある **Configure** をクリックします。

4. クラウドクエリーサーバーを設定します。

表 2 クラウドクエリーサーバーの設定項目

項目	説明
Server address	クラウドクエリーサーバーの IP アドレスまたはホスト名を入力します。 当社のクラウドクエリーサーバーのみがサポートされています。
Max cached MD5 entries	ヒットエントリリストおよび非ヒットエントリリストにキャッシュできる MD5 エントリの最大数を指定します。 ノンヒットエントリリストは、クラウドサーバーに送信された MD5 値のうち、ウィルスと判定できないもののリストである。 ヒットエントリリストは、ウィルスと判定された MD5 値のリストである。
Min cache time	MD5 エントリの最小キャッシュ時間を分単位で指定します。 MD5 エントリの最小キャッシュ時間を設定すると、指定された時間内にエントリガー削除されなくなります。 ただし、設定されている最大キャッシュ MD5 エントリの値が現在キャッシュされているエントリの値より小さい場合は、キャッシュ期間が最小キャッシュ時間以下であっても、最も古いキャッシュエントリガー削除されます。

Data filtering

このヘルプには、次のトピックが含まれています。

- Introduction
  - Basic concepts
  - Data filtering mechanism
- Restrictions and guidelines
  - Restrictions and guidelines: Profile activation
  - Restrictions and guidelines: Regular expression-based keyword match pattern configuration
- Configure data filtering
  - Configure a keyword group
  - Configure a data filtering profile

Introduction

データフィルタリングは、アプリケーション層情報に基づいてパケットをフィルタリングします。データフィルタリングを使用すると、内部情報の漏洩、不正情報の流通、インターネットへの不正アクセスを効果的に防止できます。

データフィルタリングは、次のプロトコルのパケットのフィルタリングをサポートします。

- HTTP。
- FTP。
- SMTP。
- IMAP。
- NFS。
- POP3。
- RTMP。
- SMB。

Basic concenpts

Keyword

デバイスは定義済みキーワードのリストを提供し、ユーザー定義キーワードをキーワードグループに作成することができます。

- **Predefined keyword**: **Phone**, **Bank card**, **Credit card** および **ID card** が含まれます。これらのキーワードを使用して、電話番号、銀行カード番号、クレジット・カード番号および ID カード番号を含むパケットを識別できます。

- **User-defined keyword**: パケットのアプリケーション層データ内のパターンを識別するためのテキストベースまたは正規表現ベースのストリング。

Keyword group

キーワードグループは、最大 32 個のキーワードのグループです。パケットは、グループ内のキーワードと一致する場合、キーワードグループと一致します。事前定義されたキーワードを有効または無効にしたり、キーワードグループに新しいキーワードを作成したりできます。

Data filtering rule

データフィルタルールには、一連のパケットフィルタ基準およびパケットを照合するためのアクションが含まれています。パケットフィルタ基準には、キーワードグループ、方向(**Upload**, **Download** または **Both**)およびアプリケーションが含まれます。パケット処理アクションには、**Drop**, **Permit** および **Logging** が含まれます。パケットは、ルールを適用するために指定されたアクションのすべてのフィルタ基準に一致する必要があります。

Data filtering mechanism

データフィルタリングがサポートするプロトコルのパケットを受信すると、デバイスは次の動作を実行します。

1. パケットをセキュリティーポリシーと比較します。
   パケットがデータフィルタリングプロファイルに関連付けられたセキュリティーポリシーと一致する場合、デバイスはパケットからアプリケーション層情報を抽出します。
2. 抽出されたアプリケーション層情報をデータフィルタリングポリシー内のデータフィルタリング規則と比較して、パケットに対して実行するアクションを決定します。
   - パケットがポリシー内のデータフィルタリング規則に一致しない場合、デバイスはパケットの通過を許可します。
   - パケットが 1 つのルールにしか一致しない場合、デバイスはそのルールに指定されたアクションを実行します。
   - パケットが複数のルールに一致する場合、デバイスは次のようにアクションを決定します。
     - 一致規則に permit アクションと drop アクションの両方がある場合、デバイスは drop アクションを実行します。

- 一致ルールのいずれかにロギングアクションが指定されている場合、デバイスはパケットをロギングします。

Restrictions and guidelines

Restrictions and guidelines: Profile activaiton

データフィルタプロファイルを作成、編集または削除した後、有効にするには構成をアクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化するか、デフォルトで構成が 40 秒後に自動的にアクティブ化されます。構成をアクティブ化すると、一時的な DPI サービスの中断が発生します。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。

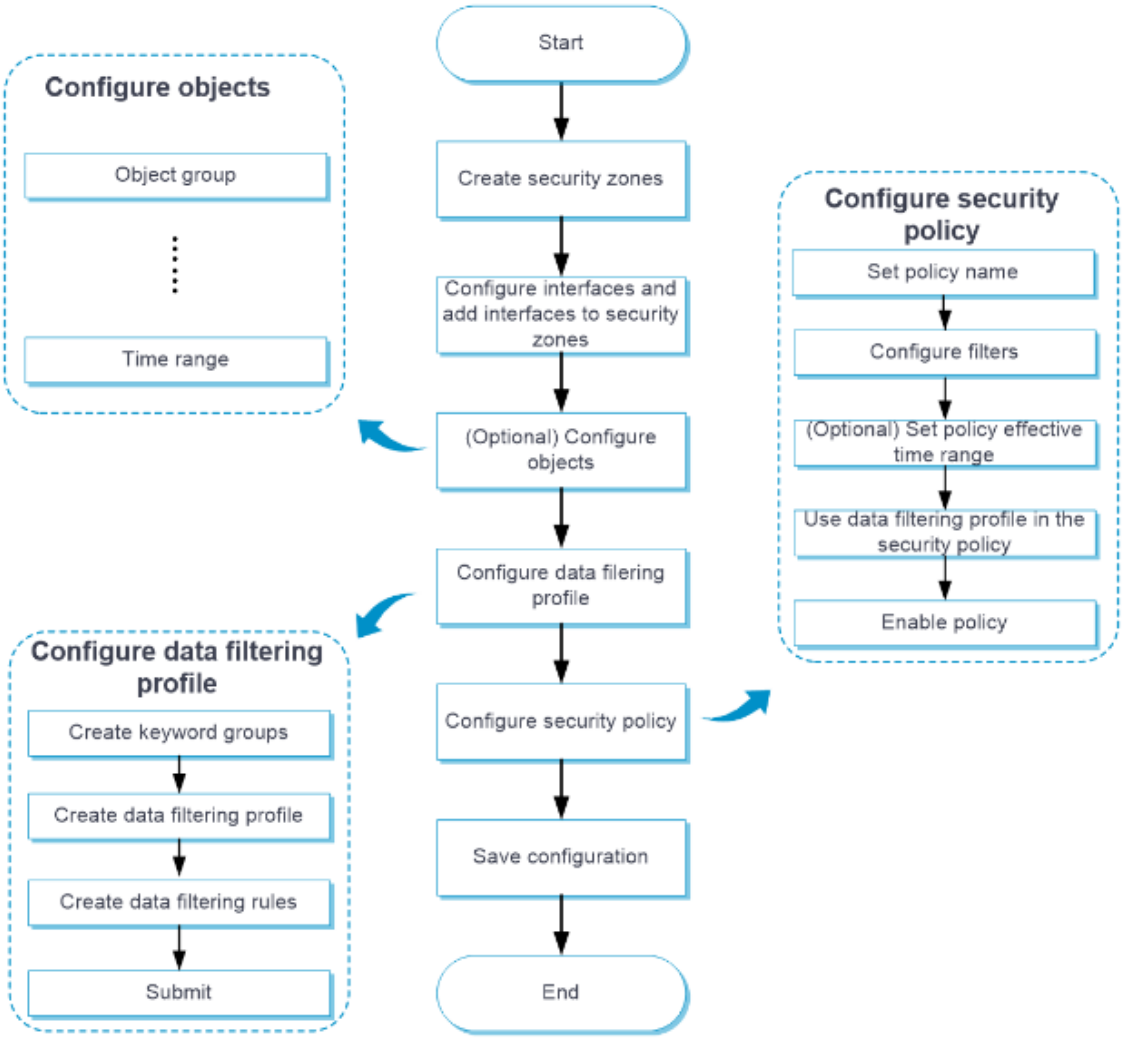
Restrictions and guidelines: Regular expression-based keyword match pattern configuration

- 正規表現パターンには、最大 4 つの分岐を含めることができます。たとえば、**'abc(c d e¥x3D)'**は有効で、**'abc(c onreset onselect onchange style¥x3D)'**は無効です。
- 中かっこは使用できません。たとえば、**'ab((abcs*?))'**は無効です。
- 分岐を別の分岐の後に指定することはできません。たとえば、**'ab(a b)(c d)^¥¥r¥¥n]+?'**は無効です。
- アスタリスク(*)または疑問符(?)の前には、4 文字以上のワイルドカード以外の文字が必要です。たとえば、**'abc*'**は無効で、**'abcd*DoS¥x2d¥d{5}¥x20¥x2bxi¥¥r¥¥nJOIN'**は有効です。

Configure data filtering

図 1 に示すように、データフィルタリングを設定します。

図 1 データフィルタリングの設定手順



Configure a keyword group

キーワードグループを作成し、キーワードグループ内のキーワードを設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **Data Filtering** > **Keyword Groups** を選択します。
3. 表示されたページで、**Create** をクリックします。
4. キーワードグループを作成します。

表 1 キーワードグループの設定項目

項目	説明
Name	キーワードグループの名前を入力します。
Description	キーワードグループの説明を入力します。

5. 定義済み **keyword list** 領域で、定義済みキーワードに対して **Enable** を選択します。たとえば、電話番号を含むパケットを識別するには、Phone で Enable を選択します。
6. ユーザー定義の **keyword list** 領域で、**Create** をクリックします。
7. キーワードを作成します。

表 2 キーワードの設定項目

項目	説明
Name	キーワードの名前を入力します。
Type	キーワード一致パターンのタイプを選択します。オプションは次のとおりです。 • **Text**: 完全一致のテキストベースの一致パターンを設定するには、このオプションを選択します。 • **Regular expression**: このオプションを選択して、正規表現ベースのマッチングパターンをファジーマッチ用に設定します。
Match pattern	キーワード一致パターンの内容を入力します。

8. **OK** をクリックします。
   キーワードは、ユーザー定義のキーワードリストに表示されます。
   最大 32 個のキーワードをキーワードグループに追加できます。
9. **OK** をクリックします。
   キーワードグループは、**Keyword Groups** ページに表示されます。

Configure a data filtering profile

データフィルタリングプロファイルを作成し、プロファイルでデータフィルタリング規則を設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **Data Filtering** > **Profiles** を選択します。
3. 表示されたページで、**Create** をクリックします。
4. データフィルタリングプロファイルを作成します。

表 3 データフィルタリングプロファイルの構成項目

項目	説明
Name	データフィルタリングプロファイルの名前を入力します。
Description	データフィルタリングプロファイルの説明を入力します。

5. **Data filtering rules** 領域で、**Create** をクリックします。
6. データフィルタリング規則を作成します。

表 4 データフィルタリング規則の設定項目

項目	説明
Name	データフィルタリング規則の名前を入力します。
Keyword group	既存のキーワードグループを選択するか、キーワードグループを作成します。
Applications	ルールが適用されるアプリケーションのアプリケーション層プロトコルを選択します。サポートされているアプリケーション層プロトコルは、FTP、HTTP、IMAP、NFS、POP3、RTMP、SMB および SMTP です。
Direction	ルールが適用されるトラフィック方向を選択します。オプションは **Upload**, **Download**、および **Both** です。
Action	パケットを照合するアクションを選択します。オプションは **Permit** と **Drop** です。
Logging	一致するパケットのロギングを有効にするかどうかを選択します。オプションは **Enable** および **Disable** です。

7. **OK** をクリックします。
   データフィルタリング規則は、データフィルタリングプロファイルのデータフィルタリング規則リストに表示されます。
8. **OK** をクリックします。
   Data Filtering Profiles ページにデータフィルタリングプロファイルが表示されます。

9. セキュリティーポリシーでデータフィルタプロファイルを使用します。セキュリティーポリシーの詳細は、セキュリティーポリシーのオンラインヘルプを参照してください。

10. **Submit** をクリックしてすぐに設定をアクティブにするか、設定が自動的にアクティブになるまで 40 秒待ちます。

データフィルタプロファイルを作成した後、有効にするには構成をアクティブ化する必要があります。デフォルトでは、構成は 40 秒後に自動的にアクティブ化されます。

URL filtering

このヘルプには、次のトピックが含まれています。

- Introduction
  - URL
  - URL filtering rule
  - URL category
  - URL filtering profile
  - URL filtering whitelist/blacklist rule
  - URL filtering cloud query
  - URL filtering action
  - HTTPS URL filtering
  - URL filtering mechanism
- Restrictions and guidelines
  - Restrictions and guidelines: Text-based URL filtering rule configuration
  - Restrictions and guidelines: Regular expression-based URL filtering rule configuration
  - Restrictions and guidelines: Whitelist
  - Restrictions and guidelines: URL filtering profile activation
  - Restrictions and guidelines: Licensing requirements
  - Restrictions and guidelines: HTTPS URL filtering
- Configure URL filtering
  - Configure a URL category
  - Configure the cloud query server
  - Configure a URL filtering profile

Introduction

URL フィルタリングは、ユーザーがアクセスする URL をフィルタリングすることによって、Web リソースへのアクセスを制御します。

URL

URL はリソースへの参照で、ネットワーク上のリソースの場所と、そのリソースを取得するためのメカニズムを指定します。URL の構文は **protocol://hostname[:port]/path/[;parameters][?query]#fragment** です。図 1 に URL の例を示します。

図 1 URL の構文

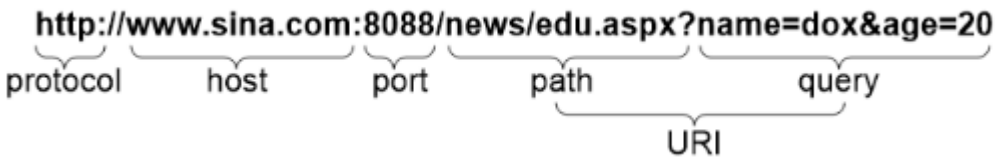


表 1 は、URL のフィールドについて説明しています。

表 1 URL フィールドの説明

フィールド	説明
protocol	伝送プロトコル(HTTP など)。
host	示されたリソースが存在するサーバーのドメイン名または IP アドレス。
[:port]	伝送プロトコルのポート番号を識別するオプションフィールド。このフィールドを省略すると、プロトコルのデフォルトのポート番号が使用されます。
/path/	示されたリソースが保管されているディレクトリーまたはファイルを識別するストリング。パスは、0 または複数のスラッシュで区切られた一連のセグメントです。
[parameters]	特殊パラメーターを含むオプションフィールド。
[?query]	動的 Web ページを照会するためにソフトウェアに渡されるパラメーターを含むオプションのフィールドです。各パラメーターは <key>=<value>のペアです。異なるパラメーターはアンパサンド(&)で区切られます。
URI	ネットワーク上のリソースを識別する統一リソース識別子。

URL filtering rule

URL フィルタリング規則は、URI またはホスト名フィールドの内容に基づいて URL を照合します。URL フィルタリングでは、次のタイプの URL フィルタリング規則が提供されます。

- **Predefined URL filtering rules**: 署名ベースの URL フィルタリング規則。デバイスは、ローカルの URL フィルタリング署名に基づいて自動的に URL フィルタリング規則を生成します。ほとんどの場合、URL フィルタリングには事前定義された規則で十分です。

- **User-defined URL filtering rules**: 手動で設定された正規表現またはテキストベースの URL フィルタリング規則。

URL フィルタリング規則では、次の URL マッチング方法がサポートされます。

- **Text-based matching**]: URL の hostname フィールドと URI フィールドをテキストパターンと照合します。

  URL のホスト名フィールドに対してテキストベースのマッチングを実行する場合、デバイスはまず、テキストパターンの先頭または末尾にアスタリスク(*)ワイルドカード文字が含まれているかどうかを判別します。

  ○ テキストパターンの先頭または末尾にアスタリスク(*)ワイルドカード文字が含まれていない場合、URL のホスト名がテキストパターンと一致すれば、ホスト名の照合は成功します。

  ○ テキストパターンの先頭にアスタリスク(*)ワイルドカード文字が含まれている場合、URL のホスト名がワイルドカード文字を含まないテキストパターンと一致するか、そのテキストパターンで終了すると、ホスト名の照合が成功します。

  ○ テキストパターンの末尾にアスタリスク(*)ワイルドカード文字が含まれている場合、URL のホスト名が、ワイルドカード文字を含まないテキストパターンと一致するか、そのテキストパターンで始まると、ホスト名の照合が成功します。

  ○ テキストパターンの先頭と末尾の両方にアスタリスク(*)ワイルドカード文字が含まれている場合、URL のホスト名がワイルドカード文字なしのテキストパターンと一致するか、含まれていれば、ホスト名の一致は成功します。

  URI フィールドに対するテキストベースのマッチングは、hostname フィールドに対するテキストベースのマッチングと同じように機能します。

- **Regular expression-based matching**: URL のホスト名および URI フィールドを正規表現と照合します。たとえば、ホスト名照合用の正規表現を **sina.*cn** に設定すると、**news.sina.com.cn** ホスト名を含む URL が照合されます。

URL category

URL フィルタリングには、フィルタリング規則の管理を容易にするための URL カテゴリ化機能があります。

複数の URL フィルタルールを 1 つの URL カテゴリに分類し、そのカテゴリの処理を指定できます。一致するルールが複数の URL カテゴリにある場合は、重大度が最も高いカテゴリの処理が実行されます。

URL フィルタリングでは、次のタイプの URL カテゴリがサポートされています。

- **Predefined URL categories**。

事前定義済の URL カテゴリには、事前定義済の URL フィル・ルールが含まれています。事前定義済の各 URL カテゴリには、1 から 999 までの一意の重大度レベルがあり、Pre-.Predefined URL カテゴリで始まるカテゴリ名は変更できません。

- **User-defined URL categories**。
  URL カテゴリを手動で作成し、フィルタルールを構成できます。ユーザー定義 URL カテゴリの重大度レベルは 1000 から 65535 の範囲です。フィルタルールを編集し、ユーザー定義 URL カテゴリの重大度レベルを変更できます。

URL filtering profile

URL フィルタリングプロファイルには複数の URL カテゴリを含めることができます。各カテゴリには、カテゴリ内のフィルタリング規則に一致するパケットに対して定義されたアクションがあります。プロファイル内のどのフィルタリング規則にも一致しないパケットに対してデフォルトアクションを指定することもできます。

URL filtering whitelist/blacklist rule

デバイスは、URL ベースのホワイトリストおよびブラックリストルールを使用した HTTP パケットのフィルタリングがサポートされています。HTTP パケット内の URL がブラックリストルールと一致する場合、パケットはドロップされます。URL がホワイトリストルールと一致する場合、パケットの通過が許可されます。

URL filtering cloud query

URL フィルタリングプロファイルでクラウドクエリーをイネーブルにして、HTTP トラフィックの URL フィルタリング精度を向上させることができます。
クラウドクエリーを有効にすると、デバイスはローカル URL フィルタリング規則に一致しない URL をクラウドサーバーに送信してクエリーを実行します。デバイスは、クラウドサーバーから返されたクエリー結果に基づいて、適用するアクションを決定します。

- URL に一致するルールが検出された場合は、ルールが属する URL カテゴリに指定されたアクションが適用されます。ルールが複数の URL カテゴリに属する場合は、重大度が最も高いカテゴリに指定されたアクションが適用されます。
- 一致するルールが見つからない場合、デバイスはパケットに対して URL フィルタリングプロファイルのデフォルトアクションを実行します。デフォルトアクションが設定されていない場合、デバイスはパケットの通過を許可します。

URL filtering action

URL カテゴリには URL フィルタリングアクションを指定し、URL フィルタリングプロファイルにはデフォルトアクションを指定できます。
デバイスは、次の URL フィルタリングアクションをサポートしています。

- **Blacklist**: 一致するパケットをドロップし、パケットの送信元を IP ブラックリストに追加します。IP ブラックリスト機能がイネーブルになっている場合、ブラックリストに掲載された送信元からのパケットはブラックリスト期間中ブロックされます。IP ブラックリスト機能がイネーブルになっていない場合、ブラックリストに掲載された送信元からのパケットはブロックされません。

  IP ブラックリスト機能の詳細については、攻撃防御のオンラインヘルプを参照してください。

  blacklist アクションのブラックリスト期間を設定するには、

  Objects > APPSecurity > Security Actions > Block に移動します。
- **Drop**: 一致するパケットをドロップします。
- **Permit**: 一致するパケットの通過を許可します。
- **Redirect**: 一致するパケットを Web ページにリダイレクトします。
- **Reset**: TCP リセットメッセージを送信して、一致するパケットの TCP 接続を閉じます。
- **Logging**: 一致するパケットをロギングします。このアクションは、URL フィルタリングプロファイルでロギング機能が有効になった後にのみ有効になります。

HTTPS URL filtering

デフォルトでは、デバイスは HTTP URL フィルタリングだけをサポートします。HTTPS トラフィックのフィルタリングをイネーブルにするには、次のいずれかの方法を使用します。

- SSL 復号化を使用して HTTPS トラフィックを復号化し、復号化されたトラフィックで HTTP URL フィルタリングを実行します。SSL 復号化の詳細は、アプリケーションプロキシのオンラインヘルプを参照してください。
- HTTPS URL フィルタリングをイネーブルにします。この機能は、復号化されていない HTTPS トラフィックに対して URL フィルタリングを実行します。デバイスはクライアントからの Client Hello メッセージを直接検出し、URL フィルタリング用の Sever Name Indication(SNI)拡張からサーバー名を抽出します。

SSL 復号化には大量の暗号化および復号化操作が含まれるため、デバイスの転送パフォーマンスが低下する可能性があります。ベストプラクティスとして、デバイスが HTTPS トラフィックに対してのみ URL フィルタリングを実行する必要がある場合は、HTTPS URL フィルタリングをイネーブルにして、HTTPS トラフィックに対して URL フィルタリングをイネーブルにします。

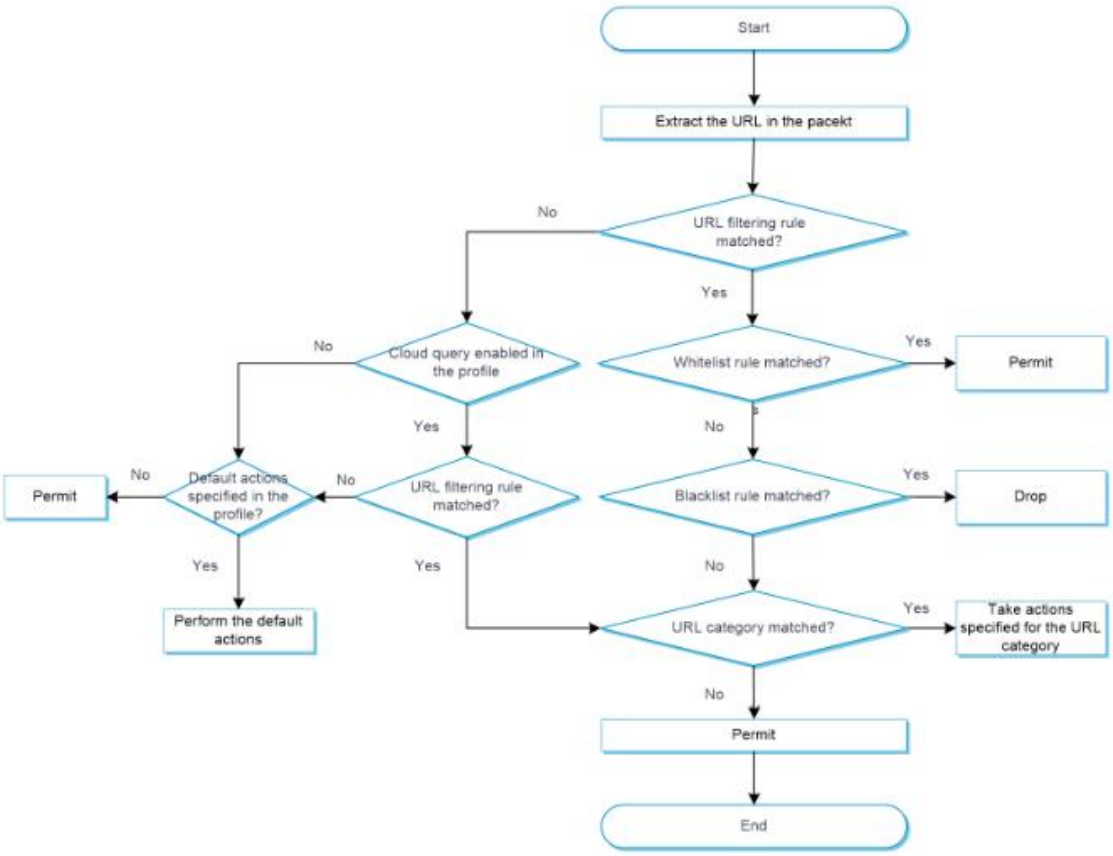
URL filtering mechanism

URL フィルタリングは、URL フィルタリングプロファイルをセキュリティーポリシー、URL フィルタリングが有効になります。

図 2 に示すように、デバイスは HTTP パケットを受信すると、以下の動作を行います。

1. デバイスは、パケットをセキュリティーポリシーと比較します。
   パケットが URL フィルタリングプロファイルに関連付けられたセキュリティーポリシーと一致する場合、デバイスはパケットから URL を抽出します。
2. デバイスは、抽出された URL を、URL フィルタリングプロファイル内のホワイトリストおよびブラックリストルールと比較します。
   - URL がホワイトリストルールと一致する場合、パケットの通過が許可されます。
   - URL がブラックリストルールと一致する場合、パケットはドロップされます。
   - URL がプロファイル内のホワイトリストルールまたはブラックリストルールと一致しない場合、デバイスはステップ 3 を実行します。
3. デバイスは、抽出された URL を、URL フィルタリングプロファイル内の URL フィルタリング規則と比較します。
   - URL がユーザー定義の URL カテゴリに属する URL フィルタリング規則と一致する場合、デバイスは URL カテゴリに指定されたアクションを実行します。
     URL フィルタリング規則が複数のユーザー定義 URL カテゴリに属する場合、最も高い重大度を持つ URL カテゴリに指定されたアクションが適用されます。
   - URL レピュテーションがイネーブルの場合、デバイスは、一致する URL フィルタリング規則が URL レピュテーションシグニチャライブラリ内の攻撃カテゴリに属するかどうかを判断します。イネーブルの場合、デバイスはパケットの攻撃カテゴリに指定されたアクションを実行します。
   - URL が、定義済みの URL カテゴリに属する URL フィルタリング規則と一致する場合、デバイスは URL カテゴリに指定されたアクションを実行します。
     URL フィルタリング規則が複数の定義済み URL カテゴリに属する場合、最も高い重大度を持つ URL カテゴリに指定されたアクションが適用されます。
4. URL がプロファイル内のどのルールとも一致せず、プロファイル内でクラウドクエリーがディセーブルになっている場合、プロファイルに指定されたデフォルトアクションが適用されます。デフォルトアクションが設定されていない場合、デバイスはパケットの通過を許可します。
   URL がプロファイル内のどのルールとも一致せず、プロファイル内でクラウドクエリーが有効になっている場合、デバイスはステップ 4 を実行します。
5. デバイスは URL をクラウドサーバーに転送して、さらにクエリーを実行します。
   - URL に一致するルールが見つかった場合、デバイスは、ステップ 3 で説明したようにパケットに対して実行するアクションを決定します。
   - 一致するルールが見つからない場合、デバイスはパケットに対してプロファイルのデフォルトアクションを実行します。デフォルトアクションが設定されていない場合、デバイスはパケットの通過を許可します。

図 2 URL フィルタリングメカニズム



Restrictions and guidelines

Restrictions and guidelines: Text-based URL filtering rule configuration

ホスト名または URI マッチングのテキストパターンでアスタリスク文字(*)を使用する場合は、次の注意事項に従ってください。

- ホスト名を照合する場合、アスタリスク(*)は、テキストパターンの先頭または末尾カード文字として、テキストパターンの先頭または末尾にだけ使用できます。0
- URI マッチングでは、アスタリスク(*)をワイルドカード文字としてテキストパターンの先頭または末尾に表示して 0 以上の文字と一致させるか、または中間に非ワイルドカード文字として表示できます。

Restrictions and guidelines: Regular expression-based URL filtering rule configuration

- 正規表現パターンには、最大 4 つの分岐を含めることができます。たとえば、**'abc(c d e¥x3D)'**は有効で、**'abc(c onreset onselect onchange style¥x3D)'**は無効です。

- 中かっこは使用できません。たとえば、**'ab((abcs*?))'**は無効です。
- 分岐を別の分岐の後に指定することはできません。たとえば、**'ab(a b)(c d)^¥¥r¥¥n]+?'**は無効です。
- アスタリスク(*)または疑問符(?)の前には、4 文字以上のワイルドカード以外の文字が必要です。たとえば、**'abc*'**は無効で、**'abcd*DoS¥x2d¥d{5}¥x20¥x2bxi¥¥r¥¥nJOIN'**は有効です。

Restrictions and guidelines: whitelist

- パケットがホワイトリストルールに一致する場合、URL フィルタリングログリストの **URL Category** カラムには **Whitelist** が表示されます。
- HTTP 要求の referer ヘッダーが URL フィルタリングのホワイトリストと一致する場合、URL フィルタリングログリストの **URL Category** カラムには **Referer Whitelist** と表示されます。
- ホワイトリストモードがイネーブルの場合、パケットがいずれかのホワイトリスト規則に一致しないと、URL フィルタリングログリストの **URL Category** カラムに **Blacklist** と表示されます。

Restrictions and guidelines: URL filtering profile activation

URL フィルタプロファイルを作成、編集または削除した後、有効にするには構成をアクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化するか、デフォルトで 40 秒後に構成が自動的にアクティブ化されます。構成をアクティブ化すると、一時的な DPI サービスの中断が発生します。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。

Restrictions and guidelines: Licensing requirements

URL フィルタリングにはライセンスが必要です。ライセンスの期限が切れた場合、既存の URL フィルタリングシグニチャライブラリは引き続き使用できますが、デバイス上のライブラリをアップグレードしたり、クラウドクエリーを使用したりすることはできません。ライセンスの詳細については、ライセンスのオンラインヘルプを参照してください。

Restrictions and guidelines: HTTPS URL filtering

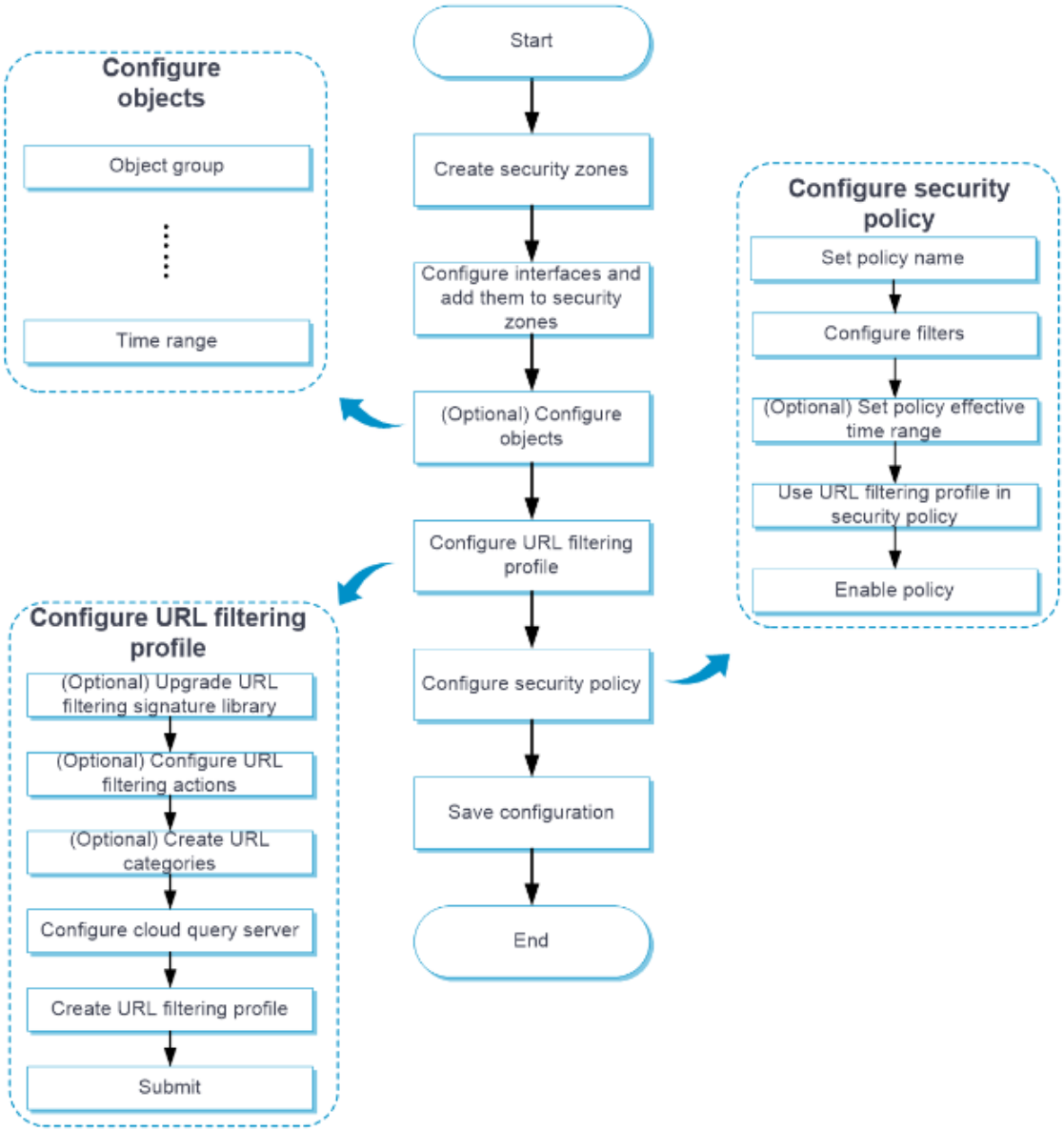
HTTPS URL フィルタリングでは、URL フィルタリング規則のホスト名一致基準のみが有効になります。URI 一致基準は有効になりません。
この機能は、URL のホスト名フィールドがサーバーのドメイン名である場合にのみ有効です。ホスト名フィールドが IP アドレスの場合、この機能は HTTPS トラフィックに適用されません。
この機能は、次の状況では有効になりません。

- クライアントブラウザは、SNI 拡張が暗号化されるため、TLS 1.3 ダウングレード拡張メカニズムを有効にします。
- HTTPS パケットには SNI 拡張がありません。

Configure URL filtering

図 3 に示すように、URL フィルタリングを設定します。

図 3 URL フィルタリングの設定手順



Configure a URL category

ユーザー定義の URL カテゴリを作成し、特定の URL フィルタリング要件を満たすフィルタリング規

則を設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **URL Filtering** > **URL Categories** を選択します。
3. **Create** をクリックします。
4. URL カテゴリを作成します。

表 2 URL カテゴリの設定項目

項目	説明
Name	URL カテゴリの名前を入力してください。カテゴリ名を **Pre-**で始めることはできません。
Description	URL カテゴリの説明を入力します。
Severity level	URL カテゴリに 1000～65535 の一意の重大度レベルを割り当てます。値が大きいほど、重大度レベルが高くなります。
Include predefined category	定義済みの URL カテゴリを選択して、そのすべての規則を URL カテゴリに追加します。

5. URL カテゴリに URL フィルタリング規則を追加します。
   a. **Add** をクリックします。
   b. **Match pattern** リストから、host name フィールドの一致パターンタイプを選択します。オプションは **Text** と **Regular expression** です。
   c. ホスト名フィールド]フィールドに一致パターンを入力します。
   d. **Match pattern** リストから、URI フィールドの一致パターンタイプを選択します。オプションは、**Text**、**Regular expression**、および**–NONE—**です。
   e. URI フィールドに一致パターンを入力します。URI フィールドの一致パターンに**–NONE—**オプションが選択されている場合は、この手順は不要です。
   f. **OK** をクリックします。
   g. 上記の手順を繰り返して、さらに URL フィルタリング規則を追加します。
6. **OK** をクリックします。

URL Categories ページに URL カテゴリが表示されます。

Configure the cloud query server

URL フィルタリング用のクラウドクエリーサーバーを設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **URL Filtering** > **URL Categories** を選択します。
3. **Cloud server connection status** フィールドの横にある **Configure** をクリックします。
4. クラウドクエリーサーバーを設定します。

表 3 クラウドクエリーサーバーの設定項目

項目	説明
Server address	クラウドクエリーサーバーの IP アドレスまたはホスト名を入力します。当社のクラウドクエリーサーバーのみがサポートされています。
Max cached URL entries	キャッシュできる URL エントリの最大数を指定します。 デバイスは、クラウドクエリーのためにクラウドクエリーサーバーに送信された一意の URL ごとに URL キャッシュエントリを作成します。クラウドクエリーの結果はキャッシュエントリに保存されます。
Min cache period	URL キャッシュエントリの最小キャッシュ期間を分単位で指定します。 URL キャッシュエントリの最小キャッシュ期間を設定すると、指定した期間中にエントリガー削除されないようになります。 URL フィルタリングキャッシュがいっぱいになると、最も古い URL キャッシュエントリのキャッシュ期間が特定され、上書きするかどうかが決定されます。 • エントリのキャッシュ期間が最小キャッシュ期間以下の場合、システムはエントリを削除しません。新しいエントリはキャッシュされません。 • エントリのキャッシュ期間が最小キャッシュ期間より長い場合、システムはエントリを新しいエントリで上書きします。 ただし、設定された最大キャッシュ URL エントリガー現在キャッシュされているエントリよりも少ない場合は、キャッシュ期間が最小キャッシュ期間以下であっても、最も古いキャッシュエントリガー削除されます。

Configure a URL filtering profile

URL フィルタリングプロファイルでは、次の設定を行うことができます。

- クラウドクエリーを有効にします。
- どの URL フィルタリング規則にも一致しないパケットのデフォルトアクションを指定します。
- ホワイトリストおよびブラックリストルールを設定します。ホワイトリストルールは、ブラックリストルールよりも優先されます。
- URL カテゴリのアクションを指定します。

  URL フィルタリングプロファイルには、デバイス上のすべての URL カテゴリが含まれています。URL フィルタリングプロファイルでは、個々の URL カテゴリに対してアクションを指定できます。HTTP パケットが URL カテゴリの URL フィルタリング規則と一致する場合、そのカテゴリに指定されたアクションがパケットに適用されます。一致規則が複数の URL カテゴリにある場合は、最も重大度の高いカテゴリに指定されたアクションが実行されます。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **URL Filtering** > **Profiles** を選択します。
3. **Create** をクリックします。
4. URL フィルタリングプロファイルを作成します。

表 4 URL フィルタリングプロファイルの構成項目

項目	説明
Name	URL フィルタリングプロファイルの名前を入力します。
Default action	URL フィルタリング規則に一致しないパケットに対して実行するデフォルトアクションを選択します。オプションは、**Permit**, **Drop**, **Reset**, **Redirect**, and **Blacklist** です。
Cloud query	クラウドクエリーを有効にするには、ボックスを選択します。
Logging	URL フィルタリング規則に一致するパケットのロギングをイネーブルにするには、このボックスを選択します。 この項目を選択する前に、最初にデフォルトアクションを設定してください。
Enable HTTPS URL filtering	復号化されていない HTTPS トラフィックで URL フィルタリングを有効にするには、このボックスを選択します。 有効なプロキシポリシーで SSL 復号化アクションが選択されている場合、この機能は有効になりません。SSL 復号化の詳細は、アプリケーションプロキシのオンラインヘルプを参照してください。

Enable referer whitelist	このチェックボックスをオンにすると、HTTP 要求の referer ヘッダーが URL フィルタリングホワイトリストと一致した場合に、HTTP 要求を通過させることができます。
Whitelist mode	チェックボックスをオンにすると、URL フィルタリングのホワイトリストにある Web サイトにのみアクセスできます。
Whitelist	必要に応じて、URL フィルタリングプロファイルにホワイトリストルールを追加します。 URL フィルタリングプロファイルにホワイトリストルールを追加するには、次の手順を実行します。 1. **Whitelist** 領域で、**Add** をクリックします。 2. **Add Whitelist Rule** ウィンドウが開きます。 3. **Match pattern** リストから、host name フィールドの一致パターンタイプを選択します。オプションは **Text** と **Regular expression** です。 4. ホスト名フィールドに一致パターンを入力します。 5. **Match pattern** リストから、**URI** フィールドの一致パターンタイプを選択します。オプションは、**Text**, **Regular expression**、および**–NONE—**です。 6. URI フィールドに一致パターンを入力します。URI フィールドの一致パターンに**–NONE—**オプションが選択されている場合は、この手順は不要です。
Blacklist	必要に応じて、URL フィルタリングプロファイルにブラックリストルールを追加します。
URL categories	**URL categories** 領域で、個々の URL カテゴリのアクションを選択します。サポートされているアクションは、**Permit**, **Drop**, **Reset**, **Redirect**, **Blacklist** および **Logging** です。URL カテゴリのロギングアクションを選択する前に、まず、**Permit**、**Drop**、**Reset**、**Redirect**、および **Blacklist** アクションからアクションを選択します。
Enable URL reputation	悪意のある URL へのアクセスをブロックする URL レピュテーションを有効にするには、このボックスを選択します。この機能を有効にすると、デバイスはパケットから抽出された URL と URL レピュテーションシグニチャライブラリ内の URL を比較します。一致が検出された場合、その URL は悪意のある URL と見なされ、一致する URL が属する攻撃カテゴリに指定されたアクションが実行されます。一致が検出されない場合、デバイスはパケットの通過を許可します。

Action configuration	URL レピュテーションシグニチャライブラリ内の個々の攻撃カテゴリに対するアクションを設定します。

5. **OK** をクリックします。
   URL Filtering Profiles ページに URL フィルタリングプロファイルが表示されます。
6. セキュリティーポリシーで URL フィルタリングプロファイルを使用します。
   セキュリティーポリシーの詳細については、セキュリティーポリシーのオンラインヘルプを参照してください。
7. 構成をただちに有効にするには、**Submit** をクリックします。または、構成が自動的に有効になるまで 40 秒間待機します。

File filtering

このヘルプには、次のトピックが含まれています。

- Introduction
  - Basic concepts
  - File filtering mechanism
- Restrictions and guidelines
- Configure file filtering
  - Configure a file type group
  - Configure a file filtering profile

Introduction

ファイルフィルタ機能は、ファイル拡張子に基づいてファイルをフィルタします。ファイル拡張子に基づいてファイルにアクションを実行するようにファイルフィルタを構成できます。
ファイルフィルタリングは、次のプロトコルのパケットのフィルタリングをサポートします。

- HTTP。
- FTP。
- SMTP。
- IMAP。
- NFS。
- RTMP。
- SMB。

Basic concepts

File type group

ファイルタイプグループには、最大 32 個のファイル拡張子を含めることができます。ファイルは、グループ内のファイル拡張子と一致する場合、ファイルタイプグループと一致します。定義済のファイル拡張子を選択し、ファイルタイプグループ内のファイル拡張子をカスタマイズできます。

File filtering rule

ファイルフィルタリングルールには、一連のファイルフィルタリング基準およびパケットを照合するためのアクションが含まれています。ファイルフィルタリング基準には、ファイルタイプグループ、方向

(**Upload**, **Download** または **Both**)およびアプリケーションが含まれます。パケット処理アクションには、**Drop**, **Permit** および **Logging** が含まれます。ルールを適用するには、ファイルがすべてのフィルタリング基準に一致する必要があります。

Common configuration

次の共通設定項目がサポートされています。

- **Action for files with false extension**: 偽の拡張子を持つファイルを含むパケットに対するアクションを選択します。実際のファイル拡張子に基づいてファイルフィルタリング検査を実行するには、**Permit** を選択します。このようなパケットを直接廃棄するには、**Drop** を選択します。
- **Max decompressed data size**: ファイルフィルタリング検査のためにファイル内で解凍できるデータの最大サイズを指定します。デバイスは ZIP ファイルだけを解凍できます。

File filtering mechanism

ファイルフィルタリングがサポートするプロトコルのパケットを受信すると、デバイスは次の動作を実行します。

1. パケットをセキュリティーポリシーと比較します。
   パケットがファイルフィルタリングプロファイルに関連付けられたセキュリティーポリシーと一致する場合、デバイスはパケットを処理するためにファイルフィルタリングモジュールに送信します。
2. パケット内のファイル拡張子を抽出して記録します。
3. 実際のファイル拡張子を識別し、記録されたファイル拡張子と比較します。
   - 2 つのファイル拡張子が一致する場合、または実際のファイル拡張子を識別できない場合、デバイスはステップ 4 に進む。
   - 2 つのファイル拡張子が一致しない場合、デバイスは **Action for files with false extension** 項目の設定をチェックします。
     - **Drop** アクションが選択されている場合、デバイスはパケットを直接ドロップします。
     - **Permit** アクションが選択されている場合、デバイスはステップ 4 に進み、実際のファイル拡張子に基づいてファイルフィルタリング検査を実行します。
4. パケットアトリビュート(ファイル拡張子、アプリケーション層アプリケーション、およびファイル転送方向)をファイルフィルタリングポリシーのファイルフィルタリング規則と比較することによって、パケットに対して実行するアクションを決定します。
   - パケットがポリシー内のファイルフィルタリング規則に一致しない場合、デバイスはパケットの通過を許可します。
   - パケットが 1 つのルールにしか一致しない場合、デバイスはそのルールに指定されたアクションを実行します。
   - パケットが複数のルールに一致する場合、デバイスは次のようにアクションを決定します。

- 一致規則に permit アクションと drop アクションの両方がある場合、デバイスは drop アクションを実行します。
- ロギングアクションは、一致ルールのいずれかに対して指定されている場合に実行されます。

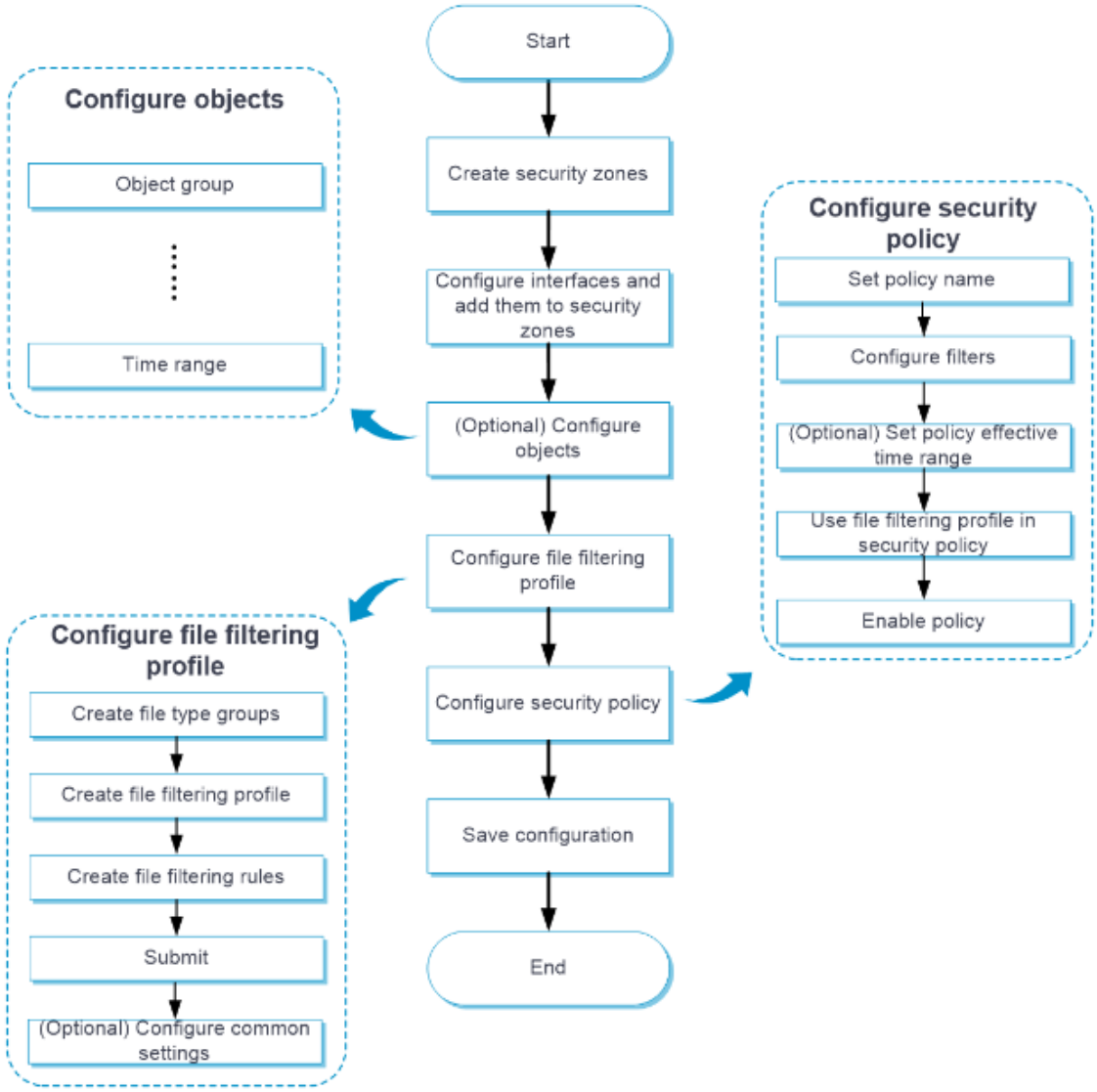
Restrictions and guidelines

ファイルフィルタリングプロファイルを作成、編集または削除した後、有効にするには構成をアクティブ化する必要があります。**Submit** をクリックして構成をすぐにアクティブ化するか、デフォルトでは構成が 40 秒後に自動的にアクティブ化されます。構成をアクティブ化すると、一時的な DPI サービスの中断が発生します。DPI ベースのサービスも中断される場合があります。たとえば、セキュリティーポリシーではアプリケーションへのアクセスを制御できません。

Configure file filtering

図 1 に示すように、ファイルフィルタリングを設定します。

図 1 ファイルフィルタリングの設定手順



Configure a file type group

ファイルタイプグループを作成し、グループ内のファイル拡張子を設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **Data Filtering** > **File Type Groups** を選択します。
3. **Create** をクリックします。
4. ファイルタイプグループを作成します。

表 1 ファイルタイプグループの設定項目

項目	説明
Name	ファイルタイプグループの名前を入力します。
Description	ファイルタイプグループの説明を入力します。
Predefined file extensions	ファイルタイプグループに定義済みのファイル拡張子を選択します。
Custom file extensions	カスタムファイル拡張子を 1 行に 1 つずつ入力します。

5. **OK** をクリックします。
   ファイルタイプグループが **File Type Groups** ページに表示されます。

Configure a file filtering profile

ファイルフィルタリングプロファイルを作成し、そのプロファイルでファイルフィルタリング規則を設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **File Filtering** > **Profiles** を選択します。
3. **Create** をクリックします。
4. ファイルフィルタリングプロファイルを作成します。

表 2 ファイルフィルタリングプロファイルの構成項目

項目	説明
Name	ファイルフィルタリングプロファイルの名前を入力します。
Description	ファイルフィルタリングプロファイルの説明を入力します。

5. **File filtering rules** 領域で、**Create** をクリックします。
6. ファイルフィルタリング規則を作成します。

表 3 ファイルフィルタリング規則の設定項目

項目	説明
Name	ファイルフィルタリングプロファイルの名前を入力します。
Applications	規則が適用されるアプリケーションのアプリケーション層プロトコルを選択します。 サポートされているアプリケーション層プロトコルは、FTP、HTTP、IMAP、NFS、POP3、RTMP、SMB、および SMTP です。
File type groups	ファイルフィルタルールのファイルタイプグループを選択します。 ファイルは、グループ内のファイル拡張子と一致する場合、ファイルタイプグループと一致します。
Direction	ルールが適用されるファイル転送方向を選択します。 オプションは **Upload**, **Download**、および **Both** です。
Action	パケットを一致させるアクションを選択します。 オプションは **Permit** と **Drop** です。
Logging	一致するパケットのロギングをイネーブルにするかどうかを選択します。 オプションは **Enable** と **Disable** です。

7. **OK** をクリックします。

   ファイルフィルタリング規則は、ファイルフィルタリングプロファイルのファイルフィルタリング規則リストに表示されます。

8. **OK** をクリックします。

   ファイルフィルタリングプロファイルは、**File Filtering Profiles** ページに表示されます。

9. セキュリティーポリシーでファイルフィルタリングプロファイルを使用します。セキュリティーポリシーの詳細は、セキュリティーポリシーのオンラインヘルプを参照してください。

10. **Submit** をクリックしてすぐに設定をアクティブにするか、設定が自動的にアクティブになるまで 40 秒待ちます。

    ファイルフィルタリングプロファイルを作成した後、有効にするには構成をアクティブ化する必要があります。デフォルトでは、構成は 40 秒後に自動的にアクティブ化されます。

APT defense

このヘルプには、次のトピックが含まれています。

- Introduction
  - APT defense implementation
  - Sandbox inspection mechanism
  - Collaboration with the anti-virus feature
- Configure APT defense
  - Configure the sandbox
  - Configure an APT defense profile

Introduction

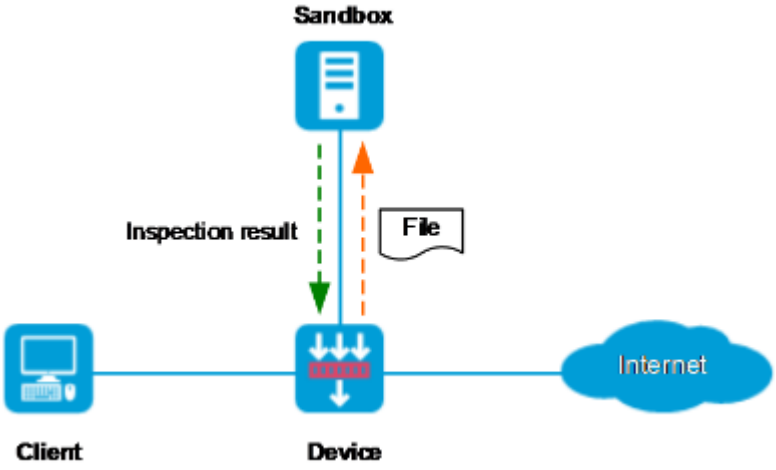
APT(Advanced Persistent Threat)とは、標的を定めたサイバー攻撃を防御するための最も効果的な方法の 1 つにサンドボックス技術があります。サンドボックス技術は、隔離された脅威検査環境を作成して、配信されたトラフィックを分析し、そのトラフィックが悪意のあるものであれば、デバイスがブロッキングなどのアクションを実行します。

APT defense implementation

図 1 に示すように、外部攻撃者が企業ネットワークに対して APT 攻撃を開始した場合、APT 防御は次のように実装されます。

1. 攻撃トラフィックがデバイス上の APT 防御ポリシーと一致する場合、デバイスはトラフィックからファイルコンテンツを抽出し、ファイルを再構成します。
2. デバイスは、脅威分析のために再構成されたファイルをサンドボックスに送信します。
3. サンドボックスはファイルを実行し、ファイルの動作を分析してファイルが悪意のあるものかどうかを判断します。検査が完了すると、サンドボックスはファイル検査結果をデバイスに送り返し、デバイスはその結果を APT 防御キャッシュに保存します。
   - トラフィックが悪意のある場合、デバイスは、指定されたアンチウィルスポリシーに基づいて、後続のトラフィックに対してブロックアクションまたはアラートアクションを実行します。
   - トラフィックが悪意のあるものでなければ、デバイスはトラフィックの通過を許可します。

図 1 APT 防衛の実施



Sandbox inspection mechanism

サンドボックスは、実際のネットワークをシミュレートして未知のファイルを実行し、ファイルの動作を記録する仮想検査システムです。サンドボックスでは、ファイルの動作が排他的な動作シグネチャライブラリと比較されます。一致するファイルが見つかった場合、サンドボックスはそのファイルが悪意のあるファイルであると判断します。

サンドボックスは、さまざまなウィルス、脆弱性、脅威のシグニチャを分析し、悪意のある動作のパターンを抽出し、一連の規則を作成することによって、動作シグニチャライブラリを構築します。

シグニチャベースの検査(アンチウィルス検査など)とは異なり、サンドボックス検査では、動作に基づいて攻撃を識別し、未知の攻撃を識別できます。

Collaboration with the anti-virus feature

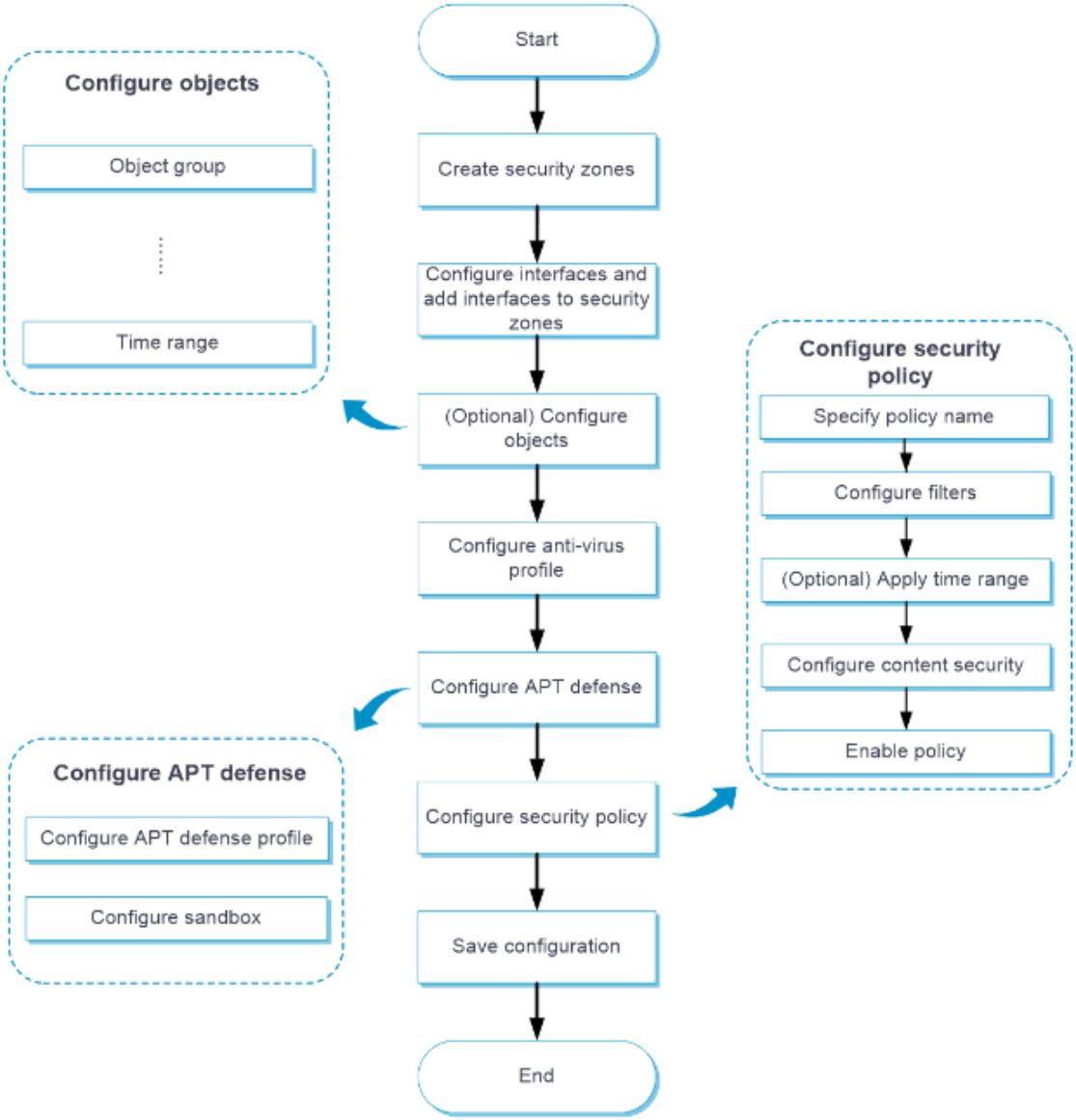
サンドボックスは、トラフィックが悪意のあるものかどうかを識別するだけで、処理アクションは提供しません。悪意のあるトラフィックに対してアクションを実行する場合、デバイスはアンチウィルス機能と連携する必要があります。アンチウィルス機能が設定されている場合、デバイスは悪意のあるトラフィックのアプリケーション層プロトコルを識別し、トラフィックをアンチウィルスポリシーと比較します。一致が検出されると、デバイスは悪意のあるトラフィックに対してアクションを実行します。

アンチウィルスプロファイルの詳細については、アンチウィルスのオンラインヘルプを参照してください。

Configure APT defense

図 2 に示すように、APT 防御を設定します。

図 2 APT 防衛構成手順



Configure the sandbox

手順

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**APPSecurity** > **APT Defense** > **Sandbox** を選択します。
3. サンドボックスを設定します。

表 1 サンドボックスの設定項目

項目	説明
Connection state	サンドボックスの接続状態を表示します。
Enable sandbox collaboration	この項目を選択すると、サンドボックスコラボレーションが有効になります。 サンドボックスコラボレーションにより、デバイスは APT 防御プロファイルに一致するパケットをサンドボックスに送信できます。
Sandbox address	サンドボックスの IP アドレスまたはドメイン名を指定します。
Protocols	デバイスとサンドボックス間でデータを転送するためのプロトコルを選択します。 デバイスは、データ伝送プロセスを暗号化できる HTTPS プロトコルだけをサポートします。
Username	サンドボックスにログインするためのユーザー名を指定します。
Password	サンドボックスにログインするためのパスワードを指定します。
Cache entries	サンドボックス検査結果をキャッシュするためのデバイスのエントリ数を設定します。 この設定は、サンドボックス検査結果をキャッシュするために、次の両方のリストに適用されます。 • **Non-hit list**: 脅威でないか、脅威として識別できないファイルの MD5 値をキャッシュします。 • **Hit list**: 脅威として識別されたファイルの MD5 値をキャッシュします。
Maximum file size for sandbox inspection	サンドボックス検査でサポートされる各ファイルタイプのファイルサイズを設定します。

4. **OK** をクリックします。

Configure APT defense profile

APT 防御プロファイルを設定するには、次の作業を実行します。

手順

1. **Objects** タブをクリックします。

2. ナビゲーションペインで、**Objects** を選択します。

APT Defense Profiles ページが開きます。

3. **Create** をクリックします。

Create APT Defense Profile ページが開きます。

4. **APT defense** プロファイルを作成します。

表 2 APT 防御プロファイルの設定項目

項目	説明
Name	APT 防御プロファイルの名前を指定します。
Description	識別しやすいように説明を入力します。
Protocols	APT 防御検出用のアプリケーション層プロトコルを選択します。
File type	サンドボックス検査のファイルタイプを選択します。
Direction	方向基準のトラフィック方向を選択します。オプションは次のとおりです。 • Upload。 • Download。 • Upload & download。

5. **OK** をクリックします。

APT 防御プロファイルは、**APT Defense Profiles** ページに表示されます。

6. セキュリティーポリシーで APT 防御プロファイルを使用します。セキュリティーポリシーの詳細は、セキュリティーポリシーのオンラインヘルプを参照してください。

APR

このヘルプには、次のトピックが含まれています。

- Introduction
  - PBAR
  - NBAR
  - Application group
- Restrictions and guidelines
- Configure APR
  - Configure an application
  - Configure an application group

Introduction

Application Recognition(APR)機能は、ポートで受信またはポートから送信されるアプリケーションベースサービスのパケットのアプリケーションプロトコルを認識し、統計情報を収集します。
APR では、次のメソッドを使用してアプリケーションプロトコルを認識します。

- Port-based application recognition(PBAR)。
- Network-Based Application Recognition(NBAR)。

このヘルプのアプリケーションプロトコルは、APR で認識できるアプリケーションプロトコルです。アプリケーションは事前定義またはユーザー定義です。

PBAR

PBAR は、ポートをアプリケーションプロトコルにマッピングし、ポートプロトコルマッピングに従ってアプリケーションプロトコルのパケットを認識します。

PBAR は、次のポートプロトコルマッピングをサポートします。

- **Predefined**: アプリケーションプロトコルは、システムによって定義されたポートを使用します。
- **User-defined**: アプリケーションプロトコルは、ユーザーによって定義されたポートを使用します。

PBAR は、ユーザー定義のポート設定を維持および適用するために、次のマッピングを提供します。

- **General port mapping**: ユーザー定義のポートをアプリケーションプロトコルにマッピングします。そのポート宛てのすべてのパケットは、アプリケーションプロトコルのパケットとみなされます。たとえば、ポート 2121 が FTP にマッピングされている場合、そのポート宛てのすべてのパケットは FTP パケットとみなされます。
- **Host-port mapping**: 特定のホストとの間で送受信されるパケットのアプリケーションプロトコルにユーザー定義ポートをマッピングします。たとえば、ポート 2121 のネットワークセグメント 10.110.0.0/16 宛てのすべてのパケットが FTP パケットとみなされるように、ホストポートマッピングを確立できます。ホストの範囲を定義するには、ACL、ホスト IP アドレス範囲またはサブネットを指定できます。

NBAR

NBAR は、事前定義またはユーザー定義の NBAR ルールを使用してパケットコンテンツを照合し、一致するパケットのアプリケーションプロトコルを認識します。事前定義された NBAR ルールは、APR シグニチャライブラリから自動的に生成されます。
現在のソフトウェアバージョンでは、事前定義された NBAR ルールだけがサポートされており、設定はできません。

Application group

同様のシグニチャまたは制限を持つアプリケーションプロトコルをアプリケーショングループに追加できます。APR は、パケットの内容をシグニチャまたは制限と照合することによってアプリケーションプロトコルのパケットを認識します。パケットがアプリケーショングループ内のアプリケーションプロトコルのパケットとして認識された場合、そのパケットはアプリケーショングループのパケットと見なされます。
アプリケーショングループには、複数の定義済みアプリケーションとユーザー定義アプリケーションを含めることができます。

Restrictions and guidelines

- APR シグニチャライブラリの更新にはライセンスが必要です。ライセンスの有効期限が切れた後も、NBAR は既存のシグニチャライブラリを引き続き使用できますが、シグニチャライブラリを更新できません。ライセンスの詳細については、ライセンス管理のオンラインヘルプを参照してください。
- APR 機能を使用する前に、APR シグニチャライブラリを最新バージョンに更新します。

Configure APR

Configure an application

Applications ページでは、PBAR のユーザー定義アプリケーションを作成および変更できます。

Port mapping categories

PBAR では、次のポートマッピングカテゴリを使用できます。

- **General port mapping**: ユーザー定義のポートをアプリケーションプロトコルにマッピングします。そのポート宛てのすべてのパケットは、アプリケーションプロトコルのパケットとみなされます。たとえば、ポート 2121 が FTP にマッピングされている場合、そのポート宛てのすべてのパケットは FTP パケットとみなされます。
- **ACL-based host-port mapping**: 指定された ACL に一致するパケットのアプリケーションプロトコルにポートをマッピングします。
- **Subnet-based host-port mapping**: 指定されたサブネットに送信されるパケットのアプリケーションプロトコルにポートをマッピングします。複数のサブネットベースマッピングがパケットに適用され、これらのサブネットが重複する場合、PBAR は重複セグメント宛てのパケットを、範囲が最も小さいサブネットのポートマッピングと一致させます。
- **IP address-based host-port mapping**: 指定された IP アドレス宛てのパケットのアプリケーションプロトコルにポートをマッピングします。

Create a port mapping

1. **Objects** タブをクリックします。
2. **APPSecurity > App Recognition > Applications** を選択します。
3. アプリケーションを作成するには、**Create** をクリックします。
4. アプリケーションの名前を入力し、リスクタイプを選択します。デバイスは、指定されたリスクタイプに基づいてリスクレベルを計算します。
5. **Port mappings** 領域で **Create** をクリックします。
6. アプリケーションのポートマッピングを作成します。

表 1 ポートマッピングの設定項目

項目	説明
Port number	アプリケーションがマップされているポートの番号を入力します。
Protocol	トランスポート層プロトコルを選択します。使用可能な値は、All、DCCP、SCTP、TCP、UDP および UDP-Lite です。 **All** を選択すると、次の条件を満たすパケットが、指定されたアプリケーションプロトコルのパケットとして認識されます。

	• パケットは、トランスポート層プロトコルによってカプセル化されます。 • パケットには指定されたポートがあります。
Type	次の値から一致タイプを選択します。 • All:一般的なポートマッピングを表します。 • IPv4 アドレスベースのホストポートマッピング。 • IPv6 アドレスベースのホストポートマッピング。 • IPv4 サブネットベースのホストポートマッピング。 • IPv6 サブネットベースのホストポートマッピング。 • IPv4 ACL ベースのホストポートマッピング。 • IPv6 ACL ベースのホストポートマッピング。
Match criteria	• IP アドレスベースのホスト/ポートマッピングを選択した場合は、IP アドレス範囲を入力します。 • サブネットベースのホスト/ポートマッピングを選択した場合は、IP サブネットを入力します。 • ACL ベースのホスト/ポートマッピングがすでに選択されている場合は、ACL を入力します。
VRF instance	VRF インスタンスを選択します。

7. **OK** をクリックします。

1 つのアプリケーションに対して複数のポートマッピングを作成できます。PBAR は、パケットのアプリケーションプロトコルを認識するポートマッピングを次の順序で選択します。

a. IP アドレスベースのポートマッピング。
b. サブネットベースのポートマッピング。
c. ACL ベースのホストポートマッピング。
d. 一般的なポートマッピング。

8. **Create Application** ページで **OK** をクリックします。

Applications ページで、**Show user-defined applications only** を選択して、設定を確認します。

Edit a predefined application

1. **Objects** タブをクリックします。
2. **APPSecurity** > **App Recognition** > **Applications** を選択します。
3. 定義済みのアプリケーションを選択し、右側の **Edit** をクリックします。
4. 「アプリケーションの構成」で説明されている手順に従って、アプリケーションのポートマッピングを追加します。

新しく追加されたポートマッピングは、編集後すぐに有効になります。新しく追加されたポートマッピングと一致するパケットは、アプリケーションのパケットとして認識できます。

Configure an application group

同様の特性または制限を持つアプリケーションをアプリケーショングループに追加できます。

手順

1. **Objects** タブをクリックします。
2. **APPSecurity** > **App Recognition** > **Application Groups** を選択します。
3. **Create** をクリックします。
4. アプリケーショングループを作成します。

表 2 アプリケーショングループの設定項目

項目	説明
Group	アプリケーショングループの名前を入力します。
Description	識別と管理のための説明を入力します。
Category	目的のアプリケーションをフィルタするカテゴリを選択します。
Risk type	リスクタイプを選択して、目的のアプリケーションをフィルタします。
Risk level	リスクレベルを選択して、必要なアプリケーションをフィルタリングします。
Filter	**Select all** または **Select** をクリックして、アプリケーションを **Available Applications** リストから **Selected Applications** リストに移動します。

5. **OK** をクリックします。
6. **Application Groups** ページで設定を確認します。

Terminal identification

このヘルプには、次のトピックが含まれています。

- Introduction

Introduction

IoT(Internet of Things 特定することは、IoT(Internet of Things)接続を安全に確立するための基本である。

端末トラフィックがデバイスを通過するとき、デバイスは次のタスクを実行します。

- 端末のベンダーやモデルなどの端末情報を解析して抽出します。
- 端末情報(カメラベンダーなど)が変更されたときにログを生成します。

Terminal

端末の特性を識別するために、デバイス特性ライブラリに端末を事前定義できます。

ターミナル ID を有効にするには、**Objects** > **APPSecurity** > **Terminal Identification** > **Terminals** を選択し、**Enable terminal identification logging** をクリックします。

Terminal group

同様の特性を共有する端末を端末グループに追加できます。デバイスは、同じ端末グループのパケットに対して同じ DPI サービスを提供できます。

端子を端子グループに追加するには **Objects** > **APPSecurity** > **Terminal Identification** > **Terminal Groups** を選択し、**Create** をクリックして、使用可能な端子をこの端子グループに追加します。

Object group for terminal identification

正確な端末アドレス識別のためにオブジェクトグループを設定できます。デバイスは、次のアドレスオブジェクトグループをサポートします。

- **Terminal address object group**: 端末 IP アドレスのセット。パケットの送信元または宛先 IP アドレスがこのグループと一致する場合、送信元または宛先 IP アドレスは端末 IP アドレスになります。
- **Manager address object group**: 端末マネージャ IP アドレスのセット。パケットの送信元または宛先 IP アドレスがこのグループと一致する場合、宛先または送信元 IP アドレスは端末 IP アドレスになります。

オブジェクトグループを設定するには、**Objects** > **APP Security** > **Terminal**

Identification > **Terminals** を選択し、**Configure object groups for terminal identification** をクリックします。マネージャアドレスオブジェクトグループまたは端末アドレスオブジェクトグループ、あるいはその両方を設定します。両方を設定した場合、マネージャアドレスオブジェクトグループが優先されます。

Security action

Introduction

セキュリティーアクションモジュールは、IPS やアンチウィルスなどの DPI サービスモジュールのアクションパラメーターを提供できます。次のアクションパラメータープロファイルを使用できます。

- **Block**: DPI サービスモジュールでのブロックソースアクションのブロック期間を定義します。ブロックソースアクションは、ブラックリスト機能がイネーブルになった後にのみ有効になります。ブラックリスト機能がイネーブルになっている場合、デバイスは一致するパケットをドロップし、パケットの送信元 IP アドレスを IP ブラックリストに追加します。送信元 IP アドレスからの後続のパケットは、ブロック期間中に直接ドロップされます。

  ブラックリスト機能の詳細については、攻撃防御のオンラインヘルプを参照してください。

- **Redirect**: DPI サービスモジュールのリダイレクトアクション用にパケットがリダイレクトされる URL を定義します。

- **Capture**: キャッシュ可能な最大バイト数やキャッシュされたパケットがエクスポートされる URL など、DPI サービスモジュールのキャプチャアクションのパラメーターを定義します。

  デバイスはキャプチャされたパケットをローカルにキャッシュし、毎日のエクスポート時またはキャッシュされたバイト数が制限に達したときに、指定された URL にキャッシュされたパケットをエクスポートします。エクスポート後、デバイスはローカルキャッシュをクリアし、新しいパケットのキャプチャを開始します。URL を指定しない場合、または指定された URL に到達できない場合、デバイスはキャッシュされたキャプチャパケットを引き続きエクスポートしますが、エクスポートは失敗し、ローカルキャッシュがクリアされます。

- **Alarm**: クライアントに表示されるアンチウィルスアラームメッセージを定義します。**Create** をクリックしてアラームメッセージテンプレートを作成し、テンプレートの右側にある **Edit** をクリックして、必要なアラームメッセージをインポートします。1 つのアラームメッセージテンプレートでは、TXT または HTML ファイルをインポートすることによってアラームメッセージを定義できます。この機能のサポートは、デバイスモデルによって異なります。

Intelligences from the threat management platform

Introduction

このデバイスは、IP レピュテーションや MD5 レピュテーションなど、脅威管理プラットフォームからのインテリジェンスの受信をサポートします。インテリジェンスは、ローカルにロードされたレピュテーションとアンチウィルスシグニチャライブラリを補完し、内部ネットワークユーザーのセキュリティーを向上させます。

Restrictions and guidelines

- 脅威管理プラットフォームからインテリジェンスを確実に受信できるようにするには、デバイスの CLI から **netconf soap http enable** および **netconf soap https enable** コマンドを実行して、デバイスで NETCONF over SOAP をイネーブルにします。
- 脅威インテリジェンスを正しく使用するには、まずデバイスで IP レピュテーションとアンチウィルス機能を設定します。

ACL

このヘルプには、次のトピックが含まれています。

- Introduction
  - ACL types
  - Match order
  - Rule numbering
- Restrictions and guidelines

Introduction

Access Control List(ACL)は、送信元 IP アドレス、宛先 IP アドレス、ポート番号などの基準に基づいてトラフィックを識別するための一連のルールです。このルールは、permit ステートメントまたは deny ステートメントとも呼ばれます。デバイスは、設定されたポリシーに従って識別されたトラフィックを処理しました。

ACL types

表 1 ACL タイプ

種類	IP バージョン	一致基準
Basic ACLs	IPv4	送信元 IPv4 アドレス。
	IPv6	送信元 IPv6 アドレス。
Advanced ACLs	IPv4	送信元 IPv4 アドレス、宛先 IPv4 アドレス、パケットプライオリティ、プロトコル番号、およびその他のレイヤー3 およびレイヤー4 ヘッダーフィールド。
	IPv6	送信元 IPv6 アドレス、宛先 IPv6 アドレス、パケットプライオリティ、プロトコル番号、およびその他のレイヤー3 およびレイヤー4 ヘッダーフィールド。
Layer 2 ACLs	IPv4 および IPv6	送信元および宛先 MAC アドレス、802.1p プライオリティ、リンク層プロトコルタイプなどのレイヤー2 ヘッダーフィールド。
User-defined ACLs	IPv4 および IPv6	プロトコルヘッダーでユーザーが指定したマッチングパターン。

Match order

ACL 内のルールは特定の順序でソートされます。パケットがルールに一致すると、デバイスは一致プロセスを停止し、ルールに定義されたアクションを実行します。ACL に重複または矛盾するルールが含まれている場合、一致結果と実行するアクションはルールの順序によって異なります。

次の ACL 一致順序を使用できます。

- **config**: ACL ルールをルール ID の昇順にソートします。ID が小さいルールは、ID が大きいルールより前に照合されます。この方法を使用する場合は、ルールとその順序を注意深く確認してください。
- **auto**: ACL ルールを深さ優先順序でソートします。深さ優先順序では、ルールのサブセットが常にルールの前に一致するようにします。表 2 に、深さ優先順序で ACL のタイプごとにルールをソートするために使用されるタイブレーカーの順序をリストします。

表 2 深さ優先順序での ACL ルールのソート

ACL タイプ	タイブレーカーのシーケンス
IPv4 basic ACL	1. VPN インスタンス。 2. 送信元 IPv4 アドレスワイルドカードに 0 が多い(0 が多いほど IPv4 アドレス範囲が狭いことを意味します)。 3. 以前に設定された規則。
IPv4 advanced ACL	1. VPN インスタンス。 2. 特定のプロトコル番号。 3. 送信元 IPv4 アドレスワイルドカードマスクに 0 を追加します。 4. 宛先 IPv4 アドレスワイルドカードに 0 を追加します。 5. より狭い TCP/UDP サービスポート番号範囲。 6. 以前に設定された規則。
IPv6 basic ACL	1. VPN インスタンス。 2. 送信元 IPv6 アドレスの長いプレフィクス(長いプレフィクスは狭い IPv6 アドレス範囲を意味します)。 3. 以前に設定された規則。
IPv6 advanced ACL	1. VPN インスタンス。 2. 特定のプロトコル番号。 3. 送信元 IPv6 アドレスの長いプレフィクス。 4. 宛先 IPv6 アドレスの長いプレフィクス。 5. より狭い TCP/UDP サービスポート番号範囲。 6. 以前に設定された規則。
Layer 2 ACL	1. 送信元 MAC アドレスマスクの 1 が多い(1 が多いほど MAC アドレスが小さいことを意味します)。 2. 宛先 MAC アドレスマスクにさらに 1 があります。

	3. 以前に設定された規則。

Rule numbering

作成するルールに ID を割り当てない場合、自動的にルール ID が割り当てられます。ルール番号付けステップでは、ルールに自動的に番号を付ける増分が設定されます。たとえば、ACL ルール番号付けステップが 5 で、作成するルールに ID を割り当てない場合、自動的に 0、5、10、15 などの番号が付けられます。番号付けステップの幅が広いほど、2 つのルール間に挿入できるルールの数が多くなります。
連続した規則番号付けではなく規則間にギャップを導入することにより、ACL に規則を挿入する柔軟性が得られます。この機能は、ACL 規則が規則 ID の昇順で照合される設定順 ACL で重要です。
ACL ルールに自動的に割り当てられた ID は、現在最も高いルール ID に最も近い番号ステップの倍数(0 から開始)を取ります。
たとえば、ステップが 5 で、0、5、9、10、12 という番号の 5 つのルールがある場合、新しく定義されたルールの番号は 15 になります。ACL にルールが含まれていない場合、最初のルールの番号は 0 になります。
ステップが変更されるたびに、ルールの番号は 0 から順に変更されます。たとえば、ステップを 5 から 2 に変更すると、ルール 5、10、13 および 15 の番号がルール 0、2、4 および 6 に変更されます。

Restrictions and guidelines

- ACL ページまたは ACL を使用する機能のページで ACL を作成できます。ただし、ACL の管理(ACL の変更または削除など)は ACL ページでのみ実行できます。
- ACL を削除または変更すると、その ACL を使用する機能に影響する場合があります。
- ACL のマッチの順番が config の場合、ACL 内の任意のルールを変更できます。ACL のマッチの順番が auto の場合、ACL 内の任意のルールを変更できません。

SSL

Introduction

Secure Sockets Layer(SSL)は、HTTP などの TCP ベースのアプリケーション層プロトコルに通信セキュリティーを提供する暗号プロトコルです。SSL は、e-ビジネスやオンラインバンキングなどのアプリケーションで広く使用され、インターネット上で安全なデータ伝送を提供しています。
SSL は、次のセキュリティーサービスを提供します。

- **Privacy**: SSL は、対称暗号化アルゴリズムを使用してデータを暗号化します。RSA の非対称キーアルゴリズムを使用して、対称暗号化アルゴリズムで使用されるキーを暗号化します。

- **Authentication**: SSL では、証明書ベースのデジタル署名を使用して SSL サーバーおよびクライアントを認証します。SSL サーバーおよびクライアントは、PKI を介してデジタル証明書を取得します。

- **Integrity**: SSL はメッセージ認証コード(MAC)を使用してメッセージの完全性を確認します。

Restrictions and guidelines

- SSL プロトコルバージョンには、SSL 2.0、SSL 3.0、TSL 1.0(または SSL 3.1)、TLS 1.1、TLS 1.2、TLS 1.3、および GM-TLS1.1 があります。デバイスは SSL サーバーとして、SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3、または GM-TLS1.1 を実行しているクライアントと通信できます。サーバーはクライアントから SSL 2.0 Client Hello メッセージを受信すると、通信に新しいバージョンの SSL を使用するようにクライアントに通知します。

- SSL サーバーポリシーは、PKI ドメインおよびサポートされている暗号スイートなど、SSL サーバーによって使用される一連の SSL パラメーターを定義します。SSL サーバーポリシーは、HTTPS などのアプリケーションに関連付けられた後にのみ有効になります。

- SSL クライアントポリシーでは、PKI ドメインや優先暗号スイートなど、SSL クライアントで使用される一連の SSL パラメーターを定義します。SSL クライアントは、クライアントポリシーの設定を使用してサーバーへの接続を確立します。SSL クライアントポリシーは、DDNS などのアプリケーションに関連付けられた後にのみ有効になります。

- SSL サーバーまたはクライアントポリシーの設定が変更された場合は、その SSL サーバーまたはクライアントポリシーを使用するサービスを再度イネーブルにして、新しい設定を適用する必要があります。

- **Advanced Settings** で SSL プロトコルバージョンを変更する場合は、デフォルトの SSL ポリシーを使用するサービスを再度有効にして、新しい SSL プロトコルバージョンを適用する必要があります。

Public key management

このヘルプには、次のトピックがあります。

- はじめに
  - 非対称キーアルゴリズムの概要
  - ローカル非対称キーペアの管理
  - ピアホスト公開キーの管理
- Restrictions and guidelines

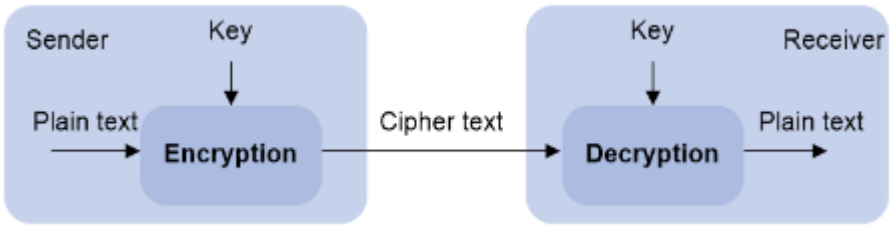
Introduction

公開キー管理機能は、非対称キーアルゴリズムのキーを管理およびアドバタイズするために使用されます。

Asymmetric key algorithm overview

非対称鍵アルゴリズムは、図 1 に示すように、2 者間の通信を保護するためにセキュリティアプリケーションによって使用されます。非対称鍵アルゴリズムでは、暗号化と復号化に 2 つの個別の鍵(1 つは公開鍵、1 つは秘密鍵)が使用されます。対称鍵アルゴリズムでは、1 つの鍵のみが使用されます。

図 1 暗号化と復号化



鍵の所有者は、公開鍵をプレーンテキストでネットワーク上に配布できますが、秘密鍵は秘密にしておく必要があります。攻撃者がアルゴリズムと公開鍵を知っていても、秘密鍵を計算することは数学的に不可能です。

非対称キーアルゴリズムには、Revest-Shamir-Adleman Algorithm(RSA)、Digital Signature Algorithm(DSA)、Elliptic Curve Digital Signature Algorithm(ECDSA)、および SM2 があります。

セキュリティアプリケーション(SSH、SSL、PKI など)は、暗号化/復号化およびデジタル署名に非対称キーアルゴリズムを使用します。

Managing local asymmetric key pairs

Creating a local key pair

ローカルデバイスでは、RSA、DSA、ECDSA、および SM2 キーペアを作成できます。

Importing a local key pair

ローカルデバイスでは、キーペアファイルからローカルキーペアをインポートできます。インポートされたキーペアが暗号化されている場合は、キーペアを正常にインポートするためにキーペアパスワードを入力する必要があります。

Displaying or exporting a host public key

デバイスでは、ローカルホストの公開キーを表示またはエクスポートできます。

- ホスト公開鍵を表示します。キーがローカルデバイスに表示された後、キーを記録します。たとえば、フォーマットされていないファイルにコピーします。ピアデバイスでは、文字通りキーを入力する必要があります。
- ホスト公開鍵を指定した形式でファイルにエクスポートします。ファイルをピアデバイスに転送します。ピアデバイスで、ファイルから鍵をインポートします。

  ホスト公開キーをファイルにエクスポートする場合、指定したファイル名にセミコロン(;)またはカンマ(,)を含めることはできません。
- ホスト公開キーを指定された形式でモニター画面にエクスポートし、ファイルに保存します。ファイルをピアデバイスに転送します。ピアデバイスで、ファイルからキーをインポートします。

Destroying a local key pair

セキュリティーを確保するために、次のいずれかの状況では、ローカルキーペアを破棄して新しいキーペアを生成します。

- ローカルキーが漏洩しました。侵入イベントが発生する可能性があります。
- デバイスのストレージメディアに障害が発生したか、ストレージメディアが交換されたために、デバイスには復号化/暗号化およびデジタル署名用の対応する秘密キーがありません。
- ローカル証明書の有効期限が切れています。

Managing peer host public key

ピアデバイスに送信される情報を暗号化したり、ピアデバイスのデジタル署名を認証したりするには、ローカルデバイスにピアデバイスの公開キーを設定する必要があります。ローカルデバイスでは、ピアデバ

イスのホスト公開キーをインポート、表示、および削除できます。

次の方法を使用して、ピアホスト公開キーを設定できます。

- 公開キーファイルからピアホスト公開キーをインポートします(推奨)。

  最初に、FTP または TFTP を使用してピアデバイスから公開キーファイルを取得する必要があります。キーをインポートすると、ローカルデバイスはインポートされた公開キーを Public Key Cryptography Standards(PKCS;公開キー暗号規格)形式の文字列に自動的に変換します。
- ピアホスト公開キーを手動で入力(入力またはコピー)します。

  最初にピアデバイスの公開キーを表示し、キーを記録する必要があります。ローカルデバイスでは、キーを手動で入力またはコピーします。

Restrictions and guidelines

ピアホスト公開キーを設定する場合は、次の制約事項および注意事項に従ってください。

- ピアホスト公開鍵を手動で入力する場合は、入力した鍵が正しい形式であることを確認してください。ピアホスト公開鍵を正しい形式で取得するには、「ホスト公開鍵の表示またはエクスポート」の説明に従って、ピアデバイスで公開鍵を表示します。他の方法で表示される公開鍵の形式は、正しくない場合があります。鍵が正しい形式でない場合、システムは鍵を破棄し、エラーメッセージを表示します。
- デバイスが記録されたピアホスト公開キーの形式をサポートしているかどうかわからない場合は、ピアホスト公開キーを入力するのではなく、必ずインポートしてください。
- SM2 キーペアの公開キーはインポートできません。

PKI

このヘルプには、次のトピックがあります。

- はじめに
  - デジタル証明書と証明書失効リスト
  - PKI アーキテクチャ
  - PKI アプリケーション
  - 証明書の管理
  - 証明書アクセス制御ポリシー
- Restrictions and guidelines

Introduction

Public Key Infrastructure(PKI;公開キーインフラストラクチャ)は、ネットワークサービスを保護するためにデータを暗号化および復号化する非対称キーインフラストラクチャです。
PKI は、デジタル証明書を使用して公開鍵を配布および使用し、ネットワーク通信および電子商取引に、ユーザー認証、データ機密性、データ整合性などのセキュリティーサービスを提供します。
デバイスの PKI システムは、IPsec および SSL の証明書管理を提供します。

Digital certificate and certificate revocation list

Digital certificate

デジタル証明書は、Certificate Authority(CA;認証局)によって署名された電子ドキュメントです。デジタル証明書は、公開キーid をバインドします。
デジタル証明書には、次の情報が含まれています。

- 発行者名(証明書を発行した CA の名前)。
- 証明書のサブジェクト(証明書が発行される個人またはグループの名前)。
- サブジェクトの ID 情報。
- サブジェクトの公開キー。
- CA の署名。
- 有効期間。

このヘルプでは、次の種類の証明書について説明します。

- **CA certificate**: CA の証明書。PKI システム内の複数の CA は、ルート CA を先頭とする CA ツリーを形成します。ルート CA は自己署名証明書を生成し、下位レベルの各 CA は、そのすぐ上にある CA

によって発行された CA 証明書を保持します。これらの証明書のチェーンは、信頼のチェーンを形成します。

- **Local certificate**: CA がローカル PKI エンティティに対して発行するデジタル証明書。エンティティの公開鍵が含まれています。

Certificate revocation list

証明書失効リスト(CRL)は、失効した証明書のシリアル番号のリストです。CRL は、証明書を最初に発行した CA によって作成され、署名されます。
CA は、証明書を失効させるために CRL を定期的に発行します。失効された証明書は信頼できません。
CA は、次のいずれかの条件が発生した場合に証明書を失効させる必要があります。

- 証明書のサブジェクト情報が変更されます。
- 秘密鍵が侵害される。
- 証明書のサブジェクトと CA 間の関連付けが変更されます。たとえば、従業員が組織での雇用を終了した場合などです。

デバイスでは、CRL の自動更新をイネーブルにし、CRL 更新間隔を設定できます。デバイスは、指定された間隔で CRL リポジトリから CRL を自動的に取得します。

PKI archtecture

PKI システムは、証明書サブジェクト、CA、RA、および証明書/CRL リポジトリで構成されます。

Certificate subject

証明書のサブジェクトは、PKI 証明書を使用するエンドユーザーです。証明書の申請者は、オペレータ、組織、デバイス、またはコンピュータ上で実行されているプロセスです。
証明書申請者は、証明書サブジェクトを使用して、ID 情報を CA に提供します。有効な証明書サブジェクトには、次の 1 つ以上の ID カテゴリが含まれている必要があります。

- 証明書のサブジェクト名。これには、共通名、国コード、州または県の名前、地域、組織名および組織単位名が含まれます。証明書のサブジェクト名を構成する場合は、共通名が必要です。
- 証明書申請者の FQDN。ネットワーク内の PKI エンティティを識別します。
- 証明書申請者の IP アドレス。

CA

証明機関(CA)は、証明書を発行し、証明書の有効期間を定義し、CRL を公開することによって証明書を取り消します。

RA

登録局(RA)は、証明書の登録要求を処理して CA の負荷を軽減します。RA は証明書要求を受け入れ、ユーザーID を確認し、CA に証明書の発行を要求するかどうかを決定します。
RA は、PKI システムにおいて任意である。CA を直接ネットワークアクセスにさらすことに関してセキュリティー上の懸念がある場合、一部のタスクを RA に委任することが望ましい。そうすれば、CA は、証明書および CRL への署名という主要なタスクに集中することができる。

Certificate/CRL repository

証明書/CRL リポジトリは、証明書および CRL を格納し、証明書および CRL を証明書申請者に配布する証明書配布ポイントです。また、問合せ機能も提供します。PKI リポジトリは、LDAP または HTTP プロトコルを使用するディレクトリーサーバーである場合があります。LDAP は、一般的に使用されるプロトコルです。

PKI applications

PKI 技術は、オンライントランザクションのセキュリティー要件を満たすことができます。PKI は、インフラストラクチャとして幅広いアプリケーションがあります。次に、アプリケーションの例を示します。

VPN

VPN は、パブリック通信インフラストラクチャ上に構築されたプライベートデータ通信ネットワークです。VPN では、機密性を確保するために、PKI ベースの暗号化およびデジタル署名テクノロジーとともに、ネットワーク層セキュリティプロトコル(IPsec など)を使用できます。

Secure emails

PKI は、機密性、整合性、認証、および否認防止に関する電子メール要件に対応できます。一般的な安全な電子メールプロトコルは Secure/Multipurpose Internet Mail Extensions(S/MIME)です。これは PKI に基づいており、署名付きの暗号化されたメールの転送を可能にします。

Web security

PKI を SSL ハンドシェイクフェーズで使用すると、デジタル証明書によって通信相手の ID を確認できます。

Certificate management

デバイスは、PKIドメインに基づいて証明書を管理し、IPsec や SSL などのアプリケーションに対して PKI ドメインベースの証明書サービスを提供します。PKI ドメインには、証明書要求のキーペアや証明書使用拡張など、証明書サブジェクトの登録情報が含まれます。

Importing certificates

PKIドメインに関連する CA 証明書およびローカル証明書を CA からインポートできます。
この方法は、CRL リポジトリが指定されていない場合、CA サーバーが SCEP をサポートしていない場合、または CA サーバーが証明書のキーペアを生成する場合に使用します。
証明書を PKIドメインにインポートする前に、次の作業を実行します。

- FTP または TFTP を使用して、証明書ファイルをデバイスのストレージメディアにアップロードします。
- ローカル証明書をインポートするには、CA 証明書チェーンが PKIドメイン内に存在するか、インポートする証明書に含まれている必要があります。CA 証明書チェーンが使用できない場合は、ローカル証明書をインポートする前に CA 証明書チェーンをインポートします。

ローカル証明書をインポートする場合は、次の制約事項および注意事項に従ってください。

- ローカル証明書に CA 証明書チェーンが含まれている場合は、CA 証明書とローカル証明書を同時にインポートできます。
- ローカル証明書に CA 証明書チェーンが含まれていないが、CA 証明書がすでに PKIドメインに存在する場合は、証明書を直接インポートできます。
- インポートする証明書ファイルにルート証明書が含まれている場合は、インポート前にルート証明書のフィンガープリントを確認するプロンプトが表示されます。CA 管理者に連絡して、正しいルート証明書のフィンガープリントを取得してください。
- インポートするローカル証明書にキーペアが含まれている場合は、秘密キーの暗号化に使用するチャレンジパスワードの入力を求められます。CA 管理者に問い合せて、チャレンジパスワードを取得してください。
- キーペアを含むローカル証明書ファイルをインポートすると、デバイスは次のようにキーペアを PKIドメインに保存します。
  - PKIドメインに、証明書ファイル内のキーペアと一致するキーペアがすでに含まれている場合は、既存のキーペアを上書きするかどうかを確認するプロンプトが表示されます。
  - PKIドメインにキーペアがない場合、デバイスは、キーアルゴリズムと証明書ファイル内のキーペアの目的に従ってキーペアを作成します。PKIドメイン名がキーペア名として使用されます。
  - PKIドメインに証明書ファイル内のキーペアとは異なるキーペアが含まれている場合は、別の名前を指定してキーペアを証明書ファイルに保存する必要があります。

次のいずれかの条件が満たされる場合は、CA 証明書を PKIドメインにインポートできます。

- インポートされる CA 証明書は、ルート CA 証明書であるか、ルート証明書を含む証明書チェーンを含んでいます。

- CA 証明書には、ルート証明書のない証明書チェーンが含まれていますが、デバイス上の既存の CA 証明書で完全な証明書チェーンを形成できます。

Exporting certificates

CA 証明書および PKI ドメイン内のローカル証明書を証明書ファイルにエクスポートできます。エクスポートされた証明書ファイルは、デバイスまたは他の PKI アプリケーションにインポートして戻すことができます。

Requesting certificates

PKI ドメイン内の証明書サブジェクトのローカル証明書を要求する前に、CA 証明書が PKI ドメイン内にすでに存在することを確認してください。CA 証明書は、取得したローカル証明書の有効性を確認するために使用されます。

PKI ドメイン内の証明書サブジェクトの証明書を要求するには、次の作業を実行します。

1. 証明書のサブジェクトを設定します。
2. PKI ドメイン内の証明書サブジェクトを使用します。PKI ドメインで、証明書要求のキーペアなどの証明書登録設定を構成します。

   キーペアの公開キーは、証明書要求内の他の情報とともに CA に送信されます。CA は要求に署名し、要求された証明書を生成します。

   PKI ドメイン内に存在しないキーペアを指定すると、証明書要求の生成時に、キーペア設定に従ってキーペアが自動的に生成されます。
3. PKI ドメイン内の証明書サブジェクトに対する証明書要求を生成します。
4. 電話や電子メールなどのアウトオブバンド方式を使用して、証明書要求を CA に送信します。

Certificate access control policy

証明書アクセスコントロールポリシーを使用すると、認証されたクライアントの証明書の属性に基づいて、デバイス(HTTPS サーバーなど)へのアクセスを許可できます。

証明書アクセス制御ポリシーは、許可規則または拒否規則のセットです。各規則には、証明書属性フィルタのセットが含まれています。証明書属性フィルタは、証明書の発行者名、サブジェクト名、または代替サブジェクト名フィールドの属性に基づいて証明書をフィルタリングします。証明書は、規則内のすべての証明書属性フィルタと一致する場合に、その規則と一致します。

デバイスは、受信した証明書を証明書アクセスポリシーの規則リストにある規則と上から下に照合します。一致する規則が見つかると、照合プロセスは停止します。

- 証明書が許可規則と一致する場合、証明書は検証に合格します。

- 証明書が拒否規則に一致する場合、またはポリシー内のどの規則にも一致しない場合、その証明書は無効と見なされます。
- セキュリティアプリケーション(HTTPS など)に指定された証明書アクセスコントロールポリシーが存在しない場合は、アプリケーション内のすべての証明書が検証に合格します。

Restrictions and guidelines

- アイデンティティ・カテゴリが必須かオプションかは、CA ポリシーによって異なります。CA ポリシーに従って、証明書のサブジェクト設定を構成します。
- Windows 2000 サーバー上の SCEP アドオンでは、認証要求のデータ長に制限があります。PKI エンティティからの要求がデータ長の制限を超えた場合、認証サーバーは認証要求に応答しません。この場合、アウトオブバンド手段を使用して要求を送信できます。RSA サーバーや OpenCA サーバーなどの他のタイプの認証サーバーには、このような制限はありません。

Trusted access controllers

このヘルプには、次のトピックがあります。

- Introduction
- Configure a trusted access controller

Introduction

デバイスは、受信したユーザー要求を信頼できるアクセスコントローラに転送して ID 認証を行い、認証を受けたユーザーが要求されたリソースへのアクセスを許可されているかどうかを確認できます。

Configure a trusted access controller

1. **Objects** タブをクリックします。
2. ナビゲーションペインで、**Trusted Access Controller** を選択します。
3. **Create** をクリックします。
4. 信頼できるアクセスコントローラのパラメーターを設定します。

表 1 Trusted Access Controller の構成項目

項目	説明
Name	信頼できるアクセスコントローラの名前を入力します。大文字と小文字は区別されません。
Local service URL	信頼できるアクセスコントローラとのコラボレーションに使用されるローカルサービス URL を入力します。信頼できるアクセスコントローラは、ローカルサービス URL を使用して、ユーザーオフラインおよびユーザー権限変更イベントをデバイスに通知できます。ローカルサービス URL は、**protocol type://server IP address:port number**.の形式である必要があります。 • プロトコルタイプは HTTP または HTTPS です。 • サーバーの IP アドレスは、現在のソフトウェアバージョンでは IPv4 アドレスである必要があります。 デバイスでは、異なる信頼できるアクセスコントローラに対して同じサーバー IP アドレスとポート番号を持つローカルサービス URL を設定できません。信頼できるアクセスコントローラのローカル URL とピアサービス URL の両方に同じサーバーIP アドレスとポート番号を指定することはできません。

Peer service URL	外部認証サービスを提供するピア URL を入力します。デバイスは、ピアサービス URL を使用して、信頼できるアクセスコントローラへの登録およびユーザー権限の認可を実行できます。ピアサービス URL は、**protocol type://server IP address:port number** の形式である必要があります。 • プロトコルタイプは HTTP または HTTPS です。 • サーバーの IP アドレスは、現在のソフトウェアバージョンでは IPv4 アドレスである必要があります。 デバイスでは、異なる信頼できるアクセスコントローラに対して同じサーバー IP アドレスとポート番号を持つピアサービス URL を設定できません。 信頼できるアクセスコントローラのローカル URL とピアサービス URL の両方に同じサーバーIP アドレスとポート番号を指定することはできません。
SSL client policy	信頼できるアクセスコントローラがデバイス(SSL クライアント)と交換するトラフィックを暗号化するために使用する SSL クライアントポリシーを指定します。 既存の SSL クライアントポリシーを選択することも、新しい SSL クライアントポリシーを作成することもできます。
SSL server policy	デバイス(SSL サーバー)と交換されるトラフィックを暗号化するために暗号化するために使用する SSL サーバーポリシーを指定します。 既存の SSL サーバーポリシーを選択することも、新しい SSL サーバーポリシーを作成することもできます。
Authentication service function	認証サービスを有効または無効にします。

5. **OK** をクリックします。

トラステッドアクセスコントローラーは、トラステッドアクセスコントローラーのページに表示されます。

VRF

Introduction

Virtual Routing and Forwarding(VRF)は、VPN のルート分離、データ非依存、およびデータセキュリティを実装します。

VRF には次のコンポーネントがあります。

- 個別の Label Forwarding Information Base(LFIB)。
- IP ルーティングテーブル。
- VRF にバインドされたインターフェース。
- Route Distinguisher(RD)を含む VRF 管理情報。

同じサイト ID を持つが異なる VPN に存在するサイトを区別するために、サイト ID の前に RD が追加されます。RD とサイト ID は、VPN サイトを一意に識別します。

RD は、次のいずれかの形式の 3～21 文字の文字列です。

- 16 ビット AS 番号:32 ビットのユーザー定義番号(101:3 など)。
- 32 ビット IP アドレス:16 ビットのユーザー定義番号。たとえば、192.168.122.15:1。
- 32 ビット AS 番号:16 ビットのユーザー定義番号。AS 番号の最小値は 65536 です(例:65536:1)。

VRF をマルチキャストまたはルーティングプロトコルの複数のインスタンスにバインドして、サービス分離を実装できます。たとえば、デバイスが複数の OSPF インスタンスをサポートしている場合、VRF を各 OSPF プロセスにバインドできます。これにより、OSPF プロセスによって学習されたルートが、バインドされた VRF のルーティングテーブルに追加されます。

Interface

このヘルプには、次のトピックがあります。

- Introduction
  - IPv4 address
  - IPv6 address
  - Link aggregation
  - VLAN termination
- Restrictions and guidelines

Introduction

デバイスは、次のタイプのイーサネットインターフェイスをサポートしています。

- **Layer 2 Ethernet interface**: データリンクスイッチングするためにデータリンク層(レイヤー2)で動作する物理イーサネットインターフェイス。
- **Layer 3 Ethernet interface**: パケットをルーティングするためにネットワーク層(レイヤー3)で動作する物理イーサネットインターフェイス。レイヤー3 イーサネットインターフェイスに IP アドレスを割り当てることができます。
- **Layer-configurable Ethernet interface**: レイヤー2 イーサネットインターフェイスとしてブリッジモードで動作するように、またはレイヤー3 イーサネットインターフェイスとしてルートモードで動作するように設定できる物理イーサネットインターフェイス。
- **Layer 3 Ethernet subinterface**: ネットワーク層で動作する論理インターフェイス。レイヤー3 イーサネットサブインターフェイスに IP アドレスを割り当てることができます。レイヤー3 イーサネットインターフェイスが複数の VLAN のパケットを転送できるようにするには、レイヤー3 イーサネットインターフェイス上にレイヤー3 サブインターフェイスを作成する必要があります。
- **Layer 2 aggregate interface**: レイヤー2 集約グループに一意に対応する論理インターフェイス。このタイプのインターフェイスは、レイヤー2 リンク集約の実装に使用されます。
- **Layer 3 aggregate interface**: レイヤー3 集約グループに一意に対応する論理インターフェイス。このタイプのインターフェイスには IP アドレスを割り当てることができ、レイヤー3 リンク集約の実装に使用されます。
- **Layer 3 aggregate subinterface**: IP アドレスを割り当てることができる論理インターフェイス。このタイプのインターフェイスは、レイヤー3 集約インターフェイスが VLAN タグ付きパケットを送受信できるようにするために使用されます。

- **Loopback interface**: IP アドレスを割り当てることができる論理インターフェイス。ループバックインターフェイスが作成されると、ループバックインターフェイスが手動でシャットダウンされない限り、ループバックインターフェイスの物理層の状態は常に up になります。
- **VLAN interface**: 論理インターフェイス。各 VLAN は 1 つの VLAN インターフェイスに対応します。IP アドレスが VLAN インターフェイスに割り当てられると、その IP アドレスは VLAN 内のネットワークデバイスのゲートウェイアドレスとして使用でき、VLAN インターフェイスはレイヤー3 の別の IP サブネット宛てのパケットを転送できます。VLAN インターフェイスの詳細については、「VLAN」を参照してください。
- **SSL VPN interface**: IP アドレスを割り当てることができる論理インタフェース。ユーザーが IP アクセス方式を使用して SSL VPN ゲートウェイにアクセスすると、ゲートウェイはこのインタフェースを使用してクライアントと通信します。SSL VPN インタフェースの詳細は、「SSL VPN」を参照してください。
- **Reth interface**: IP アドレスを割り当てることができる論理インタフェース。Reth インタフェースは、リンクの可用性を確保するために 2 つのメンバー・インタフェースを使用します。Reth インタフェースの詳細は、「ホットバックアップ」を参照してください。
- **Reth subinterface**: IP アドレスを割り当てることができる論理インターフェイス。このタイプのインターフェイスは、Reth インターフェイスがレイヤー2 VLAN タグ付きパケットを送受信できるようにするために使用されます。Reth サブインターフェイスの詳細については、「ホットバックアップ」を参照してください。

IPv4 address

IP address representation and classes

IP アドレッシングでは、32 ビットアドレスを使用して IPv4 ネットワーク上の各ホストを識別します。アドレスを読みやすくするために、アドレスはドット付き 10 進表記で記述されます。各アドレスの長さは 4 オクテットです。たとえば、バイナリのアドレス 00001010000000010000000100000001 は 10.1.1.1 と記述されます。

各 IP アドレスは、次のセクションに分かれています。

Net ID: ネットワークを識別します。ネット ID の最初の数ビットはクラスフィールドまたはクラスビットと呼ばれ、IP アドレスのクラスを識別します。

Host ID: ネットワーク上のホストを識別します。

IP アドレスは、表 1 に示すように、5 つのクラスに分けられます。最初の 3 つのクラスが最も一般的に使用されます。

表 1:IP アドレスのクラスと範囲

クラス	アドレス範囲	備考

A	0.0.0.0 から 127.255.255.255	IP アドレス 0.0.0.0 は、起動時に一時的な通信のためにホストによって使用されます。このアドレスは有効な宛先アドレスではありません。 127 で始まるアドレスは、ループバックテスト用に予約されています。これらのアドレス宛てのパケットは、リンクに送信されるのではなく、入力パケットとしてローカルで処理されます。
B	128.0.0.0 から 191.255.255.255	該当なし
C	192.0.0.0 から 223.255.255.255	該当なし
D	224.0.0.0 から 239.255.255.255	マルチキャストアドレス。
E	240.0.0.0 から 255.255.255.255	ブロードキャストアドレス 255.255.255.255 を除き、将来の使用のために予約されています。

Subnetting and masking

サブネット化では、ホスト ID の一部のビットを使用してサブネット ID を作成することにより、ネットワークをサブネットと呼ばれる小さなネットワークに分割します。
マスキングは、ホスト ID と、ネット ID とサブネット ID の組み合わせとの境界を識別します。
各サブネットマスクは、IP アドレスのビットに対応する 32 ビットで構成されます。サブネットマスクでは、連続する 1 はネット ID とサブネット ID を表し、連続するゼロはホスト ID を表します。
クラス A、B、および C ネットワークは、サブネット化される前に、次のデフォルトマスク(ナチュラルマスクとも呼ばれます)を使用します。それぞれ 255.0.0.0、255.255.0.0、および 255.255.255.0 です。
サブネット化により、ホストに割り当てることができないアドレスの数が増加します。したがって、サブネットを使用することは、より少ないホストに対応することを意味します。
たとえば、サブネット化されていないクラス B ネットワークは、512 のサブネットにサブネット化された同じネットワークよりも 1022 多くのホストを収容できます。

Without subnetting: 65534(2^{16} – 2)ホスト(2 つの除外されたアドレスは、すべて 1 のホスト ID を持つブロードキャストアドレスと、すべて 0 のホスト ID を持つネットワークアドレスです)。

With subnetting: 最初の 9 ビットをサブネット化に使用すると、512(29)個のサブネットが提供されます。ただし、ホスト ID に使用できるのは 7 ビットのみです。これにより、各サブネットで 126(27-2)個のホスト、合計 64512(512×126)個のホストが許可されます。

IP address assignment

インターフェイスに IP アドレスを手動で割り当てることも、DHCP または PPPoE を使用して IP アドレスを

取得するようにインターフェイスを設定することもできます。DHCP および PPPoE のサポートは、デバイスモデルによって異なります。

Interface MTU

パケットが送信インターフェイスの MTU を超えると、デバイスは次のいずれかの方法でパケットを処理します。

- パケットがフラグメンテーションを許可しない場合、デバイスはパケットを廃棄します。
- パケットのフラグメンテーションが許可されている場合、デバイスはパケットをフラグメント化し、フラグメントを転送します。

フラグメンテーションと再構成はシステムリソースを消費するため、フラグメンテーションを回避するためにネットワーク環境に基づいて MTU を設定します。

Last hop holding

この機能がイネーブルになっているインターフェイスは、転送トラフィックの最初のパケットを受信すると、トラフィック特性と最終ホップを高速キャッシュに記録します。逆方向トラフィックが転送のためにデバイスに到達すると、デバイスは記録された最終ホップ情報に基づいてパケット転送をガイドできます。この機能により、ピアエンドからローカルエンドへの転送トラフィックと、ローカルエンドからピアエンドへの逆方向トラフィックが同じパス上で転送されます。したがって、同じセッションのトラフィックを同じ方法で処理できます。

IPv6 address

IPv6 は(IPng)とも呼ばれる IPv6 は、IPv4 の後継として IETF によって設計されました。IPv6 と IPv4 の大きな違いの 1 つは、IPv6 では IP アドレスのサイズが 32 ビットから 128 ビットに増加することです。

IPv6 address format

IPv6 アドレスは、コロン(:)で区切られた 16 ビットの 16 進数のセットとして表されます。IPv6 アドレスは 8 つのグループに分割され、各 16 ビットグループは 4 つの 16 進数で表されます。たとえば、2001:0000:130F:0000:0000:09C0:876A:130B のようになります。
IPv6 アドレスの表記を簡略化するために、次の方法を使用して IPv6 アドレスのゼロを処理できます。

- 各グループの先頭のゼロは削除できます。たとえば、上記のアドレスは、2001:0:130F:0:0:9C0:876A:130B のように短い形式で表すことができます。

- IPv6 アドレスに 1 つ以上の連続したゼロのグループが含まれている場合は、二重コロン(::)で置き換えることができます。たとえば、上記のアドレスは、2001:0:130F::9C0:876A:130B のような最短の形式で表すことができます。

IPv6 アドレスは、アドレスプレフィクスとインターフェイス ID で構成されます。これらは、IPv4 アドレスのネットワーク ID とホスト ID に相当します。
IPv6 アドレスプレフィクスは、IPv6 アドレス/プレフィクス長表記で記述されます。プレフィクス長は、アドレスプレフィクス内の IPv6 アドレスの左端のビット数を示す 10 進数です。

IPv6 address type

IPv6 アドレスには次の種類があります。

Unicast address: 単一インターフェイスの ID。IPv4 ユニキャストアドレスに似ています。ユニキャストアドレスに送信されたパケットは、そのアドレスで識別されたインターフェイスに配信されます。
Multicast address: IPv4 マルチキャストアドレスに類似した、一連のインターフェイス(通常は異なるノードに属する)の識別子。マルチキャストアドレスに送信されたパケットは、そのアドレスで識別されるすべてのインターフェイスに配信されます。IPv6 では、ブロードキャストアドレスはマルチキャストアドレスに置き換えられます。
Anycast address: 一連のインターフェイス(通常は異なるノードに属する)の識別子。エニーキャストアドレスに送信されたパケットは、そのアドレスで識別されたインターフェイスの中で最も近いインターフェイスに配信されます。最も近いインターフェイスは、ルーティングプロトコルの距離の測定に従って選択されます。
IPv6 アドレスのタイプは、フォーマットプレフィックスと呼ばれる最初の数ビットで指定されます。

表 2 アドレス・タイプとフォーマット・プレフィックスのマッピング

タイプ		フォーマット接頭辞(バイナリ)	IPv6 プレフィクス ID	説明
Unicast address	Unspecified address	00.0(128 ビット)	::/128	どのノードにも割り当てることはできません。有効な IPv6 アドレスを取得する前に、ノードはこのアドレスを IPv6 パケットの送信元アドレスフィールドに入力します。指定されていないアドレスは宛先 IPv6 アドレスとして使用できません。
	Loopback address	00.1(128 ビット)	::1/128	これは IPv4 のループバックアドレスと同じ機能を持ちます。どの物理インタフェースにも割り当てることができませ

タイプ		フォーマット接頭辞(バイナリ)	IPv6 プレフィクス ID	説明
				ん。ノードはこのアドレスを使用して IPv6 パケットをそれ自身に送信します。
	Link-local address	1111111010	FE80::/10	近隣探索とステートレス自動設定のためのリンクローカルノード間の通信に使用されます。リンクローカルな送信元アドレスまたは宛先アドレスを持つパケットは、他のリンクに転送されません。
	Global unicast address	その他の形態	該当なし	グローバルユニキャストアドレスは、パブリック IPv4 アドレスと同じように、インターネットサービスプロバイダに提供されます。このタイプのアドレスを使用すると、プレフィクスの集約によってグローバルルーティングエントリの数を制限できます。
Multicast address			FF00::/8	該当なし
Anycast address				該当なし

IEEE EUI-64 address-based interface identifiers

インターフェイス ID は 64 ビット長で、リンク上のインターフェイスを一意に識別します。

IEEE 802 インターフェイス(VLAN インターフェイスなど)では、インターフェイス ID はインターフェイスのリンクレイヤードレス(通常は MAC アドレス)から取得されます。MAC アドレスは 48 ビット長です。

EUI-64 アドレスベースのインターフェイス ID を取得する手順は、次のとおりです。

1. MAC アドレスの上位 24 ビット目の後ろに、16 ビットの 2 進数 1111111111111110(FFFE の 16 進数)を挿入します。
2. ユニバーサル/ローカル(U/L)ビット(上位 7 ビット)を反転します。この操作により、インターフェイス ID が MAC アドレスと同じローカルまたはグローバルな意味を持つようになります。

トンネルインターフェイスでは、EUI-64 アドレスベースのインターフェイス ID の下位 32 ビットがトンネルインターフェイスの送信元 IPv4 アドレスです。

ISATAP トンネルインターフェイスの EUI-64 アドレスベースのインターフェイス ID の上位 32 ビットは 0000:5EFE ですが、他のトンネルインターフェイスの ID はすべてゼロです。
別のタイプのインターフェイス(シリアルインターフェイスなど)では、EUI-64 アドレスベースのインターフェイス ID がデバイスによってランダムに生成されます。

Configure an IPv6 global unicast address for an interface

インターフェイスの IPv6 グローバルユニキャストアドレスを設定するには、次のいずれかの方法を使用します。

EUI-64 IPv6 address: インターフェイスの IPv6 アドレスプレフィクスは手動で設定され、インターフェイス ID はインターフェイスによって自動的に生成されます。

Manual configuration: IPv6 グローバルユニキャストアドレスは手動で設定されます。

Stateless address autoconfiguration: IPv6 グローバルユニキャストアドレスは、RA メッセージに含まれているアドレスプレフィクス情報に基づいて自動的に生成されます。

Stateful address autoconfiguration: IPv6 グローバルユニキャストアドレスは、DHCPv6 を介して取得されます。

1 つのインターフェイスに複数の IPv6 グローバルユニキャストアドレスを設定できます。

Configure an IPv6 link-local address for an interface

次のいずれかの方法を使用して、IPv6 リンクローカルアドレスを設定します。

Automatic generation: デバイスは、リンクローカルアドレスプレフィクス(FE80::/10)およびインターフェイスのリンクレイヤードレスに従って、インターフェイスのリンクローカルアドレスを自動的に生成します。

Manual assignment: インターフェイスの IPv6 リンクローカルアドレスを手動で設定します。

インタフェースは 1 つのリンクローカルアドレスのみを持つことができます。リンク・ローカル・アドレスの競合を回避するには、自動生成方式を使用することをお薦めします。自動生成方式と手動割当て方式の両方を使用する場合は、手動割当てが優先されます。

- 最初に自動生成を使用してから手動割り当てを使用すると、手動で割り当てられたリンクローカルアドレスによって、自動生成されたリンクローカルアドレスが上書きされます。
- 最初に手動割当を使用してから自動生成を使用すると、次の両方が発生します。
  - リンクローカルアドレスは、依然として手動で割り当てられたものです。
  - 自動的に生成されたリンクローカルアドレスは有効になりません。手動で割り当てられたアドレスを削除すると、自動的に生成されたリンクローカルアドレスが有効になります。

Last hop holding

この機能がイネーブルになっているインターフェイスは、転送トラフィックの最初の IP パケットを受信する

と、トラフィック特性と最終ホップを高速キャッシュに記録します。逆方向トラフィックが転送のためにデバイスに到達すると、デバイスは記録された最終ホップ情報に基づいてパケット転送をガイドできます。この機能により、ピアエンドからローカルエンドへの転送トラフィックとローカルエンドからピアエンドへの逆方向トラフィックが同じパス上で転送されます。したがって、同じセッションのトラフィックを同じ方法で処理できます。

Link aggregation

イーサネットリンク集約は、複数の物理イーサネットリンクを 1 つの論理リンク(集約リンクと呼ばれます)にバンドルします。リンク集約には次の利点があります。

単一の個別リンクの制限を超える帯域幅の増加。集約リンクでは、トラフィックはメンバーポート間で分散されます。

リンクの信頼性が向上しました。メンバーポートは相互に動的にバックアップします。メンバーポートに障害が発生すると、そのトラフィックは自動的に他のメンバーポートに切り替えられます。

Aggregation groups

各リンク集約は、論理集約インタフェースによって表されます。各集約インタフェースには、自動的に作成された集約グループがあります。この集約グループには、集約に使用されるメンバー・ポートが含まれています。集約グループのタイプと数は、集約インタフェースと同じです。

集約インタフェースは、次のいずれかのタイプになります。

Layer 2: レイヤー2 集約グループ内のメンバーポートは、レイヤー2 イーサネットインターフェイスだけです。

Layer 3: レイヤー3 集約グループのメンバーポートは、レイヤー3 イーサネットインターフェイスだけにできます。

集約インターフェイスのポートレートは、その Selected メンバポートの合計レートに等しくなります。デュプレックスモードは、Selected メンバポートと同じです。

Aggregation states of member ports in an aggregation group

集約グループ内のメンバーポートは、次の集約状態のいずれかになります。

Selected: 選択したポートはトラフィックを転送できます。

Unselected: 非選択ポートはトラフィックを転送できません。

Operational k

ポートを集約する場合、システムはポートレートやデュプレックスモードなどのポート情報に基づいて、各ポートに動作キーを自動的に割り当てます。この情報を変更すると、動作キーの再計算がトリガーされま

す。
集約グループでは、すべての Selected ポートが同じ操作キーを持ちます。

Attribute configuration

選択済ポートになるには、メンバー・ポートの属性構成が集約インタフェースと同じである必要があります。
表 3 に、属性構成を示します。

表 3 属性の構成

機能	属性設定
Port isolation	隔離グループ内のポートのメンバシップ。 隔離グループ番号。
VLAN	VLAN アトリビュート設定: • 許可 VLAN ID。 • PVID。 VLAN タギングモード。

Link aggregation modes

集約グループは、次のいずれかのモードで動作します。
スタティック:スタティックモードの集約グループは、スタティック集約グループと呼ばれます。
動的-動的モードの集約グループは、動的集約グループと呼ばれます。動的集約は、IEEE 802.3 ad Link Aggregation Control Protocol(LACP)を実装します。

How static link aggregation works

1. 参照ポートの選択プロセス

集約グループ内のポートの集約状態を設定する場合、システムは自動的にメンバー・ポートを参照ポートとして選択します。選択されたポートは、参照ポートと同じ操作キーおよび属性構成を持つ必要があります。
集約インターフェイスと同じアトリビュート設定を持つすべてのアップメンバーポートは、候補参照ポートです。
システムは、次のタイブレークに基づいて、候補参照ポートの中から降順で参照ポートを選択します。

a 最も高いポートプライオリティ。
b 全二重および高速。
c 全二重および低速。
d 半二重および高速。
e 半二重および低速。

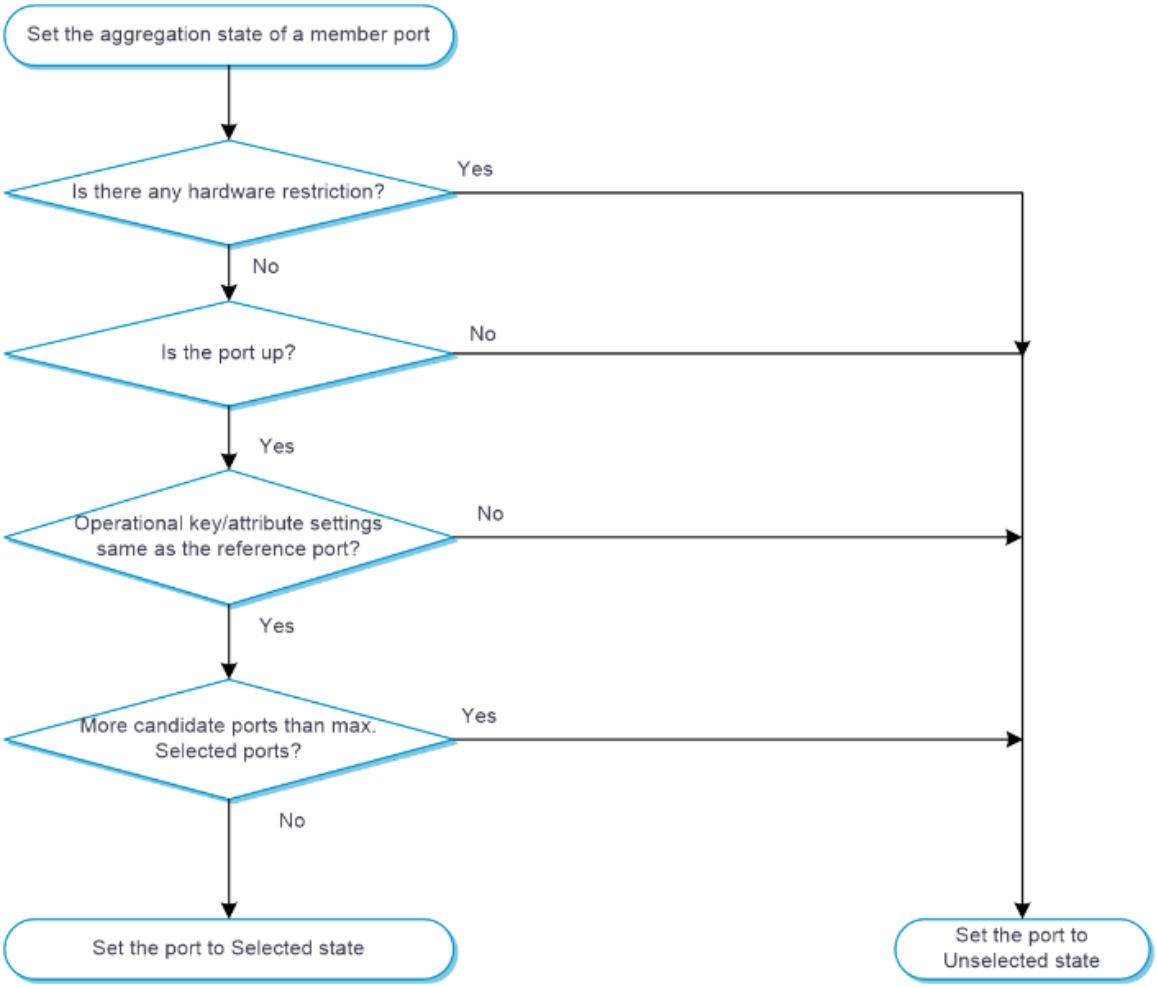
f　以前選択されていたポート。

g　最も小さい番号のポート。

2. 各メンバーポートの集約状態の設定

基準ポートが選択されると、システムはスタティック集約グループ内の各メンバーポートの集約状態を設定します。

図 1 スタティック集約グループ内のメンバーポートの集約状態の設定



How dynamic link aggregation works

動的集約は、IEEE 802.3 ad Link Aggregation Control Protocol(LACP)の実装です。

LACP は、LACPDU を使用して、LACP システム間で集約情報を交換します。動的集約グループ内の各メンバーポートは、そのピアと集約情報を交換し、受信した情報を他のメンバーポートで受信した情報と比較します。交換された集約情報に基づいて、2 つのシステムは、どのポートが選択状態になるかについて合意に達します。

1. リファレンスポートの選択

システムは、アップ状態のメンバーポートから基準ポートを選択します。選択されたポートには、基準ポートと同じ動作キーおよび属性設定が必要です。

ローカルシステム(アクター)とピアシステム(パートナー)は、次のワークフローを使用して参照ポートをネゴシエートします。

a 2 つのシステムは、システム ID が小さい方のシステムを決定します。

システム ID には、LACP システムプライオリティとシステム MAC アドレスが含まれています。

- 2 つのシステムは、それぞれの LACP プライオリティ値を比較します。

  LACP プライオリティが低いほど、システム ID は小さくなります。LACP プライオリティ値が同じ場合、2 つのシステムは次の手順に進みます。

- 2 つのシステムは、それぞれの MAC アドレスを比較します。

  MAC アドレスが小さいほど、システム ID は小さくなります。

b システム ID が小さいシステムは、最小のポート ID を持つポートを参照ポートとして選択します。

ポート ID には、ポートプライオリティとポート番号が含まれます。ポートプライオリティが低いほど、ポート ID は小さくなります。

- プライオリティ値が最も低いポートが参照ポートとして選択されます。

  ポートのプライオリティが同じ場合、システムは次の手順に進みます。

- システムはポート番号を比較します。

  ポート番号が小さいほど、ポート ID も小さくなります。

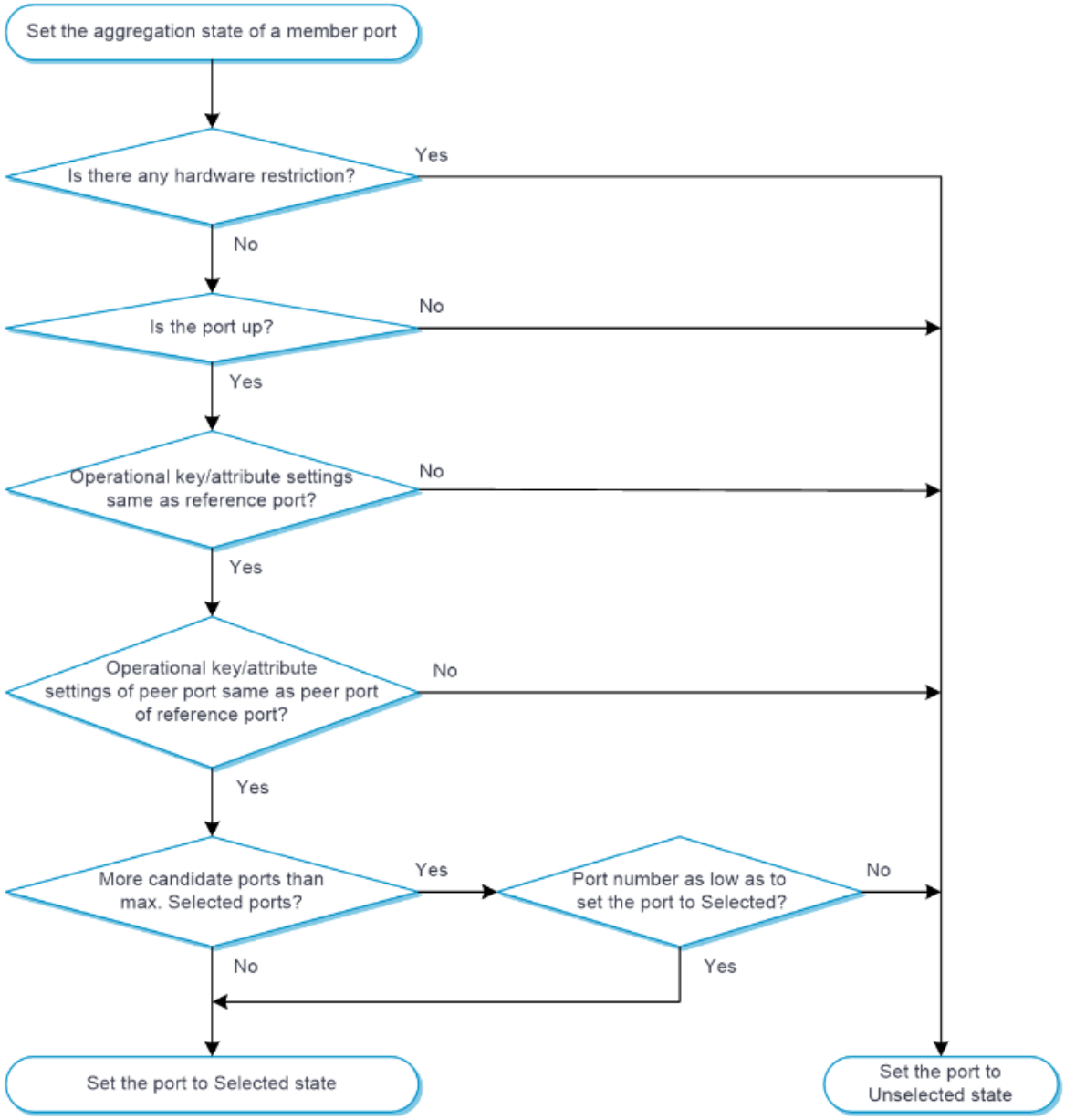
  最小のポート番号を持ち、集約インターフェイスと同じアトリビュート設定を持つポートが、参照ポートとして選択されます。

2. 各メンバーポートの集約状態の設定

a 参照ポートが決定されると、システム ID が小さい方のシステムが、その側の各メンバーポートの状態を設定します。

b システム ID が大きいシステムは、ピアシステムでの集約状態の変化を検出します。次に、ローカルメンバーポートの集約状態をピアポートと同じに設定します。

図 2 動的集約グループ内のメンバーポートの状態の設定



A comparison of static link aggregation and dynamic link aggregation

スタティックリンク集約モードとダイナミックリンク集約モードの違いは次のとおりです。

Static: スタティックな集約は安定しています。ピアシステムはメンバーポートの集約状態をネゴシエートしません。ピアポートの集約状態が変更されても、メンバーポートの集約状態は自動的には変更されません。

Dynamic: ローカルシステムとピアシステムは、メンバポートの集約状態を自動的にネゴシエートし、維持します。

VLAN termination

About VLAN termination

VLAN 終端は通常、VLAN タグを含むパケットを処理します。VLAN 終端対応インターフェイスは、VLAN タグ付きパケットを受信すると、次のタスクを実行します。

- VLAN タグに従ってパケットをインターフェイスに割り当てます。
- パケットの VLAN タグを削除します。
- パケットをレイヤー3 フォワーディングまたは他の処理パイプラインに配信します。

VLAN 終端対応インターフェイスは、パケットを送信する前に、VLAN 終端タイプに基づいて、パケットに新しい VLAN タグを追加するかどうかを決定します。

VLAN termination types

VLAN 終端タイプ	インタフェース上で終端されるパケットのタイプ	インターフェイス上の発信パケットのタグ
Dot1q termination	パケットは、次の両方の要件を満たす必要があります。 • パケットには、1 つまたは複数のレイヤーの VLAN タグが含まれています。 • 最も外側の VLAN ID は、設定された値と一致します。	単一タグ
Untagged termination	タグなしパケット。	タグなし
Default termination	同じメインインターフェイスの他のサブインターフェイスで処理できないパケット。	タグなし

VLAN termination mechanism

レイヤー3 イーサネットサブインターフェイスやレイヤー3 集約サブインターフェイスなどの VLAN インターフェイスおよびサブインターフェイスは、次のパケットを終端できます。

- 最も外側の VLAN ID が設定値と一致するパケット。
- VLAN ID の最も外側の 2 つのレイヤーが設定値と一致するパケット。

VLAN インターフェイスは、最も外側の VLAN ID が VLAN インターフェイス番号と同じパケットだけを終端します。たとえば、VLAN-interface 10 は、最も外側の VLAN タグ 10 を持つパケットだけを終端します。メインインターフェイスは、VLAN タグ付きパケットを終端しません(たとえば、レイヤー3 イーサネットインターフェイスまたはレイヤー3 集約インターフェイス)。VLAN タグ付きパケットを終端するには、メインインタ

ーフェイスのサブインターフェイスを作成します。
同じメインインターフェイスのサブインターフェイスは、異なるタイプの VLAN 終端を使用できます。受信したパケットを処理するために、システムは次の VLAN 終端タイプに基づいて、優先順位の高いサブインターフェイスを選択します。

- Dot1q 終端または Dot1q 終端のサポート(デフォルト)。
- タグなし終端。
- デフォルトの終了。

これらの VLAN 終端タイプのいずれも適用されない場合、メインインターフェイスがパケットを処理します。
インターフェイスのサブインターフェイスでデフォルトの終端がイネーブルになっている場合、パケットはメインインターフェイスではなくサブインターフェイスによって処理されます。
メインインターフェイスが VLAN インターフェイスにバインドされている場合、メインインターフェイスは、VLAN インターフェイスの VLAN 終端設定に従って VLAN タグ付きパケットを処理します。

Restrictions and guidelines

- インターフェイスがシャットダウンされると、そのインターフェイスに接続されているネットワーク上で、デバイスを通過する必要があるすべてのサービスが中断されます。
- 集約リンクの両端で同じ集約モードを設定する必要があります。
- スタティック集約を成功させるには、各リンクの両端のポートが同じ集約状態であることを確認します。
- レイヤー2 集約インターフェイスを削除すると、そのレイヤー2 集約グループも削除されます。同時に、集約グループのメンバーポート(存在する場合)も集約グループから削除されます。
- リンク集約の場合、アトリビュート設定は集約インターフェイス上でだけ設定可能であり、すべてのメンバーポートに自動的に同期されます。集約インターフェイスから同期された設定は、集約インターフェイスが削除された後もメンバーポート上で保持されます。
- インターフェイスが Reth インターフェイスのメンバーであるか、冗長グループノード上にある場合、そのインターフェイスをレイヤー3 集約グループに割り当てることはできません。
- ダイナミックリンク集約の両端のポートが正しい集約グループに割り当てられていることを確認します。両端は、各メンバーポートの集約状態を自動的にネゴシエートできます。

Interface pairs

このヘルプには、次のトピックがあります。

- Introduction
  - Forwarding of tunneled packets
  - VLAN ID check
  - Security service bypass
- Restrictions and guidelines

Introduction

インターフェースペアは、データリンク層でトラフィックを監視します。これは通常、セキュリティデバイスで使用されます。デバイスに到達したレイヤー2 トラフィックは、セキュリティデバイスにリダイレクトされ、フィルタリングされてから、宛先に転送されます。
次の転送モードがサポートされています。

- **Reflect-type forwarding**: パケットの受信ポートを介してパケットを転送します。
- **Blackhole-type forwarding**: 受信したパケットをドロップします。
- **Forward-type forwarding**: パケットの受信ポートとは異なるポートを経由してパケットを転送します。

Forwarding of tunneled packets

デフォルトでは、トンネルパケットはトンネルヘッダーに基づいて転送されます。
元のパケットヘッダーに基づいてトンネルパケットを転送するようにデバイスを設定できます。

VLAN ID check

この機能を使用すると、インライン転送中にセッションエントリと一致する各パケットの VLAN ID をデバイスでチェックできます。

- VLAN ID チェックがイネーブルの場合、デバイスは、VLAN ID が一致するセッションエントリの VLAN ID と同じである場合にだけパケットを許可します。

- VLAN ID チェックがディセーブルの場合、デバイスはセッションエントリと一致するパケットを許可します。

ホットバックアップシステムでは、プライマリおよびセカンダリデバイス上のトラフィック着信インターフェースが異なる VLAN に属する場合、VLAN ID チェックをディセーブルにする必要があります。VLAN ID チェックをイネーブルにすると、プライマリ/セカンダリデバイスのスイッチオーバーが発生した後、または非対称パストラフィックが存在する場合に、トラフィックがセッションエントリと正しく一致しなくなります。

Security service bypass

デフォルトでは、パケットは最初にセキュリティサービスによって処理されてから、設定されたブリッジ転送モードに従って転送されます。
セキュリティサービスバイパス機能を使用すると、ユーザートラフィックはセキュリティデバイスのセキュリティサービス処理をバイパスして、設定されたブリッジ転送モードに従って直接転送されます。
セキュリティサービスバイパスは、内部バイパスと外部バイパスに分類できます。

- **Internal bypass**: ユーザートラフィックはセキュリティデバイスに送信されますが、セキュリティデバイスによって処理されません。セキュリティデバイスは、設定されたブリッジ転送モードに従って、トラフィックを直接転送またはドロップします。
- **External bypass**: ユーザートラフィックは、セキュリティデバイスを通過せずに、Power Free Connector(PFC)デバイスによって直接転送されます。

Internal bypass

ユーザートラフィックはセキュリティデバイスに送信されますが、セキュリティデバイスによって処理されません。セキュリティデバイスは、設定されたブリッジ転送モードに従って、トラフィックを直接転送またはドロップします。
内部バイパスは、リフレクトタイプ、ブラックホールタイプ、またはフォワードタイプのフォワーディングモードで動作するインターフェースペアで使用できます。

External bypass

ユーザートラフィックは、セキュリティデバイスを通過せずに、Power Free Connector(PFC)デバイスによって直接転送されます。
内部バイパスは、forward-type forwarding モードを使用するインターフェースペアだけで使用できます。
外部バイパスはさらに次のタイプに分類できます。

Static external bypass: 外部バイパスは、設定するとすぐに有効になるため、手動で無効にする必要があります。

Dynamic external bypass: 外部バイパスは、セキュリティデバイスと PFC 間のリンクのステータスに基づいて自動的にイネーブルまたはディセーブルになります。セキュリティデバイスはリンクステータスを定期的にポーリングし、一方または両方のリンクがダウンした場合に外部バイパスをイネーブルにします。外部バイパスは、障害が発生したリンクがアップした場合に自動的にディセーブルになります。

Restrictions and guidelines

- リフレクトタイプ、ブラックホールタイプ、またはフォワードタイプのフォワーディングモードで動作するインターフェースペアに追加できるのは、レイヤー2 またはレイヤー3 イーサネットインターフェース、またはレイヤー2 集約インターフェースだけです。
- ハードウェアバイパスサブカードの挿入時に自動的に作成されるフォワードタイプのインターフェースペアでは、インターフェースペアの内部バイパスだけをイネーブルにできます。
- 外部バイパス機能のサポートは、デバイスモデルによって異なります。

Interface collaboration

Introduction

インターフェースコラボレーション機能は、デバイス上のさまざまなインターフェースをコラボレーショングループに割り当て、これらのインターフェースの状態を関連付けます。コラボレーショングループ内のすべてのメンバーインターフェースは、同時にパケットを送信することも送信しないこともできます。

How it works

インターフェースコラボレーション機能は、次のように動作します。

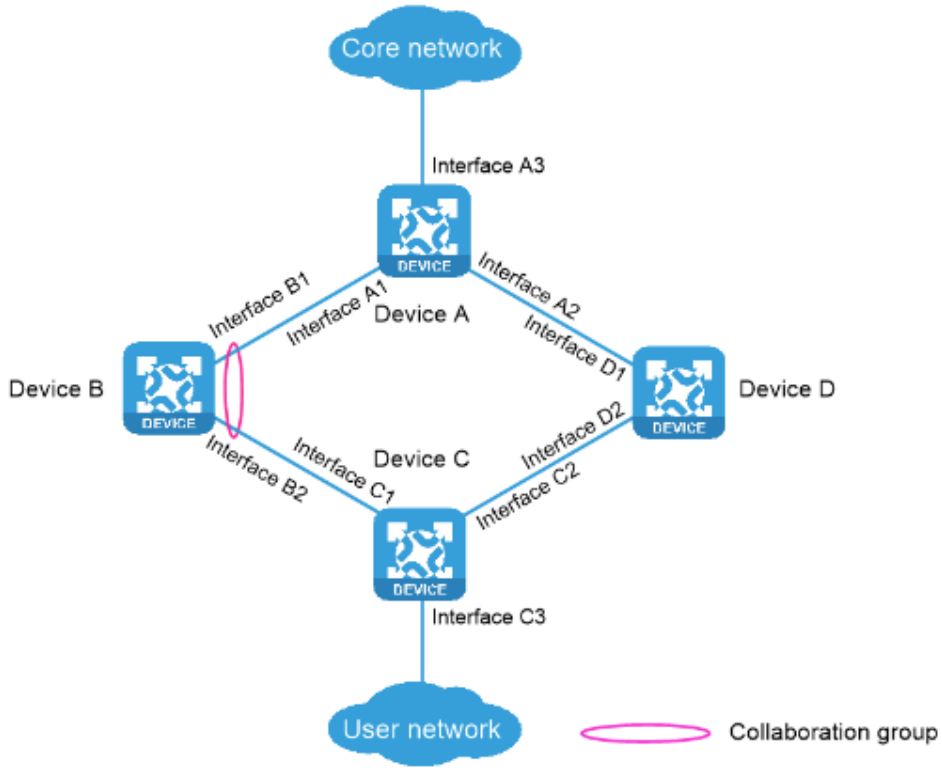
- コラボレーショングループ内のいずれかのメンバーインターフェースがダウンすると、デバイスはコラボレーショングループ内の他のすべてのメンバーインターフェースを **Collaboration-down** 状態に設定します。コラボレーショングループの状態はダウンであり、コラボレーショングループ内のどのメンバーインターフェースもパケットを送信できません。
- **DOWN** 状態または **Collaboration-down** 状態のメンバーインターフェースが起動すると、デバイスはコラボレーショングループ内の他のすべてのメンバーインターフェースを起動しようとします。
  - 他のすべてのメンバーインターフェースが 10 秒以内に起動すると、コラボレーショングループが起動します。コラボレーショングループ内のすべてのメンバーインターフェースはパケットを送信できます。
  - いずれかのメンバーインターフェースが 10 秒以内にアップ状態にならない場合、デバイスはそのメンバーインターフェースを **DOWN** 状態に設定し、他のすべてのメンバーインターフェースを **Collaboration-down** 状態に設定します。コラボレーショングループはダウン状態のままであり、コラボレーショングループ内のメンバーインターフェースはパケットを送信できません。

Typical networking

図 1 に示すように、LAN ユーザーはデバイス B を介してインターネットにアクセスします。インターフェース B1 がダウンすると、トラフィックはデバイス B からデバイス C に切り替えられます。インターフェース B2 がまだアップ状態であり、ルートの更新が遅いため、スイッチオーバーは遅くなります。

2 つのインターフェースが 1 つのコラボレーショングループに属している場合、高速トラフィックスイッチオーバーを実現するためにインターフェース B1 がダウンすると、デバイス B はインターフェース B2 をダウンさせます。同様に、インターフェース B2 がダウンすると、デバイスはインターフェース B1 をダウンさせます。

図 1 ネットワーク図



Restrictions and guidelines

- コラボレーショングループは、モニターリンクがグローバルに有効になっている場合にのみ有効になります。
- インターフェースは、1 つのコラボレーショングループにのみ属することができます。
- デバイスが複数のインターフェースを介してピアデバイスに接続されている場合は、これらのすべてのインターフェースを同じ集約グループに割り当てないでください。これらのすべてのインターフェースを同じ集約グループに割り当てると、これらのインターフェースのいずれかがダウンしたときに、接続されているすべてのピアインターフェースがダウンします。
- コラボレーショングループが正しく機能するためには、そのメンバーインターフェースを集約グループまたは冗長グループに割り当てないでください。
- 1 つのコラボレーショングループに割り当てることができるリンクのインターフェースは 1 つだけです。

4G

このヘルプには、次のトピックがあります。

- Introduction
- Restrictions and guidelines
  - Restrictions for using the 4G feature
  - Restrictions and guidelines for using a USB 4G modem
- Configure 4G

Introduction

4G 機能を使用すると、デバイスから 4G ネットワークにアクセスできます。
このデバイスは、固定セルラーインターフェースを使用して 4G 機能を管理します。セルラーインターフェースは、Eth チャネルインターフェースにチャネル化できます。Eth チャネルインターフェースのデータリンク層プロトコルはイーサネットです。ネットワーク層で IP をサポートします。Eth チャネルインターフェースは、DHCP を介して IP アドレスを取得します。

Restrictions and guidelines

Restrictions for using the 4G feature

デバイスの 4G モデムは、LTE ネットワークへのアクセスのみを提供します。

Restrictions and guidelines for using a USB 4G modem

USB 4G モデムのサポートは、デバイスのモデルによって異なります。USB 4G モデムを使用する場合は、次の Restrictions and guidelines に従ってください。

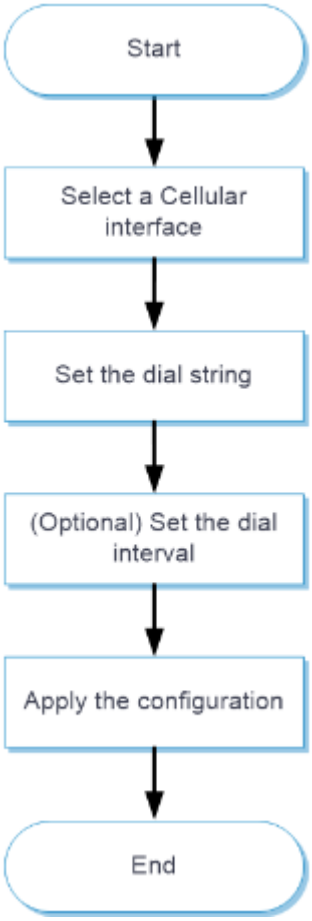
- 4G 機能を設定する前に、デバイスに USB 4G モデムをインストールします。
- データの送信中は USB 4G モデムを取り外さないでください。USB 4G モデムを取り外す前に、**shutdown** コマンドを実行して USB 4G モデムをシャットダウンすることをお勧めします。
- USB 4G モデムは、接続されている USB インターフェースがシャットダウンされている場合は使用できません。
- USB 4G モデムはホットスワップ可能です。

USB 4G モデムを取り外しても、セルラーインターフェースビューの設定はそのまま残ります。

Configure 4G

図 1 に示すように、4G を設定します。

図 1 4G 構成手順



手順

1. **Network** > **Interface Configuration** > **4G** を選択します。
2. セルラーインターフェースを選択します。
   デバイスは Eth-channel インターフェース 0 を作成し、そのインターフェースをダイヤラグループ 1 に関連付けて、すべての IPv4 パケットを許可します。Eth-channel インターフェースは DHCP を介して IP アドレスを取得します。Eth-channel インターフェースでは、従来の DDR がデフォルトでイネーブルになっています。
3. コールを発信するためのダイヤル文字列を設定します。ダイヤラ番号を設定すると、デバイスはピアデバイスに自動的にダイヤルします。

4. DDR が次の通話を試行する間隔を設定します。DDR は、接続が確立されるまで、指定された間隔で番号を自動的にダイヤルします。
5. **Apply** をクリックします。
6. 設定をクリアして Eth チャネルインターフェースを削除するには、**Clear** をクリックします。

Security zones

Introduction

セキュリティーゾーンは、同じセキュリティー要件を持つインターフェースの集合です。セキュリティーゾーンを構成して、セキュリティーゾーンベースのセキュリティー管理を実装できます。

Security zone members

セキュリティーゾーンには、次の種類のメンバーを含めることができます。

・レイヤー2 インターフェースと VLAN の組み合わせ

・レイヤー3 インターフェース:

- レイヤー3 イーサネットインターフェース
- レイヤー3 サブインターフェースなどのレイヤー3 論理インターフェース

Security zone-based packet processing rules

次の表は、セキュリティーゾーンベースのセキュリティー管理が設定されている場合にデバイスがパケットを処理する方法を示しています。

パケット	アクション
セキュリティーゾーンにあるインターフェースとセキュリティーゾーンにないインターフェース間のパケット	破棄。
同じセキュリティーゾーンにある 2 つのインターフェース間のパケット	デフォルトでは破棄されます。
異なるセキュリティーゾーンに属する 2 つのインターフェース間のパケット	一致するセキュリティー制御ポリシーに応じて、転送または破棄します。ポリシーが適用されていない場合、またはポリシーが存在しないか有効でない場合、パケットは破棄されます。
どのセキュリティーゾーンにもない 2 つのインターフェース間のパケット	破棄。
デバイス自体から発信されたパケット、またはデバイス自体宛てのパケット	一致するオブジェクトポリシーに応じて、転送または廃棄します。デフォルトでは、これらのパケットは廃棄されます。

Restrictions and guidelines

デバイス管理インターフェースは **Management** セキュリティーゾーンに属します。管理インターフェースからデバイスの Web インターフェースにログインして、デバイスをリモートで管理できます。**Management** セキュリティーゾーンから管理インターフェースを削除すると、Web アクセスはすぐに終了します。

レイヤー3 インターフェースは、1 つのセキュリティーゾーンだけに追加できます。

レイヤー2 インターフェースと VLAN の組み合わせは、1 つのセキュリティーゾーンだけに追加できます。

パケットが特定のセキュリティーゾーン間のどのゾーンペアとも一致しない場合、デバイスは any-to-any ゾーンペアを検索します。

ゾーンペアが存在する場合、デバイスは、ゾーンペアに適用されたセキュリティーポリシーを使用してパケットを処理します。

ゾーンペアが存在しない場合、デバイスはパケットを廃棄します。

デフォルトでは、デバイスは **Management** ゾーンと **Local** ゾーンの間でパケットを転送します。

Management セキュリティーゾーンと **Local** セキュリティーゾーン間のパケットでは、デバイスは 2 つのセキュリティーゾーンのゾーンペアに適用されたセキュリテーィ制御ポリシーだけを使用します。

VLAN

Introduction

仮想ローカルエリアネットワーク(VLAN)テクノロジーは、物理 LAN を複数の論理 LAN に分割します。次のようなメリットがあります。

Security: 同じ VLAN 内のホストはレイヤー2 で相互に通信できますが、レイヤー2 では他の VLAN 内のホストから隔離されます。

Broadcast traffic isolation: VLAN は、ブロードキャストパケットの送信を制限するブロードキャストドメインです。

Flexibility: VLAN はワークグループ単位で論理的に分割できます。同じワークグループ内のホストは、物理的な場所に関係なく、同じ VLAN に割り当てることができます。

Port-based VLANs

ポートベース VLAN は、ポートごとに VLAN メンバーをグループ化します。ポートは、VLAN に割り当てられた後にのみ、VLAN からパケットを転送します。

VLAN では、ポートをタグなしポートリストに追加してタグなしポートにしたり、タグ付きポートリストに追加してタグ付きポートにしたりできます。VLAN のタグなしポートはタグなしパケットを送信し、VLAN のタグ付きポートはタグ付きパケットを送信します。

ポートのリンクタイプをアクセス、トランク、またはハイブリッドに設定できます。リンクタイプでは、次の VLAN タグ処理方式が使用されます。

Access: アクセスポートは、1 つの VLAN からのパケットだけを転送し、これらのパケットをタグなしで送信できます。アクセスポートをタグなしポートリストに追加できる VLAN は 1 つだけです。

Trunk: トランクポートは、複数の VLAN からのパケットを転送できます。port VLAN ID(PVID)からのパケットを除き、トランクポートから送信されるパケットは VLAN タグ付きです。トランクポートの PVID では、ポートはタグなしポートリストにだけ追加できます。他の VLAN では、ポートはタグ付きポートリストにだけ追加できます。

Hybrid: ハイブリッドポートは、複数の VLAN からのパケットを転送できます。ハイブリッドポートによって転送されるパケットのタグ付けステータスは、ポート設定によって異なります。異なる VLAN では、ハイブリッドポートは、設定要件に応じて、タグなしポートリストまたはタグ付きポートリストに追加できます。

VLAN interfaces

異なる VLAN のホストは、VLAN インターフェースを使用してレイヤー3 で通信します。VLAN インターフェースは、デバイス上に物理エンティティとして存在しない仮想インターフェースです。VLAN ごとに、1 つの VLAN インターフェースを作成し、それに IP アドレスを割り当てることができます。VLAN インターフェースは、レイヤー3 の別の IP サブネット宛てのパケットを転送するための VLAN のゲートウェイとして機能します。

Restrictions and guidelines

システムのデフォルト VLAN として、VLAN 1 は作成または削除できません。

MAC

このヘルプには、次のトピックがあります。

Introduction

イーサネットデバイスは、MAC アドレステーブルを使用してフレームを転送します。MAC アドレスエントリには、宛先 MAC アドレス、発信インターフェース、および VLAN ID が含まれます。デバイスはフレームを受信すると、そのフレームの宛先 MAC アドレスを使用して、MAC アドレステーブル内で一致するものを検索します。

一致が見つかった場合、デバイスは一致するエントリ内の発信インターフェースからフレームを転送します。
一致するものが見つからない場合、デバイスはフレームの VLAN にフレームをフラッディングします。

Types of MAC address entries

MAC アドレステーブルには、次のタイプのエントリを含めることができます。

Dynamic entries: ダイナミックエントリは、関連付けられたインターフェースから特定の宛先 MAC アドレスを持つフレームを転送するように手動で設定することも、ダイナミックに学習することもできます。ダイナミックエントリは期限切れになることがあります。手動で設定されたダイナミックエントリは、ダイナミックに学習されたエントリと同じプライオリティを持ちます。
Static entries: スタティックエントリは、関連付けられたインターフェースから特定の宛先 MAC アドレスを持つフレームを転送するために手動で追加され、期限切れになることはありません。スタティックエントリは、動的に学習されたエントリよりもプライオリティが高くなります。
Blackhole entries: ブラックホールエントリは手動で設定され、期限切れになりません。ブラックホールエントリは、特定の送信元または宛先 MAC アドレスを持つフレームをフィルタリングするように設定され

ます。たとえば、ユーザー宛てまたはユーザーから送信されたすべてのフレームをブロックするには、ユーザーの MAC アドレスをブラックホール MAC アドレスエントリとして設定できます。

Aging timer for dynamic MAC address entries

セキュリティーとテーブルスペースの効率的な使用のために、MAC アドレステーブルでは、すべてのインターフェースで学習されたダイナミックエントリに対してエージングタイマーが使用されます。エージングタイマーの期限が切れる前にダイナミック MAC アドレスエントリが更新されなかった場合、デバイスはそのエントリを削除します。このエージングメカニズムにより、最新のネットワークトポロジの変更に対応するために、MAC アドレステーブルを迅速に更新できます。
安定したネットワークではより長いエージングインターバルが必要であり、不安定なネットワークではより短いエージングインターバルが必要です。

エージングインターバルが長すぎると、MAC アドレステーブルに古いエントリが保持される可能性があります。その結果、MAC アドレステーブルのリソースが使い果たされ、MAC アドレステーブルが最新のネットワーク変更に対応するためのエントリの更新に失敗する可能性があります。
間隔が短すぎると、有効なエントリが削除され、不要なフラッドが発生してデバイスのパフォーマンスに影響する可能性があります。

安定したネットワークでフラッディングを削減するには、長いエージングタイマーを設定するか、タイマーをディセーブルにして、ダイナミックエントリが不必要にエージングアウトしないようにします。フラッディングを削減すると、ネットワークのパフォーマンスが向上します。フラッディングを削減すると、データフレームが意図しない宛先に到達する可能性が低くなるため、セキュリティーも向上します。

MAC address learning

MAC アドレス学習はデフォルトでイネーブルになっています。デバイスが攻撃を受けているときに MAC アドレステーブルが飽和状態にならないようにするには、MAC アドレス学習をディセーブルにします。たとえば、MAC アドレス学習をディセーブルにすると、送信元 MAC アドレスが異なる大量のフレームによるデバイスの攻撃を防ぐことができます。
グローバル MAC アドレス学習がイネーブルの場合、1 つのインターフェースで MAC アドレス学習をディセーブルにできます。
また、インターフェースに MAC 学習制限を設定して、MAC アドレステーブルのサイズを制限することもできます。MAC アドレステーブルが大きいと、転送パフォーマンスが低下します。制限に達すると、インターフェースは MAC アドレスの学習を停止します。また、送信元 MAC アドレスが MAC アドレステーブルにないフレームを転送するかどうかも設定できます。

VLAN ID check

この機能により、デバイスは、レイヤー2 転送中にセッションエントリと一致する各パケットの VLAN ID をチェックできます。

VLAN ID チェックがイネーブルの場合、デバイスは、VLAN ID が一致するセッションエントリの VLAN ID と同じである場合にだけパケットを許可します。

VLAN ID チェックがディセーブルの場合、デバイスはセッションエントリと一致するパケットを許可します。

ホットバックアップシステムでは、プライマリおよびセカンダリデバイス上のトラフィック着信インターフェースが異なる VLAN に属する場合、VLAN ID チェックをディセーブルにする必要があります。VLAN ID チェックをイネーブルにすると、プライマリ/セカンダリデバイスのスイッチオーバーが発生した後、または非対称パストラフィックが存在する場合に、トラフィックがセッションエントリと正しく一致しなくなります。

Restrictions and guidelines

MAC アドレスエントリを設定する場合は、次の制約事項および注意事項に従ってください。

手動で設定されたスタティックおよびブラックホール MAC アドレスエントリは、設定を保存しないとリブート後も存続できません。

手動で設定されたダイナミック MAC アドレスエントリは、設定を保存するかどうかにかかわらず、リブート時に失われます。

DNS

このヘルプには、次のトピックがあります。

Introduction

DNS

DDNS

DNS proxy

Restrictions and guidelines

Introduction

DNS

ドメインネームシステム(DNS)は、TCP/IP アプリケーションがドメイン名を IP アドレスに変換するために使用する分散データベースです。IPv4 DNS はドメイン名を IPv4 アドレスに変換し、IPv6 DNS はドメイン名を IPv6 アドレスに変換します。
デバイスは DNS クライアントとして機能できます。ユーザーがドメイン名を使用してデバイス上でプログラムを実行すると(デバイスまたはホストへの Telnet など)、DNS はドメイン名を IP アドレスに解決します。ドメイン名の解決は、静的または動的に行うことができます。

静的ドメイン名解決

静的ドメイン名解決とは、ドメイン名と IP アドレス間のマッピングを手動で作成することを意味します。たとえば、デバイスの静的 DNS マッピングを作成して、ドメイン名を使用してデバイスに Telnet 接続できるようにすることができます。

動的なドメイン名解決

動的ドメイン名解決を使用するには、DNS サーバーの IP アドレスを指定する必要があります。ドメイン名解決クエリーは DNS サーバーに送信されます。
リゾルバが不完全な名前の欠落部分を提供するためにドメイン名接尾辞リストを使用できるように、ドメイン名接尾辞リストを構成できます。たとえば、aabbcc.com の接尾辞として com を構成できます。ユーザーが **aabbcc** と入力する必要があるのは、aabbcc.com の IP アドレスを取得する場合のみです。リゾルバは、名前を DNS サーバーに渡す前に接尾辞とデリミタを追加します。
名前リゾルバは、ユーザーが入力したドメイン名に基づいてクエリーを処理します。
ユーザーがドット(.)なしでドメイン名を入力すると(たとえば、abbcc)、リゾルバはそのドメイン名をホスト名と見なします。リゾルバは、問合せ操作を実行する前に、ホスト名に DNS 接尾辞を追加します。ホス

ト名と接尾辞の組合せに一致するものが見つからない場合、リゾルバはユーザーが入力したドメイン名(たとえば、abbcc)を IP アドレス問合せに使用します。
ユーザーが文字の中にドット(.)を含むドメイン名を入力した場合(www.aabbcc など)、リゾルバはこのドメイン名をクエリー操作に直接使用します。クエリーが失敗した場合、リゾルバは別のクエリー操作に DNS サフィックスを追加します。
ユーザーが最後にドット(.)を付けてドメイン名を入力すると(aabbcc.com.など)、リゾルバはそのドメイン名を FQDN と見なし、成功または失敗した問合せ結果を戻します。ドメイン名の最後のドットは、終了記号とみなされます。

ユーザーが名前を指定すると、デバイスは静的名前解決テーブルで IP アドレスをチェックします。使用可能な IP アドレスがない場合は、動的名前解決のために DNS サーバーに接続しますが、静的名前解決よりも時間がかかります。効率を向上させるために、頻繁にクエリーされる名前から IP アドレスへのマッピングをローカルの静的名前解決テーブルに置くことができます。

DDNS

DNS は、ドメイン名と IP アドレスの間の静的マッピングのみを提供します。ノードの IP アドレスが変更されると、ノードへのアクセスは失敗します。
Dynamic Domain Name System(DDNS)は、DNS サーバーのドメイン名と IP アドレス間のマッピングを動的に更新できます。
DDNS を使用するには、最初に DDNS サーバーにログインしてアカウントを登録する必要があります。デバイスは DDNS クライアントとして動作し、デバイスの IP アドレスが変更されると DNS サーバーに DDNS 更新要求を送信します。この要求には、ドメイン名、IP アドレスおよびユーザーアカウント資格証明(ユーザー名とパスワード)の最新のマッピングが含まれています。DDNS クライアントが認証を通過すると、DDNS サーバーは DNS サーバーに対して、DDNS クライアントのドメイン名と IP アドレスを更新するように通知します。
DDNS は IPv4 DNS だけでサポートされています。これはドメイン名と IPv4 アドレス間のマッピングを更新するために使用されます。
DDNS ポリシーには、DDNS サーバードレス、ユーザー名、パスワード、関連付けられた SSL クライアントポリシー、およびアップデート時間間隔が含まれています。DDNS ポリシーを作成したら、複数のインターフェースに適用して DDNS 設定を簡素化できます。

DNS proxy

DNS プロキシは、次の機能を実行します。

DNS クライアントからの要求を指定された DNS サーバーに転送します。
DNS サーバーからの応答をクライアントに伝えます。

DNS プロキシを使用すると、ネットワーク管理が簡素化されます。DNS サーバーアドレスが変更された場合は、各 DNS クライアントではなく、DNS プロキシでのみ構成を変更できます。

Restrictions and guidelines

DNS クエリーを解決のために正しいサーバーに送信できるようにするには、DNS サーバードレスが必要です。IPv4 アドレスと IPv6 アドレスの両方を指定すると、デバイスは次の操作を実行します。
最初に IPv4 DNS クエリーを DNS サーバーの IPv4 アドレスに送信します。クエリーが失敗した場合、デバイスは DNS サーバーの IPv6 アドレスを使用します。
最初に IPv6 DNS クエリーを DNS サーバーの IPv6 アドレスに送信します。クエリーが失敗した場合、デバイスは DNS サーバーの IPv4 アドレスを使用します。
以前に指定された DNS サーバーアドレスの方が優先度が高くなります。手動で指定された DNS サーバーアドレスは、DHCP などを介して動的に取得された DNS サーバーアドレスよりも優先されます。デバイスは最初に、最も優先度の高い DNS サーバーアドレスに DNS クエリーを送信します。最初のクエリーが失敗した場合は、2 番目に優先度の高い DNS サーバーアドレスに DNS クエリーを送信します。
以前に構成された DNS サフィックスの方が優先順位が高くなります。手動で構成された DNS サフィックスは、DHCP などを介して動的に取得された DNS サフィックスよりも優先されます。デバイスは最初に最も高い優先順位を持つサフィックスを使用します。クエリーが失敗した場合、デバイスは 2 番目に高い優先順位を持つサフィックスを使用します。

ARP

Introduction

ARP

ARP は、イーサネットネットワーク上で IP アドレスを MAC アドレスに解決します。
ARP テーブルには、ダイナミック ARP エントリとスタティック ARP エントリが格納されます。

Dynamic ARP entries

ARP はダイナミックエントリを自動的に作成して更新します。ダイナミック ARP エントリは、エージングタイマーが期限切れになるか、出力インターフェースがダウンすると削除されます。また、ダイナミック ARP エントリはスタティック ARP エントリで上書きできます。
ダイナミック ARP エントリはスタティック ARP エントリに変換できますが、再度ダイナミック ARP エントリに変換することはできません。
インターフェースが保持する ARP エントリ arp エントリを保持しないようにするには、インターフェースが学習できるダイナミック ARP エントリの最大数を設定します。

Static ARP entries

スタティック ARP エントリは手動で設定および管理されます。期限切れになることはなく、ダイナミック ARP エントリで上書きすることもできません。
攻撃パケットはスタティック ARP エントリ内の IP-to-MAC マッピングを変更できないため、スタティック ARP エントリはデバイス間の通信を保護します。
固定 IP-to-MAC マッピングを使用してホストと通信するには、デバイスに短いスタティック ARP エントリを設定します。VLAN 内のインターフェースを介して固定 IP-to-MAC マッピングを使用してホストと通信するには、デバイスに長いスタティック ARP エントリを設定します。

IP-MAC binding entries

デバイスは、IP-MAC バインディングテーブルを使用して、偽造された送信元 IP アドレスまたは MAC アドレスを持つ不正なパケットをフィルタリングすることにより、ユーザースプーフィング攻撃を防止します。
IP-MAC バインディングエントリは、手動で作成することも、まとめて生成することもできます。

Manual creation: IP-MAC バインディングエントリを 1 つずつ手動で作成できます。この方法は、多数のホストを含まないネットワークにだけ適用できます。

Bulk generation: インターフェース上の ARP エントリに基づいて IPv4-MAC バインディングエントリをバルク生成するようにデバイスを設定できます。この方法は、多数のホストを含むネットワークにだけ適用できます。

デバイスに IP-MAC バインディングエントリを設定して、通信セキュリティーを向上させます。デバイスはパケットを受信すると、パケット内の送信元 IP アドレスと送信元 MAC アドレスを IP-MAC バインディングエントリと比較します。

送信元 IP アドレスと送信元 MAC アドレスが同じエントリと一致する場合、デバイスはパケットが正当なユーザーからのものであると判断し、パケットの通過を許可します。

次の状況では、デバイスはパケットが偽造パケットであると判断し、そのパケットをドロップします。

送信元 IP アドレスまたは送信元 MAC アドレスだけがバインディングエントリと一致します。

送信元 IP アドレスと送信元 MAC アドレスは、2 つの異なるバインディングエントリと一致します。

送信元 IP アドレスと送信元 MAC アドレスがバインディングエントリと一致しない場合、デバイスはデフォルトアクションに基づいてパケットを処理します。

ND

Introduction

IP-MAC binding entries

デバイスは、IP-MAC バインディングテーブルを使用して、偽造された送信元 IPv6 アドレスまたは MAC アドレスを持つ不正なパケットをフィルタリングすることにより、ユーザースプーフィング攻撃を防止します。

ND

IPv6 Neighbor Discovery(ND)プロセスでは、アドレス解決、ネイバー到達可能性検証、およびネイバーデバイストラッキングのために ICMP メッセージが使用されます。
表 1 に、IPv6 ND プロトコルで使用される ICMPv6 メッセージを示します。

表 1 ND によって使われる ICMPv6 メッセージ

ICMPv6 メッセージ	タイプ	機能
Neighbor Solicitation (NS)	135	ローカルリンク上のネイバーのリンクレイヤードレスを取得します。
		ネイバーの到達可能性を確認します。
		重複アドレスを検出します。
Neighbor Advertisement (NA)	136	NS メッセージに応答します。
		リンク層の変更を隣接ノードに通知します。
Router Solicitation (RS)	133	起動後の自動設定のために、アドレスプレフィクスおよびその他の設定情報を要求します。
Router Advertisement (RA)	134	RS メッセージに応答します。
		プレフィクス情報オプションやフラグビットなどの情報をアドバタイズします。
Redirect	137	特定の条件が満たされた場合に、特定の宛先へのパス上のより適切なネクストホップを送信元ホストに通知します。

Restrictions and guidelines

Restrictions and guidelines: IP-MAC binding entries

IP-MAC バインディングエントリは、手動で作成することも、まとめて生成することもできます。

Manual creation: IP-MAC バインディングエントリを 1 つずつ手動で作成できます。この方法は、多数のホストを含まないネットワークにだけ適用できます。
Bulk generation: インターフェース上の ND エントリに基づいて、IPv6-MAC バインディングエントリをバルク生成するようにデバイスを設定できます。この方法は、多数のホストを含むネットワークに適用できます。

通信セキュリティーを向上させるために、デバイスに IP-MAC バインディングエントリを設定します。デバイスはパケットを受信すると、パケット内の送信元 IPv6 アドレスと送信元 MAC アドレスを IP-MAC バインディングエントリと比較します。

送信元 IPv6 アドレスと送信元 MAC アドレスが同じ IP-MAC バインディングエントリと一致する場合、デバイスはパケットを転送します。
次の状況では、デバイスはパケットが偽造パケットであると判断し、そのパケットをドロップします。
送信元 IP アドレスまたは送信元 MAC アドレスだけがバインディングエントリと一致します。
送信元 IP アドレスと送信元 MAC アドレスは、2 つの異なるバインディングエントリと一致します。
送信元 IPv6 アドレスと送信元 MAC アドレスの両方が IP-MAC バインディングエントリと一致しない場合、デバイスはデフォルトのアクション設定に基づいてパケットを許可またはドロップします。

Restrictions and guidelines: ND entries

ネイバーエントリには、リンクローカルノードに関する情報が格納されます。このエントリは、NS および NA メッセージを使用して動的に作成することも、静的に設定することもできます。
スタティックネイバーエントリを設定するには、次のいずれかの方法を使用します。
Method 1: ネイバーの IPv6 アドレスとリンクレイヤードレスをローカルレイヤー3 インターフェースに関連付けます。

Method 2: ネイバーの IPv6 アドレスとリンクレイヤードレスを VLAN 内のレイヤー2 ポートに関連付けます。

いずれかの方法を使用して、VLAN インターフェースのスタティックネイバーエントリを設定できます。

方法 1 を使用する場合、デバイスは関連する VLAN 内のレイヤー2 ポートを解決する必要があります。

方法 2 を使用する場合は、レイヤー2 ポートが指定された VLAN に属し、対応する VLAN インターフェースがすでに存在することを確認します。

ALG

Introduction

アプリケーション層のパケットペイロードを分析および処理するために、指定したアプリケーションプロトコルタイプの ALG をイネーブルにできます。デバイスでは、次のサービスの ALG をイネーブルにできます。

NAT ALG

NAT44 は、次のプロトコルの ALG をサポートします。

DNS。

H323。

RTSP。

ILS。

PPTP。

FTP。

SIP。

SQLNET。

MGCP。

RSH。

ICMP error packets。

TFTP。

XDMCP。

NBT。

SCCP。

SCTP。

NAT64 は、次のプロトコルの ALG をサポートします。

DNS。

FTP。

HTTP。

ICMP error packets。

NAT66 は、次のプロトコルの ALG をサポートします。

FTP。

ICMP error packets。

LB ALG

LB LAG は、次のプロトコルの ALG をサポートします。

DNS。

H323。

RTSP。

ILS。

PPTP。

FTP。

SIP。

SQLNET。

MGCP。

RSH。

ICMP error packets。

TFTP。

XDMCP。

NBT。

SCCP。

ASPF ALG

ASPF ALG は FTP プロトコル用の ALG をサポートします。

GRE

このヘルプには、次のトピックがあります。

Introduction

GRE encapsulation format

GRE tunnel operating principle

GRE keepalive mechanism

GRE security mechanisms

Restrictions and guidelines

Introduction

Generic Routing Encapsulation(GRE)は、ネットワーク(IPv6 ネットワークなど)上の仮想ポイントツーポイントトンネルにプロトコル(IPv4 など)をカプセル化できるトンネリングプロトコルです。パケットは一方のトンネルエンドでカプセル化され、もう一方のトンネルエンドでカプセル化解除されます。カプセル化前とカプセル化後のパケットのネットワーク層プロトコルは、同じであっても異なっていてもかまいません。

GRE encapsulation format

GRE トンネル型パケットには、次の部分があります。

Payload packet: 元のパケット。ペイロードパケットのプロトコルタイプはパッセンジャプロトコルと呼ばれます。パッセンジャプロトコルは、任意のネットワーク層プロトコルにできます。

GRE header: ペイロードパケットを GRE パケットに変更するためにペイロードパケットに追加されるヘッダー。GRE ヘッダーには、カプセル化の数、バージョン、パッセンジャプロトコルタイプ、チェックサム、およびキーが含まれます。GRE はカプセル化プロトコルと呼ばれます。

Delivery header: トンネルエンドに配信するために GRE パケットに追加されるヘッダー。トランスポートプロトコル(または配信プロトコル)は、GRE パケットを転送するネットワーク層プロトコルです。

デバイスは、トランスポートプロトコルとして IPv4 および IPv6 を使用する GRE トンネルをサポートします。トランスポートプロトコルが IPv4 の場合、GRE トンネルモードは GRE over IPv4(GRE/IPv4)です。トランスポートプロトコルが IPv6 の場合、GRE トンネルモードは GRE over IPv6(GRE/IPv6)です。

GRE tunnel operating principle

IPv4 または IPv6 プロトコルパケットは、次のように GRE トンネルを介してトランスポートネットワークを通過します。

送信元デバイスは、カスタマー側インターフェースから IPv4 または IPv6 プロトコルパケットを受信すると、パケットを次のように処理します。
ルーティングテーブルを検索して、パケットの発信インターフェースを識別します。
パケットを発信インターフェース(GRE トンネルインターフェース)に送信します。
パケットを受信すると、トンネルインターフェースはパケットを GRE でカプセル化してから、配信ヘッダーでカプセル化します。配信ヘッダーでは、送信元アドレスはトンネルの送信元アドレスであり、宛先アドレスはトンネルの宛先アドレスです。
送信元デバイスは、配信ヘッダー内の宛先アドレスに従ってルーティングテーブルを検索します。次に、デバイスはカプセル化されたパケットを GRE トンネルの物理インターフェースから転送します。
パケットが GRE トンネルの宛先に到達すると、宛先デバイスは宛先アドレスをチェックします。宛先はデバイス自体であり、IP ヘッダーのプロトコル番号は 47(GRE のプロトコル番号)であるため、デバイスはカプセル化を解除するためにパケットを GRE に送信します。
GRE は最初に配信ヘッダーを削除し、次に GRE キー、チェックサム、およびパケットシーケンス番号をチェックします。GRE はチェックを完了すると、GRE ヘッダーを削除し、転送のためにペイロードをパッセンジャプロトコルに送信します。

GRE keepalive mechanism

このメカニズムにより、トンネルインターフェースは指定された間隔でキープアライブパケットを送信できます。タイムアウト時間内にピアからの応答を受信しない場合、デバイスはローカルトンネルインターフェースをシャットダウンします。デバイスは、ピアからキープアライブ確認応答パケットを受信すると、ローカルトンネルインターフェースを起動します。タイムアウト時間は、キープアライブ間隔にキープアライブ番号を乗算した結果です。
デバイスは、GRE キープアライブがイネーブルであるかどうかにかかわらず、受信したキープアライブパケットを常に確認応答します。

GRE security mechanisms

GRE は、GRE キーおよび GRE チェックサムセキュリティメカニズムをサポートします。

GRE key

GRE キーはパケットの有効性を保証します。送信者は GRE キーをパケットに追加します。受信者は GRE キーを自身の GRE キーと比較します。2 つのキーが同じ場合、受信者はパケットを受け入れます。2 つのキーが異なる場合、受信者はパケットをドロップします。

GRE checksum

GRE チェックサムはパケットの整合性を保証します。送信側は GRE ヘッダーとペイロードのチェックサムを計算し、チェックサムを含むパケットをトンネルピアに送信します。受信側は受信したパケットのチェックサムを計算し、パケットで伝送されたものと比較します。チェックサムが同じ場合、受信側はパケットがそのままであると判断し、パケットの処理を続けます。チェックサムが異なる場合、受信側はパケットを廃棄します。

Restrictions and guidelines

GRE トンネルを設定する場合は、この項の制約事項および注意事項に従ってください。

Restrictions and guidelines: Address configuration

パッセンジャプロトコルが IPv4 の場合は、各トンネルエンドでトンネルインターフェースの IPv4 アドレスを設定します。パッセンジャプロトコルが IPv6 の場合は、各トンネルエンドでトンネルインターフェースの IPv6 アドレスを設定します。
トンネルの送信元アドレスと宛先アドレスは、トンネルの両端で設定する必要があります。一方の端のトンネル送信元アドレスまたは宛先アドレスは、もう一方の端のトンネル宛先アドレスまたは送信元アドレスである必要があります。
トンネルインターフェースの IP アドレスとトンネルインターフェースに設定されたトンネル宛先アドレスは、異なるサブネット内にある必要があります。

Restrictions and guidelines: Routing configuration

パケット転送が正しく行われるようにするには、パケットの宛先ネットワークとローカルトンネルインターフェースの IP アドレスが同じサブネット上にあるかどうかを確認します。同じサブネット上にない場合は、トンネルインターフェースを介して宛先ネットワークに到達するルートを設定します。ルートを設定するには、次のいずれかの方法を使用します。

ローカルトンネルインターフェースをルートの発信インターフェースとして使用して、スタティックルートを設定します。
トンネルインターフェースとプライベートネットワークに接続するインターフェースの両方で、ダイナミックルーティングプロトコルをイネーブルにします。これにより、ダイナミックルーティングプロトコルは、トンネルインターフェースを発信インターフェースとして使用してルーティングエントリを確立できます。

Restrictions and guidelines: Keepalive configuration

GREトンネルの両端でキープアライブをイネーブルにする必要はありません。必要に応じて、GREトンネルの一端でキープアライブをイネーブルにします。

Restrictions and guidelines: GRE security mechanism configuration

GREトンネルの両端は、同じキーを持つか、両方ともキーを持たない必要があります。
トンネルの各端で GRE チェックサムをイネーブルまたはディセーブルにできます。トンネル端で GRE チェックサムがイネーブルになっている場合、トンネル端はチェックサムを含むパケットをピア端に送信します。トンネル端は、受信したパケットが GRE チェックサムを含む場合、トンネル端が GRE チェックサムでイネーブルになっているかどうかに関係なく、受信したパケットの GRE チェックサムをチェックします。

IPsec

このヘルプには、次のトピックがあります。

Introduction

IP Security(IPsec)は、IP 通信に対して相互運用可能で高品質な暗号化ベースのセキュリティーを提供するために、IETF によって定義されています。これは、2 つのエンドポイント(2 つのセキュリティゲートウェイなど)間に確立された安全なチャネルでデータを送信するレイヤー3 VPN テクノロジーです。このような安全なチャネルは通常、IPsec トンネルと呼ばれます。
IPsec は、次のプロトコルとアルゴリズムを持つセキュリティフレームワークです。

Authentication Header(AH)。
Encapsulating Security Payload(ESP)。
Internet Key Exchange(IKE)。
認証および暗号化のアルゴリズム。

AH および ESP は、セキュリティーサービスを提供するセキュリティプロトコルです。IKE は自動キー交換を実行します。

Security protocols and encapsulation modes

Security protocols

IPsec には、AH と ESP という 2 つのセキュリティプロトコルが用意されています。これらのプロトコルは、IP パケットをカプセル化する方法と、IP パケットが提供できるセキュリティーサービスを定義します。

AH は、IP パケット内の AH ヘッダーのカプセル化を定義します。AH は、データ送信元認証、データ整合性、およびデータ改ざんを防止するためのリプレイ防止サービスを提供できますが、盗聴を防止することはできません。したがって、機密性のないデータの送信に適しています。
ESP は、IP パケット内の ESP ヘッダーおよびトレーラーのカプセル化を定義します。ESP は、データ暗号化、データ送信元認証、データ整合性およびリプレイ防止サービスを提供できます。AH とは異なり、ESP はデータを IP パケットにカプセル化する前に暗号化できるため、データの機密性を保証できます。

AH と ESP はどちらも認証サービスを提供しますが、AH が提供する認証サービスの方が強力です。実際には、いずれかまたは両方のセキュリティプロトコルを選択できます。AH と ESP の両方が使用される場合、IP パケットは最初に ESP によってカプセル化され、次に AH によってカプセル化されます。

Encapsulation modes

IPsec は次のカプセル化モードをサポートしています。

トランスポートモード
: セキュリティプロトコルは、IP パケットの上位層データを保護します。トランスポートモードは、エンドツーエンドのセキュリティー保護が必要な場合に使用できます(保護された送信の開始ポイントと終了ポイントは、データの実際の開始ポイントと終了ポイントです)。通常、トランスポートモードは、ホスト間の通信を保護するために使用されます。

トンネルモード
: セキュリティプロトコルは、IP パケット全体を保護します。保護された送信の開始ポイントと終了ポイントがデータパケットの実際の開始ポイントと終了ポイントでない場合(たとえば、2 つのゲートウェイが IPsec を提供しているが、データの開始ポイントと終了ポイントがゲートウェイの背後にある 2 つのホストである場合)は、トンネルモードを使用する必要があります。トンネルモードは通常、ゲートウェイ間の通信を保護するために使用されます。

Authentication and encryption

Authentication algorithms

IPsec は、ハッシュアルゴリズムを使用して認証を実行します。ハッシュアルゴリズムは、任意の長さのメッセージに対して固定長のダイジェストを生成します。IPsec ピアはそれぞれ、各パケットのメッセージダイジェストを計算します。受信者は、ローカルダイジェストを送信者から受信したダイジェストと比較します。IPsec は、次のタイプの認証アルゴリズムをサポートします。

Hash-based Message Authentication Code(HMAC)ベースの認証アルゴリズム(HMAC-MD5 および HMAC-SHA を含む)。

HMAC-MD5 は、HMAC-SHA よりも高速ですが、安全性は劣ります。

SM3 認証アルゴリズム。

Encryption algorithms

IPsec では、同じキーを使用してデータを暗号化および復号化する対称暗号化アルゴリズムが使用されます。デバイス上の IPsec では、次の暗号化アルゴリズムを使用できます。

DES: 64 ビットのプレーンテキストブロックを 56 ビットのキーで暗号化します。DES は最も安全性が低いアルゴリズムですが、最も高速なアルゴリズムです。

3DES: 3 つの 56 ビット DES キーを使用してプレーンテキストデータを暗号化します。キーの長さは合計で 168 ビットまでです。中程度のセキュリティー強度を提供し、DES よりも低速です。

AES: 128 ビット、192 ビット、または 256 ビットのキーを使用してプレーンテキストデータを暗号化します。AES は最高のセキュリティー強度を提供し、3 DES よりも低速です。

SM: プレーンテキストデータを 128 ビットキーで暗号化します。SM は、AES と同じレベルのセキュリティー強度を提供します。

IPsec SA

Security Association(SA)は、2 つの IPsec ピア間でネゴシエートされる合意です。SA には、データ保護のための次のパラメーターが含まれています。

セキュリティプロトコル。

カプセル化モード。

認証アルゴリズム。

暗号化アルゴリズム。

共有キーとそのライフタイム。

SA は単方向です。双方向通信でデータフローを保護するには、少なくとも 2 つの SA が必要です。2 つのピアが AH と ESP の両方を使用して相互間のデータフローを保護する場合は、各方向のプロトコルごとに独立した SA を構築します。

SA は、セキュリティパラメータインデックス(SPI)、宛先 IP アドレス、およびセキュリティプロトコル ID で構成されるトリプレットによって一意に識別されます。SPI は 32 ビットの番号です。AH/ESP ヘッダーで送信されます。

IKE によって作成された SA にはライフタイムがあり、時間ベースまたはトラフィックベースのライフタイム

タイマーが期限切れになると削除されます。SA ライフタイムタイマーが期限切れになる前に、IKE は新しい SA をネゴシエートします。新しい SA は作成直後に処理を引き継ぎます。

IKE negotiation

IKE は IPsec 用に SA をネゴシエートし、SA を IPsec に転送します。IPsec は SA を使用して IP パケットを保護します。IKE は、次の 2 つのフェーズで IPsec 用にキーと SA をネゴシエートします。

Phase 1: 2 つのピアが IKE SA を確立します。IKE SA は、通信用の安全な認証チャネルです。
フェーズ 1 ネゴシエーションでは、メインモード、アグレッシブモードまたは GM メインモードを使用できます。アグレッシブモードはメインモードより高速ですが、アイデンティティ情報の保護は提供しません。メインモードはアイデンティティ情報の保護を提供しますが、低速です。要件に応じて適切なネゴシエーションモードを選択してください。ローカル IKE ピアが RSA-DE または SM2-DE デジタルエンベロープ認証方式を使用する場合は、GM メインモードを使用する必要があります。

Phase 2: フェーズ 1 で確立された IKE SA を使用して、2 つのピアが IPsec SA を確立するようにネゴシエートし、IP パケットを保護します。

IPsec tunnel establishment

2 つのピアは、インターフェースに IPsec ポリシーを適用することによって、間に IPsec トンネルを確立します。IPsec ポリシーは、IPsec によって保護されるパケットの範囲と、保護に使用されるセキュリティーパラメーターを定義します。
IPsec ピアは、セキュリティーポリシーに従って保護するパケットを識別すると、IPsec トンネルを設定し、トンネルを介してリモートピアにパケットを送信します。IPsec トンネルは、パケットによってトリガーされる IKE ネゴシエーションを介して設定できます。IPsec トンネルは、実際には IPsec SA です。着信パケットは着信 SA によって保護され、発信パケットは発信 SA によって保護されます。

パケットを送信するとき、IPsec ポリシーで構成されたインターフェースは、ポリシーの優先順位の昇順で IPsec ポリシーを調べます。パケットが IPsec ポリシーの保護されたフローと一致する場合、インターフェースは IPsec ポリシーに従ってパケットをカプセル化します。一致するものが見つからない場合、インターフェースは IPsec 保護なしでパケットを送信します。
インターフェースは、ローカルデバイス宛ての IPsec パケットを受信すると、カプセル化解除のために IPsec パケットヘッダー内の SPI に従って着信 IPsec SA を検索します。カプセル化解除されたパケットが保護されたデータフローと一致する場合、デバイスはそのパケットを処理します。カプセル化解除されたパケットが保護されたデータフローと一致しない場合、デバイスはそのパケットをドロップします。

IPsec ポリシーでは、アクション([保護する]または[保護しない])を選択して、データフローを保護するかどうかを指定できます。IPsec ポリシーでは、複数のデータフローを定義できます。デバイスは、パケットの

最初の一致データフローで定義されたアクションに従ってパケットを処理します。

インターフェースのインバウンドパケットとアウトバウンドパケットの両方が、IPsec ポリシーで定義されたデータフローと一致する必要があります。デバイスは、アウトバウンドパケットのデータフローのフォワードマッチングと、インバウンドパケットのデータフローのバックワードマッチングを実行します。
発信方向では、「protect」データフローに一致するパケットは IPsec によって保護されます。データフローに一致しないパケットや「unprotect」データフローに一致するパケットは IPsec によって保護されません。
着信方向では、「保護」データフローと一致する非 IPsec パケットはドロップされます。ローカルデバイス宛ての IPsec パケットはカプセル化解除されます。

IPsec smart link selection

ネットワークの安定性と可用性を向上させるために、通常、複数のリンクがネットワーク出力に配置され、宛先ネットワークに接続されます。これらのリンクの品質(パケット損失率と遅延)は静的ではなく、時間とともに変化し続けます。ゲートウェイデバイスが、宛先への IPsec トンネルを確立するために、必要な伝送品質のリンクを動的に選択できることが重要です。IPsec スマートリンク選択は、この要件を満たすことができます。
IPsec スマートリンク選択を使用すると、ゲートウェイは、IPsec トンネルが確立されているアクティブリンクのリアルタイムパケット損失率および遅延を監視できます。リンクのパケット損失率または遅延が指定したしきい値を超えると、IPsec スマートリンク選択によって IPsec トンネルのリンクが再選択されます。また、手動でリンクをアクティブにして、そのリンクを介して IPsec トンネルを確立することもできます。
IPsec スマートリンク選択には、次の利点があります。

ロードバランシングのために複数のリンクがネットワーク出力に配置されている場合は、一部のリンクがビジー状態で、一部のリンクがアイドル状態になる状態を回避してください。
お客様が自分でリンクを選択できない場合は、お客様に適したリンクを選択します。
ネットワーク出力デバイスと宛先デバイス間の障害リンクにトラフィックを転送しないようにします。

Auto-generate security policy

IPsec ポリシーを作成するは、[セキュリティーポリシーの自動生成]を選択できます。この機能を使用すると、デバイスは、IKE ネゴシエーションパケットを許可するセキュリティーポリシーを自動的に生成できます。

Restrictions and guidelines

IPsec ポリシーでリモートホスト名を指定する場合は、次の制約事項および注意事項に従ってください。

リモートホスト名が DNS サーバーによって解決される場合、ローカルデバイスは、キャッシュされた DNS エントリが期限切れになると、DNS サーバーにクエリーを送信して、ホスト名に対応する最新の IP アドレスを取得します。DNS エントリの期限切れ情報は、DNS サーバーから取得されます。
ローカルに設定されたスタティック DNS エントリによってリモートホスト名が解決され、エントリ内の IP アドレスが変更された場合は、IPsec ポリシーでリモートホスト名を再指定して、新しい IP アドレスを取得する必要があります。
SA を設定し、IPsec で保護されたトラフィックが 2 つの IPsec ピア間で正しく処理されるようにするには、IPsec ピア上にミラーイメージ ACL を作成します。IPsec ピア上の ACL 規則が相互にミラーイメージを形成しない場合は、次の両方の要件が満たされている場合にのみ SA を設定できます。
一方のピアの ACL ルールで指定された範囲は、もう一方のピアの対応する ACL ルールでカバーされます。
より狭いルールを持つピアが SA ネゴシエーションを開始します。

SA 発信側がより広い ACL ルールを使用する場合、一致するトラフィックが応答側のスコープを超えているために、ネゴシエーション要求が拒否されることがあります。

IPsec ポリシーでローカル ID を構成しない場合、ポリシーでは、詳細設定で構成されたグローバルローカル ID 設定が使用されます。
IPsec ポリシーの次の設定に対する変更は、変更後に設定された IPsec SA に対してのみ有効です。
カプセル化モード。
セキュリティプロトコル。
セキュリティアルゴリズム。
PFS です。
IPsec SA ライフタイム。
IPsec SA アイドルタイムアウト。

変更を既存の IPsec SA に反映させるには、IPsec SA をリセットする必要があります。

IPsec トンネルの IPsec ピアには、同じセキュリティプロトコル、セキュリティアルゴリズム、およびカプセル化モードを使用する IPsec ポリシーが必要です。
IKE は IPsec SA をネゴシエートするときに、IPsec ポリシーで構成された IPsec SA ライフタイム設定を使用して、ピアと IPsec SA ライフタイムをネゴシエートします。IPsec SA ライフタイム設定が IPsec ポリシーで構成されていない場合は、グローバル IPsec SA ライフタイム設定が使用されます。IKE はローカルライフタイム設定またはピアによって提案されたライフタイム設定のいずれか小さい方を使用します。
スマートリンク選択で使用されるリンクがゲートウェイアドレスをネクストホップアドレスとして使用する場合、ゲートウェイアドレスが変更されるたびに、リンクのネクストホップアドレスを手動で変更する必要があります。
量子暗号化を使用するには、**Advanced Settings** ページの **Quantum Encryption** 領域で次の設定を行います。
量子暗号化を有効にします。
サーバードレスタイプ、サーバードレス、およびサーバーポートを設定します。

GD-quantum アクセス ID、GD-quantum 認証キー、および GD-quantum 復号化キーを設定します。

GD-quantum サーバーの管理者に問い合わせて、以前の量子鍵配送パラメーターに関する情報を入手してください。

ADVPN

このヘルプには、次のトピックがあります。

Introduction

自動検出 Virtual Private Network(ADVPN)を使用すると、ダイナミックパブリックアドレスを使用する企業の支店で VPN ネットワークを確立できます。ADVPN では、VPN Address Management(VAM)プロトコルを使用して、ダイナミックパブリックアドレスを収集、維持、および配布します。
VAM はクライアント/サーバーモデルを使用します。すべての VAM クライアント(VAMCs)は、VAM サーバー(VAMS)にパブリックアドレスを登録します。VAMC は、VAMS から他の VAMCs のパブリックアドレスを取得して、ADVPN トンネルを確立します。

ADVPN structures

ADVPN はドメインを使用して VPN を識別します。VPN 内の VAMCs は同じ ADVPN ドメインに割り当てる必要があります。VAMC は 1 つの ADVPN ドメインにしか所属できません。VAMS は複数の ADVPN ドメインにサービスを提供し、VAMCs を管理できます。
VAMCs にはハブとスポークが含まれます。

Hub: ハブはルーティング情報の交換センターです。ハブスポークネットワーク内のハブは、データ転送センターでもあります。
Spoke: スポークはブランチのゲートウェイです。他の ADVPN ノードから受信したデータは転送されません。

ADVPN は、フルメッシュ、ハブスポーク、およびハブグループ構造をサポートしています。

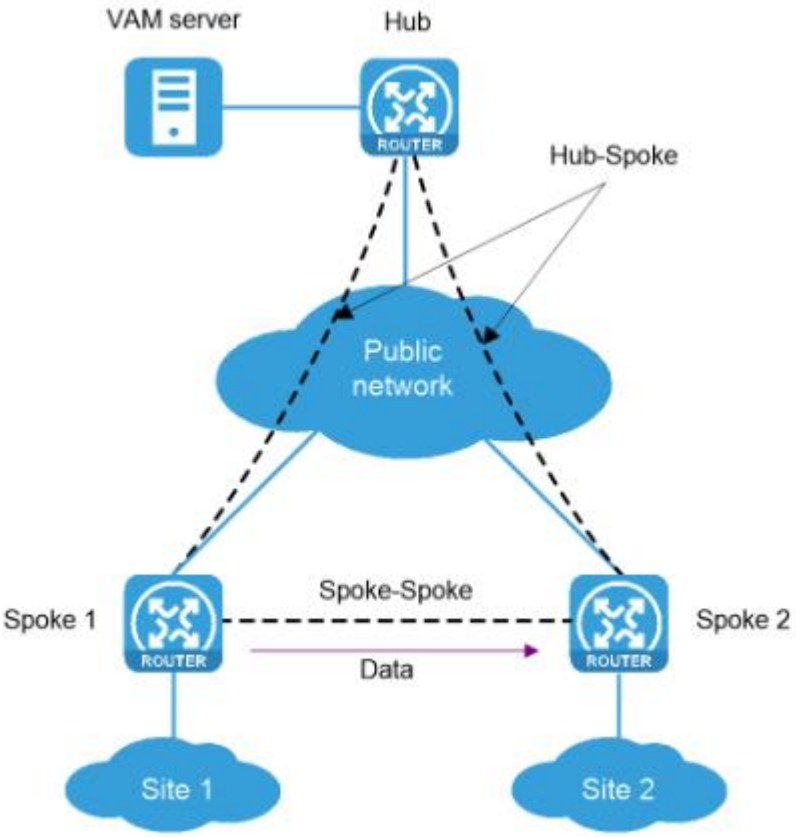
Full-mesh ADVPN

フルメッシュ ADVPN では、スポークは相互に直接通信できます。ハブはルート交換センターとして機能します。

図 1 に示すように、スポークは VAMS に登録し、ADVPN ドメイン内のハブ情報を取得します。次に、ハブへの永続的なトンネルを確立します。

任意の 2 つのスポークは、データを直接交換するためのダイナミックトンネルを確立できます。アイドルタイムアウト時間内にデータが存在しない場合、トンネルは削除されます。

図 1:フルメッシュ ADVPN

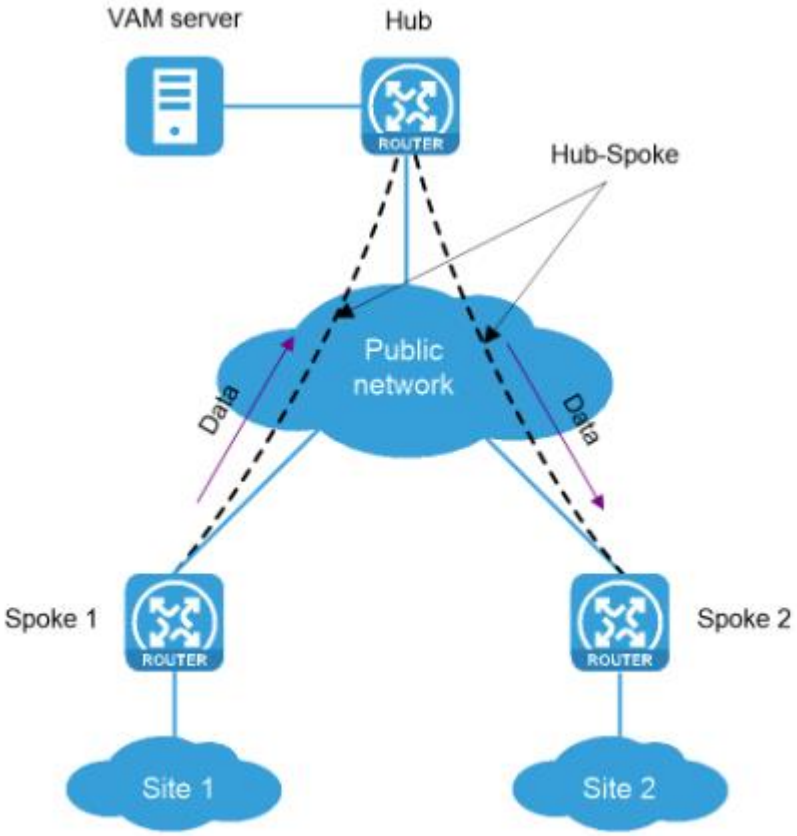


Hub-spoke ADVPN

ハブスポーク ADVPN では、スポークはハブを介して相互に通信します。ハブはルート交換センターとデータ転送センターの両方の役割を果たします。

図 2 に示すように、各スポークはハブへの永続的なトンネルを確立します。スポークはハブを介して相互に通信します。

図 2 ハブスポーク ADVPN



Hub-group ADVPN

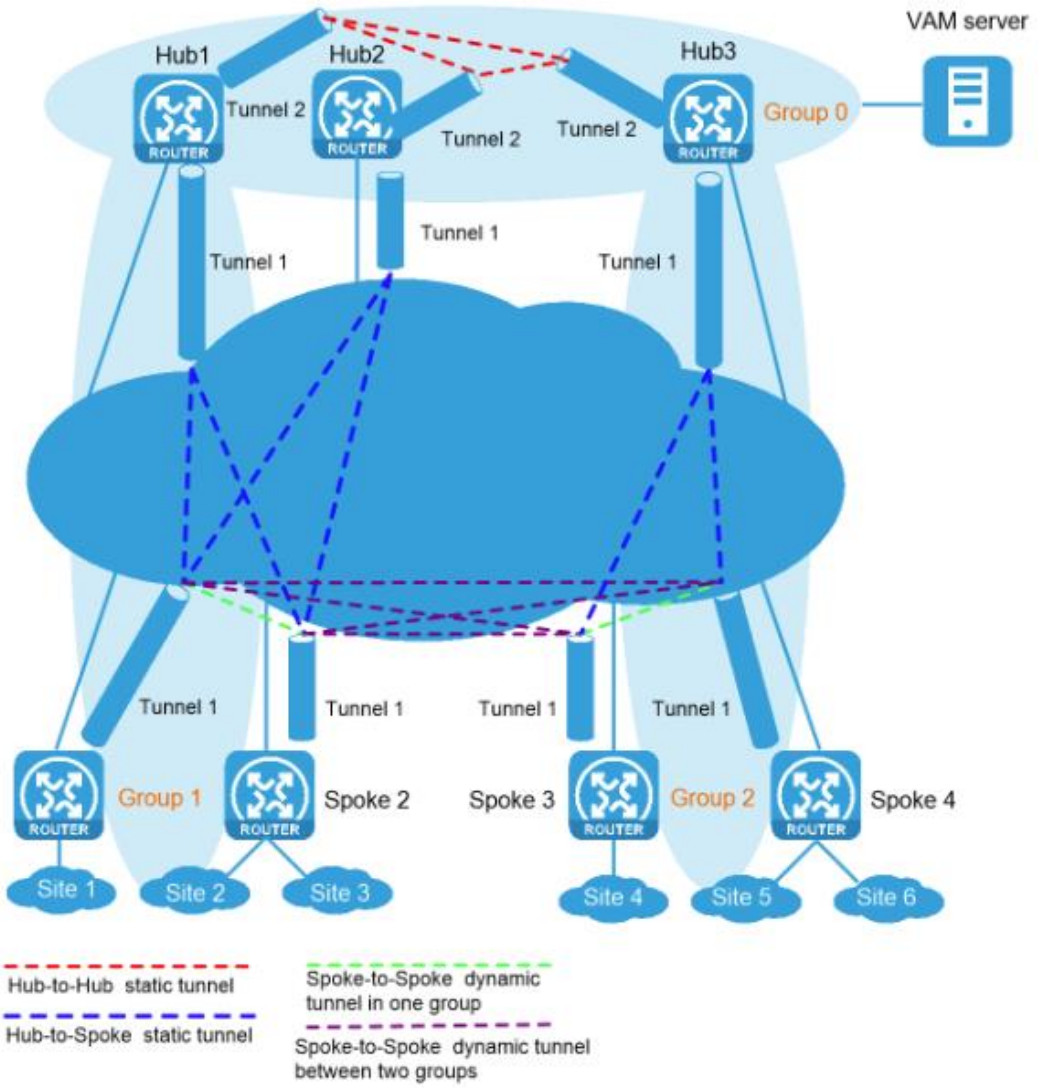
ハブグルーADVPN は、より多くの ADVPN クライアントを収容できます。これにより、1 つのハブですべてのクライアントを管理できます。図 3 に示すように、ハブグループ ADVPN には複数のハブグループが含まれます。各ハブグループには、1 つ以上のハブとスポークがあります。

ハブグループを分類するには、次のガイドラインに従ってください。

すべてのハブはバックボーンハブグループに属している必要があります。このハブグループはフルメッシュバックボーンエリアを形成します。すべてのハブは、VAMS から他のハブに関する情報を取得し、相互に永続的な ADVPN トンネルを確立します。
スポークは、非バックボーンハブグループに属している必要があります。各非バックボーンハブグループには 1 つ以上のハブが含まれ、フルメッシュ構造またはハブスポーク構造のいずれかを使用します。スポークは、ADVPN ドメイン内のハブ情報を VAMS から取得し、ハブへの永続的なトンネルを確立します。スポークは、ハブグループ内のハブへのトンネルだけを確立できます。

ハブグループでのトンネルの確立とデータ転送は、ネットワーク構造に依存します。スポーク間のグループ間通信は、グループのハブを通過する必要があります。グループ間通信中のハブへの負荷を軽減するために、異なるハブグループ内のスポークに動的トンネルの確立を許可できます。アイドルタイムアウト時間内にデータが存在しない場合、動的トンネルは削除されます。

図 3 ハブグループ ADVPN



ADVPN working mechanisms

VAMS には、静的パブリックアドレスが必要です。VAMCs には、パブリックアドレスとプライベートアドレスの両方が必要です。パブリックアドレスは、パブリックネットワークに接続されているインターフェースのアドレスです。手動で構成することも、動的に割り当てることもできます。プライベートアドレスは、ADVPN トンネルインターフェースのアドレスです。手動で構成する必要があります。ADVPN ドメイン内の VAMCs

のすべてのプライベートアドレスは、同じネットワークセグメントに属する必要があります。
ADVPN には次の段階があります。

Connection initialization : VAMS と VAMC は、次の操作を実行して接続を初期化します。
VAMC は、暗号化アルゴリズムと認証アルゴリズムを接続要求で VAMS に送信します。
VAMS は、そのアルゴリズムを優先度の高い順に VAMC によって送信されたアルゴリズムと比較する。
VAMS は、一致する暗号化および認証アルゴリズムを VAMC に送信します。
一致するものが見つからない場合、ネゴシエーションは失敗します。
VAMS と VAMC は、事前共有キーに基づいて暗号化キーと認証キーを生成します。
認証と暗号化が必要ない場合、キーは生成されません。
VAMS と VAMC は、キーを使用して保護されたネゴシエーション確認応答パケットを交換します。
VAMS と VAMC は、保護されたネゴシエーション確認応答パケットを復元できる場合、キーを使用して後続のパケットを保護します。
パケットを復元できない場合、ネゴシエーションは失敗します。
Registration: VAMC は VAMS への登録を要求し、VAMS は VAMC を認証します。VAMS は、VAMC から送信された情報に基づいて、VAMC の暗号化および認証アルゴリズムを選択します。一致するものが見つからない場合、登録は失敗します。
Tunnel establishment: ハブグループでは、各スポークがすべてのハブへの永続的なトンネルを確立し、各ハブが相互に永続的なトンネルを確立する必要があります。
Route learning and packet forwarding: ルートは、ルーティングプロトコルを介して学習されます。ルーティングプロトコルはネットワークタイプを決定し、ネットワークタイプはパケット転送方式を決定します。

ADVPN tunnel NAT traversal

ADVPN トンネルは、NAT ゲートウェイを通過できます。

トンネルイニシエータだけが NAT ゲートウェイの背後に存在する場合は、NAT ゲートウェイを介してスポーク間トンネルを確立できます。
トンネルレシーバが NAT ゲートウェイの背後にある場合、レシーバがトンネル確立要求を発信する前に、ハブによってパケットが転送される必要があります。NAT ゲートウェイがエンドポイントに依存しないマッピングを使用する場合、NAT ゲートウェイを介してスポーク間トンネルを確立できます。
両端が NAT ゲートウェイの背後にある場合、トンネルは確立されず、両端間のパケットはハブによって転送される必要があります。

Restrictions and guidelines

General restrictions and guidelines

ネットワークの到達可能性を確保するには、ADVPN トンネルインターフェースをセキュリティーゾーンに追加し、VAMCs が相互に到達できるようにセキュリティーポリシーを設定します。
同じ ADVPN ドメイン内の VAMSs と VAMCs には、同じ事前共有キーが必要です。
同じ ADVPN ドメイン内のすべてのトンネルインターフェースでは、キープアライブパケットの送信間隔と最大再試行回数を同じ設定にする必要があります。
IP アドレスの設定を除き、プライマリおよびセカンダリ VAMSs の ADVPN 設定はすべて同じです。
VAMS に設定された ADVPN ポートは、VAMC 上の VAMS に指定された ADVPN ポートと同じである必要があります。
VAMC を正しく登録するには、VAMC のプライベートアドレスが VAMS 上のハブグループのプライベートネットワーク内にあることを確認します。

Restrictions and guidelines: OSPF configuration

正しい通信を確保するために、同じハブグループ内のすべての VAMSs と VAMCs で OSPF ネットワークタイプが同じであることを確認します。

Restrictions and guidelines: GRE key configuration

VAMC 上の一方の GRE モード ADVPN トンネルインターフェースに GRE キーが設定されている場合、同じハブグループ内のもう一方の VAMCs 上の ADVPN トンネルインターフェースは、同じ GRE キーを使用する必要があります。
複数の GRE モード ADVPN トンネルインターフェースが同じ送信元アドレスまたは送信元インターフェースを持つ場合は、インターフェースに異なる GRE キーを設定する必要があります。

Configure ADVPN

ADVPN を設定する前に、次の項目を確認します。

ADVPN domain。

VAMS パブリックアドレス、事前共有キー、認証方式、暗号化アルゴリズム、および認証アルゴリズム。
VAMC のパブリックアドレス、プライベートアドレス、およびプライベートネットワーク情報。

Configure a VAMS

VAMS Web 構成のサポートは、デバイスモデルによって異なります。

1. **Network** > **VPN** > **ADVPN** > **VAMS** を選択します。

2. **Create** をクリックします。
3. 表 1 の項目を VAMS 用に設定し、VAMS を有効にします。

   また、既存の VAMS を有効化、無効化、または変更することもできます。

表 1 VAMS 構成項目

項目	説明
ADVPN domain	VAMS の ADVPN ドメインを入力します。 ドメイン名は一意である必要があります。
ADVPN domain ID	VAMS の ADVPN ドメイン ID を入力します。 ドメイン ID は一意である必要があります。
Preshared key	事前共有キーを入力します。 VAMS は事前共有キーを使用して、VAMC との接続初期化中に初期暗号化キーと認証キーを生成します。このキーは、暗号化と認証が必要な場合に、後続のパケットの暗号化キーと認証キーを生成するためにも使用されます。
Authentication method	VAMS が VAMCs を認証するための認証方式を選択します。
ISP domain	VAMCs が認証される ISP ドメインを選択します。 詳細については、ISP ドメインのオンラインヘルプを参照してください。 この項目は、認証方式が PAP または CHAP の場合にのみ使用できます。
Hub group	ハブグループリスト。 このリストには、ハブグループを作成、編集および削除するためのインターフェースも表示されます。ハブグループの構成の詳細は、表 2 を参照してください。
Authentication algorithms	VAMS が VAMCs と通信するために使用する認証アルゴリズムを選択します。 VAMS と VAMC の間のアルゴリズムネゴシエーションでは、前に指定された認証アルゴリズムの優先度が高くなります。VAMS は、優先度の高い順に、自身のアルゴリズムを VAMC から送信されたアルゴリズムと比較します。一致が検出されると、VAMS は一致するアルゴリズムを VAMC に送信します。一致が検出されない場合、ネゴシエーションは失敗します。 **None** (認証なし)を選択した場合は、他のすべてのアルゴリズムの後に **None** が配置されていることを確認します。**None** の後のアルゴリズムは有効になりません。
Encryption algorithms	VAMS が VAMCs と通信するために使用する暗号化アルゴリズムを選択します。 優先順位と選択のメカニズムは、認証アルゴリズムと同じです。
Keepalive packets: Sending interval	VAMC がキープアライブパケットを VAMS に送信する間隔を設定します。 この項目を変更しても、登録された VAMCs には影響しません。変更は、その後登録された VAMCs にのみ有効です。

Keepalive packets: Max retries	VAMC が VAMS にキープアライブパケットを再送信する最大試行回数を設定します。 この項目を変更しても、登録された VAMCs には影響しません。変更は、その後登録された VAMCs にのみ有効です。
VAM packet retry interval	VAMS が VAM パケットを再送信する間隔を設定します。
Enable VAMS	VAMS を有効にするには、この項目を選択します。

表 2 ハブグループの構成項目

項目	説明
Group name	ハブグループ名を入力します。
Shortcut rule	スポーク間直接トンネルの確立を制御する規則を選択します。 **None**: スポークは直接トンネルを確立できません。 **ACL**: スポーク間直接トンネルの確立を制御する ACL を指定します。 **All**: スポーク間直接トンネルの確立に関する制限はありません。
Hub	ハブリスト。 ハブリストには、ハブを作成、編集および削除するためのインターフェースも用意されています。ハブが NAT ゲートウェイの背後にある場合、**Public address** および **ADVPN port** フィールドはハブに必要です。値は、NAT によって変換されるパブリックアドレスおよびポート番号です。
Spoke	スポークリスト。 スポークリストには、スポークを作成および削除するためのインターフェースもあります。

Configure a VAMC

1. **Network** > **VPN** > **ADVPN** > **VAMC** を選択します。
2. **Create** をクリックします。
3. 表 3 の項目を VAMC 用に設定し、VAMC を有効にします。

   また、既存の VAMC をイネーブル、ディセーブル、または変更することもできます。

表 3 VAMC の構成項目

項目	説明

VAMC name	VAMC 名を入力します。 名前は ADVPN ドメイン内で一意である必要があります。
ADVPN domain	VAMC の ADVPN ドメイン名を入力します。
Preshared key	事前共有キーを入力します。 VAMC は事前共有キーを使用して、VAMS との接続初期化中に初期暗号化キーと認証キーを生成します。このキーは、暗号化と認証が必要な場合に、後続のパケットの暗号化キーと認証キーを生成するためにも使用されます。
Username Password	VAMC が VAMS への登録に使用するユーザー名とパスワードを入力します。
Enable VAMC	VAMC を有効にするには、この項目を選択します。
Dumb time	VAMC のダムタイムを設定します。 VAMC は、VAMS への接続がタイムアウトになると(キープアライブタイムアウト)、ダムタイマーを開始します。ダムタイマーの期限が切れると、VAMC は新しい接続要求を VAMS に送信します。
VAM packet retry interval	VAMC が VAMS に要求を再送信する間隔を設定します。 VAMC が VAMS に要求を送信した後、再試行間隔内に応答を受信しなかった場合は、要求を再送信します。
VAM packet max retries	VAMC が VAMS に要求を再送信する最大試行回数を設定します。
Primary server address Secondary server address	プライマリまたはセカンダリ VAMS のパブリックアドレスを指定する方法を選択します。IP アドレスまたはドメイン名を入力できます。 パブリックアドレスは、固定 IP アドレスです。
Primary server port Secondary server port	ポート番号を入力します。 VAMC はポートを使用して、プライマリまたはセカンダリ VAMS をリッスンします。
Tunnel mode	ADVPN トンネルのカプセル化モードを選択します。
Tunnel interface ID	ADVPN トンネルインターフェース ID を入力します。
Tunnel private address	ADVPN トンネルインターフェースのプライベートアドレスとネットワークマスクを入力します。
Tunnel public address	トンネルパブリックアドレスを指定する方法を選択します。

	IP アドレスを入力するか、送信元インターフェースを選択できます。選択したインターフェースのプライマリ IP アドレスが使用されます。
VRF	VAMC の VRF を選択します。 VRF のルーティングテーブルは、ADVPN トンネル経由でトラフィックを転送するために使用されます。詳細については、VRF オンラインヘルプを参照してください。
OSPF settings	ADVPN トンネルの OSPF インスタンスを選択します。詳細については、OSPF オンラインヘルプを参照してください。
Network type	ADVPN 構造に影響する OSPF ネットワークタイプを選択します。 この項目は、OSPF インスタンスを選択した場合にのみ使用できます。
DR priority	VAMC の OSPF DR プライオリティを設定します。 この項目は、OSPF インスタンスを選択した場合にのみ使用できます。
GRE key	GRE モードで使用される GRE キーを設定します。GRE キーが必要ない場合は、この項目を設定しないでください。詳細については、GRE オンラインヘルプを参照してください。
Enable GRE checksum	この項目を選択すると、GRE チェックサムが有効になり、GRE モードでのパケットの整合性が保証されます。詳細については、GRE オンラインヘルプを参照してください。
Source UDP port	UDP モードでパケットの送信元ポート番号を設定します。 **ADVPN V0 version compatible** を選択した場合、このトンネルの送信元 UDP ポートは、他の ADVPN トンネルの送信元 UDP ポートと同じにはできません。
Register private address list	VAMC が VAMS に登録する ADVPN トンネルプライベートネットワーク情報。パケットがリモートプライベートネットワーク宛ての場合、VAMC は VAMS にパケットの宛先アドレスを解決するように要求します。VAMS は、解決されたアドレスがリモート VAMC のレジスタプライベートアドレス内にあることを検出した後、リモート VAMC のノード情報を現在の VAMC に送信します。 このリストには、既存のプライベートネットワークが表示されます。また、プライベートネットワークを作成、編集および削除するためのインターフェースも提供されます。ベストプラクティスとして、**Preference** フィールドには、他の動的ルーティングプロトコルよりも高く、静的ルーティングよりも低い値を割り当てます。値が大きいほど、プリファレンスは低くなります。
ADVPN V0 version compatible	VAMC が ADVPN V0 バージョンと互換性があるかどうかを設定します。
Tunnel dumb time	待機時間を設定します。 ADVPN トンネルの確立に失敗すると、待機タイマーが開始されます。

Idle timeout time	スポーク/スポークトンネルのアイドルタイムアウト時間を設定します。アイドルタイムアウト時間内にスポーク/スポークトンネルに沿ってデータが転送されない場合、トンネルは自動的に削除されます。
ToS of tunneled packets	ADVPN トンネルパケットの ToS を設定します。
TTL of tunneled packets	ADVPN トンネルパケットの TTL を設定します。
Set DF bit	トンネリングされたパケットの DF ビットを設定するには、この項目を選択します。
Enable IPsec	IPsec を有効にするには、この項目を選択します。
IPsec profile name	IPsec プロファイル名を入力します。
IKE settings	IKE 設定を構成します。
AuthN method	IKE 認証方式を選択します。 ・**Preshared key**。 ・**Signatur**。
Preshared key	**Preshared key** 認証方式の事前共有キーを入力します。
PKI domain	**Signatur** 認証方法で証明書の PKI ドメインを選択します。詳細については、PKI オンラインヘルプを参照してください。
Cert access policy	**Signatur** 認証方式の証明書アクセスポリシーを選択します。詳細は、PKI オンラインヘルプを参照してください。
IKE proposal	IPsec プロファイルで使用される IKE プロポーザルを選択します。詳細については、IPsec オンラインヘルプを参照してください。
Negotiation mode	IKE ネゴシエーションモードを選択します。
IPsec configuration	IPsec を設定します。
Encapsulation mode	IPsec カプセル化モードを選択します。
Security protocol	IPsec セキュリティプロトコルを選択します。
ESP authentication	ESP または AH-ESP セキュリティプロトコルの ESP 認証アルゴリズムを選択します。
ESP encryption	ESP または AH-ESP セキュリティプロトコルの ESP 暗号化アルゴリズムを選択します。

AH authentication	AH または AH-ESP セキュリティプロトコルの AH 認証アルゴリズムを選択します。
PFS	PFS のグループを選択します。 PFS 機能は、DH アルゴリズムに基づくセキュリティー機能です。PFS がイネーブルになると、IKE フェーズ 2 で追加の DH 交換が実行され、IPsec キーが IKE キーとの派生関係を持たないこと、および破損したキーが他のキーに脅威を与えないことが確認されます。
DPD check	IKE DPD チェックをイネーブルにするには、この項目を選択します。
Check method	IKE DPD チェック方式を選択します。
Detect interval	IKE DPD 検出間隔を設定します。 **On demand**: 指定した期間内にピアから IPsec パケットを受信しなかった場合、デバイスは DPD 検出を実行します。 **Periodic**: デバイスは、ピアから IPsec パケットを受信したかどうかに関係なく、指定された間隔で DPD 検出を実行します。
Retry interval	ローカルエンドが IKE PDP パケットを再送信する間隔を設定します。 ローカルエンドは、リトライ間隔内にピアからの応答を受信しない場合、DPD 要求を再送信します。ローカルエンドがピアからの応答を受信せずに 2 回の再試行を行った場合、IKE キーおよび IKE キーに対応する IPsec キーを削除します。

L2TP

このヘルプには、次のトピックがあります。

Introduction

Typical L2TP network components

L2TP tunneling modes

Troubleshooting L2TP

Tunnel setup failure

Data transmission failure

Introduction

Layer 2 Tunneling Protocol(L2TP)は、Virtual Private Dialup Network(VPDN)トンネリングプロトコルです。L2TP は、パブリックネットワーク(たとえば、インターネット)上にポイントツーポイントトンネルを設定し、カプセル化された PPP フレーム(L2TP パケット)をトンネル経由で送信します。L2TP を使用すると、リモートユーザーは、PPP を使用してパブリックネットワークに接続した後、L2TP トンネル経由でプライベートネットワークにアクセスできます。

Typical L2TP network components

一般的な L2TP ネットワークには、次のコンポーネントがあります。

リモートシステム:通常、リモートシステムは、プライベートネットワークにアクセスする必要があるリモートユーザーのホストまたはリモートブランチのデバイスです。

LAC: L2TP Access Concentrator(LAC)は、PPP と L2TP の両方に対応しています。通常は、ローカル ISP にある Network Access Server(NAS)であり、主に PPP ユーザーにアクセスサービスを提供します。

LAC は、L2TP トンネルのエンドポイントであり、LNS とリモートシステムの間にあります。LAC は、L2TP を使用してリモートシステムから受信したパケットをカプセル化し、カプセル化されたパケットを LNS に送信します。また、LNS から受信したパケットのカプセル化を解除し、カプセル化解除されたパケットを目的のリモートシステムに送信します。

LNS: L2TP Network Server(LNS)は、PPP と L2TP の両方に対応しています。通常、エンタープライズネットワーク上のエッジデバイスです。

LNS は、L2TP トンネルのもう一方のエンドポイントです。LNS は、LAC によってトンネリングされる PPP セッションの論理的な終端ポイントです。L2TP は、トンネルを確立することによって、PPP セッションの終端ポイントを NAS から LNS に拡張します。

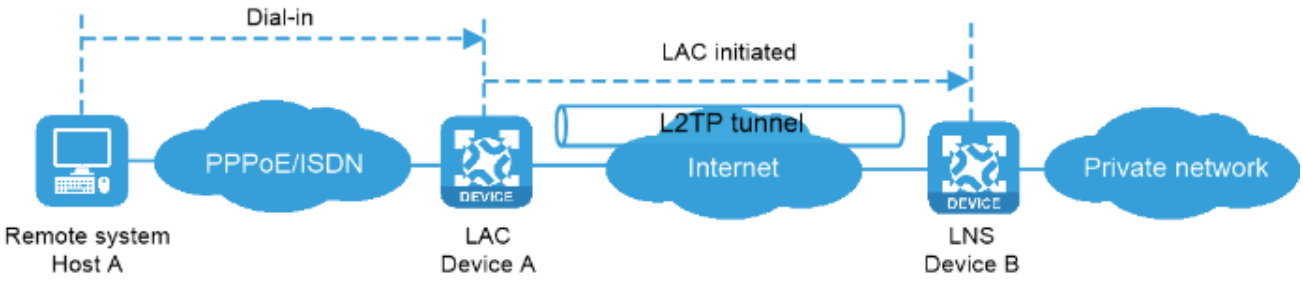
L2TP tunneling modes

L2TP トンネリングモードには、NAS 開始、クライアント開始、および LA C 自動開始があります。

NAS-initiated tunneling mode

図 1 に示すように、リモートシステムは PPPoE/ISDN ネットワークを介して LAC にダイヤルインします。LAC はインターネットを介して LNS へのトンネリング要求を開始します。

図 1 NAS が開始するトンネリングモード



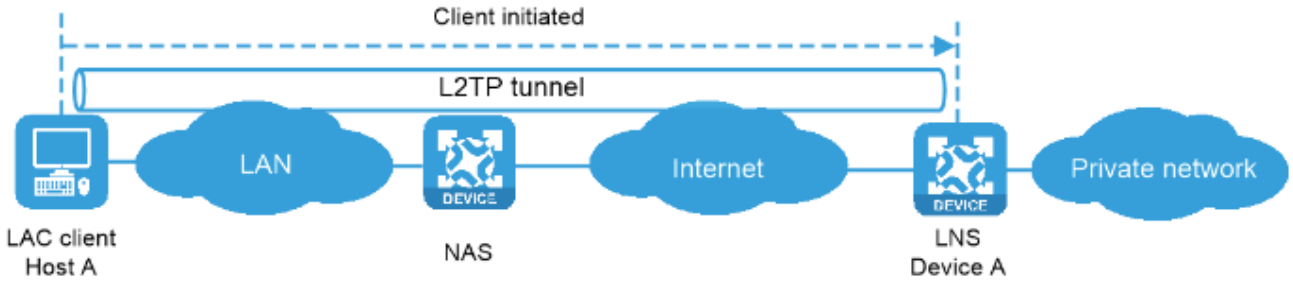
NAS が開始するトンネルには、次の特性があります。

リモートシステムは PPP をサポートする必要があるだけで、L2TP をサポートする必要はありません。
リモートシステムの認証およびアカウンティングは、LAC または LNS に実装できます。

Client-initiated tunneling mode

図 2 に示すように、L2TP を実行しているリモートシステム(LAC クライアント)には、インターネットを介して LNS と通信するためのパブリック IP アドレスがあります。LAC クライアントは、専用の LAC デバイスなしで LNS へのトンネリング要求を直接開始できます。

図 2 クライアントが開始するトンネリングモード



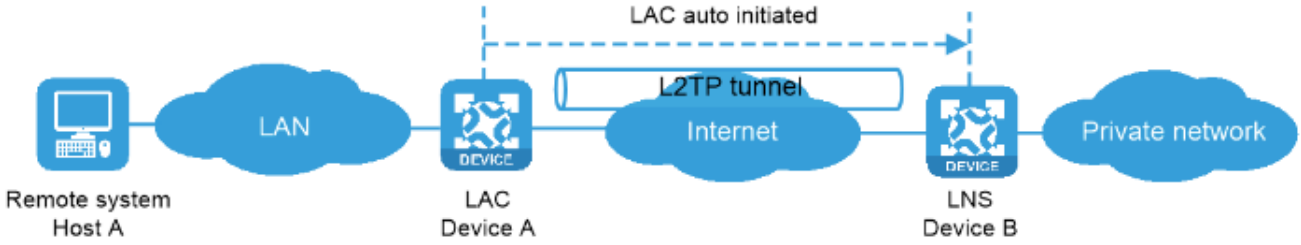
クライアントが開始するトンネルには、次の特性があります。

クライアントが開始するトンネルは、リモートシステムと LNS 間で確立されるため、セキュリティーが高くなります。
リモートシステムは L2TP をサポートし、LNS と通信できる必要があります。これにより、拡張性が低下します。

LAC-auto-initiated tunneling mode

NAS 起動モードでは、リモートシステムは PPPoE または ISDN を介して LAC に正常にダイヤルインする必要があります。
LAC 自動開始モードでは、LAC 上でトンネル設定を行い、LAC が LNS へのトンネリング要求を開始するようにトリガーできます。リモートシステムがプライベートネットワークにアクセスすると、LAC は L2TP トンネルを介してデータを転送します。

図 3 LAC 自動開始トンネリングモード



LA C 自動開始トンネルには、次の特性があります。

リモートシステムと LAC 間の接続は、ダイヤルアップ接続に限定されず、任意の IP ベースの接続を使用できます。
リモートシステム上でダイヤルアップによる L2TP トンネル確立をトリガーする必要はありません。

L2TP セッションは、L2TP トンネルが確立された直後に確立されます。次に、PPPoE クライアントおよび PPPoE サーバーとしてそれぞれ動作する LAC および LNS が、PPP ネゴシエーションを実行します。
L2TP トンネルは、1 つの L2TP セッションだけを伝送できます。
LNS は、リモートシステムではなく LAC にプライベート IP アドレスを割り当てます。

Troubleshooting L2TP

Tunnel setup failure Tunnel setup failure

Symptom

VPN > L2TP > TunnelInfo を選択すると、トンネル情報は表示されず、トンネルの確立に失敗します。

Solution

この問題を解決するには、次の項目を確認して、トンネルセットアップの失敗を回避します。

LNS のアドレスが LAC 上で正しく設定されている。
LAC と LNS に同じ PPP 認証モードが設定されています。
ユーザー名とパスワードが LAC および LNS 上で正しく設定されている。
LNS 上で L2TP グループ番号が 1 でない場合、LAC と LNS に同じトンネル名が設定されます。
トンネル認証が成功します。
トンネル認証は、両側またはいずれかの側でイネーブルにできます。トンネル認証が両側またはいずれかの側でイネーブルになっている場合にトンネルが正常に確立されるようにするには、LAC と LNS に同じ非ヌルキーを設定します。

Data transmission failure

Symptom

VPN > L2TP > TunnelInfo を選択すると、トンネルが正常に確立されたことを示すページが表示されます。ただし、データ送信に失敗します。たとえば、LAC と LNS は相互に ping を実行できません。

Solution

この問題を解決するには、次の手順に従います
LAC に LNS の背後にあるプライベートネットワークへのルートがあり、その逆もあることを確認します。
使用可能なルートがない場合は、スタティックルートまたはダイナミックルーティングプロトコルを設定します。

LNS 上の仮想テンプレートインターフェースをセキュリティーゾーンに追加し、セキュリティーゾーンからセキュリティーゾーン Local へのトラフィックを許可します。

リンク帯域幅を増やして、リンクの可用性を向上させます。

インターネットバックボーンの輻輳と高いパケット損失率は、データ伝送の障害を引き起こす可能性があります。L2TP データ伝送は UDP に基づいており、UDP はパケットエラー制御機能を提供しません。回線が不安定な場合、LAC と LNS は相互に ping できない可能性があります。

SSL VPN

このヘルプには、次のトピックがあります。

Introduction

SSL VPN は、SSL VPN ゲートウェイを介して SSL ベースのセキュアなリモートアクセスサービスを提供します。インターネット上の任意の場所からのユーザーは、SSL 対応ブラウザを介して SSL VPN ゲート

ウェイへのセキュアな接続を確立し、ゲートウェイの背後にある保護されたリソースにアクセスできます。

SSL VPN operating mechanism

SSL VPN ゲートウェイの背後にある保護されたリソースへのリモートユーザーアクセスを許可するには、これらのリソースをゲートウェイ上で設定する必要があります。リモートユーザーは、ゲートウェイへの SSL 暗号化接続を確立し、ID 認証を通過すると、自分に許可されたリソースだけにアクセスできます。
SSL VPN は次のように動作します。

リモートユーザーは、SSL VPN ゲートウェイへの HTTPS 接続を確立します。
　　このプロセスでは、リモートユーザーと SSL VPN ゲートウェイが SSL 証明書認証を実行します。
リモートユーザーがユーザー名とパスワードを入力します。
SSL VPN ゲートウェイは、ユーザーが入力したクレデンシャルを認証し、ユーザーに一連のリソースへのアクセスを許可します。
ユーザーはアクセスするリソースを選択します。
　　そのリソースに対するアクセス要求は、SSL 接続を介して SSL VPN ゲートウェイに送信されます。
SSL VPN ゲートウェイは要求を解決し、対応する内部サーバーに要求を転送します。
SSL VPN ゲートウェイは、SSL 接続を介してサーバーの応答をユーザーに転送します。

SSL VPN networking modes

SSL VPN は、次のネットワーキングモードをサポートします。

Gateway mode: ゲートウェイモードでは、SSL VPN ゲートウェイは、リモートユーザーと内部サーバーネットワークを接続するゲートウェイとして機能します。SSL VPN ゲートウェイはインライン展開されるため、内部ネットワークを完全に保護できますが、データ伝送のパフォーマンスに影響します。
Single-arm mode: シングルアームモードでは、SSL VPN ゲートウェイはネットワークゲートウェイに接続されます。ゲートウェイは、ユーザーからサーバーへのトラフィックを SSL VPN ゲートウェイに転送します。SSL VPN ゲートウェイはトラフィックを処理し、処理されたトラフィックをゲートウェイに送り返します。ゲートウェイはトラフィックを内部サーバーに転送します。SSL VPN ゲートウェイはキーパス上に展開されないため、ネットワークのパフォーマンスのボトルネックにはなりません。ただし、SSL VPN ゲートウェイは内部ネットワークを完全に保護することはできません。

SSL VPN access modes

Web access

Web アクセスモードでは、リモートユーザーはブラウザを使用して、HTTPS 経由で SSL VPN ゲートウェイによって許可された Web リソースにアクセスします。ログイン後、ユーザーは Web ページにリストされ

た任意のリソースにアクセスできます。Web アクセスモードでは、すべての操作が Web ページ上で実行されます。
SSL VPN Web アクセスユーザーが使用できるリソースは、Web サーバーだけです。

TCP access

TCP アクセスモードでは、ユーザーはアプリケーションのオープンポートにアクセスすることによって、内部サーバー上の TCP アプリケーションにアクセスします。サポートされるアプリケーションには、リモートアクセスサービス(Telnet など)、デスクトップ共有サービス、メールサービス、Notes サービス、および固定ポートを使用するその他の TCP サービスが含まれます。
TCP アクセスモードでは、ユーザーは TCP アクセスクライアントソフトウェアを SSL VPN クライアント(ユーザーが使用する端末デバイス)にインストールします。クライアントソフトウェアは SSL 接続を使用してアプリケーション層データを送信します。

IP access

IP アクセスは、リモートユーザーと内部サーバー間のセキュアな IP 通信を実現します。
IP アクセスモードで内部サーバーにアクセスするには、専用の IP アクセスクライアントソフトウェアをインストールする必要があります。クライアントソフトウェアは、SSL VPN クライアントに Virtual Network Interface Card(VNIC)をインストールします。

BYOD access

BYOD アクセスにより、モバイルクライアントを介した内部リソースへの安全なアクセスが可能になります。
モバイルクライアントが BYOD アクセスモードで内部リソースにアクセスする場合:

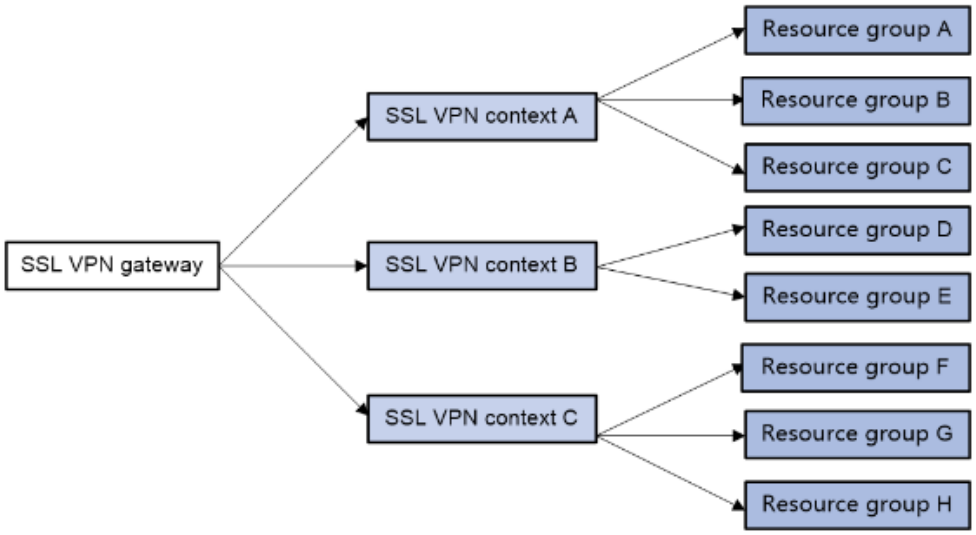
SSL VPN ゲートウェイでは、モバイルクライアント用の Endpoint Mobile Office(EMO)サーバーを指定する必要があります。モバイルクライアントは、EMO サーバーを介して内部リソースにアクセスします。モバイルクライアントには、モバイルクライアント専用の SSL VPN クライアントソフトウェアをインストールする必要があります。

Resource access control

SSL VPN は、リソースへのユーザークセスをユーザー単位で制御します。

図 1 に示すように、SSL VPN ゲートウェイは複数の SSL VPN コンテキストに関連付けることができます。SSL VPN コンテキストには複数のリソースグループが含まれます。リソースグループは、アクセス可能な Web リソース、TCP リソース、および IP リソースを定義します。

図 1 SSL VPN リソースアクセスコントロール



SSL VPN ユーザーは、次の方法を使用して SSL VPN ゲートウェイにアクセスできます。

Direct access: SSL VPN ゲートウェイが 1 つの SSL VPN コンテキストだけに関連付けられている場合、ユーザーは SSL VPN ゲートウェイの IP アドレスとポート番号を入力することで、SSL VPN コンテキストに直接アクセスできます。
By domain list: SSL VPN ゲートウェイは、異なるドメイン名を介して複数の SSL VPN コンテキストに関連付けることができます。ユーザーは、SSL VPN ゲートウェイのログインページに表示されるドメインリストからドメイン名を選択するように求められます。SSL VPN ゲートウェイは、選択したドメイン名に基づいて、ユーザーが属する SSL VPN コンテキストを決定します。
By virtual host name: SSL VPN ゲートウェイは、異なる仮想ホスト名を介して複数の SSL VPN コンテキストに関連付けることができます。SSL VPN ゲートウェイは、SSL VPN ゲートウェイのログインページで入力された仮想ホスト名に基づいて、ユーザーが属する SSL VPN コンテキストを決定します。

ユーザーの SSL VPN コンテキストが決定されると、SSL VPN ゲートウェイは、コンテキストに指定された ISP ドメインの認証方式と認可方式を使用して、ユーザーの認証と認可を実行します。

SSL VPN ゲートウェイがユーザーにリソースグループの使用を許可した場合、ユーザーはそのリソースグループで許可されているリソースにアクセスできます。
SSL VPN ゲートウェイがユーザーにリソースグループの使用を許可しない場合、ユーザーはデフォルトのリソースグループで許可されているリソースにアクセスできます。

SSL VPN ゲートウェイは、AAA を使用してユーザー認証および認可を実行します。SSL VPN は、AAA プロトコルである RADIUS および LDAP をサポートしています。RADIUS が最もよく使用されます。

Restrictions and guidelines

SSL VPN AC インターフェースを無効にすると、進行中の IP アクセスサービスが中断される可能性があります。この操作は慎重に実行してください。

Restrictions and guidelines: SSL VPN gateway configuration

SSL VPN ゲートウェイで使用される SSL サーバーポリシーが変更された場合、またはポリシー設定が変更された場合は、ゲートウェイを再度イネーブルにして、設定を有効にする必要があります。

Restrictions and guidelines: TCP access configuration

SSL VPN ゲートウェイでポート転送項目のクライアントアドレスを設定する場合は、ネットワークセグメント 127.0.0.0/8 内のアドレスを使用するか、ホスト名またはドメイン名を使用します。
ユーザーがホストを介して TCP リソースにアクセスするには、ホスト上の hosts ファイルの変更が必要になる場合があります。ユーザーがホストの管理者権限を持っていることを確認してください。
TCP アクセスに使用するホストには、Java Runtime Environment がインストールされている必要があります。

Restrictions and guidelines: IP access configuration

IP アクセスクライアントの IP アクセスアドレスプールを設定する場合は、次の制約事項および注意事項に従ってください。

IP アクセスアドレスプールと、IP アクセスクライアントホストで使用される NIC の IP アドレスは、異なるネットワークセグメントに属している必要があります。
アドレスの競合を回避するには、IP アクセスプールに SSL VPN ゲートウェイデバイス上のインターフェースの IP アドレスが含まれていないことを確認します。
アクセス可能な IP リソースをホストしている内部サーバーの IP アクセスアドレスプールと IP アドレスが、異なるネットワークセグメントに属していることを確認します。

SSL VPN ユーザーに IP アドレスをバインドする場合は、次の制約事項および注意事項に従ってください。

ユーザーに認可された SSL VPN リソースグループに IP アクセスアドレスプールが指定されている場合、IP アドレスはアドレスプールに存在する必要があります。

SSL VPN リソースグループにアドレスプールが指定されていない場合、、ユーザーの SSL VPN コンテキストに指定されたアドレスプールに IP アドレスが存在する必要があります。
同じ IP アドレスを異なる SSL VPN ユーザーにバインドできるのは、ユーザーの SSL VPN コンテキストが異なる VPN インスタンスに関連付けられている場合だけです。

Restrictions and guidelines: Domain name configuration

Web リソース URL やポート転送エントリなどの SSL VPN 設定項目に有効なドメイン名を指定していることを確認します。
SSL VPN は、指定されたドメイン名の存在または有効性をチェックしません。

Restrictions and guidelines: Webpage template configuration

アップロードするテンプレートファイルは.zip ファイルである必要があります。
アップロードされたテンプレート.zip ファイルには、.zip ファイルのルートディレクトリに home.html ファイルと login html ファイルの両方が含まれている必要があります。

Restrictions and guidelines: LDAP authentication configuration

SSL VPN ユーザーに LDAP 認証を設定する場合は、LDAP 認可も設定する必要があります。デバイスの CLI から LDAP 認可設定を行います。

Restrictions and guidelines: SSO login configuration

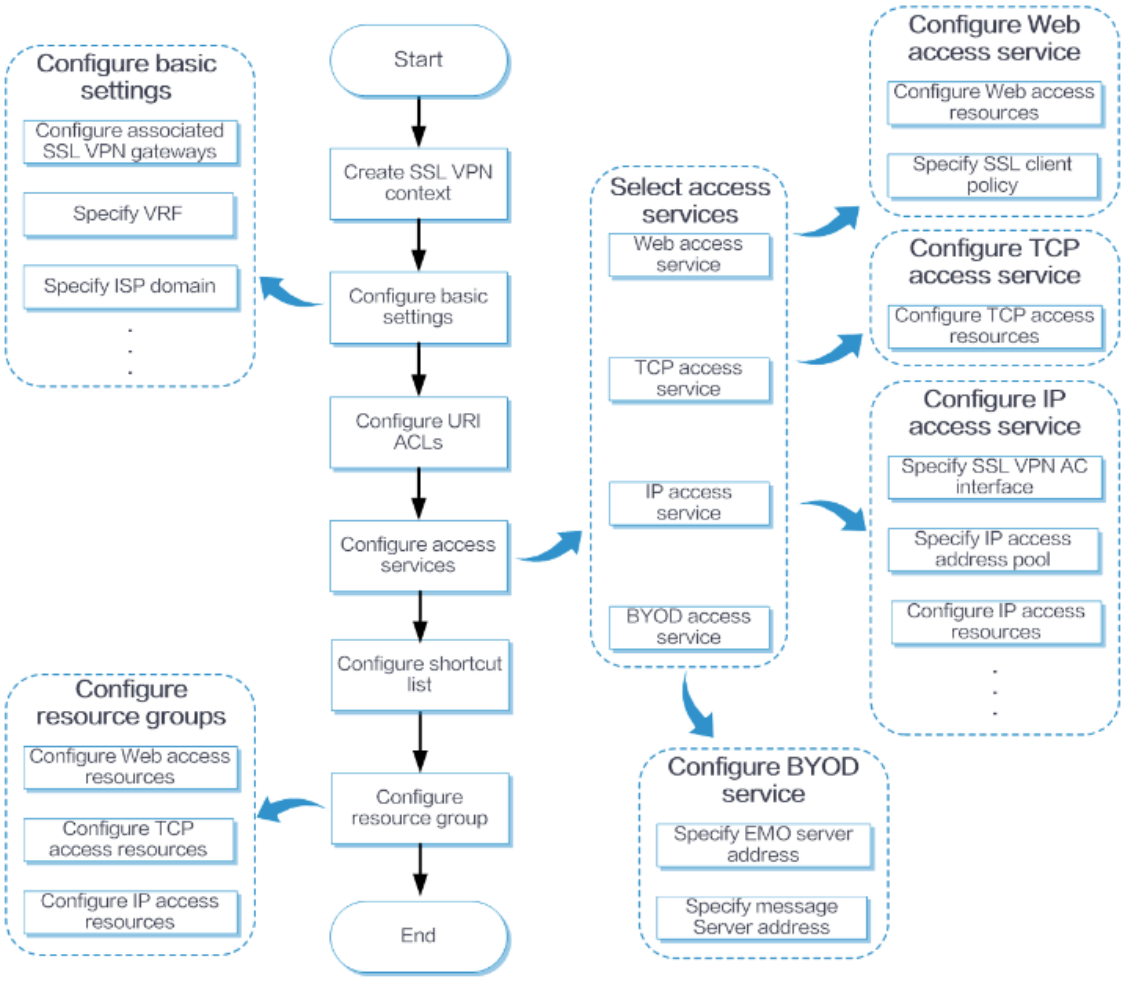
自動構築 SSO 方式では、次の要件を満たす必要があります。

ユーザーグループ名が SSO ログインパラメータとして指定されている場合、リモートユーザーだけがサポートされます。
SSO ログインは、SSL VPN Web インターフェース上の URL リンクをクリックしてリソースにアクセスする場合にだけ使用できます。ブラウザのアドレスバーまたは URL 入力ボックスに URL を入力してリソースにアクセスする場合、SSO は機能しません。
SSO ログインは、グラフィック検証コードを必要とする Web リソースでは使用できません。
SSO ログインは、2 要素認証またはスクリプト呼び出しを必要とする Web リソースでは使用できません。

Configure SSL VPN

図 2 に示すように、SSL VPN コンテキストを設定します。

図 2 SSL VPN の設定手順



上記の設定手順に加えて、SSL VPN では次の作業も実行できます。

Network > **SSL VPN** > **SSL VPN Gateways** ページで、SSL VPN ゲートウェイを作成および編集します。

Network > **SSL VPN** > **IP Access Address Pools Network** > **SSL VPN** > **IP Access Address Pools** ページで、IP アクセスアドレスプールを作成および編集します。

Network > **SSL VPN** > **SSL VPN AC Interfaces** ページで、SSL VPN AC インターフェースを作成および編集します。

Edit SSL VPN Context ページの **Webpage settings** タブで、SSL VPN Web ページの Web ページテンプレート、タイトル、ログインウェルカムメッセージ、非表示パスワードボックス設定、およびロゴを編集します。

Edit SSL VPN Context ページの **Webpage settings** タブで、次の設定を編集します。

SSL VPN ゲートウェイのログインページおよびリソースページに表示される中国語および英語の通知。

中国語と英語の Web ページファイル。

中国語と英語のパスワードの複雑さの説明。

サーバー応答メッセージの書き換え。

Network > **SSL VPN** > **Global Settings** ページでカスタム IP アクセスクライアントファイルをアップロードします。ユーザーはクライアントをダウンロードし、それを使用して SSL VPN ゲートウェイにログインできます。このページでは、Web ページテンプレートをグローバル SSL VPN Web ページテンプレートとして選択することもできます。

ユーザー定義の SSL VPN Web ページテンプレートを追加します。

Network > **SSL VPN** > **TempManagement** ページに移動し、**Create** をクリックします。

開いたページで、ユーザー定義の Web ページテンプレートをアップロードします。

アップロードされたテンプレートは、**Network** > **SSL VPN** > **Global Settings** または **Network** > **SSL VPN** > **Statistics** ページで使用できます。

Network > **SSL VPN** > **Global Settings** ページで、オンラインユーザー情報および IP アクセス統計情報を表示します。

SSO ログインの場合は、**Network** > **SSL VPN** > **Global Settings** ページでユーザーカスタム設定をエクスポートおよびインポートできます。

Export user custom configuration をクリックして、現在のユーザーのカスタムユーザー名とパスワードをエクスポートし、SSO ログインを実行します。

Export user custom configuration をクリックして、現在のユーザーのカスタムユーザー名とパスワードをインポートし、SSO ログインを実行します。

Configure basic settings in an SSL VPN context

関連付けられた SSL VPN ゲートウェイ、SSL VPN コンテキストが属する VRF(VPN インスタンス)、および SSL VPN コンテキストのイネーブルステータスなどの基本設定を行います。

手順

1. **Network** タブをクリックします。
2. ナビゲーションペインで、**SSL VPN** > **SSL VPN Contexts** を選択します。

   SSL VPN Contexts ページが開きます。
3. **Create** をクリックします。

   Create SSL VPN Context ページが開きます。

Basic settings タブで、SSL VPN コンテキストの基本設定を行い、**Next** をクリックします。

表 1 SSL VPN コンテキストの基本的な設定項目

項目	説明

Context name	SSL VPN コンテキスト名を入力します。
Associated gateways	SSL VPN コンテキストに関連付けられたゲートウェイを設定します。 SSL VPN コンテキストに関連付けられたゲートウェイを追加するには、次の手順を実行します。 **Associated gateways** フィールドで **Create** をクリックします。 表示されるダイアログボックスで、**GateWay** リストからゲートウェイを選択します。使用可能なゲートウェイがない場合は、**SSL VPN Gateway** をクリックしてゲートウェイを作成します。 アクセス方法を選択します。オプションには、**Exclusive**, **Domain name**, および **Virtual host name** があります。SSL VPN ゲートウェイが他の SSL VPN コンテキストに関連付けられている場合、または関連付けられる予定の場合は、ドメイン名または仮想ホスト名を指定する必要があります。コンテキストでゲートウェイを排他的に使用するには、**Exclusive** アクセス方法を選択します。
VRF	SSL VPN コンテキストが属する VPN インスタンスを選択します。
Max sessions	SSL VPN コンテキストの SSL VPN セッションの最大数を指定します。この制限に達すると、新しいユーザーは SSL VPN ゲートウェイにアクセスできなくなります。
Login control	アカウントごとの同時ログインの最大数を指定します。 同じアカウントを使用したログイン数が制限に達すると、ユーザーはログインできなくなります。強制ログアウトを有効にすると、ログインが試行されたときにアカウントを使用したログイン数が最大に達した場合に、アイドル時間が最も長いユーザーがログアウトされ、新しいログインが許可されます。
Max connt per session	セッション内の接続数の制限を有効にするか無効にするかを選択します。 セッション内の接続数が制限に達すると、そのセッションへの新しい接続要求は 503 Service Unavailable メッセージで拒否されます。
Session idle timeout	SSL VPN セッションの最大アイドル時間を指定します。SSL VPN セッションのアイドル時間が指定されたアイドルタイムアウト時間を超えると、セッションは終了します。
Idle-cut traffic threshold	アイドルカットトラフィックしきい値をキロバイト単位で指定します。 セッションアイドルタイムアウト時間内に観察されたセッショントラフィックがアイドルカットトラフィックしきい値を下回ると、SSL VPN セッションは切断されます。
Rate limit per session	SSL VPN セッションのある方向のパケット伝送レートが指定された制限を超えると、その方向の後続のパケットはドロップされます。アップリンクトラフィックとは、ユーザーからサーバーに送信されるトラフィックを指します。ダウンリンクトラフィックとは、サーバーからユーザーに送信されるトラフィックを指します。
User login logging	ユーザーログインおよびログアウトイベントのロギングを使用可能にするには、この項目を選択します。

Resource access logging	リソースアクセスのログを有効にするには、この項目を選択します。 リソースアクセスロギングを有効にした後、ロギング方法を選択できます。オプションには、**Log filtering** および **Summary log** があります。ログフィルタ処理が有効な場合、デバイスは、同じユーザーによる同じリソースへの 1 分間のアクセスに対して 1 つのログのみを生成します。ログフィルタ処理が無効な場合、デバイスは、リソースアクセスごとにログを生成します。
Online password change	パスワードの変更をイネーブルにするには、この項目を選択します。SSL VPN ユーザーは、この機能が SSL VPN ユーザービューと SSL VPN コンテキストビューの両方でイネーブルになっている場合にだけ、パスワードを変更できます。
Enable SSL VPN context	SSL VPN コンテキストをイネーブルにするには、この項目を選択します。
Global URL Masking	この項目を選択すると、SSL VPN コンテキスト内のすべての Web リソースに対して URL マスキングがイネーブルになります。
Auto-generate security	SSL VPN コンテキストの作成時に SSL VPN パケットの通過を許可するセキュリティーポリシーをデバイスが自動的に生成できるようにするには、この項目を選択します。

Configure authentication settings

ユーザーが SSL VPN コンテキストにログインするための認証モードには、パスワード認証、証明書認証、および IMC SMS 検証が含まれます。

手順

AuthN Config タブで、認証設定を行います。

表 2 SSL VPN コンテキストの認証設定項目

項目	説明
ISP domain	認証、承認、およびアカウンティングに使用する ISP ドメインを選択します。
Code verification	コード検証を有効にするには、この項目を選択します。 コード検証をイネーブルにした後、ユーザーが SSL VPN Web インターフェースにログインするには、正しい検証コードを入力する必要があります。
Certificate auth	証明書認証を有効にするには、この項目を選択します。 証明書認証を使用するには、SSL サーバーポリシーでクライアント認証がイネーブルになっていることを確認します。SSL VPN ゲートウェイは、SSL VPN クライアントから送信されたデジタル証明書を使用してクライアントを認証します。

Username attribute	SSL VPN ユーザー名として使用する証明書アトリビュートを選択します。デフォルトでは、証明書の[Subject]フィールドの CN アトリビュートがユーザー名として使用されます。
Enable password	パスワード認証を有効にするには、この項目を選択します。 パスワード認証がイネーブルになると、ユーザーはユーザー名とパスワードを使用して SSL VPN Web インターフェースにログインできます。
Certificate and pwdN	証明書とパスワードの両方の認証方法が有効になっている場合は、ユーザーの認証モードを選択します。 ユーザーが証明書とパスワードの両方の認証にパスすることを要求するには、**Use all methods** を選択します。ユーザーが証明書またはパスワードのいずれかの認証にパスすることを要求するには、**Use any method** を選択します
IMC user pwd modify	IMC 認証ユーザーのパスワード変更をイネーブルにするには、この項目を選択します。 IMC サーバーの IP アドレスとポート番号、および IMC サーバーが属する VRF インスタンスを指定する必要があります。 この機能を有効にするには、オンラインパスワード変更機能が有効になっていることを確認します。
IMC SMS verification	IMC SMS 検証を有効にするには、この項目を選択します。 この機能を使用するには、IMC サーバーで SMS メッセージ検証が設定されていることを確認します。SMS メッセージ検証がイネーブルになると、SSL VPN クライアントは、SSL VPN ゲートウェイログイン認証用の検証コードを IMC サーバーから動的に取得できます。
Enable WeChat Work authN	WeChat Work 認証を有効にするには、この項目を選択します。 この機能を使用するには、次のタスクが完了していることを確認します。 WeChat Work 管理プラットフォーム上で企業アプリを設定する。 WeChat Work 管理プラットフォーム上の各 App に対して、App ホームページのリダイレクトリンクと SSL VPN ゲートウェイの信頼できるドメイン名を設定する。 ドメイン名の所有権確認の完了:WeChat Work 管理プラットフォームからドメイン名の所有権確認ファイルをダウンロードし、**Network** > **SSL VPN** > **Global Settings** ページでファイルをアップロードします。 WeChat Work 認証が有効になると、デバイスは WeChat Work のサードパーティからユーザー情報を取得し、そのユーザー情報を認証と承認に使用します。
API server address	WeChat Work API サーバーのアドレスを入力します。 このアドレスが設定されると、デバイスは WeChat Work API サーバーと対話して、WeChat Work サーバーからリダイレクトされたメッセージの受信に関するユーザー情報を取得します。そして、デバイスは取得した情報をユーザー認証と認可に使用します。
Corp ID	WeChat Work 上の企業を一意に識別する企業 ID を入力します。

App secret	App の秘密キーを入力します。 各 App には独立したアクセスキーがあります。データセキュリティのために、App の秘密キーが漏洩しないようにしてください。
AuthN request timeout	SSL VPN ゲートウェイから API サーバーに送信される認証要求のタイムアウト時間を入力します。SSL VPN ゲートウェイが HTTP 要求を送信してからタイムアウト時間内に API サーバーからの応答を受信しない場合、WeChat Work 認証は失敗します。
User ID field name	ユーザーID フィールド名を入力します。SSL VPN ゲートウェイはこの項目を使用して、内部サーバーに送信されるアクセス要求内のユーザー情報を伝送するパラメーターを構築します。
AuthZ policy group field name	許可ポリシーグループ名を入力します。SSL VPN ゲートウェイは、この項目を使用して、WeChat Work API サーバーの応答から許可ポリシーグループ名を取得します。
WeChat open platform URL	WeChat オープンプラットフォームの URL を設定する方法を選択します。オプションには次のものがあります。 **Predefined**: URL はデフォルトで **https://open.weixin.qq.com** に設定され、編集できません。 **User-defined**: 必要に応じて URL を入力できます。 この項目を設定すると、内部サーバーがクライアント認証を再度要求したときに、クライアントは WeChat オープンプラットフォームに直接アクセスして認証を完了できます。

Configure URI ACL

1 つの SSL VPN コンテキストに複数の URI ACL を作成できます。
URI ACL は、リソースへのアクセスを許可または拒否する一連のルールです。URI ACL には複数のルールを追加できます。デバイスは、ルール ID の昇順でパケットをルールと照合します。一致するルールが見つかると、照合プロセスは停止します。

URL ACL は、次の目的で使用できます。

URL 項目で指定された URL の下のリソースをフィルタします。
SSL VPN リソースグループ内の Web、TCP、および IP アクセス要求をフィルタリングします。

手順

1. **URI ACL** タブで、**Create** をクリックします。
2.表示された **Add URI ACL** ページで、ACL 名を入力します。
3. **URI ACL Resources** セクションで、**Create** をクリックします。
4.表示された **Add URI ACL Rule** ページで、URI ACL ルールを作成します。

表 3 ルールの構成項目

項目	説明
Rule ID	ルール ID を入力します。
Action	一致するパケットのアクションを選択します。オプションには、**Permit** と **Deny** があります。
URI pattern	プロトコルとホストが必要な protocol://host:port/path,の形式で URI パターンを入力します。

5. **OK** をクリックします。
   規則が **Add URI ACL** ページに表示されます。
6.OK をクリックします。
   URI ACL が **URI ACL** ページに表示されます。
7. **Next** をクリックします。

Configure access services

Web アクセスサービス、TCP アクセスサービス、および IP アクセスサービスのアクセスリソースを設定できます。

Configure the Web access service

Web アクセスサービスの設定ページで、次のタスクを実行します。

SSL VPN ゲートウェイが内部 HTTPS サーバーにアクセスするために使用する SSL クライアントポリシーを選択します。
デフォルトでは、SSL VPN ゲートウェイはデフォルトの SSL クライアントポリシーを使用して内部 HTTPS サーバーにアクセスします。デフォルトの SSL クライアントポリシーでは、暗号スイート **rsa_rc4_128_md5** が使用されます。
内部 Web リソースの URL 項目を作成します。
URL 項目を作成します。
URL 項目の Web リソースの URL を指定します。
既存の URI ACL を選択して、指定した URL の Web リソースをフィルタ処理します。
リソース URL のマッピングタイプを選択します。オプションは、**Normal mapping** (デフォルト)、**Domain mapping** および **Port mapping** です。

SSL VPN ゲートウェイは、クライアントに送信する前にリソース URL を書き換えます。URL マッピングタイプは、ゲートウェイが URL を書き換える方法を決定します。
次に、ユーザーが SSL VPN ゲートウェイの背後にある内部リソース URL **http://www.server.com:8080** (名前 **gw**、ドメイン名 **https://www.gateway.com:4430**,、および IP アドレス **1.1.1.1**)にアクセスする場合の URL マッピングの動作例を示します。

Normal mapping: クライアントに返されるリソース URL は、**https://www.gateway.com:4430/_proxy2/http/8080/www.server.com** に書き換えられます。通常のマッピングでは、URL の書き換えミスや書き換えエラーなどの問題が発生し、SSL VPN クライアントが内部リソースにアクセスできなくなることがあります。ドメインマッピングまたは URL マッピングをベストプラクティスとして使用してください。

Domain mapping : **Domain Mapping** を選択すると、**Domain Name** アイテムが表示されます。クライアントに戻されるリソース URL は、**https://mapped domain name:4430** に書き換えられます。ここで、***mapped domain name*** は、**Domain Name** アイテムに入力したドメイン名です。

Port mapping: Port mapping を選択すると、**Gateway name** および **Virtual host** 項目が表示されます。仮想ホスト名はオプションです。

Gateway name 項目に **gw2** と入力し、仮想ホスト名を入力しない場合、リソース URL は **https://2.2.2.2:4430**,に書き換えられます。ここで、2.2.2.2 と 4430 は SSL VPN ゲートウェイ **gw2** の IP アドレスとポート番号です。

ゲートウェイ名の項目に **gw** と入力し、**Virtual host** 項目に **vhosta** と入力すると、リソース URL は **https://vhosta:4430** に書き換えられます。
URL リストを作成し、その URL リストに URL 項目を割り当てます。
URL リストはリソースグループに割り当てることができます。AAA サーバーがユーザーにリソースグループの使用を許可すると、ユーザーはリソースグループ内の URL リストによって提供される Web リソースにアクセスできます。

Web アクセスサービスを構成するには:

Access services タブで、**Web access** を選択し、**Next** をクリックします。
Web access resources セクションで、**URL Items** 領域の **Create** をクリックします。
開いたページで、URL 項目を構成し、**OK** をクリックします。

表 4 URL 項目の構成項目

項目	説明
URL item name	URL 項目名を入力します。
URL	URL 項目に URL を入力します。
URI ACL	フィルタリング基準として URI ACL を選択します。
Mapping type	マッピングタイプを選択します。オプションには、**Normal mapping**, **Domain mapping**, 及び **Port mapping** があります。
Enable URL masking	指定した URL のマスキングを有効にするかどうかを選択します。 この機能をイネーブルにすると、ユーザーはアクセスした内部サーバーの実際のアドレスを表示できなくなります。
Single sign-on	SSO ログインを有効にするかどうかを選択します。 この機能を有効にすると、ユーザーは 1 組のログイン資格情報を使用して複数の信頼されたシステムにアクセスできます。
SSO mode	SSO ログインモードを選択します。次のオプションがあります。 **Basic access request**: ログインパラメータの設定が必要です。 **Auto-build access request**: 要求方式、符号化モード、要求パラメーター、および暗号化ファイルのアップロードを設定する必要があります。
Login parameters	この項目は、**SSO mode** フィールドで **Basic access request** を選択した場合にのみ使用できます。 ログインパラメータを取得する方法を選択します。オプションは次のとおりです。 **Use SSL VPN login username and password**: SSO ログインに SSL VPN ログインユーザー名とパスワードを使用します。 **Use custom username and password**: SSO ログインにカスタムユーザー名とパスワードを使用します。カスタムユーザー名とパスワードは、SSL VPN Web インターフェースで設定されます。
Request method	この項目は、**SSO mode** フィールドで **Auto-build access request** を選択した場合にのみ使用できます。 要求メソッドを選択します。オプションには、**GET** および **POST** があります。
Encoding mode	この項目は、**SSO mode** フィールドで **Auto-build access request** を選択した場合にのみ使用できます。 エンコード方法を選択します。オプションには、**GB18030** および **UTF-8** があります。
Request parameters	この項目は、**SSO mode** フィールドで **Auto-build access request** を選択した場合にのみ使用できます。

	要求パラメータ(属性名と値)を追加するには、このフィールドで **Add** をクリックし、表示されたダイアログボックスで次の項目を設定します。 **Parameter name**： パラメーター名を入力します。パラメーター名は、SSO ログイン要求に使用される属性名です。 **Type**： パラメータタイプを選択します。SSO ログインに使用されるパラメーター値は、パラメータタイプに従って抽出された実際の値です。次のオプションがあります: **Login name**:SSL VPN ログインユーザー名を SSO 要求パラメーターの値として使用します。 **Login password**:SSL VPN ログインパスワードを SSO 要求パラメーターの値として使用します。 **Certificate subject**: ト証明書のタイトルを SSO 要求パラメーターの値として使用します。 **Certificate serial number**: 証明書のシリアル番号を SSO 要求パラメーターの値として使用します。 **Certificate fingerprint**: ト証明書フィンガープリントを SSO 要求パラメーターの値として使用します。 **Phone number**:SSO 要求パラメーターの値として携帯電話番号を使用します。 **User group**:ユーザーグループ名を SSO 要求パラメーターの値として使用します。 **Custom name**:カスタマイズされたユーザー名を SSO 要求パラメーターの値として使用します。 **Custom password**:カスタマイズしたパスワードを SSO 要求パラメーターの値として使用します。 **Custom**: **Parameter value** フィールドに SSO 要求パラメーターの実際のパラメーター値を指定します。 **Encrypt parameter value**:パラメーター値の暗号化をイネーブルにするかどうかを選択します。
Set encryption file	この項目は、**SSO mode** フィールドで **Auto-build access request** を選択した場合にのみ使用できます。 パラメーター値の暗号化用の暗号化ファイルをアップロードします。暗号化ファイルは.js ファイルである必要があり、200 KB を超えることはできません。 暗号化ファイルをアップロードするには、**Select file** をクリックして.js ファイルを選択し、**Upload** をクリックします。 現在の暗号化ファイルの使用をキャンセルするには、[暗号化のキャンセル]をクリックします。

Current encryption file	現在の暗号化ファイルを表示します。

7 **URL List** 領域で **Current encryption file** をクリックします。
8.開いたページで、URL リストを設定し、**OK** をクリックします。

表 5 URL リストの構成項目

項目	説明
URL list name	URL リスト名を入力します。
Heading	URL リストの見出しを入力します。
URL entry list	URL リストに追加する URL 項目を選択します。

Configure the TCP access service

TCP access service configuration ページで、次の作業を実行します。

1.ポート転送項目を作成します。

ポート転送項目は、内部サーバーで提供される TCP サービス(Telnet、SSH、POP3 など)を SSL VPN クライアント上のローカルアドレスおよびポート番号にマッピングします。リモートユーザーは、ローカルアドレスおよびポート番号を使用して TCP サービスにアクセスできます。

たとえば、ポート転送項目を設定して、クライアントがサーバー192.168.0.213 のポート 80 で提供される HTTP サービスに IP アドレス 127.0.0.1 とポート 80 を介してアクセスできるようにすることができます。

ポート転送項目を次のように設定します。

ポート転送項目の名前を指定します。

クライアントホストアドレス、クライアントポート番号、サーバードレス、およびサーバーポート番号を指定します。

ポート転送項目の説明を設定します。

必要に応じて、ポート転送項目のリソースリンクを指定します。

ポート転送項目のリソースリンクを設定すると、ポート転送項目名が SSL VPN Web ページにリンクとして表示されます。リンクをクリックすると、リソースに直接アクセスできます。

ポート転送リストを作成します。

ポート転送リストの名前を指定します。

ポート転送項目をポート転送リストに追加します。

ポート転送リストはリソースグループに割り当てることができます。AAA サーバーがユーザーにリソースグループの使用を許可すると、ユーザーはリソースグループ内のポート転送リストによって提供される TCP サービスにアクセスできます。

TCP アクセスサービスを設定するには、次の手順を実行します。

Access services タブで、**TCP access** を選択し、**Next** をクリックします。
TCP access resources セクションの **Port Forwarding Item** 領域で、**Create** をクリックします。
開いたページで、ポート転送項目を構成し、**OK** をクリックします。

表 6 ポート転送項目の構成項目

項目	説明
Name	ポート転送項目名を入力します。
Client host	内部サーバー上の TCP サービスがマッピングされる SSL VPN クライアントのローカルアドレスまたはホスト名を指定します。
Client port	内部サーバー上の TCP サービスがマッピングされる SSL VPN クライアントのローカルポートを指定します。
Server address	TCP サービスを提供する内部サーバーの IP アドレスまたは FQDN を指定します。
Server port	TCP サービスを提供する内部サーバーのポートを指定します。
Description	ポート転送項目の説明を入力します。
Resource link	ポート転送項目のリソースリンクを指定します。SSL VPN ユーザーは、SSL VPN Web インターフェースのリソースリンクをクリックして、リソースにアクセスできます。

Port Forwarding List 領域で **Create** をクリックします。
開いたページで、ポート転送リストを設定し、**OK** をクリックします。

表 7 ポート転送リストの構成項目

項目	説明
Port forwarding list	ポート転送リスト名を入力します。
Port forwarding items	ポート転送リストに追加するポート転送項目を指定します。

Configure the IP access service

IP アクセスサービスの設定ページで、次の作業を実行します。

IP アクセス用の SSL VPN AC インターフェースを指定します。
IP アクセスアドレスプールを指定します。
ユーザーが認証に合格すると、SSL VPN ゲートウェイは、指定されたアドレスプールからユーザーの VNIC に IP アドレスを割り当てます。
ルートリストを設定します。
ルートリストには、SSL VPN クライアントに発行されるルーティングエントリが含まれています。
ルートリストには、次のタイプのルーティングエントリを設定できます。
Included route: インクルードされたルーティングエントリと一致するクライアントパケットは、クライアントホストの VNIC を介して SSL VPN ゲートウェイに転送されます。
Excluded route: 除外されたルーティングエントリと一致するクライアントパケットは、SSL VPN ゲートウェイに転送されません。
ルートリストはリソースグループに割り当てることができます。AAA サーバーがユーザーにリソースグループの使用を許可すると、SSL VPN ゲートウェイはリソースグループのルートリスト内のルーティングエントリをユーザーに発行します。これにより、ユーザーはリソースグループ内のルートリストによって提供される IP リソースにアクセスできるようになります。
Web ログイン後に IP アクセスクライアントの自動起動をイネーブルにするには、**Start IP access client** を選択します。ユーザーが Web ブラウザを介して SSL VPN ゲートウェイにログインすると、ユーザーホスト上の IP アクセスクライアントが自動的にゲートウェイに接続します。IP アクセスクライアントソフトウェアがインストールされていない場合は、ソフトウェアのインストールを求めるプロンプトが表示されます。IP アクセスクライアントが SSL VPN ゲートウェイに正しく接続するには、SSL VPN ゲートウェイに IP アクセスリソースが設定されていることを確認します。
アクセス可能なリソースを IP アクセスユーザーに自動的にプッシュするには、**Push Web resources** を選択します。ユーザーが IP アクセスクライアントを介して SSL VPN ゲートウェイにログインすると、SSL VPN ゲートウェイはアクセス可能な SSL VPN リソースを Web ページを介して自動的にユーザーにプッシュします。Web ページを介して SSL VPN リソースを正常にプッシュするには、SSL VPN リソースが SSL VPN ゲートウェイに設定されていることを確認します。
アップストリームトラフィックおよびダウンストリームトラフィックのレート制限を設定します。レート制限を超えると、IP アクセスパケットはドロップされます。
ユーザーと IP アドレスのバインディングを作成します。
次のいずれかの方法で、SSL VPN ユーザーに IP アドレスをバインドします。
IP アドレスの範囲をユーザーにバインドします。
SSL VPN ゲートウェイをイネーブルにして、IP アクセスアドレスプール内の指定した数のフリーアドレスをユーザーに自動的にバインドします。

ユーザーが IP アクセスモードで SSL VPN ゲートウェイにアクセスすると、SSL VPN ゲートウェイはバインドされた IP アドレスをユーザーに割り当てます。指定された IP アドレス範囲内の IP アドレスが別のユーザーに割り当てられている場合、SSL VPN ゲートウェイはそのユーザーの接続を終了し、IP アドレスを解放します。

IP アクセスサービスを設定するには、次の手順を実行します。

Access services タブで、**IP access** を選択し、**Next** をクリックします。
IP access ページで、IP アクセスサービスの基本設定を行います。

表 8 IP アクセスサービスの基本的な構成項目

項目	説明
SSL VPN AC interface	IP アクセス用の SSL VPN AC インターフェースを選択します。
IP access address pool	SSL VPN ゲートウェイが IP アドレスをクライアントに割り当てるアドレスプールを選択します。
Mask length	アドレスプールのマスク長を指定します。
Primary DNS server	内部プライマリ DNS サーバーの IP アドレスを指定します。
Secondary DNS server	内部セカンダリ DNS サーバーの IP アドレスを指定します。
Primary WINS server	内部プライマリ WINS サーバーの IP アドレスを指定します。
Secondary WINS server	内部セカンダリ WINS サーバーの IP アドレスを指定します。
Keepalive interval	キープアライブインターバルを指定します。クライアントは SSL VPN ゲートウェイにキープアライブメッセージを送信して、クライアント間のセッションを維持します。
Start IP access client	Web ログイン後の IP アクセスクライアントの自動起動を有効にするには、この項目を選択します。ユーザーが Web ブラウザから SSL VPN ゲートウェイにログインすると、ユーザーホスト上の IP アクセスクライアントが自動的に起動し、ゲートウェイに接続します。
Push Web resources	この項目を選択すると、ユーザーが IP アクセスクライアントを介して SSL VPN ゲートウェイにログインした後、Web 経由でアクセス可能なリソースをユーザーに自動的にプッシュできます。
Rate limit	アップストリームトラフィックおよびダウンストリームトラフィックのレート制限を指定します。

	アップストリームトラフィックとは、ユーザーからサーバーに送信されるトラフィックを指します。ダウンストリームトラフィックとは、サーバーからユーザーに送信されるトラフィックを指します。
Packet drop logging	IP アクセスパケットドロップイベントのロギングをイネーブルにするには、この項目を選択します。SSL VPN IP アクセスユーザーのパケットがドロップされると、SSL VPN ゲートウェイによってログが生成されます。
IP connt close logging	IP アクセス接続のクローズイベントのロギングをイネーブルにするには、この項目を選択します。SSL VPN IP アクセスユーザーに対して確立された接続がクローズされると、SSL VPN ゲートウェイによってログが生成されます。
IP addr asgmt and release logging	IP アドレスの割り当ておよび解放イベントのロギングをイネーブルにするには、この項目を選択します。SSL VPN ゲートウェイは、SSL VPN クライアントの VNIC との間で IP アドレスの割り当てまたは解放を行うと、ログを生成します。

IP access resources セクションで、**IP Access Resources** 領域の **Create** をクリックします。
表示されたページで、ルートリスト名を入力します。
Route entries セクションで、**Create** をクリックします。
開いたページで、ルートエントリを設定します。

表 9 ルートエントリの設定項目

項目	説明
Type	ルートエントリタイプを選択します。次のオプションがあります: **Included route** ト: ルートエントリをインクルードルートとしてルートリストに追加します。 **Excluded route**: 除外ルートとしてルートエントリをルートリストに追加します。 SSL VPN ゲートウェイはログインクライアントにルートリストを発行します。クライアントはルートをローカルルーティングテーブルに追加します。含まれているルートと一致するトラフィックは SSL VPN ゲートウェイに送信されます。除外されているルートと一致するトラフィックは SSL VPN ゲートウェイに送信されません。
Subnet address	ルートエントリの宛先アドレスを指定します。インクルードルートを構成するには、ルートエントリの宛先ネットワークは、内部サーバーが存在するネットワークである必要があります。
Mask length	サブネットマスクの長さを指定します。

OK をクリックします。
ルートエントリが **Route entries** セクションに表示されます。
OK をクリックします。

ルートリストが **IP Access Resources** 領域に表示されます。

URL-to-IP Address Binding 領域で、**Create** をクリックします。

開いたページで、ユーザーと IP アドレスのバインディングを設定します。

表 10 ユーザーから IP アドレスへのバインドの構成項目

項目	説明
Username	SSL VPN ユーザー名を入力します。
Auto binding	ユーザーと IP アドレスの自動バインドを有効にするには、この項目を選択します。 この機能を使用すると、SSL VPN ゲートウェイは、IP アクセスアドレスプール内の指定した数のフリーアドレスをユーザーに自動的にバインドできます。
Number of IP	この項目は、自動バインドが有効な場合にのみ使用できます。 バインドする IP アドレスの数を指定します。
Start IP address	バインドする IP アドレスの範囲の開始 IP アドレスを指定します。
End IP address	バインドする IP アドレス範囲の終了 IP アドレスを指定します。

Configure the BYOD access service

Access services タブで、**BYOD access** を選択し、**Next** をクリックします。

BYOD access ページで、次の項目を設定します。

EMO サーバーのアドレスとポート番号。

メッセージサーバーのアドレスとポート番号。

Next をクリックします。

Configure a shortcut list

SSL VPN Web ページで頻繁にアクセスされる内部リソースにすばやくアクセスできるようにするには、これらのリソースのショートカットを設定し、ショートカットリストにショートカットを追加します。

1 つの SSL VPN コンテキストに複数のショートカットリストを作成できます。

リソースグループを設定するときに、グループにショートカットリストを割り当てることができます。ショートカットリストのショートカットは、リソースグループの使用を許可されたユーザーの SSL VPN Web ページに表示されます。ユーザーはショートカットをクリックして、関連付けられたリソースに直接アクセスできます。

手順

Shortcuts タブで、**Shortcut** 領域の **Create** をクリックします。
開いたページで、ショートカットを構成し、**OK** をクリックします。

表 11 ショートカットの構成項目

項目	説明
Shortcut name	ショートカットの名前を入力します。
Description	ショートカットの説明を入力します。
Resource address	ショートカットのリソースアドレスを指定します。SSL VPN ユーザーは、SSL VPN Web インターフェースのリンクをクリックしてリソースにアクセスできます。リソースアドレスは、次のいずれかの方法で構成できます。 **url**('url-value')形式でリソースリンクを入力します。url-value 引数には、対応するリソースを指定します。url-value の完全な形式は、protocol://hostname またはアドレス(ポート番号/リソースパス)です。 **app**('app-value')の形式でアプリケーションのパスを入力します。app-value 引数には、対応するリソースを指定します。app-value の完全な形式は、絶対パスまたは環境変数です。たとえば、c:¥windows¥system 32¥notepad++.exe のようになります。 リソースへのアクセスを提供するために、リソースの実行可能 JavaScript を入力します。

Shortcut List 領域で、**Create** をクリックします。
開いたページで、ショートカットリストを構成し、**OK** をクリックします。

表 12 ショートカットリストの構成アイテム

項目	説明
List name	ショートカットリストの名前を入力します。
Select shortcuts	ショートカットを選択してショートカットリストに追加します。

Next をクリックします。

Configure a resource group

リソースグループは、SSL VPN ユーザーがアクセスできる Web リソース、TCP リソース、および IP リソ

ースを定義します。また、リソースグループで ACL を使用して、ユーザーアクセスをより具体的に制御することもできます。

手順

Resource groups タブで、**Resource groups** セクションの **Create** をクリックします。
開いたページで、リソースグループの基本設定を構成します。

表 13 基本的なリソースグループ設定の構成項目

項目	説明
Resource group name	リソースグループの名前を入力します。
Instant access resource after login	ユーザーが SSL VPN ゲートウェイにログインした直後に開くリソースを選択します。ユーザーは、リソースにアクセスするために SSL VPN リソースページでリソースを選択する必要はありません。
Shortcut list	リソースグループのショートカットリストを選択します。

Web access セクションで、アクセス可能な Web リソースを構成します。
1 つまたは複数の URL リストを選択します。
IPv4 Web アクセス要求をフィルタリングする IPv4 ACL を指定します。
IPv6 Web アクセス要求をフィルタリングするための IPv6 ACL を指定します。
Web アクセス要求をフィルタリングするための URI ACL を指定します。
TCP access セクションで、アクセス可能な TCP リソースを設定します。
TCP ポート転送リストを選択します。
IPv4 ACL を指定して、IPv4 TCP アクセス要求をフィルタリングします。
IPv6 ACL を指定して、IPv6 TCP アクセス要求をフィルタリングします。
TCP アクセス要求をフィルタリングするための URI ACL を指定します。
IP access セクションで、アクセス可能な IP リソースを設定します。

表 14 IP アクセスの構成項目

項目	説明
Force all traffic to SSL VPN	ローカルルーティングテーブルで一致するルートが見つからないすべてのクライアントパケットを強制的に SSL VPN ゲートウェイに送信するには、この項目を選択します。 SSL VPN ゲートウェイは、SSL VPN クライアントにデフォルトルートを発行します。デフォルトルートは、出力インターフェースとして VNIC を使用し、クライアント上のすべてのデフォルトルートの中で最も高いプライオリティを持ちます。ルーティングテーブルにない

	宛先へのパケットは、VNIC を介して SSL VPN ゲートウェイに送信されます。SSL VPN ゲートウェイは、SSL VPN クライアントをリアルタイムで監視します。クライアントがデフォルトルートを削除したり、プライオリティの高いデフォルトルートを追加したりすることはできません。
Issue routes to client	リスト内のルートをクライアントに発行するには、ルートリストを選択します。または、**Host IPv4 address** を選択して、クライアントに発行するルーティングエントリを設定します。
IP access address pool	SSL VPN ゲートウェイがリソースグループの使用を許可された IP アクセスユーザーに IP アドレスを割り当てるアドレスプールを指定します。 許可されたリソースグループに IP アクセスアドレスプールが指定されていない場合、SSL VPN ゲートウェイは、SSL VPN コンテキストに指定されたアドレスプールの IP アドレスを IP アクセスユーザーに割り当てます。 ユーザーのアドレスプールに使用可能なアドレスがない場合、ユーザーの IP アクセス要求は拒否されます。
IPv4 ACL	IPv4 ACL を指定して、IPv4 TCP アクセス要求をフィルタリングします。
IPv6 ACL	IPv6 ACL を指定して、IPv6 TCP アクセス要求をフィルタリングします。
URI ACL	TCP アクセス要求をフィルタリングするための URI ACL を指定します。

OK をクリックします。

新しく作成されたリソースグループが **Resource groups** ページに表示されます。

Finish をクリックします。

よくある質問

SSL VPN でリソース認可設定を変更した後、設定がすぐに有効になりません。なぜですか。

SSL VPN ゲートウェイは動的認可をサポートしません。表 15 は、SSL VPN で変更されたリソース認可設定がいつどのように有効になるかを示しています。

表 15 変更された許可設定が有効になる方法とタイミング

変更されたアイテム	変更がいつどのように有効になるか
リモートサーバーへの許可	変更は新規ユーザーにのみ有効です。すでにログインしているユーザーは影響を受けません。

リソースグループ内の ACL または ACL ルール	IP、TCP、および Web アクセスユーザーの場合、変更はすぐに有効になります。
アクセス可能な Web リソース	変更は、ユーザーが SSL VPN Web ページをリフレッシュした後に有効になります。
アクセス可能な TCP リソース	変更は、ユーザーが TCP アクセスクライアントソフトウェアを再起動した後に有効になります。
IP アクセスサービス用に設定されたルーティングエントリ、DNS サーバードレス、および WINS サーバードレス	変更はただちに有効になります。

SSL VPN ユーザーが SSL VPN ゲートウェイにログインするには、証明書認証を渡す必要がありますか。

ユーザーが SSL VPN ゲートウェイにログインするために証明書認証を通過する必要があるかどうかは、次の設定によって異なります。

SSL VPN ゲートウェイに関連付けられた SSL VPN コンテキストで証明書認証をイネーブルにするかどうか。
SSL VPN ゲートウェイで使用される SSL サーバーポリシーで設定されている証明書認証方式のタイプ。

表 16 は、ユーザーが SSL VPN ゲートウェイに接続するときに使用する可能性のある証明書認証方式を示しています。

表 16 証明書認証方式

認証方式	説明
Certificate authentication disabled	Web ブラウザを介して SSL VPN ゲートウェイに接続する場合、ユーザーは認証用の証明書を選択する必要はありません。
Mandatory certificate authentication enabled	Web ブラウザから SSL VPN ゲートウェイに接続する際に、認証用の証明書の選択を要求されますが、証明書を持っていない場合は接続要求が拒否されます。
Optional certificate authentication enabled	Web ブラウザから SSL VPN ゲートウェイにアクセスする場合、認証用の証明書を選択するように求められます。SSL VPN ゲートウェイへの接続は、次のいずれかの場合に確立されます。 ユーザーは証明書を選択し、ID 認証を渡します。 ユーザーは、証明書を選択せずに接続要求を続行することを選択します。

ユーザーが証明書認証を通過して SSL VPN ゲートウェイにログインできるようにする場合は、次の要件が満たされていることを確認します。

証明書認証は、SSL VPN ゲートウェイに関連付けられた SSL VPN コンテキストでイネーブルになります。
必須またはオプションの SSL クライアント認証は、SSL VPN ゲートウェイで使用される SSL サーバーポリシーでイネーブルになっています。

クライアント証明書を受信すると、SSL VPN ゲートウェイは証明書の CN フィールドからユーザー名を抽出し、そのユーザー名を AAA サーバーに送信します。抽出されたユーザー名がローカル AAA サーバーに存在する場合にだけ、ユーザーは認証を通過します。
必須の証明書認証は、Web ユーザーおよび IP アクセスユーザーに対してだけサポートされます。TCP アクセスユーザーおよびモバイルクライアントユーザーが SSL VPN ゲートウェイに正常にアクセスするには、オプションの SSL クライアント認証をイネーブルにする必要があります。

Routing table

Introduction

ルーティングテーブル情報(簡単なルーティングテーブル情報やルート統計情報など)を表示できます。

Static routing

Introduction

スタティックルートは手動で設定されます。ネットワークのトポロジが単純な場合は、ネットワークが正しく動作するようにスタティックルートを設定するだけで済みます。
スタティックルートは、ネットワークトポロジの変更に適応できません。ネットワークで障害またはトポロジの変更が発生した場合、ネットワーク管理者はスタティックルートを手動で変更する必要があります。
デフォルトルートは、ルーティングテーブル内の特定のルーティングエントリと一致しないパケットを転送するために使用されます。デフォルト IPv4 ルートを宛先アドレス 0.0.0.0/0 で設定し、デフォルト IPv6 ルートを宛先アドレス::/0 で設定できます。

Policy-based routing

このヘルプには、次のトピックがあります。

Introduction

About PBR

Policy

Node

PBR and Track

Introduction

About PBR

Policy-Based Routing(PBR)は、ユーザー定義のポリシーを使用してパケットをルーティングします。ポリシーでは、ACL、パケット長、サービスオブジェクトグループ、アプリケーショングループなどの特定の基準と一致するパケットのパラメーターを指定できます。パラメーターには、ネクストホップ、出力インターフェース、デフォルトネクストホップ、およびデフォルト出力インターフェースが含まれます。

Policy

ポリシーには、一致基準と、一致するパケットに対して実行されるアクションが含まれます。ポリシーには、次のように 1 つまたは複数のノードを含めることができます。

各ノードはノード番号で識別されます。ノード番号が小さいほど優先度が高くなります。
ノードには、**if-match** 句と **apply** 句が含まれます。**if-match** 句は一致基準を指定し、**apply** 句はアクションを指定します。
ノードには、**permit** または **deny** の一致モードがあります。

ローカルで生成されたパケットの転送をガイドするローカル PBR のポリシーを指定したり、インターフェースで受信したパケットの転送をガイドするポリシーをインターフェースに適用したりできます。
ポリシーは、パケットとノードを優先順位に従って比較します。パケットがノードの基準に一致する場合は、ノードのアクションによって処理されます。一致しない場合は、次のノードに移動して一致します。パケットがどのノードの基準にも一致しない場合、デバイスはルーティングテーブルの検索を実行します。

Node

Match criteria

ACL、サービスオブジェクトグループ、アプリケーショングループ、またはパケット長の一致基準を設定して、パケットを一致させることができます。
ノードと一致するには、パケットがノードのすべてのタイプの一致基準と一致する必要があります。
サポートされる一致基準は、デバイスモデルによって異なります。

Actions

現在のノードで障害が発生した場合に、パケットを次のノードと比較します。このアクションは、指定されたアクション(VPN インスタンス、ネクストホップ、出力インターフェース、デフォルトネクストホップ、およびデフォルト出力インターフェースの設定)が設定されていないか、無効になった場合に実行されます。たとえば、指定されたネクストホップが到達不能である場合、指定された出力インターフェースがダウンしている場合、または指定された VPN インスタンスでパケットを転送できない場合です。
IP precedence を設定します。
IP ヘッダーの DF ビットを設定します。
一致するパケットに使用できる転送テーブルを指定します。
トラックエントリに関連付けられたネクストホップおよびデフォルトネクストホップを設定します。ネクストホップを有効にするには、ネクストホップを直接接続する必要があることを指定できます。
トラックエントリに関連付けられた出力インターフェースとデフォルトの出力インターフェースを設定します。

PBR and Track

PBR は Track 機能と連動して、アクションの可用性ステータスを追跡対象オブジェクトのリンクステータスに動的に適応させることができます。

トラッキング対象オブジェクトは、ネクストホップ、出力インターフェース、デフォルトネクストホップ、またはデフォルト出力インターフェースです。このアクションは、トラックエントリのステータスが **Positive** または **NotReady** に変更された場合にだけ有効です。

OSPF

このヘルプには、次のトピックがあります。

Introduction

OSPF instances

OSPF areas

OSPF neighbors

Configure OSPF

Configure an OSPF instance

Configure an OSPFv2 area

Configure an OSPFv3 area

Introduction

Open Shortest Path First(OSPF)は、プロトコル番号 89 を使用してデータを IP パケットに直接カプセル化するリンクステート IGP です。
OSPF バージョン 2 および OSPF バージョン 3 がサポートされています。OSPF バージョン 2 は IPv4 に使用されます。OSPF バージョン 3 は IPv6 に使用されます。

OSPF instances

OSPF を有効にするには、まず OSPF インスタンスを作成し、そのインスタンスに関連付けられたエリアを指定し、そのエリアのネットワークセグメントとインターフェースを指定する必要があります。エリアのネットワークに接続されたインターフェースは、そのエリアで OSPF を実行します。OSPF は、インターフェースの直接ルートをアドバタイズします。
OSPF は複数のインスタンスをサポートします。OSPF インスタンスに異なる名前を指定することで、デバイス上の複数の OSPF インスタンスを有効にできます。OSPF インスタンス名はローカルで意味があります。2 つのデバイスは、インスタンス名が異なっていても、相互にパケットを交換できます。

OSPF areas

OSPF は AS を複数のエリアに分割します。各エリアはエリア ID で識別されます。エリア間の境界はリンクではなくデバイスです。デバイスは異なるエリアに属することができますが、ネットワークセグメント(また

はリンク)は 1 つのエリアにしか存在できません。OSPF インターフェースごとにエリアを指定する必要があります。ABR にルート集約を設定して、他のエリアにアドバタイズされる LSA の数を減らし、トポロジ変更の影響を最小限に抑えることができます。

OSPF neighbors

OSPF ネットワークでは、2 つのデバイスがネイバー関係を確立した後にのみリンクステート情報を交換できます。OSPF インターフェースから hello パケットを受信すると、デバイスはパケット内のパラメーター(ルータ ID、エリア ID、認証情報、サブネットマスク、hello 間隔など)をチェックします。パラメーターが自身のパラメーターと一致する場合、受信デバイスは送信デバイスを OSPF ネイバーと見なします。

Configure OSPF

Configure OSPF instance

Network タブをクリックします。
ナビゲーションペインで、**Routing** > **OSPF** を選択します。
OSPF Instance タブをクリックします。
Create をクリックします。
OSPF インスタンスパラメータを設定します。

表 1 OSPF インスタンスの構成項目

項目	説明
Version	OSPF バージョンを選択します。オプションには、**OSPFv2** および **OSPFv3** があります。
Instance name	OSPF インスタンスの名前を入力します。同じバージョンの OSPF インスタンスに同じ名前を付けることはできません。
VRF	OSPF インスタンスの VPN インスタンスを選択します。
Router ID	デバイスのルータ ID を設定します。

OK をクリックします。
OSPF インスタンスが OSPF インスタンスページに表示されます。

Configure OSPFv2 area

Network タブをクリックします。

ナビゲーションペインで、**Routing** > **OSPF** を選択します。

OSPF Instance タブをクリックします。

OSPFv2 インスタンスの **Number of OSPF areas** カラムの番号をクリックします。

Create をクリックします。

OSPFv2 エリアパラメータを設定します。

表 2 OSPFv2 エリアの設定項目

項目	説明
Instance name	OSPFv2 エリアが属する OSPFv2 インスタンスの名前。
Area ID	エリア ID を設定します。
Area type	エリアタイプを選択します。
Subnet	エリアのネットワークセグメントを指定します。ネットワークセグメントは 1 つのエリアにのみ存在できます。ネットワークセグメントは 1 つずつ指定することも、デバイスのすべてのネットワークセグメントを指定することもできます。
Interface	エリアにインターフェースを追加し、インターフェースパラメータを設定します。

OK をクリックします。

OSPFv2 エリアは、OSPFv2 エリアページに表示されます。

OSPF Instance タブをクリックしてから、OSPFv2 インスタンスの **Number of redistributed routes** カラムの数値をクリックします。

Create をクリックします。

OSPFv2 再配布ルートパラメータを設定します。

表 3 OSPFv2 再配布ルートの設定項目

項目	説明
Protocol type	指定されたルーティングプロトコルからルートを再配布およびアドバタイズします。
Instance name	指定されたルーティングプロトコルのインスタンス ID。

OK をクリックします。

Configure OSPFv3 area

Network タブをクリックします。

ナビゲーションペインで、**Routing** > **OSPF** を選択します。

OSPF Instance タブをクリックします。

OSPFv3 インスタンスの **Number of OSPF areas** カラムの番号をクリックします。

Create をクリックします。

OSPFv3 エリアパラメータを設定します。

表 4:OSPFv3 エリアの設定項目

項目	説明
Area type	エリアタイプを選択します。
Area ID	エリア ID を設定します。

OK をクリックします。

OSPFv3 エリアは、OSPFv3 エリアページに表示されます。

OSPF Instance タブをクリックし、次に OSPFv3 インスタンスの **Number of OSPF interfaces** カラムの番号をクリックします。

Create をクリックします。

OSPFv3 インターフェースパラメータを設定します。

表 5 OSPFv3 インターフェースの設定項目

項目	説明
Area ID	インターフェースが属する OSPFv3 エリアを指定します。
Interface name	インターフェースを選択します。
Interface instance ID	インターフェースインスタンス ID を設定します。インターフェースのさまざまなインターフェースインスタンスを、さまざまな OSPFv3 インスタンスに追加できます。

OK をクリックします。

OSPFv3 インターフェースページにインターフェースが表示されます。

BGP

Introduction

Border Gateway Protocol(BGP)は、Exterior Gateway Protocol(EGP)です。AS 内で実行される場合は Internal BGP(IBGPP)と呼ばれ、AS 間で実行される場合は External BGP(EBGP)と呼ばれます。AS とは、同じルーティングポリシーを使用し、同じ管理下で動作するルータのグループを指します。
現在使用されているバージョンは BGP-4 です。これは Internet Service Provider(ISP)によって広く使用されています。

Basic concepts

BGP speaker and BGP peer

BGP を実行するルータは BGP スピーカです。BGP スピーカは、他の BGP スピーカとのピア関係を確立して、TCP 接続を介してルーティング情報を交換します。
BGP ピアには、次のタイプがあります。

IBGP peers: ローカルルータと同じ AS 内に存在します。
EBGP peers: ローカルルータとは異なる AS に存在します。

> アドレスファミリを選択せずに BGP ピアを作成すると、BGP ピアはアイドル状態のままになります。Open メッセージを使用したピア関係の確立は試行されません。

MP-BGP

BGP-4 は IPv4 ユニキャストルーティング情報だけをアドバタイズできます。
Multiprotocol Extensions for BGP-4(MP-BGP)は、次のアドレスファミリのルーティング情報をアドバタイズできます。

IPv6 ユニキャストアドレスファミリ。
IPv4 マルチキャストアドレスファミリおよび IPv6 マルチキャストアドレスファミリ。
> PIM は、スタティックおよびダイナミックユニキャストルートを使用して、マルチキャストルーティングエントリを作成する前に RPF チェックを実行します。マルチキャストトポロジとユニキャストトポロジが異なる場合は、MP-BGP を使用して RPF チェックのルートをアドバタイズできます。MP-BGP は、ルートを BGP マルチキャストルーティングテーブルに格納します。

IPv4 MDT アドレスファミリ。

MP-BGP は、マルチキャスト VPN がパブリックネットワーク上のルートとして PE を使用するデフォルト MDT を作成できるように、PE アドレスとデフォルトグループを含む MDT 情報をアドバタイズします。マルチキャスト VPN の詳細については、『IP Multicast Configuration Guide』を参照してください。

Controlling BGP route generation

BGP routes can be generated in the following ways:

ローカルネットワークを挿入します。BGP が BGP ピアにネットワークをアドバタイズできるように、ローカルルーティングテーブル内のネットワークを BGP ルーティングテーブルに挿入するには、次の作業を実行します。この方法でアドバタイズされる BGP ルートの ORIGIN 属性は IGP です。ルーティングポリシーを使用してルートアドバタイズメントを制御することもできます。

指定されたネットワークは、ローカル IP ルーティングテーブルで使用可能であり、アクティブである必要があります。

IGP ルートの再配布:IGP から BGP へのルート再配布を設定するには、次の作業を実行します。
デフォルトでは、BGP はデフォルト IGP ルートを再配布しません。デフォルト IGP ルートを BGP ルーティングテーブルに再配布するように BGP を設定できます。

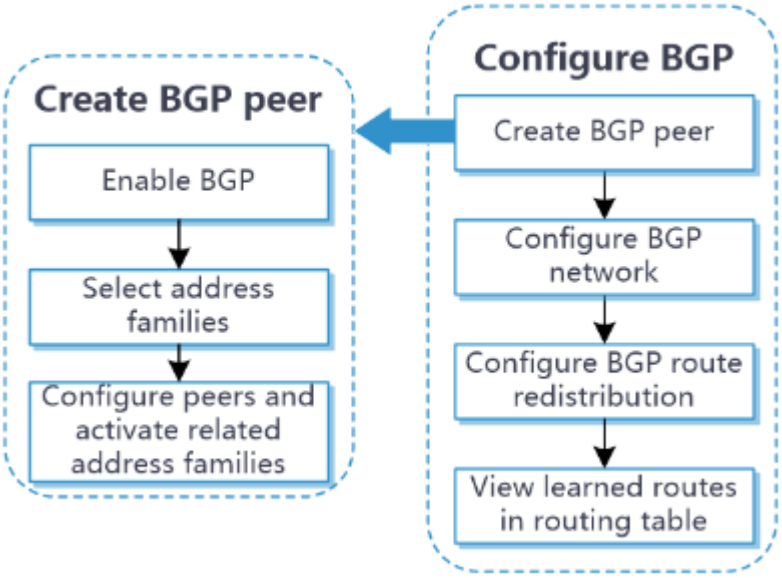
IGP から再配布された BGP ルートの ORIGIN アトリビュートは INCOMPLETE です。
再配布できるのは、アクティブなルートだけです。

Restrictions and guidelines

BGP Network タブおよび **BGP Route Redistribution** タブで操作を実行する前に、まず[BGP Address Family]タブでアドレスファミリを選択します。この手順に従わないと、エラーメッセージが表示されます。
BGP が設定されているデバイスの場合、**BGP status** で **Enable BGP** オプションをクリアして **Apply** をクリックすると、BGP プロセスがディセーブルになり、BGP 設定が失われます。

Configure BGP

図 1 に示すように、BGP を設定します。
図 1:BGP 設定手順


Configure BGP
Create BGP peer
Configure BGP network
Configure BGP route redistribution
View learned routes in routing table
Create BGP peer
Enable BGP
Select address families
Configure peers and activate related address families

RIP

Introduction

Routing Information Protocol(RIP)は、小規模なネットワークに適したディスタンスベクタ型の Interior Gateway Protocol(IGP)です。設定とメンテナンスが容易であるため、現在でも広く使用されています。

Restrictions and guidelines

複数の RIP プロセスが存在する場合、[Advertise all networks]オプションは使用できません。
インターフェースは、インターフェース固有の RIP バージョンを優先的に使用します。インターフェース固有のバージョンが指定されていない場合、インターフェースはグローバルな RIP バージョンを使用します。

IPv4 Multicast routing

Introduction

IPv4 マルチキャストルーティングがイネーブルになっている場合にだけ、他のレイヤー3 マルチキャスト機能(IGMP や PIM など)を有効にできます。

次の表は、IPv4 マルチキャストルーティングおよび転送に関係しています。

各マルチキャストルーティングプロトコルの IPv4 マルチキャストルーティングテーブル(PIM ルーティングテーブルなど)。

異なるマルチキャストルーティングプロトコルによって生成されたマルチキャストルーティング情報を要約した一般的な IPv4 マルチキャストルーティングテーブル。

PIM

Introduction

Protocol Independent Multicast(PIM)は、任意のユニキャストルーティングプロトコルによって生成されたユニキャストスタティックルートまたはユニキャストルーティングテーブルを活用して、IP マルチキャスト転送を提供します。PIM は、基礎となるユニキャストルーティングを使用して、特定のユニキャストルーティングプロトコルに依存せずにマルチキャストルーティングテーブルを生成します。

実装メカニズムに基づいて、PIM には次のカテゴリがあります。

Protocol Independent Multicast Dense Mode(PIM-DM):PIM-DM は、マルチキャストメンバーが高密度に分散している小規模なネットワークに適しています。

Protocol Independent Multicast-Sparse Mode(PIM-SM):PIM-SM は、マルチキャストグループメンバーがまばらで広範囲に分散している大規模および中規模のネットワークに適しています。

Protocol Independent Multicast Source-Specific Multicast(PIM-SSM):PIM-SSM は、PIM-SM テクニックの一部を活用して実装できます。PIM-SSM を設定する前に、まず PIM-SM をイネーブルにする必要があります。

インターフェース上で PIM-DM をイネーブルにした場合、PIM-DM モードが使用されます。インターフェース上で PIM-SM をイネーブルにした場合、インターフェース上の PIM モードは、マルチキャストパケットが送信されるマルチキャストグループによって異なります。

マルチキャストグループが SSM グループ範囲内にある場合は、PIM-SSM モードが使用されます。

マルチキャストグループが SSM グループ範囲内にない場合は、PIM-DM モードが使用されます。

IGMP

Introduction

Internet Group Management Protocol(IGMP)は、レイヤー3 マルチキャストデバイスと直接接続されたサブネット上のホストとの間にマルチキャストグループメンバシップを確立し、維持します。

IGMP には次のバージョンがあります。

IGMPv 1: IGMPv 1 は、クエリーおよび応答メカニズムに基づいてマルチキャストグループメンバシップを管理します。

IGMPv2: IGMPv1 との下位互換性があります。IGMPv2 では、クエリア選択メカニズムと脱退グループメカニズムが導入されています。

IGMPv3: IGMPv1 および IGMPv2 に基づいており、これらと互換性があります。IGMPv3 は、ホストの制御機能と IGMP ルータのクエリーおよびレポート機能を強化します。

IGMPv3 では、2 つの送信元フィルタリングモード(Include および Exclude)が導入されました。これらのモードにより、ホストは、指定されたマルチキャスト送信元からのマルチキャストデータを受信または拒否できます。

IGMPv3 では、グループレコードを伝送する IGMP グループおよび送信元クエリーと IGMP レポートが導入されています。

IGMP がインターフェースでイネーブルになると、インターフェースはマルチキャストグループメンバシップを確立して維持できます。

DHCP

このヘルプには、次のトピックがあります。

Introduction

DHCP server

DHCP address pool

IP address allocation sequence

DHCP options

IP address conflict detection

Configure DHCP

Introduction

Dynamic Host Configuration Protocol(DHCP)は、ネットワーク設定情報をネットワークデバイスに割り当てるためのフレームワークを提供します。
DHCP はクライアントサーバーモデルを使用します。通常、DHCP ネットワークには DHCP サーバーと複数の DHCP クライアントが含まれます。DHCP クライアントと DHCP サーバーが異なるサブネット上にある場合、DHCP クライアントは DHCP リレーエージェントを介して DHCP サーバーから構成パラメーターを取得できます。

DHCP server

DHCP サーバーを使用して、次のネットワークに IP アドレスを割り当てます。

一元管理が必要な大規模ネットワーク。
十分な IP アドレススペースがないネットワーク。ホストの数が割り当て可能な IP アドレスの数よりも多い場合、すべてのホストが同時に IP アドレスを持つことができるわけではありません。
固定 IP アドレスを必要とするホストが数台しかないネットワーク。

DHCP サーバーは、IP アドレス、リース期間、ネットワーク情報、ドメイン名サフィックス、DNS サーバードレス、WINS サーバードレス、NetBIOS ノードタイプ、および DHCP オプション情報をアドレスプールに格納します。DHCP サーバーは、アドレスプールから IP アドレスと構成パラメーターを選択し、要求元の

DHCP クライアントに割り当てます。
IP アドレスをクライアントに割り当てる前に、DHCP サーバーは IP アドレスの競合検出を実行します。

DHCP address pool

次のアドレス割り当てメカニズムを使用できます。

Static address binding: クライアントの MAC アドレスまたは ID を DHCP アドレスプールの IP アドレスに手動でバインドします。クライアントが IP アドレスを要求すると、DHCP サーバーは静的バインディングの IP アドレスをクライアントに割り当てます。
Dynamic address allocation: DHCP アドレスプールで IP アドレス範囲を指定します。DHCP 要求を受信すると、DHCP サーバーはアドレスプールで一致する IP アドレス範囲から IP アドレスを動的に選択します。

静的および動的に割り当てられたアドレスのリース期間を指定できます。
DHCP サーバーは、次の原則に従ってクライアントのアドレスプールを選択します。

IP アドレスがクライアントの MAC アドレスまたは ID に静的にバインドされているアドレスプールがある場合、DHCP サーバーはこのアドレスプールを選択し、静的にバインドされた IP アドレスおよびその他の設定パラメーターをクライアントに割り当てます。
上記の条件が満たされない場合、DHCP サーバーはクライアントの場所に応じてアドレスプールを選択します。
Client on the same subnet as the server: DHCP サーバーは受信インターフェースの IP アドレスをすべてのアドレスプールのサブネットと比較し、最も長いサブネットが一致するアドレスプールを選択します。
Client on a different subnet than the server: DHCP サーバーは、DHCP 要求の giaddr フィールド内の IP アドレスをすべてのアドレスプールのサブネットと比較し、最も長く一致するプライマリサブネットを持つアドレスプールを選択します。

IP address allocation sequence

DHCP サーバーは、次の順序でクライアントの IP アドレスを選択します。

クライアントの MAC アドレスまたは ID に静的にバインドされた IP アドレス。
クライアントに割り当てられたことのある IP アドレス。
クライアントが送信する DHCP-DISCOVER メッセージの Option 50 フィールドで指定された IP アドレス。

Option 50 は Requested IP Address オプションです。クライアントはこのオプションを使用して、DHCP-DISCOVER メッセージで必要な IP アドレスを指定します。Option 50 の内容はユーザー定義です。

動的割り当てルールに基づいて最初に検出された割り当て可能な IP アドレス。

競合していたか、リース期間を過ぎた IP アドレス。割り当て可能な IP アドレスがない場合、サーバーは応答しません。

DHCP options

DHCP はオプションフィールドを使用して、動的アドレス割り当てのための情報を伝送し、クライアントに追加の構成情報を提供します。

DHCP options は、次の目的で使用します。

新しい DHCP オプションを追加します。

ベンダー固有のオプション内容を定義します。たとえば、ベンダー固有の情報をオプション 43 に埋め込むことができます。

他の DHCP Web ページでサポートされていない機能を構成します。たとえば、オプション 4 を使用して、IP アドレス 1.1.1.1 を DHCP クライアントのタイムサーバードレスとして指定できます。

既存の DHCP オプションを拡張して p オプションを拡張します。たとえば、Web ページには最大 8 つの DNS サーバードレスを構成できます。さらに多くの DNS サーバーを構成する必要がある場合は、拡張用の DHCP オプションを使用できます。

表 1 に、一般的な DHCP オプションを示します。

表 1 一般的な DHCP オプション

オプション番号	オプション名	推奨オプションパディングタイプ
3	ルータオプション	IP アドレス
6	ドメインネームサーバーオプション	IP アドレス
15	ドメイン名	ASCII 文字列
43	ベンダー固有の情報	16 進文字列
44	NetBIOS over TCP/IP ネームサーバーオプション	IP アドレス
46	NetBIOS over TCP/IP ノードタイプオプション	16 進文字列

66	TFTP サーバー名	ASCII 文字列
67	ブートファイル名	ASCII 文字列

IP address confliction detection

IP アドレスを割り当てる前に、DHCP サーバーはその IP アドレスに ping を実行します。

サーバーは、指定された期間内に応答を受信すると、別の IP アドレスを選択して ping を実行します。応答がない場合、サーバーは ping パケットの最大数が送信されるまで IP アドレスへの ping を続行します。それでも応答がない場合、サーバーは要求元クライアントに IP アドレスを割り当てます。

Configure DHCP

Configure the DHCP server

DHCP サーバー機能を実装するには、次の作業を実行します。

DHCP サービスを有効にします。
DHCP サーバーモードで動作するようにインターフェースを設定します。
DHCP アドレスプールを設定します。アドレス割り当ての動的割り当て方式または静的バインドを選択できます。DHCP アドレスプールのリース期間、ドメイン名サフィックス、ゲートウェイアドレス、およびその他のネットワークパラメータを設定できます。

HTTP/HTTPS

Introduction

デバイスには Web サーバーが組み込まれています。Web ブラウザを使用して、HTTP または HTTPS 経由でデバイスにログインできます。

HTTP ログイン

デバイスは、HTTP 1.0 および HTTP 1.1 をサポートします。

HTTPS ログイン

HTTPS は SSL を使用して、クライアントとサーバー間で交換されるデータの整合性とセキュリティーを確保します。HTTPS は HTTP よりも安全です。

HTTPS ログインを許可するには、HTTPS サービスをイネーブルにする必要があります。デフォルトでは、デバイスは自己署名証明書(デバイス自体によって生成され、署名された証明書)およびデフォルトの SSL 設定を使用します。

クライアントとサーバー間で交換されるデータの整合性とセキュリティーを向上させるために、SSL サーバーポリシーを HTTPS に関連付けて SSL 設定を定義できます。

デバイスは、次の HTTPS ログインタイプをサポートします。

Username: ユーザーはログイン時にユーザー名とパスワードを入力する必要があります。

Certificate: ユーザーはログイン時にデジタル証明書を提供する必要があります。

Username and certificate: ユーザーは、ログイン時にユーザー名とパスワードをデジタル証明書とともに入力する必要があります。

USB キーログインは、証明書ベースの HTTPS ログイン方式です。ユーザーがログインページで **Log in using a USB key** をクリックした場合、ログインのプロンプトに従って USB キー内のデジタル証明書を選択する必要があります。

デバイスは ACL を使用して、不正な HTTP および HTTPS アクセスを防止できます。使用されている ACL が存在し、ルールが設定されている場合は、ACL で許可されたユーザーだけが HTTP または HTTPS を介してデバイスにアクセスできます。

SSH

このヘルプには、次のトピックがあります。

Introduction

Restrictions and guidelines

Configure SSH

Introduction

Secure Shell(SSH)はネットワークセキュリティープロトコルです。SSH では、暗号化と認証を使用して、安全でないネットワークを介した安全なリモートアクセスとファイル転送を実装できます。
SSH は、一般的なクライアント/サーバーモデルを使用して、TCP に基づく安全なデータ転送のためのチャネルを確立します。
デバイスは、次の SSH アプリケーションをサポートします。

Secure Telnet : Stelnet は、安全で信頼性の高いネットワーク端末アクセスサービスを提供します。
Secure File Transfer Protocol: SSH2 に基づいて、SFTP は SSH 接続を使用してセキュアなファイル転送を実現します。
Secure Copy: SSH2 に基づいて、SCP はファイルをコピーするための安全な方法を提供します。

SSH には、SSH1.x と SSH2.0(以下、SSH1 と SSH2)の 2 つのバージョンがありますが、互換性はありません。SSH2 は、SSH1 よりもパフォーマンスとセキュリティーが優れています。
デバイスが SSH サーバーとして動作する場合、ローカルパスワード認証を使用して SSH クライアントのユーザー名とパスワードを確認します。SSH クライアントが認証に合格すると、SSH クライアントと SSH サーバーはセッションを確立し、このセッションを使用してデータを交換できます。

Restrictions and guidelines

異なるタイプのキーペアを使用する SSH クライアントをサポートするには、SSH サーバーで DSA、ECDSA、および RSA キーペアを生成します。
SSH サーバーのローカル DSA、ECDSA および RSA キーペアでは、デフォルト名が使用されます。キーペアに名前を割り当てることはできません。
SSH サーバーで DSA キーペアを生成する場合、キー係数の長さは 2048 ビット未満である必要があります。

SSH クライアントが認証を通過すると、SSH クライアントに割り当てられた属性(ユーザーロールや FTP ディレクトリなど)は、SSH サーバーの管理者設定によって決定されます。
SSH クライアントの接続要求をフィルタリングする ACL が存在しない場合、または ACL に規則が含まれていない場合は、すべての SSH クライアントがデバイスにアクセスできます。
SFTP サーバーとして動作する場合、デバイスは SSH1 クライアントによって開始された SFTP 接続をサポートしません。

Configure SSH

SSH サーバーが Stelnet、SFTP、または SCP サービスを提供できるようにするには、次の作業を実行します。

RSA、DSA、または ECDSA キーペアを生成します。
Stelnet、SFTP、または SCP サービスをイネーブルにします。
SSH サービスタイプの管理者を設定します。

NTP

Introduction

Network Time Protocol(NTP)は、ネットワーク上の分散タイムサーバーとクライアント間でシステムクロックを同期するために使用されます。

NTP は、ストラタム 1～15 を使用してクロックの精度を定義します。ストラタム値が小さいほど、精度が高くなります。

ネットワーク上のデバイスが信頼できる時刻源に同期できない場合は、次の作業を実行して、ネットワーク上で NTP 同期を実行できます。

- ネットワーク上で比較的正確なクロックを持つデバイスを選択します。
- デバイスのローカルクロックをリファレンスソースとして設定します。
- デバイスをタイムサーバーとして設定し、ネットワーク上の他のデバイスと同期させます。

Web インターフェースからローカルクロックをリファレンスソースとして設定できます。

Restrictions and guidelines

ローカルクロックをリファレンスソースとして設定する前に、ローカルクロックの時刻を調整して、正確であることを確認します。

FTP

Introduction

ファイル転送プロトコル(FTP)は、IP ネットワークを介して 1 つのホストから別のホストにファイルを転送するためのアプリケーション層プロトコルです。TCP ポート 20 を使用してデータを転送し、TCP ポート 21 を使用して制御コマンドを転送します。
FTP はクライアント/サーバーモデルを使用します。デバイスは FTP サーバーとして機能できます。

Telnet

Introduction

デバイスは Telnet サーバーとして動作し、Telnet ログインを許可できます。
デバイスは ACL を使用して、不正な Telnet アクセスを防止できます。使用されている ACL が存在し、ルールが設定されている場合は、ACL で許可されたユーザーだけがデバイスに Telnet 接続できます。

Restrictions and guidelines

Telnet ログインをイネーブルにするには、Telnet サーバーをイネーブルにし、ログイン認証と共通アトリビュートを設定して、ユーザーロールを割り当てる必要があります。

Hot backup

このヘルプには、次のトピックがあります

Introduction

ホットバックアップは、デバイスレベルの高可用性(HA)ソリューションです。これにより、2 つのデバイスが相互に動的にバックアップされ、一方のデバイスで障害が発生した場合にユーザーサービスの継続性が確保されます。

ホットバックアップシステムは Remote Backup Management(RBM)と連動して、複数の VRRP グループを管理したり、2 つのメンバーデバイス上のルーティングプロトコルのリンクコストを調整したりして、デバイスが一貫した役割と状態を持つようにします。ホットバックアップシステムは、デバイス間で重要な設定とサービスエントリを同期させて、サービスの継続性を確保できます。ホットバックアップシステムに参加するには、2 つのデバイスのソフトウェア環境とハードウェア環境が同じである必要があります。

Basic concepts in hot backup configuration

ホットバックアップ構成の基本概念は次のとおりです。

Primary and secondary roles: デバイス間の構成の同期化の方向を制御します。プライマリおよびセカンダリの役割は、ホットバックアップシステム内の 2 つのデバイスに割り当てられます。プライマリデバイスはその構成をセカンダリデバイスに同期化し、セカンダリデバイスの構成は上書きされます。

Active and standby states: データプレーンでトラフィックを転送および処理するデバイスを決定します。アクティブデバイスは、サービスのトラフィックを転送し、サービスエントリをリアルタイムでスタンバイデバイスにバックアップします。アクティブデバイスに障害が発生すると、スタンバイデバイスがアクティブデバイスの役割を引き継ぎ、サービスの継続性を確保します。

VRRP active and standby groups: ホットバックアップシステムを VRRP に関連付けて、ホットバックアップシステムが複数の VRRP グループのステータスを集中管理できるようにします。

Hot backup channels: ステータス情報、重要な設定、およびサービスエントリをホットバックアップメンバー間で転送します。

Hot backup modes: アクティブ/スタンバイモードとデュアルアクティブモードがあります。アクティブ/スタンバイモードでは、アクティブなデバイスがすべてのサービスを処理します。デュアルアクティブモードでは、両方のデバイスがサービスを処理して、ホットバックアップシステムとロードシェアトラフィックの機能を向上させます。

Hot backup packets: ホットバックアップメンバ間のホットバックアップチャネルを介して TCP を介して送信されます。

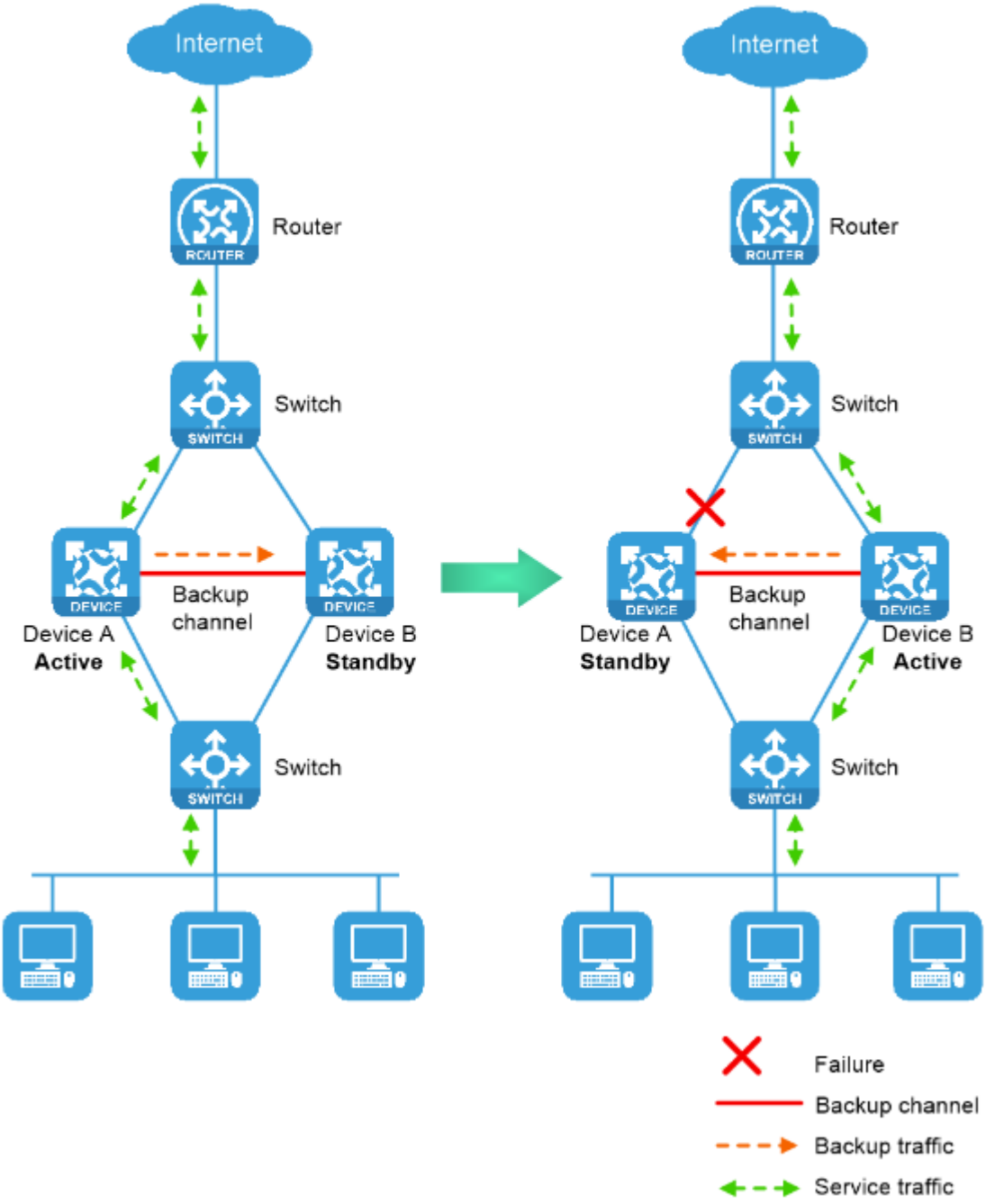
Operating modes of the hot backup system

ホットバックアップシステムは、アクティブ/スタンバイモードとデュアルアクティブモードをサポートしています。

Active/standby mode

アクティブ/スタンバイモードでは、図 1 に示すように、一方のデバイスがサービスを処理するためにアクティブになり、もう一方のデバイスが待機します。アクティブデバイス上のインターフェースまたはリンクに障害が発生した場合、またはアクティブデバイスに障害が発生した場合、スタンバイデバイスがサービスを処理するためにアクティブになります。

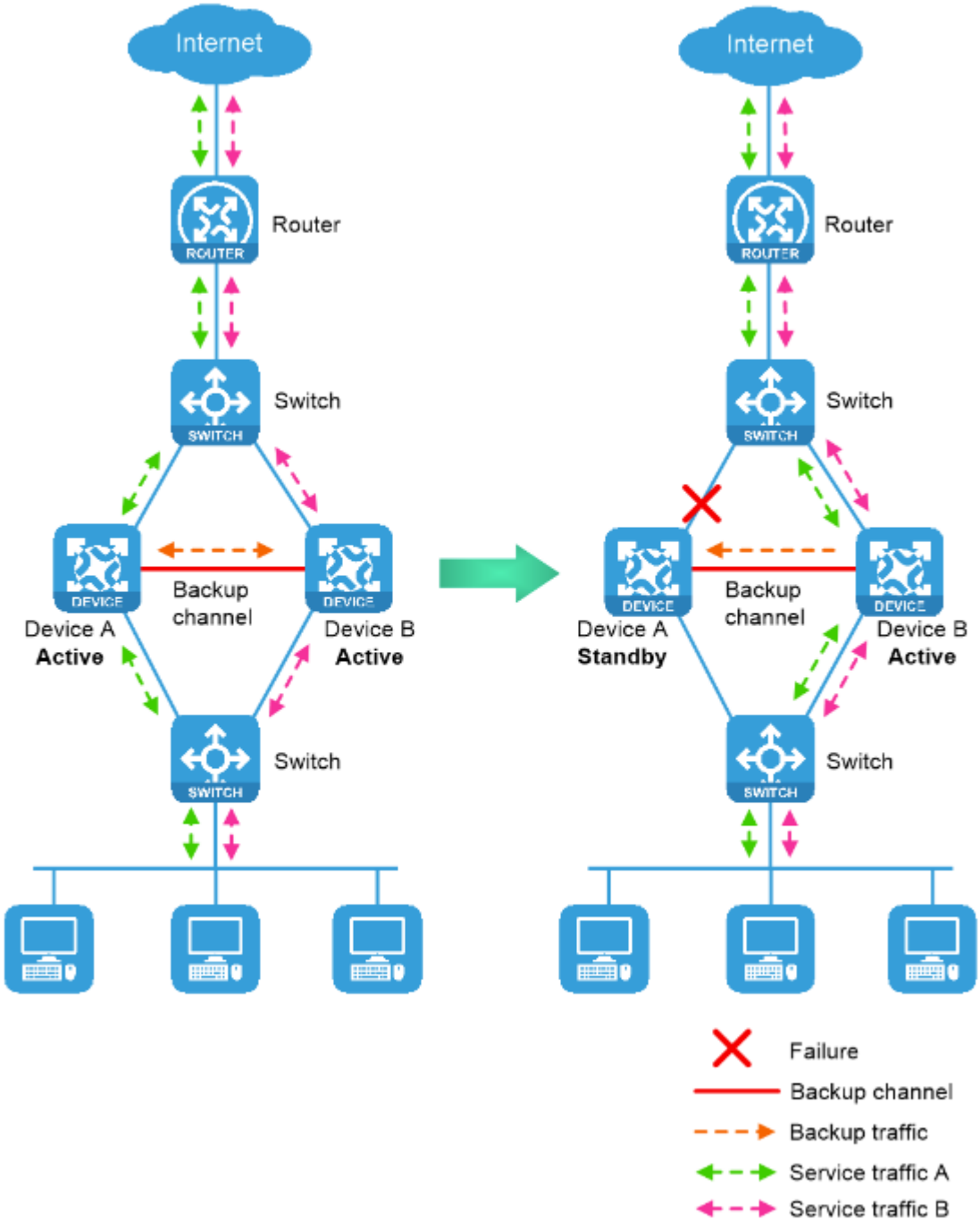
図 1 ホットバックアップシステムのアクティブ/スタンバイモード



Dual-active mode

デュアルアクティブモードでは、図 2 に示すように、両方のデバイスがサービスを処理してホットバックアップシステムの機能を向上させます。一方のデバイスに障害が発生すると、そのトラフィックは転送のためにもう一方のデバイスに切り替えられます。

図 2 ホットバックアップシステムのデュアルアクティブモード



Hot backup channels

overview

ホットバックアップメンバーは、ホットバックアップシステムステータス、重要な設定、およびサービスエントリを次のチャネルを介して送信します。

Control channel: パケットを使用してデータを送信します。パケットには、ホットバックアップシステムステータスパケット、構成整合性チェックパケット、サービスエントリのバックアップパケット、透過的な送信を必要とするデータパケット、および構成同期パケットが含まれます。
Data channel: バックアップパケットおよび透過的な送信が必要なパケットのみを送信します。データチャネルは、データ送信にハードウェアドライバを使用し、レイヤー2 転送のみをサポートします。

Establishment and keepalive mechanism of the control channel

制御チャネルは、到達可能性検出に TCP のキープアライブメカニズムを使用します。制御チャネルは TCP を介して確立されます。ホットバックアップシステムでは、IP アドレスが大きいデバイスがサーバーとして機能し、もう一方のデバイスがクライアントとして機能して TCP 接続を開始します。
各メンバーデバイスは、ホットバックアップ制御チャネルを介してホットバックアップピアにホットバックアップキープアライブパケットを定期的に送信します。ホットバックアップキープアライブの最大試行回数に達したときにデバイスがピアから応答を受信しなかった場合、ホットバックアップ制御チャネルは切断されます。

Service entry backup

overview

ホットバックアップシステムは、アクティブ/スタンバイスイッチオーバーが発生したときにサービスが中断されないように、アクティブデバイス上で生成されたサービスエントリをスタンバイデバイスにバックアップします。
ファイアウォールなどのセキュリティデバイスは、動的接続ごとにセッションエントリを生成します。ホットバックアップシステムでは、アクティブデバイスだけがトラフィックを処理し、セッションエントリを生成します。サービスの継続性を確保するために、アクティブデバイスはセッションエントリをリアルタイムでスタンバイデバイスにバックアップします。アクティブ/スタンバイスイッチオーバー後、新しいアクティブデバイスは、セッションエントリに基づいて既存のサービスのパケットを中断なく転送できます。

Supported services

ホットバックアップシステムは、次のサービスエントリに対してホットバックアップを実行できます。
セッションエントリ。
セッション関係エントリ。
NAT ポートブロック。
AFT ポートブロック。
セキュリティーサービスモジュールによって生成されたエントリ。
これらのエントリのサポートは、デバイスモデルによって異なります。

Configuration backup

overview

ホットバックアップシステムは、プライマリデバイスからセカンダリデバイスに重要な構成をバックアップして、アクティブ/スタンバイスイッチオーバーが発生したときにサービスが中断されないようにします。セカンダリデバイスの構成は上書きされます。単一方向バックアップメカニズムは、特にデュアルアクティブモードでの構成の競合を回避します。ホットバックアップの役割は、デバイスに手動でのみ割り当てることができます。ホットバックアップシステムが正しく動作するようにするためのベストプラクティスとして、プライマリデバイスで構成のバックアップを有効にします。

Backup type

ホットバックアップシステムは、自動バックアップと手動バックアップの両方をサポートしています。

Supported services

ホットバックアップシステムは、次のサービスの設定バックアップを実行できます。

Resouces: VPN インスタンス、ACL、オブジェクトグループ、時間範囲、セキュリティーゾーン、セッション管理、APR、AAA。

DPI: アプリケーションレイヤー検査エンジン、IPS、URL フィルタ、データフィルタ、ファイルフィルタ、ウイルス対策、データ解析センター、WAF。

Policies: オブジェクトポリシー、セキュリティーポリシー、ASPF、攻撃の検出と防止、接続制限、NAT、AFT、ロードバランシング、帯域幅管理、アプリケーションの監査と管理、共有ネットワークアクセス管理、プロキシポリシー。

ログ:高速ログ出力、フローログ。

SSL VPN。

VLAN。

インフォメーションセンター。

これらのサービスのサポートは、デバイスモデルによって異なります。

Configuration consistency check

ホットバックアップシステムでは、構成整合性チェックパケットを使用して、ホットバックアップメンバー間の構成整合性が検証されます。デバイスで構成の不一致が検出されると、手動で構成を同期化するためのログが生成されます。

Hot backup system in collaboration with VRRP

overview

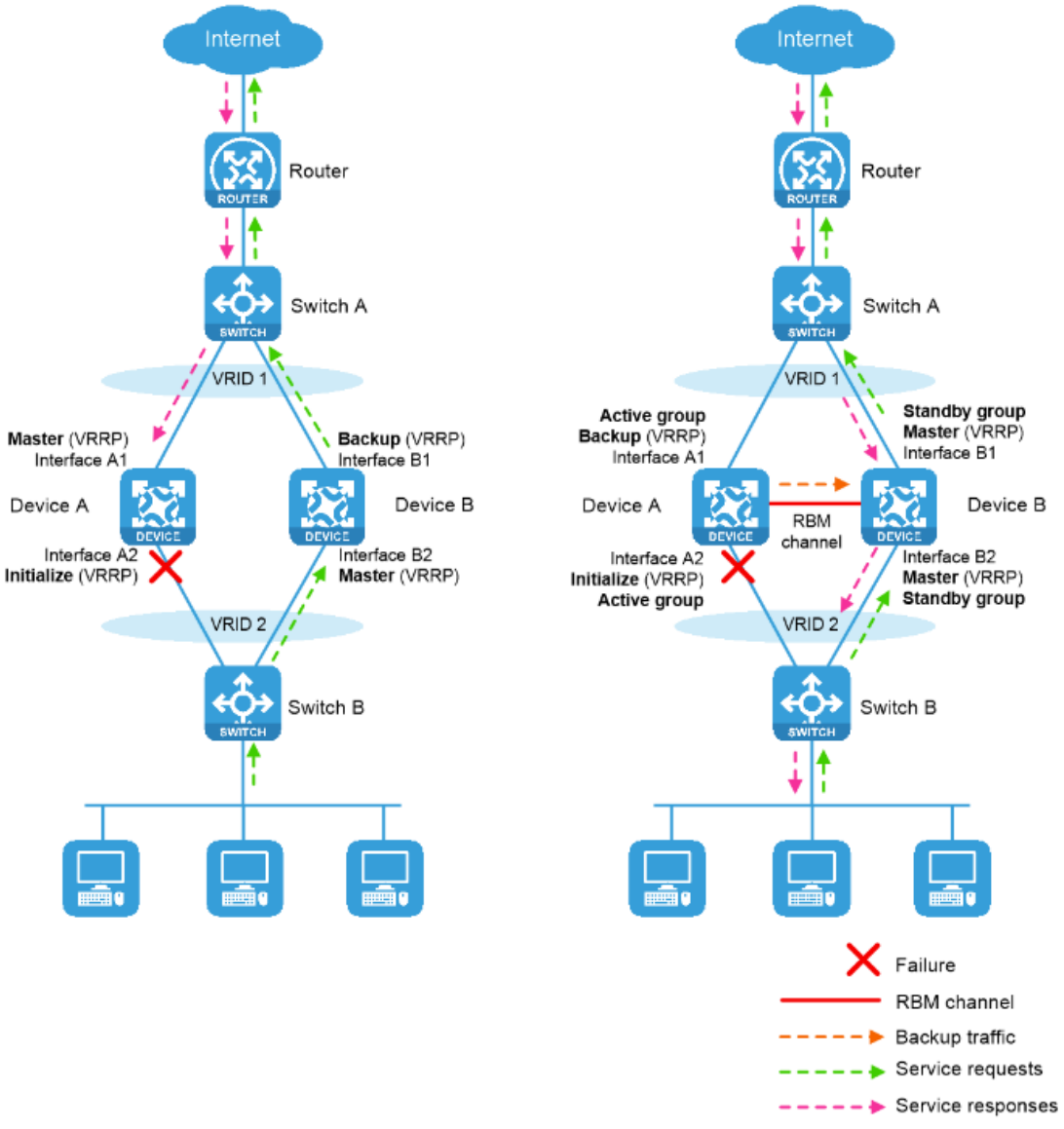
ホットバックアップと VRRP を組み合わせて使用すると、マスター/バックアップスイッチオーバーを制御して、複数の VRRP グループでデバイスロールの一貫性(マスターまたはバックアップ)を保つことができます。これにより、着信トラフィックと発信トラフィックの両方を新しいマスターにスイッチングして、デバイス障害時に対称転送を行うことができます。

図 3 は、アクティブ/スタンバイモードでのホットバックアップシステムと VRRP の関連付けを示しています。

左に示すように、VRRP はデバイス上で障害が発生した場合に対称転送を保証できないため、トラフィックが中断されます。

右に示すように、ホットバックアップ制御チャネルが確立されると、ホットバックアップシステムはすべての VRRP グループ内のデバイスの役割を決定します。VRRP のマスター選択メカニズムは有効ではなくなります。ホットバックアップ制御チャネルが切断されると、VRRP のマスター選択メカニズムが再び有効になります。

図 3 VRRP と連携したホットバックアップシステム



VRRP active/standby group

ホットバックアップシステムは、VRRP アクティブグループおよびスタンバイグループによって VRRP に関連付けられます。
VRRP アクティブ/スタンバイグループは、マスター状態またはバックアップ状態になることができます。これにより、関連付けられた VRRP グループ内のデバイスの状態が決まります。たとえば、VRRP アクティブグループがマスター状態の場合、関連付けられた VRRP グループ内のすべてのデバイスがマスターになります。
VRRP アクティブ/スタンバイグループの初期状態は次のとおりです。

Active/Standby mode: プライマリデバイスでは、VRRP アクティブグループとスタンバイグループの初期状態はマスターです。セカンダリデバイスでは、VRRP アクティブグループとスタンバイグループの初期状態はバックアップです。
Dual-active mode: VRRP アクティブ/スタンバイグループの状態は、ホットバックアップロールの影響を受けません。初期状態は、VRRP アクティブグループではマスターであり、VRRP スタンバイグループではバックアップです。

VRRP master election in the hot backup system

ホットバックアップシステムが VRRP に関連付けられると、ホットバックアップシステムは VRRP グループ内のデバイスの役割を決定します。図 3 に示すように、デバイス A は VRRP グループ 1 および VRRP グループ 2 のマスターであり、デバイス B は VRRP グループ 1 および VRRP グループ 2 のバックアップです。デバイス A のインターフェース A2 に障害が発生すると、次のイベントが発生します。
ホットバックアップシステムはインターフェース障害イベントを受信し、VRRP アクティブグループとスタンバイグループのステータス変更情報をデバイス B に送信します。
デバイス B は、その役割を VRRP スタンバイグループのマスターに設定してから、VRRP グループ 1 および VRRP グループ 2 のマスターになります。
デバイス B は、マスター/バックアップスイッチオーバー後にデバイス A に応答を送信します。
デバイス A は、その役割を VRRP アクティブグループ内のバックアップに設定し、その後、VRRP グループ 1 および VRRP グループ 2 内のバックアップになります。
インターフェース A2 が回復すると、ホットバックアップシステムは同じ手順に従って別のマスター/バックアップスイッチオーバーを実行します。トラフィックはスイッチオーバー後にデバイス A に戻されます。

ARP and MAC learning in VRRP

VRRP グループのメンバーがグループの仮想 IP アドレスに対する ARP 要求を受信すると、マスターはグループの仮想 MAC アドレスで応答します。これにより、アップストリームおよびダウンストリームのレイ

ヤー2 デバイスおよびホストは仮想 MAC アドレスを学習できます。

Hot backup system in collaboration with routing protocols

overview

ホットバックアップを設定すると、スタンバイデバイス上のルーティングプロトコルが変更されたリンクコストをアドバタイズできるようになります。この機能により、着信トラフィックと発信トラフィックの両方を新しいアクティブデバイスにスイッチングして、対称転送を行うことができます。

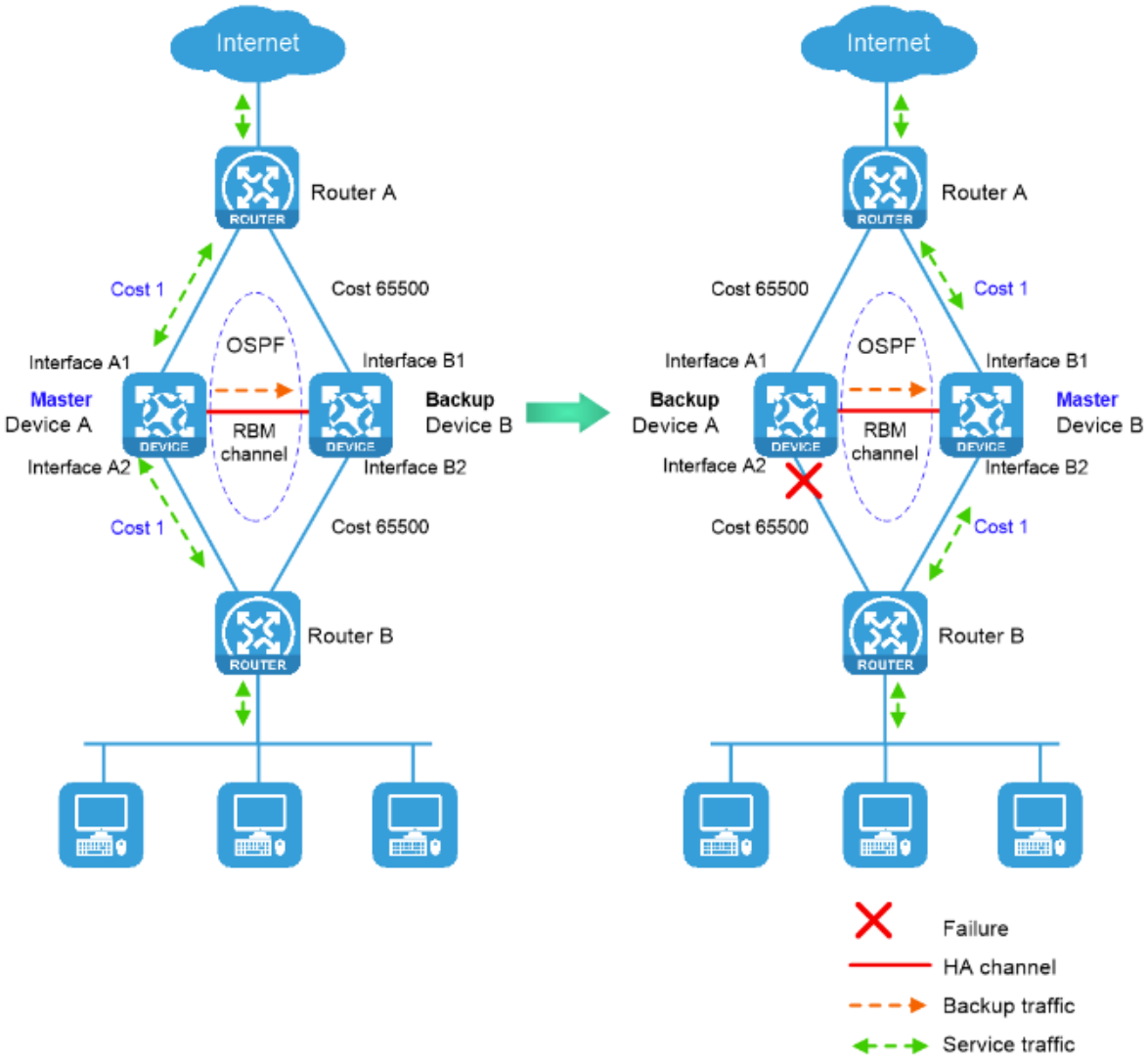
ルーティングプロトコルでホットバックアップを使用するには、トラックエントリを使用して、ホットバックアップシステムのアップリンクインターフェースとダウンリンクインターフェースのステータスを監視し、リンクまたはインターフェースに障害が発生したときにアクティブ/スタンバイスイッチオーバーを実行する必要があります。

次の情報では、アクティブ/スタンバイモードのホットバックアップシステムで OSPF を使用して、ホットバックアップシステムがダイナミックルーティングプロトコルとどのように連携するかを説明します。

図 4 に示すように、デバイス A(アクティブ)とデバイス B(スタンバイ)の両方が正常に動作している場合、デバイス A は元のリンクコスト 1 をアドバタイズし、デバイス B はホットバックアップシステムによって調整されたリンクコスト 65500 をアドバタイズします。その結果、デバイス A はホットバックアップシステムを通過するすべてのトラフィックを転送します。

図 4 に示すように、デバイス A のダウンリンクインターフェース A2 に障害が発生すると、デバイス A とデバイス B は状態を切り替えます。次に、デバイス B(アクティブ)は元のリンクコスト 1 をアドバタイズし、デバイス A(スタンバイ)は調整されたリンクコスト 65500 をアドバタイズします。その結果、デバイス B はホットバックアップシステムを通過するすべてのトラフィックを転送します。

図 4 ルーティングプロトコルと連携したホットバックアップシステム



Mechanism

ホットバックアップシステムは、次のいずれかの方法を使用して、ダイナミックルーティングプロトコルによってアドバタイズされるリンクコストを調整します。

元のリンクコストを、設定した絶対リンクコストに置き換える。

元のリンクコストに増分値を追加する。

リンクコストの変更は、デバイスのホットバックアップロールに影響しないため、ホットバックアップメンバーデバイスに同じリンクコスト調整設定を設定する必要があります。

Transparent in-path deployment of the hot backup system

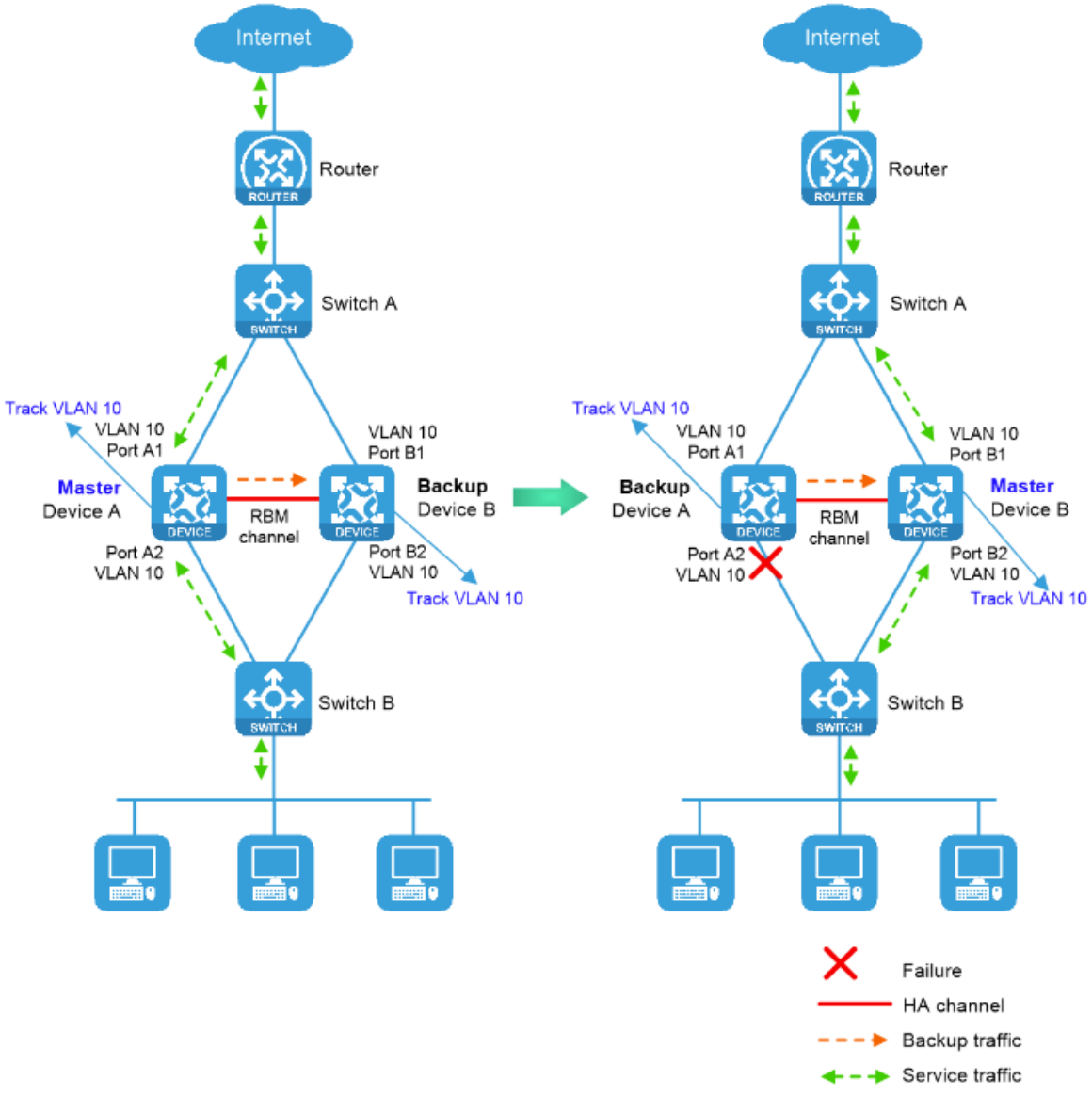
このネットワーキング方式を使用する場合は、インターフェースまたは VLAN を監視してアップリンクインターフェースとダウンリンクインターフェース間のコラボレーションをイネーブルにするようにホットバックア

ップシステムを設定できます。モニタリング設定により、インターフェースのグループが同じステータスになり、アップリンクトラフィックとダウンリンクトラフィックをメンバーデバイス間で同時にスイッチングできます。次の情報では、インターフェースのコラボレーション方法を説明する例として、VLAN モニタリングを使用しています。

図 5 に示すように、デバイス A(アクティブ)とデバイス B(スタンバイ)の両方が正常に動作している場合、追跡対象の VLAN 10 はデバイス A ではアクティブ状態、デバイス B では非アクティブ状態になります。その結果、デバイス A はホットバックアップシステムを通過するすべてのトラフィックを転送します。

図 5 に示すように、デバイス A のダウンリンクポート A2 に障害が発生すると、デバイス A とデバイス B はそれぞれの状態を切り替えます。その後、ホットバックアップシステムは VLAN 10 をデバイス A 上で非アクティブ状態(スタンバイ)にし、デバイス B 上でアクティブ状態(アクティブ)にします。その結果、デバイス B はホットバックアップシステムを通過するすべてのトラフィックを転送します。

図 5 ホットバックアップシステムの透過的なパス内導入



Restrictions and guidelines

ホットバックアップは、VRRP マスター/バックアップモードでのみ使用できます。VRRP ロードシェアリングモードでは、ホットバックアップはサポートされません。
ホットバックアップシステムを設定して、トラックエントリ、VLAN、またはインターフェースをモニターできますが、VLAN モニタリングをトラックエントリモニタリングまたはインターフェースモニタリングと組み合せて設定することはできません。トラックエントリとインターフェースの両方をモニターするようにホットバックアップシステムを設定する場合は、トラックエントリがモニター対象インターフェースに関連付けられていないことを確認してください。

Configure hot backup

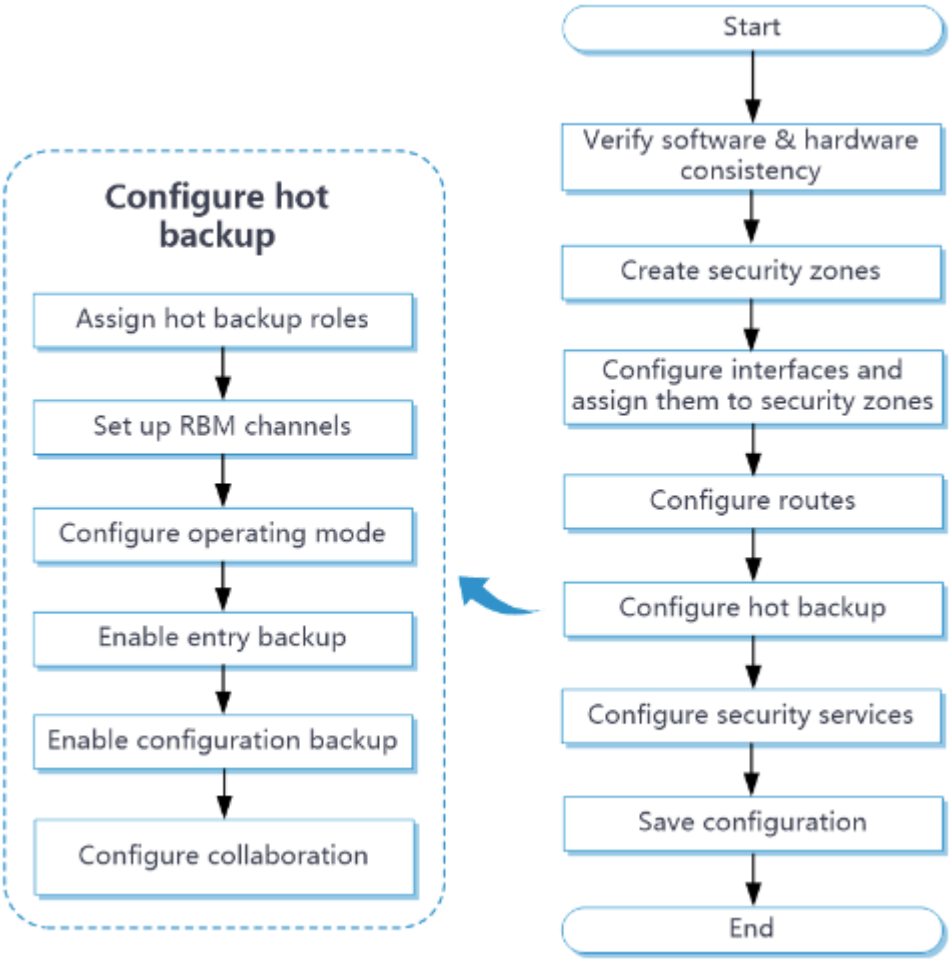
Prerequisites

ホットバックアップシステムを設定する前に、次のハードウェアとソフトウェアの設定が、ホットバックアップシステムに割り当てるデバイスで同じであることを確認します。

デバイスモデル。
ソフトウェアのバージョン。
インターフェース番号。
制御チャネルを設定するためのインターフェース。
データチャネルを設定するためのインターフェース。
同じインターフェース番号を持つインターフェース上のセキュリティーゾーン設定。

Hot backup system configuration flow

図 6 ホットバックアップシステムの構成フローチャート



Configure hot backup

System タブをクリックします。

ナビゲーションペインで、**High Availability** > **Hot Backup** を選択します。

Hot Backup ページが開きます。

Configure をクリックします。

Configure Hot Backup]ページが開きます。

ホットバックアップを構成します。関連するパラメーターの詳細については、表 1 を参照してください。

表 1 ホットバックアップパラメータ

パラメーター	説明
Hot Backup	ホットバックアップ機能のステータスを設定します。
Operating mode	ホットバックアップシステムの動作モードを設定します。 **Active/standby**:アクティブデバイスがサービスを処理し、スタンバイデバイスが待機します。

	Dual-active：両方のホットバックアップメンバーデバイスがサービスを処理します。
Device role	ホットバックアップロールをホットバックアップシステム内のメンバーデバイスに割り当てます。
Local IP	ローカル IP アドレスを入力して、制御チャネルを設定します。サーバーエンドは、この IP アドレスで TCP 接続要求をリスニングします。IPv4 または IPv6 アドレスを入力できますが、両方は入力できません。
Peer IP	制御チャネルの設定に使用するピア IP アドレスを入力します。IPv4 または IPv6 アドレスを入力できますが、両方は入力できません。
Peer port	制御チャネルのポート番号を入力します。ホットバックアップメンバーデバイスのポート番号は同じである必要があります。
Data channel	バックアップパケットおよびトランスペアレント伝送を必要とするパケットを送信するデータチャネルを設定するインターフェースを選択します。
Keepalive interval	デバイスがキープアライブパケットをピアデバイスに定期的に送信する間隔を設定します。
Max keepalive retries	キープアライブの最大再試行回数を設定します。デバイスがピアデバイスから応答を受信する前にこの制限に達すると、デバイスはピアデバイスへのホットバックアップチャネルを切断します。
Fallback	回復時にトラフィックを元のアクティブデバイスに戻すには、この機能をイネーブルにします。
Traffic reversion delay	ホットバックアップメンバーがスイッチバックの前に待機する必要がある遅延を設定します。この遅延により、デバイスはサービスエントリのバックアップを完了して、トラフィックの損失を防ぐことができます。
Back up sessions	セッションバックアップのステータスを設定します。この機能を有効にすると、アクティブデバイスはサービスモジュールエントリをリアルタイムでスタンバイデバイスにバックアップします。アクティブデバイスに障害が発生すると、サービスを中断することなくスタンバイデバイスが処理を引き継ぎます。
Back up HTTP Back up DNS	受信した DNS および HTTP プロトコルパケットに対して作成されたセッションエントリをバックアップします。 ホットバックアップシステムは、サービスエントリのバックアップが有効になっている限り、他のアプリケーションプロトコル用に作成されたセッションをバックアップします。 非対称パストラフィックがホットバックアップシステムを通過する場合に、HTTP および DNS バックアップをイネーブルにします。HTTP および DNS バックアップは、フローおよびそのリターントラフィックがホットバックアップメンバーで正しく処理されることを保証します。

	ホットバックアップのアクティブ/スタンバイモードが使用されている場合、または対称パストラフィックのみがホットバックアップシステムを通過する場合は、HTTP および DNS バックアップを無効にすると、遅延データ同期を犠牲にしてホットバックアップメンバーのパフォーマンスを向上させることができます。HTTP および DNS バックアップを無効にする場合は、ネットワークへの影響を十分に認識していることを確認してください。パケット交換がアクティブでない場合、デバイスは DNS または HTTP 接続を削除します。スイッチオーバーによって接続が中断されると、DNS または HTTP クライアントはすぐに接続を再開しますが、ユーザーサービスへの影響はほとんどありません。
Configuration consistency check	コンフィギュレーション一貫性チェック機能のステータスを設定します。
Automatic configuration synchronization	自動設定同期機能のステータスを設定します。 この機能をイネーブルにすると、プライマリデバイスはその設定をセカンダリデバイスに一括でバックアップします。プライマリデバイスの設定が変更されると、プライマリデバイスは新しい設定をセカンダリデバイスにリアルタイムでバックアップします。 同期化する構成の量が多い場合、バルク同期化には 1 時間から 2 時間かかることがあります。バルク同期化の時間を短縮するためのベストプラクティスとして、ホットバックアップシステムを構成するときにこの機能を有効にします。

トラック設定を構成します。関連するパラメーターの詳細については、表 2 を参照してください。

表 2:トラックパラメーター

パラメーター	説明
Track entry association	ホットバックアップシステムで監視するトラックエントリを選択します。監視対象のトラックエントリの 1 つが Negative になった場合、ホットバックアップシステムはアクティブ/スタンバイスイッチオーバーを実行し、トラフィックを新しいアクティブデバイスに切り替えてサービスの継続性を確保します。

OK をクリックします。

Check または **Synchronize configuration** をクリックして、**Hot Backup** ページで設定の一貫性をチェックするか、設定を同期します。

表 3 構成の整合性チェックと構成の同期パラメーター

パラメーター	説明

Check	構成の整合性チェックを手動で実行します。
Synchronize configuration	プライマリデバイスの設定をセカンダリデバイスに手動で同期します。

Hot Backup ページの **Switch states** をクリックして、ホットバックアップシステム内のデバイスの状態を切り替えます。

表 4 状態切り替えパラメーター

パラメーター	説明
Switch states	ホットバックアップシステム内のデバイスの状態を手動で切り替えます。このタスクは、アクティブデバイスのハードウェアの交換が必要な場合に実行できます。 この作業は、ホットバックアップシステムがアクティブ/スタンバイモードで動作しているときに、アクティブメンバーデバイスだけで実行できます。 ホットバックアップで VRRP が使用されている場合、このタスクの実行後に一時的な VRRP 仮想 IP の競合が発生する可能性があります。この競合はサービスには影響しません。

Configure VRRP collaboration

VRRP ページでホットバックアップシステムを VRRP に関連付けます。設定手順の詳細については、VRRP のヘルプを参照してください。

Configure the hot backup system to collaborate with a routing protocol

System タブをクリックします。

ナビゲーションペインで、**High Availability** > **Hot Backup** を選択します。

Hot Backup ページが開きます。

Configure をクリックします。

Configure Hot Backup ページが開きます。

ルーティングコラボレーションパラメータを構成します。関連パラメーターの詳細については、表 3 を参照してください。

表 5 ルーティングコラボレーションパラメーター

パラメーター	説明
OSPF	OSPF によってアドバタイズされるリンクコストを調整します。
IS-IS	IS-IS によってアドバタイズされるリンクコストを調整します。

BGP	BGP によってアドバタイズされるリンクコストを調整します。
OSPFv3	OSPFv3 によってアドバタイズされるリンクコストを調整します。
Set absolute cost	絶対リンクコストを入力します。ホットバックアップシステムは、この値を使用して、アドバタイズされるリンクコストを置き換えます。
Set increment cost	増分値を入力します。ホットバックアップシステムは、アドバタイズされるリンクコストにこの値を追加します。

OK をクリックします。

Configure transparent in-path deployment

System タブをクリックします。
ナビゲーションペインで、**High Availability** > **Hot Backup** を選択します。
Hot Backup ページが開きます。
Configure をクリックします。
Configure Hot Backup ページが開きます。
監視パラメーターを構成します。関連するパラメーターの詳細は、表 4 を参照してください。

表 6 監視パラメーター

パラメーター	説明
Interface	ホットバックアップシステムで監視するインターフェースを選択します。 集約メンバーポートを監視するようにホットバックアップシステムを設定することはできません。 ホットバックアップシステムは、インターフェースステータスの一貫性を確保するために、監視対象インターフェースのステータスを監視します。監視対象インターフェースは、すべての監視対象インターフェースが起動している場合にのみトラフィックを転送できます。
VLAN	ホットバックアップシステムで監視する VLAN を選択します。 ホットバックアップシステムは、監視対象 VLAN のメンバーポートを監視して、メンバーポートステータスの一貫性を確保します。監視対象 VLAN 内のポートは、VLAN 内のすべてのポートが起動している場合にだけトラフィックを転送できます。 VLAN 1 を監視するようにホットバックアップシステムを設定することはできません。デフォルトでは、すべてのアクセスポートは VLAN 1 に属しています。VLAN 1 を監視するようにホットバックアップシステムを設定すると、未使用のポートが VLAN 1 でダウン状態になると、使用中のポートのトラフィック転送が影響を受けます。

OK をクリックします。

VRRP

このヘルプには、次のトピックがあります。

Introduction

Virtual Router Redundancy Protocol(VRRP)は、ネットワークゲートウェイのグループを仮想ルータと呼ばれる VRRP グループに追加します。VRRP グループには 1 つのマスターと複数のバックアップがあり、仮想 IP アドレスを提供します。サブネット上のホストは、仮想 IP アドレスをデフォルトのネットワークゲートウェイとして使用して、外部ネットワークと通信します。

VRRP は単一障害点を回避し、ホスト上の設定を簡素化します。マルチキャストまたはブロードキャスト LAN(イーサネットネットワークなど)上の VRRP グループ内のマスターに障害が発生すると、VRRP グループ内の別のデバイスが処理を引き継ぎます。スイッチオーバーは、動的なルートの再計算、ルートの再検出、ホスト上のゲートウェイの再設定、またはトラフィックの中断を引き起こすことなく完了します。

VRRP group

VRRP は、仮想ルータと呼ばれる VRRP グループにネットワークゲートウェイのグループを追加します。VRRP グループには 1 つのマスターと複数のバックアップがあります。

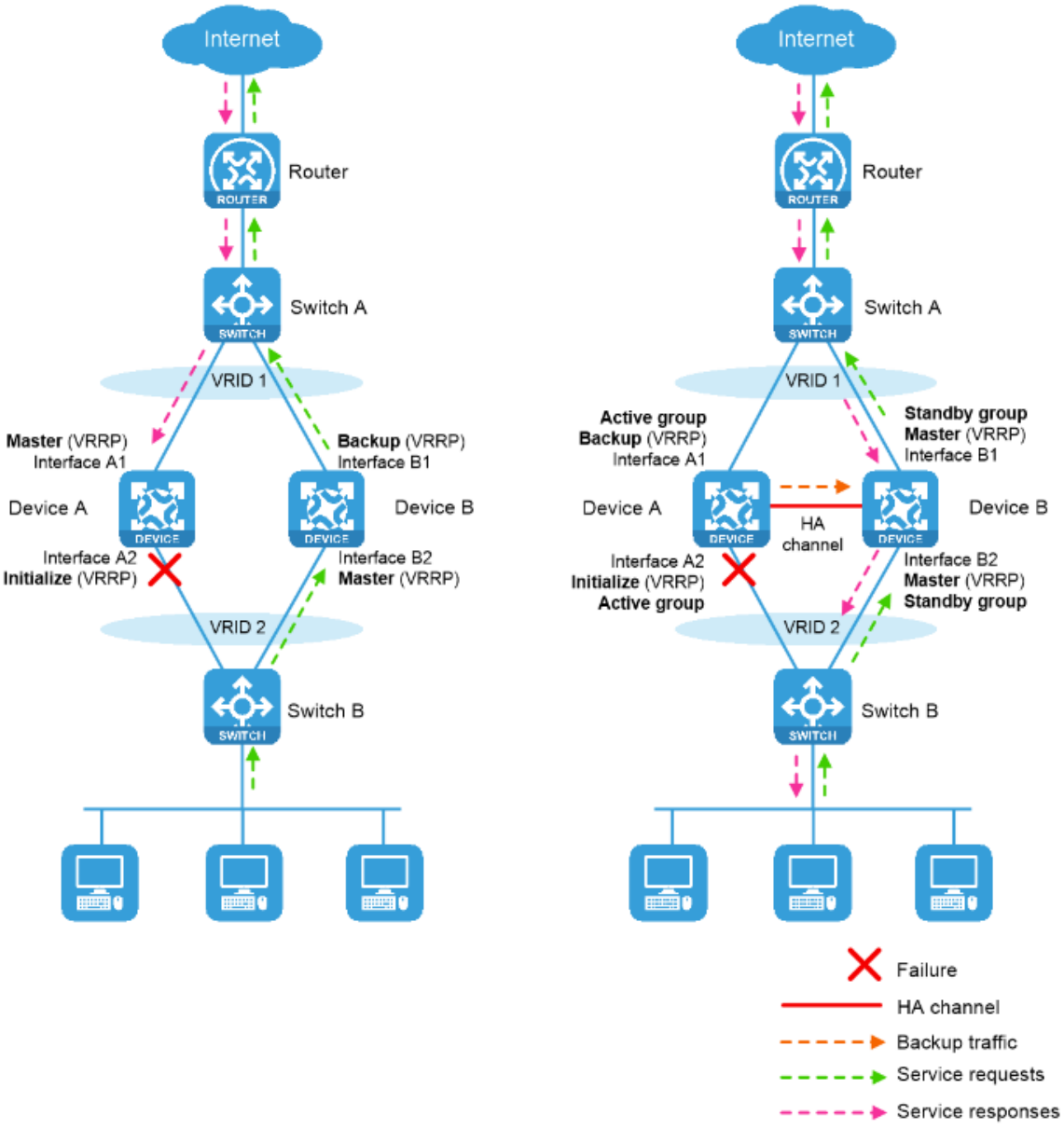
Collaboration with HA group

About collaboration with HA group

図 1 は、一般的な VRRP ネットワーク(左側)と VRRP-HA グループアソシエーションが設定されたネットワーク(右側)を示しています。一般的な VRRP ネットワークでリンクスイッチオーバーが発生すると、アップリンクとダウンリンクの VRRP グループのマスターが異なるデバイス上にある場合、トラフィックが中断されることがあります。

この問題を解決するには、HA グループを使用して、さまざまな VRRP グループでマスター/バックアップ状態のスイッチオーバーを制御します。

図 1 ネットワーク図



VRRP active/standby group

VRRP アクティブ/スタンバイグループは、マスター状態またはバックアップ状態になることができます。これにより、関連付けられた VRRP グループ内のデバイスの状態が決まります。たとえば、VRRP アクティブグループがマスター状態の場合、関連付けられた VRRP グループ内のすべてのデバイスがマスターになります。

VRRP アクティブ/スタンバイグループの初期状態は次のとおりです。

Active/Standby mode: プライマリ管理デバイスでは、VRRP アクティブグループとスタンバイグループの初期状態はマスターです。セカンダリ管理デバイスでは、VRRP アクティブグループとスタンバイグループの初期状態はバックアップです。

Dual-active mode: VRRP アクティブ/スタンバイグループの状態は、HA ロールの影響を受けません。初期状態は、VRRP アクティブグループではマスターであり、VRRP スタンバイグループではバックアップです。

VRRP master election in the HA group environment

図 1 に示すように、VRRP-HA グループアソシエーションが設定されたネットワークでは、VRRP グループ内のマスター/バックアップ状態のスイッチオーバーは次のようになります。

通常、VRRP アクティブグループステートはデバイス A 上のマスター(プライマリデバイスと想定)であるため、デバイス A は VRRP グループ 1 と VRRP グループ 2 の両方の両方のマスターです。VRRP スタンバイグループの状態は、デバイス B(セカンダリデバイスと想定)上のバックアップであるため、デバイス B は VRRP グループ 1 と VRRP グループ 2 の両方のバックアップです。

インターフェース A2(デバイス A 上のダウンリンクインターフェース)に障害が発生すると、HA グループはインターフェース障害イベントを受信します。次に、HA グループはアップデートパケットで VRRP アクティブ/スタンバイグループステート変更イベントをデバイス B に通知し、VRRP スタンバイグループステートをマスターに変更するようデバイス B に要求します。

デバイス B はアップデートパケットを受信すると、VRRP スタンバイグループの状態をマスターに変更します。その間に、デバイス B は VRRP グループ 1 および VRRP グループ 2 の状態をマスターに変更します。状態の変更後、デバイス B はデバイス A に応答を送信します。

応答を受信すると、デバイス A は VRRP アクティブグループの状態を backup に変更します。その間、デバイス A は VRRP グループ 1 および VRRP グループ 2 の状態を backup に変更します。

インターフェース A2 が回復したときにトラフィックを元に戻すために、デバイスは、上記の手順と同様の別のマスター/バックアップ状態のスイッチオーバーを実行します。

Virtual IP address

VRRP グループは仮想 IP アドレスを提供します。サブネット上のホストは、仮想 IP アドレスをデフォルトのネットワークゲートウェイとして使用して、外部ネットワークと通信します。
仮想ルータの仮想 IP アドレスは、次のいずれかの IP アドレスになります。
VRRP グループが存在するサブネット上の未使用の IP アドレス。
VRRP グループ内のデバイス上のインターフェースの IP アドレス。
後者の場合、ルータは IP アドレスオーナーと呼ばれます。

Device priority in a VRRP group

VRRP は、VRRP グループ内の各ルータの役割(マスターまたはバックアップ)をプライオリティによって決定します。プライオリティが高いルータは、マスターになる可能性が高くなります。
VRRP プライオリティは 0～255 の範囲で指定できます。値が大きいほどプライオリティが高くなります。プライオリティ 1～254 は設定可能です。プライオリティ 0 は特別な用途のために予約されており、プライオリティ 255 は IP アドレスオーナー用です。VRRP グループ内の IP アドレスオーナーの実行プライオリティは常に 255 であり、正常に動作している限りマスターとして機能します。VRRP グループに設定できる IP アドレスオーナーは 1 つだけです。

Preemption

VRRP グループ内のルータは、非プリエンプティブモードまたはプリエンプティブモードで動作します。
Preemptive mode:バックアップは新しいマスターの選定を開始し、現在のマスターよりも高いプライオリティを持つことを検出するとマスターを引き継ぎます。プリエンプティブモードでは、VRRP グループ内で最高のプライオリティを持つルータが常にマスターとして動作します。
Non-preemptive mode:マスタールータは、後でバックアップルータに高いプライオリティが割り当てられた場合でも、正常に動作している限りマスターとして機能します。非プリエンプティブモードを使用すると、マスタールータとバックアップルータ間の頻繁なスイッチオーバーを回避できます。
VRRP プリエンプション遅延タイマーは、次の目的で設定できます。
VRRP グループ内のメンバー間で状態が頻繁に変更されないようにします。
情報(ルーティング情報など)を収集するための十分な時間をバックアップに与えます。
プリエンプティブモードでは、ローカルプライオリティよりも低いプライオリティを持つアドバタイズメントを受信しても、バックアップはすぐにマスターになることはなく、一定時間待機してからマスターになります。

Preemption delay

プリエンプティブモードでは、ローカル優先度よりも低い優先度の通知を受信すると、バックアップは一定期間(プリエンプト遅延)待機してからマスターを引き継ぎます。プリエンプト遅延が 0 の場合、バックアップはすぐにマスターを引き継ぎます。

VRRP advertisement interval

VRRP グループ内のマスターは、定期的に VRRP アドバタイズメントを送信して、その存在を宣言します。システムの安定性を維持するためのベストプラクティスとして、VRRP アドバタイズメントインターバルを 100 センチ秒よりも大きく設定します。

VRVRv 2 では、IPv4 VRRP グループ内のすべてのルータは、同じ VRRP 通知間隔を持たなければなりません。

VRVRv 3 では、VRRP グループ内のルータは、VRRP 通知を送信するために異なる間隔を持つことができます。VRRP グループ内のマスターは、指定された間隔で VRRP 通知を送信し、通知内の間隔を保持します。バックアップが通知を受信した後、バックアップは通知内の間隔を記録します。バックアップがタイマー(3×記録された間隔+Skew_Time)の期限が切れる前に VRRP 通知を受信しない場合、バックアップはマスターを障害が発生したと見なし、引き継ぎます。

大量のネットワークトラフィックがあると、バックアップが指定された時間内にマスターから VRRP 通知を受信できない場合があります。その結果、予期しないマススイッチオーバーが発生します。この問題を解決するには、より大きな間隔を設定します。

Authentication method

許可されていないユーザーからの攻撃を回避するために、VRRP メンバーは VRRP パケットに認証キーを追加して、相互に認証します。VRRP は次の認証方式を提供します。

Simple authentication:送信側は VRRP パケットに認証キーを設定し、受信側は受信した認証キーを自身のローカル認証キーと比較します。2 つの認証キーが一致する場合、受信した VRRP パケットは正当です。一致しない場合、受信したパケットは不正であり、廃棄されます。

MD5 authentication:送信側は認証キーと MD5 アルゴリズムを使用して VRRP パケットのダイジェストを計算し、その結果をパケットに保存します。受信側は認証キーと MD5 アルゴリズムを使用して同じ操作を実行し、その結果を認証ヘッダーの内容と比較します。結果が一致する場合、受信した VRRP パケットは正当です。一致しない場合、受信したパケットは不正であり、廃棄されます。

安全なネットワークでは、VRRP パケットを認証しないように選択できます。

VRRP control VLAN

デフォルトでは、あいまいな VLAN 終端が設定されたマスター上のレイヤー3 イーサネットサブインターフェースは、ブロードキャストパケットまたはマルチキャストパケットの送信をサポートしません。マスターがマルチキャストで VRRP アドバタイズメントをバックアップに定期的に送信できるようにするには、VLAN 終端対応サブインターフェースをイネーブルにして、ブロードキャストパケットおよびマルチキャストパケットを送信します。これにより、マスターは、VLAN パケットがサブインターフェースによって終端されるように設定されているすべての VLAN 内で VRRP アドバタイズメントを送信できます。広範囲の VLAN のレイ

ヤー3 イーサネットサブインターフェース上であいまいな VLAN 終端が設定されている場合、VRRP アドバタイズメントによってサブインターフェースが過負荷になる可能性があります。これは、ルータのパフォーマンスに悪影響を及ぼします。

この問題を解決するには、VLAN 終端対応サブインターフェースによるブロードキャストパケットおよびマルチキャストパケットの送信をディセーブルにして、VRRP 制御 VLAN を設定します。マスターは、制御 VLAN 内だけで VRRP アドバタイズメントを送信します。

VLAN 終端タイプに従って VRRP 制御 VLAN を指定します。

Dot1q 終端があいまいな場合は、VLAN タグの最も外側のレイヤーで 1 つのコントロール VLAN を指定します。

あいまいな QinQ 終端の場合は、VLAN タグの最も外側の 2 つのレイヤーで 2 つのコントロール VLAN を指定します。

Restrictions and guidelines

IPv4 VRVRv 3 と IPv6 VRVRv 3 は VRRP パケット認証をサポートしません。

インターフェース上の VRRP グループには、異なる認証モードと認証キーを設定できます。ただし、同じ VRRP グループのメンバーは、同じ認証モードと認証キーを使用する必要があります。

Configure VRRP

Configure basic VRRP settings

System > High Availability > VRRP を選択します。

Create をクリックします。

VRRP グループを作成します。

表 1 基本的な VRRP 設定項目

項目	説明
Interface	VRRP グループが存在するインターフェースを指定します。
VRID	VRRP グループを一意に識別する仮想ルータ ID を入力します。異なるデバイス上で同じ VRID を共有する VRRP グループは、1 つの VRRP グループを示します。
IP type	IPv4 または IPv6 VRRP を指定します。
Associate with HA Group	VRRP-HA グループアソシエーションシナリオでこのパラメータを設定して、VRRP グループ間のコラボレーションをイネーブルにします。

Virtual IP/mask length	VRRP グループの仮想 IP アドレスを入力します。
Priority	プライオリティを入力します。プライオリティが高いほど、デバイスが VRRP グループのマスターになる可能性が高くなります。
Preemption mode	プリエンプトモード(プリエンプトまたは非プリエンプト)を選択します。
Preemption delay	プリエンプト遅延時間を入力します。バックアップデバイスは、マスターとしてプリエンプトされる前に、指定された時間待機します。0 は、デバイスがマスターとしてすぐにプリエンプトされることを意味します。
Advertisement interval	VRRP パケットのアドバタイズメント間隔を設定します。 VRRPv 2 では、有効値は 100 の倍数だけです。例えば、値を 10~100、101~200、4001~4095 と設定した場合、有効値はそれぞれ 100、200、4100 となります。 VRRPv3 では、設定された値が有効になります。
Auth mode	**no authentication**、**simple authentication**、または **MD5 authentication** モードを指定します。 VRRP は、認証キーを追加して VRRP パケットを検証し、偽造パケットによる攻撃を防止します。

Configure advanced VRRP settings

System > High Availability > VRRP Advanced Settings の順に選択します。
ターゲット VRRP グループの **Edit** をクリックします。
高度な VRRP グループ設定を行います。

表 2 高度な VRRP 設定項目

項目	説明
Interface	VRRP グループがバインドされるインターフェースを指定します。
Version	VRRPv 2 または VRRPv 3 を選択します。VRRPv 2 は IPv4 VRRP のみをサポートします。VRRPv 3 は IPv4 VRRP と IPv6 VRRP の両方をサポートします。 IPv4 VRRP グループ内のすべてのルータは、同じ IPv4 VRRP バージョンを使用する必要があります。
Control VLAN	あいまいな Dot1q 終端が設定されたサブインターフェースのコントロール VLAN を指定します。
Inner VLAN	あいまい QinQ 終端が設定されたサブインターフェースの内部 VLAN を指定します。

TRACK

このヘルプには、次のトピックがあります。

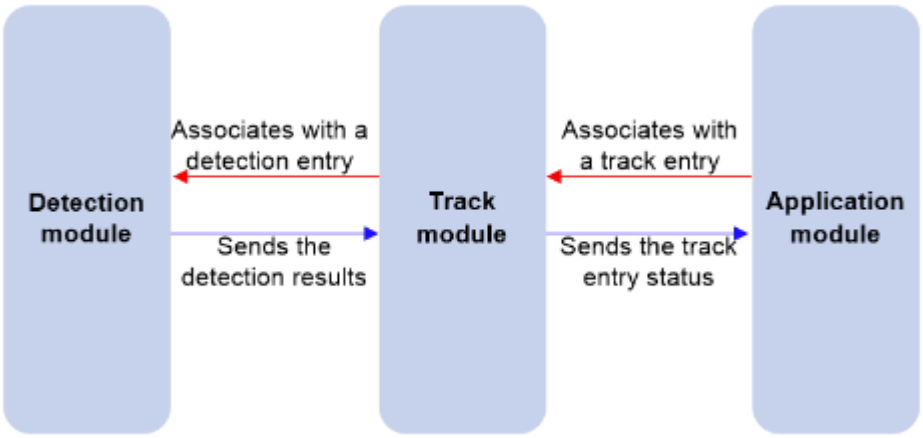
Introduction

Track モジュールは、アプリケーションモジュールと検出モジュールの間で機能します。Track モジュールは、アプリケーションモジュールから様々な検出モジュール間の差異を遮蔽します。

Collaboration mechanism

Track モジュールは、検出モジュールおよびアプリケーションモジュールと連携します。
図 1 に示すように、Track モジュールを検出モジュールおよびアプリケーションモジュールに関連付けると、コラボレーションが有効になり、次のように動作します。
検出モジュールは、インターフェースステータス、リンクステータス、ネットワーク到達可能性、ネットワークパフォーマンスなどの特定のオブジェクトをプローブし、検出結果を Track モジュールに通知します。
Track モジュールは、検出結果をアプリケーションモジュールに送信します。
追跡対象オブジェクトの変更が通知されると、アプリケーションモジュールは、通信の中断およびネットワークパフォーマンスの低下を回避するように対応できます。

図 1 Track モジュールを介したコラボレーション



Collaboration between the Track module and a detection module

検出モジュールは、追跡されたオブジェクトの検出結果を Track モジュールに送信します。Track モジュールは、次のようにトラックエントリのステータスを変更します。

トラックされたオブジェクトが正常に動作している場合、トラックエントリの状態は Positive です。たとえば、次のいずれかの条件では、トラックエントリの状態は Positive です。

ターゲットインターフェースがアップしています。

ターゲットネットワークに到達可能です。

トラックされたオブジェクトが正しく動作しない場合、トラックエントリの状態は Negative です。たとえば、次のいずれかの状況では、トラックエントリの状態は Negative です。

ターゲットインターフェースがダウンしています。

ターゲットネットワークに到達できません。

検出結果が無効の場合、トラックエントリの状態は NotReady になります。たとえば、関連する NQA 操作が存在しない場合、トラックエントリの状態は NotReady になります。

Collaboration between the Track module and an application module

トラックモジュールは、トラックエントリのステータス変更をアプリケーションモジュールに報告します。アプリケーションモジュールは、通信の中断とネットワークパフォーマンスの低下を回避するために、正しいアクションを実行できます。

Configure Track

System > **High Availability** > **Track**.を選択します。

Add をクリックします。

トラックエントリを作成します。

表 1 基本的なトラック構成項目

項目	説明
Track entry	トラックエントリを一意に識別するトラックエントリ ID を入力します。
Detection module	トラックに関連付ける検出モジュールを選択します。
Positive notification delay	トラックエントリの状態が Positive に変更されたことをアプリケーションモジュールに通知する遅延を指定します。 Track モジュールがアプリケーションモジュールに対して、トラックエントリの状態変更を即時に通知しても、ルートの収束が完了しない場合は、通信障害が発生する可能性があります。このような場合は、通知の遅延を設定して、トラックエントリの状態変更が即時に通知されないようにできます。 通知遅延設定は、トラックエントリがアプリケーションモジュールに関連付けられていない場合は有効になりません。
Negative notification delay	トラックエントリの状態が Negative に変化したことをアプリケーションモジュールに通知する遅延を指定します。 Track モジュールがアプリケーションモジュールに対して、トラックエントリの状態変更を即時に通知しても、ルートの収束が完了しない場合は、通信障害が発生する可能性があります。このような場合は、通知の遅延を設定して、トラックエントリの状態変更が即時に通知されないようにできます。 通知遅延設定は、トラックエントリがアプリケーションモジュールに関連付けられていない場合は有効になりません。

表 2 Track-BFD アソシエーションの設定項目

項目	説明
BFD packet output interface	BFD エコーパケットを送信するインターフェースを選択します。トラックは、エコーモード BFD セッションだけに関連付けることができます。
Local IP	BFD セッションのローカル IP アドレスを入力します。
Remote IP	BFD セッションのリモート IP アドレスを入力します。

表 3 Track-NQA 関連付け構成項目

項目	説明

NQA operation administrator	NQA オペレーションを作成する NQA オペレーション管理者の名前を入力します。
Operation tag	NQA オペレーションタグを入力します。
Sequence number	トラックエントリに関連付けるリアクションエントリの ID を入力します。

表 4 Track-interface アソシエーションの構成項目

項目	説明
Monitored interface	トラックに関連付けるインターフェースを選択します。
Monitored interface attribute	物理状態、データリンク層状態、IPv4、または IPv6 のいずれかのインターフェース属性を選択します。

表 5 トラックとルートの関連付けの構成項目

項目	説明
VPN instance	[Track]に関連付けるルートの VPN インスタンスを選択します。
IP	ルートエントリの IP アドレスをドット付き 10 進表記で入力します。
Mask length	IP アドレスのマスク長を入力します。

BFD

Introduction

Bidirectional Forwarding Detection(BFD)は、メディアおよびプロトコルに依存しない汎用の標準高速障害検出メカニズムです。BFD は、転送パスの接続を検出および監視して、通信障害を迅速に検出できるため、サービスの継続性を確保し、ネットワークの可用性を向上させるための措置を講じることができます。

BFD は、ルーティングプロトコルなどの上位層プロトコルについて、2 つのデバイス間の双方向転送パスの障害を均一かつ迅速に検出できます。上位層プロトコルで使用される hello メカニズムでは、リンク障害の検出に数秒かかりますが、BFD ではミリ秒単位で検出できます。

BFD セッションはエコーパケットを使用して検出を実装します。エコーパケットは、ポート番号 3785 の UDP パケットにカプセル化されます。

リンクのローカルエンドはエコーパケットを送信して、BFD セッションを確立し、リンクステータスを監視します。ピアエンドは BFD セッションを確立せず、パケットを発信元エンドに戻すだけです。ローカルエンドが検出時間内にピアエンドからエコーパケットを受信しない場合、セッションはダウンしていると見なされます。

Configure BFD

System > **High Availability** > **BFD** を選択します。

BFD を設定します。

表 1:BFD 設定項目

項目	説明
Echo packet source IPv4	エコーパケットの送信元 IPv4 アドレスを指定します。 ベストプラクティスとして、ローカルインターフェースの IP アドレスと同じネットワークセグメント上にない IPv4 アドレスを指定します。この動作により、ピアが大量の ICMP リダイレクトパケットを送信してリンク輻輳が発生するのを防ぐことができます。
Echo packet source IPv6	エコーパケットの送信元 IPv6 アドレスを指定します。 ベストプラクティスとして、ローカルインターフェースの IP アドレスと同じネットワークセグメント上にない IPv6 アドレスを指定します。この動作によ

	り、ピアが大量の ICMPv6 リダイレクトパケットを送信してリンク輻輳が発生することが防止されます。

NQA

Introduction

NQA

Network Quality Analyzer(NQA)を使用すると、ネットワークパフォーマンスの測定、IP サービスとアプリケーションのサービスレベルの確認、およびネットワークの問題のトラブルシューティングを行うことができます。

NQA operating mechanism

図 1 に示すように、NQA ソースデバイス(NQA クライアント)は、IP サービスとアプリケーションをシミュレートしてネットワークパフォーマンスを測定することによって、NQA ターゲットデバイスにデータを送信します。
すべてのタイプの NQA 操作には NQA クライアントが必要ですが、NQA サーバーが必要なのは TCP 操作のみです。FTP などの宛先デバイスによってすでに提供されているサービスの NQA 操作には、NQA サーバーは必要ありません。NQA サーバーを構成して、特定の IP アドレスおよびポートをリスニングして応答し、様々なテストニーズを満たすことができます。

図 1 ネットワーク図

Collaboration with Track

NQA は Track モジュールと連携して、アプリケーションモジュールが事前定義されたアクションを実行できるように、状態またはパフォーマンスの変更をアプリケーションモジュールに通知できます。Track の詳細については、Track のヘルプを参照してください。

Threshold monitoring

しきい値の監視により、NQA 操作のパフォーマンスメトリックが指定されたしきい値に違反した場合に、NQA クライアントは事前定義されたアクションを実行できます。

Configure NQA

NQA を設定するには:

System タブをクリックします。

ナビゲーションペインで、**High Availability** > **NQA** を選択します。

Add をクリックします。

NQA 操作を設定します。

表 1 NQA オペレーションの構成項目

項目	説明
NQA operation administrator	nQA 操作の管理者名を入力します。nQA 操作は、管理者名と操作タグで識別されます。
Operation tag	NQA 操作タグを入力します。
Probe mode	プローブモードを選択します。NQA は、リンク検出に異なるプロトコルのパケットを使用することをサポートします。
Destination IP	プローブパケットの宛先 IP アドレスを入力します。 このパラメータは、UDP ジッタ動作だけに適用されます。
Destination port	プローブパケットの宛先ポート番号を入力します。
Probe interval	NQA 操作を繰り返す間隔を設定します。 間隔を 0 に設定すると、NQA は操作を 1 回だけ実行し、統計情報は生成しません。
Probe times	プローブ時間を指定します。1 つの操作で複数のプローブを実行する場合、NQA クライアントは次のいずれかの条件で新しいプローブを開始します。 NQA クライアントは、最後のプローブで送信されたパケットに対する応答を受信します。 プローブタイムアウト時間が経過します。
Probe timeout	応答待ちのタイムアウト時間を設定します。
Save history records	NQA 操作の履歴レコードの保存を有効にします。この機能を無効にすると、NQA 操作の既存の履歴レコードが削除され、履歴レコードは保存されなくなります。
Max history records	NQA 操作用に保存できる履歴レコードの最大数を設定します。 NQA 操作の履歴レコードの数が最大数を超えると、最も古い履歴レコードが削除されます。
Starting time	NQA 操作の開始時間を設定します。 **Immediately**: 設定が展開された直後に NQA 操作が開始されます。

	Scheduled time: NQA 動作はスケジュールされた時刻に開始されます。
Operation duration	動作期間を設定します。 **Permanent**:: デバイスは NQA 動作を無期限に繰り返します。 **Specified duration**: デバイスは期間中に NQA 動作を繰り返します。

表 2 NQA しきい値モニタリングの構成項目

項目	説明
Reaction entry ID	応答エントリの ID を入力します。
Monitored element	モニターされる要素を選択します。 **probe-duration**:プローブの継続時間。 **probe-fail**:プローブ障害の数。
Threshold type	しきい値のタイプを選択します。 **Accumulate**:しきい値違反の合計数をチェックします。 **Consecutive**:NQA 操作の開始後に連続して発生したしきい値違反の数をチェックします。
Probe failures	動作の失敗を判断するためのプローブの失敗回数を設定します。
Threshold value range	しきい値の範囲を入力します。
Triggered action	トリガーされたアクションを選択します。 **None**:モニタリング結果をローカルに記録します。 **Trap-only**:モニタリング結果を記録し、SNMP トラップメッセージを NMS に送信します。このアクションを選択した場合は、**System** > **Maintenance** > **SNMP** ページでトラップメッセージレシーバホストを設定する必要があります。 **Trigger-only**: 監視結果をローカルに記録し、他のモジュールとのコラボレーションをトリガーします。このパラメーターは、監視対象要素が **probe-fail** である場合にのみサポートされます。

Basic log settings

このヘルプには、次のトピックが含まれています。

- Introduction
  - Syslog
  - Flow log
  - Fast log
  - Storage space settings
  - Log severity levels
  - Security management and audit
- Restrictions and guidelines
- Configure basic log settings
  - Configure syslog
  - Configure flow log
  - Configure fast log output
  - Configure storage space settings
  - Configure security management and audit

Introduction

デバイスは、サービスモジュールによって処理されたパケットに基づいて、サービスモジュールのさまざまなタイプのログを生成します。これらのログは、ネットワーク管理者によるネットワークパフォーマンスの監視、ネットワーク問題のトラブルシューティング、およびユーザーのネットワークアクセス動作の追跡、記録、分析、監査に役立ちます。

デバイスは、次の方法を使用したログ出力をサポートします。

- Syslog。
- Flow log。
- Fast log output。

syslog

syslog エントリは ASCII 形式です。

デバイス上の情報センターは、ソースモジュールによって生成された syslog メッセージを受信し、次の宛先にログを出力します。

- Console。

- Monitor terminal。
- Log buffer。
- Log host。
- Log file。

Flow log

About flow log

フローログには、フローに基づいて外部ネットワークへのユーザーアクセスが記録されます。各フローは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル番号の 5 タプルによって識別されます。
フローログは、NAT セッションに基づいてエントリを作成します。

Flow log versions

フローログには、バージョン 1.0、バージョン 3.0 およびバージョン 5.0 の 3 つのバージョンがあります。表 1、表 2 および表 3 に、各バージョンで使用可能なフィールドを示します。デバイスに表示されるフィールドは、使用したログ分析ツールによって、表にリストされているフィールドと異なる場合があります。

表 1 フローログ 1.0 のフィールド

フィールド	説明
SrcIP	NAT 前の送信元 IP アドレス。
DestIP	NAT 前の宛先 IP アドレス。
SrcPort	NAT 前の送信元 TCP/UDP ポート番号。
DestPort	NAT 前の宛先 TCP/UDP ポート番号。
StartTime	フローの開始時間(秒単位)。
EndTime	フローの終了時間(秒単位)。 **Operator** フィールドが **6**(アクティブフローの通常の接続チェックレコード)の場合、このフィールドは 0 です。
Protocol	プロトコル番号。
Operator	フローログエントリが生成された理由: • 0: 予約済み • 1: フローは正常に終了しました。 • 2: エージングタイマーの期限切れにより、フローがエージングアウトしました。

	• 3: 設定変更または手動による削除のため、フローがエージングアウトしました。 • 4: リソース不足のため、フローが期限切れになりました。 • 5: 予約。 • 6: アクティブフローの通常の接続チェックレコード。 • 7: フローテーブルがいっぱいになったときに新しいフローが作成されたため、フローが削除されました。 • 8: フローが作成されました。 • FE: その他の理由 • 10-FE-1: 将来の使用のために予約済み。
Reserved	将来の使用のために予約されています。

表 2:フローログ 3.0 のフィールド

フィールド	説明
Protocol	プロトコル番号。
Operator	フローログが生成された理由: • 0: 予約済み • 1: フローは正常に終了しました。 • 2: エージングタイマーの期限切れにより、フローがエージングアウトしました。 • 3: 設定変更のため、フローがエージングアウトしました。 • 4: リソース不足のため、フローが期限切れになりました。 • 5: 予約。 • 6: アクティブフローの通常の接続チェックレコード。 • 7: フローテーブルがいっぱいになったときに新しいフローが作成されたため、フローが削除されました。 • 8: フローが作成されました。 • FE: その他の理由 • 10-FE-1: 将来の使用のために予約済み。
IPVersion	IP パケットのバージョン。
TosIPv4	IPv4 パケットの ToS フィールド。
SourceIP	NAT 前の送信元 IP アドレス。
SrcNatIP	NAT 後の送信元 IP アドレス。

DestIP	NAT 前の宛先 IP アドレス。
DestNatIP	NAT 後の宛先 IP アドレス。
SrcPort	NAT 前の送信元 TCP/UDP ポート番号。
SrcNatPort	NAT 後の送信元 TCP/UDP ポート番号。
DestPort	NAT 前の宛先 TCP/UDP ポート番号。
DestNatPort	NAT 後の宛先 TCP/UDP ポート番号。
StartTime	フローの開始時間(秒単位)。
EndTime	フローの終了時間(秒単位)。 Operator フィールドが 6(アクティブフローの通常の接続チェックレコード)の場合、このフィールドは 0 です。
InTotalPkg	セッションで受信されたパケット数。
InTotalByte	セッションで受信したバイト数。
OutTotalPkg	セッションで送信されたパケットの数。
OutTotalByte	セッションで送信されたバイト数。
InVPNID	送信元 VPN インスタンスの ID。
OutVPNID	宛先 VPN インスタンスの ID。
Reserved1	予約済みフィールド。
AppID	アプリケーションプロトコル ID。
Reserved3	予約済みフィールド。

表 3 フローログ 5.0 のフィールド

フィールド	説明
Protocol	プロトコル番号。

Operator	フローログが生成された理由: • 0: 予約済み • 1: フローは正常に終了しました。 • 2: エージングタイマーの期限切れにより、フローがエージングアウトしました。 • 3: 設定変更のため、フローがエージングアウトしました。 • 4: リソース不足のため、フローが期限切れになりました。 • 5: 予約。 • 6: アクティブフローの通常の接続チェックレコード。 • 7: フローテーブルがいっぱいになったときに新しいフローが作成されたため、フローが削除されました。 • 8: フローが作成されました。 • FE: その他の理由 • 10-FE-1: 将来の使用のために予約済み。
IPVersion	IP パケットのバージョン。
TosIPv4	IPv4 パケットの ToS フィールド。
SourceIP	NAT 前の送信元 IP アドレス。
SrcNatIP	NAT 後の送信元 IP アドレス。
DestIP	NAT 前の宛先 IP アドレス。
DestNatIP	NAT 後の宛先 IP アドレス。
SrcPort	NAT 前の送信元 TCP/UDP ポート番号。
SrcNatPort	NAT 後の送信元 TCP/UDP ポート番号。
DestPort	NAT 前の宛先 TCP/UDP ポート番号。
DestNatPort	NAT 後の宛先 TCP/UDP ポート番号。
StartTime	フローの開始時間(秒単位)。
EndTime	フローの終了時間(秒単位)。 **Operator** フィールドが **6**(アクティブフローの通常の接続チェックレコード)の場合、このフィールドは 0 です。

InTotalPkg	セッションで受信されたパケット数。
InTotalByte	セッションで受信したバイト数。
OutTotalPkg	セッションで送信されたパケットの数。
OutTotalByte	セッションで送信されたバイト数。
InVPNID	送信元 VPN インスタンスの ID。
OutVPNID	宛先 VPN インスタンスの ID。
AppID	アプリケーションプロトコル ID。
UserName	ユーザー名。
Reserved1 Reserved2 Reserved3	予約済みフィールド。

Fast log

高速ログ出力機能により、ログホストへのログの高速出力が可能になります。
通常、サービスモジュールで生成されたログは、まずインフォメーションセンターに送信され、指定された宛先(ログホストなど)に出力されます。高速ログ出力が設定されている場合、サービスモジュールのログは、インフォメーションセンターではなくホストに直接送信されます。高速ログ出力は、インフォメーションセンターにログを出力する場合と比較して、システムリソースを節約します。

Storage space settings

デバイスは、サービスモジュールからログデータを収集して、集中分析とレポート作成を行います。
収集されたログデータは、ハードディスクに格納されることが好ましい。ハードディスクが存在しない場合、データは U ディスクに格納される。U ディスクも存在しない場合、データはメモリーに格納される。新しいハードディスクまたは U ディスクは、ログデータの格納に使用する前にパーティション化およびフォーマット化する必要がある。U ディスクへのログデータの格納のサポートは、デバイスモデルに依存する。
ストレージスペース設定機能を使用すると、トラフィックサービスおよび DPI サービスのストレージ時間制限、ストレージスペース制限、およびストレージ制限違反アクションを設定できます。

ストレージデバイスを取り外す前に、ストレージデバイスまたは保存されているデータが損傷しないように、次の手順を実行してください。

- Web インターフェースで **Unload** をクリックして、ストレージデバイスのファイルシステム上のサービスログプロセスの占有を削除します。
- CLI から、ユーザービューで **umount** コマンドを実行して、ストレージデバイス上のすべてのファイルシステムをアンマウントします。

ストレージスペース設定のサポートは、デバイスモデルによって異なります。

Storage time limit

保管期限は、ログデータを保管できる最大日数を指定します。
期限切れログデータの処理は、指定したアクションによって異なります。

- アクションが **Delete** の場合、システムは期限切れのログデータを削除し、イベントを記録するログメッセージを生成します。
- アクションが **Log-only** の場合、システムはログメッセージを生成しますが、期限切れデータは削除されません。

Storage space limit

ストレージスペース制限は、サービスのログデータが使用できる合計ストレージスペースの割合を指定します。
ストレージスペース制限を超えたサービスのログデータの処理は、指定したアクションによって異なります。

- アクションが **Delete** の場合、システムは古いログデータを削除して新しいデータを保存します。イベントを記録するログメッセージが生成されます。
- アクションが **Log-only** の場合、システムはログメッセージを生成しますが、古いログデータを削除して新しいデータを保存することはありません。

Action

サービスの記憶域制限に指定されたアクションは、記憶域制限を超えたときにシステムがサービスのログデータを処理する方法を決定します。
サポートされているアクションは次のとおりです。

- **Delete**: 最も古い日付で収集されたデータを削除し、ログメッセージを生成します。当日のデータは削除できません。
- **Log-only**: ログメッセージのみを生成します。記憶域の制限を超えると、古いデータは削除されず、新しいデータは保存できません。ログデータを表示するには、**Monitor > Device Logs > System Logs** に移動します。

Log severity level

ログは、0 から 7 までの 8 つの重大度レベルに降順で分類されます。ログ出力に重大度レベルを指定すると、指定したレベル以上の重大度レベルのログが出力されます。たとえば、重大度レベル 6(情報)を指定すると、重大度レベル 0 から 6 までのログが出力されます。

表 4 ログの重大度レベル

重大度の値	レベル	説明
0	Emergency	システムは使用できません。たとえば、システム認証が期限切れになっています。
1	Alert	ただちにアクションを実行する必要があります。たとえば、インターフェース上のトラフィックが上限を超えた場合です。
2.	Critical	クリティカルな状態です。たとえば、デバイス温度が上限を超えている、電源モジュールに障害が発生している、またはファントレイに障害が発生しています。
3.	Error	エラー状態。たとえば、リンク状態が変化した。
4.	Warning	警告状態。たとえば、インターフェースが切断された、メモリーリソースが使い果たされたなどです。
5.	Notification	正常ですが重要な状態です。たとえば、端末がデバイスにログインしたり、デバイスが再起動したりします。
6.	Informational	情報メッセージ。たとえば、コマンドまたは ping 操作が実行されます。
7.	Debugging	デバッグメッセージ。

Security management and audit

セキュリティー管理機能は、デバイス上でセキュリティー管理サービスプロセスをイネーブルにします。この機能がディセーブルの場合、セキュリティー管理サーバーを使用してデバイス上のセキュリティーサービスを管理または監査することはできません。

セキュリティー監査ログ機能を使用すると、デバイスはセキュリティー関連の設定をログに記録し、ログメッセージをセキュリティー監査サーバーに報告できます。ログメッセージには主に、管理者ポリシー、システムポリシー、およびセキュリティー関連ポリシーの操作で生成される syslog メッセージが含まれます。

セキュリティー管理および監査機能のサポートは、デバイスモデルによって異なります。

Restrictions and guidelines

指定されたログホストにモジュールのログを出力する方法(優先順位の高い順)をサポートしています。

- Fast log output。
- Flow log output。
- Syslog output。

モジュールに複数のログ出力方式を設定した場合は、最も高いプライオリティを持つ方式だけが有効になります。

Configure basic log settings

Configure syslog

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Log Settings** > **Basic Settings** を選択します。
3. **Syslog** タブをクリックします。
4. 基本的な syslog 設定を行います。

表 5 Syslog 設定項目

項目	説明
Output to log buffer	ログバッファへのシステムログ出力を有効にするには、この項目を選択します。 ログソースモジュールに基づいて、ログバッファへのシステムログ出力を有効にします。 • 別々のログバッファを持つモジュールによって生成されたログは、それぞれのログバッファに保存されます。 • たとえば、セッションログと攻撃防御ログは、それぞれセッションログバッファと攻撃防御ログバッファに保存されます。 • 他のモジュールによって生成されたログは、汎用ログバッファに保存されます。
Log buffer size	バッファできるログの最大数を入力します。 ログバッファがいっぱいになると、システムは最も古いログを新しいログで上書きします。 一般ログバッファのサイズを指定します。

5. **Apply** をクリックします。
6. **Create** をクリックします。

   Create Log Host ウィンドウが開きます。
7. ログホストを作成します。

表 6 ログホスト構成項目

項目	説明
Log host address	ログホストの IP アドレスまたはホスト名を入力します。
Port number	ログホストのポート番号を入力します。
VRF	ログホストが属する VRF(VPN インスタンス)を選択します。ログホストがパブリックネットワークに属している場合は、**Public network** を選択します。

8. **OK** をクリックします。
   新しいログホストが、**Syslog** タブのログホストリストに表示されます。

Configure flow log

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Log Settings** > **Basic Settings** を選択します。
3. **Flow Log** タブをクリックします。
4. 基本的なフローログ設定を行います。

表 7 フローログの設定項目

項目	説明
Log version	フローログバージョンを選択します。オプションは **1.0**、**3.0** および **5.0** です。 フローログエクスポート用に指定されたログホストで、指定されたフローログバージョンがサポートされていることを確認します。
Load balancing	フローログエントリのロードバランシングをイネーブルにするには、この項目を選択します。 デフォルトでは、ロードバランシングはディセーブルです。デバイスは、使用可能なすべてのログホストに各フローログエントリのコピーを送信します。 ロードバランシングモードでは、フローログエントリは、エントリに記録されている送信元 IP アドレス(NAT 前)に基づいてログホスト間で分散されます。同じ送信元 IP アドレスに対して生成されたフローログエントリは、同じログホストに送信されます。ログホストがダウンすると、送信されたフローログは失われます。

Source IP for log packets	フローログパケットの送信元 IP アドレスを指定します。 デフォルトでは、フローログパケットの送信元 IP アドレスは、発信インターフェースの IP アドレスです。 ログホストの送信元 IP アドレスによってフローログをフィルタリングする必要がある場合は、この項目を設定します。 ループバックインターフェースのアドレスをフローログパケットの送信元 IP アドレスとして使用することをお勧めします。ループバックインターフェースは常にアップ状態です。この設定により、ダウンする可能性のあるインターフェースでのエクスポートの失敗を回避できます。

5. **Apply** をクリックします。
6. **Create** をクリックします。

Create Log Host ウィンドウが開きます。

表 8 ログホスト構成項目

項目	説明
Log host address	ログホストの IP アドレスまたはホスト名を入力します。
Port number	ログホストのポート番号を入力します。
VRF	ログホストが属する VPN インスタンスを選択します。ログホストがパブリックネットワークに属している場合は、**Public network** を選択します。

7. **OK** をクリックします。

Flow Log タブのログホストリストに新しいログホストが表示されます。

Configure fast log output

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Log Settings** > **Basic Settings** を選択します。
3. **Fast Log Output** タブをクリックします。
4. 高速ログ出力設定を構成します。

表 9 高速ログ出力の設定項目

項目	説明

Log timestamp	ログタイムスタンプで使用するタイムゾーンを選択します。オプションは次のとおりです。 • **Greenwich Mean Time(GMT)**: 標準グリニッジ標準時(GMT)。 • **Local time**: 標準 GMT プラスまたはマイナスタイムゾーンオフセット。
Source IP for log packets	高速ログ出力の送信元インターフェースを選択します。発信インターフェースに関係なく、指定されたインターフェースのプライマリ IP アドレスが高速出力ログの送信元 IP アドレスとして使用されます。 デフォルトでは、高速出力ログの送信元 IP アドレスは、発信インターフェースのプライマリ IP アドレスです。 ログホストの送信元 IP アドレスでログをフィルタリングする必要がある場合は、この項目を設定します。 ログ出力を高速化するには、ループバックインターフェースのアドレスを送信元 IP アドレスとして使用することをお勧めします。ループバックインターフェースは常にアップ状態です。この設定により、ダウンする可能性のあるインターフェースでのエクスポートの失敗を回避できます。
Log character encoding	ログ出力を高速化するエンコードモードを選択します。オプションは次のとおりです: • **Default encoding**: GB18030 エンコーディングを使用してログを出力します。 • **UTF-8**: UTF-8 エンコーディングを使用してログを出力します。

5. **Apply** をクリックします。
6. **Create** をクリックします。

Create Log Host ウィンドウが開きます。

表 10:ログホスト構成項目

項目	説明
Log host address	ログホストの IP アドレスまたはホスト名を入力します。
Port numbe	ログホストのポート番号を入力します。
VRF	ログホストが属する VPN インスタンスを選択します。ログホストがパブリックネットワークに属している場合は、**Public network** を選択します。
Session logs	ログホストへのセッションログの高速出力を有効にするには、この項目を選択します。
NAT logs	ログホストへの NAT logs の高速出力を有効にするには、この項目を選択します。
Log format	この項目は、NAT logs 項目が選択されている場合にのみ使用できます。ログ出力形式を選択します。選択肢は、**China Unicom**、**China Telecom**、および **CMCC** です。
NAT session logs	この項目は、NAT logs 項目が選択されている場合にのみ使用できます。ログホストへの NAT セッションログの高速出力を有効にするには、この項目を選択します。
NAT444 user logs	この項目は、NAT logs 項目が選択されている場合にのみ使用できます。この項目を選択すると、NAT444 ユーザーログがログホストに高速で出力されます。
AFT logs	ログホストへの AFT ポートブロックログの高速出力を有効にするには、この項目を選択します。
Application audit logs	ログホストへのアプリケーション監査ログの高速出力を有効にするには、この項目を選択します。
URL filtering logs	ログホストへの URL フィルタリングログの高速出力を有効にするには、この項目を選択します。
Attack defense logs	攻撃防御ログをログホストに出力できるようにする場合に選択します。
Reputation logs	IP、URL、およびドメインレピュテーションログをログホストに高速で出力するには、この項目を選択します。
Netshare logs	この項目を選択すると、netshare 制御ログがログホストに高速で出力されます。
Security policy configuration logs	セキュリティーポリシーの構成ログをログホストにすばやく出力できるようにするには、この項目を選択します。
Heartbeat logs	ログホストへのハートビートログの高速出力を有効にするには、この項目を選択します。

IPS logs	ログホストへの IPS ログの高速出力をイネーブルにするには、この項目を選択します。
Bandwidth management logs	この項目を選択すると、帯域幅管理ログがログホストに高速で出力されます。
Sandbox logs	この項目を選択すると、サンドボックスログがログホストに高速で出力されます。
WAF logs	ログホストに WAF のログを高速で出力する場合に選択します。
LB logs	ロードバランシングログをログホストに高速で出力できるようにするには、この項目を選択します。LB ログには、インバウンドリンク LB ログと Server Load Balancing(SLB;サーバーロードバランシング)ログが含まれます。
Terminal identification logging	この項目を選択すると、端末識別ログをログホストに高速で出力できます。
Anti-virus logs	この項目を選択すると、アンチウィルスログがログホストに高速で出力されます。
External authentication logs	外部認証ログをログホストに高速出力できるようにするには、この項目を選択します。
Notification logs	ポリシー通知ログのログホストへの高速出力を有効にするには、この項目を選択します。

7. **OK** をクリックします。

Fast Log Output タブのログホストリストに、新しいログホストが表示されます。

Configure storage space settings

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Log Setting** > **Basic Settings** を選択します。
3. **Storage Space Settings** タブをクリックし、必要に応じてサービス設定を構成します。

Configure security management and audit

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Log Settings** > **Basic Settings** を選択します。
3. **Security Management&Audit** タブをクリックします。

表 11 セキュリティー管理と監査の構成項目

項目	説明
Security management	この機能をイネーブルにすると、デバイスはセキュリティー管理サービスプロセスを開きます。
Send security audit logs	この機能をイネーブルにすると、デバイスはセキュリティー監査関連のログメッセージを記録し、そのログメッセージをセキュリティー監査サーバーに報告します。
Security audit server IP	セキュリティー監査サーバーの IPv4 アドレスを指定します。
Security audit server port	セキュリティー監査サーバーがセキュリティー監査ログメッセージを受信するポート番号を指定します。

4. **Apply** をクリックします。
5. デバイスのセキュリティー管理サービス設定ファイルをローカルデバイスにエクスポートするには、**Export** をクリックします。

Email server

- Introduction
- Configure the email server

Introduction

ログを電子メールで出力する場合は、電子メールサーバーを構成する必要があります。その後、ログを電子メールの受信者に送信できます。

Configure the email server

1. **System** タブをクリックします。
2. ナビゲーションペインで **Log Settings** > **Email Server** を選択します。
3. **Create** をクリックします。
4. 電子メールサーバーの設定を行います。

表 1 メールサーバーの構成項目

項目	説明
Email server name	電子メールサーバーの名前を入力します。
Email server address	電子メールサーバーの IP アドレスまたはホスト名を入力します。
Sender address	電子メールの送信者アドレスを入力します。
Recipient addresses	電子メール受信者のアドレスをコロンで区切って入力します。
Identity authentication	電子メールクライアント認証を有効にするには、**Enable** を選択します。電子メールサーバーで ID 認証が必要な場合は、この機能を有効にします。
Secure user info transmission	ユーザー認証資格情報の安全な転送を有効にするには、この項目を選択します。
Username	電子メールサーバーにログインするためのユーザー名を入力します。

Password	電子メールサーバーにログインするためのパスワードを入力します。
Email sending interval	電子メールの送信間隔を入力します。デバイスは送信する電子メールをキャッシュし、間隔が終了したときにのみ送信します。
Max. emails per interval	間隔ごとに送信される電子メールの最大数を指定します。 送信間隔内に最大数に達し、送信する電子メールがさらに生成された場合、デバイスは新しい電子メールと既存の電子メールの重大度レベルを比較します。新しい電子メールの重大度レベルが既存のキャッシュされた電子メールの重大度レベルよりも高い場合、新しい電子メールは最新の電子メールを最も低い重大度レベルで上書きします。 電子メールの重大度レベルは、ログの一致する IPS シグニチャの重大度レベルです。 複数のサービスモジュールが同時に動作している場合、この設定は各サービスモジュールで個別に有効になります。

5. **OK** をクリックします。

Session log settings

Introduction

セッションログは、セキュリティー監査用のユーザーセス、IP アドレス変換およびネットワークトラフィックに関する情報を提供します。これらは、フローログまたは高速ログ出力フォーマットで出力できます。
デバイスは、時間ベースまたはトラフィックベースのロギングをサポートしています。

- **Time-based logging**: デバイスはセッションログを定期的に出力します。
- **Traffic-based logging**: セッションのトラフィック量がしきい値に達すると、デバイスはセッションログを出力します。

時間ベースとトラフィックベースの両方のロギングを設定した場合、デバイスはいずれかに達した時点でセッションログを出力します。セッションログを出力した後、デバイスはトラフィックカウンタをリセットし、セッションの間隔を再開します。
セッションログは、セッションロギングがインターフェースでイネーブルになっている場合にだけ生成できます。

Configure session log settings

手順

1. **system** タブをクリックします。
2. **Log Settings > Session Log Settings** を選択します。
3. セッションロギングを設定します。

表 1 セッションロギングの構成項目

項目	説明
Log type	ログタイプを選択します。デフォルトでは、フローログが使用されます。
Session creation logging	この機能により、デバイスはセッションエントリが作成されたときにセッションログを出力できます。
Session deletion logging	この機能により、セッションエントリが削除されたときに、デバイスはセッションログを出力できます。
Traffic-based logging	バイトベースのしきい値またはパケットベースのしきい値を設定します。セッションのトラフィック量が設定した閾値に達すると、セッションログを出力します。

Time-based logging	デバイスがセッションログを出力する時間ベースのしきい値を設定します。

4. **Apply** をクリックします。
5. **Add interface** をクリックして、指定したインターフェースでセッションロギングをイネーブルにします。

表 2 インターフェース上でセッションロギングをイネーブルにするための設定項目

項目	説明
IP version	IP バージョン(IPv4 または IPv6)を選択します。
Port	ポートを選択します。 ポートの指定された方向でセッションロギングをイネーブルにすることもできます。
ACL	インターフェース上でセッションロギングをトリガーできる IPv4 または IPv6 セッションをフィルタリングする ACL を選択します。 ACL が指定されていない場合、デバイスはインターフェース上のすべての IPv4 または IPv6 セッションのセッションログを出力します。

6. **OK** をクリックします。
7. **Session Logging** ページで設定を確認します。

NAT log settings

Introduction

NAT session log settings

NAT セッションロギングは、変換情報およびアクセス情報を含む NAT セッション情報を記録します。NAT セッションログは、フローログまたは高速ログに出力できます。デフォルトでは、NAT セッションログはフローログに出力されます。

デバイスは、次のイベントの NAT セッションログを生成します。

- NAT セッションの確立。
- NAT セッションの削除。このイベントは、プライオリティの高い設定の追加、設定の削除、ACL の変更を行った場合、NAT セッションが期限切れになった場合、または NAT セッションを手動で削除した場合に発生します。
- アクティブな NAT セッションロギング。

NAT444 log settings

NAT444 ログはユーザートレースに使用されます。NAT444 ゲートウェイは、ポートブロックを割り当てまたは取り消すたびにユーザーログを生成します。ログには、プライベート IP アドレス、パブリック IP アドレスおよびポートブロックが含まれます。パブリック IP アドレスおよびポート番号を使用して、ユーザーログからユーザーのプライベート IP アドレスを検索できます。NAT444 ログは高速ログでのみ出力できます。

NAT444 ゲートウェイは、次のいずれかのイベントが発生すると、NAT444 ログを生成します。

- ポートブロックが割り当てられます。

  NAT444 スタティックポートブロックマッピングの場合、NAT444 ゲートウェイは、プライベート IP アドレスからの最初の接続を変換するときにユーザーログを生成します。

  NAT444 ダイナミックポートブロックマッピングでは、NAT444 ゲートウェイがプライベート IP アドレスのポートブロックを割り当てたり拡張したりすると、ユーザーログが生成されます。
- ポートブロックが引き出されます。

  NAT444 スタティックポートブロックマッピングの場合、プライベート IP アドレスからのすべての接続が切断されると、NAT444 ゲートウェイはユーザーログを生成します。

  NAT444 ダイナミックポートブロックマッピングでは、次のすべての条件が満たされると、NAT444 ゲートウェイによってユーザーログが生成されます。
  - プライベート IP アドレスからのすべての接続が切断されます。
  - プライベート IP アドレスに割り当てられたポートブロック(拡張ブロックを含む)は取り消されます。
  - 対応するマッピングエントリーが削除されます。

NAT resources exhausting log settings

NAT リソース枯渇ロギングをイネーブルにすると、デバイスは NAT リソースが枯渇したときにログを出力します。NO-PAT では、NAT リソースはパブリック IP アドレスを参照します。EIM PAT では、NAT リソースはパブリック IP アドレスおよびポートを参照します。NAT444 では、NAT リソースはパブリック IP アドレス、ポートブロック、またはポートブロック内のポートを参照します。デバイスが NAT444 リソース枯渇イベントに関するログを生成できるようにするには、この機能と併せて高速ログ出力をイネーブルにします。

AFT log settings

Introduction

AFT session log settings

セキュリティー監査では、AFT セッション情報を記録するように AFT ロギングを構成できます。AFT セッションとは、発信元アドレスと宛先アドレスが AFT によって変換されたセッションのことです。
AFT セッションログは、フローログにのみ出力できます。AFT は、AFT セッションの作成および削除イベントをログに記録できます。

Port block log settings

PAT モードでダイナミック変換ポリシーにポートブロックサイズが指定されている場合、AFT セッションが作成または削除されると、AFT はポートブロックログを生成します。
ポートブロックログは、システムログまたはファストログに出力できます。デフォルトでは、ポートブロックログはシステムログに出力されます。

Sandbox log settings

Introduction

サンドボックスログには、サンドボックス検査の結果が記録されます。サンドボックスログは高速ログ出力のみをサポートします。

Threat log settings

このヘルプには、次のトピックが含まれています。

- Introduction
  - IPS log settings
  - Anti-virus log settings
- Restrictions and guidelines

Introduction

脅威ログは、検出されたネットワーク攻撃の挙動を記録するものであり、IPS ログとウィルス対策ログに分類することができる。

IPS log settings

IPS ログは、システムログとしてインフォメーションセンターに出力したり、高速ログとして指定されたログホストに出力したり、指定された電子メール受信者に電子メール経由で出力したりできます。
IPS ログは、次のいずれかの形式で高速ログとして出力できます。

- Standard。
- SGCC。

  SGCC 形式で出力できるのは、IPS アラームログとシグニチャ更新ログだけです。SGCC 形式のシグニチャ更新ログの 1 日のログ出力時刻を設定できます。
  SGCC フォーマットのサポートは、デバイスモデルによって異なります。

Anti-virus log settings

アンチウィルスログは、システムログとして情報センターに出力したり、指定されたログホストに高速ログとして出力したり、指定された電子メール受信者に電子メール経由で出力することができます。

Restrictions and guidelines

IPS ログは中国語で出力できます。IPS ログの出力に中国語を選択すると、IPS ログメッセージの攻撃名、攻撃カテゴリ、攻撃サブカテゴリのフィールドが中国語で表示されます。

Application audit log settings

Introduction

アプリケーション監査ログには、ユーザーのインターネットアクセス動作が記録されます。アプリケーション監査ログは、システムログまたは高速ログとして出力できます。デフォルトでは、アプリケーション監査ログは高速ログとして出力されます。

NetShare log settings

このヘルプには、次のトピックがあります。

- Introduction

Introduction

NetShare ログには、ネットワーク共有の動作が記録されます。NetShare ログ出力では、システムログ出力と高速ログ出力がサポートされています。デフォルトでは、NetShare ログはシステムログとして出力されます。

URL filtering log settings

このヘルプには、次のトピックが含まれています。

- Introduction

Introduction

URL フィルタリングログには、ユーザーの Web サイトアクセス動作が記録されます。
URL フィルタリングログは、システムログまたはファストログとして出力できます。デフォルトでは、URL フィルタリングログはシステムログとして出力されます。
高速ログ出力オプションを選択すると、non-standard format オプションが表示されます。このオプションでは、高速ログ出力用のキャリアカスタマイズ形式(Unicom)を指定できます。初期設定では、高速ログは標準形式で出力されます。

Attack defense log settings

Introduction

攻撃防御ログは、システムログまたはファストログに出力できます。デフォルトでは、攻撃防御ログはシステムログに出力されます。

Log aggregation for single-packet attack events

単一パケット攻撃のロギングを有効にすると、単一パケット攻撃を検出したときにログが生成されます。単一パケット攻撃が頻繁に発生する場合は、ログの生成と出力により多くのシステムリソースが必要になります。**Log aggregation for single-packet attacks** を有効にすると、システムリソースを節約できます。この機能により、一定期間に生成された複数のログが集約され、1 つのログが送信されます。集約されるログには、共通する次の属性が必要です。

- 攻撃は同じインターフェースまたはセキュリティーゾーンで検出されるか、デバイス宛てに送信されます。
- **Attack type**。
- **Attack defense action**。
- **Source and destination IP addresses**。
- **VRF to which the victim IP address belongs**。

Blacklist logging

ブラックリスト機能のロギングがイネーブルになっている場合、次の状況でログが出力されます。

- ブラックリストエントリは手動で追加されます。
- ブラックリストエントリは、スキャン攻撃検出機能によって動的に追加されます。
- ブラックリストエントリは手動で削除されます。
- ブラックリストエントリは期限切れになります。

ブラックリストログには、次の情報が記録されます。

- ブラックリストエントリの送信元 IP アドレス。
- DS-Lite トンネルのリモート IP アドレス。
- VRF 名。
- ブラックリストエントリを追加または削除する理由。
- ブラックリストエントリのエージングタイム。

Log buffer and log file

デバイスには、ブラックリストモジュールと攻撃防御モジュール用に別々のログバッファとログファイルが用意されています。サービスモジュールのログをログバッファおよびログファイルに出力できるようにするには、syslog の基本設定ページで **Output to log buffer** オプションを選択します。
ログは、ログファイルに保存される前にログファイルバッファに保存されます。システムがログをログファイルに保存すると、ログファイルバッファがクリアされます。
ログファイルの最大容量に達すると、システムは最も古いログを新しいログに置き換えます。

Reputation log settings

Introduction

デバイスは、特定の基準に一致するパケットの IP レピュテーションログ、URL レピュテーションログ、およびドメインレピュテーションログの生成と、これらのログの指定されたログホストへの高速出力をサポートします。

Bandwidth alarm logs

Introduction

この機能は、デバイス上の合計着信トラフィックを監視します。デバイスは、合計着信トラフィックレートを5秒ごとに調べ、5秒間の平均トラフィックレートを使用してしきい値と比較します。ログメッセージは、デバイス上の合計着信トラフィックレートが指定された期間にしきい値に達したか、しきい値を超えた場合に生成されます。その後、ログメッセージは、5 秒間の平均トラフィックレートがしきい値に達したか、しきい値を超えた場合に生成されます。ログメッセージは、平均トラフィックレートが初めてしきい値を下回った場合にも生成されます。帯域幅アラームログは、システムログとしてのみ出力できます。

Configuration log settings

Introduction

この機能は、管理者がデバイスで実行する操作をログに記録します。
デバイスは、専用の構成ログ バッファと別のログ ファイルを作成して、構成ログ メッセージを保存できます。 デバイスでこれを行うには、**System** タブをクリックし、**Log Settings > Basic Settings** を選択してから、**Syslog** ページで **Output to log buffer** オプションを選択します。
デバイスは、メッセージをログ ファイルに一括で書き込む前に、設定ログ メッセージをログ ファイル バッファに保存します。 ログ ファイル バッファ内のログ メッセージをログ ファイルに書き込んだ後、デバイスはログ ファイル バッファをクリアします。
ログ ファイルのサイズには制限があります。 制限に達すると、デバイスは最も古いログ メッセージを新しいログ メッセージに置き換えます。

Security policy log

Introduction

この機能により、有効なセキュリティーポリシーの設定を、SGCC 形式のログとして、毎日指定した時刻に高速で出力できます。

Terminal identification logging

Introduction

端末情報(カメラベンダなど)が変更された場合、端末識別ログを生成します。
端末識別ログは、ログホストへの高速なログ出力をサポートします。

Heartbeat log settings

Introduction

ハートビートロギングがイネーブルになると、デバイスはハートビートログメッセージをログサーバーに定期的に送信します。ログサーバーが特定の時間内にハートビートログメッセージを受信できない場合、デバイスがダウンしていると判断されます。

Session settings

このヘルプには、次のトピックがあります。

- Introduction
  - Session management operation
  - Session management functions
  - Session types
- Restrictions and guidelines

Introduction

セッション管理は共通モジュールであり、サービスモジュールがセッションベースのサービスを実装するための基本的なサービスを提供します。
セッション管理は、トランスポート層でのパケット交換をセッションとして定義します。セッション状態を更新し、イニシエータまたはレスポンダからのデータフローに従ってセッションを期限切れにします。セッション管理では、複数の機能が同じサービスパケットを処理できます。

Session management operation

セッション管理は、トランスポート層プロトコル情報を検査することによってセッションステータスを追跡します。セッション管理は、セッションテーブル基づいて、すべての接続の統合されたステータスメンテナンスおよび管理を実行します。
クライアントからサーバーへの接続要求がデバイスを通過すると、デバイスはセッションエントリを作成します。このエントリには、次のような要求および応答情報を含めることができます:

- 送信元 IP アドレスおよびポート番号。
- 宛先 IP アドレスおよびポート番号。
- トランスポート層プロトコル。
- アプリケーション層プロトコル。
- セッションのプロトコルステート。

マルチチャネルプロトコルでは、アプリケーションを実装するために、クライアントとサーバーが既存の接続に基づいて新しい接続をネゴシエートする必要があります。セッション管理を使用すると、デバイスはネゴシエーションフェーズ中に接続ごとに関係エントリを作成できます。このエントリは、接続をアプリケーションに関連付けるために使用されます。関係エントリは、関連付けられた接続が確立された後に削除されます。
パケットの宛先 IP アドレスがマルチキャスト IP アドレスである場合、パケットは複数のポートから転送さ

れます。マルチキャスト接続要求が着信インターフェースで受信されると、デバイスは次の操作を実行します。

- インバウンドインターフェース上にマルチキャストセッションエントリを作成します。
- 各発信インターフェースに対応するマルチキャストセッションエントリを作成します。

特に明記しない限り、このドキュメントの「セッションエントリ」は、ユニキャストとマルチキャストの両方のセッションエントリを指します。

実際のアプリケーションでは、セッション管理は他のサービスモジュールと連携する必要があります。接続ステータスのみを追跡します。潜在的な攻撃パケットはブロックしません。

Session management function

セッション管理を使用すると、デバイスは次の機能を提供できます。

- プロトコルパケットのセッションを作成し、セッション状態を更新し、異なるプロトコル状態のセッションのエージングタイムを設定します。
- アプリケーション層プロトコルのポートマッピングをサポートし(APR オンラインヘルプを参照)、アプリケーション層プロトコルがカスタマイズされたポートを使用できるようにします。
- アプリケーション層プロトコルに基づいて、セッションのエージングタイムを設定します。
- ICMP/ICMPv6 エラーパケットマッピングをサポートし、デバイスが ICMP/ICMPv6 エラーパケット内のペイロードに従って元のセッションを検索できるようにします。
- アプリケーション層プロトコル(FTP など)の制御チャネルおよび動的データチャネルのセッション管理をサポートします。

Session types

データフローの最初のパケットを受信すると、デバイスはパケットを処理し、処理結果に基づいてセッションエントリを作成します。データフローの後続のパケットについては、デバイスはセッションエントリに基づいて高速転送を実行します。

セッションは、セッションエントリと一致するパケットに対して実行されるアクションに従って、次のタイプに分類されます。

- **Permit session**: デバイスは、許可セッションのすべてのパケットを許可します。デバイスは、データフローの最初のパケットを許可した場合、データフローの許可セッションエントリを生成します。

  許可セッションで追跡できるのは接続ステータスのみです。潜在的な攻撃パケットを拒否することはできません。特定のパケットを拒否するには、許可セッションとセキュリティー機能を併用する必要があります。

- **Deny session**: デバイスは拒否セッションのすべてのパケットをドロップします。データフローの最初のパケットをドロップすると、デバイスはデータフローの拒否セッションエントリを生成します。

  デバイスでドロップされたパケットの拒否セッションを生成するには、拒否セッション機能をイネーブルにする必要があります。

特に明記されていない限り、このドキュメントのセッションは許可セッションを指します。

Restrictions and guidelines

- 異なるアプリケーションのセッションのエージングタイムは、ESTABLISHED 状態の安定したセッション TCP セッションまたは READY 状態の UDP セッションに有効です。
- 安定した状態のセッションの場合、関連するエージングタイムの優先順位は次のとおりです。
  - アプリケーション層プロトコルのセッションのエージングタイム。
  - 異なるプロトコル状態のセッションのエージングタイム。
- デバイスは、ASPF または接続制限モジュールによってドロップされたパケットに対してだけ拒否セッションを生成します。
- 拒否セッション機能は、ソフトウェアベースの高速パケットドロップだけをサポートします。ハードウェアベースの高速パケットドロップはサポートしません。
- セッションのホットバックアップでは、拒否セッションはサポートされていません。

Report settings

このヘルプには、次のトピックが含まれています。

- Introduction
  - Report export
  - Report subscription
  - Email server
- Configure report settings
  - Export reports
  - Configure report subscription
  - Configure the email server

Introduction

Report export

スケジュール済エクスポートと手動エクスポートの両方がサポートされています。定期的にレポートをエクスポートするか、必要に応じて 1 つのレポートのみをエクスポートできます。

- **Scheduled export**: デバイスは、指定されたエクスポートスケジュールに従って、ユーザーが指定したアドレスにレポートをエクスポートします。レポートの統計オブジェクトは、レポートテンプレートを使用して構成できます。
- **Manual export**: デバイスは、設定された測定オブジェクトと時間範囲に従って、レポートをただちにエクスポートします。

Report subscription

レポートのサブスクライバを追加すると、レポートは電子メールでサブスクライバに送信されます。
ユーザーがレポートを受信するには、電子メールサーバーを設定する必要があります。
デバイスは、最も負荷の少ない時間帯(午前 1 時～午前 5 時)に日報を送信します。前月の月報は毎月 1 日に送信されます。
レポートサブスクリプション機能では、次のタイプのレポートがサポートされています。

- **Summary report** : ある時間範囲で収集されたサービス統計情報の要約を表示します。
- **Comparison report**: 同じ日数を含む 2 つの時間範囲で収集されたサービス統計情報を比較します。
- **Intelligent report**: ネットワークアクセス動作に基づいて、ユーザーの作業効率、データ漏洩、およびターンオーバーリスクをインテリジェントに分析します。

- **Comprehensive report**: 重要なサービス統計情報の分析に基づいて、デバイスの全体的な動作ステータスとネットワークセキュリティーステータスを示します。

Email server

指定された電子メールアドレスにレポートを送信するようにデバイスを設定するか、レポートサブスクリプション機能をイネーブルにするには、電子メールサーバーを設定する必要があります。

Configure report settings

Export reports

Export reports periodically

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Report Settings > Report Export** 選択します。
3. **Report Templates** タブをクリックします。
4. **Create** をクリックします。

表 1 レポートテンプレートの設定項目

項目	説明
Template name	レポートテンプレート名を入力します。
Language	レポート言語を選択します。 オプションは **Chinese** と **English** です。
Statistical object	レポートでカウントされるオブジェクトを選択します。 次のオプションを使用できます。 • **Link**. • **Routing policy**. • **Virtual server**. • **Real server**. • **Server farm**. • **Server farm member**.

Link statistics Link Link measured items	リンクを選択し、リンクの測定項目を選択します。 オプションは次のとおりです。 • **Application**. • **Packet loss rate**. • **Network delay**. • **Connections**. • **Concurrent connections**. • **Abnormal traffic**. • **Status**.
Routing policy statistics Routing policy	ルーティングポリシーを選択します。 ルーティングポリシーを選択すると、ルーティングポリシー内の異なるクラスと一致した数がカウントされます。
Virtual server statistics Virtual server Statistics items	仮想サーバーを選択し、仮想サーバーのレポートでカウントする項目を選択します。 次のアイテムを使用できます。 • **Status**. • **HTTP status code**. • **Traffic compression ratio**.
Real server statistics Real server Statistics items	実サーバーを選択し、実サーバーのレポートでカウントする項目を選択します。 サポートされている項目は、**Status** と **HTTP delay** です。
Server farm statistics Server farm	サーバーファームを選択します。 サーバーファームを選択すると、そのサーバーファームのステータス統計情報がカウントされます。
Server farm member statistics Server farm Server farm member Statistics items	サーバーファームからメンバーを選択し、サーバーファームメンバーのレポートでカウントする項目を選択します。 サポートされている項目は、**Status** と **HTTP delay** です。

5. **OK** をクリックします。

レポートテンプレートが **Report Templates** ページに表示されます。

6. **Auto Export** タブをクリックします。
7. **Create** をクリックします。

表 2 レポートエクスポートタスクの設定項目

項目	説明
Export destination	レポートのエクスポート先を選択します。 オプションは **Local** と **Email** です。
Export schedule	レポートのエクスポートスケジュールを選択します。 オプションは、**Hourly**、**Daily**、**Weekly**、**Monthly**、**Quarterly**、および **Yearly** です。
Report template	定期レポートタイプに使用するレポートテンプレートを選択します。

Export report manually

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Report Settings** > **Report Export** を選択します。
3. **Manual Export** タブをクリックします。

表 3 構成アイテムの手動エクスポート

項目	説明
Statistical object	レポートでカウントされるオブジェクトを選択します。 次のオプションを使用できます。 • **Link**. • **Routing policy**. • **Virtual server**. • **Real server**. • **Server farm**. • **Server farm member**.

Link statistics Link Link measured items	リンクを選択し、リンクの測定項目を選択します。 オプションは次のとおりです。 • **Application**. • **Packet loss rate**. • **Network delay**. • **Connections**. • **Concurrent connections**. • **Abnormal traffic**. • **Status**.
Routing policy statistics Routing policy	ルーティングポリシーを選択します。 ルーティングポリシーを選択すると、ルーティングポリシー内の異なるクラスと一致した数がカウントされます。
Virtual server statistics Virtual server Statistics items	仮想サーバーを選択し、仮想サーバーのレポートでカウントする項目を選択します。 次のアイテムを使用できます。 • **Status**. • **HTTP status code**. • **Traffic compression ratio**.
Real server statistics Real server Statistics items	実サーバーを選択し、実サーバーのレポートでカウントする項目を選択します。 サポートされている項目は、**Status** と **HTTP delay** です。
Server farm statistics Server farm	サーバーファームを選択します。 サーバーファームを選択すると、そのサーバーファームのステータス統計情報がカウントされます。
Server farm member statistics Server farm Server farm member Statistics items	サーバーファームからメンバーを選択し、サーバーファームメンバーのレポートでカウントする項目を選択します。 サポートされている項目は、**Status** と **HTTP delay** です。
Time range	レポートの時間範囲を指定します。

4. **Export now** をクリックします。

デバイスは、設定されたパラメーターに従ってレポートをエクスポートします。

Configure report subscription

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Report Settings** > **Report Subscription** を選択します。
3. **Add** をクリックしてレポートを表示します。
4. レポートユーザーの電子メールアドレスを入力し、レポートの言語を選択します.

Configure the email server

1. **System** タブをクリックします。
2. ナビゲーションペインで、**Report Settings** > **Email Server** を選択します。
3. 電子メールサーバーを設定します。

表 4 メールサーバーの設定項目

項目	説明
Email server address	電子メールサーバーの IP アドレスまたはホスト名を入力します。
Sender address	電子メールの送信者アドレスを入力します。
Identity authentication	電子メールクライアント認証を有効にするには、**Enable** を選択します。電子メールサーバーの要求に応じて電子メールクライアント認証を有効にします。
Secure user credential transmission	ユーザー認証資格証明のセキュアな転送を有効にするには **Enable** を選択します。
Username	電子メールサーバーに接続するためのユーザー名を入力します。
Password	電子メールサーバーに接続するためのパスワードを入力します。

4. **Apply** をクリックします。

Signature upgrade

このヘルプには、次のトピックがあります。

Introduction

DPI 署名ライブラリは、DPI がサービスの識別に使用する共通の署名のコレクションです。同社の公式 Web サイトでは、最新の署名が DPI 署名ライブラリファイルの形式で公開されています。ファイルを手動でダウンロードしたり、ファイルを自動的にダウンロードして DPI 署名ライブラリを更新するようにデバイスを構成したりできます。また、DPI サービスモジュールの署名ライブラリをロールバックすることもできます。DPI シグニチャライブラリには、IPS シグニチャライブラリ、URL フィルタリングシグニチャライブラリ、Web アプリケーション保護、APR シグニチャライブラリ、ウィルスシグニチャライブラリ、IP レピュテーションシグニチャライブラリ、URL レピュテーションシグニチャライブラリ、およびドメインレピュテーションシグニチャライブラリが含まれます。

Signature library upgrade

DPI サービスモジュールのシグニチャライブラリを更新するには、次の方法があります。

Automatic update。

デバイスは、最新のシグニチャファイルを自動的にダウンロードして、ローカルシグニチャライブラリを定期的に更新します。

Online update。

操作をトリガーするとすぐに、デバイスは最新のシグニチャファイルをダウンロードして、ローカルシグニチャライブラリを更新します。

Manual update。

この方法は、デバイスがシグニチャファイルを自動的に取得できない場合に使用します。
最新のシグニチャファイルを手動でダウンロードし、そのファイルを使用してデバイス上のシグニチャライブラリを更新する必要があります。

Signature library roll back

DPI サービスモジュールで誤ったアラームのフィルタリングまたは例外のフィルタリングが頻繁に発生する場合は、シグニチャライブラリを以前のバージョンまたは工場出荷時のデフォルトバージョンにロールバックできます。

Restrictions and guidelines

シグニチャライブラリのアップグレードおよびロールバックは、DPI サービスの一時的な停止を引き起こす可能性があります。DPI サービスに基づくサービスも中断される可能性があります。たとえば、セキュリティーポリシーはアプリケーションへのアクセスを制御できません。

APR、IPS、ウィルス対策、Web アプリケーション保護、URL フィルタ、IP レピュテーション、ドメインレピュテーション、および URL レピュテーションなどの DPI サービスモジュールの署名ライブラリをアップグレードするには、正しいライセンスが必要です。DPI サービスモジュールのライセンスの有効期限が切れた場合でも、既存の署名ライブラリは使用できますが、署名ライブラリをアップグレードすることはできません。ライセンスの詳細については、ライセンスのオンラインヘルプを参照してください。

デバイスの空きメモリーが正常な状態のしきい値を下回っている場合は、シグニチャライブラリの更新またはロールバックを実行しないでください。このような状況で実行されるシグニチャライブラリの更新またはロールバック操作は失敗する可能性が高く、DPI サービスに影響します。

一度に更新できるシグニチャライブラリは 1 つだけです。

デフォルトコンテキストのみがシグネチャライブラリの更新をサポートします。ユーザーコンテキストは、シグネチャライブラリのバージョンの表示のみをサポートします。

IP レピュテーション、URL レピュテーション、およびドメインレピュテーションは時間依存型であり、ファクトリバージョンは現在サポートされていません。これらの関数を使用する前に、ベストプラクティスとして対応するシグニチャライブラリをアップグレードしてください。

ライブラリの最新のシグニチャファイルを入手するには、h3c 公式 Web サイト (https://www.h3c.com/ja/support/resource_center/ja/security/catalog/database/database/?tbox=Software)の **Signature Database Services** ページにアクセスします。

Configure signature library upgrade and rollback

DPI サービスモジュールのシグニチャライブラリを最新バージョンにアップグレードしたり、シグニチャライブラリを以前のバージョンまたは工場出荷時のデフォルトバージョンにロールバックしたりできます。

また、プロキシサーバーを設定して、デバイスから会社の公式 Web サイトにアクセスし、オンラインシグ

ニチャライブラリを自動的または即時に更新することもできます。

Configure automatic signature library update

DPI サービスモジュールの自動シグニチャライブラリアップデートを設定するには、次の作業を実行します。
署名ライブラリの自動更新が正しく機能するように、デバイスが会社の公式 Web サイトにアクセスして最新の署名ファイルを取得できることを確認します。

手順

System タブをクリックします。
ナビゲーションペインで、**Upgrade Center** > **Signature Upgrade** を選択します。
シグニチャライブラリの **Auto update** カラムのボックスをクリックします。
この例では、IPS シグニチャライブラリの **Auto update** カラムのボックスをクリックします。
Configure Scheduled Update For IPS Signature Library ウィンドウが開きます。
スケジュールされた更新時刻を設定します。
自動シグニチャライブラリの更新は、実際には次の時点の間のランダムな時間に開始されます。
スケジュールされた更新時刻の 1 時間前。
スケジュールされた更新時刻の 1 時間後。
OK をクリックします。

Trigger immediate online update

会社の公式 Web サイトで新しいシグニチャライブラリバージョンのリリースを見つけたときはいつでも、デバイスをトリガーしてローカルシグニチャライブラリをすぐに更新できます。

手順

System タブをクリックします。
ナビゲーションペインで、**Upgrade Center** > **Signature Upgrade** を選択します。
シグニチャライブラリの **Actions** カラムで **Online update** をクリックします。
表示された確認ダイアログボックスで **OK** をクリックします。

Perform a manual signature library update

ローカルに保存されたシグニチャファイルを使用して DPI サービスモジュールのシグニチャライブラリを手動で更新するには、次の作業を実行します。

デバイスが会社の公式 Web サイト上のシグニチャデータベースサービスにアクセスできない場合は、この方法を使用します。
シグニチャライブラリを正常にアップデートするために、アップデートファイルをマスターデバイスに保存します。

手順

System タブをクリックします。
ナビゲーションペインで、**Upgrade Center** > **Signature Upgrade** を選択します。
シグニチャライブラリの **Actions** カラムで **Manual update** をクリックします。この例では、IPS シグニチャライブラリの **Manual update** をクリックします。
Update IPS Signature Library ウィンドウが開きます。
Select をクリックして、ローカル更新ファイルを選択します。
OK をクリックします。

Configure a proxy server

デバイスは、オンラインまたは自動でシグニチャライブラリを更新するために、会社の公式 Web サイトにアクセスする必要があります。直接接続が使用できない場合、デバイスは指定されたプロキシサーバーを介して会社の公式 Web サイトにアクセスできます。

手順

System タブをクリックします。
ナビゲーションペインで、**Upgrade Center** > **Signature Upgrade** を選択します。
Configure proxy server をクリックします。
Configure proxy server ウィンドウが開きます。
サーバードレス、ポート番号、ログインユーザー名、ログインパスワードなど、プロキシサーバーの設定を行います。
OK をクリックします。

Roll back a signature library

シグニチャライブラリの更新によって例外が発生したり、誤アラーム率が高くなったりする場合は、シグニチャライブラリをロールバックできます。
シグニチャライブラリをロールバックする前に、デバイスは現在のシグニチャライブラリを以前のバージョンとしてバックアップします。たとえば、以前のライブラリバージョンは V1 で、現在のライブラリバージョンは V2 です。以前のバージョンへのロールバックを実行すると、ライブラリバージョン V1 が現在のバージ

ョンになり、ライブラリバージョン V2 が以前のバージョンになります。以前のバージョンへのロールバックを再度実行すると、ライブラリはライブラリバージョン V2 にロールバックされます。

手順

System タブをクリックします。
ナビゲーションペインで、**Upgrade Center** > **Signature Upgrade** を選択します。
シグニチャライブラリの **Actions** 列で **Roll back** をクリックします。この例では、IPS シグニチャライブラリの **Roll back** をクリックします。
Roll Back IPS Signature Library ウィンドウが開きます。
Roll back to previous version または **Roll back to factory default** を選択します。
OK をクリックします。

Test the signature library server connectivity

即時オンライン更新のトリガー、自動シグニチャライブラリ更新の設定、またはプロキシサーバーを使用したシグニチャライブラリの更新を行う前に、**Test signature library server connectivity** をクリックします。デバイスがシグニチャライブラリサーバーに接続できない場合は、ページのプロンプトに従って問題を解決します。

Software upgrade

このヘルプには、次のトピックがあります。

Introduction

デバイスは、ブート ROM イメージとネットワーク OS イメージを実行して、機能とサービスを提供します。インターフェースモジュールおよびスイッチングファブリックモジュールのイメージは、MPU のイメージパッケージに統合されています。MPU をアップグレードすると、インターフェースモジュールおよびスイッチングファブリックモジュールは自動的にアップグレードされます。

サービスモジュールには個別のイメージファイルがあります。イメージファイルは、MPU 用のイメージファイルとともにリリースされます。サービスモジュールは手動でアップグレードする必要があります。

Boot ROM image

起動時に、デバイスは最初にブート ROM イメージを実行してハードウェア初期化を実行し、システムをブートストラップします。

ブート ROM イメージは、デバイスのブート ROM に格納されます。基本セグメントと拡張セグメントが含まれています。

基本セグメントは、システムをブートストラップする最小限のコードです。

拡張セグメントはハードウェアの初期化を可能にし、システム管理メニューを提供します。デバイスが正常に起動できない場合は、メニューを使用してソフトウェアイメージおよび構成ファイルをロードしたり、ファイルを管理したりできます。

通常、ブート ROM イメージは、ソフトウェア互換性エラーを回避するためにブートイメージに統合されます。

Network OS images

Network OS image types

Boot image: Linux オペレーティングシステムのカーネルを含む.bin ファイル。プロセス管理、メモリー管理、ファイルシステム管理、および緊急シェルを提供します。

System image : ネットワーク OS カーネルと、デバイス管理、インターフェース管理、構成管理、ルーティングなどの標準機能を含む.bin ファイル。

Feature image: 高度なソフトウェア機能またはカスタマイズされたソフトウェア機能を含む.bin ファイル。

Patch image: デバイスを再起動せずにバグを修正するためにリリースされる.bin ファイル。パッチイメージは、機能を追加または削除しません。

デバイスが動作するには、ブート ROM イメージ、ブートイメージ、およびシステムイメージが必要です。必要に応じて、機能イメージを購入してインストールできます。

Software release forms

ソフトウェアイメージは、次のいずれかの形式でリリースされます。

bin ファイルを分離します。ソフトウェアイメージ間の互換性を確認する必要があります。

1 つの.ipe パッケージファイルに全体として.ipe パッケージファイル内のイメージは互換性があります.ipe パッケージファイルを使用してソフトウェアをアップグレードする場合、システムは自動的に.ipe ファイルを解凍し、.bin イメージをロードして、起動ソフトウェアイメージとして設定します。

Restrictions and guidelines

ソフトウェアアップグレード中にデバイスが再起動し、サービスが中断されます。ベストプラクティスとして、計画的なソフトウェアアップグレードを実行してください。

リリースノートを読んで、アップグレードイメージにライセンスが必要かどうかを確認します。ライセンスが必要な場合は、ライセンスベースのイメージごとにライセンスを登録してアクティベーションを行います。

機能イメージまたはパッチイメージをインストールする前に、イメージがデバイス上で実行されているイメージと互換性があることを確認します。

IRF ファブリックから機能イメージをアンインストールするには、グローバルスタンバイ MPU からイメージをアンインストールしてから、グローバルアクティブ MPU からイメージをアンインストールします。

デバイスが使用している機能またはパッチイメージファイルを削除した後は、ファイルをアンインストールできません。

IRF ファブリックでは、イメージファイルの管理中にスイッチオーバーを実行しないでください。

デバイスに MPU とサービスモジュールの両方がある場合、イメージファイルをインポートできるのは MPU だけです。

Manage image files

デバイス上のイメージファイルをインポート、削除、インストール、およびアンインストールしたり、起動イメージファイルを指定したりできます。指定した起動イメージファイルは、デバイスの再起動後に有効になります。

手順

System > **Upgrade Center** > **Software Upgrade** を選択します。
Manage file をクリックします。

表 1 イメージファイルの管理

項目	説明
Import	bin または.ipe イメージファイルをデバイスに転送します.ipe ファイルをデバイスに転送すると、デバイスは自動的に.ipe ファイルを解凍し、.bin ファイルを保存します。
Delete	未使用のイメージファイルを削除します。
Operation	次のタスクを実行できます。 起動イメージファイルを指定します。 機能またはパッチイメージファイルをインストールします。 機能またはパッチイメージファイルをアンインストールします。
Set as next startup files	次回の起動時にロードする起動イメージファイルを指定します。起動イメージファイルには、ブートイメージファイルと同じバージョンのシステムイメージファイルが含まれます。起動イメージファイルは、デバイスの再起動後に有効になります。
Install feature/patch files	システムの停止を引き起こすことなく、機能およびパッチイメージファイルをインストールまたはアップグレードします。デバイスは、複数の機能イメージファイルを同時にインストールできます。新しいパッチイメージファイルをインストールするには、最初に古いパッチイメージファイルをアンインストールする必要があります。
Uninstall feature/patch files	機能およびパッチイメージファイルをアンインストールします。アンインストールされたイメージファイルはアクティブではなく、サービスを提供しませんが、デバイスに保存されます。

Upgrade software immediately

Use an .ipe file to upgrade the software

System > **Upgrade Center** > **Software Upgrade** を選択します。

Upgrade immediately をクリックし、スタートアップファイルの種類として **ipe** を選択します。
Select をクリックしてアップグレード・ファイルを選択します。他のパラメーターにはデフォルト設定を使用します。
OK をクリックします。

Use .bin files to upgrade the software

System > **Upgrade Center** > **Software Upgrade** を選択します。
Upgrade immediately をクリックし、スタートアップファイルの種類として **bin** を選択します。
Select をクリックして、アップグレードブートファイルとシステムファイルを選択します。他のパラメーターにはデフォルト設定を使用します。
(オプション)**.bin** ファイルのサイズが空きストレージ容量を超える場合は、**Delete all startup files** オプションを選択します。
OK をクリックします。

License management

このヘルプには、次のトピックがあります。

Introduction

ライセンスベースの機能を使用するには、正式なライセンスを購入するか、試用版ライセンスを取得して、機能のライセンスをインストールする必要があります。

Available licenses

表 1 に、使用可能なライセンスを示します。ライセンスのサポートは、デバイスモデルによって異なります。

表 1 使用可能なライセンス

ライセンス	機能	ライセンスのインストール前	ライセンスの期限切れ後	有効期限
SLB	サーバーのロードバランシング	サーバーロードバランシングは使用できません。	該当なし	永続的
ACG	アプリケーション認識(APR)	APR 署名ライブラリの更新はサポートされていません。	APR 署名ライブラリの更新はサポートされていません。	1 年 3 年
AV	ウィルス対策	アンチウィルスは使用できません。また、ウィルスシグニチャライブラリの更新はサポートされていません。	アンチウィルスは引き続き使用できますが、ウィルスシグニチャライブラリを更新したり、クラウドクエリー、拡張検査、およ	1 年 3 年

ライセンス	機能	ライセンスのインストール前	ライセンスの期限切れ後	有効期限
			びサンドボックスコラボレーション機能を使用したりすることはできません。	
IPRPT	脅威インテリジェンス(IP レピュテーション、URL レピュテーション、およびドメインレピュテーションを含む)	脅威インテリジェンスは使用できず、脅威インテリジェンスシグニチャライブラリの更新はサポートされていません。	脅威インテリジェンスは引き続き使用できますが、脅威インテリジェンスシグニチャライブラリの更新はサポートされていません。	1 年 3 年
IPS	IPS	IPS は使用できません。また、IPS シグニチャライブラリの更新はサポートされていません。	IPS は引き続き使用できますが、IPS シグニチャライブラリの更新はサポートされていません。	1 年 3 年
SSL VPN	SSL VPN	システムは、SSL VPN ユーザーのデフォルトの最大数だけをサポートします。	該当なし	永続的
UFLT	URL フィルタリング	URL クラウドクエリーは使用できません。また、URL 署名ライブラリの更新はサポートされていません。	URL クラウドクエリーは使用できません。また、URL 署名ライブラリの更新はサポートされていません。	1 年 3 年
WAF	WAF の保護	WAF の保護機能は利用できません。また、WAF シグネチャライブラリの更新機能もサポートされていません。	WAF による保護は可能ですが、WAF シグネチャライブラリの更新はできません。	1 年 3 年

License validity period

次のタイプの有効期間を使用できます。

Permanent： 永続ライセンスは常に有効で、期限は切れません。

Date restricted: 絶対日付範囲(2015-05-01～2015-05-30 など)で有効なライセンス。

Trial and formal licenses

ライセンスには、試用ライセンスと正式ライセンスが含まれます。試用ライセンスには通常、期限があり、転送できません。試用ライセンスの期限が切れる前に、ライセンスベースの機能の正式ライセンスを購入してインストールし、機能を引き続き使用できるようにします。

Restrictions and guidelines

General restrictions and guidelines

作業中のデバイスで他のユーザーがライセンス管理タスクを実行していないことを確認します。
期限切れになった正式ライセンスはアンインストールできません。期限切れになったライセンスは、ライセンス保存領域を圧縮しない限り、ライセンス保存領域に残ります。ライセンス保存領域が使い果たされると、新しいライセンスのインストールが失敗します。
ライセンスを登録する前に、**Compress License Storage** ページで使用可能な数とインストールされている数を確認します。登録されているライセンスとインストールされているライセンスの数が、使用可能な数を超えていないことを確認してください。
ライセンス格納領域を圧縮すると、DID が変更され、期限切れのライセンスおよびアンインストールされたライセンス情報が削除されます。ライセンス格納領域を圧縮する前に、アンインストールキーをバックアップし、古い DID に基づいて生成されたすべてのアクティベーションファイルがインストールされていることを確認してください。これらのアクティベーションファイルは、圧縮後にはインストールできません。
ライセンスをインストールすると、システムは一致する機能パッケージのストレージメディアも検索します。一致するパッケージが見つかると、検索を停止してパッケージをインストールします。
ライセンスをアンインストールする場合、システムはライセンスの機能パッケージが実行されているかどうかを確認します。実行されている場合は、パッケージが自動的にアンインストールされます。
HTTP クライアントのオペレーティングシステムやブラウザのエラーなどの問題が原因でアクティベーションファイルを取得または再登録できない場合は、テクニカルサポートに連絡してください。

Restrictions and guidelines: File safety

紛失した場合に備えて、入手したアクティベーションファイルを保存してバックアップします。
ファイルの破損を防ぐために、DID ファイルまたはアクティベーションファイルは開かないでください。
ライセンスエラーを避けるために、DID ファイルまたはアクティベーションファイルの名前は変更しないでください。
デバイス上で **In use** または **Usable** 状態のアクティベーションファイルは削除しないでください。使用可能または使用中のアクティベーションファイルを削除すると、関連する機能が正しく機能しなくなります。
ファイルが見つからないか破損している場合は、バックアップファイルをライセンスフォルダにコピーして、ライセンスを回復します。回復したライセンスの状態が **In use** であっても、ライセンスされたすべての機能が機能するわけではない場合は、デバイスを再起動します。

Configure license management

Install licenses

各ロケーションのハードウェアのライセンスキーを購入する必要があります。ハードウェアにライセンスを付与するには、ハードウェアのライセンスキー、SN および DID を使用してアクティベーションファイルを登録し、指定したロケーションにアクティベーションファイルをインストールします。ハードウェアは、別のデバイスにインストールされている場合でもライセンスが付与されます。

手順

System > **License Config** に移動します。
ライセンスを付与する機能を特定します。
ライセンスキーを購入します。
SN および DID を取得します。
アクティベーションファイルを登録するには、製品カテゴリ、ライセンスキー、SN、および DID を使用します。
Install をクリックして、アクティベーションファイルをインストールします。

Compress the license storage area

アクティベーションファイルを登録する前に、ライセンス格納領域に新しいアクティベーションファイルをインストールするための十分な領域があることを確認してください。ライセンス格納領域が十分でない場合は、ライセンス格納領域を圧縮します。圧縮により、期限切れのライセンスおよびアンインストールされたライセンス情報が削除されます。

IRF

このヘルプには、次のトピックがあります。

Introduction
IRF network model
Basic concepts
Master election
IRF bridge MAC persistence
IRF software auto-update
Restrictions and guidelines
Configure IRF

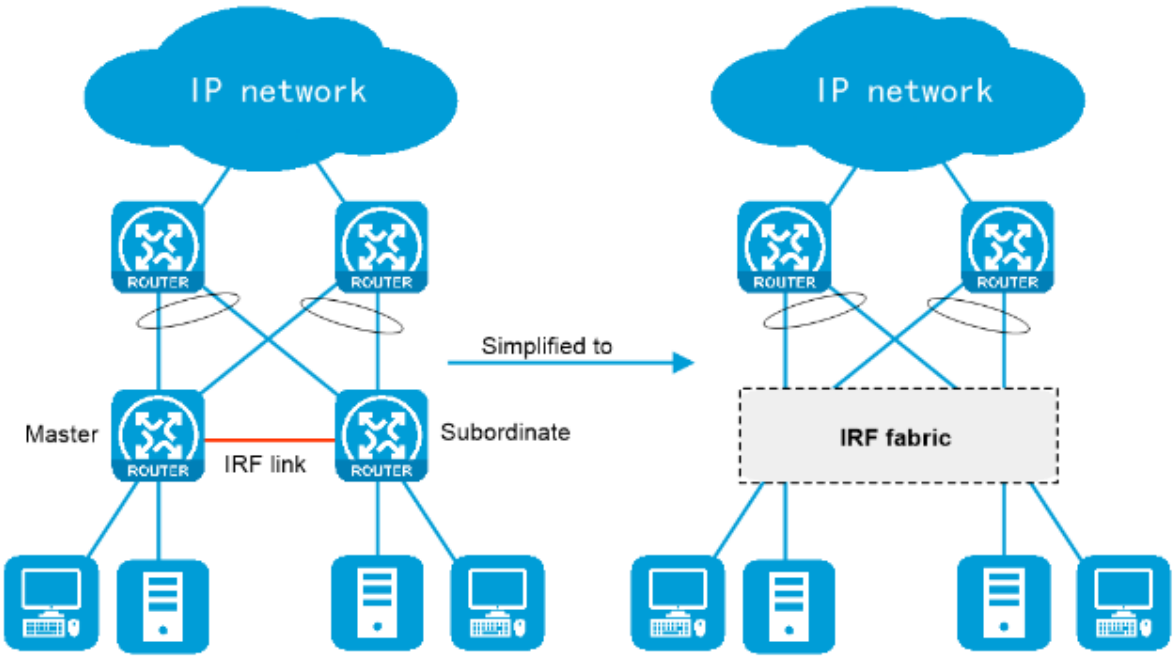
Introduction

Intelligent Resilient Framework(IRF)テクノロジーは、同じレイヤーにある複数の物理デバイスを 1 つの仮想ファブリックに仮想化して、データセンタークラスの可用性と拡張性を実現します。IRF 仮想化テクノロジーは、複数のデバイスの処理能力、相互作用、統合管理、および中断のないメンテナンスを提供します。

IRF network model

図 1 は、2 つのデバイスを持つ IRF ファブリックを示しています。これらのデバイスは、上位層および下位層のデバイスに対して単一ノードとして表示されます。

図 1:IRF アプリケーションのシナリオ



Basic concepts

IRF member roles

IRF は、マスターとスタンバイ(従属とも呼ばれる)の 2 つのメンバーロールを使用します。

デバイスが IRF ファブリックを形成すると、IRF ファブリックを管理および制御するためにマスターが選択され、他のすべてのデバイスがマスターをバックアップします。マスターデバイスに障害が発生すると、他のデバイスが自動的に新しいマスターを選択します。

IRF domain ID

1 つの IRF ファブリックが 1 つの IRF ドメインを形成します。IRF は IRF ドメイン ID を使用して IRF ファブリックを一意に識別し、IRF ファブリックが互いに干渉しないようにします。

IRF member ID

IRF ファブリックは、メンバーID を使用してメンバーを一意に識別および管理します。このメンバーID 情報は、インターフェース番号およびファイルパスの最初の部分として含まれ、IRF ファブリック内のインターフェースおよびファイルを一意に識別します。2 つのデバイスが同じメンバーID を使用する場合、それらのデバイスは IRF ファブリックを形成できません。メンバーID がファブリック内で使用されている場合、デバイスは IRF ファブリックに参加できません。

Member priority

メンバープライオリティは、メンバーデバイスがマスターに選出される可能性を決定します。より高いプライオリティを持つメンバーは、マスターに選出される可能性が高くなります。

IRF port

IRF ポートは、IRF メンバーデバイスを接続する論理インターフェースです。すべての IRF 対応デバイスには 2 つの IRF ポートがあります。

IRF ポートには、IRF-port n/1 および IRF-port n/2 という名前が付けられます。n はデバイスのメンバー ID です。2 つの IRF ポートは、簡略化のために IRF-port 1 および IRF-port 2 とも呼ばれます。

IRF ポートを使用するには、少なくとも 1 つの物理インターフェースをバインドする必要があります。IRF ポートに割り当てられた物理インターフェースは、自動的に集約 IRF リンクを形成します。すべての IRF 物理インターフェースがダウンすると、IRF ポートはダウンします。

IRF physical interface

IRF 物理インターフェースは IRF メンバーデバイスを接続し、IRF ポートにバインドされる必要があります。IRF 物理インターフェースは、IRF メンバーデバイス間でトラフィックを転送します。これには、IRF メンバーデバイス間を通過する必要がある IRF プロトコルパケットおよびデータパケットが含まれます。

IRF split

IRF スプリットは、図 2 に示すように、IRF リンク障害のために IRF ファブリックが 2 つの IRF ファブリックに分割された場合に発生します。分割された IRF ファブリックは同じ IP アドレスで動作します。IRF スプリットは、ネットワーク上でルーティングおよび転送の問題を引き起こします。

図 2 IRF の分割

IRF merge

IRF マージは、図 3 に示すように、2 つの分割された IRF ファブリックが再結合する場合、または 2 つの独立した IRF ファブリックが結合される場合に発生します。

図 3:IRF マージ

Master election

マスター選択は、次の状況で IRF ファブリックトポロジが変更されるたびに実行されます。

IRF ファブリックを確立。

マスターデバイスで障害が発生するか、マスターデバイスが切断されます。

IRF ファブリックが分割されます。

独立した IRF ファブリックがマージされます。

スプリット IRF ファブリックがマージされた場合、マスター選択は行われません。

マスター選択では、マスターが降順で選択されます。

新しいメンバーの優先度が高い場合でも、現在のマスター。

IRF ファブリックが形成されると、すべてのメンバーは自分自身をマスターと見なします。このルールはスキップされます。

優先度の高いメンバー。

システム稼動時間が最も長いメンバー。

起動時間の差が 10 分以下の場合は、2 つのメンバーが同時に起動したとみなされます。これらのメンバーには、次のタイブレーカーが適用されます。

最小の CPU MAC アドレスを持つメンバー。

新しい IRF ファブリックをセットアップするには、マスターの選択後に、下位デバイスをリブートしてセットアップを完了する必要があります。

IRF マージでは、デバイスがマスター選択に失敗した IRF ファブリック内にある場合、デバイスはリブートする必要があります。

IRF bridge MAC persistence

デフォルトでは、IRF ファブリックはマスターデバイスのブリッジ MAC アドレスをブリッジ MAC アドレスとして使用します。LACP などのレイヤー2 プロトコルは、このブリッジ MAC アドレスを使用して IRF ファブリックを識別します。スイッチド LAN では、ブリッジ MAC アドレスは一意である必要があります。

ブリッジ MAC アドレスの重複を回避するために、IRF ファブリックは、ブリッジ MAC オーナーが脱退した後にブリッジ MAC アドレスを自動的に変更できます。ただし、変更によって一時的にトラフィックが中断されます。

ネットワークの状態に応じて、アドレス所有者が脱退した後に IRF ファブリックがブリッジ MAC アドレスを保持または変更できるようにします。使用可能なオプションは次のとおりです。

6 minutes： IRF ファブリックのブリッジ MAC アドレスは、アドレスオーナーが脱退してから 6 分間更されません。タイマーの期限が切れる前にオーナーが戻らない場合、IRF ファブリックは現在のマスター

のブリッジ MAC アドレスをブリッジ MAC アドレスとして使用します。このオプションを使用すると、デバイスのリブート、一時的なリンク障害、または意図的なリンク切断によってブリッジ MAC アドレスが不必要に変更されるのを防ぐことができます。

Always： アドレスオーナーが脱退しても、IRF ファブリックのブリッジ MAC アドレスは変更されません。

Not retain： 元のブリッジ MAC のオーナーが脱退するとすぐに、現在のマスターのブリッジ MAC アドレスが元のアドレスと置き換えられます。

IRF software auto-update

ソフトウェア自動アップデート機能は、マスターの現在のソフトウェアイメージを、IRF ファブリックへの加入を試行しているデバイスに自動的に同期させます。
IRF ファブリックに加入するには、デバイスはファブリック内のマスターと同じソフトウェアイメージを使用する必要があります。
デバイスを IRF ファブリックに追加すると、ソフトウェア自動更新によって、デバイスの起動ソフトウェアイメージと IRF マスターの現在のソフトウェアイメージが比較されます。2 つのイメージセットが異なる場合、デバイスは自動的に次の操作を実行します。

マスターの現在のソフトウェアイメージをダウンロードします。
ダウンロードしたイメージをメイン起動ソフトウェアイメージとして設定します。
新しいソフトウェアイメージでリブートして、IRF ファブリックに再加入します。

ソフトウェア自動アップデートがディセーブルになっている場合は、IRF ファブリック上で実行されているソフトウェアイメージで新しいデバイスを手動でアップデートする必要があります。

> マルチユーザー環境でソフトウェアの自動更新を成功させるには、自動更新プロセス中にメンバーデバイスが再起動されないようにします。自動更新のステータスを管理者に通知するには、ステータスメッセージを設定端末に出力するように **Log Settings** を設定します。

Restrictions and guidelines

次の情報は、基本的な IRF 設定の制限とガイドラインのみを示しています。詳細については、デバイスのコンフィギュレーションガイドの「IRF の設定」を参照してください。

Hardware compatibility with IRF

ファイアウォールは、同じシリーズのファイアウォールとだけ IRF ファブリックを形成できます。

Software requirements for IRF

すべての IRF メンバーデバイスは、同じソフトウェアイメージバージョンを実行する必要があります。ソフトウェア自動更新機能がすべてのメンバーデバイスで有効になっていることを確認してください。

IRF fabric size

ファイアウォール IRF ファブリックには、最大 2 つのメンバーデバイスを含めることができます。

Member ID configuration restrictions

メンバーデバイスのメンバーID を変更すると、新しいメンバーID は再起動時に有効になります。デバイスの再起動後、設定を保存したかどうかにかかわらず、メンバーID に関連するすべての物理リソース(共通物理ネットワークポートを含む)の設定は削除されます。
IRF ファブリックでは、IRF メンバーID を変更すると、望ましくない設定変更やデータ損失が発生する可能性があります。その前に、設定をバックアップし、ネットワークへの影響を十分に理解してください。

Bridge MAC address restrictions for IRF members

IRF ファブリックがマージされるか、または IRF ファブリックが設定されると、IRF は IRF ブリッジ MAC アドレスを無視して、各メンバーデバイスのブリッジ MAC アドレスをチェックします。2 つのメンバーデバイスが同じブリッジ MAC アドレスを持つ場合、IRF のセットアップまたはマージは失敗します。

Candidate IRF physical interfaces

候補 IRF 物理インターフェースはデバイスモデルによって異なります。詳細については、デバイスのコンフィギュレーションガイドの「IRF コンフィギュレーション」を参照してください。

IRF port connection

2 つの隣接する IRF メンバーを接続する場合は、次の制約事項および注意事項に従ってください。
図 4 に示すように、一方のメンバーの IRF-port 1 の物理インターフェースを、もう一方のメンバーの IRF-port 2 の物理インターフェースに接続する必要があります。
IRF ファブリックは、デイジーチェーントポロジーのみを使用できます。隣接する IRF メンバーデバイス間の中間デバイスは許可されません。

集約 IRF リンクの両端に同じ数の IRF 物理インターフェースがあり、IRF 物理インターフェースのタイプが同じであることを確認します。

図 4:IRF 物理インターフェースの接続

IRF physical interface configuration restrictions and guidelines

アップ状態の物理インターフェースを IRF ポートにバインドすると、その物理インターフェースでサービスが中断されます。
マスターデバイス上のすべての IRF 物理インターフェースを一時的にシャットダウンするには、マスターデバイスのプライオリティが下位デバイスよりも高いことを確認する必要があります。
物理インターフェースを IRF ポートにバインドする前、またはバインディングを削除する前に、物理インターフェースのピアインターフェースを必ずシャットダウンする必要があります。

IRF domain ID restrictions

IRF ファブリックには IRF ドメイン ID が 1 つだけあります。ドメイン ID はすべての IRF メンバーデバイスに有効です。ネットワーク内の各 IRF ファブリックに一意のドメイン ID があることを確認してください。

License installation requirements for license-based features

ライセンスベースの機能を IRF ファブリック上で正しく実行するには、すべてのメンバーデバイスにインストールされているライセンスが同じであることを確認します。

Configure IRF

IRF を正常にセットアップするには、次の IRF ファブリックセットアップ手順に従います。
IRF ファブリックのセットアップを計画します。マスター、メンバーID の割り当て、および IRF 接続スキームを決定します。
各メンバーデバイスで次の作業を実行します。
一意のメンバーID とプライオリティを含む基本的な IRF 設定を設定します。

物理インターフェースを IRF ポートにバインドします。
設定をスタートアップコンフィギュレーションファイルに保存します。
IRF 物理インターフェースを接続します。接続が IRF ポートバインディングと一致していることを確認します。
デバイスを再起動します。

メンバーID の割り当てはリブート時に有効になります。メンバーデバイスはマスター選択を実行して、1 つのマスターと 1 つの従属デバイスを含む IRF ファブリックを形成します。

IRF ファブリックにログインします。マスターデバイスの管理ポートの IP アドレスで、IRF ファブリックの Web インターフェースにログインできます。
次のタスクを実行します。
IRF ファブリックトポロジを表示して、その正しさを確認します。
(任意)メンバーID、プライオリティ、または IRF ポートバインディングの設定を変更します。

IRF ファブリックでメンバーID を変更すると、メンバーID 関連の設定が無効になり、予期しない問題が発生する可能性があります。メンバーID を変更する前に、ライブネットワークへの影響を理解してください。

インディングを変更すると、IRF スプリットが発生する可能性があります。IRF ポートバインデする前に、ライブネットワークへの影響を理解してください。

IRF ファブリックで高度な IRF 設定を構成します。
設定をスタートアップコンフィギュレーションファイルに保存します。

IRF ファブリックでは、スタンドアロンデバイスと同じようにソフトウェア機能を設定できます。

Contexts

このヘルプには、次のトピックがあります。

Introduction
Default context and non-default contexts
Assigning resources to a context
Collecting information
Rate limiting
Restrictions and guidelines
Restrictions and guidelines: Stopping a context
Restrictions and guidelines: VLAN assignment
Restrictions and guidelines: Interface assignment
Restrictions and guidelines: Information collection
Configure a context

Introduction

物理ファイアウォールまたは IRF ファブリックは、コンテキストと呼ばれる複数の論理ファイアウォールに仮想化できます。各コンテキストには個別のハードウェアおよびソフトウェア・リソースが割り当てられ、他のコンテキストとは独立して動作します。ユーザーから見ると、コンテキストはスタンドアロンのファイアウォールです。

Default context and non-default contexts

コンテキストをサポートするデバイスは、コンテキストとみなされます。このコンテキストはデフォルトコンテキストと呼ばれます。デフォルトコンテキストでは、常に **Admin** という名前と ID 1 が使用されます。このコンテキストを削除したり、名前または ID を変更したりすることはできません。
物理ファイアウォールにログインすると、デフォルトコンテキストにログインします。デフォルトコンテキストでは、次のタスクを実行できます。

物理ファイアウォール全体を管理します。
デフォルト以外のコンテキストを作成および削除します。
CPU リソース、ディスクスペース、メモリースペース、インターフェース、VLAN など、デフォルト以外のコンテキストリソースを割り当てます。

デフォルト以外のコンテキストにコンテキストを作成することはできません。
デフォルト以外のコンテキストは、それに割り当てられたリソースのみを使用できます。デフォルト以外のコンテキストに割り当てられていないリソースは、デフォルトのコンテキストに属します。

特に明記しない限り、Web ページ上の「コンテキスト」という用語は、デフォルト以外のコンテキストを指します。

Assigning resources to a context

コンテキスト CPU リソース、ディスクスペース、メモリースペース、インターフェース、および VLAN を割り当てることができます。

Assigning VLANs to a context

コンテキストの作成時に、コンテキストが他のコンテキストと VLAN リソースを共有するかどうかを指定できます。

Shared mode : VLAN リソースを他のコンテキストと共有します。VLAN はデフォルトコンテキスト上でのみ作成および管理できます。デフォルト以外のコンテキストは、デフォルトコンテキストから割り当てられた VLAN だけを使用できます。VLAN は複数のコンテキストで使用できます。パケットを受信した物理デバイスは、パケットの着信インターフェースおよび VLAN タグと一致するコンテキストにパケットを転送します。このモードは、複数のコンテキストが同じ VLAN を共有するシナリオに適用されます。

Exclusive mode: VLAN リソースを他のコンテキストと共有しません。コンテキストの管理者は、コンテキストにログインし、コンテキストの VLAN を作成する必要があります。このモードは、コンテキストが独立した VLAN を必要とするシナリオに適用されます。

Assigning interfaces to a context

デフォルトでは、すべてのインターフェースがデフォルトコンテキストに属します。デフォルト以外のコンテキストはインターフェースを使用できません。デフォルト以外のコンテキストが通信できるようにするには、インターフェースを割り当てる必要があります。
インターフェースは、排他モードまたは共有モードでコンテキストに割り当てることができます。

Exclusive mode: このモードでコンテキストに割り当てられたインターフェースは、コンテキストに排他的に属します。コンテキストにログインすると、インターフェースを表示して、インターフェースでサポートされているすべてのコマンドを使用できます。

Shared mode: 共有モードで複数のコンテキストにインターフェースを割り当てると、コンテキストごとに仮想インターフェースが作成されます。仮想インターフェースは物理インターフェースと同じ名前を使用しますが、MAC アドレスと IP アドレスは異なります。仮想インターフェースは物理インターフェースを介してパケットを転送および受信します。共有モードを使用すると、インターフェースの使用率が向上します。

デフォルトコンテキストから物理インターフェースを表示し、インターフェースでサポートされているすべてのコマンドを実行できます。コンテキストの管理者は、コンテキストの仮想インターフェースを表示し、shutdown、description、および network-and-security-related コマンドだけを使用できます。

Specifying a CPU weight for a context

CPU リソースがコンテキストからの処理要件を満たすことができない場合、システムは次のように CPU リソースを割り当てます。

すべてのコンテキストの CPU 重みを指定します。

すべてのコンテキストの CPU 加重のうち、各コンテキストの CPU 加重の割合を計算します。

CPU の重みの割合に基づいて、コンテキストに CPU リソースを割り当てます。

たとえば、3 つのコンテキストが同じ CPU を共有しているとします。キー・コンテキストには重み 2 を割り当て、他の 2 つの各コンテキストには重み 1 を割り当てることができます。システムの CPU リソースが不足すると、キー・コンテキストは他の 2 つの各コンテキストが使用できる CPU リソースの約 2 倍を使用できます。

Assigning disk and memory resources to a context

1 つのコンテキストが大量のディスクリソースまたはメモリーリソースを占有しないようにするには、コンテキストのディスク領域の割合とメモリー領域の割合を指定します。

コンテキストのディスクスペースまたはメモリースペースの割合を指定する前に、コンテキストを開始して、コンテキストが使用しているディスクスペースまたはメモリースペースの量を表示します。コンテキストに割り当てるディスクスペースまたはメモリースペースが、コンテキストの開始と正常な動作に十分であることを確認してください。

Setting the maximum number of concurrent unicast sessions

多数のセッションが大量のメモリーを占有します。これにより、コンテキストのパフォーマンスが低下し、他のコンテキストに影響します。最大数に達すると、追加のセッションは確立されません。この問題を解決するには、コンテキストの同時ユニキャストセッションの最大数を設定します。

この機能は、FTP トラフィックや Telnet トラフィックなどのローカルトラフィックには影響しません。

設定した最大数が既存の同時ユニキャストセッション数よりも小さい場合でも、この設定は有効です。コンテキストでは、余分な既存の同時ユニキャストセッションは削除されず、同時ユニキャストセッション数が最大数を下回った場合にのみ新しいユニキャストセッションが作成されます。

Setting the upper limit of the session establishment rate

この機能は、コンテキストに対して 1 秒当たりに確立できるセッション数を制限します。コンテキストがセッションを確立する頻度が高すぎる場合、CPU 処理能力が不十分なため、他のコンテキストはセッションを確立できません。コンテキストの上限に達すると、追加のセッションは確立できません。

この機能は、FTP トラフィックや Telnet トラフィックなどのローカルトラフィックには影響しません。

Setting the maximum number of security policy rules

この機能では、コンテキストに構成できるセキュリティーポリシールールの数が制限されます。セキュリティーポリシールールはメモリー領域を占有します。構成するセキュリティーポリシールールが多すぎると、他の機能の操作に影響する場合があります。コンテキストの上限に達すると、追加のセキュリティーポリシールールは構成できません。

設定した最大数が既存のセキュリティーポリシールールの数より小さい場合でも、この設定は有効です。コンテキストでは、余分な既存のセキュリティルールは削除されず、セキュリティーポリシールールの数が最大数を下回った場合にのみ、新しいセキュリティーポリシールールを作成できます。

Setting the maximum number of SSL VPN users

この機能は、コンテキストにログインできる SSL VPN ユーザーの数を制限します。最大数に達すると、コンテキストは新しい SSL VPN ユーザーのログイン要求を拒否します。

設定した最大数が、コンテキストにすでにログインしている SSL VPN ユーザーの数よりも小さい場合でも、この設定は有効です。コンテキストは現在ログインしているユーザーをログアウトせず、ログインしているユーザーの数が最大数を下回った場合にだけ、新しいユーザーのログインを許可します。

Setting a throughput threshold

この機能は、コンテキストのスループットを制限して、コンテキストがデバイス上に、コンテキストのスループットを制限します。この機能は、プロトコルパケットの転送を保証するために、サービスパケットを優先的にドロップします。

Collecting information

デフォルトコンテキストでは、複数またはすべてのコンテキストに関するログメッセージ、診断情報、および設定情報を収集できます。

Rate limiting

レート制限は、他のコンテキストとインターフェースを共有するアクティブコンテキストでだけ有効です。

レート制限は、コンテキスト上の 1 秒間の着信ブロードキャストパケットおよびマルチキャストパケットの数を制御します。この機能により、コンテキストが大量のリソースを使用して、他のコンテキストのサービス処理能力を低下させることがなくなります。

この機能では、次の制限が使用されます。

Total broadcast rate limit: デバイス上の 1 秒間の着信ブロードキャストパケットの合計数に対する制限。

Total multicast rate limit: デバイス上の 1 秒間の着信マルチキャストパケットの合計数に対する制限。

Per-context broadcast rate limit: 1 つのコンテキストでの 1 秒間の着信ブロードキャストパケット数の制限。

Per-context multicast rate limit: 1 つのコンテキストでの 1 秒間の着信マルチキャストパケット数の制限。

コンテキスト単位の制限と対応する合計制限の両方に到達すると、デバイスはコンテキストに到着するタイプの後続のパケットをドロップします。
合計制限を 0 に設定すると、対応するレート制限機能がディセーブルになります。
コンテキストごとの有効な制限値が 1000 より小さい場合、その値がデフォルトの制限値になります。デフォルトの制限値は、対応する合計制限値を、他のコンテキストとインターフェースを共有するアクティブコンテキストの数で割った値です。
コンテキストごとの有効な制限が 1000 以上の場合、値はデフォルトの制限または設定された制限になります。

Restrictions and guidelines

Restrictions and guidelines: Stopping a context

コンテキストの停止には注意が必要です。コンテキストを停止すると、そのコンテキストのすべてのサービスが停止され、そのコンテキストのすべてのユーザーがログアウトされます。

Restrictions and guidelines: VLAN assignment

共有する VLAN がすでに存在している必要があります。VLAN をコンテキストに割り当てる前に、デフォルトコンテキストで VLAN を作成する必要があります。
次の VLAN は、コンテキスト間で共有できません。
VLAN 1。
ポートのデフォルト VLAN。
VLAN インターフェースが作成されている VLAN。

Restrictions and guidelines: Interface assignment

物理インターフェースは、共有モードまたは排他モードでコンテキストに割り当てることができます。サブインターフェースや集約インターフェースなどの論理インターフェースは、共有モードでのみコンテキストに割り当てることができます。
サブインターフェースをコンテキストに割り当てた後は、そのプライマリインターフェースをどのコンテキストにも割り当てることはできません。プライマリインターフェースをコンテキストに割り当てた後は、そのサブインターフェースをどのコンテキストにも割り当てることはできません。
共有モードで 1 つのコンテキストにインターフェースを割り当てた後は、コンテキストからインターフェースを再利用する前に、排他モードで他のコンテキストにインターフェースを割り当てることはできません。
デバイスが IRF モードで動作している場合は、IRF 物理インターフェースをデフォルト以外のコンテキストに割り当てないでください。
集約インターフェースのメンバーインターフェースは、コンテキストに割り当てることができません。
Reth インターフェースのメンバーインターフェースは、コンテキストに割り当てることができません。Reth インターフェースのメンバーインターフェースがサブインターフェースである場合、対応するプライマリインターフェースもコンテキストに割り当てることができません。

Restrictions and guidelines: Information collection

デフォルトコンテキストでは、起動されていない非デフォルトコンテキストのログメッセージを収集できません。
デフォルトコンテキストでは、起動されていない非デフォルトコンテキストのコンフィギュレーション情報を収集できません。

Configure a context

インターフェースに関する割り当ておよび設定情報を表示します。
コンテキストを作成します。
コンテキストへのリソースの割り当て:
VLAN およびインターフェースをコンテキストに割り当てます。
コンテキストへの CPU、ディスク、およびメモリーリソースの割り当て
同時ユニキャストセッションの最大数を設定します。
セッション確立レートの上限を設定します。
セキュリティーポリシー規則の最大数を設定します。
SSL VPN ログインユーザーの最大数を設定します。
スループットしきい値を設定します。
コンテキストのリソース使用率を監視します。

Administrators

Introduction

管理者は、次の観点からデバイスを設定および管理します。

User account management: ユーザーカウント情報およびアトリビュート(ユーザー名やパスワードなど)を管理します。

Role-based access control: ユーザー役割ごとにユーザーのアクセス許可を管理します。

Password control: ユーザーのパスワードを管理し、事前定義されたポリシーに基づいてユーザーのログインステータスを制御します。

管理者のサービスタイプは、HTTP、HTTPS、SSH、Telnet、FTP、PAD、または端末です。端末ユーザーは、コンソールポートを介してデバイスにアクセスできます。

User account management

デバイス上のユーザーカウントは、同じユーザー名でデバイスにログインするユーザーのアトリビュートを管理します。アトリビュートには、ユーザー名、パスワード、ロール、サービス、およびパスワード制御パラメーターが含まれます。

Role-based access control

デバイスは、ロールをユーザーに割り当てることによって、ユーザーのアクセス許可制御を実装します。ロールには、ユーザーがアクセスできる機能とアクセスできない機能のセットが含まれます。

Access permission control

Web インターフェースでは、特定の Web ページへのアクセス権限を持つロールを構成し、特定の Web ページへのアクセスを拒否できます。これらの Web ページは Web メニューと呼ばれます。

Web メニューは、次のオプションに基づいて制御されます。

Read-only: このオプションを選択すると、設定するロールには、指定した項目の設定およびメンテナンス情報を表示する Web メニューへのアクセス権限が与えられます。

Read and write: このオプションを選択すると、構成する役割には、指定した項目の次の Web メニューへのアクセス許可が与えられます。

設定およびメンテナンス情報を表示する Web メニュー。

項目を設定する Web メニュー。

No permissions: このオプションを選択すると、構成するロールには、指定したアイテムに対するアクセス許可が与えられません。

Predefined roles

システムには事前定義済のロールが用意されています。表 1 に示すように、これらのロールのアクセス権限は異なります。事前定義済のロールではユーザーの要件を満たせない場合、管理者は必要に応じてユーザーのロールを構成できます。

表 1 事前定義された役割と権限のマトリックス

ロール名	アクセス許可
network-admin	このロールには、システム内のすべての機能にアクセスする権限があります。
security-admin	この役割には、セキュリティーサービス機能を構成し、セキュリティーサービスの処理ステータスを監視する権限があります。
audit-admin	この役割には、デバイス操作を監査する権限のみがあります。
system-admin	このロールには、システム機能を設定し、デバイスの実行ステータスを監視する権限があります。
context-admin	このロールには、コンテキスト内のすべてのフィーチャーにアクセスする権限があります。
vsys-admin	このロールには、vSystem のすべての機能にアクセスする権限があります。この役割のサポートは、デバイスモデルによって異なります。

Role assignment

ユーザーにロールを割り当てることによって、ユーザーにアクセス権を割り当てます。ユーザーは、ユーザーに割り当てられたロールにアクセス可能なアイテムのコレクションを使用できます。

認証方式に応じて、ロール割り当てには次の方式があります。

Local AAA authorization: ユーザーがローカル認可を通過すると、デバイスはローカルユーザーカウントで指定されたロールをユーザーに割り当てます。

Remote AAA authorization: ユーザーがリモート認可を通過すると、リモート AAA サーバーはサーバーで指定されたロールをユーザーに割り当てます。

ユーザーにロールが割り当てられていない場合は、デバイスにログインできません。

ユーザーに割り当てることができるロールは 1 つだけです。

Password control

パスワード制御には、次の機能があります。

ローカルユーザーのログインおよびスーパーパスワードの設定、有効期限、更新を管理します。

事前定義されたポリシーに基づいてユーザーのログインステータスを制御します。

パスワード制御設定には、グローバル設定とユーザー固有の設定が含まれます。

Administrator Password Control ページの設定は、すべての管理者ユーザーに適用されるグローバルなパスワード制御設定です。

Create Administrator ページまたは **Edit Administrator** ページで設定されたパスワード制御設定はユーザー固有の設定であり、ユーザーだけに適用されます。

特に明記されていない限り、ユーザー固有のパスワード制御設定は、グローバルなパスワード制御設定よりも優先されます。

Minimum password length

ユーザーパスワードの最小長を定義できます。パスワードが構成済の最小長より短い場合、システムはパスワードを拒否します。

Password complexity check

パスワードの強度は、その複雑さが増すにつれて増大します。あまり複雑でないパスワードは、解読される可能性が高くなります。たとえば、ユーザー名または繰り返される文字を含むパスワードは、そうでないパスワードよりも解読される可能性が高くなります。システムセキュリティーを強化するには、パスワードの複雑さポリシーを構成して、ユーザーが構成したパスワードがほとんどのパスワード攻撃に対して十分に複雑であることを確認します。

次のパスワード複雑度要件を適用できます。

パスワードには、ユーザー名または逆スペルのユーザー名を含めることはできません。たとえば、ユーザー名が **abc** の場合、パスワードを **abc982** または **2cba** にすることはできません。この要件をユーザーに有効にするには、グローバルおよびユーザー固有のパスワード制御構成ページの両方で有効にする必要があります。

パスワードには、連続する同一の文字を 2 つ以上含めることはできません。たとえば、パスワード **a111** は許可されません。この要件をユーザーに適用するには、ユーザー固有のパスワード制御構成ページまたはグローバルパスワード制御構成ページで有効にする必要があります。

Password composition check

この機能のユーザー固有の設定を有効にするには、グローバルパスワード制御設定ページでもこの機能をイネーブルにする必要があります。

パスワードには、次の種類の文字を組み合わせて使用できます。

大文字の A～Z。
小文字の a～z。
数字の 0～9。
特殊文字。表 2 を参照してください。

表 2 特殊文字

キャラクタ名	記号	キャラクタ名	記号
Ampersand sign	&	アポストロフィ	'
Asterisk	*	アット記号	@
Back quote	`	バックスラッシュ	¥
Blank space	N/A	キャレット	^
Colon	:	カンマ	,
Dollar sign	$	ドット	.
Equal sign	=	感嘆符	!
Left angle bracket	<	左中括弧	{
Left bracket	[	左括弧	(
Minus sign	-	パーセント記号	%
Plus sign	+	ポンド記号	#
Quotation marks	"	右山括弧	>
Right brace	}	右ブラケット	]
Right parenthesis	)	セミコロン	;
Slash	/	ティルダ	~
Underscore	_	縦棒	|

システムのセキュリティー要件に応じて、表 3 に示すように、パスワードに含める必要がある文字タイプの最小数と、各タイプの最小文字数を設定できます。

表 3 パスワード構成ポリシー

パスワードの組み合わせレベル	文字タイプの最小数	各タイプの最小文字数
レベル 1	1	1
レベル 2	2	1
レベル 3	3	1

レベル 4	4	1

ユーザーがパスワードを設定または変更すると、システムは、パスワードが組合せ要件を満たしているかどうかを調べます。パスワードが要件を満たしていない場合、操作は失敗します。

Password updating

この機能を使用すると、ユーザーがパスワードを変更できる最小間隔を設定できます。ユーザーは、指定した間隔内に 1 回のみパスワードを変更できます。

最小間隔は、次の状況には適用されません。

- ユーザーは、最初のログイン時にパスワードの変更を求められます。
- パスワードの有効期限が切れます。

Password expiration

この機能のユーザー固有の設定を有効にするには、グローバルパスワード制御設定ページでもこの機能をイネーブルにする必要があります。

パスワードの有効期限は、ユーザーパスワードにライフサイクルを強制します。パスワードの有効期限が切れた後、ユーザーはパスワードを変更する必要があります。

有効期限が切れたパスワードを使用してログインしようとすると、エラーメッセージが表示されます。ユーザーは新規パスワードの入力を求められます。新規パスワードは有効である必要があり、ユーザーは確認時に同じパスワードを入力する必要があります。

Telnet ユーザー、SSH ユーザーおよびコンソールユーザーは、自分のパスワードを変更できます。FTP ユーザーは、管理者がパスワードを変更する必要があります。

Password expiration notification

ユーザーがログインすると、システムは、指定された通知期間以下の時間にパスワードが期限切れになるかどうかを判断します。期限切れになると、システムはユーザーにパスワードの期限切れを通知し、ユーザーがパスワードを変更できるようにします。

- ユーザーが新しい有効なパスワードを設定すると、システムは新しいパスワードとセットアップ時間を記録します。
- ユーザーがパスワードを変更しないか、変更しなかった場合、システムは、パスワードが期限切れになるまで、現在のパスワードを使用してユーザーがログインすることを許可します。

Telnet ユーザー、SSH ユーザーおよびコンソールユーザーは、自分のパスワードを変更できます。FTP ユーザーは、管理者がパスワードを変更する必要があります。

Login with an expired password

パスワードの有効期限が切れた後、一定期間内に一定回数ログインすることをユーザーに許可できます。たとえば、有効期限が切れたパスワードによる最大ログイン数を 3 に設定し、期間を 15 日に設定した場

合、ユーザーはパスワードの有効期限が切れた後、15 日以内に 3 回ログインできます。

Password history

この機能を使用すると、ユーザーが使用したパスワードをシステムに格納できます。ユーザーがパスワードを変更すると、システムは新規パスワードを現行パスワードおよびパスワード履歴レコードに格納されているパスワードと比較します。新規パスワードは、現行パスワードおよび履歴レコードに格納されているパスワードと 4 文字以上異なる必要があります。新規パスワードがこの要件を満たしていない場合は、エラーメッセージが表示され、パスワード変更操作が拒否されます。

各ユーザーに対してシステムが保持する履歴パスワードレコードの最大数を設定できます。履歴パスワードレコードの数が設定を超えると、最新のレコードが最も古いレコードを上書きします。

現在のログインパスワードは、管理者のパスワード履歴には格納されません。管理者のパスワードは暗号テキストで保存され、プレーンテキストのパスワードに戻すことはできません。

Login attempt limit

連続ログイン失敗回数を制限すると、パスワードの推測を効果的に防止できます。この機能のユーザー固有の設定を有効にするには、グローバルパスワード制御構成ページでもこの機能を有効にする必要があります。

ログイン試行回数の制限は、FTP および VTY ユーザーに適用されます。次のタイプのユーザーには適用されません。

存在しないユーザー(デバイスに設定されていないユーザー)。

コンソールポートを介してデバイスにログインするユーザー。

ユーザーがログインに失敗すると、システムはユーザーアカウントとユーザーの IP アドレスをパスワード制御ブラックリストに追加します。ユーザーが最大連続試行回数を超えてログインに失敗した場合、ログイン試行制限はユーザーとユーザーアカウントを次のいずれかの方法で制限します。

Lock permanently: パスワード制御ブラックリストからアカウントが手動で削除されるまで、ユーザーカウントを無効にします。

Not lock: ユーザーがユーザーカウントを引き続き使用できるようにします。ユーザーがこのアカウントを使用してデバイスに正常にログインすると、ユーザーの IP アドレスとユーザーカウントがパスワード制御ブラックリストから削除されます。

Lock temporarily: 一定期間、ユーザーカウントを無効にします。

次のいずれかの条件が存在する場合、ユーザーはアカウントを使用してログインできます。

ロックタイマーが期限切れになります。

ロックタイマーの期限が切れる前に、パスワード制御ブラックリストからアカウントが手動で削除されます。

このアカウントは、このユーザーに対してのみロックされています。他のユーザーはこのアカウントを使用でき、ブラックリストに掲載されたユーザーは他のユーザーカウントを使用できます。

Maximum account idle time

ユーザーアカウントの最大アイドル時間を設定できます。最後に正常にログインしてからこの時間の間にアカウントがアイドル状態になると、そのアカウントは無効になります。

Password strength management

管理者ユーザーが脆弱なパスワードを使用してログインすると、パスワード制御がイネーブルになっているかどうかにかかわらず、デバイスはユーザーにパスワードの変更を要求します。

強制的な弱いパスワードの変更がイネーブルになっている場合、ユーザーはデバイスにログインするために、弱いパスワードを複雑なパスワードに変更する必要があります。

強制的な弱いパスワード変更がディセーブルになっている場合、ユーザーはパスワード変更プロンプトを無視してデバイスへのログインを続行できます。

デバイスは、パスワードが次の特性を持つ場合、そのパスワードが脆弱であると判断します。

パスワードの最小長より短い。詳細は、「パスワードの最小長」を参照してください。

パスワード構成ポリシーに準拠していません。詳細は、「パスワード構成チェック」を参照してください。

ユーザー名または逆のスペルのユーザー名が含まれます。詳細は、「パスワードの複雑性のチェック」を参照してください。

パスワード制御が使用可能な場合は、連続する 3 文字以上の同一文字を使用します。詳細は、「パスワードの複雑度チェック」を参照してください。

Restrictions and guidelines

Restrictions and guidelines: Role-based access control

ロールに対するアクセス権の変更は、変更後にそのロールでログインしたユーザーに対してのみ有効です。

Restrictions and guidelines: Password control

ユーザーが最大連続試行回数に失敗すると、システムはユーザーカウントを使用してユーザーの IP アドレスを介してログインすることを禁止します。

パスワード制御の設定を有効にするには、パスワード制御を有効にする必要があります。パスワード制御を有効にするには **Administrators** ページの **Password control** をクリックして **Administrator Password Control** ページに入り、**Enable password control** を選択します。

Administrator Password Control ページと **User Password Control** ページでは、パスワード制御の設定が共有されます。一方のページでパスワード制御の設定を変更すると、新しい設定がもう一方のページに自動的に同期化されます。

パスワード制御機能が有効になっている場合、新しいパスワードには少なくとも 4 つの異なる文字が含まれている必要があります。
Administrator Password Control ページおよび **Create Administrator** または **Edit Administrator** ページの **Advanced settings** 領域では、以下の設定を指定できます。
パスワードの有効期限。
パスワードの最小長。
パスワード複雑性ポリシー。
パスワード構成ポリシー。
最大ログイン試行回数。

Administrator Password Control ページのパスワード制御設定は、すべての管理者に有効です。ただし、**Create Administrator** ページまたは **Edit Administrator** ページの設定は、**Administrator Password Control** ページの設定よりも優先度が高くなります。

Restrictions and guidelines: Password strength management

必須の脆弱なパスワード変更をイネーブルにするには、少なくとも 1 つのパスワード強度チェック基準をイネーブルにする必要があります。
強制脆弱パスワード変更機能は、この機能がイネーブルにされた後にデバイスにログインしたユーザーに対してだけ有効です。この機能は、デバイスにログインしたユーザーには影響しません。

Restrictions and guidelines: FTP users

FTP ユーザーはアカウンティングをサポートしません。これらのユーザーは、**Max concurrent logins** フィールドの値による制限を受けません。
FTP ユーザーは、期限切れのパスワードを使用してデバイスにログインできません。FTP ユーザーは、管理者がパスワードを変更する必要があります。

MAC address learning through a Layer 3 device

Introduction

この機能を使用すると、ネットワークトラフィック制御のためにデバイスと端末の間にレイヤー3 デバイス(通常はゲートウェイ)が存在する場合に、デバイスは端末(PC など)の MAC アドレスを学習できます。

図 1:レイヤー3 デバイスワークフローによる MAC アドレスの学習

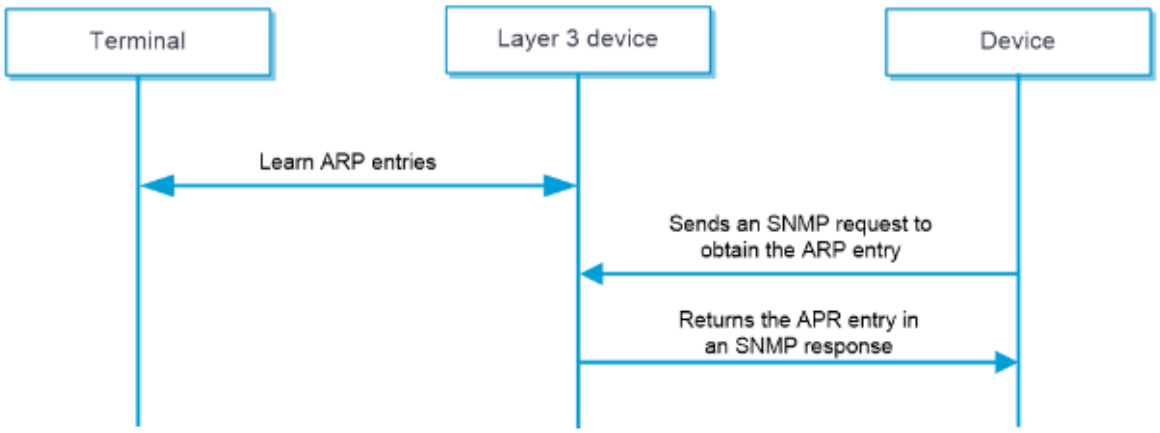


図 1 に示すように、レイヤー3 デバイスを介した MAC アドレスの学習は次のように進みます。
レイヤー3 デバイスは端末の IP-MAC バインディングを学習し、ARP エントリを生成します。
デバイスは、指定された間隔で SNMP 要求をレイヤー3 デバイスに送信して、ARP エントリを要求します。
レイヤー3 デバイスは、ARP エントリを含む応答を送信します。
応答を受信すると、デバイスは ARP エントリをメモリーに保存します。その後、端末の MAC アドレスを学習できます。

Restrictions and guidelines

レイヤー3 デバイスが SNMPv2c または SNMPv3 をサポートし、SNMP エージェントがイネーブルになっており、コミュニティ名が設定されていることを確認します。
IPv4 アドレスからマッピングされた MAC アドレスだけを学習できます。
デバイスとレイヤー3 デバイスの間に NAT デバイスが存在しないことを確認します。
この機能は、VRF ネットワークには適用されません。

Configure MAC address learning through a Layer 3 device

手順

System > **Maintenance** > **MAC Learning Through L3 Device** > **L3 Device Access Setting** を選択します。

Enable をクリックして、レイヤー3 デバイスを介した MAC アドレス学習をイネーブルにします。

(任意)ポーリング間隔とアイドルタイムアウトを設定します。

表 1 レイヤー3 デバイスを介した MAC アドレス学習の構成項目

項目	説明
Polling interval	SNMP 要求の送信間隔(秒単位)
Idle timeout	SNMP 応答のアイドルタイムアウト(秒単位)

Apply をクリックします。

レイヤー3 デバイスを追加します。

Add をクリックします。

次の設定を行います。

項目	説明
SNMP version	SNMP バージョン。オプションには v2c および v3 があります。
IP address	ターゲットレイヤー3 デバイスの IP アドレス(通常はターミナルネットワークのゲートウェイ)。IPv4 アドレスだけがサポートされます。
Community name (SNMPv2c)	コミュニティ内のデバイスは、認証にコミュニティ名を使用します。デバイスは、レイヤー3 デバイス上の SNMP エージェントと同じコミュニティ名を持つ場合にのみ、レイヤー3 デバイスと通信できます。
Username (SNMPv3)	認証を実行できるのは、デバイスとレイヤー3 デバイス上の SNMP エージェントのユーザー名が同じ場合だけです。
Authentication algorithm	認証を成功させるには、これらの設定がレイヤー3 デバイスの SNMP エージェントの設定と同じであることを確認します。
Authentication password	
Encryption algorithm	
Encryption password	

OK をクリックします。

SNMP

Introduction

Simple Network Management Protocol(SNMP;簡易ネットワーク管理プロトコル)は、ベンダー、物理特性、および相互接続テクノロジーに関係なく、管理ステーションがネットワーク上のデバイスにアクセスして操作するために使用されます。
SNMP を使用すると、ネットワーク管理者は、状態の監視、トラブルシューティング、統計情報の収集、およびその他の管理目的で、管理対象デバイス上の変数を読み取って設定できます。

SNMP framework

SNMP フレームワークには、次の要素があります。

SNMP manager: NMS 上で動作し、ネットワーク内の SNMP 対応デバイスを監視および管理します。

SNMP agent: 管理対象デバイス上で動作し、NMS からの要求を受信して処理します。また、インターフェースの状態変更などのイベントが発生した場合は、NMS に通知を送信します。

Management Information Base(MIB): SNMP マネージャが読み取りと設定を行うために SNMP エージェントによって維持される変数(インターフェースステータスや CPU 使用率など)を指定します。

SNMP versions

デバイスは SNMPv1、SNMPv2c、および SNMPv3 をサポートしています。NMS と SNMP エージェントが SNMP 接続を確立するには、同じ SNMP バージョンを使用する必要があります。

SNMPv 1: 認証にコミュニティ名を使用します。SNMP エージェントにアクセスするには、NMS は SNMP エージェントに設定されているのと同じコミュニティ名を使用する必要があります。NMS が使用するコミュニティ名がエージェントに設定されているコミュニティ名と異なる場合、NMS は SNMP セッションを確立してエージェントにアクセスしたり、エージェントからトラップを受信したりできません。

SNMPv2c: 認証にコミュニティ名を使用します。SNMPv2c は SNMPv1 と互換性がありますが、より多くの動作タイプ、データタイプ、およびエラーコードをサポートします。

SNMPv 3: User-Based Security Model(USM)を使用して SNMP 通信を保護します。整合性、真正性、および機密性のために SNMP パケットを認証および暗号化する認証およびプライバシーメカニズムを設定できます。

Configuration management

Introduction

構成ファイルには、デバイスのソフトウェア機能設定のセットが含まれています。ソフトウェア機能設定は構成ファイルに保存できるため、構成は再起動後も保持されます。構成ファイルは、将来使用するためにサーバーにバックアップすることもできます。たとえば、同じ構成を共有する複数のデバイスに構成ファイルをインポートできます。

Configuration types

Factory defaults

出荷時のデフォルトは、デバイスに付属の基本設定です。スタートアップコンフィギュレーションファイルが使用できない場合、デバイスは出荷時のデフォルトで起動します。

Startup configuration

デバイスはスタートアップ時にスタートアップコンフィギュレーションを使用してソフトウェア機能を設定します。デバイスの起動後、次の起動時にロードされるコンフィギュレーションファイルを指定できます。スタートアップコンフィギュレーションファイルが使用できない場合、デバイスは工場出荷時のデフォルトで起動します。

Running configuration

実行コンフィギュレーションは、デバイスの動作中に有効になります。これには、変更されていないスタートアップ設定と新しい設定が含まれます。実行コンフィギュレーションはメモリーに格納され、デバイスのリブートまたは電源オフ時にクリアされます。電源の再投入またはリブート後に実行コンフィギュレーションを使用するには、コンフィギュレーションファイルに保存します。

Configuration backup

この機能を使用して、デバイス上の実行コンフィギュレーションをローカルコンフィギュレーションファイルまたは FTP または TFTP サーバー上のコンフィギュレーションファイルにバックアップします。デバイスは、即時バックアップおよび定期バックアップをサポートします。
バックアップコンフィギュレーションファイルは、コンフィギュレーションロールバックに使用できます。

Configuration rollback

この機能を使用して、実行コンフィギュレーションをコンフィギュレーションファイル内のコンフィギュレーシ

ョンに置き換えます。コンフィギュレーションファイルは、ローカルデバイス、FTP サーバー、または TFTP サーバーに保存できます。コンフィギュレーションロールバック用に FTP サーバーまたは TFTP サーバー上のコンフィギュレーションファイルを使用する場合は、ロールバック時間を指定する必要があります。

Restrictions and guidelines

工場出荷時のデフォルトに戻すと、デバイスから作成したすべての設定が削除されます。
サーバーベースのバックアップまたはロールバックを使用する場合は、デバイスがリモート FTP または TFTP サーバーに到達できることを確認します。

Manage the running configuration

Back up the running configuration

System タブをクリックします。
ナビゲーションペインで、**Maintenance** > **Configuration Management**.を選択します。
Back up current configuration をクリックします。
設定バックアップパラメーターを設定します。

表 1 構成バックアップの構成項目

項目	説明
Backup type	バックアップ設定ファイルを保存する場所を選択します。 **Back up to local**。 **Back up to server**。
Auto backup interval	定期的な設定バックアップの間隔を入力します。 このパラメーターを設定しないと、デバイスは実行コンフィギュレーションを定期的にバックアップしません。
Max backup files	デバイスに保存できるバックアップコンフィギュレーションファイルの最大数を入力します。 最大数に達すると、システムは新しいバックアップファイルの最も古いバックアップファイルを削除します。
Local backup path	バックアップコンフィギュレーションファイルを保存するデバイス上のディレクトリーを入力します。 ディレクトリーは、デバイス上にすでに存在している必要があります。
Prefix name	バックアップ構成ファイルのファイル名プレフィックスを入力します。 バックアップ構成ファイルには、prefix_serial number.**cfg** の形式で名前が付けられます。

Immediate backup	実行コンフィギュレーションをただちにバックアップするには、この項目を選択します。
Server type	ファイル転送プロトコルを選択します。オプションには、FTP と TFTP があります。
Address	ファイルサーバーの IPv4 または IPv6 アドレスを入力します。
VRF	ファイルサーバーが属する VPN インスタンスの名前を選択します。
Username	ファイルサーバーにログインするためのユーザー名を入力します。
Password	ファイルサーバーにログインするためのパスワードを入力します。
Port	ファイルサーバーのポート番号を入力します。
Backup path	バックアップコンフィギュレーションファイルが保存されるサーバー上のパスを入力します。

OK をクリックします。

Roll back the configuration

System タブをクリックします。
ナビゲーションペインで、**Maintenance** > **Configuration Management** を選択します。
Configure rollback をクリックします。
ロールバックファイルの場所を選択します。
ローカルストレージデバイスに保存されている設定ファイルを使用するには、**Local device** を選択します。
リモートファイルサーバーに保存されている設定ファイルを使用するには、**Server** を選択します。
設定をロールバックするか、またはロールバックをスケジュールします。
ロールバックにローカル構成ファイルを使用している場合は、**Location** フィールドでローカルディレクトリーを指定し、**Access to the file** をクリックしてディレクトリー内の構成ファイルを表示し、使用している構成ファイルを識別して、**Roll Back** リンクをクリックして構成をロールバックします。
ロールバックにリモートサーバー上の構成ファイルを使用している場合は、表 2 に示すパラメーターを構成してロールバックをスケジュールし、**OK** をクリックします。

表 2 サーバーベースのロールバックの構成項目

項目	説明
Server type	サーバータイプを選択します。オプションには、FTP および TFTP があります。
Address	サーバーの IPv4 または IPv6 アドレスを入力します。
VRF	サーバーが属する VPN インスタンスの名前を選択します。
Username	FTP または TFTP サーバーにログインするためのユーザー名を入力します。
Password	FTP または TFTP サーバーにログインするためのパスワードを入力します。

Port	FTP または TFTP サーバーのポート番号を入力します。
Rollback file path	ロールバックコンフィギュレーションファイルが保存されるパスを入力します。
Default rollback file	デフォルトのロールバックコンフィギュレーションファイルの名前を入力します。 ロールバックコンフィギュレーションファイルを指定しない場合は、デフォルトのロールバックコンフィギュレーションファイルが使用されます。
Rollback file	ロールバックコンフィギュレーションファイルの名前を入力します。
Rollback date	コンフィギュレーションロールバックを実行する日付を設定します。
Rollback time	コンフィギュレーションロールバックを実行する時間を設定します。 ロールバック時間の設定が必要です。
Cancel scheduled rollback	ロールバックスケジュールをキャンセルするには、このオプションを選択します。

Packet capture

このヘルプには、次のトピックがあります。

Introduction
Restrictions and guidelines
Perform packet capture
Start packet capture
Configure packet capture settings

Introduction

パケットキャプチャ機能は、着信および発信パケットをキャプチャし、パケットキャプチャレコードを生成し、レコードを.cap ファイルに保存します。このファイルは、デバイスまたはリモートファイルサーバー上に存在できます。Wireshark などのパケットアナライザを使用して、トラフィック分析用のファイルを表示できます。

Restrictions and guidelines

デバイス上で実行できるパケットキャプチャプロセスは 1 つだけです。
パケットキャプチャパラメーターを設定できるのは、パケットキャプチャが開始されていない場合だけです。
必要な場合にのみパケットキャプチャを開始します。パケットキャプチャはデバイスのパフォーマンスに影響します。
パケットキャプチャによってデバイス上の.cap ファイルが保存される場合は、パケットキャプチャの終了後に、必要に応じてデバイス上の.cap ファイルをバックアップします。パケットキャプチャを再度開始すると、既存の.cap ファイルは削除されます。
パケットキャプチャは、デフォルト以外のコンテキストの共有インターフェースではサポートされません。

Perform packet capture

Start packet capture

System > **Diagnosis Center** > **Packet Capture** を選択します。
Start packet capture をクリックします。
表 1 に示すようにフィルタを構成します。

表 1 フィルタを設定するための構成項目

項目	説明
Interface	インターフェースで送受信されたパケットをキャプチャします。
ACL	拡張 ACL によって許可されたパケットをキャプチャします。

Start をクリックします。

Packet Capture ページの **Packet Capture Status** フィールドに、**Started** と表示されます。パケットのキャプチャを停止するには、**Stop packet capture** をクリックします。

Packet Capture Status フィールドに **Stopped** と表示されます。下部のペインには、生成された.cap ファイルに関する情報が表示されます。

Configure packet capture settings

System > **Diagnosis Center** > **Packet Capture** を選択します。

Set packet capture parameters をクリックします。

表 2 に示すように、パケットキャプチャパラメーターを設定します。

表 2 パケットキャプチャの設定項目

項目	説明
Maximum bytes per packet	キャプチャレコードの最大バイト数を指定します。 パケットがこの項目の値よりも長い場合、システムはパケットを切り捨てます。
Maximum packets per file	cap ファイルのパケットキャプチャレコードの最大数を指定します。 システムは最初にパケットキャプチャレコードをメモリーに保存します。ファイルのパケットキャプチャレコードの最大数に達すると、システムはレコードをファイルに保存し、メモリー内のレコードをクリアします。 この項目の値を大きくすると、より多くのメモリー領域が必要になります。使用可能なメモリー領域が制限されている場合は、値を小さくします。
Save files on the device	cap ファイルをデバイスに保存します。 このオプションを選択すると、**Maximum storage space** 項目を設定して、.cap ファイルの最大ストレージ領域を指定できます。最大ストレージ領域に達すると、システムはパケットのキャプチャを停止します。
Save files to a remote server	cap ファイルを FTP または TFTP サーバーに保存します.cap ファイルを FTP サーバーに保存するには、FTP サーバーにアクセスするためのユーザー名とパスワードを設定する必要があります。

OK をクリックします。

Webpage Diagnosis

このヘルプには、次のトピックがあります。

Introduction

Restrictions and guidelines

Perform a webpage diagnosis

Introduction

この機能は、内部ユーザーの Web ページへのアクセス障害を迅速にトラブルシューティングするのに役立つ、読みやすい診断結果を出力します。この機能を使用すると、サーバーに手動で ping を実行したり、ログメッセージを表示したりする必要がありません。

Restrictions and guidelines

この機能は IPv4 だけをサポートします。

この機能は、HTTP Web ページだけをサポートします。

Web ページの診断を開始する前に、セキュリティーポリシーを構成して、次のセキュリティーゾーン間の接続を確保する必要があります。

ユーザーが存在するセキュリティーゾーン。

Web サーバーが存在するセキュリティーゾーン。

セキュリティーゾーン **Local**。

Perform a webpage diagnosis

System > **Diagnosis Center** > **Webpage Diagnosis** を選択します。

Web ページ診断パラメーターを設定します。

表 1 Web ページ診断構成項目

項目	説明
User IP	ユーザーの IP アドレス。
User VRF	ユーザーが所属する VPN インスタンス。

Webpage URL	ユーザーがアクセスした URL(http://www.example.com など)。
Webpage VRF	Web ページが属する VPN インスタンス。

Diagnose をクリックします。

Web ページの診断結果を表示して、障害を分析し、問題を解決します。

(オプション)Web ページの診断結果を.xml ファイルにエクスポートするには **Export** をクリックします。

Packet trace

このヘルプには、次のトピックがあります。

Introduction

Application scenarios

Packet trace modes

Restrictions and guidelines

Configure packet trace

Introduction

パケットトレース機能は、セキュリティーサービスによって処理されたパケットをトレースし、ネットワーク障害のトラブルシューティングに役立つパケットに関する詳細情報を提供します。セキュリティーサービスの例には、攻撃保護、uRPF、セッション管理、接続制限サービスなどがあります。

Application scenarios

パケットトレースは、多数のセキュリティーサービスが展開されており、ネットワーク障害を迅速かつ正確に特定することが困難なシナリオに適用されます。

Packet trace modes

さまざまな状況でのトラブルシューティング要件を満たすために、パケットトレース機能には次のパケットトレースモードが用意されています。

Tracing real traffic: ライブネットワーク内のデバイス上の実トラフィックをトレースします。このモードは、ライブネットワークでのトラブルシューティングに使用します。

Tracing imported packets: .cap または.pcap ファイルからキャプチャされたパケットをインポートし、パケットを分析します。トラブルシューティングに必要なパケットがキャプチャされている場合は、このモードを使用します。このモードを使用すると、他のネットワークでの障害のトラブルシューティングに役立ちます。

Tracing constructed packets: 管理者が設定した設定を使用してパケットを構築し、構成されたセキュリティーサービスのパケット処理結果を確認します。デバイスの構成が完了したら、このモードを使用してパケットを作成し、予想されるパケット処理結果を確認します。

Restrictions and guidelines

cap ファイルは、Diagnose をクリックする前に Capture diagnose packets を選択した場合にだけ、.cap ファイルが生成
同じ.cap ファイルを繰り返しエクスポートすることはできません。エクスポートすると、.cap ファイルはデバイスから削除されます。
cap または.pcap ファイルからキャプチャされたパケットをインポートすると、最初の 10 個のデータフローのパケット(各データフローに 10 個のパケット)だけがインポートされます。パケットトレース機能は、インポートされた完全なパケットだけをトレースします。不完全なパケットはトレースしません。

Configure packet trace

パケットトレースをイネーブルにする前に、次の項目を設定して、トレース対象のパケットを特定します。
IP type: IPv4 または IPv6 パケットタイプを指定します。IPv4 パケットをトレースするには、**IPv4** を選択します。IPv6 パケットをトレースするには、**IPv6** を選択します。

Incoming interface:パケットの着信インターフェースを指定します。

Protocol:パケットで使用されるプロトコルを指定します。

Source address:パケットの送信元アドレスを指定します。

Source port:パケットの送信元ポートを指定します。

Destination address:パケットの宛先アドレスを指定します。

Destination port:パケットの宛先ポートを指定します。

Source MAC:パケットの送信元 MAC を指定します。

Destination MAC:パケットの宛先 MAC を指定します。

VLAN ID:パケットの VLAN ID を指定します。

Diagnosis time:パケットトレースの継続時間を指定します。指定した時間が経過すると、パケットトレースは停止します。この設定は、実際のトラフィックモードでのみサポートされます。

Capture diagnose packets: トレースされたパケットをキャプチャして.cap ファイルに保存するかどうかを指定します。パケットをキャプチャして保存するには、このオプションを選択します.cap ファイルをエクスポートするには、Export をクリックして Captured diagnostic packets を選択し、OK をクリックします。

パケットトレース出力には、セキュリティーサービスモジュールのパケット処理手順が表示されます。サービスモジュールがパケットを正しく処理する場合は、システムによって  が表示されます。サービスモジュールがパケットをドロップする場合は、システムによって  が表示され、パケット損失の原因となります。

IPsec diagnosis

Introduction

IPsec 診断では、IPsec 接続のステータスを検出できます。診断された IPsec 接続に障害がある場合は、診断結果を使用して、設定ミスをチェックし、考えられる原因を見つけることができます。
次の診断モードがサポートされています。

Data flow: システムは指定されたデータフローに従って IPsec ポリシーを取得し、ピアとの IPsec の診断を開始します。

Interface: システムは指定されたインターフェースに従って IPsec ポリシーを取得し、ピアとの IPsec の診断を開始します。

IP address: ピアが IPsec 接続を開始したあと、システムはピア(IP アドレスで指定)との IPsec 診断を開始します。

表 1 IPsec 診断項目

項目	説明
Interface state	ピア IP アドレスへのルートがルーティングテーブルに存在するかどうかを判別します。
If IPsec policy applied on interface	インターフェースの物理層ステータスおよび IP プロトコル層ステータスを決定します。 システムは診断モードに従ってチェックするインターフェースを決定します。 データフローモードおよび IP アドレスモードでは、ルーティングテーブルルックアップによって検出された発信インターフェースがチェックされます。 インターフェースモードでは、ユーザーが指定したインターフェースがチェックされます。
If ACL rule in IPsec policy matches specified flow	インターフェースに IPsec ポリシーを適用するかどうかを指定します。
If ACL rule can match flow on the interface	この項目は、データフローモードでの IPsec 診断でのみ使用できます。 この項目に No と表示されている場合は、IPsec ポリシーの設定を確認します。
IPsec policy configuration check	この項目は、インターフェースモードでの IPsec 診断でのみ使用できます。

	この項目は、IPsec ポリシーで使用される ACL に、IPsec 保護を必要とするトラフィックを識別するための許可規則が含まれているかどうかを示します。許可規則は、IPsec が正しく動作するために必要です。
IKE negotiation result	IPsec ポリシーの設定が完了しているかどうかを確認します。 データフローモードまたはインターフェースモードでは、次の設定がチェックされます。 保護するトラフィックを識別するために使用される ACL。 IPsec SA ネゴシエーションのセキュリティパラメーター。 IPsec トンネルのローカルおよびリモート IP アドレス。 SA パラメーター。 IP アドレスモードでは、次の設定がチェックされます。 IPsec SA ネゴシエーションのセキュリティパラメーター。 SA パラメーター。
IPsec negotiation result	IKE ネゴシエーションが正常に動作している場合、この項目には、IKE negotiation succeeded または IKE SA already exists が表示されます。 その他の情報は、IKE ネゴシエーションに障害があることを示します。指示に従って原因を特定します。たとえば、ローカルエンドとピアエンドの IKE プロファイルが正しく、一致していることを確認します。
Interface state	IPsec ネゴシエーションが正常に動作している場合、この項目には、IPsec negotiation succeeded か、IPsec tunnel already exists ことが表示されます。 その他の情報は、IPsec ネゴシエーションに障害があることを示します。指示に従って原因を特定します。たとえば、ローカルエンドとピアエンドの IPsec ポリシー設定が正しく、一致していることを確認します。

Restrictions and guidelines

データフローモードでは、IPsec カプセル化前のデータフローの送信元および宛先 IP アドレスを **Source IP address** フィールドと **Destination IP address** フィールドに指定します。
データフローモードおよびインターフェースモードでは、IPsec 診断は、デバイスが IPsec 接続を開始するための IPsec ポリシーを検出できる場合にのみ機能します。IPsec ポリシーテンプレートを使用して構成された IPsec ポリシーは、IPsec 接続を開始できないため、データフローモードまたはインターフェースモードでの IPsec 診断では無視されます。
データフローモードまたはインターフェースモードでの IPsec 診断は、最大 20 分間継続できます。タイマーの期限が切れると、診断は停止し、完了した診断項目が表示されます。
IP アドレスモードでの IPsec 診断は、ピアによって開始された IPsec 接続を検出すると開始され、IPsec 接続の診断を完了すると停止します。
一度に実行できる IPsec 診断は 1 つだけです。

IPsec 診断は、IPv4 ネットワークでのみ使用できます。
デバイスは、IPsec ポリシーベースの IPsec 診断をサポートしますが、IPsec プロファイルベースの IPsec 診断はサポートしません。
VRF は、IPsec ポリシーが適用されるインターフェースの VPN インスタンスです。

Fast Internet Access

Introduction

インターネットにアクセスするようにデバイスを迅速に設定するには、次の作業を実行します。

Access mode

アクセスモードには、ルーティングモードとトランスペアレントモードがあります。

Routing mode

このモードは、デバイスゲートウェイのルーティング機能を使用します。このモードでは、3 つのインターネットアクセス方法がサポートされています。サービスプロバイダーから提供された情報に従って方法を選択してください。

WAN インターフェースを設定します。

WAN インターフェースは、表 1 に示すように、次のアクセス方式をサポートします。

表 1 アクセス方法

項目	説明
Specified IP address	サービスプロバイダーから固定 IP アドレスを取得する場合は、この方法を選択します。
DHCP	サービスプロバイダー(または DHCP サーバー)から IP アドレスを自動的に取得する場合は、この方法を選択します。
PPPoE	サービスプロバイダーからインターネットアクセスアカウントを取得する場合は、この方法を選択します。

インターネットアクセス方式に **Specified IP address** を選択した場合、表 2 に WAN インターフェースの構成項目を示します。

表 2:[Specified IP address]を選択した場合の WAN インターフェース構成項目

項目	説明
Interface	WAN インターフェースを選択します。
IP address/subnet mask	WAN インターフェースの IP アドレスとサブネットマスク。このパラメーターはサービスプロバイダーによって提供されます。IP アドレスは、10.1.1.1 などのドット付き 10 進表記です。サブネットマスクの範囲は 1 から 31 です。

Default route	WAN インターフェースのデフォルトルートのネクストホップ IP アドレス。内部ネットワークのユーザーがインターネットにアクセスするために送信するパケットは、WAN インターフェースを介してネクストホップアドレスに送信されます。その後、ネクストホップがパケットを転送します。このパラメーターはサービスプロバイダーによって提供され、ドット付き 10 進表記(10.1.1.254 など)で表されます。
Primary DNS server	プライマリ DNS サーバーの IP アドレス。DNS の詳細については、DNS のヘルプを参照してください。このパラメーターはサービスプロバイダーから提供されます。
Secondary DNS server	セカンダリ DNS サーバーの IP アドレス。プライマリ DNS サーバーに障害が発生すると、デバイスは名前解決にセカンダリ DNS サーバーを使用します。このパラメーターはサービスプロバイダーから提供されます。

インターネットアクセス方式として **DHCP** を選択した場合、表 3 に WAN インターフェースの構成項目を示します。

表 3 DHCP が選択されている場合の WAN インターフェース構成項目

項目	説明
Interface	WAN インターフェースを選択します。

インターネットアクセス方式として **PPPoE** を選択した場合、表 4 に WAN インターフェースの構成項目を示します。

表 4 PPPoE が選択されている場合の WAN インターフェース構成項目

項目	説明
Interface	WAN インターフェースを選択します。
Username	サービスプロバイダーによって提供されるインターネットアクセスアカウントのユーザー名。
Password	インターネットアクセスアカウントのパスワード。サービスプロバイダーから提供されます。
Online mode	**Permanently online**: PPPoE セッションは、確立後も永続的に存在します。 **Auto offline after idle timeout**:指定した時間内にトラフィックが通過しない場合、デバイスは自動的に PPPoE セッションを切断します。ベストプラクティスとして、時間ベ

	ースのアカウンティングユーザーにはこのモードを選択します。
Automatically obtain IP address	インターネットアクセスインターフェースは、サービスプロバイダーから IP アドレスを自動的に取得します。
Use specified IP address	インターネットアクセスインターフェースの IP アドレスを手動で設定します。
IP address/subnet mask	このパラメーターはサービスプロバイダーによって提供されます。IP アドレスは、10.1.1.1 のようにドット付き 10 進表記です。サブネットマスクは 1 から 31 の範囲です。

LAN インターフェースを設定します。

表 5 に、LAN インターフェースの構成項目を示します。

表 5 LAN インターフェース構成項目

項目	説明
Interface	LAN に接続するためのインターフェースを選択します。
IP address/subnet mask	LAN インターフェースの IP アドレスとサブネットマスクを指定します。IP アドレスは、172.16.1.1 のようにドット付き 10 進表記で指定します。サブネットマスクの範囲は 1 から 31 です。
DHCP	DHCP を有効にすると、LAN 内のユーザーは自動的に IP アドレスを取得できます。DHCP の詳細については、DHCP のヘルプを参照してください。
Address pool name	DHCP アドレスプール名
Address range for allocation	DHCP クライアントに割り当てられたアドレス範囲。

DMZ インターフェースを設定します。

表 6 に、DMZ インターフェースの構成項目を示します。

表 6 DMZ インターフェースの構成項目

パラメーター	説明
Interface	DMZ ゾーンに接続するためのインターフェースを選択します。通常、DMZ ゾーンは、外部サービスを提供するデバイス(サーバーなど)を配置するために使用されます。
IP address/subnet mask	DMZ インターフェースの IP アドレスとサブネットマスクを指定します。IP アドレスは、172.16.1.1 のようにドット付き 10 進表記で指定します。サブネットマスクの範囲は 1 から 31 です。

セキュリティーを設定します。

IPS 機能は、企業の情報システムおよびネットワークを攻撃から保護します。

IPS 機能にはライセンスが必要です。この機能を使用するには、ライセンスを購入して正しくインストールしてください。

この機能のサポートは、デバイスモデルによって異なります。

WAN アクセラレーションを設定します。

この機能により、帯域幅が制限されている場合でも、企業の重要なデータを確実に転送できます。

この機能のサポートは、デバイスモデルによって異なります。

フロー制御を設定します。

この機能は、各 WAN インターフェースの予想帯域幅と、各アプリケーションの最大帯域幅および保証帯域幅を制限します。

サービスプロバイダーによって割り当てられた帯域幅に従って、WAN インターフェースの予想帯域幅を設定します。

この機能のサポートは、デバイスモデルによって異なります。

クラウドマネージャサーバーの接続を設定します。

クラウドマネージャサーバーは、セキュリティデバイスを管理するためのプラットフォームであり、セキュリティデバイス構成の迅速な導入、セキュリティー機能の差別化された導入、デバイス構成の変更、およびデバイスステータスの視覚化をサポートします。

デバイスがクラウドマネージャサーバーに接続するためのクラウドマネージャサーバーのドメイン名を設定します。

この機能のサポートは、デバイスモデルによって異なります。

Transparent mode

このモードでは、現在のネットワーク構造は変更されません。WAN インターフェース、LAN インターフェース、および DMZ インターフェースとして設定されたインターフェースは、レイヤー2 インターフェースになります。表 7 に、透過モードの設定項目を示します。

表 7 トランスペアレントモードの設定項目

パラメーター	説明
WAN interface	WAN インターフェースを選択します。
LAN interface	LAN に接続するためのインターフェースを選択します。
DMZ interface	DMZ ゾーンに接続するためのインターフェースを選択します。
Security configuration	IPS を設定します。 この機能のサポートは、デバイスモデルによって異なります。
WAN acceleration	WAN アクセラレーションを設定します。 この機能のサポートは、デバイスモデルによって異なります。
Flow control	フロー制御を設定します。 この機能のサポートは、デバイスモデルによって異なります。

Cloud manager server connection	クラウドマネージャサーバー接続を有効にし、サーバーのドメイン名とポート番号を入力してデバイスをサーバーに接続します。 この機能のサポートは、デバイスモデルによって異なります。