



# H3C Firewall 製品 Comware 7 Web コンフィギュレーションガイド

New H3C Technologies Co., Ltd.  
<http://www.h3c.com>

ソフトウェアバージョン: Release 1118、Release 1118P07  
文書バージョン: 6W101-20180821

**無断転載を禁じます。**

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または配布することはできません。

**商標**

H3C, **H3C**, H3CS, H3CIE, H3CNE, Aolynk, , H<sup>3</sup>Care, , IRF, NetPilot, Netflow, SecEngine, SecPath, SecCenter, SecBlade, Comware, ITCMM および HUASAN は、New H3C Technologies Co.,Ltd.の商標です。その他のすべての商標は、各所有権者の財産です。

**注意**

このドキュメントの情報は、予告なく変更されることがあります。このドキュメントのすべての内容(説明、情報、推奨事項を含む)は正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提示されます。H3C は、このドキュメントに含まれる技術的または編集上の誤りや脱落について責任を負いません。

# はじめに

このコンフィギュレーションガイドでは、スイッチの導入に役立つ次の機能と作業について説明します。

この Web 構成ガイドでは、H3C ファイアウォール製品のソフトウェア機能について説明し、これらの機能の Web 構成例を示します。

この序文には、ドキュメントに関する次のトピックが含まれています。

- 対象者
- 表記法
- 文書のフィードバック

## 対象者

このマニュアルの対象者:

- ネットワークプランナー。
- フィールドテクニカルサポート/サービスエンジニア
- ネットワーク管理者

## 表記法

ここでは、マニュアルで使用されている表記法について説明します。

コマンドの表記法

規約	説明
太字	太字のテキストは、文字どおりに入力したコマンドとキーワードを示します。
イタリック体	斜体のテキストは、実際の値に置き換える引数を表します。
[]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{x y ...}	中カッコは、必要な構文の選択肢を縦棒で区切って囲みます。この中から1つを選択します。
[x y ...]	角カッコは、オプションの構文選択のセットを縦棒で区切って囲みます。この中から1つまたは何も選択しません。
{x y ...}*	アスタリスクの付いた中括弧は、必須構文の選択肢を縦棒で区切って囲みます。この中から少なくとも1つを選択します。
[x y ...]*	アスタリスクの付いた角括弧は、オプションの構文選択肢を縦棒で区切って囲みます。選択肢は1つ、複数、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1~n回入力できます。
#	シャープ記号(#)で始まる行はコメントです。

## GUI のルール

規約	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニューアイテムは太字で表示されます。たとえば、New Userウィンドウが開き、OKをクリックします。
>	マルチレベルメニューは、File Create > Folderのように、山かっこで区切られています。

## シンボル

規約	説明
 <b>警告!</b>	重要な情報を理解していない場合や、その情報に従っていない場合に、けがをするおそれがある場合に注意を促す警告。
 <b>注意:</b>	重要な情報が理解されていない場合、または情報が理解されていない場合に、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性がある場合に、注意を促す警告。
 <b>重要:</b>	重要な情報への注意を喚起するアラート。
<b>注:</b>	追加情報または補足情報を含むアラート。
 <b>ヒント:</b>	役立つ情報を提供するアラート。

## ネットワークポロジアイコン

規約	説明
	ルーター、スイッチ、ファイアーウォールなどの汎用ネットワークデバイスを表します。
	ルーターまたはレイヤー3スイッチなどのルーティング対応デバイスを表します。
	レイヤー2スイッチやレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2および他のレイヤー2機能をサポートするルーターを表します。
	アクセスコントローラー、Unified Wired-WLANモジュール、またはUnified Wired-WLANスイッチ上のアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向信号を表します。
	指向性信号を表します。
	ファイアーウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。
	ファイアーウォール、ロードバランシング、NetStream、SSL VPN、IPS、またはACGモジュールなどのセキュリティモジュールを表します。

## 本書に記載されている例

このドキュメントの例では、ハードウェアモデル、設定、またはソフトウェアバージョンがデバイスと異なるデバイスを使用している場合があります。通常、例のポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイスの内容とは異なります。

## 文書のフィードバック

製品マニュアルに関するコメントは、[info@h3c.com](mailto:info@h3c.com) まで電子メールでお送りください。

ご意見をお寄せください。

## 内容

Web ログインの設定例 .....	2
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:Web ログインの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	8
スタティック IP アドレスによるインターネットアクセスの設定例 .....	2
はじめに .....	2
前提条件 .....	2
例:スタティック IP アドレスによるインターネットアクセスの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	2
PPPoE によるインターネットアクセスの設定例 .....	2
はじめに .....	2
前提条件 .....	2
例:PPPoE によるインターネットへのアクセス .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	9
ライセンスのアクティベーションとインストールの設定例 .....	2
はじめに .....	2
前提条件 .....	2
例:ライセンス管理の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	2

手順 .....	2
設定の確認 .....	6
<b>シグニチャライブラリアップデートの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:シグニチャライブラリのスケジュールされた自動アップデートの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	5
例:シグニチャライブラリの即時オンラインアップデートの設定 .....	5
ネットワーク構成 .....	5
使用するソフトウェアバージョン .....	6
制限事項とガイドライン .....	6
手順 .....	6
設定の確認 .....	6
例:ローカルシグニチャファイルを使用したデバイスシグニチャライブラリの更新 .....	7
ネットワーク構成 .....	7
使用するソフトウェアバージョン .....	7
手順 .....	7
設定の確認 .....	8
<b>ソフトウェアアップグレードの例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:ソフトウェアのアップグレード .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	5
<b>スタティックルーティングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2

例:スタティックルートの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	5
<b>OSPF の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:OSPF の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	11
<b>BGP の設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
例:BGP の設定 .....	1
ネットワーク構成 .....	1
使用するソフトウェアバージョン .....	2
制限事項とガイドライン .....	2
手順 .....	2
設定の確認 .....	11
<b>RIP の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:RIP の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	9
<b>DHCP の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2

例:DHCP の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	8
<b>DNS 設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:DNS プロキシの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	5
例:DDNS の設定 .....	6
ネットワーク構成 .....	6
使用するソフトウェアバージョン .....	7
前提条件 .....	7
手順 .....	7
設定の確認 .....	9
<b>オブジェクトグループの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	3
例:IPv4 アドレスオブジェクトグループの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	6
例:IPv6 アドレスオブジェクトグループの設定 .....	6
ネットワーク構成 .....	6
使用するソフトウェアバージョン .....	7
手順 .....	7
設定の確認 .....	9
例:MAC アドレスオブジェクトグループの設定 .....	9
ネットワーク構成 .....	9
使用するソフトウェアバージョン .....	10

手順 .....	10
設定の確認 .....	12
例:サービスオブジェクトグループの設定.....	12
ネットワーク構成 .....	12
使用するソフトウェアバージョン.....	13
手順 .....	13
設定の確認 .....	15
例:時間範囲の設定 .....	15
ネットワーク構成 .....	15
使用するソフトウェアバージョン.....	16
手順 .....	16
設定の確認 .....	19
<b>公開鍵管理の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:ピアホスト公開キーの入力.....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン.....	3
手順 .....	3
設定の確認 .....	5
例:公開鍵ファイルからのピアホスト公開鍵のインポート.....	7
ネットワーク構成 .....	7
使用するソフトウェアバージョン.....	8
手順 .....	8
設定の確認 .....	10
<b>セキュリティポリシーの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:基本セキュリティポリシーの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン.....	3
手順 .....	3
設定の確認 .....	9
例:セキュリティポリシーと DPI の設定.....	9
ネットワーク構成 .....	9
使用するソフトウェアバージョン.....	10

手順 .....	10
設定の確認 .....	15
<b>攻撃防御の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	3
例:スキャン攻撃防御の設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	4
設定の確認 .....	5
例:フラッド攻撃防御の設定 .....	6
ネットワーク構成 .....	6
使用するソフトウェアバージョン .....	7
手順 .....	7
設定の確認 .....	9
<b>接続制限の設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
例:接続制限の設定 .....	1
ネットワーク構成 .....	1
使用するソフトウェアバージョン .....	2
手順 .....	2
設定の確認 .....	6
<b>IPS の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:IPS の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	7
<b>URL フィルタリングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2

制限事項とガイドライン .....	2
例:URL フィルタリングの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	6
<b>アンチウイルスの設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
制限事項とガイドライン .....	1
例:アンチウイルスの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	2
手順 .....	2
設定の確認 .....	5
<b>データフィルタリングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:データフィルタリングの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	11
<b>ファイルフィルタリングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:ファイルフィルタリングの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	8
<b>APR ベースのセキュリティポリシー設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1

制限事項とガイドライン .....	1
例:APR ベースの厳密なセキュリティポリシーの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
分析 .....	3
手順 .....	5
設定の確認 .....	19
例:APR ベースの緩いセキュリティポリシーの設定 .....	21
ネットワーク構成 .....	21
使用するソフトウェアバージョン .....	22
制限事項とガイドライン .....	22
分析 .....	22
手順 .....	23
設定の確認 .....	31
<b>NAT の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:スタティック NAT の設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	5
例:ダイナミック NAT の NO-PAT の設定 .....	6
ネットワーク構成 .....	6
使用するソフトウェアバージョン .....	6
手順 .....	6
設定の確認 .....	9
例:ダイナミック NAT の PAT 設定 .....	10
ネットワーク構成 .....	10
使用するソフトウェアバージョン .....	10
手順 .....	10
設定の確認 .....	13
例:NAT サーバーの設定 .....	14
ネットワーク構成 .....	14
使用するソフトウェアバージョン .....	14
手順 .....	14
設定の確認 .....	16
例:スタティック NAT444 の設定 .....	16
ネットワーク構成 .....	16

使用するソフトウェアバージョン .....	17
手順 .....	17
設定の確認 .....	19
例:ダイナミック NAT444 の設定 .....	20
ネットワーク構成 .....	20
使用するソフトウェアバージョン .....	20
手順 .....	20
設定の確認 .....	23
<b>IPsec VPN 設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:IPv4 サブネット用の IPsec トンネルの設定 .....	4
ネットワーク構成 .....	4
使用するソフトウェアバージョン .....	4
手順 .....	4
設定の確認 .....	12
<b>SSL VPN 設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:自己署名サーバー証明書による Web アクセスの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	10
例:相互証明書認証による Web アクセスの設定 .....	12
ネットワーク構成 .....	12
使用するソフトウェアバージョン .....	13
手順 .....	13
設定の確認 .....	32
例:自己署名サーバー証明書による TCP アクセスの設定 .....	34
ネットワーク構成 .....	34
使用するソフトウェアバージョン .....	35
制限事項とガイドライン .....	35
手順 .....	35
設定の確認 .....	42
例:CA 署名付きサーバー証明書による TCP アクセスの設定 .....	45
ネットワーク構成 .....	45

使用するソフトウェアバージョン .....	45
制限事項とガイドライン .....	46
手順 .....	46
設定の確認 .....	61
例:ローカル認証と自己署名証明書による IP アクセスの設定 .....	63
ネットワーク構成 .....	63
使用するソフトウェアバージョン .....	64
制限事項とガイドライン .....	64
手順 .....	65
設定の確認 .....	75
例:RADIUS 認証による IP アクセスの設定 .....	77
ネットワーク構成 .....	77
使用するソフトウェアバージョン .....	78
制限事項とガイドライン .....	78
手順 .....	79
設定の確認 .....	107
例:LDAP 認証による IP アクセスの設定 .....	110
ネットワーク構成 .....	110
使用するソフトウェアバージョン .....	111
制限事項とガイドライン .....	111
手順 .....	112
設定の確認 .....	140
<b>透過的 DNS プロキシの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:透過 DNS プロキシの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	12
<b>コンテキストの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:コンテキストの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	4

手順 .....	4
設定の確認 .....	6
<b>IRF 設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:IRF ファブリックの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	5
<b>ホットバックアップの設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
例:1つの冗長グループによるアクティブ/スタンバイモードでの IRF ホットバックアップシステムの設定	1
ネットワーク構成 .....	1
使用するソフトウェアバージョン .....	2
前提条件 .....	2
手順 .....	3
設定の確認 .....	8
例:2つの冗長グループがあるデュアルアクティブモードでの IRF ホットバックアップシステムの設定	10
ネットワーク構成 .....	10
使用するソフトウェアバージョン .....	11
前提条件 .....	11
手順 .....	12
設定の確認 .....	18
例:アクティブ/スタンバイモードでの VRRP ホットバックアップシステムの設定	19
ネットワーク構成 .....	19
使用するソフトウェアバージョン .....	20
前提条件 .....	21
手順 .....	21
設定の確認 .....	28
例:デュアルアクティブモードでの VRRP ホットバックアップシステムの設定	29
ネットワーク構成 .....	29
使用するソフトウェアバージョン .....	30
前提条件 .....	30
手順 .....	31
設定の確認 .....	36

## ユーザーID の設定例 ..... 2

はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	3
例:RADIUS 認証(RADIUS シングルサインオン)を通過するポータルユーザーのユーザーID の設定	3
ネットワーク構成 .....	3
分析 .....	6
使用するソフトウェアバージョン .....	6
制限事項とガイドライン .....	7
手順 .....	7
デバイス(ファイアウォール)の設定 .....	9
設定の確認 .....	32
例:RADIUS 認証(非 RADIUS シングルサインオン)をパスするポータルユーザーのユーザーID の設定	41
ネットワーク構成 .....	41
分析 .....	43
使用するソフトウェアバージョン .....	43
制限事項とガイドライン .....	44
手順 .....	44
設定の確認 .....	72
構成ファイル .....	76

## SSL 復号化の設定例 ..... 2

はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:SSL 復号化の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	5

## 帯域幅管理の設定例 ..... 2

はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:単一のトラフィックプロファイルの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	4

手順 .....	4
設定の確認 .....	9
例:親/子トラフィックプロファイルの設定 .....	9
ネットワーク構成 .....	9
使用するソフトウェアバージョン .....	10
手順 .....	10
設定の確認 .....	16
例:ユーザーベースのトラフィックプロファイルの設定 .....	17
ネットワーク構成 .....	17
使用するソフトウェアバージョン .....	17
手順 .....	17
設定の確認 .....	25
<b>NAT ヘアピンの設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
例:NAT ヘアピンの設定 .....	1
ネットワーク構成 .....	1
使用するソフトウェアバージョン .....	2
手順 .....	2
設定の確認 .....	4
<b>サーバーロードバランシングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:レイヤー4 サーバーロードバランシングの設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	14
例:レイヤー7 サーバーロードバランシングの設定 .....	18
ネットワーク構成 .....	18
使用するソフトウェアバージョン .....	19
手順 .....	19
設定の確認 .....	31
<b>アウトバウンドリンクロードバランシングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2

例:アウトバウンドリンクロードバランシングの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	13
<b>インバウンドリンクロードバランシングの設定例 .....</b>	<b>15</b>
はじめに .....	15
前提条件 .....	15
例:インバウンドリンクロードバランシングの設定 .....	15
ネットワーク構成 .....	15
使用するソフトウェアバージョン .....	16
制限事項とガイドライン .....	16
手順 .....	16
設定の確認 .....	30
<b>NAT フローロギングの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:NAT フローロギングの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
制限事項とガイドライン .....	3
手順 .....	3
設定の確認 .....	7
<b>サーバー接続検出の設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
例:SCD の構成 .....	1
ネットワーク構成 .....	1
使用するソフトウェアバージョン .....	2
手順 .....	2
設定の確認 .....	5
<b>IP レピュテーションの設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2

例:IP レピュテーションの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	4
<b>NPTv6 の設定例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
例:送信元アドレス変換の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	4
例:宛先アドレス変換の設定 .....	5
ネットワーク構成 .....	5
使用するソフトウェアバージョン .....	5
手順 .....	5
設定の確認 .....	7
<b>レイヤー3 デバイスによる MAC アドレス学習の設定例 .....</b>	<b>1</b>
はじめに .....	1
前提条件 .....	1
例:レイヤー3 デバイスを介した MAC アドレス学習の設定 .....	1
ネットワーク構成 .....	1
使用するソフトウェアバージョン .....	2
手順 .....	2
設定の確認 .....	5
<b>WAF の構成例 .....</b>	<b>2</b>
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:WAF の設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	7

NetShare コントロールの設定例 .....	2
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:NetShare コントロールの設定 .....	2
ネットワーク構成 .....	2
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	5
4G 構成例 .....	2
はじめに .....	2
前提条件 .....	2
制限事項とガイドライン .....	2
例:4G の設定 .....	3
ネットワーク構成 .....	3
使用するソフトウェアバージョン .....	3
手順 .....	3
設定の確認 .....	4

# Web ログインの設定例

## はじめに

次に、Web ログインの設定例を示します。

デバイスはHTTPとHTTPSの両方をサポートしています。どちらかを使用してデバイスのWebインターフェイスにログインできます。

デバイスの出荷時には、HTTPSがイネーブルになっており、次の設定が行われていました。

- ユーザー名 **admin**
- パスワード **admin**
- ユーザーロール **network-admin**
- 管理インターフェイス IP アドレス 192.168.0.1/24

設定を使用して、デバイスのWebインターフェイスにログインできます。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、Web ログイン機能の基本的な知識があることを前提としています。

## 制限事項とガイドライン

Web ログインを設定する場合は、次の制限事項およびガイドラインに従ってください。

- Chrome40 以降、Firefox19 以降、または Internet Explorer9 以降のいずれかの Web ブラウザを使用することをお勧めします。

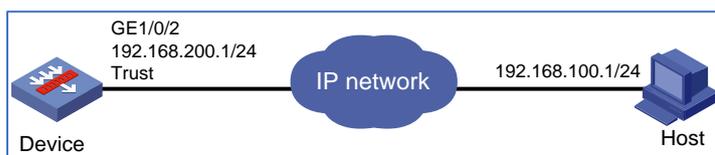
- Web サイトから Cookie を受け入れ、アクティブなスクリプトまたは JavaScript を使用するように Web ブラウザを構成します。Web ブラウザの構成方法の詳細は、Web ブラウザのユーザーガイドを参照してください。
- Internet Explorer を使用するには、次の機能も有効にする必要があります。
- セキュリティで保護されたスクリプトとしてマークされている ActiveX コントロールのスクリプトを実行する
- ActiveX コントロールとプラグインを実行します。
- デバイスソフトウェアのバージョン変更後、ブラウザキャッシュをクリアして、Web インターフェイスに正しい情報が表示されるようにします。

## 例:Webログインの設定

### ネットワーク構成

図 1 に示すように、ホストをデバイスに接続します。ホストが非管理インターフェイスを介してデバイスの Web インターフェイスにログインできるようにデバイスを設定します。

図1 ネットワーク図



### 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの Ess9345 で作成および確認されています。

### 手順

工場出荷時のデフォルト設定を使用したログイン

---

❗ **重要:**

デバイスセキュリティのために、出荷時のデフォルトアカウントのパスワードをすぐに変更してください。

---

1. イーサネットケーブルを使用して、ホストをデバイスの管理インターフェイス GE1/0/0 に接続します。
2. ホストに IP アドレス 192.168.0.2/24 を割り当てます。

この IP アドレスは、管理インターフェイス GE1/0/0 と同じサブネットに属しています。ホストとデバイスは互いに到達できます。

3. Web ブラウザを起動し、アドレスバーに https://192.168.0.1 と入力します。

Web インターフェイスのログインページが開きます。

4. ユーザー名 **admin** とパスワード **admin** を入力し、言語を選択して **Login** をクリックします。
5. デバイスセキュリティのために、出荷時のデフォルトアカウントのパスワードをすぐに変更してください。

#### 非管理インターフェイスによる Web ログインの設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

# トップナビゲーションバーで、**network** をクリックします。

# ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

# GE1/0/2 の **edit** アイコンをクリックします。

# 開いたダイアログボックスで、インターフェイスを設定します。

- A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
- B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、192.168.200.1/24 と入力します。

- C) **OK** をクリックします。

2. IPv4 アドレスオブジェクトグループを作成し、グループ内のユーザーが指定したインターフェイスを介してデバイスにアクセスできるようにします。

# トップナビゲーションバーで、**object** をクリックします。

# ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

# **create** をクリックします。

# 開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。

- A) グループ名を入力します。この例では、**obj1** と入力します。
- B) **add** をクリックします。

C) 表示されるダイアログボックスで、**Network segment** オブジェクトを選択し、IPv4 アドレスとマスク 192.168.100.0/24 を入力します。

D) **OK** をクリックします。

図 2 IPv4 アドレスオブジェクトグループの設定

Create IPv4 Address Object Group

Group name: obj1 (1-31 chars)

Description: (1-127 chars)

Security zone: Trust

Type	Content	Excluded addresses	Edit
<input type="checkbox"/> Network segment	192.168.100.0/255.255.255.0		

Page 1 of 1 | Entries per page 25 | Displaying 1 - 1 of 1

OK Cancel

3. ゾーン **trust** からゾーン **local** へのセキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **trust-to-local** を入力します。
- ソースゾーンの **trust** を選択します。
- 宛先ゾーン **Local** を選択します。
- アクション **deny** を選択

- 送信元 IP アドレス **obj1** を選択します。

#OK をクリックします。

図 3 セキュリティポリシーの設定

**Create Security Policy**

Name  \*  Auto naming

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User

Time range

VRF

---

**Content security**

WAF profile

IPS profile

Data filtering profile

File filtering profile

Anti-virus profile

URL filtering profile

OK Cancel

#### 4. Webログインユーザーの設定

#トップナビゲーションバーで、**system** をクリックします。

#ナビゲーションペインで、**Administrators > Administrators** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、Web ログインユーザーを設定します。

- ユーザー名 **user1** を入力します。
- パスワードを入力して確認します。
- ユーザーロール **network-admin** を選択します。
- サービス **HTTPS** を選択します。

#**OK** をクリックします。

図 4 Web ログインユーザーの設定

Create Administrator

Username  \* (1-55 chars)

Password  \* (1-63 chars)

Confirm  \*

User role  \*

User group

Services  Terminal  SSH  HTTPS  FTP  
 Telnet  PAD  HTTP

Max concurrent logins  (1-1024)

FTP directory

[Advanced settings?](#)

OK Cancel

# 設定の確認

1. Web ブラウザを起動し、アドレスバーに **https://192.168.200.1** と入力します。  
Web インターフェイスのログインページが開きます。
2. ユーザー名 **user1** とパスワードを入力し、言語を選択して **Login** をクリックします。  
デバイスの Web インターフェイスが開きます。

# スタティック IP アドレスによるインターネットアクセスの設定例

## はじめに

次に、スタティック IP アドレスを使用してインターネットにアクセスする設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、IP 機能の基本的な知識があることを前提としています。

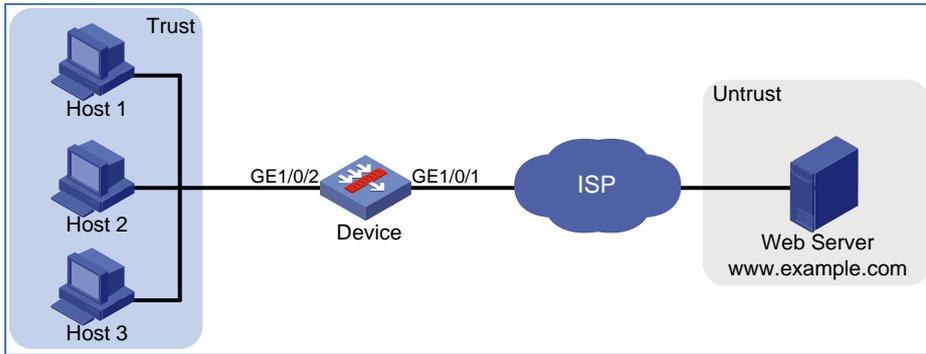
## 例:スタティックIPアドレスによるインターネットアクセスの設定

### ネットワーク構成

図 1 に示すように、ファイアウォールは、内部ネットワークを ISP に接続する出力デバイスとして配置されます。内部ユーザーがインターネットにアクセスできるようにするには、次の作業を実行します。

- プライベート IP アドレスと DNS サーバアドレスをホストに割り当てるように、デバイス上の DHCP サーバーを設定します。
- 内部ユーザーがインターネット上の Web サーバーにアクセスできるようにします。Web サーバーの Web サイトは `www.example.com` です。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

デバイス上でDHCPサーバーを設定する場合は、次の作業を実行します。

- DHCP クライアントが IP アドレスを取得できるようにするために、(DHCP サーバーが属する)セキュリティゾーン **Trust** からローカルへのトラフィックを許可します。
- デバイス上で DNS プロキシをイネーブルにして、DNS サーバーと DNS クライアント間で DNS 要求を伝達します。

## 手順

### デバイスの設定

1. スタティックIPアドレスを設定します。

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**Configuration Wizard > Internet Access** を選択します。

図2 インターネットアクセス設定ページ

Internet Access

Access mode

Routing mode (using the routing function of firewall gateways)

Transparent mode (without changing the original networking)

Configure

#ルーティングモードを選択し、**Configure** をクリックします。

#WAN インターフェイスを設定します(図3を参照)。

図3 WAN インターフェイスコンフィギュレーション

Routing Mode

1 WAN interface configuration

2 LAN interface configuration

3 DMZ interface configuration

4 Security configuration

5 WAN acceleration

6 Flow control

7 Check configuration

Interface: GE1/0/1

Access method:  Specified IP address  DHCP  PPPoE

IP address/subnet mask: 202.0.0.1 / 255.255.255.0

Default gateway: 202.0.0.254

Primary DNS server: 219.141.136.102

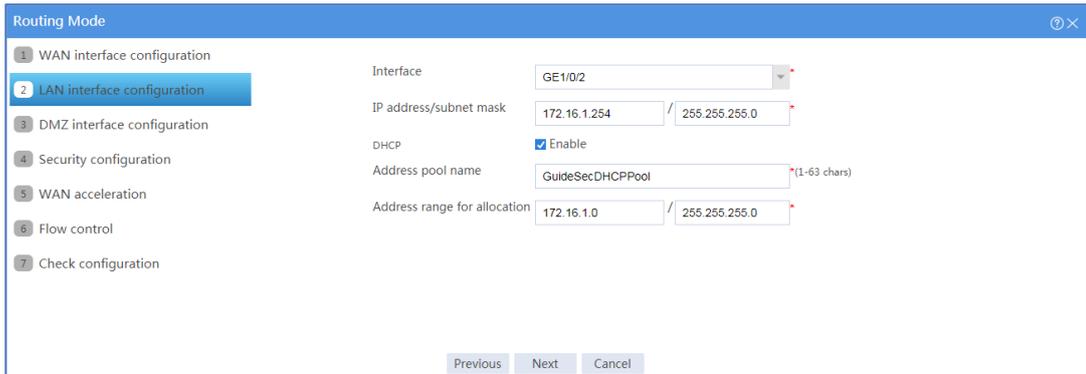
Secondary DNS server: 219.141.140.10

Previous Next Cancel

#**next** をクリックします。

#LAN インターフェイスを設定します (図4を参照)。

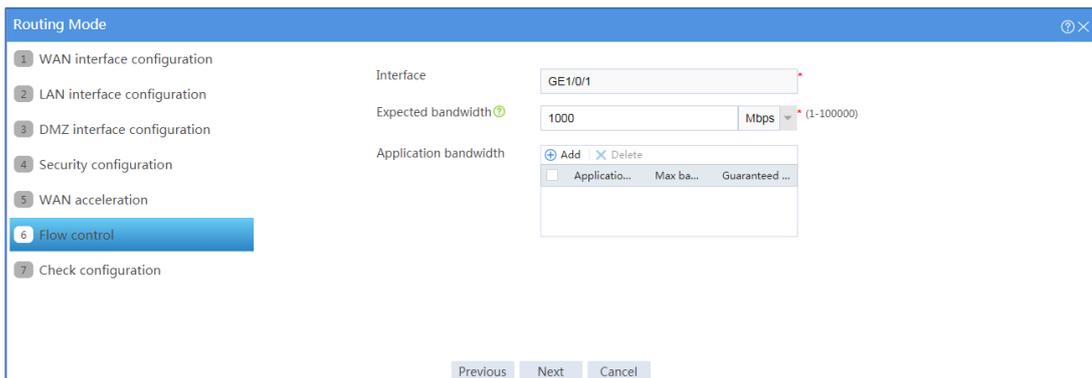
図4 LAN インターフェイスコンフィギュレーション



#Next をクリックします。DMZ インターフェイス、セキュリティ設定、および WAN アクセラレーションの設定をスキップします。

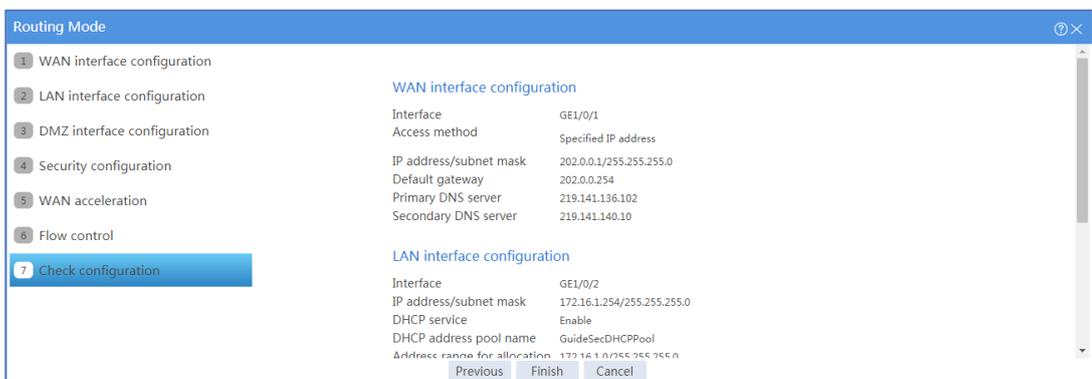
#フロー制御を設定します(図5を参照)。

図5 フロー制御設定



#next をクリックします。次のページが開きます。

図6 構成の確認



#構成を確認し、**Finish** をクリックします。次のページが開きます。

図7 インターフェイスアクセスの設定

**Internet Access**

**Internet access configuration**

<b>Current mode</b>	<b>Routing mode</b>
---------------------	---------------------

**WAN interface configuration**

Interface	GE1/0/1
Access method	Specified IP address
IP address/subnet mask	202.0.0.1/255.255.255.0
Default gateway	202.0.0.254
Primary DNS server	219.141.136.102
Secondary DNS server	219.141.140.10

**LAN interface configuration**

Interface	GE1/0/2
IP address/subnet mask	172.16.1.254/255.255.255.0
DHCP service	Enable
DHCP address pool name	GuideSecDHCPPool
Address range for allocation	172.16.1.0/255.255.255.0

#インターネットアクセスの設定が完了すると、ダイナミック NAT ポリシーも作成されます。NAT ポリシーを表示するには:

- A) トップナビゲーションバーで、**Policies** をクリックします。
- B) ナビゲーションペインで、**NAT > Dynamic NAT > Policy Configuration** を選択します。

図8 発信ダイナミック NAT 設定

Interface	Interface description	ACL	Address gr...	Address gr...	VRF	Translatio...	Reverse NA...	Port preservati...	Quick Setti...	Stat...	Hits	Cou...	Edit
<input checked="" type="checkbox"/>	GE1/0/1	GuideWan Interface	EasyIP		Public netw...	PAT	No	Disable	Yes	Enab...			Disa...

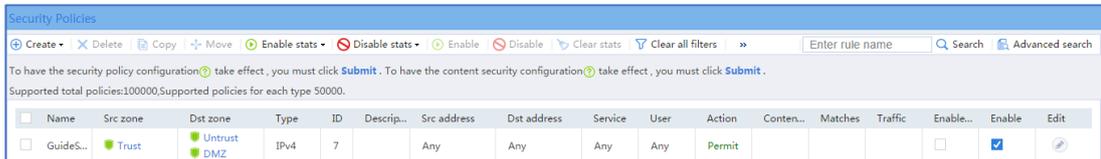
- 2. セキュリティポリシーを設定します。

#スタティック IP アドレスを使用してインターネットアクセスを設定すると、**GuideSecPolicy** という名前のセキュリティポリシーが自動的に作成されます。

#セキュリティポリシーを表示するには:

- A) トップナビゲーションバーで、「ポリシー」をクリックします。
- B) ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

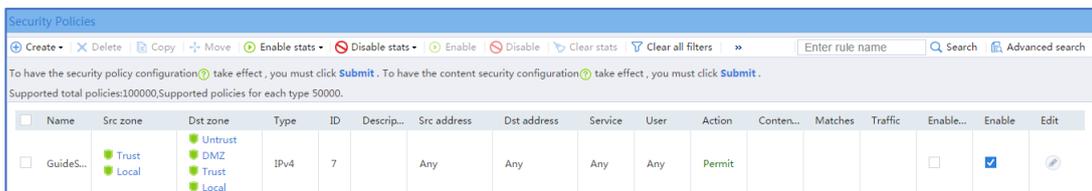
図 9 セキュリティポリシー設定ページ



#このセキュリティポリシーの **Edit** アイコンをクリックします。

#開いたダイアログボックスで、セキュリティゾーン **Local** をソースゾーンに追加し、セキュリティゾーン **Trust** および **Local** を宛先ゾーンに追加します。

図 10 セキュリティポリシーの編集



### 3. DHCPを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**DHCP > DHCP Address Pools** を選択します。

#**Address Pool Options** タブをクリックし、のように設定します。

図 11 アドレスプールオプションの設定

Address Pool

GuideSecDHCPPool ✕ Delete ⊕ Create address pool

Address Allocation | **Address Pool Options** | Assigned Addresses

Lease duration  Infinite  1 days 0 hours 0 minutes 0 seconds

Domain name suffix  (1-50 chars)

Gateways

Gateways	Edit
<input type="checkbox"/> 172.16.1.254	<input type="button" value="✎"/>

DNS servers

DNS servers	Edit
<input type="checkbox"/> 219.141.136.102	<input type="button" value="✎"/>

4. DNSプロキシを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**DNS > Advanced Settings** を選択します。

#DNS プロキシを有効にします。

図 12 DNS プロキシ設定ページ

Advanced Settings

The DNS advanced settings apply to both IPv4 DNS and IPv6 DNS.

**DNS proxy**

Enable

The DNS proxy forwards the request from the DNS client to the designated DNS server, and conveys the reply from the DNS server to the client.

## ホストの構成

#DHCP経由でIPアドレスを取得するようにホストを設定します。

## 設定の確認

1. ホストが取得するIPアドレスを表示します。

```
C:¥>ipconfig /all
```

```
Ethernet adapter Ethernet 1:
```

Connection-specific DNS Suffix.:  
Description.....: Intel(R) 82579LM Gigabit Network Connection  
Physical Address.....: E8-39-35-5C-92-B8  
DHCP Enabled .....: Yes  
Autoconfiguration Enabled.....: Yes  
Link-local IPv6 Address.....: fe80::b8dd:d091:201a:6db2%13(Preferred)  
IPv4 Address.....: 172.16.1.3(Preferred)  
Subnet Mask.....: 255.255.255.0  
Lease Obtained.....: Monday, October 8, 2018 2:44:36 AM  
Lease Expires.....: Tuesday, October 9, 2018 2:44:36 AM  
Default Gateway.....: 172.16.1.254  
DHCP Server.....: 172.16.1.254  
DHCPv6 IAID.....: 384317749  
DHCPv6 Client DUID.....: 00-01-00-01-1F-B4-A3-F5-B8-A3-86-6F-0F-02  
DNS Server.....: 219.141.136.102  
NetBIOS over Tcpi.....: Enabled

2. ホストからパブリックネットワーク上のドメイン名にpingできることを確認します。

C:¥>ping www.example.com

Pinging www.example.com [192.168.100.201] with 32 bytes of data:

Reply from 192.168.100.201: bytes=32 time<1ms TTL=253

Ping statistics for 192.168.100.201:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

# PPPoE によるインターネットアクセスの設定例

## はじめに

次に、PPPoEの例を使用したインターネットアクセスについて説明します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

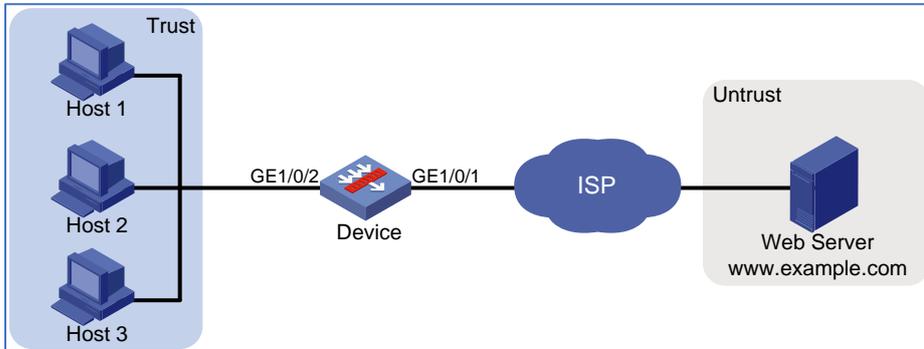
次の情報は、PPPoE の基本的な知識があることを前提としています。

## 例:PPPoEによるインターネットへのアクセス

### ネットワーク構成

図1に示すように、ファイアウォールは企業ネットワークの出力側に配置されています。企業は、pppoeuser1 というユーザー名と 123456 というパスワードを持つ PPPoE アカウントを ISP から適用します。インターネットの www.example.com というアドレスを持つ Web サーバーにアクセスするように PPPoE を設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

デバイスが DHCP サーバーとして動作する場合、DHCP クライアントが IP アドレスを取得するには、DHCP 対応インターフェイスが存在するセキュリティゾーンからローカルセキュリティゾーンへのトラフィックを許可する必要があります。この例では、セキュリティゾーン Trust からセキュリティゾーン Local へのトラフィックを許可する必要があります。

## 手順

### デバイスの設定

1. PPPoEを設定します。

#トップナビゲーションバーで、システムをクリックします。

#ナビゲーションペインで、Configuration Wizard > Internet Access を選択します。に示すページが開きます。

図2 インターネットアクセス



The screenshot shows a configuration window titled "Internet Access". Inside, there is a section labeled "Access mode" with two radio button options: "Routing mode (using the routing function of firewall gateways)" which is selected, and "Transparent mode (without changing the original networking)". Below these options is a "Configure" button.

#Routing mode を選択し、Configure をクリックします。に示すように、WAN インターフェイスパラメータを設定します。

図3 WAN インターフェイスコンフィギュレーション

Routing Mode

1 WAN interface configuration

2 LAN interface configuration

3 DMZ interface configuration

4 Security configuration

5 WAN acceleration

6 Flow control

7 Check configuration

Interface: GE1/0/1

Access method:  Specified IP address  DHCP  PPPoE

Username: pppoeuser1 (1-80 chars)

Password: ..... (1-255 chars)

Online mode:  Permanently online  Auto offline after idle timeout

Automatically obtain IP address

Use specified IP address

IP address/subnet mask: /

Previous Next Cancel

#Next をクリックします。に示すように、LAN インターフェイスパラメータを設定します。

図4 LAN インターフェイスコンフィギュレーション

Routing Mode

1 WAN interface configuration

2 LAN interface configuration

3 DMZ interface configuration

4 Security configuration

5 WAN acceleration

6 Flow control

7 Check configuration

Interface: GE1/0/2

IP address/subnet mask: 172.16.1.254 / 255.255.255.0

DHCP:  Enable

Address pool name: GuideSecDHCPPool (1-63 chars)

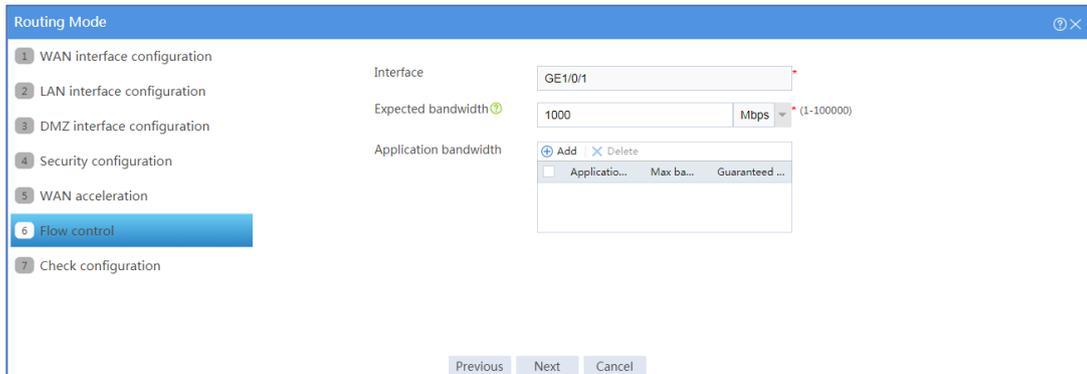
Address range for allocation: 172.16.1.0 / 255.255.255.0

Previous Next Cancel

#Next をクリックします。表示されるページで DMZ インターフェイス、セキュリティ、または WAN アクセラレーションの設定を行わず、Next をクリックしてフロー制御を設定します。

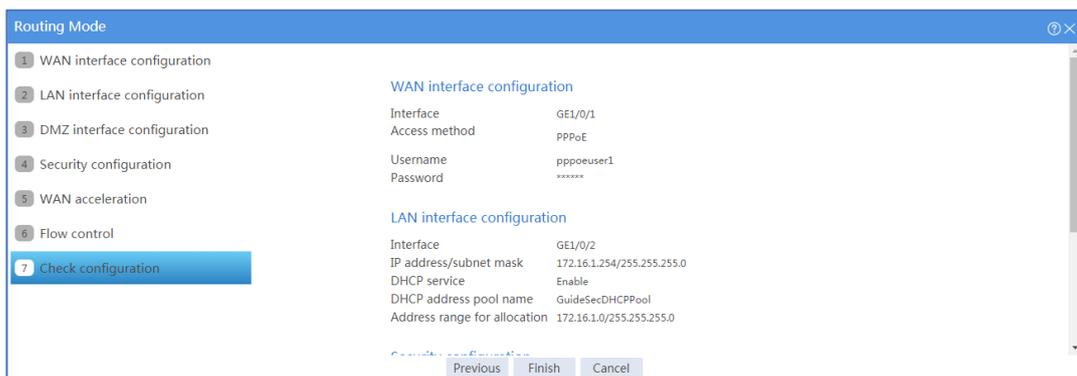
#サービスプロバイダーによって割り当てられた帯域幅に従って、WAN インターフェイスの予想帯域幅を設定します(図5を参照)。

図5 フロー制御



#Next をクリックします。に示す Check configuration ページが開きます。

図6 構成のチェック



#設定が正しいことを確認し、Finish をクリックします。PPPoE の設定情報を示します。

図 7 PPPoE 設定情報

Internet Access

Internet access configuration

<b>Current mode</b>	Routing mode
---------------------	--------------

WAN interface configuration

Interface	GE1/0/1
Access method	PPPoE
Username	pppoeuser1
Password	*****
Online mode	Permanently online

LAN interface configuration

Interface	GE1/0/2
IP address/subnet mask	172.16.1.254/255.255.255.0
DHCP service	Enable
DHCP address pool name	GuideSecDHCPPool
Address range for allocation	172.16.1.0/255.255.255.0

2. セキュリティポリシーを設定します。

PPPoE が設定されると、システムは GuideSecPolicy という名前のセキュリティポリシーを自動的に作成します。

#トップナビゲーションバーで、Policies をクリックします。

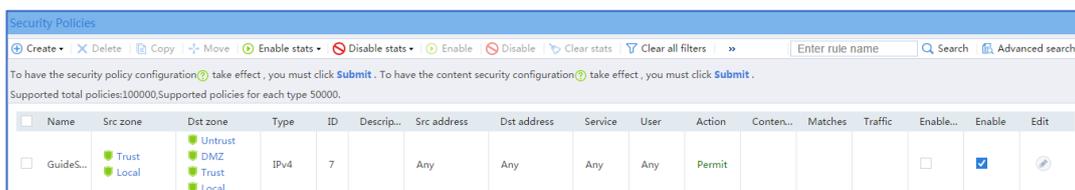
#ナビゲーションペインで、Security Policies > Security Policies を選択します。に示す Security Policies ページが開きます。

図 8 セキュリティポリシー設定ページ

Name	Src zone	Dst zone	Type	ID	Descrip...	Src address	Dst address	Service	User	Action	Conten...	Matches	Traffic	Enable...	Enable	Edit
GuideS...	Trust	Untrust DMZ	IPv4	7		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

#セキュリティポリシー GuideSecPolicy を選択し、Edit 列のアイコンをクリックします。ソースゾーン Local を追加し、宛先ゾーン Trust および Local を追加します(を参照)。

図 9 セキュリティポリシーの追加



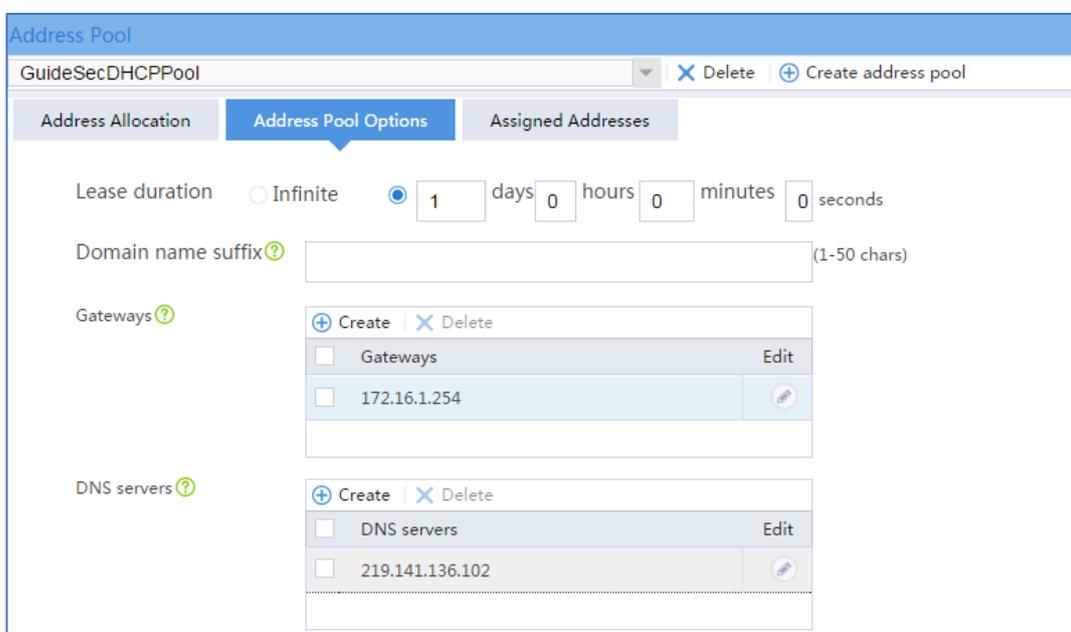
### 3. DHCPを設定します。

#トポロジナビゲーションバーで、ネットワークをクリックします。

#ナビゲーションペインで、DHCP > DHCP Address Pools を選択します。

#Address Pool Options タブをクリックします。パラメータを設定します(図10を参照)。

図 10 アドレスプールオプション

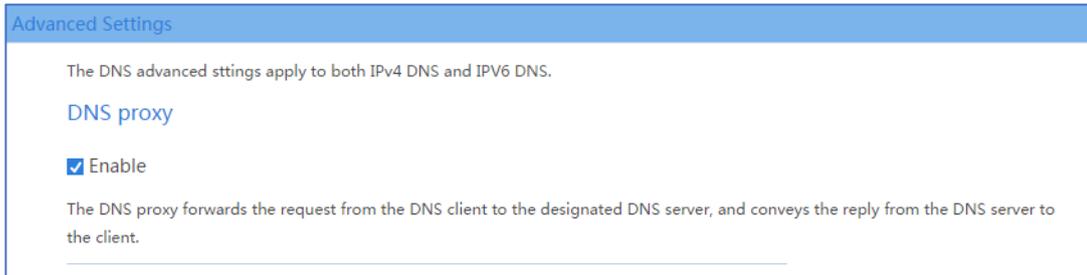


### 4. DNSプロキシを設定します。

#トポロジナビゲーションバーで、ネットワークをクリックします。

#ナビゲーションペインで、DNS > Advanced Settings を選択します。に示すページで、DNS プロキシを有効にします。

図 11 DNS プロキシ



### ホストの構成

#IP アドレスを自動的に取得するようにホストを構成します。

## 設定の確認

1. ホストが取得するアドレス情報を表示します。

```
C:¥>ipconfig /all
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix.....:
Description.....: Intel(R) 82579LM Gigabit Network Connection
Physical Address.....: E8-39-35-5C-92-B8
DHCP Enabled .....: Yes
Autoconfiguration Enabled.....: Yes
Link-local IPv6 address.....: fe80::b8dd:d091:201a:6db2%13(Preferred)
IPv4 Address.....: 172.16.1.3(Preferred)
Subnet Mask.....: 255.255.255.0
Lease Obtained.....: May 25, 2017 14:01:30
Lease Expires.....: May 26, 2017 14:01:30
Default Gateway.....: 172.16.1.254
DHCP Server.....: 172.16.1.254
DHCPv6 IAID.....: 384317749
DHCPv6 Client DUID.....: 00-01-00-01-1F-B4-A3-F5-B8-A3-86-6F-0F-02

DNS Servers.....: 172.16.1.254
NetBIOS over Tcpi.....: Enabled
```

2. ホストがサーバアドレス `www.example.com` に ping できることを確認します。

```
C:¥>ping www.example.com
```

```
Ping www.example.com [192.168.100.201]: 32 data bytes
32 bytes from 192.168.100.201: time<1ms TTL=253
```

```
--- Ping statistics for 192.168.100.201 ---
```

```
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

# ライセンスのアクティベーションとインストールの設定例

## はじめに

ライセンスに、ライセンスのアクティベーションとインストールの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、ライセンス機能についての基本的な知識があることを前提します。

## 例:ライセンス管理の設定

### ネットワーク構成

ライセンスベースの機能を使用するには、ライセンスが必要です。ライセンスベースの機能を使用するには、ライセンスをアクティブにする必要があります。

### 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

---

#### ❗ 重要:

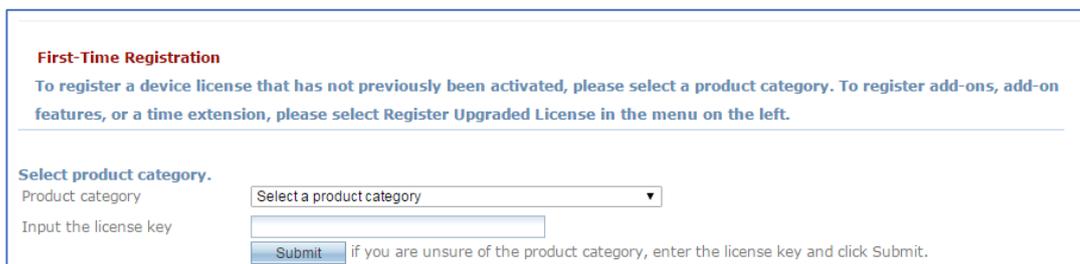
このドキュメントでは、Security\_NG Firewall 製品を例ために、Security\_NG Firewall 製品を例として使用しています。製品カテゴリはデバイスモデルによって異なります。

---

1. h3cのWebサイト([http://www.h3c.com/en/Support/Online\\_Help/License\\_Service/](http://www.h3c.com/en/Support/Online_Help/License_Service/))に

アクセスします。**Register the First Time**を選択します。

図1 初めてライセンスを登録する

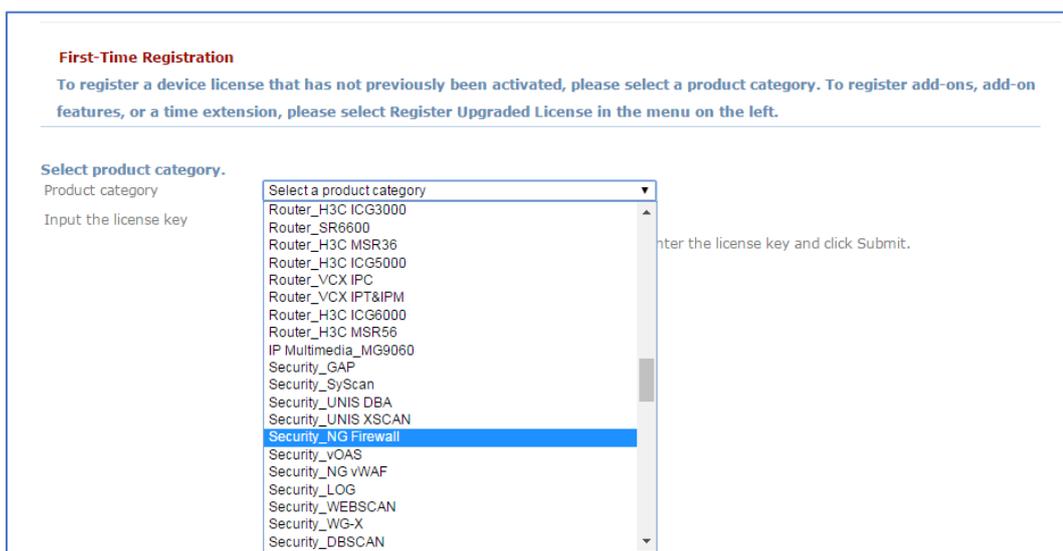


**First-Time Registration**  
To register a device license that has not previously been activated, please select a product category. To register add-ons, add-on features, or a time extension, please select Register Upgraded License in the menu on the left.

Select product category.  
Product category: Select a product category  
Input the license key:   
Submit: if you are unsure of the product category, enter the license key and click Submit.

2. **Product category**のドロップダウンリストから**Security\_NG Firewall**を選択します。

図2 製品カテゴリの選択



**First-Time Registration**  
To register a device license that has not previously been activated, please select a product category. To register add-ons, add-on features, or a time extension, please select Register Upgraded License in the menu on the left.

Select product category.  
Product category: Router\_H3C ICG3000, Router\_SR6600, Router\_H3C MSR36, Router\_H3C ICG5000, Router\_VCX IPC, Router\_VCX IPT&IPM, Router\_H3C ICG6000, Router\_H3C MSR56, IP Multimedia\_MG9060, Security\_GAP, Security\_SyScan, Security\_UNIS DBA, Security\_UNIS XSCAN, **Security\_NG Firewall**, Security\_vOAS, Security\_NG vWAF, Security\_LOG, Security\_WEBSCAN, Security\_WG-X, Security\_DBSCAN  
Input the license key:   
Submit: if you are unsure of the product category, enter the license key and click Submit.

3. ライセンス、デバイス、および連絡先情報を入力し、**I accept all terms of H3C Legal Statement**を選択して**Get activation key or file**をクリックします。フィールドの詳細については、表を参照してください。

図3 情報を入力する

## Register the First Time

Registers licenses for a device that has never been activated.

---

**First-Time Registration**  
 To register a device license that has not previously been activated, please select a product category. To register add-ons, add-on features, or a time extension, please select Register Upgraded License in the menu on the left.

---

**Select product category.**  
 Product category Security\_NG Firewall ▼

**License information**  
 Upload license keys from excel file Browse... Upload [Download the template](#)

Input license keys or select by sales contract  Clear

Continue adding license key

**Device information**  
 Device information file Browse... Upload \*

**Contact Information**

Customer company/organization  \*

Company/Organization  \*

First name  \*

Last name  \*

Phone number  \*

Email address  \*

Zip code

Address

Project name

Verify code  8 5 1 6

I accept all terms of H3C Legal Statement \*

Get activation key or file Cancel

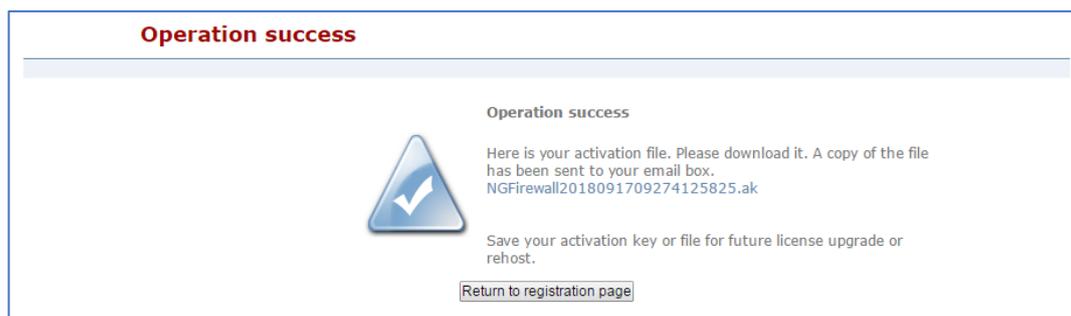
For comments or questions, please contact us.

項目	説明	備考
ライセンス情報	ソフトウェアライセンス証明書のライセンス番号は、2つの方法で指定できます。	必須。
デバイス情報	did 形式のデバイス情報ファイルを選択します。デバイス情報ファイルを取得するには、 <b>System &gt; License Config &gt; Obtain DID file</b> を選択し、OK をクリックします。	必須。
お客様の会社/組織	デバイスを使用する会社または組織の名前を入力します。	必須
会社/組織	会社名または組織名を入力します。	必須
名/姓	名前を入力します。	必須

項目	説明	備考
番号電話番号	電話番号を入力します。	必須
電子メールアドレス	メールアドレスを入力します。 H3Cはアクティベーションファイルのコピーを電子メールボックスに送信し、アクティベーションファイルへのリンクを提供します。	必須
郵便番号	地域の郵便番号を入力します。	選択
住所	住所を入力します。	選択
プロジェクト名	デバイスを使用するプロジェクトの名前を入力します。	選択
コードの確認	テキストボックスの右側のイメージに表示されているとおりにコードを入力します。	必須

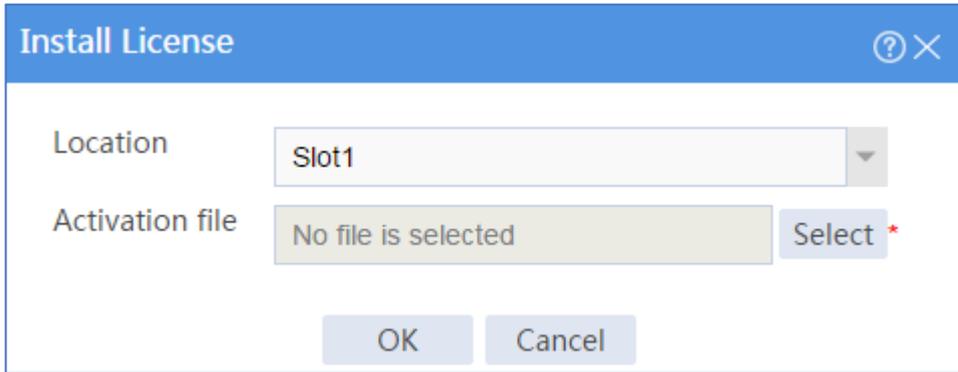
4. 登録成功メッセージが表示されたら、**.ak**リンクをクリックしてアクティベーションファイルをデバイスに保存します。

図4 登録成功メッセージ



5. アクティベーションファイルをインストールします。  
 #トップナビゲーションバーで、**System** をクリックします。  
 #ナビゲーションペインで、**license Config** を選択します。  
 #**install** をクリックします。

#開いたダイアログボックスで、場所として **slot1** を選択し、ローカルに保存したアクティベーションファイルを選択して **OK** をクリックします。この例では、**slot1** を使用して説明します。場所はデバイスタイプによって異なります。



## 設定の確認

ライセンスが正常にインストールされると、ライセンス状態が **In Use** であり、ライセンスマークが **Y** であることが設定ページに表示されます。

# シグニチャライブラリアップデートの設定例

## はじめに

次に、シグニチャライブラリのアップデート設定例を示します。

デバイス上のシグニチャライブラリをアップデートするには、次の方法を使用できます。

- **Automatic scheduled 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。
- **Immediate online update:** デバイスは、した直後に、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のシグニチャライブラリを更新する必要があります。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、シグニチャライブラリのアップグレード機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

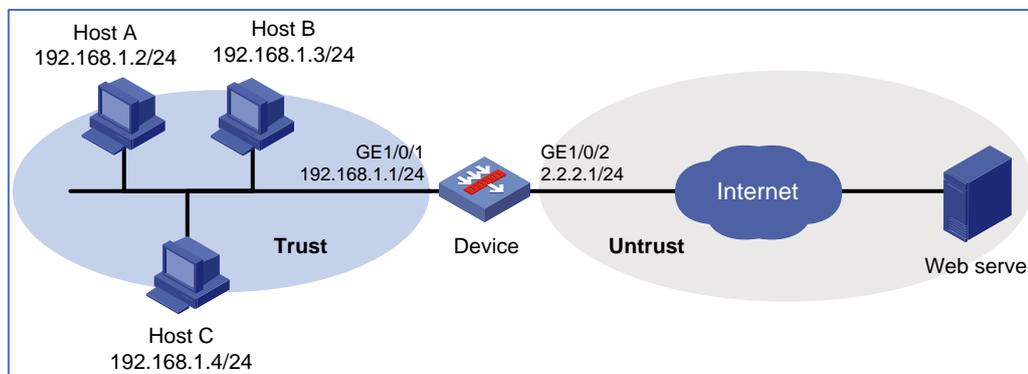
各セキュリティサービスのシグニチャライブラリをデバイス上で実行するには、ライセンスが必要です。ライセンスの期限が切れると、関連するサービスはデバイス上の既存のシグニチャライブラリを使用できますが、ライブラリは更新できません。

# 例:シグニチャライブラリのスケジュールされた自動アップデートの設定

## ネットワーク構成

図1に示すように、信頼セキュリティゾーン内の内部ユーザーは、信頼解除セキュリティゾーン内のインターネットリソースにアクセスできます。毎週土曜日の 3:00:00 に IPS シグニチャライブラリをアップデートするようにデバイスを設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

この機能を設定する前に、次のことを確認してください。

- デバイスは、アップデートサーバーに直接またはプロキシサーバー経由でアクセスできます。
- IP S ライセンスは実行ステータスです。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、ネットワークをクリックします。

#ナビゲーションペインで、Interface Configuration > Interfaces を選択します。

#GE1/0/1 の編集アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- 基本**basic configuration**タブで、**Trust**セキュリティゾーンを選択します。
- **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、192.168.1.1/24と入力します。
- **OK**をクリックします。

#**Untrust** セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 2.2.2.1./24 に設定します。

2. セキュリティゾーン**Trust**および**Local**のセキュリティポリシーを設定し、内部ユーザーがPCを使用してインターネットにアクセスできるようにします(詳細は省略)。
3. セキュリティゾーン**Trust**および**Untrust**のセキュリティポリシーを設定し、内部ユーザーがPCを使用してインターネットにアクセスできるようにします。
4. IP シグニチャライブラリをスケジュールされた時刻に自動的にようにデバイスを設定します。

#トップナビゲーションバーで、**System** 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。

#IPS シグニチャライブラリの **Auto update** チェックボックスをオンにします。

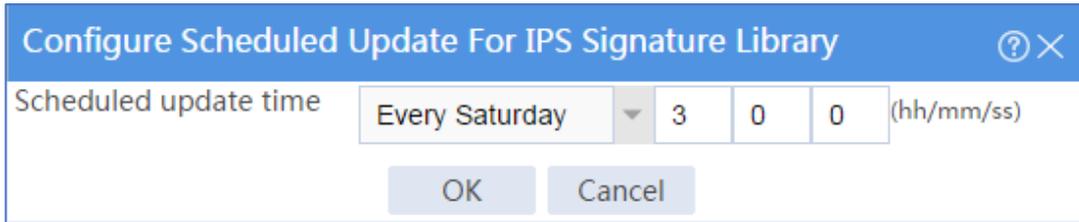
#表示されるダイアログボックスで、毎週土曜日のスケジュールされた更新時刻を 03:00:00 に設定します。

スケジュールされた自動ライブラリ更新は、次の時点の間のランダムな時間に発生します。



- 指定された開始時刻の 1 時間前。
- 指定された開始時刻の 1 時間後。

図 IP S シグニチャライブラリのアップデートのスケジュール設定



#OK をクリックします。

## 設定の確認

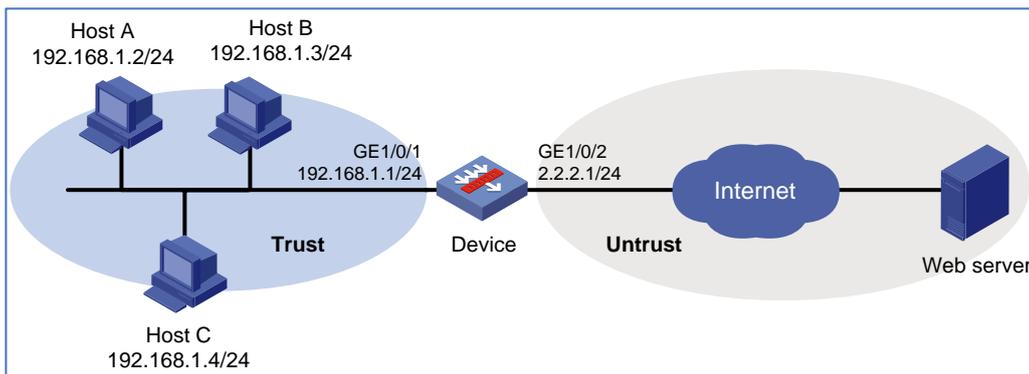
スケジュールされた更新時間が経過したら、シグニチャライブラリの更新リストにアクセスし、IPS シグニチャライブラリが更新されたことを確認します。

## 例:シグニチャライブラリの即時オンラインアップデートの設定

## ネットワーク構成

図1に示すように、信頼セキュリティゾーン内の内部ユーザーは、信頼解除セキュリティゾーン内のインターネットリソースにアクセスできます。IP S シグニチャライブラリをただちに更新して、IPS 機能が最新のシグニチャライブラリを使用して内部ネットワークを保護できるようにします。

図1 ネットワーク図



# 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

この機能を設定する前に、デバイスがアップデートサーバーに直接またはプロキシサーバー経由でアクセスできることを確認してください。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。
  - 基本**basic configuration**タブで、**Trust**セキュリティゾーンを選択します。
  - **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、192.168.1.1/24と入力します。
  - **OK**をクリックします。  
#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 2.1.1.1./24 に設定します。
2. セキュリティゾーン**Trust**および**Local**のセキュリティポリシーを設定し、内部ユーザーがPCを使用してインターネットにアクセスできるようにします(詳細は省略)。
3. セキュリティゾーン**Trust**および**Untrust**のセキュリティポリシーを設定し、内部ユーザーがPCを使用してインターネットにアクセスできるようにします(詳細は省略)。
4. IP シグニチャライブラリをただちに更新します。  
#トップナビゲーションバーで、**System** 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。  
#IPS シグニチャライブラリの **Online update** リンクをクリックします。  
#開いたダイアログボックスで、操作を確認します。

## 設定の確認

シグニチャライブラリのアップデートリストで、IPSシグニチャライブラリがアップデートされているこ

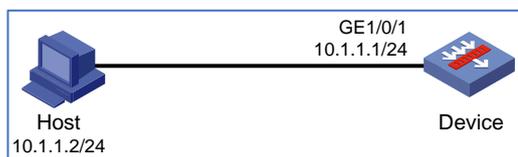
とを確認します。

## 例:ローカルシグニチャファイルを使用したデバイスシグニチャライブラリの更新

### ネットワーク構成

図 4 に示すように、最新の IPS シグニチャファイル V7-IPS-1.0.54.dat がローカルに保存されます。デバイス IPS シグニチャライブラリのアップデートにファイルをロードするには、手動アップデート方式を使用します。

図 4 ネットワーク図



### 使用するソフトウェアバージョン

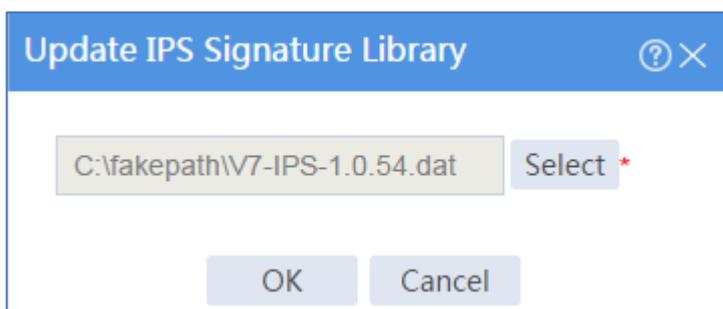
この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、ネットワークをクリックします。
  - #ナビゲーションペインで、Interface Configuration > Interfaces を選択します。
  - #GE1/0/1 の編集アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) 基本**basic configuration**タブで、**Trust**セキュリティゾーンを選択します。
    - B) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。
    - C) **OK**をクリックします。
2. セキュリティゾーンTrustおよびLocalのセキュリティポリシーを設定し、内部ユーザーがPCを使用してインターネットにアクセスできるようにします(詳細は省略)。

- ローカルIPSシグニチャファイルをインポートします。  
#トップナビゲーションバーで、**System** 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。  
#IPS シグニチャライブラリの **Manual update** リンクをクリックします。  
#開いたダイアログボックスで、ローカルに保存されたシグニチャファイル V7-IPS-1.0.54.dat を選択します。

図 5 ローカルに保存された署名ファイルの選択



#OK をクリックします。

## 設定の確認

シグニチャライブラリのアップデートリストで、IPSシグニチャライブラリがアップデートされていることを確認します。

# ソフトウェアアップグレードの例

## はじめに

次に、Web ベースのソフトウェアアップグレードの例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、ソフトウェアアップグレード機能に関する基本的な知識があることを前提としていません。

## 制限事項とガイドライン

デバイスソフトウェアをアップグレードするには、次の制限事項およびガイドラインに従ってください。

- ユーザーへの影響を軽減するには、ユーザートラフィックが少ない場合にソフトウェアをアップグレードします。
- ソフトウェアをアップグレードする前に、現在のソフトウェアイメージをバックアップしてください。
- アップグレード中に、設定端末とデバイス間の接続が閉じていないことを確認してください。
- デバイスの出荷時には、HTTPS がイネーブルになっており、次の設定が行われていました。
  - ユーザー名 **admin**
  - パスワード **admin**
  - ユーザーロール **network-admin**

- 管理インターフェイス IP アドレス **192.168.0.1/24**

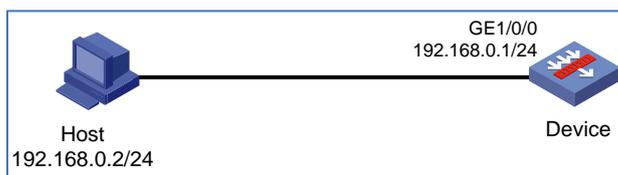
デフォルトでは、設定端末を管理インターフェイスに接続し、その設定を使用してデバイスの Web インターフェイスにログインし、デバイスを管理できます。

## 例:ソフトウェアのアップグレード

### ネットワーク構成

図1に示すように、ホストを使用してデバイスにログインし、デバイスソフトウェアをアップグレードします。

図1ネットワーク図



### 使用するソフトウェアバージョン

この例は、F1060 デバイスの E9345 で作成および確認されたものです。

### 手順

#### ホストの構成

1. イーサネットケーブルを使用して、ホストをデバイスの管理インターフェイス GE1/0/0 に接続します。
2. ホストに IP アドレス 192.168.0.2/24 を割り当てます。
3. この IP アドレスは、管理インターフェイス GE1/0/0 と同じサブネットに属しています。ホストとデバイスは互いに到達できます。
4. Web ブラウザを起動し、アドレスバーに **https://192.168.0.1** と入力します。
5. Web インターフェイスのログインページが開きます。
6. ユーザー名 **admin** とパスワード **admin** を入力し、言語を選択して **Login** をクリックします。

---

❗ **重要:**

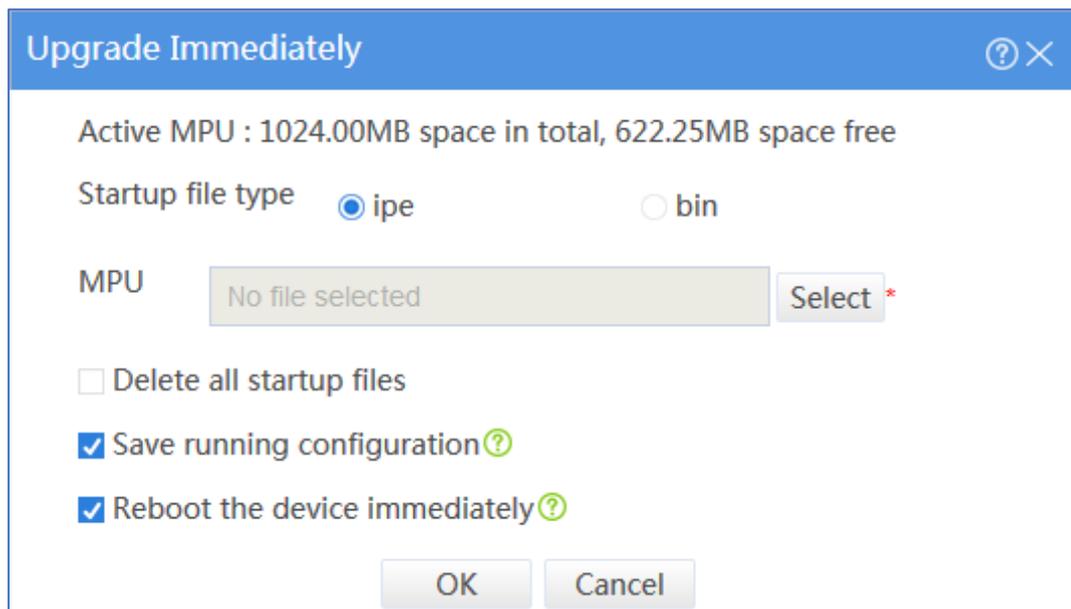
デバイスセキュリティのために、出荷時のデフォルトアカウントのパスワードをすぐに変更してください。

---

### ソフトウェアのアップグレード

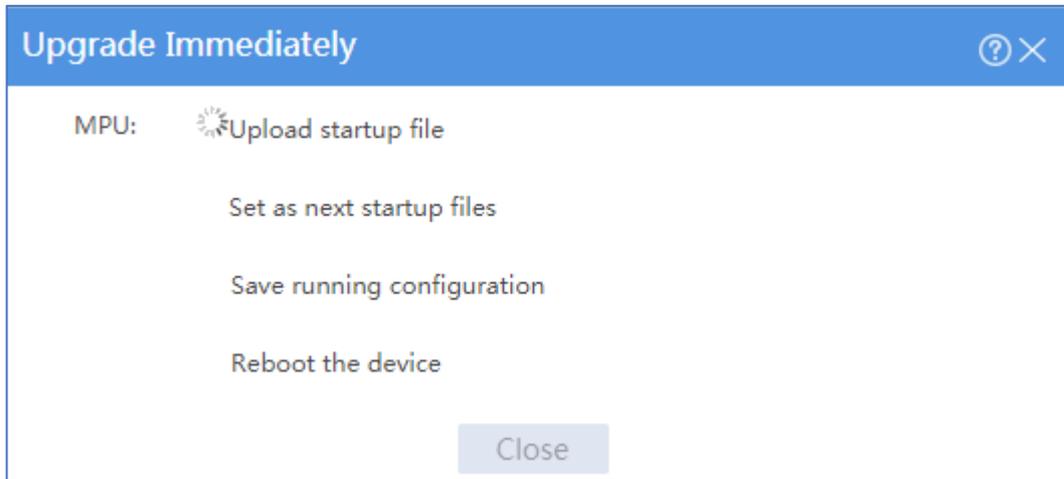
1. 上部のナビゲーションバーで、**System** をクリックします。
2. ナビゲーションペインで、**Upgrade Center > Software Upgrade** を選択します。
3. **Upgrade immediately** をクリックします。
4. 選択をクリックし、**.ipe** アップグレードファイルを選択します。
5. **Reboot the device immediately** オプションが選択されていることを確認します。
6. **OK** をクリックします。

図 2 ソフトウェアのアップグレード



Upgrade Immediately ページに、ソフトウェアアップグレードの進行状況が表示されます(図3を参照)。

図 3 アップグレードの進行状況



## 設定の確認

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**Maintenance > About > Version Info** を選択します。

#バージョン情報を表示します。

# スタティックルーティングの設定例

## はじめに

次に、スタティックルーティングの設定例を示します。

静的ルートは手動で構成されます。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静的ルートを構成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。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、スタティックルーティング機能の基本的な知識があることを前提としています。

## 制限事項とガイドライン

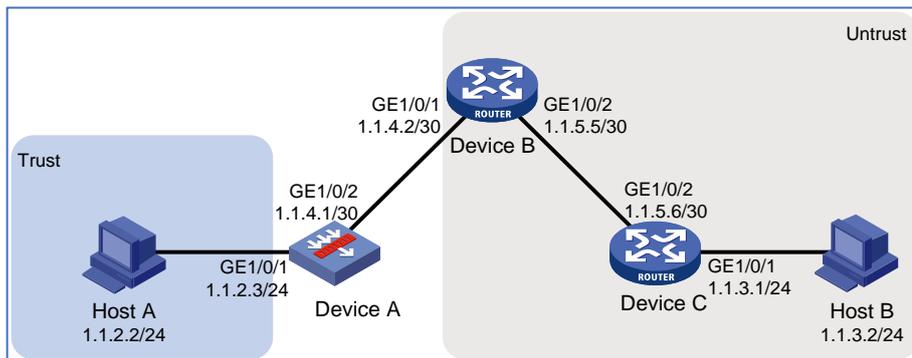
スタティックルートを設定する場合は、ネクストホップのネットワークが到達可能であることを確認してください。また、ネクストホップデバイスがローカルデバイスに到達するための最低1つのルートを持っていることを確認してください。

## 例:スタティックルートの設定

### ネットワーク構成

図1に示すように、ホスト A とホスト B 間の相互接続用に、デバイス A、デバイス B、およびデバイス C にスタティックルートを設定します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060デバイスのE9345で作成および確認されています。

## 手順

### デバイス A の設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/2 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、1.1.4.1/30 と入力します。
    - C) **OK** をクリックします。
  - #GE1/0/2 を設定するのと同じ方法で、GE1/0/1 を **Trust** セキュリティゾーンに追加し、その IP アドレスを 1.1.2.3/24 に設定します。
2. セキュリティポリシーを設定します。
  - #トップナビゲーションバーで、**Policies** をクリックします。
  - #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
  - #**Create > Create a policy** を選択します。
  - #開いたダイアログボックスで、ゾーン **Trust** とゾーン **Untrust** 間のトラフィックを許可するセキュリティポリシーを設定します。

- セキュリティポリシー名 **Trust-Untrust** を入力します。
- ソースゾーンの **Trust** と **Untrust** を選択します。
- ターゲットゾーンの **Trust** と **Untrust** を選択します。
- アクションを **permit** に設定します。

#OK をクリックします。

セキュリティポリシーが表示されます(図2を参照)。

**図2 セキュリティポリシーの作成**

Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matches	Traffic	Enable...	Enable	Edit
Trust-...	Trust Untrust	Untrust Trust	IPv4	5		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

2. スタティックルートを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > Static Routing** を選択します。

#**IPv4 Static Routing** タブで、**Create** をクリックします。

#表示されるダイアログボックスで、IPv4 スタティックルートを設定します(図3を参照)。

図 IPv4 スタティックルートの作成

The screenshot shows a configuration window titled "Create IPv4 Static Route". The fields are as follows:

- VPN instance: Public network
- Destination address: 1.1.3.0
- Mask length: 24
- Next hop:  Next hop VRF instance,  Output interface (Please select...), Next hop address: 1.1.4.2
- Preference: 60
- Route tag: 0
- Description: (Empty)

Buttons: OK, Cancel

#OK をクリックします。

### デバイス B の設定

#ネットワーク1.1.2.0/24(デバイスA)および1.1.3.0/24(デバイスC)に到達する2つのスタティックルートを設定します。設定方法は、デバイスAにスタティックルートを設定する方法と同じです(詳細は省略)。

### デバイス C の設定

#ネットワーク1.1.2.0/24(デバイスA)および1.1.4.0/30(デバイスB)に到達する2つのスタティックルートを設定します。設定方法は、デバイスAにスタティックルートを設定する方法と同じです(詳細は省略)。

## 設定の確認

#ホストAがホストBにpingできることを確認します。

```
C:¥Users¥abc> ping 1.1.3.2
```

Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=255

Ping statistics for 1.1.3.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

この出力は、ホストBがホストAからpingできることを示しています。

# OSPF の設定例

## はじめに

次に、OSPF の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業する場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解していることを確認してください。

次の情報は、OSPF の基本的な知識があることを前提としています。

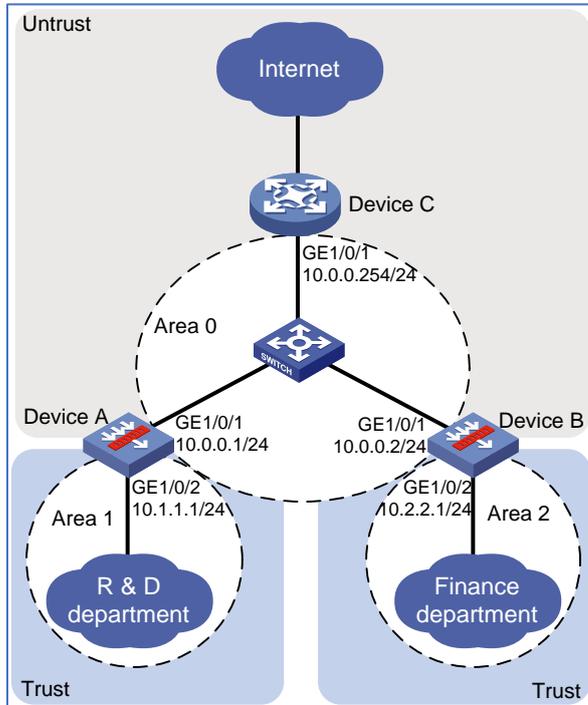
## 例:OSPFの設定

## ネットワーク構成

図1に示すように、デバイス A とデバイス B は、それぞれ研究開発部門と財務部門のファイアウォールです。デバイス C は、インターネットへのゲートウェイとして動作するルータです。

研究開発部門と財務部門が相互にルーティング情報を学習できるように、デバイスにOSPF を設定します。ネクストホップがデバイスCのゲートウェイアドレス200.2.2.254であるデフォルトルートを設定し、デフォルトルートをOSPFに再配布します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

OSPF は、マルチキャストアドレス 224.0.0.5 および 224.0.0.6 を使用してネイバー関係を確立します。ローカルセキュリティゾーンと OSPF インターフェイスを含むセキュリティゾーン間のトラフィックを許可するセキュリティポリシーを設定する必要があります。詳細については、設定手順を参照してください。

## 手順

### デバイス A の設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加し

ます。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。

B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.0.0.1/24 と入力します。

C) **OK** をクリックします。

#GE1/0/ge1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.1.1.1/24 に設定します。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** タブをクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Create > Create a policy** を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **ospf1** を入力します。
- ソースゾーン **Trust**、**Untrust**、および **Local** を選択します。
- **Trust**、**Untrust**、および **Local** の宛先ゾーンを選択します。
- アクション **permit** を選択します。

#**OK** をクリックします。

図 2 セキュリティポリシー

Name	Src zone	Dist zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matches	Traffic	Enable...	Enable	Edit
ospf1	Trust Untrust Local	Trust Untrust Local	IPv4	4		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 3. OSPFを設定します。

#トップナビゲーションバーで、**Network** 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。

図 3 OSPF の設定



#create をクリックします。

#開いたダイアログボックスで、OSPF インスタンスを設定します。

図 4 OSPF インスタンスの作成

Instance name: 1 \* (1-65535)

Router ID: 1.1.1.1 (Dotted decimal notation)

Buttons: OK, Cancel

#OK をクリックします。

図 5 OSPF インスタンス

Instance name	VRF	Router ID	Number of OSPF areas	Number of OSPF interfaces	Number of neighbors	Number of redistributed r...
1	Public network	1.1.1.1	0	0	0	0

#作成された OSPF インスタンスの **Number of OSPF areas** 列で **0** をクリックします。

図6 OSPF エリア

Area ID	Area type	Subnet address	Area interface	Edit
---------	-----------	----------------	----------------	------

#開いた OSPF エリア設定ページで、**Create** をクリックします。

#開いたダイアログボックスで、Area0 を設定します。

図7 エリア0の作成

Create OSPF Area

Instance name: 1 \* (1-65535)

Area ID: 0.0.0.0 \* (Format: Dotted decimal notation.)

Area type: Please select...

Subnet:  Add subnet  Add all subnets

+ Add | X Delete

<input type="checkbox"/>	Subnet address	Subnet mask	Edit
<input type="checkbox"/>	10.0.0.0	255.255.255.0	

Interface: + Add | X Delete

<input type="checkbox"/>	Interface	Interface type	Edit
--------------------------	-----------	----------------	------

OK Cancel

#OK をクリックします。

#OSPF エリア設定ページで、**Create** をクリックします。

#開いたダイアログボックスで、Area1 を設定します。

図8 エリア 1 の作成

Create OSPF Area

Instance name: 1 (1-65535)

Area ID: 0.0.0.1 (Format: Dotted decimal notation.)

Area type: Please select...

Subnet:  Add subnet  Add all subnets

Subnet address	Subnet mask	Edit
<input type="checkbox"/> 10.1.1.0	255.255.255.0	<input type="button" value="Edit"/>

Interface:  Add  Delete

Interface	Interface type	Edit
-----------	----------------	------

OK Cancel

## デバイス B の設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.0.0.2/24と入力します。  
C) **OK** をクリックします。  
#GE1/0/ge1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.2.2.1/24 に設定します。
2. セキュリティポリシーを作成します。  
#トップナビゲーションバーで、**Policies** タブをクリックします。  
#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

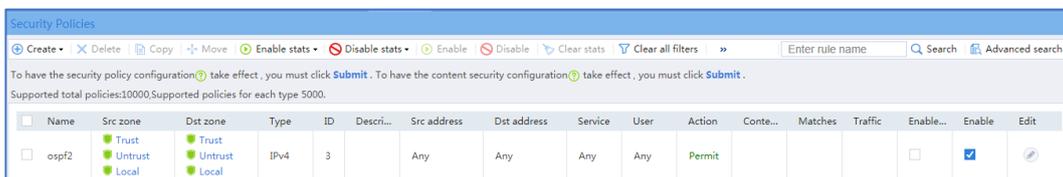
#Create > Create a policy を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **ospf2** を入力します。
- ソースゾーン **Trust**、**Untrust**、および **Local** を選択します。
- **Trust**、**Untrust**、および **Local** の宛先ゾーンを選択します。
- アクション **permit** を選択します。

#OK をクリックします。

図9 セキュリティポリシー



Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matches	Traffic	Enable...	Enable	Edit
ospf2	Trust Untrust Local	Trust Untrust Local	IPv4	3		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

3. OSPFを設定します。

#トップナビゲーションバーで、**Network** 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。

図10 OSPF の設定

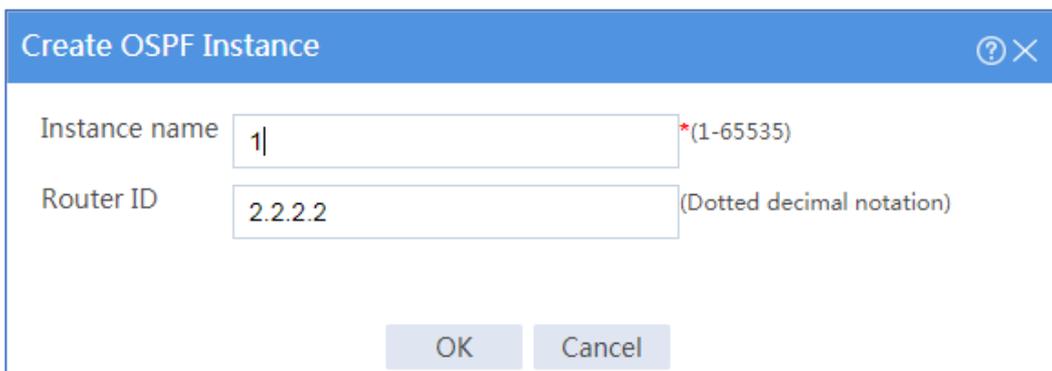


Instance name	VRF	Router ID	Number of OSPF areas	Number of OSPF interfaces	Number of neighbors	Number of redistributed r...
---------------	-----	-----------	----------------------	---------------------------	---------------------	------------------------------

#create をクリックします。

#開いたダイアログボックスで、OSPF インスタンスを設定します。

図11 OSPF インスタンスの作成



Create OSPF Instance

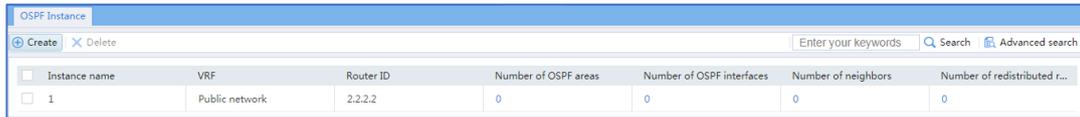
Instance name: 1 \* (1-65535)

Router ID: 2.2.2 (Dotted decimal notation)

OK Cancel

#OK をクリックします。

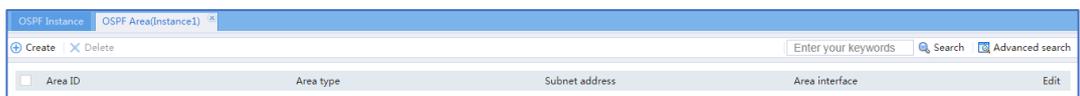
図12 OSPF インスタンス



Instance name	VRF	Router ID	Number of OSPF areas	Number of OSPF interfaces	Number of neighbors	Number of redistributed r...
1	Public network	2.2.2.2	0	0	0	0

#作成された OSPF インスタンスの Number of OSPF areas 列で 0 をクリックします。

図13 OSPF エリア

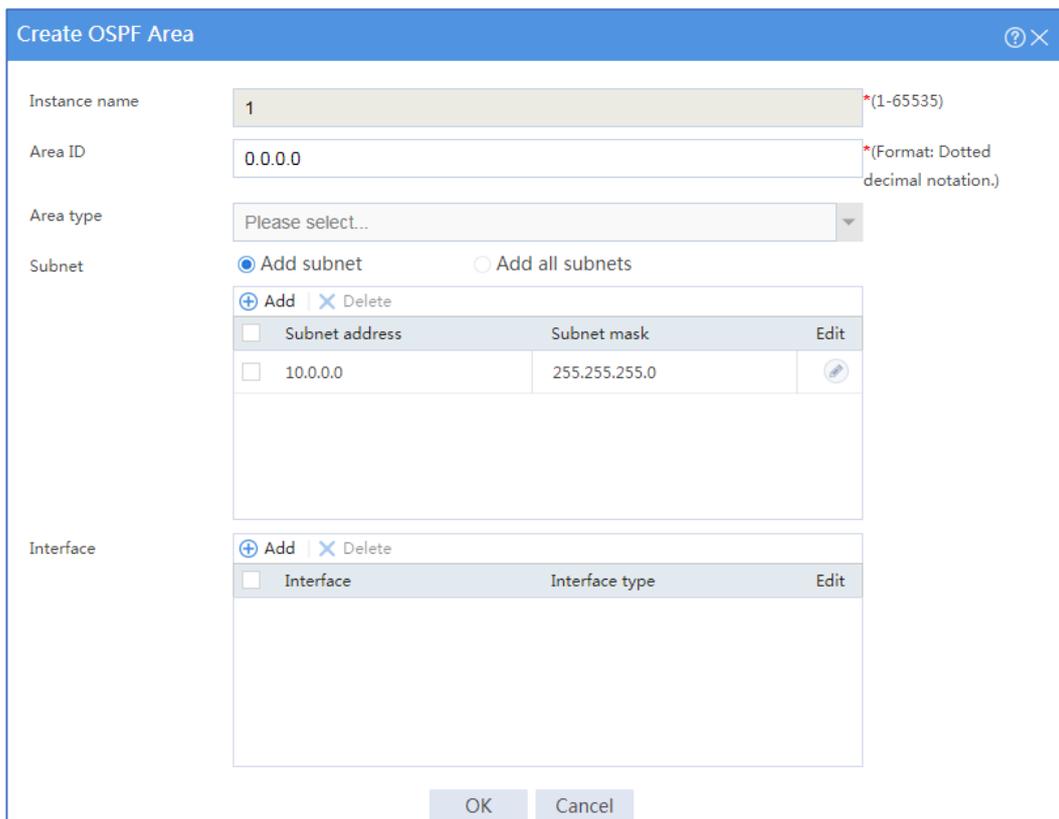


Area ID	Area type	Subnet address	Area interface	Edit
1				

#開いた OSPF エリア設定ページで、Create をクリックします。

#開いたダイアログボックスで、Area0 を設定します。

図14 エリア 0 の作成



Create OSPF Area

Instance name: 1 (1-65535)

Area ID: 0.0.0.0 (Format: Dotted decimal notation.)

Area type: Please select...

Subnet:  Add subnet  Add all subnets

Subnet address	Subnet mask	Edit
10.0.0.0	255.255.255.0	

Interface:

Interface	Interface type	Edit
-----------	----------------	------

OK Cancel

#OK をクリックします。

#OSPF エリア設定ページで、**Create** をクリックします。

#開いたダイアログボックスで、エリア 2 を設定します。

図15 エリア 2 の作成

The screenshot shows a 'Create OSPF Area' dialog box with the following fields and options:

- Instance name:** 1 (with a red asterisk and '(1-65535)' constraint)
- Area ID:** 0.0.0.2 (with a red asterisk and '(Format: Dotted decimal notation.)' constraint)
- Area type:** Please select... (dropdown menu)
- Subnet:**  Add subnet,  Add all subnets
- Subnet table:**

<input type="checkbox"/>	Subnet address	Subnet mask	Edit
<input type="checkbox"/>	10.2.2.0	255.255.255.0	
- Interface:**  Interface,  Interface type, Edit

Buttons: OK, Cancel

#OK をクリックします。

## デバイス C の設定

1. インターフェイスにIPアドレスを割り当てます(詳細は省略)。
2. OSPFを設定します。

#OSPF プロセス 1 を有効にし、ルータ ID に 3.3.3.3 を指定します。

```
<Device C> system-view
```

```
[Device C] ospf 1 router-id 3.3.3.3
```

#Area0 を作成し、Area0 ビューを入力します。

```
[Device C-ospf-1] area 0.0.0.0
```

#ネットワーク 10.0.0.0/24 をアドバタイズします。

```
[Device C-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

```
[Device C-ospf-1-area-0.0.0.0] quit
```

#デフォルトルートが OSPF ルーティングテーブルに再配布されます。

```
<Sysname> system-view
```

```
[Device C-ospf-1] default-route-advertise always
```

```
[Device C-ospf-1] quit
```

#ISP へのデフォルトルートを設定します。

```
[Device C] ip route-static 0.0.0.0 0 200.2.2.254
```

## 設定の確認

1. デバイスAのOSPFルーティングテーブルに関する情報を表示します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > Routing Table** を選択します。

#**IPv4 Routing Table** タブで、OSPF ルーティングテーブル情報を表示します。

図16 デバイス A の OSPF ルーティングテーブル

Destination address	Mask length	Protocol	Preference	Next
0.0.0.0	0	Static	60	192.1
0.0.0.0	32	Direct	0	127.0
127.0.0.0	8	Direct	0	127.0
127.0.0.0	32	Direct	0	127.0
127.0.0.1	32	Direct	0	127.0
127.255.255.255	32	Direct	0	127.0
192.168.100.0	24	Direct	0	192.1
192.168.100.0	32	Direct	0	192.1
192.168.100.80	32	Direct	0	127.0
192.168.100.255	32	Direct	0	192.1
224.0.0.0	4	Direct	0	0.0.0
224.0.0.0	24	Direct	0	0.0.0
255.255.255.255	32	Direct	0	127.0

2. デバイスBのOSPFルーティングテーブルに関する情報を表示します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > Routing Table** を選択します。

#**IPv4 Routing Table** タブで、OSPF ルーティングテーブル情報を表示します。

図17 デバイス B の OSPF ルーティングテーブル

Destination address	Mask length	Protocol	Preference	Next
0.0.0.0	0	Static	60	192.1
0.0.0.0	32	Direct	0	127.0
127.0.0.0	8	Direct	0	127.0
127.0.0.0	32	Direct	0	127.0
127.0.0.1	32	Direct	0	127.0
127.255.255.255	32	Direct	0	127.0
192.168.100.0	24	Direct	0	192.1
192.168.100.0	32	Direct	0	192.1
192.168.100.80	32	Direct	0	127.0
192.168.100.255	32	Direct	0	192.1
224.0.0.0	4	Direct	0	0.0.0.
224.0.0.0	24	Direct	0	0.0.0.
255.255.255.255	32	Direct	0	127.0

3. デバイスAがISPIにpingできることを確認します。

<Device A> ping -a 10.1.1.1 200.2.2.254

```
Ping 200.2.2.254 (200.2.2.254) from 10.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.423 ms
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.222 ms
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.173 ms
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.170 ms
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.167 ms
```

--- Ping statistics for 200.2.2.254 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss  
 round-trip min/avg/max/std-dev = 0.167/0.231/0.423/0.098 ms

この出力は、ISP が ping 可能であることを示しています。

4. デバイスBがISPIにpingできることを確認します。

<Device B> ping -a 10.0.0.2 200.2.2.254

```
Ping 200.2.2.254 (200.2.2.254) from 10.0.0.2: 56 data bytes, press CTRL_C to break
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.437 ms
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.209 ms
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.194 ms
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.174 ms
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.179 ms
```

--- Ping statistics for 200.2.2.254 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss  
 round-trip min/avg/max/std-dev = 0.174/0.239/0.437/0.100 ms

この出力は、ISP が ping 可能であることを示しています。

# BGP の設定例

## はじめに

次に、BGP の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

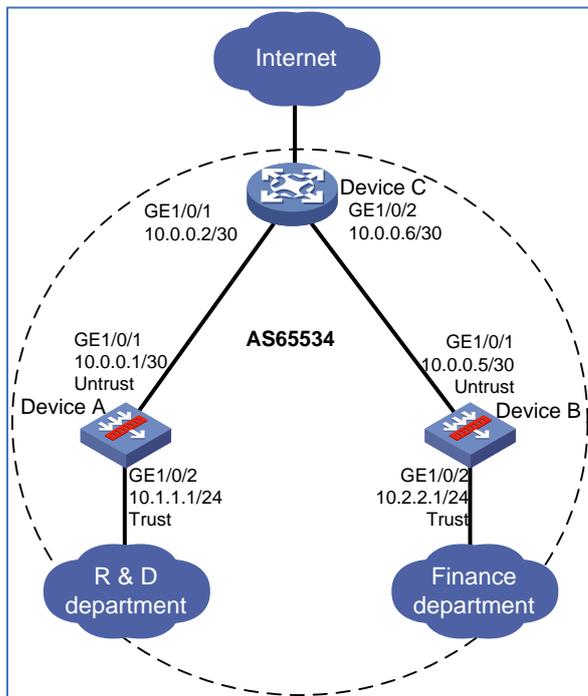
次の情報は、BGP に関する基本的な知識があることを前提としています。

## 例:BGPの設定

## ネットワーク構成

図1に示すように、デバイス A とデバイス B は、それぞれ研究開発部門と財務部門のファイアウォールです。デバイス C は、インターネットへのゲートウェイとして動作するルータです。研究開発部門と財務部門が相互にルーティング情報を学習できるように、デバイスにBGPを設定します。ネクストホップがデバイスCのゲートウェイアドレス200.2.2.254であるデフォルトルートを設定し、デフォルトルートをBGPに再配布します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

BGP は TCP(ポート番号 179)を使用してピア関係を確立します。ローカルセキュリティゾーンと BGP インターフェイスを含むセキュリティゾーン間のトラフィックを許可するセキュリティポリシーを設定する必要があります。詳細については、設定手順を参照してください。

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には、import-route コマンドとともに default-route imported コマンドを使用する必要があります。

## 手順

### デバイス A の設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加し

ます。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。

B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.0.0.1/30と入力します。

C) **OK** をクリックします。

#GE1/0/ge1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.1.1.1/24 に設定します。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

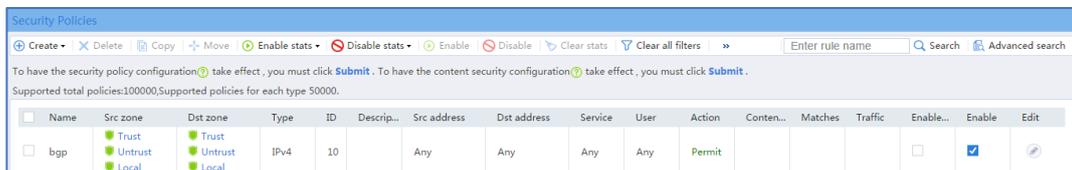
#**Create > Create a policy** を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **bgp** を入力します。
- ソースゾーン **Trust**、**Untrust**、および **Local** を選択します。
- **Trust**、**Untrust**、および **Local** の宛先ゾーンを選択します。
- アクション **permit** を選択します。

#**OK** をクリックします。

### 図2 セキュリティポリシー。



Name	Src zone	Dst zone	Type	ID	Descrip...	Src address	Dst address	Service	User	Action	Conten...	Matches	Traffic	Enable...	Enable	Edit
bgp	Trust Untrust Local	Trust Untrust Local	IPv4	10		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 3. 基礎となるルーティングプロトコルを構成します。この例では、RIPを構成します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > RIP** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、RIP インスタンスを設定します。

図3 RIPインスタンス

Instance ID	VRF	Network address	Protocol	Redistributed routes Instance ID	Interface name	Edit
1	Public network	10.0.0.0 / 255.255.255.0				

4. BGPを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > BGP** を選択します。

#**Enable BGP** を選択し、AS 番号 **65534** を入力して **Apply** をクリックします。

図4 BGPの設定

**BGP Configuration**

**BGP status**

Enable BGP

AS number  \*(1-4294967295)

**Apply**

#**BGP Address Family** タブでアドレスファミリーを選択し、**Apply** をクリックします。

図5 BGPアドレスファミリーの選択

**BGP Configuration**

BGP status

Enable BGP

AS number  \*(1-4294967295)

**Apply**

**BGP Address Family** | BGP Peer | BGP Network | BGP Route Redistribution

IPv4 unicast       IPv4 multicast       IPv6 unicast       IPv6 multicast

MDT       VPNv4       VPNv6       L2VPN

**Apply**

#**BGP Peer** タブで、**Create** をクリックします。

#開いたダイアログボックスで BGP ピアを指定し、**OK** をクリックします。

図6 BGPピアの指定

Create BGP Peer

Peer IP address: 10.0.0.2 \*

AS number: 65534 \*(1-4294967295)

IPv4 unicast:

OK Cancel

#上記の2つの手順を繰り返して、別のBGPピアを指定します。

図7 別のBGPピアの指定

Create BGP Peer

Peer IP address: 10.0.0.5 \*

AS number: 65534 \*(1-4294967295)

IPv4 unicast:

OK Cancel

図8 BGPピア

Peer IP address	AS number	Status	IPv4 unicast	Edit
<input type="checkbox"/> 10.0.0.2	65534	Connect	Enabled	
<input type="checkbox"/> 10.0.0.5	65534	Idle	Enabled	

#**BGP Network** タブで、**Create** をクリックします。

#表示されるダイアログボックスで、指定したアドレスファミリーに対してアドバタイズするネットワークを指定し、**OK** をクリックします。

図9 BGPネットワークアドバタイズメント

Create BGP Network

This function enables BGP to advertise networks in the specified BGP address families.

Address family: IPv4 unicast \*

IP address: 10.1.1.0 \*

Mask/Prefix length: 24 \*(1-32)

OK Cancel

図10 BGPネットワークアドバタイズメント

IP address	Mask/Prefix length	Address family	Edit
10.1.1.0	24	IPv4 unicast	

## デバイス B の設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.0.0.5/30と入力します。  
C) **OK** をクリックします。  
#GE1/0/ge1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.2.2.1/24 に設定します。
2. セキュリティポリシーを作成します。  
#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

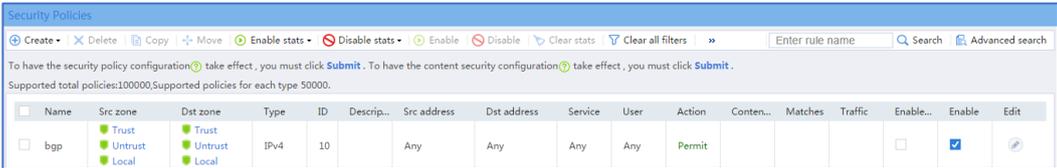
#**Create > Create a policy** を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **bgp** を入力します。
- ソースゾーン **Trust**、**Untrust**、および **Local** を選択します。
- Trust、Untrust、および Local の宛先ゾーンを選択します。
- アクション **permit** を選択します。

#**OK** をクリックします。

図11 セキュリティポリシー



Name	Src zone	Dst zone	Type	ID	Descrip...	Src address	Dst address	Service	User	Action	Conten...	Matches	Traffic	Enable...	Enable	Edit
bgp	Trust Untrust Local	Trust Untrust Local	IPv4	10		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

### 3. 基礎となるルーティングプロトコルを構成します。この例では、RIPを構成します。

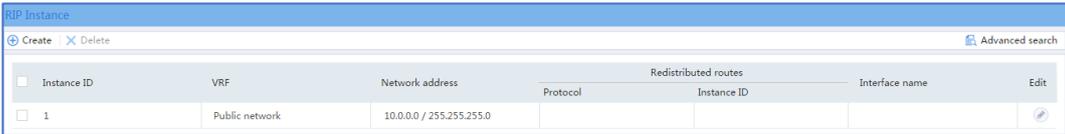
#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > RIP** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、RIP インスタンスを設定します。

図12 RIPインスタンス



Instance ID	VRF	Network address	Protocol	Redistributed routes Instance ID	Interface name	Edit
1	Public network	10.0.0.0 / 255.255.255.0				

### 4. BGPを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > BGP** を選択します。

#**Enable BGP** を選択し、AS 番号 **65534** を入力して **Apply** をクリックします。

図13 BGPの設定

BGP Configuration

BGP status

Enable BGP

AS number  \*(1-4294967295)

Apply

#BGP Address Family タブでアドレスファミリーを選択し、Apply をクリックします。

図14 BGPアドレスファミリーの選択

BGP Configuration

BGP status

Enable BGP

AS number  \*(1-4294967295)

Apply

BGP Address Family | BGP Peer | BGP Network | BGP Route Redistribution

IPv4 unicast  IPv4 multicast  IPv6 unicast  IPv6 multicast

MDT  VPNv4  VPNv6  L2VPN

Apply

#BGP Peer タブで、Create をクリックします。

#開いたダイアログボックスで BGP ピアを指定し、OK をクリックします。

図15 BGPピアの指定

Create BGP Peer

Peer IP address  \*

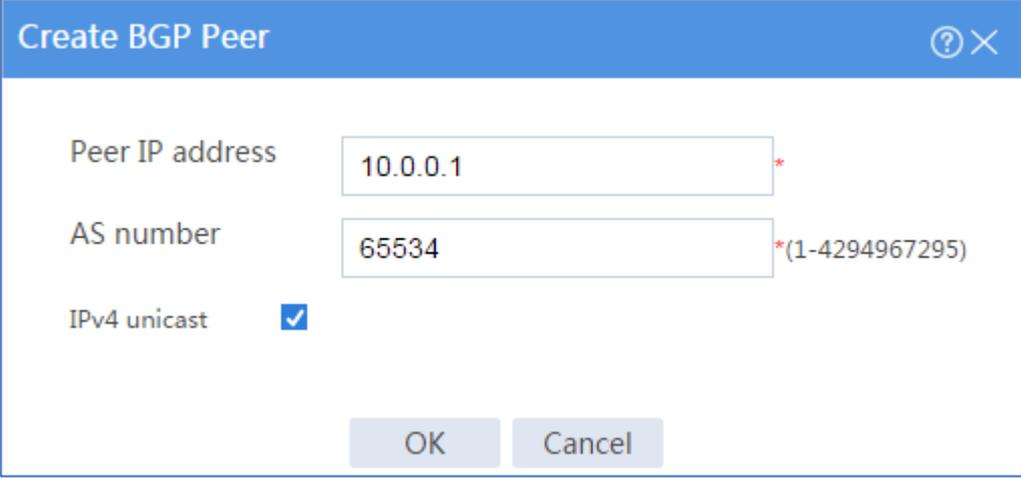
AS number  \*(1-4294967295)

IPv4 unicast

OK Cancel

#上記の 2 つの手順を繰り返して、別の BGP ピアを指定します。

図16 別のBGPピアの指定



The 'Create BGP Peer' dialog box contains the following fields and controls:

- Peer IP address: 10.0.0.1 \*
- AS number: 65534 \*(1-4294967295)
- IPv4 unicast:
- Buttons: OK, Cancel

図17 BGPピア

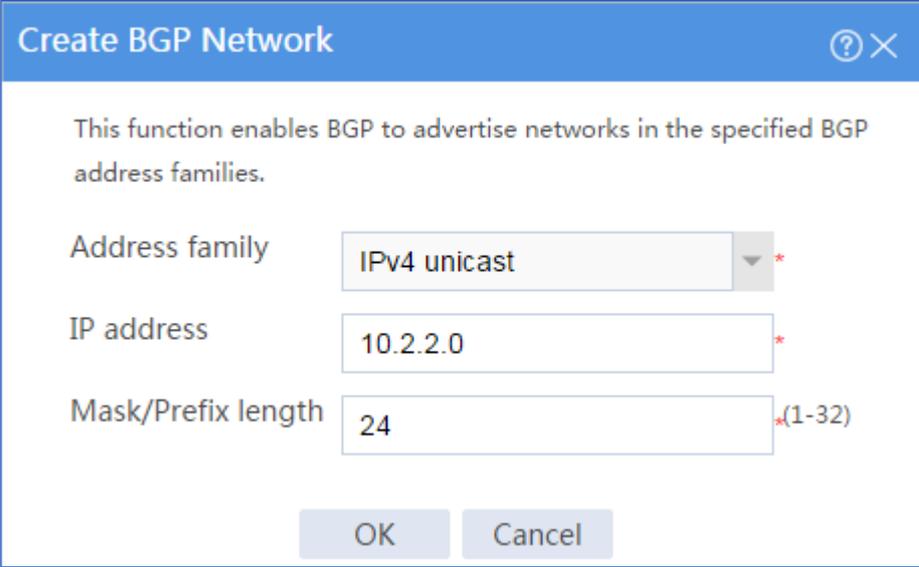


Peer IP address	AS number	Status	IPv4 unicast	Edit
<input type="checkbox"/> 10.0.0.1	65534	Idle	Enabled	
<input type="checkbox"/> 10.0.0.6	65534	Connect	Enabled	

#BGP Network タブで、Create をクリックします。

#表示されるダイアログボックスで、指定したアドレスファミリーに対してアドバタイズするネットワークを指定し、OK をクリックします。

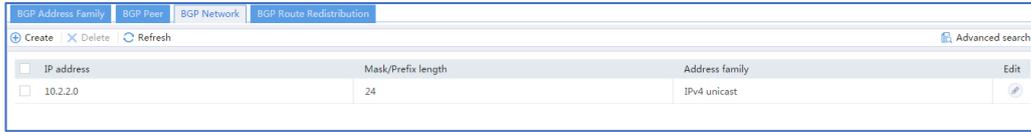
図18 BGPネットワークアドバタイズメント



The 'Create BGP Network' dialog box contains the following fields and controls:

- Text: This function enables BGP to advertise networks in the specified BGP address families.
- Address family: IPv4 unicast \*
- IP address: 10.2.2.0 \*
- Mask/Prefix length: 24 \*(1-32)
- Buttons: OK, Cancel

図19 BGPネットワークアドバタイズメント



IP address	Mask/Prefix length	Address family	Edit
10.2.2.0	24	IPv4 unicast	

## デバイス C の設定

1. インターフェイスにIPアドレスを割り当てます(詳細は省略)。
2. 基礎となるルーティングプロトコルを構成します。この例では、RIPを構成します。

```
<Device C> system-view  
[Device C] rip  
[Device C-rip-1] network 10.0.0.0 0.0.0.255
```

3. 定めます。

#BGP を有効にします。

```
<Device C> system-view  
[Device C] bgp 65534
```

#BGP ピアを指定します。

```
[Device C-bgp-default] peer 10.0.0.1 as 65534  
[Device C-bgp-default] peer 10.0.0.5 as 65534
```

#BGP ピアを有効にします。

```
[Device C-bgp-default] address-family ipv4 unicast  
[Device C-bgp-default-ipv4] peer 10.0.0.1 enable  
[Device C-bgp-default-ipv4] peer 10.0.0.5 enable  
[Device C-bgp-default-ipv4] quit  
[Device C-bgp-default] quit
```

#ISP へのデフォルトルートを設定します。

```
[Device C] ip route-static 0.0.0.0 0 200.2.2.254
```

#デフォルトルートを BGP ルーティングテーブルに再配布します。

```
[Device C] bgp 65534  
[Device C-bgp-default] address-family ipv4 unicast  
[Device C-bgp-default-ipv4] import-route static  
[Device C-bgp-default-ipv4] default-route imported
```

# 設定の確認

1. デバイスAのBGPピアに関する情報を表示します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Routing > BGP** を選択します。  
#**BGP Peer** タブで、BGP ピアが **Established** 状態であることを確認します。

図20 デバイスAのBGPLルーティングテーブル

Peer IP address	AS number	Status	IPv4 unicast	Edit
<input type="checkbox"/> 10.0.0.2	65534	Established	Enabled	
<input type="checkbox"/> 10.0.0.5	65534	Established	Enabled	

BGP ピアが Established 状態であることがわかります。

2. デバイスBのBGPピアに関する情報を表示します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Routing > BGP** を選択します。  
#**BGP Peer** タブで、BGP ピアが **Established** 状態であることを確認します。

図21 デバイスBのBGPLルーティングテーブル

Peer IP address	AS number	Status	IPv4 unicast	Edit
<input type="checkbox"/> 10.0.0.1	65534	Established	Enabled	
<input type="checkbox"/> 10.0.0.6	65534	Established	Enabled	

BGP ピアが Established 状態であることがわかります。

3. デバイスAのBGPLルーティングテーブルに関する情報を表示します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Routing > Routing Table** を選択します。  
#**IPv4 Routing Table** タブで、BGPLルーティングテーブル情報を表示します。

図22 デバイスAのBGPLルーティングテーブル

Destination address	Mask length	Protocol	Preference	Next hop	Output interface
0.0.0.0	0	BGP	255	10.0.0.2	GE1/0/1
10.2.2.0	24	BGP	255	10.0.0.5	GE1/0/1

再配布された BGPLルートとデフォルトルートが表示されます。

4. デバイスBのBGPLルーティングテーブルに関する情報を表示します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Routing > Routing Table** を選択します。

#IPv4Routing Table タブで、BGP ルーティングテーブル情報を表示します。

図23 デバイスBのBGPLルーティングテーブル

Destination address	Mask length	Protocol	Preference	Next hop	Output interface
0.0.0.0	0	BGP	255	10.0.0.6	GE1/0/1
10.1.1.0	24	BGP	255	10.0.0.1	GE1/0/1

再配布された BGP ルートとデフォルトルートが表示されます。

5. デバイスAがISPにpingできることを確認します。

```
<Device A> ping -a 10.1.1.1 200.2.2.254
```

```
Ping 200.2.2.254 (200.2.2.254) from 10.1.1.1: 56 data bytes, press CTRL_C to break  
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.423 ms  
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.222 ms  
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.173 ms  
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.170 ms  
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.167 ms
```

```
--- Ping statistics for 200.2.2.254 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss  
round-trip min/avg/max/std-dev = 0.167/0.231/0.423/0.098 ms
```

この出力は、ISP が ping 可能であることを示しています。

6. デバイスBがISPにpingできることを確認します。

```
<Device B> ping -a 10.0.0.5 200.2.2.254
```

```
Ping 200.2.2.254 (200.2.2.254) from 10.0.0.5: 56 data bytes, press CTRL_C to break  
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.437 ms  
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.209 ms  
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.194 ms  
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.174 ms  
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.179 ms
```

```
--- Ping statistics for 200.2.2.254 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss  
round-trip min/avg/max/std-dev = 0.174/0.239/0.437/0.100 ms
```

この出力は、ISP が ping 可能であることを示しています。

# RIP の設定例

## はじめに

次に、RIP の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、RIP 機能の基本的な知識があることを前提としています。

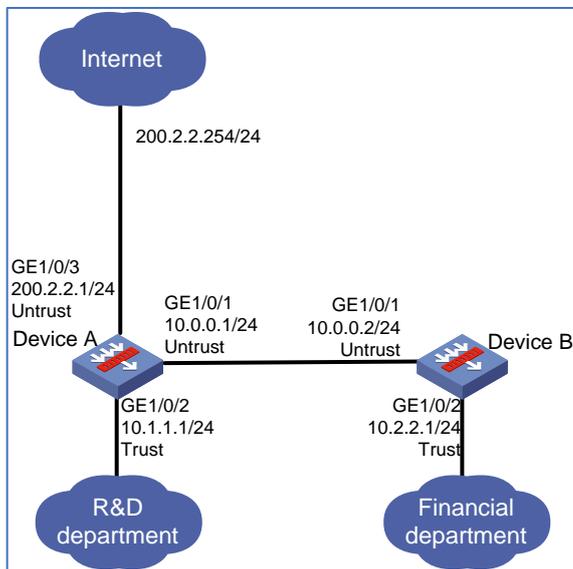
## 例:RIPの設定

### ネットワーク構成

図1に示すように、企業はデバイス A とデバイス B をそれぞれ研究開発部門と財務部門のファイアウォールとして展開します。デバイス A はインターネットへのゲートウェイとしても機能します。

部門が相互にルートを学習するように RIP を設定します。ネクストホップがゲートウェイアドレス 200.2.2.254 を指しているデバイス A にデフォルトルートを設定し、デフォルトルートを RIP に再配布します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

RIP はマルチキャストを介してルーティングテーブル情報を更新します。ローカルセキュリティゾーンとRIP インターフェイスを含むセキュリティゾーン間のトラフィックを許可するセキュリティポリシーを設定する必要があります。詳細については、設定手順を参照してください。

## 手順

### デバイス A の設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。

- A) **Basic Configuration**タブで、**Untrust**セキュリティゾーンを選択します。
- B) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.0.0.1/24と入力します。
- C) **OK**をクリックします。

#GE1/0/ge1/1/2を追加し、GE1/0/1の設定と同じ方法でIPアドレスを10.1.1.1/24に設定します。

#UntrustセキュリティゾーンにGE1/0/3を追加し、GE1/0/1の設定と同じ方法でIPアドレスを200.2.2.1/24に設定します。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies**をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies**を選択します。

#**Create > Create a policy**を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **rip** を入力します。
- ソースゾーン **Trust**、**Untrust**、および **Local** を選択します。
- **Trust**、**Untrust**、および **Local** の宛先ゾーンを選択します。
- アクション **permit** を選択します。

#**OK**をクリックします。作成されたセキュリティポリシーを示します。

図2 セキュリティポリシー

Name	Src zone	Dst zone	Type	ID	Descrip...	Src address	Dst address	Service	User	Action	Conten...	Matches	Traffic	Enable...	Enable	Edit
rip	Trust Untrust Local	Trust Untrust Local	IPv4	14		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 3. ISPへのデフォルトルートを設定します。

#トップナビゲーションバーで、**network**をクリックします。

#ナビゲーションペインで、**Routing > Static Routing**を選択します。

#**create**をクリックします。

#表示されるダイアログボックスで、スタティックルートを設定します(図3を参照)。

図3 スタティックルートの作成

Create IPv4 Static Route

VPN instance: Public network

Destination address: 0.0.0.0

Mask length: 0

Next hop:  Next hop VRF instance  
Public network  
 Output interface  
Next hop address: 200.2.2.254

Preference: 60

Route tag: 0

Description: (1-60 chars)

OK Cancel

#OK をクリックします。

4. RIPを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > RIP** を選択します。RIP 設定ページが開きます(図4を参照)。

図4 RIP設定ページ

Instance ID	VRF	Network address	Protocol	Redistributed routes Instance ID	Interface name	Edit
-------------	-----	-----------------	----------	-------------------------------------	----------------	------

#create をクリックします。

#表示されるダイアログボックスで、RIP インスタンスを設定します(図5を参照)。設定済みスタティックルートおよび研究開発部門の直接ネットワークを再配布ルートとして追加します。

図5 RIPインスタンスの作成

**Create RIP Instance**

Instance ID: 1 \*(1-65535)

VRF: Public network

Networks:  Advertise specified networks  Advertise all networks

Network address      Mask      Edit

<input type="checkbox"/>	10.0.0.0	255.255.255.0	
--------------------------	----------	---------------	--

Redistributed routes:  Protocol      Instance ID      Edit

<input type="checkbox"/>	Direct		
<input type="checkbox"/>	Static		

Interface:  Interface name      Edit

OK      Cancel

#OK をクリックします。RIP インスタンスが作成されます(を参照)。

図6 RIPインスタンス

Instance ID	VRF	Network address	Redistributed routes		Interface name	Edit
			Protocol	Instance ID		
<input type="checkbox"/> 1	Public network	10.0.0.0 / 255.255.255.0	Direct Static			

### デバイス B の設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **Basic Configuration**タブで、**Untrust**セキュリティゾーンを選択します。

B) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.0.0.2/24と入力します。

C) **OK**をクリックします。

#GE1/0/ge1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.2.2.1/24 に設定します。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

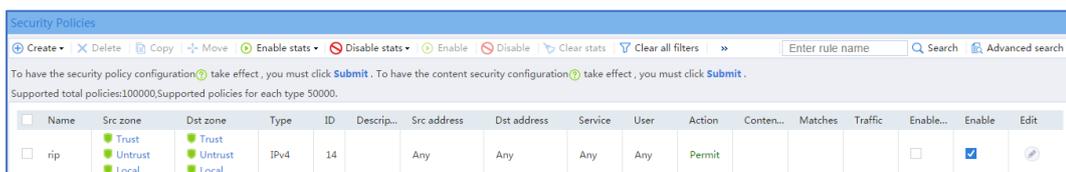
#**Create > Create a policy** を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **rip** を入力します。
- ソースゾーン **Trust**、**Untrust**、および **Local** を選択します。
- **Trust**、**Untrust**、および **Local** の宛先ゾーンを選択します。
- アクション **permit** を選択します。

#**OK** をクリックします。セキュリティポリシーが作成されます(図7を参照)。

図7 セキュリティポリシー



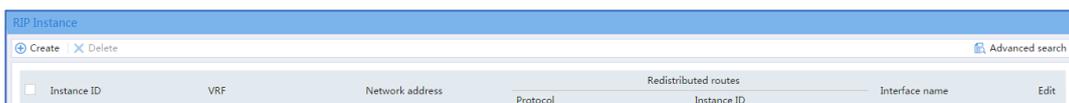
Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conten...	Matches	Traffic	Enable...	Enable	Edit
rip	Trust Untrust Local	Trust Untrust Local	IPv4	14		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 3. RIPを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > RIP** を選択します。RIP 設定ページが開きます(を参照)。

図8 RIP設定ページ



Instance ID	VRF	Network address	Protocol	Redistributed routes Instance ID	Interface name	Edit

#**create** をクリックします。

#表示されるダイアログボックスで、RIP インスタンスを設定します(を参照)。再配布ルートとして財務部門の直接ネットワークを追加します。

図9 RIPインスタンスの作成

Instance ID: 1 \*(1-65535)

VRF: Public network

Networks:  Advertise specified networks  Advertise all networks

<input type="checkbox"/>	Network address	Mask	Edit
<input type="checkbox"/>	10.0.0.0	255.255.255.0	

Redistributed routes:  Direct

<input type="checkbox"/>	Interface name	Edit
--------------------------	----------------	------

OK Cancel

#OK をクリックします。RIP インスタンスが作成されます(図10を参照)。

図10 RIPインスタンス

<input type="checkbox"/>	Instance ID	VRF	Network address	Protocol	Redistributed routes Instance ID	Interface name	Edit
<input type="checkbox"/>	1	Public network	10.0.0.0 / 255.255.255.0	Direct			

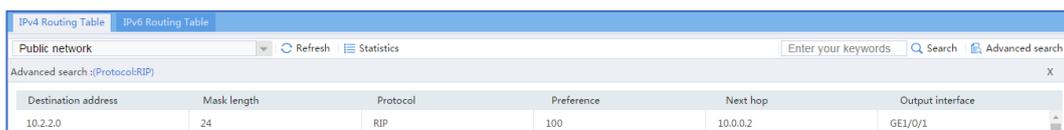
# 設定の確認

1. デバイスAのRIPルーティングテーブルを表示します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > Routing Table** を選択します。に示すように、ルーティングテーブルが表示されます。

図11 デバイスAのRIPルーティングテーブルの表示



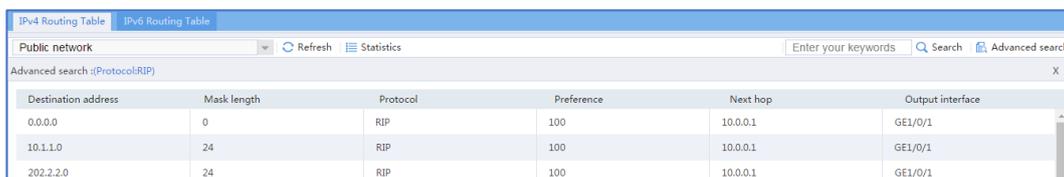
Destination address	Mask length	Protocol	Preference	Next hop	Output interface
10.2.2.0	24	RIP	100	10.0.0.2	GE1/0/1

2. デバイスBのRIPルーティングテーブルを表示します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > Routing Table** を選択します。に示すように、ルーティングテーブルが表示されます。

図12 デバイスBのRIPルーティングテーブルの表示



Destination address	Mask length	Protocol	Preference	Next hop	Output interface
0.0.0.0	0	RIP	100	10.0.0.1	GE1/0/1
10.1.1.0	24	RIP	100	10.0.0.1	GE1/0/1
202.2.2.0	24	RIP	100	10.0.0.1	GE1/0/1

3. デバイスAのISPのゲートウェイアドレス200.2.2.254に対してpingを実行します。

```
<Device A> ping -a 10.1.1.1 200.2.2.254
```

```
Ping 200.2.2.254 (200.2.2.254) from 10.1.1.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.423 ms
```

```
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.222 ms
```

```
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.173 ms
```

```
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.170 ms
```

```
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.167 ms
```

```
--- Ping statistics for 200.2.2.254 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 0.167/0.231/0.423/0.098 ms
```

この出力は、ゲートウェイが ping 可能であることを示しています。

4. デバイスBのISPのゲートウェイアドレス200.2.2.254にpingを実行します。

```
<Device B> ping -a 10.0.0.2 200.2.2.254
Ping 200.2.2.254 (200.2.2.254) from 10.0.0.2: 56 data bytes, press CTRL_C to break
56 bytes from 200.2.2.254: icmp_seq=0 ttl=254 time=0.437 ms
56 bytes from 200.2.2.254: icmp_seq=1 ttl=254 time=0.209 ms
56 bytes from 200.2.2.254: icmp_seq=2 ttl=254 time=0.194 ms
56 bytes from 200.2.2.254: icmp_seq=3 ttl=254 time=0.174 ms
56 bytes from 200.2.2.254: icmp_seq=4 ttl=254 time=0.179 ms

--- Ping statistics for 200.2.2.254 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.174/0.239/0.437/0.100 ms
```

この出力は、ゲートウェイが ping 可能であることを示しています。

# DHCP の設定例

## はじめに

次に、DHCPの設定例を示します。

Dynamic Host Configuration Protocol(DHCP)は、ネットワークデバイスに設定情報を割り当てるためのフレームワークを提供します。

DHCP では、ネットワーク構成パラメータにクライアント/サーバーモデルを使用します。DHCP クライアントは DHCP サーバーからネットワーク構成パラメータを要求し、DHCP サーバーは DHCP クライアントにネットワーク構成パラメータを割り当てます。このドキュメントでは、DHCP サーバーの構成について説明します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、DHCP の基本的な知識があることを前提としています。

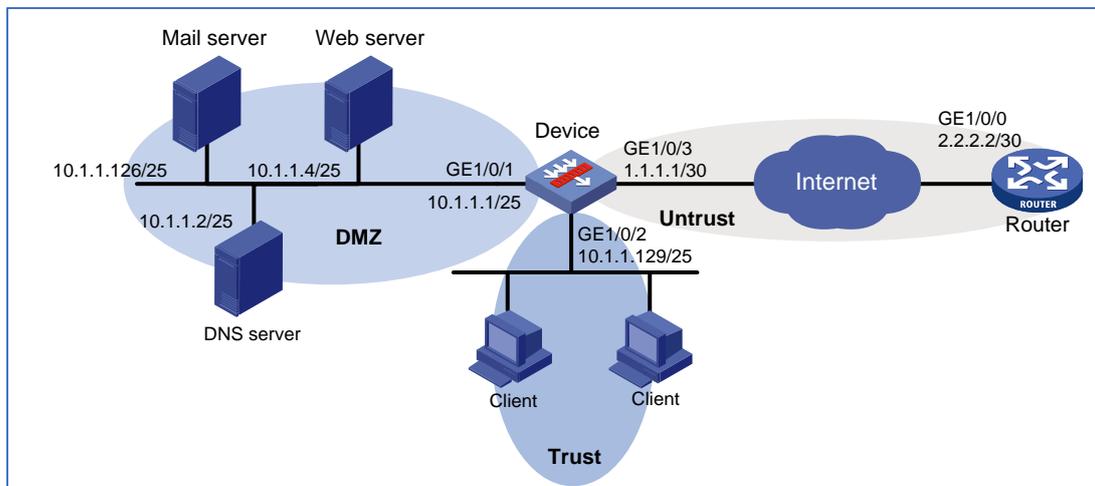
## 例:DHCPの設定

### ネットワーク構成

図1に示すように、クライアントと内部サーバーは異なるサブネット上にあります。次の要件を満たす DHCP アドレスプールをデバイス上に作成します。

- 内部サーバーは、スタティック IP アドレス、DNS サーバードレス、およびゲートウェイをデバイスから取得します。
- クライアントはデバイスから動的に IP アドレスを取得します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

- 動的割り当てのネットワークセグメントが、DHCP サーバー対応のインターフェイスと同じサブネット上にあることを確認してください。そうでない場合、クライアントは DHCP サーバーから IP アドレスを取得できません。
- ローカルセキュリティゾーンと DHCP サーバー対応インターフェイスのセキュリティゾーン間の通信を保証するには、ローカルセキュリティゾーンと DHCP サーバー対応インターフェイス間のセキュリティポリシーを設定します。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- A) **Basic Configuration** タブで、**DMZ** セキュリティゾーンを選択します。
- B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、10.1.1.1/25 と入力します。
- C) **OK** をクリックします。

#GE1/0/ge1/1/2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.1.1.129/25 に設定します。

#Untrust セキュリティゾーンに GE1/0/3 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 1.1.1.1/30 に設定します。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies > Security Policies を選択します。

#DMZ ゾーンとローカルゾーンの間にセキュリティポリシーを作成し、信頼ゾーンとローカルゾーンの間にセキュリティポリシーを作成します。セキュリティポリシーにより、セキュリティゾーン間の通信が保証されます。設定を示します。

図2 セキュリティポリシーの設定

<input type="checkbox"/>	Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matches	Traffic	Enable...	Enable	Edit
<input type="checkbox"/>	DMZ-...	DMZ Local	DMZ Local	IPv4	0		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	TRU-L...	Trust Local	Trust Local	IPv4	1		Any	Any	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 3. 静的に割り当てられた IP アドレスを設定します。

#トップナビゲーションバーで **network** をクリックします。

#ナビゲーションペインで、**DHCP > DHCP service** を選択します。

#**DHCP service** を **enable** に選択します。

#ナビゲーションペインで、**DHCP > DHCP Address Pools** を選択します。

#アドレスプールの **create** をクリックします。

#アドレスプール名を入力し、**OK** をクリックします(図3を参照)。

図3 DHCP アドレスプールの作成

Create DHCP Address Pool

Address pool name: test \* (1-63 chars)

OK Cancel

#Address Allocation タブをクリックします。

#静的に割り当てられた IP アドレスを追加します(図4を参照)。

図4 アドレス割り当ての設定

Address Pool

test ✕ Delete ⊕ Create address pool

**Address Allocation** | Address Pool Options | Assigned Addresses

Subnet for dynamic allocation ⓘ  /

Static binding list

⊕ Create ✕ Delete

<input type="checkbox"/>	IP address	Mask	Type	Hardware address/client ID	Edit
<input type="checkbox"/>	10.1.1.2	255.255.255.128	Ethernet	6c45-7b5d-0806	
<input type="checkbox"/>	10.1.1.4	255.255.255.128	Ethernet	6805-ca21-dda0	

The mask length is in the range of 1 to 30.  
The hardware address is a string of 4 to 39 characters.

OK

#Address Pool Options タブをクリックし、に示すようにアドレスプールオプションを設定します。

図5 アドレスプールオプションの設定

Address Pool

test ✕ Delete ⊕ Create address pool

Address Allocation **Address Pool Options** Assigned Addresses

Lease duration  Infinite  1 days 0 hours 0 minutes 0 seconds

Domain name suffix  (1-50 chars)

Gateways

<input type="checkbox"/>	Gateways	<input type="button" value="Edit"/>
--------------------------	----------	-------------------------------------

DNS servers

<input type="checkbox"/>	DNS servers	<input type="button" value="Edit"/>
<input type="checkbox"/>	10.1.1.1	<input type="button" value="Edit"/>

#OK をクリックします。

4. ダイナミックアドレス割り当てを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**DHCP > DHCP service** を選択します。

# **DHCP service** の **Enable** を選択します。

#ナビゲーションペインで、**DHCP > DHCP Address Pools** を選択します。

#アドレスプールの **create** をクリックします。

#アドレスプール名を入力し、OK をクリックします(図6を参照)。

図6 DHCP アドレスプールの作成

Create DHCP Address Pool ? ✕

Address pool name  \*(1-63 chars)

#Address Allocation タブをクリックします。

#動的割り当てのサブネットアドレスを入力します。設定を示します。

図7 アドレス割り当ての設定

Address Pool

test1 ✕ Delete ⊕ Create address pool

**Address Allocation** | Address Pool Options | Assigned Addresses

Subnet for dynamic allocation ?  /

Static binding list

⊕ Create ✕ Delete

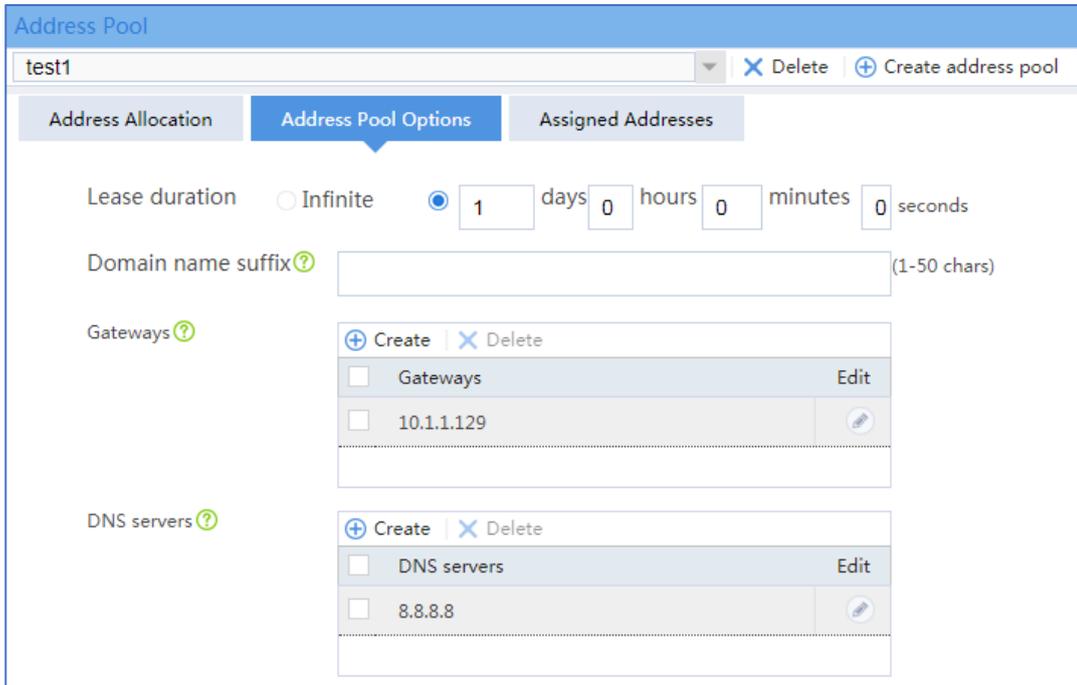
<input type="checkbox"/>	IP address	Mask	Type	Hardware address/client ID	Edit
--------------------------	------------	------	------	----------------------------	------

The mask length is in the range of 1 to 30.  
The hardware address is a string of 4 to 39 characters.

OK

#Address Pool Options タブをクリックし、ゲートウェイアドレスと DNS サーバードレスを追加します(図8を参照)。

図8 アドレスプールオプションの設定



#OK をクリックします。

## 設定の確認

### 静的にバインドされた IP アドレス割り当ての確認

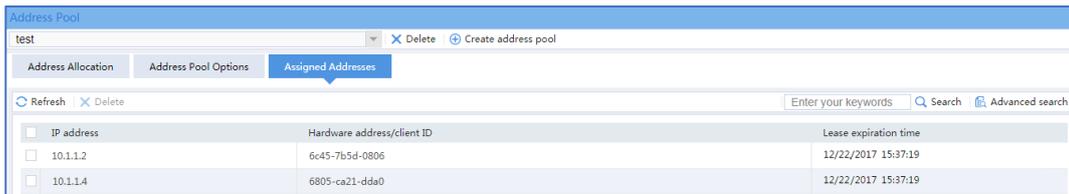
#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**DHCP > DHCP Address Pools** を選択します。

#スタティック割り当ての DHCP アドレスプールを選択し、**Assigned Addresses** タブをクリックします。

#デバイスが内部サーバーにスタティックアドレスを割り当てていることを確認します。

図9 静的に割り当てられた IP アドレスの確認



## 動的 IP アドレス割り当ての確認

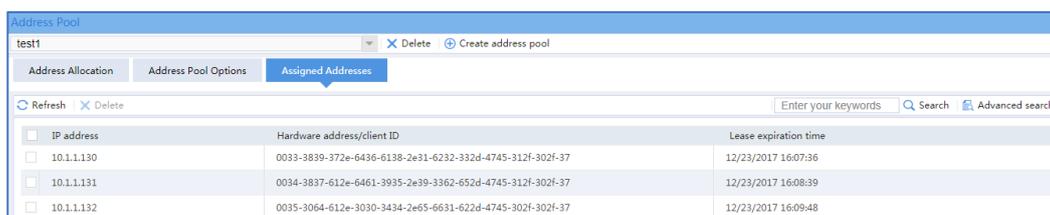
#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**DHCP > DHCP Address Pools** を選択します。

#動的割り当て用の DHCP アドレスプールを選択し、**Assigned Addresses** タブをクリックします。

#デバイスがクライアントにアドレスを動的に割り当てていることを確認します。

図10 動的に割り当てられた IP アドレスの確認



IP address	Hardware address/client ID	Lease expiration time
<input type="checkbox"/> 10.1.1.130	0033-3839-372e-6436-6138-2e91-6232-332d-4745-312f-302f-37	12/23/2017 16:07:36
<input type="checkbox"/> 10.1.1.131	0034-3837-612e-6461-3935-2e39-3362-652d-4745-312f-302f-37	12/23/2017 16:08:39
<input type="checkbox"/> 10.1.1.132	0035-3064-612e-3030-3434-2e65-6631-622d-4745-302f-302f-37	12/23/2017 16:09:48

# DNS 設定例

## はじめに

次に、DNSの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

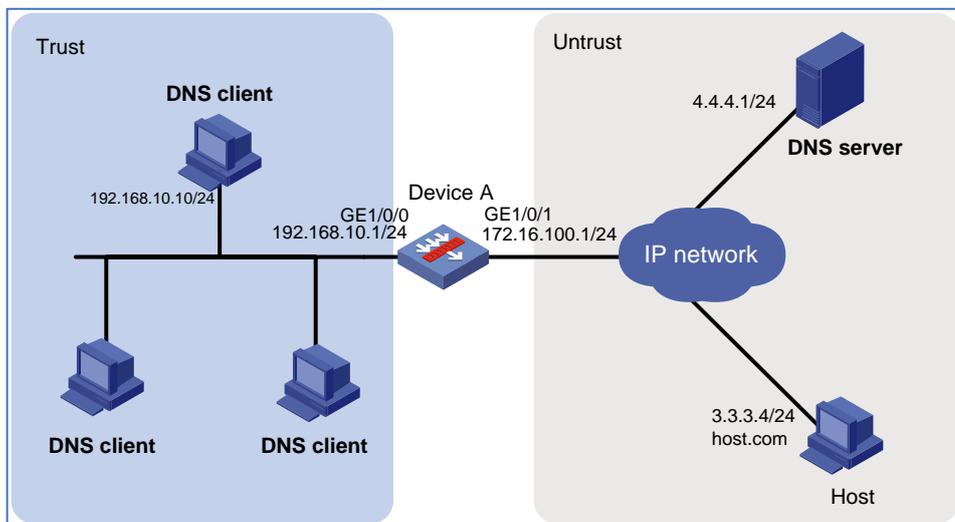
次の情報は、DNSに関する基本的な知識があることを前提としています。

## 例:DNSプロキシの設定

### ネットワーク構成

図1に示すように、デバイス A は DNS プロキシとして動作し、DNS クライアントと DNS サーバー間で DNS パケットをリレーします。DNS クライアントは、DNS プロキシを介して host.com というドメイン名のホストにアクセスします。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

DNS サーバーの IP アドレスが変更された場合、またはドメイン名と IP アドレスのマッピングが変更された場合は、DNS プロキシおよび DNS クライアント上の DNS キャッシュをクリアします。

## 手順

### デバイス A の設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - # トップナビゲーションバーで、**network** をクリックします。
  - # ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - # GE1/0/1 の **edit** アイコンをクリックします。
  - # 開いたダイアログボックスで、インターフェイスを設定します。
    - A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、172.16.100.1/24 と入力します。

C) **OK**をクリックします。

#GE1/0/0 を **trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 192.168.10.1/24 に設定します。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#ゾーン **Untrust** とゾーン **Trust** の間にセキュリティポリシーを作成します。設定をに示します。

図2 セキュリティポリシーの設定

Name	Src zone	Dist zone	Type	ID	Descrip...	Src address	Dst address	Service	User	Action	Conten...	Matches	Traffic	Enable...	Enable	Edit
TR-UN...	Untrust	Trust	IPv4	9		Any	Any	Any	Any	Permit				<input checked="" type="checkbox"/>	<input type="checkbox"/>	

## 3. DNSプロキシを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**DNS > Advanced Settings** を選択します。

#**enable** を選択します。

図3 DNS プロキシの有効化

The DNS advanced sttings apply to both IPv4 DNS and IPV6 DNS.

**DNS proxy**

Enable

The DNS proxy forwards the request from the DNS client to the designated DNS server, and conveys the reply from the DNS server to the client.

## 4. DNSサーバーのIPアドレスを指定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**DNS > DNS Client** を選択します。

#DNS サーバーの IP アドレスを入力します。

#**add** アイコンをクリックします。

図4 DNS サーバーの指定

## DNS クライアントの構成

#DNSクライアントにIPアドレスを割り当て、DNSクライアント上のDNSサーバーのIPアドレスを指定します。

## 設定の確認

1. 各DNSクライアントがhost.comというドメイン名のホストに正常にpingできることを確認します。

```
C:¥Users¥abc>ping host.com
```

```
Pinging host.com [3.3.3.4] with 32 bytes of data:  
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253  
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253  
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253  
Reply from 3.3.3.4: bytes=32 time<1ms TTL=253
```

Ping statistics for 3.3.3.4:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

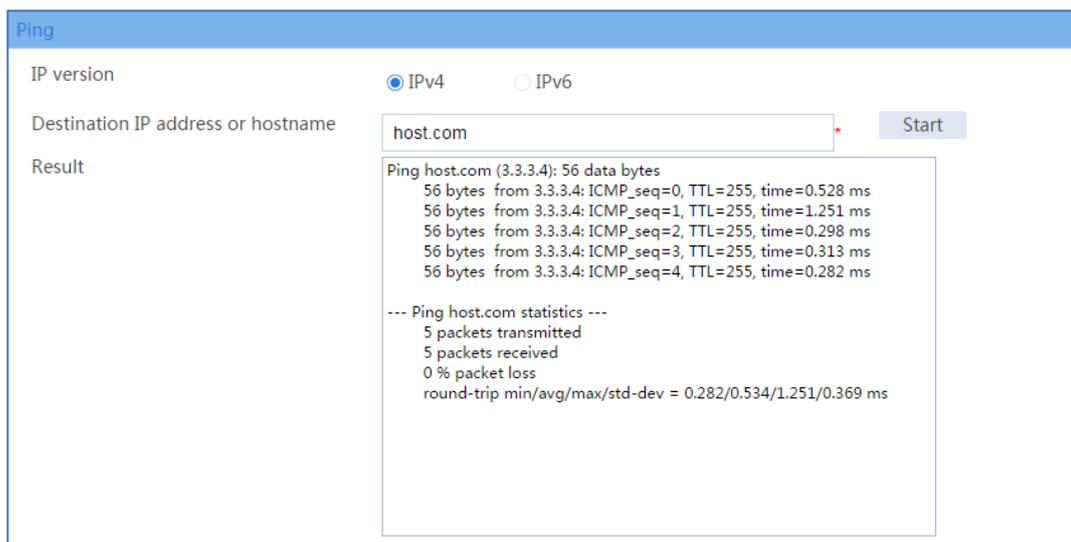
2. デバイスAがドメイン名host.comを持つホストに正常にpingできることを確認します。

#トップナビゲーションバーで、システムをクリックします。

#ナビゲーションペインで、Diagnosis Center>Ping を選択します。

#Destination IP address or hostname フィールドに host.com と入力し、Start をクリックします。

図5 ping 操作



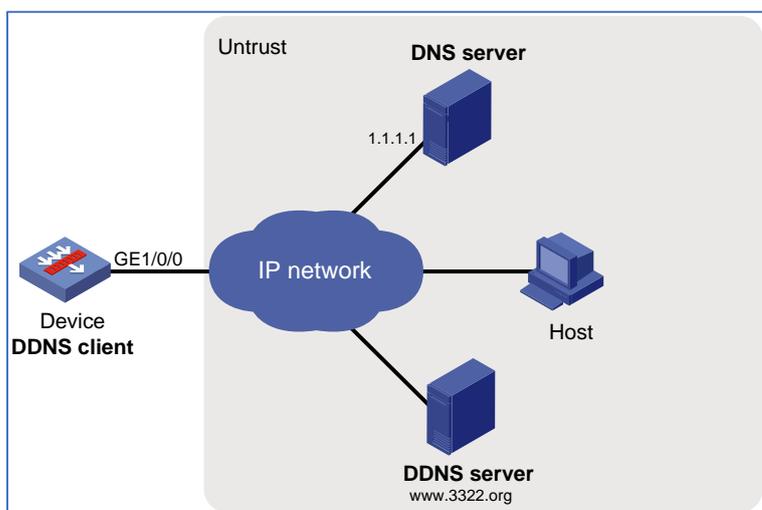
## 例:DDNSの設定

### ネットワーク構成

図1に示すように、デバイスはドメイン名 whatever.3322.org を持つ Web サーバーであり、DHCP を通じて動的に取得される IP アドレスを使用します。IP アドレスが変更されたときに、デバイスが常に何らかの.3322.org の Web サービスを提供できるようにするには、デバイス上で次の作業を実行します。

- DDNS サーバー上のデバイスのドメイン名から IP アドレスへのマッピングを更新するように DDNS ポリシーを構成します。DDNS サーバーは DNS サーバー上のマッピングを更新します。
- デバイスがドメイン名を介して DDNS サーバーにアクセスできるように、DNS サーバーの IP アドレスを指定します。

図 6 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 前提条件

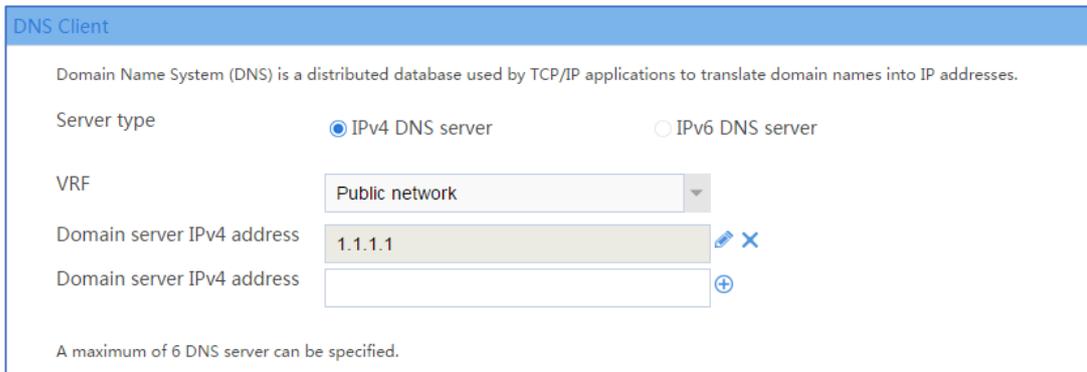
デバイスで DDNS を設定する前に、次の作業を実行します。

- ユーザー名 **hell** およびパスワード **neve** は、<http://www.3322.org/> で登録してください。
- デバイスの FQDN と DNS サーバー上の IP アドレス間のマッピングを作成します。

## 手順

1. セキュリティポリシーを設定します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。  
#セキュリティポリシーを設定します(詳細は省略)。
2. DNSサーバーのIPアドレスを指定します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**DNS > DNS Client** を選択します。  
#DNS サーバーの IP アドレスを追加します(図7を参照)。

図7 DNS サーバーの指定



DNS Client

Domain Name System (DNS) is a distributed database used by TCP/IP applications to translate domain names into IP addresses.

Server type  IPv4 DNS server  IPv6 DNS server

VRF Public network

Domain server IPv4 address 1.1.1.1

Domain server IPv4 address

A maximum of 6 DNS server can be specified.

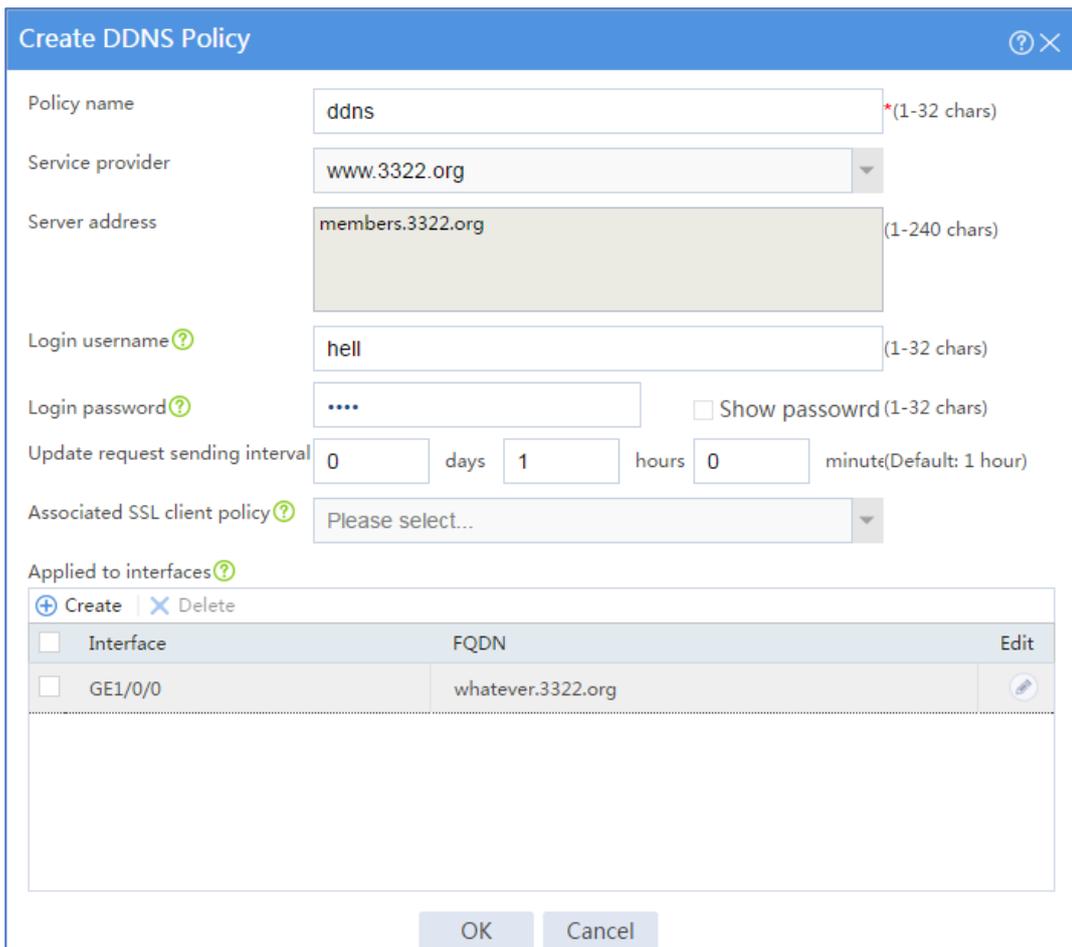
3. DDNSポリシーを設定します。

#ナビゲーションペインで、**DNS > DDNS Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、DDNS ポリシーを作成します(図8を参照)。

図8 DDNS ポリシーの作成



Create DDNS Policy

Policy name ddns (1-32 chars)

Service provider www.3322.org

Server address members.3322.org (1-240 chars)

Login username hell (1-32 chars)

Login password .....  Show password (1-32 chars)

Update request sending interval 0 days 1 hours 0 minute(Default: 1 hour)

Associated SSL client policy Please select...

Applied to interfaces

+ Create | X Delete

Interface	FQDN	Edit
<input type="checkbox"/> GE1/0/0	whatever.3322.org	

OK Cancel

#OK をクリックします。

## 設定の確認

IP アドレスが変更されたときに、デバイスが DDNS プロバイダ [www.3322.org](http://www.3322.org) を介してドメイン名と IP のマッピングを更新できることを確認します。インターネットユーザーは、ドメイン名 **whatever.3322.org** を介して正しい IP アドレスを解決し、Web サービスにアクセスできます。

# オブジェクトグループの設定例

## はじめに

次に、IPv4 アドレス、IPv6 アドレス、MAC アドレス、およびサービスオブジェクトグループと時間範囲の設定例を示します。

- **IPv4 address object group:**パケット内の IPv4 アドレスの照合に使用される IPv4 アドレスオブジェクトのグループ。
- **IPv6 address object group:**パケット内の IPv6 アドレスの照合に使用される IPv6 アドレスオブジェクトのグループ。
- **MAC address object group:**パケット内の MAC アドレスの照合に使用される MAC アドレスオブジェクトのグループ。
- **Service object group:**パケット内のプロトコルタイプおよびプロトコル特性(TCP/UDP 送信元/宛先ポート、ICMP メッセージタイプおよびコードなど)を照合するために使用されるサービスオブジェクトのグループ。
- **Time range:**時間範囲を適用して、時刻に基づくサービスを実装できます。時間ベースサービスは、時間範囲で指定された期間にのみ有効です。時間範囲が存在しない場合、時間範囲に基づくサービスは有効になりません。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

以下の情報は、オブジェクトグループ機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

オブジェクトグループを設定する場合は、次の制限事項およびガイドラインに従ってください。

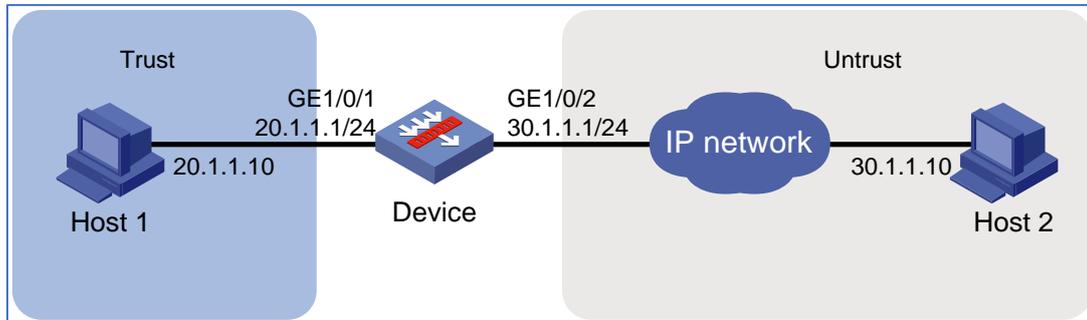
- システムは最大 5 つのオブジェクトグループ階層レイヤーをサポートします。たとえば、グループ 1、2、3 および 4 がそれぞれグループ 2、3、4 および 5 を使用する場合、グループ 5 は別のグループを使用できず、グループ 1 は別のグループによって使用できません。
- 2 つのオブジェクトグループが同時に使用することはできません。

## 例:IPv4アドレスオブジェクトグループの設定

### ネットワーク構成

図1に示すように、ホスト 1 がホスト 2 と通信できるように、デバイス上で IPv4 アドレスオブジェクトグループを設定します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、ネットワークをクリックします。

#ナビゲーションペインで、Interface Configuration > Interfaces を選択します。

#GE1/0/1 の編集アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- A) 基本**basic configuration**タブで、**Trust**セキュリティゾーンを選択します。
- B) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、20.1.1.1/24と入力します。
- C) **OK**をクリックします。

#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 30.1.1.1./24 に設定します。

## 2. IPv4アドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、**object** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。

- A) グループ名を入力します。この例では、**test-a**と入力します。
- B) 説明を入力します。この例では、**20.1.1.0/24**と入力します。
- C) **add**をクリックします。

図2 IPv4アドレスオブジェクトグループを作成する

Create IPv4 Address Object Group

Group name: test-a (1-31 chars)

Description: 20.1.1.0/24 (1-127 chars)

Security zone: [Dropdown]

Type	Content	Excluded addresses	Edit
------	---------	--------------------	------

Page 0 of 0 | Entries per page 25 | No data

OK Cancel

D) 表示されるダイアログボックスで、**Network Segment**オブジェクトを選択し、IPv4アドレスとマスク長20.1.1.0/24を入力します。

E) **OK**をクリックします。

図3 オブジェクトを作成する

Create Object

Object: Network segment

Excluded addresses: 20.1.1.1, 255.255.255.0 (IPv4 address/mask length (0-32))

OK Cancel

F) IPv4アドレスオブジェクトグループの作成ページで、**OK**をクリックします。

3. ゾーン Trust からゾーン Untrust へのセキュリティポリシーを作成します。
- #トップナビゲーションバーで、**Policies** をクリックします。
- #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
- #create をクリックします。
- #表示されるダイアログボックスで、セキュリティポリシーを設定します。
- ポリシー名 **test-a** を入力します。
  - ソースゾーンの **Trust** を選択します。
  - 宛先ゾーン **Untrust** を選択。
  - タイプ **IPv4** を選択します。
  - アクション **permit** を選択します。
  - 送信元 IP/MAC アドレス **test-a** を選択します。
- #OK をクリックします。

## 設定の確認

#ホスト 1 からホスト 2 に正常に ping できることを確認します。

```
C:¥Users¥abc> ping 30.1.1.10
```

#セッション情報を表示するには、次のとおりです。

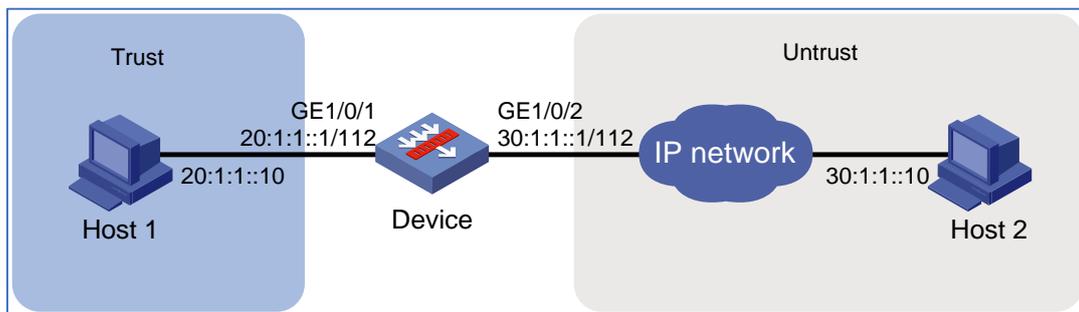
1. トップナビゲーションバーで **monitor** をクリックします。
2. ナビゲーションペインで、**Session** を選択します。

## 例:IPv6アドレスオブジェクトグループの設定

### ネットワーク構成

図 4 に示すように、ホスト 1 がホスト 2 と通信できるように、デバイス上で IPv6 アドレスオブジェクトグループを設定します。

図 4 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. IPv6アドレスをインターフェイスに割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    1. **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    2. **IPv6 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、20:1:1::1/112 と入力します。
    3. **OK** をクリックします。
  - #Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 30:1:1::1/112 に設定します。
2. IPv6アドレスオブジェクトグループを作成します。
  - #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > IPv6Address Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、IPv6 アドレスオブジェクトグループを設定します。
    - A) グループ名を入力します。この例では、**test-6a** と入力します。
    - B) **add** をクリックします。

図5 IPv6 アドレスオブジェクトグループを作成する

Create IPv6 Address Object Group

Group name: test-6a (1-31 chars)

Description: (1-127 chars)

Security zone: [Dropdown]

+ Add X Delete

Type	Object	Excluded addresses	Edit
------	--------	--------------------	------

OK Cancel

表示されるダイアログボックスで、ネットワークセグメントオブジェクトを選択し、IPv6 アドレスとプレフィクス長 20:1:1::/112 を入力します。

OK をクリックします。

図6 オブジェクトを作成する

Create Object

Object: Network segment

Excluded addresses: 20:1:1:: / 112 (IPv6 address/prefix length (1-128))

OK Cancel

E) **Create IPv6 Address Object Group** ページで、**OK** をクリックします。

3. ゾーン **Trust** からゾーン **Untrust** へのセキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **test-6a** を入力します。
- ソースゾーンの **Trust** を選択します。
- 宛先ゾーン **Untrust** を選択。
- タイプ **IPv6** を選択します。
- アクション **permit** を選択します。
- 送信元 IP/MAC アドレス **test-6a** を選択します。

#**OK** をクリックします。

## 設定の確認

#ホスト 1 からホスト 2 に正常に ping できることを確認します。

```
C:¥Users¥abc> ping 30:1:1::10
```

#セッション情報を表示するには、次のとおりです。

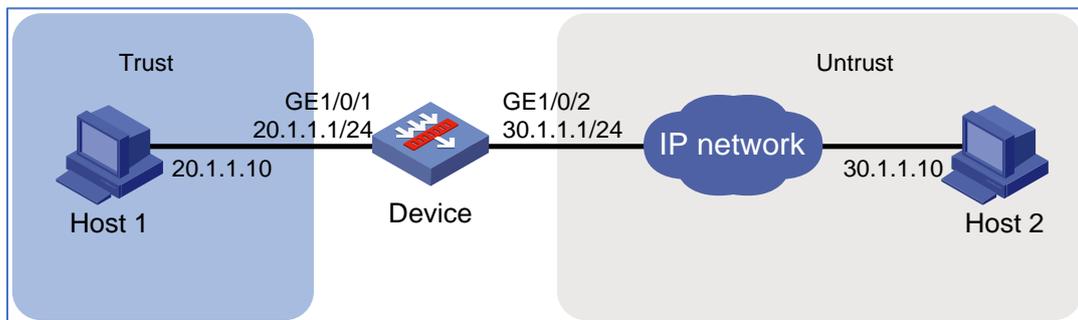
1. トップナビゲーションバーで **Monitor** をクリックします。
2. ナビゲーションペインで、**Session** を選択します。

## 例:MACアドレスオブジェクトグループの設定

### ネットワーク構成

図 7 に示すように、ホスト 1 がホスト 2 と通信できるように、デバイス上で MAC アドレスオブジェクトグループを設定します。ホスト 1 の MAC アドレスは 3C-52-82-72-03-1F です。

図 7 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、20.1.1.1/24 と入力します。
    - C) **OK** をクリックします。
  - #GE1/0/GE1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 30.1.1.1/24 に設定します。
2. MACアドレスオブジェクトグループを作成します。
  - #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > MAC Address Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、MAC アドレスオブジェクトグループを設定します。
    - A) グループ名を入力します。この例では、**test-mac** と入力します。

B) 説明を入力します。この例では、**Host1-mac**と入力します。

C) **add**をクリックします。

図8 MAC アドレスオブジェクトグループを作成する

The dialog box titled "Create MAC Address Object Group" has a blue header bar with a help icon and a close button. It contains two text input fields: "Group name" with the value "test-mac" and a character count "(1-31 chars)", and "Description" with the value "Host1-mac" and a character count "(1-127 chars)". Below these fields is a table with a header row containing "Type", "Content", and "Edit". Above the table are buttons for "Add" (with a plus icon) and "Delete" (with a minus icon). At the bottom of the dialog are "OK" and "Cancel" buttons.

D) 表示されるダイアログボックスで、MACアドレスオブジェクトを設定します。

② タイプ **MAC Address** を選択します。

③ MAC アドレス **3C-52-82-72-03-1F** を入力します。

E) **OK**をクリックします。

図9 オブジェクトを作成する

The dialog box titled "Create Object" has a blue header bar with a help icon and a close button. It contains a "Type" section with two radio buttons: "MAC address object group" (unselected) and "MAC address" (selected). Below this is a "MAC address" field with a help icon and a character count, containing the value "3C-52-82-72-03-1F". At the bottom of the dialog are "OK" and "Cancel" buttons.

F) **Create MAC Address Object Group** ページで、**OK** をクリックします。

3. ゾーン **Trust** からゾーン **Untrust** へのセキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **test-mac** を入力します。
- ソースゾーンの **Trust** を選択します。
- 宛先ゾーン **Untrust** を選択。
- タイプ **IPv4** を選択します。
- アクション **permit** を選択します。
- 送信元 IP/MAC アドレス **test-mac** を選択します。

#**OK** をクリックします。

## 設定の確認

#ホスト 1 からホスト 2 に正常に ping できることを確認します。

```
C:¥Users¥abc> ping 30.1.1.10
```

#セッション情報を表示するには、次のとおりです。

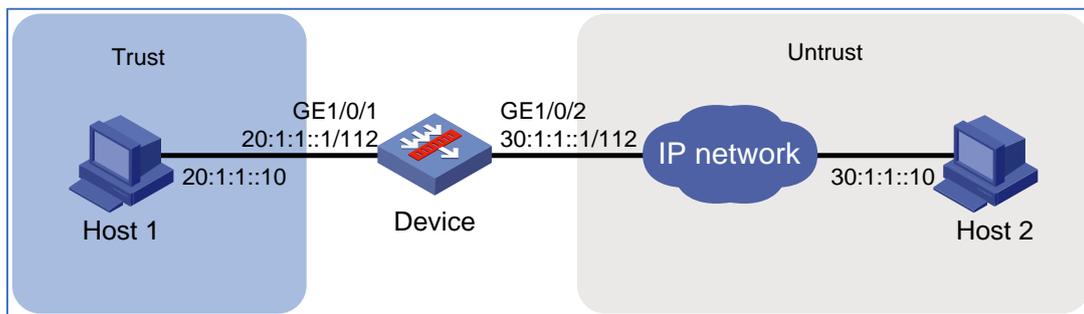
1. トップナビゲーションバーで **Monitor** をクリックします。
2. ナビゲーションペインで、**Session** を選択します。

## 例: サービスオブジェクトグループの設定

### ネットワーク構成

図 10I に示すように、ホスト 1 が ICMPv6 経由でホスト 2 と通信できるように、デバイス上でサービスオブジェクトグループを設定します。

図 10 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. IPv6アドレスをインターフェイスに割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv6 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、20:1:1::1/112 と入力します。
    - C) **OK** をクリックします。
  - #Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 30:1:1::1/112 に設定します。
2. サービスオブジェクトグループを作成します。
  - #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > Service Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、サービスオブジェクトグループを設定します。
    - A) グループ名を入力します。この例では、**test-fa** と入力します。
    - B) **add** をクリックします。

図11 サービスオブジェクトグループを作成する

Create Service Object Group

Group name: test-fa (1-31 chars)

Description: (1-127 chars)

Type	Content	Edit
------	---------	------

OK Cancel

C) 開いたダイアログボックスで、サービスオブジェクトを設定します。

④ オブジェクト **Protocol name** を選択します。

⑤ **ICMPv6** タイプを選択します。

D) OKをクリックします。

図12 オブジェクトを作成する

Create Object

Object ?  Protocol name  Protocol number  Object group

Type: ICMPv6

Message type: (1-255)

Message code: (1-255)

OK Cancel

- E) サービスオブジェクトグループの作成ページで、OKをクリックします。
3. ゾーンTrustからゾーンUntrustへのセキュリティポリシーを作成します。
- #トップナビゲーションバーで、**Policies** をクリックします。
- #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
- #**create** をクリックします。
- #表示されるダイアログボックスで、セキュリティポリシーを設定します。
- ポリシー名 **test-fa** を入力します。
  - ソースゾーン **Trust** を選択します。
  - 宛先ゾーン **Untrust** を選択。
  - タイプ **IPv6** を選択します。
  - アクション **permit** を選択します。
  - サービス **test-fa** を選択します。
- #OK をクリックします。

## 設定の確認

#ホスト 1 からホスト 2 に正常に ping できることを確認します。

```
C:¥Users¥abc> ping 30:1:1::10
```

#セッション情報を表示するには、次のとおりです。

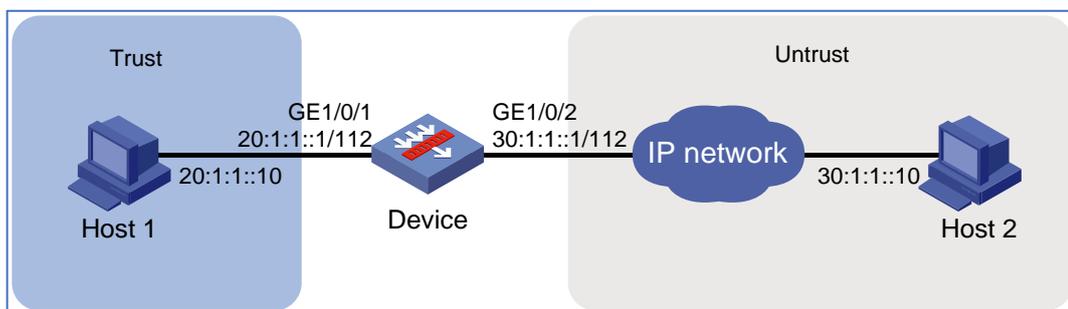
1. トップナビゲーションバーで **Monitor** をクリックします。
2. ナビゲーションペインで、**Session** を選択します。

## 例:時間範囲の設定

## ネットワーク構成

図 13 に示すように、デバイス上でサービスオブジェクトグループを設定し ICMPv6 を介してホスト 2 と通信できるように、デバイス上でサービスオブジェクトグループを設定します。

図 13 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. IPv6アドレスをインターフェイスに割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv6 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、20:1:1::1/112 と入力します。
    - C) **OK** をクリックします。
  - #Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 30:1:1::1/112 に設定します。
2. サービスオブジェクトグループを作成します。
  - #トップナビゲーションバーで、**Object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > Service Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、サービスオブジェクトグループを設定します。
    - A) グループ名を入力します。この例では、**test-fa** と入力します。
    - B) **add** をクリックします。

図14 サービスオブジェクトグループを作成する

Create Service Object Group

Group name: test-fa (1-31 chars)

Description: (1-127 chars)

Type	Content	Edit
------	---------	------

OK Cancel

C) 開いたダイアログボックスで、サービスオブジェクトを設定します。

9. オブジェクト **Protocol name** を選択します。

10. **ICMPv6** タイプを選択します。

D) OKをクリックします。

図15 オブジェクトを作成する

Create Object

Object:  Protocol name  Protocol number  Object group

Type: ICMPv6

Message type: (1-255)

Message code: (1-255)

OK Cancel

E) サービスオブジェクトグループの作成ページで、OKをクリックします。

3. 時間範囲を作成します。

#トップナビゲーションバーで、**Object** をクリックします。

#ナビゲーションペインで、**Object Groups > Time Ranges** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、**test-time** という名前を入力し、**Periodic time range** の **Create** をクリックします。

#表示されるダイアログボックスで、時間範囲を設定します。

- 開始時刻を **08:10** に設定します。
- 終了時刻を **17:10** に設定します。
- **Monday、Tuesday、Wednesday、Thursday**、および **Friday** を選択し

#OK をクリックします。

図16 時間範囲の設定

The screenshot shows a dialog box titled "Create Periodic Time Range". It features a blue header bar with a question mark icon and a close button (X). The main content area includes two rows of time selection: "Start time" with input boxes for "8" and "10", and "End time" with input boxes for "17" and "10". Below the time fields is a list of days of the week with corresponding checkboxes: Sunday (unchecked), Monday (checked), Tuesday (checked), Wednesday (checked), Thursday (checked), Friday (checked), and Saturday (unchecked). At the bottom of the dialog are two buttons: "OK" and "Cancel".

#時間範囲の作成ページで、OK をクリックします。

4. ゾーン **Trust** からゾーン **Untrust** へのセキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **test-time** を入力します。
- ソースゾーン **trust** を選択します。
- 宛先ゾーン **Untrust** を選択。
- タイプ **IPv6** を選択します。
- アクション **permit** を選択します。
- サービス **test-fa** を選択します。
- 時間範囲 **test-time** を選択します。

#**OK** をクリックします。

## 設定の確認

#指定された時間範囲内で、ホスト 1 からホスト 2 への ping が成功することを確認します。

```
C:¥Users¥abc> ping 30:1:1::10
```

#ホスト 1 からホスト 2 に ping できず、対応するセッションが時間範囲で指定された時間を超えて存在しないことを確認します。

# 公開鍵管理の設定例

## はじめに

次に、公開キー管理の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

以下の情報は、公開鍵管理の基本的な知識があることを前提としています。

## 制限事項とガイドライン

ピアホスト公開キーを手動で入力する場合は、入力したキーが正しい形式であることを確認してください。正しい形式でピアホスト公開キーを取得するには、ピアデバイスで公開キーを表示し、キーを記録します。その他の方法で表示される公開キーの形式が正しくない可能性があります。キーが正しい形式でない場合、システムはキーを破棄し、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不明な場合は、ピアホスト公開キーを入力するのではなくインポートすることをお勧めします。

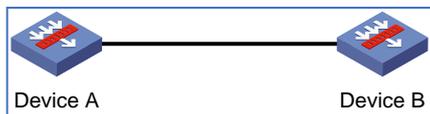
# 例:ピアホスト公開キーの入力

## ネットワーク構成

図1に示すように、デバイス A からデバイス B への不正アクセスを防止するために、デバイス B はデジタル署名を使用してデバイス A を認証します。デバイス B で認証パラメータを設定する前に、次の手順に従ってデバイス B のデバイス A の公開キーを設定します。

- デバイス A で RSA キーペアを作成し、RSA キーペアの公開キーを表示します。
- デバイス B のデバイス A の RSA ホスト公開キーを手動で指定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイスAの設定

#トップナビゲーションバーで、**object** をクリックします。

#ナビゲーションペインで、**Public Key Management > Local Key Pairs** を選択します。

#**Create** をクリックします。**Create Local Key Pair** ページが開きます。

#次のように RSA ローカルキーペアを作成します。

- キーペア名 **devicea-rsa** を入力します。
- **RSA** アルゴリズムを選択します。
- キーの長さ **1800** を入力します。

#OK をクリックします。

#キーペア名 `devicea-rsa` をクリックして、**Key Pair Details** ページを開きます。

#**Public key** フィールドに表示されるデータを記録します。

図2 ローカルキーペアの作成

Create Local Key Pair

Name  (1-64 chars)

Algorithm  \*

Key length  \*bits(512-2048)

OK Cancel

図3 キーの詳細

Key Pair Details

Name devicea-rsa

Algorithm RSA

Key strength 1800 bits

Creation time 2018-09-12 10:27:01

Public key  
30820100300D06092A864886F70D01010105000381EE003081EA0281E200AB93  
6D13D22B68A4B720261654DBC5060E7BC5FC20ED0443B7CAA72C56F2005C9E  
C042D5B09869E6A7152B80B8764122799025C4940F17EAAB43DC6185BA3C00A  
DAE62E3CBD47DCEF348320715EB6600C927C16156A976D37580F9A1CB3747AF  
3BCED6689E6F3806162FF27EBF886C32AFEB6F4A18A8A1533CC88430DE763825  
1ED675F8F72201D95D949BCCE1BD3B8FF2CA4E382D8120C8D953ED0C82C375  
CEF4E12FE4F4A4C8B17EB6EC7BD86BA870F657FC4C305D209B5D1588BF841572  
7DD9811B7C635764A1F887560DFA021205501DFD15B4339107F9597D6D69EC3  
8DDB90203010001

Close

## デバイスBの設定

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Public Key Management > Local Key Pairs** を選択します。

#**Import** をクリックします。**Import Peer Host Public Key** ページが開きます。

#ピアホスト公開キーを次のように設定します。

- パブリックキー名 **peer-rsa** を入力します。
- **Type or copy peer public key import method** を選択します。
- **Public key data** フィールドに、デバイス A の公開キーデータを入力するか、デバイス A の公開キーデータをコピーして貼り付けます。

#**OK** をクリックします。

図4 ピアホスト公開キーの入力

The screenshot shows a dialog box titled "Import Peer Host Public Key". It has three main sections:

- Public key name:** A text input field containing "peer-rsa". To the right of the field is a red asterisk and the text "(1-64 chars)".
- Import method:** Two radio button options. The first is "Import peer public key from file" (unselected). The second is "Type or copy peer public key" (selected).
- Public key data:** A large text area containing a long alphanumeric string: "30820100300D06092A864886F70D01010105000381EE003081EA0281E200AB936D13D22B68A4B720261654DBC5060E7BC5FC20ED0443B7CAA72C56F2005C9EC042D5B09869E6A7152B80B8764122799025C4940F17EAAB43DC6185BA3C00ADAE62E3CBD47DCEF348320715EB6600C927C16156A976D37580F9A1CB3747AF3BCED6689E6F3806162FF27EBF886C32AFEB6F4A18A8A1533CC88430DE7638251ED675F8F72201D95D949BCCE1BD3B8FF2CA4E382D8120C8D953ED0C82C375CEF4E12FE4F4A4C8B17EB6EC7BD86BA870F657FC4C305D209B5D158BBF8415727DD9811B7C635764A1F887560DFA021205501DFD15B4339107F9597D6D69EC38DDB90203010001". To the right of the field is a red asterisk and the text "(1-2047 chars)".

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

## 設定の確認

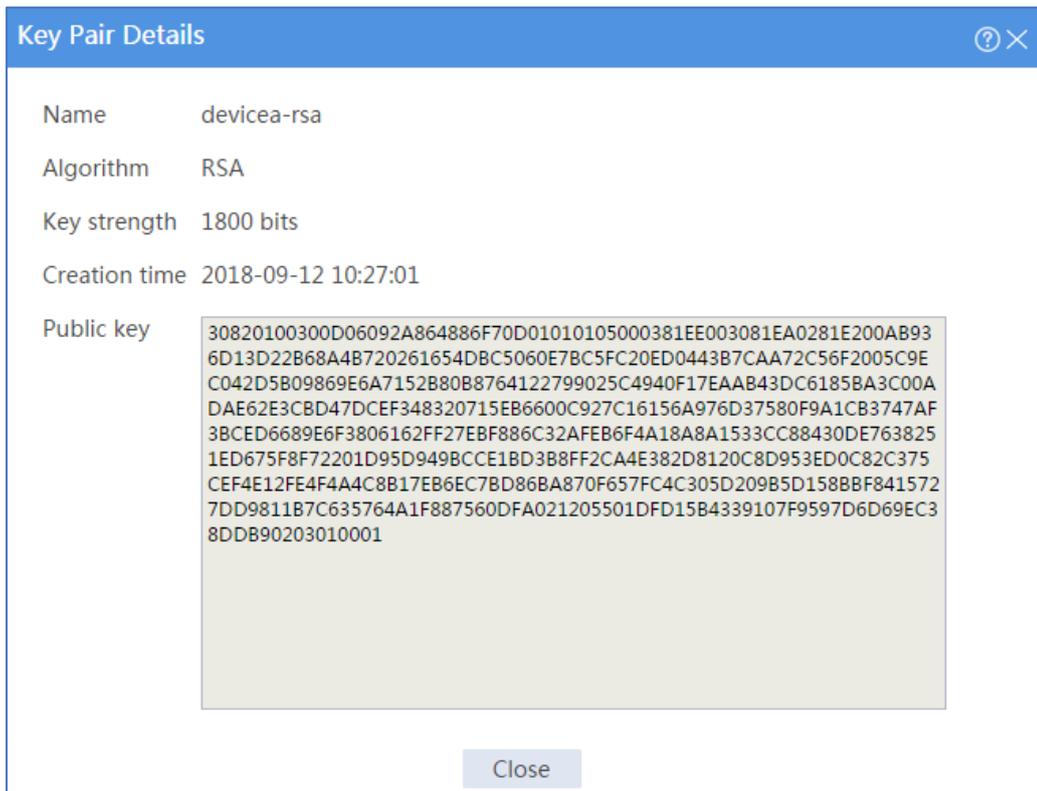
1. デバイスAのローカル公開キーに関する情報を表示します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Public Key Management > Local Key Pairs** を選択します。

#キーペア **devicea-rsa** の **Details** アイコンをクリックして、**Key Pair Details** ページを開きます。**Public key** フィールドには、公開キーの内容が表示されます。

図5 ローカルホスト公開鍵情報



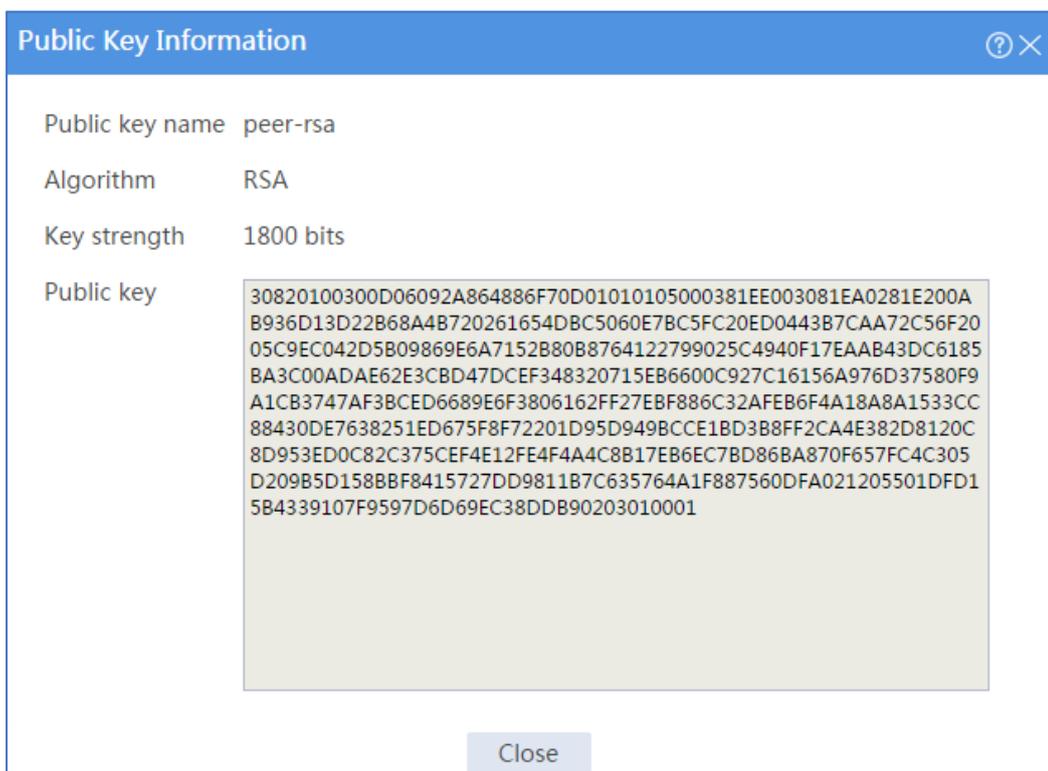
1. デバイス B に設定されているピア公開キーに関する情報を表示します。

#トップナビゲーションバーで、**Object** をクリックします。

#ナビゲーションペインで、**Public Key Management > Peer Public Keys** を選択します。

#公開キー **peer-rsa** の **Details** アイコンをクリックします。

図6 手動で設定されたピアホスト公開キー



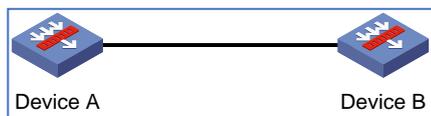
## 例:公開鍵ファイルからのピアホスト公開鍵のインポート

### ネットワーク構成

図7に示すように、デバイス A からデバイス B への不正アクセスを防止するために、デバイス B はデジタル署名を使用してデバイス A を認証します。デバイス B で認証パラメータを設定する前に、次の手順に従ってデバイス B のデバイス A の公開キーを設定します。

- デバイス A で RSA キーペアを作成し、RSA ホスト公開キーをファイルにエクスポートします。
- デバイス A の RSA ホスト公開キーを公開キーファイルからデバイス B にインポートします。

図7 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイスAの設定

#トップナビゲーションバーで、**Object** をクリックします。

#ナビゲーションペインで、**Public Key management > Local Key Pairs** を選択します。

#**Create** をクリックします。**Create Local Key Pair** ページが開きます。

図8 ローカルキーペアの作成

A screenshot of a dialog box titled 'Create Local Key Pair'. The dialog has a blue header bar with a question mark icon and a close button. It contains three input fields: 'Name' with the value 'devicea-rsa' and a '(1-64 chars)' label; 'Algorithm' with a dropdown menu showing 'RSA' and a red asterisk; and 'Key length' with the value '1800' and a '\*bits(512-2048)' label. At the bottom, there are 'OK' and 'Cancel' buttons.

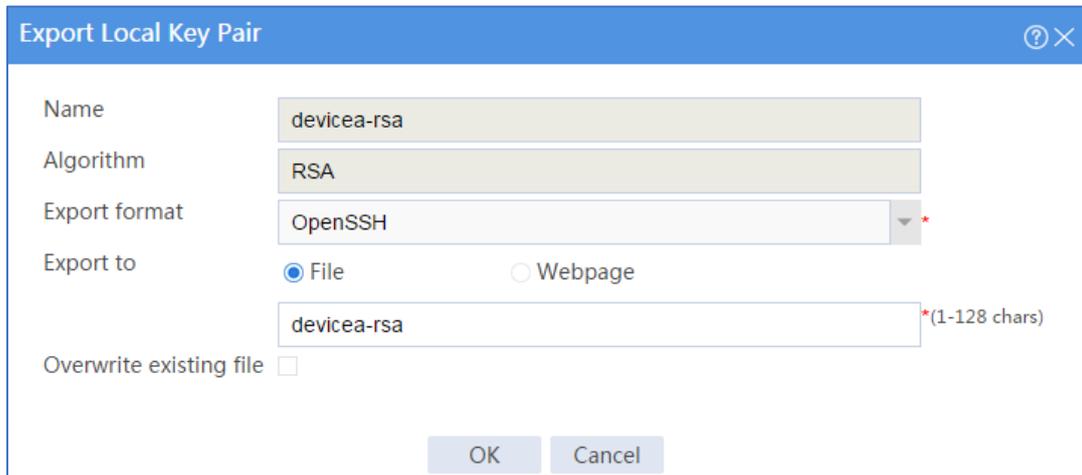
#次のように RSA ローカルキーペアを作成します。

- キーペア名 **devicea-rsa** を入力します。
- **RSA** アルゴリズムを選択します。
- キーの長さ **1800** を入力します。

#**OK** をクリックします。

#キーペア **devicea-rsa** を選択し、**Export** をクリックします。**Export Local Key Pair** が開きます。

図9 ローカルホスト公開キーのエクスポート



#**OpenSSH** エクスポート形式を選択し、ホスト公開キーを **devicea-rsa** という名前のファイルにエクスポートして、**OK** をクリックします。

#キーがファイル **devicea-rsa** にエクスポートされたら、ファイルをピアデバイス(デバイス B)に転送します(詳細は省略)。

## デバイス B の設定

#トップナビゲーションバーで、**Object** をクリックします。

#ナビゲーションペインで、**Public Key Management > Local Key Pairs** を選択します。

#**Import** をクリックします。**Import Peer Host Public Key** ページが開きます。

#ピアホスト公開キーを次のように設定します。

- パブリックキー名 **peer-rsa** を入力します。
- **Import peer public key from file import method** を選択します。
- 公開鍵ファイル **devicea-rsa** のパスを選択します。

#**OK** をクリックします。

図10 公開鍵ファイルからのピアホスト公開鍵のインポート

Import Peer Host Public Key

Public key name  \* (1-64 chars)

Import method  Import peer public key from file  Type or copy peer public key

Import file

## 設定の確認

2. デバイス A のローカル公開キーに関する情報を表示します。  
#トップナビゲーションバーで、**Object** をクリックします。  
#ナビゲーションペインで、**Public Key Management > Local Key Pairs** を選択します。  
#キーペア **devicea-rsa** の **Details** アイコンをクリックして、**Key Pair Details** ページを開きます。**Public key** フィールドには、公開キーの内容が表示されます。

図11 ローカルホスト公開鍵情報

Key Pair Details

Name devicea-rsa

Algorithm RSA

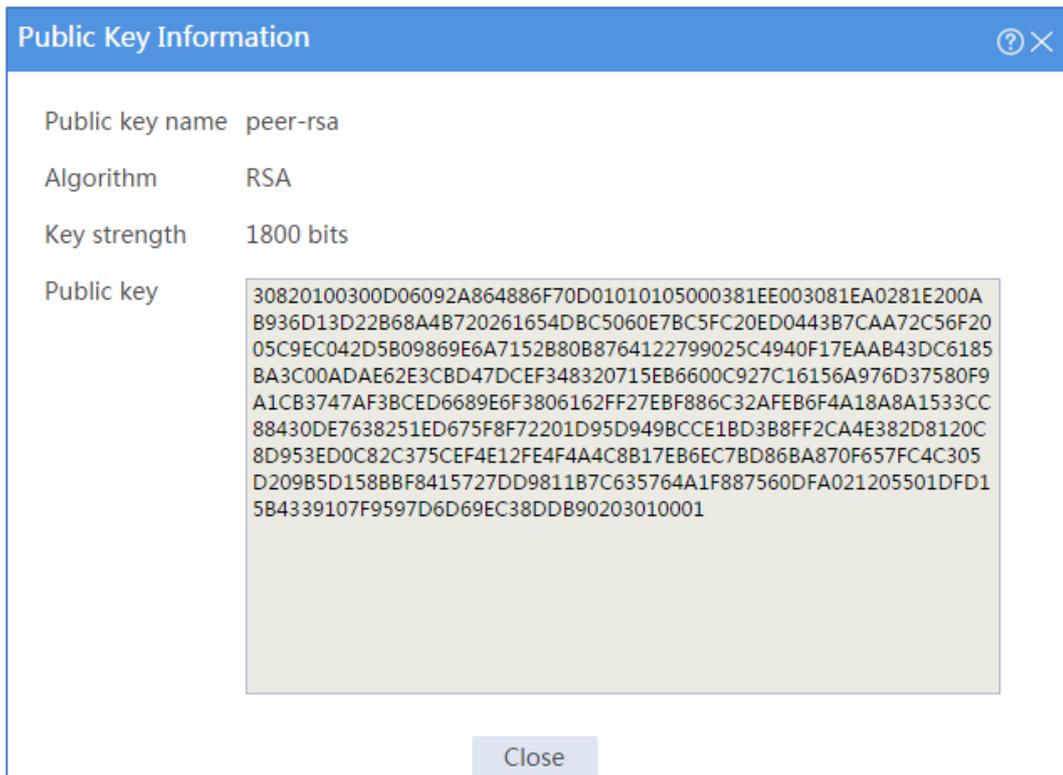
Key strength 1800 bits

Creation time 2018-09-12 10:27:01

Public key  
30820100300D06092A864886F70D01010105000381EE003081EA0281E200AB93  
6D13D22B68A4B720261654DBC5060E7BC5FC20ED0443B7CAA72C56F2005C9E  
C042D5B09869E6A7152B80B8764122799025C4940F17EAAB43DC61858A3C00A  
DAE62E3CBD47DCEF348320715EB6600C927C16156A976D37580F9A1CB3747AF  
3BCED6689E6F3806162FF27EBF886C32AFEB6F4A18A8A1533CC88430DE763825  
1ED675F8F72201D95D949BCCCE1BD3B8FF2CA4E382D8120C8D953ED0C82C375  
CEF4E12FE4F4A4C8B17EB6EC7BD86BA870F657FC4C305D209B5D158BBF841572  
7DD9811B7C635764A1F887560DFA021205501DFD15B4339107F9597D6D69EC3  
8DDB90203010001

2. デバイス B に設定されているピア公開キーに関する情報を表示します。  
#トップナビゲーションバーで、**Object** をクリックします。  
#ナビゲーションペインで、**Public Key Management > Peer Public Keys** を選択します。  
#公開キー **peer-rsa** の **Details** アイコンをクリックします。

図12 公開鍵ファイルからインポートされたピアホスト公開鍵



# セキュリティポリシーの設定例

## はじめに

次に、セキュリティポリシーの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、セキュリティポリシー機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

パケットフィルタリング(設定されている場合)は、どのセキュリティポリシールールにも一致しないパケットに対してのみ実行されます。ベストプラクティスとして、セキュリティポリシーには、パケットフィルタリングよりも厳しいフィルタリング基準が設定されていることを確認してください。これにより、一致しないパケットはパケットフィルタリングによってフィルタリングできます。

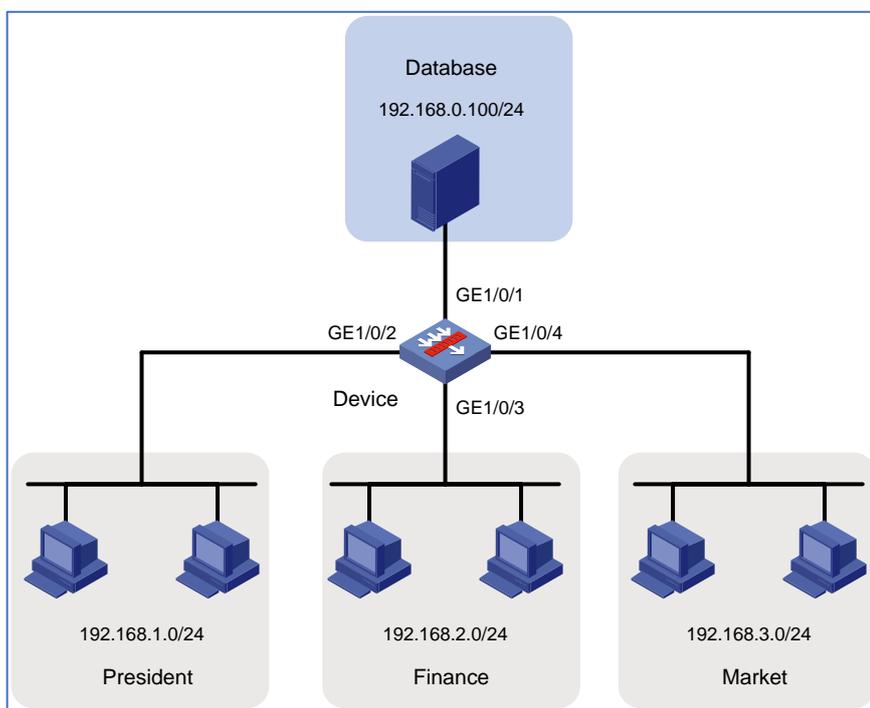
## 例:基本セキュリティポリシーの設定

### ネットワーク構成

図 1 に示すように、次の目標を達成するようにセキュリティポリシーを設定します。

- **President** オフィスは、HTTP を通じていつでも **financial** データベースサーバーにアクセスできる。
- **financial** オフィスは、平日の 8:00~18:00 に HTTP 経由で **financial** データベースサーバーにアクセスできます。
- **marketing** オフィスは、HTTP を介して **financial** データベースサーバーにいつでもアクセスできません。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** をクリックします。
  - #ナビゲーションペインで **Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **Edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
  - A) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、192.168.0.1/24と入力します。
  - B) **Ok** をクリックします。
  - #GE1/0/2、GE1/0/3、GE1/0/4の//3、GE1/0/4のIPアドレスをそれぞれ192.168.1.1/24、192.168.2.1/24、192.168.3.1/24に設定します。
2. セキュリティゾーンを作成します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Security Zones** を選択します。

#次のタスクを実行します。

- **database** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/1 を追加します。
- **president** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/2 を追加します。
- **finance** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/3 を追加します。
- **market** という名前のセキュリティゾーンを作成し、そのゾーンに GigabitEthernet1/0/4 を追加します。

3. 時間範囲を作成します。

#トップナビゲーションバーで、**Object** をクリックします。

#ナビゲーションペインで、**Object Groups > Time Ranges** を選択します。

#**Create** をクリックします。

#表示されるダイアログボックスで、名前 **work** と入力し、**Periodic time range** の **Create** をクリックします。

#表示されるダイアログボックスで、時間範囲を設定します。

- 開始時刻を **08:00** に設定します。
- 終了時刻を **18:00** に設定します。
- **Monday、Tuesday、Wednesday、Thursday**、および **Friday** を選択し

#**OK** をクリックします。

4. IPv4アドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、**object** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#次のタスクを実行します。

- IPv4 アドレスオブジェクトグループ **database** を作成し、サブネットアドレスが 192.168.0.0/24 の IPv4 アドレスオブジェクトをグループに設定します。

- IPv4 アドレスオブジェクトグループの **president** を作成し、サブネットアドレス 192.168.1.0/24 の IPv4 アドレスオブジェクトをグループに設定します。
  - IPv4 アドレスオブジェクトグループ **finance** を作成し、サブネットアドレス 192.168.2.0/24 の IPv4 アドレスオブジェクトをグループに設定します。
  - IPv4 アドレスオブジェクトグループ **market** を作成し、サブネットアドレス 192.168.3.0/24 の IPv4 アドレスオブジェクトをグループに設定します。
5. サービスオブジェクトグループを作成します。
- #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > Service Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、サービスオブジェクトグループを設定します。
    - A) グループ名を入力します。この例では、**web**と入力します。
    - B) **add**をクリックします。
    - C) 表示されるダイアログボックスで、オブジェクトグループ**http**を選択します。
    - D) **ok**をクリックします。
6. セキュリティゾーン **president** からセキュリティゾーン **database** へのセキュリティポリシーを作成し、**president** オフィスがいつでも HTTP を介してデータベースにアクセスできるようにします。
- #トップナビゲーションバーで、**Policies** をクリックします。
  - #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、図 2 に示すセキュリティポリシーを作成します。

図2 presidentオフィスのセキュリティポリシーを作成する

Create Security Policy

Name   Auto name

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User

Time range

VRF

Content security

WAF profile

OK Cancel

#OK をクリックします。

7. セキュリティゾーン **finance** からセキュリティゾーン **database** へのセキュリティポリシーを作成し、平日の 8:00 から 18:00 まで、財務オフィスが HTTP を介してデータベースにアクセスできるようにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、図 3 に示すセキュリティポリシーを作成します。

図3 financeオフィスのセキュリティポリシーを作成する

The screenshot shows a 'Create Security Policy' dialog box with the following fields and values:

- Name: finance-database
- Source zone: finance
- Destination zone: database
- Type: IPv4 (selected)
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Permit (selected)
- Source IP/MAC address: finance
- Destination IP: database
- Service: web
- Application: Select or enter applications
- User: Select or enter users
- Time range: work
- VRF: Select a public network
- Content security: WAF profile set to --NONE--

#OK をクリックします。

8. セキュリティゾーン **market** からセキュリティゾーン **database** のセキュリティポリシーを作成し、**marketing** オフィスがいつでも HTTP を介してデータベースにアクセスできないようにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、図3に示すセキュリティポリシーを作成します。

図3 marketingオフィスのセキュリティポリシーを作成する

Create Security Policy

Name   Auto naming

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User

Time range

VRF

Content security

OK Cancel

#OK をクリックします。

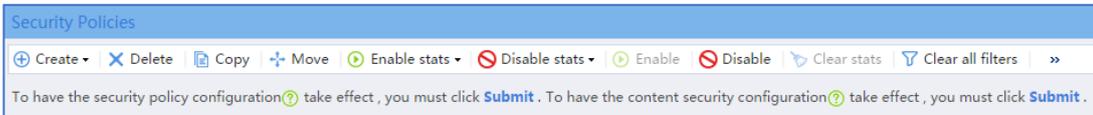
9. セキュリティポリシーをすぐに有効にするには、セキュリティポリシー一致アクセラレーションをアクティブにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#Activate(この例では最初の **Submit**)をクリックします。

図5 セキュリティポリシーマッチングアクセラレーションを有効にする



## 設定の確認

#各オフィスの PC を使用して、ブラウザから財務データベースサーバーの Web サービスにアクセスします。

#セキュリティポリシーが正しく設定されていることを確認します(図 6 を参照)。

図6 セキュリティポリシーの設定

<input type="checkbox"/>	Name	Src zone	Dst zone	Type	ID	Descr...	Src address	Dst address	Service	User	Action	Cont...	Matc...	Traffic	Enabl...	Enable	Edit
<input type="checkbox"/>	president-database	president	database	IPv4	4		president	database	web	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	finance-database	finance	database	IPv4	5		finance	database	web	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	market-database	market	database	IPv4	6		market	database	web	Any	Deny				<input type="checkbox"/>	<input checked="" type="checkbox"/>	

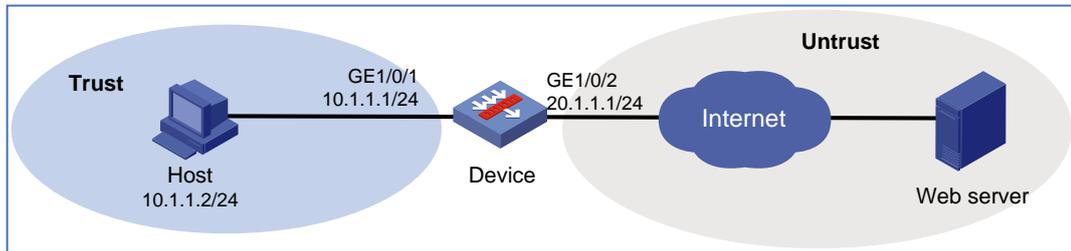
## 例:セキュリティポリシーとDPIの設定

### ネットワーク構成

図 7 に示すように、内部ネットワーク内のホストはデバイスを介してインターネットにアクセスします。次の設定でデバイスのセキュリティポリシーと DPI を設定します。

- 内部ネットワークからのデータパケットに対してアンチウイルス検出を実行し、パケットのウイルスをドロップします。
- ウイルス例外として ID90321 のウイルスを指定します。
- アプリケーション例外として RenMinWang を指定します。システムがウイルスを含むパケットを RenMinWang に許可し、アラームを生成できるようにします。

図7 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。
    - C) **ok** をクリックします。
  - #GE1/0/GE1/2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。
2. IPv4アドレスオブジェクトグループを作成します。
  - #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、サービスオブジェクトグループを設定します。
    - A) グループ名 **private** を入力します。
    - B) **add** をクリックします。
    - C) 表示されるダイアログボックスで、**network segment** オブジェクトを選択し、IPv4アドレスと

マスク長10.1.1.0/24を入力します。

D) **OK**をクリックします。

E) **Create IPv4 Object Group**ページで、**ok**をクリックします。

3. アンチウイルスプロファイルを作成します。

#トップナビゲーションバーで、**objects** をクリックします。

#ナビゲーションペインで、**APPSecurity > Anti-Virus > Profile** を選択します。

#**Create** をクリックします。

#表示されるダイアログボックスで、アンチウイルスプロファイルを作成します(図 8 を参照)。

図8 ウイルス対策プロファイルを作成する

**Create Anti-Virus Profile**

Name: antivirus (1-63 chars)

Description: (1-255 chars)

Enable cloud query:

Protocols: [dropdown]

Application exceptions

Name	Action
RenMinWang	Alarm

Total entries: 1

Virus exceptions

ID	Name
90321	Antivirus.360

Total entries: 1

By default, the action set for a protocol applies to all applications running over that protocol. To customize the action for an application, set the application as an application exception and select the action.

MD5 value exceptions

MD5 value
-----------

Enter MD5 value: [input] Add Delete

OK Cancel

A) **ok**をクリックします。

4. セキュリティポリシーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#図 9 と図 10 に表示されるダイアログボックスで、およびに示すセキュリティポリシーを作成します。

図9 基本セキュリティポリシー設定を作成する

**Create Security Policy** [?] [X]

Name ?  \*  Auto naming

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User

Time range

VRF

---

Content security

WAF profile

図10 コンテンツセキュリティ設定を構成する

Application: Select or enter applications [Edit]

User: Select or enter users

Time range: Select a time range

VRF: Select a public network

---

Content security

WAF profile: --NONE--

IPS profile: --NONE--

Data filtering profile: --NONE--

File filtering profile: --NONE--

Anti-virus profile: antivirus [Edit]

URL filtering profile: --NONE--

---

Logging:  Enable  Disable

Match counting:  Enable  Disable

Session aging:  Enable

Persistent session aging:  Enable

Policy status:  Enable  Disable

OK Cancel

#OKをクリックします。

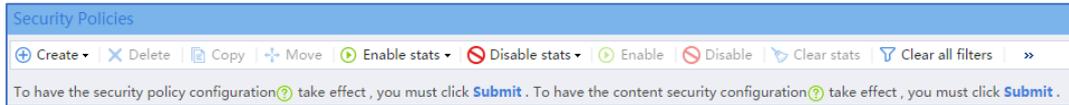
5. セキュリティポリシーをすぐに有効にするには、セキュリティポリシー一致アクセラレーションをアクティブにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

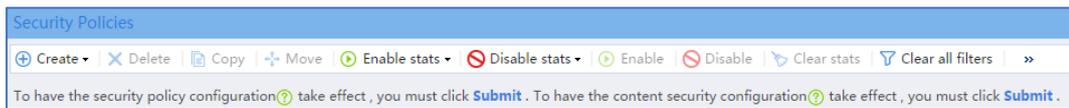
#**Activate**(この例では最初の **Submit**)をクリックします。

図 11 Acceleration に合致するセキュリティポリシーを Activate させる



- 設定を有効にするには、コンテンツセキュリティ設定を送信します。
  - #トップナビゲーションバーで、**Policies** をクリックします。
  - #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
  - #**Submit**(この例では 2 番目の **Submit**)をクリックします。

図 12 コンテンツセキュリティ設定の送信



## 設定の確認

#セキュリティポリシーが正しく設定されていることを確認します。

図 13 セキュリティポリシーの設定

Name	Src zone	Dist zone	Type	ID	Descri...	Src address	Dist address	Service	User	Action	Conte...	Matches	Traffic	Enable...	Enable	Edit
antivirus	Trust	Untrust	IPv4	7		private	Any	Any	Any	Permit	AV:antivi			<input type="checkbox"/>	<input checked="" type="checkbox"/>	

# 攻撃防御の設定例

## はじめに

次に、攻撃防御の設定例を示します。

次の攻撃防御機能がサポートされています。

### スキャン攻撃防御

スキャン攻撃検出は、ターゲットシステムへの接続の着信パケットレートを検査します。外部ネットワークに接続されているセキュリティゾーンにスキャン攻撃防御ポリシーを適用します。

### グローバルな flood 攻撃防御

外部ネットワークに接続されているセキュリティ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。

### IP固有のフラッド攻撃防御

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。非特定の IP アドレスに対しては、デバイスはグローバルなフラッド攻撃防御設定を使用します。

### 周知の単一パケット攻撃防御

単一パケット攻撃検出は、パケットシグニチャに基づいて着信パケットを検査します。外部ネットワークに接続されているセキュリティゾーンに単一パケット攻撃防御ポリシーを適用します。

### ユーザー定義の単一パケット攻撃防御

デバイスは、ユーザー定義シグニチャによる攻撃パケットの検出をサポートしています。

## 免除リスト

攻撃防御ポリシーは、ACL を使用して除外パケットを識別します。ポリシーは、ACL によって許可されたパケットをチェックしません。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

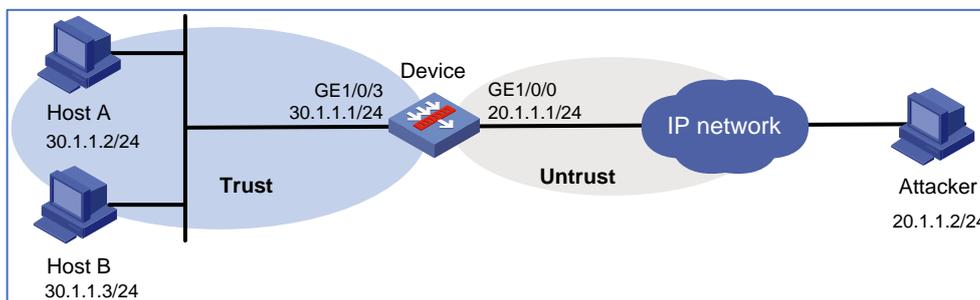
次の情報は、攻撃の検出と防御に関する基本的な知識があることを前提としています。

## 例: スキャン攻撃防御の設定

### ネットワーク構成

図1に示すように、GigabitEthernet1/0/0 が存在する Untrust セキュリティゾーンで、中間レベルのスキャン攻撃検出および防御を設定して、スキャン攻撃から内部ホストを保護します。防御アクションは、攻撃パケットのログギングおよびドロップです。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

# 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/0 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。
  1. **Basic Configuration**タブで、**Untrust**セキュリティゾーンを選択します。
  2. **IPv4 Address**タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、20.1.1.1/24と入力します。
  3. **OK**をクリックします。  
#GE1/0/ge1/3を追加し、GE1/0/0と同じ方法でIPアドレスを30.1.1.1/24に設定します。
  2. ゾーン Untrust からゾーン Trust へのセキュリティポリシーを作成します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。  
#**create** をクリックします。  
#開いたダイアログボックスで、セキュリティポリシーを設定します。
    - ポリシー名 **Untrust-Trust** を入力します。
    - ソースゾーン **Untrust** を選択します。
    - ターゲットゾーン **Trust** を選択します。  
#**OK** をクリックします。
3. スキャン攻撃防御ポリシーを設定します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Attack Defense > Attack Defense Policies** を選択します。  
#**create** をクリックします。  
#スキャン攻撃防御ポリシーを作成します(図2を参照)。

図2 スキャン攻撃防御ポリシーの作成

Policy name: atk1 (1-31 chars)

Apply to: Untrust [Edit]

Scanning Attack Defense | Flood Attack Defense Global Settings | IP-Specific Flood Attack Defense | Well-Known Sin

Detection sensitivity: Medium

Enable port scan attack prevention  
Threshold (packets): 40000 (1-1000000000)

Enable address scan attack prevention  
Threshold (packets): 40000 (1-1000000000)

Detection periodcycle: 10 seconds (1-1000000000. Default: 10.)

Actions:  Generate logs,  Drop attack packets,  Add attackers' IP addresses to blacklist

OK Cancel

#OK をクリックします。

攻撃防御ポリシーは、に示すように、攻撃防御ポリシーリストに表示されます。

図3 攻撃防御ポリシーリスト

Policy name	Apply to	Edit
atk1	Untrust	[Edit]

## 設定の確認

- 20.1.1.2のホストで、異なる宛先ポート番号を持つ多数のSYNパケットを宛先アドレス30.1.1.2に送信する攻撃をシミュレートします。
- ファイアウォールで、攻撃防御ログ情報を表示します。

#トップナビゲーションバーで **Monitor** をクリックします。

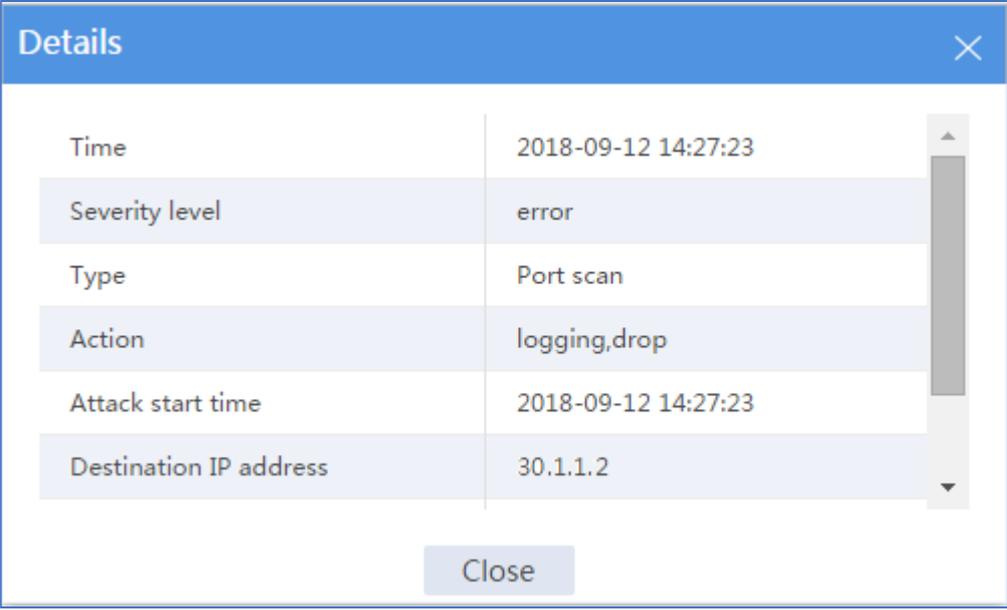
#ナビゲーションペインで、**Security Logs > Scanning Attack Logs** を選択します。

図4 スキャン攻撃ログリスト

Time	Severity/level	Type	Action	VPN name	Destination IP address	Attack start time
------	----------------	------	--------	----------	------------------------	-------------------

3. 攻撃ログをダブルクリックして詳細を表示します。

図5 スキャン攻撃ログに関する詳細情報



The screenshot shows a 'Details' dialog box with a blue header and a close button (X) in the top right corner. The dialog contains a table with the following information:

Time	2018-09-12 14:27:23
Severity level	error
Type	Port scan
Action	logging,drop
Attack start time	2018-09-12 14:27:23
Destination IP address	30.1.1.2

At the bottom center of the dialog is a 'Close' button.

4. SYNパケットがドロップされているため、SYNパケットのセッションが作成されていないことを確認します。

#トップナビゲーションバーで **Monitor** をクリックします。

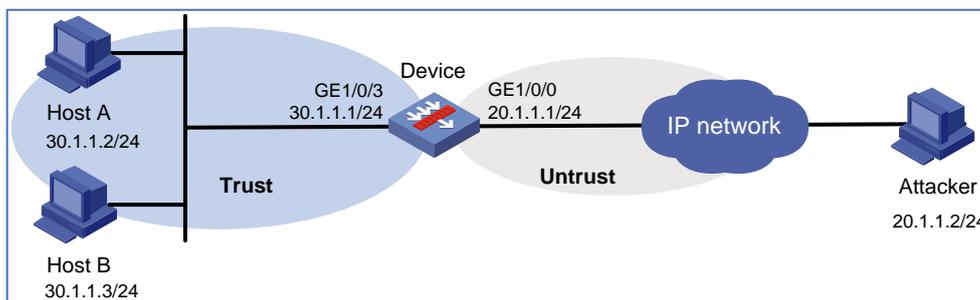
#ナビゲーションペインで、**Session** を選択します。

## 例:フラッド攻撃防御の設定

### ネットワーク構成

図 6 に示すように、内部ネットワークホストを SYN フラッド攻撃から保護するために、GigabitEthernet1/0/0 が存在するセキュリティゾーン内部ネットワークホストを SYN フラッド攻撃から保護します。ファイアウォールは、攻撃者が送信したパケット数が 1 秒あたり 1000 個以上に達したことを検出すると、ログを出力し、攻撃パケットをドロップします。

図 6 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/0 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、20.1.1.1/24 と入力します。  
C) **OK** をクリックします。  
#GE1/0/ge1//3 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 30.1.1.1/24 に設定します。
  2. ゾーン Untrust からゾーン Trust へのセキュリティポリシーを作成します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。  
#**create** をクリックします。  
#開いたダイアログボックスで、セキュリティポリシーを設定します。
11. ポリシー名 **Untrust-Trust** を入力します。
  12. ソースゾーン **Untrust** を選択します。

13. ターゲットゾーン **Trust** を選択します。

#**OK** をクリックします。

3. フラッド攻撃防御のグローバル設定。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Attack Defense > Attack Defense Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、攻撃防御ポリシーを作成します(図7を参照)。

図7 攻撃防御ポリシーの作成

Attack type	Threshold (pps)	Logg...	Detect all IPs	Client verif...	Pack...	Target ports
SYN	1000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
ACK	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SYN-ACK	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
RST	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
FIN	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
UDP	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
ICMP	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

#**OK** をクリックします。

攻撃防御ポリシーは、に示すように、攻撃防御ポリシーリストに表示されます。

図8 攻撃防御ポリシーリスト

Policy name	Apply to	Edit
atk1	Untrust	

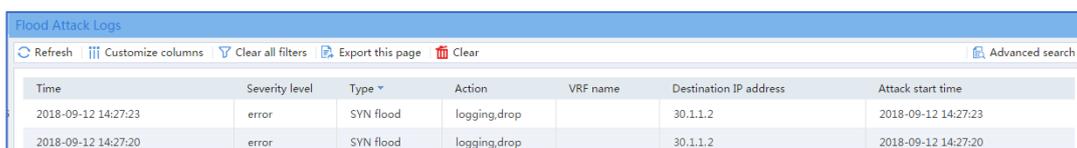
## 設定の確認

1. 20.1.1.2のホストで、送信元ポート番号が異なる多数のSYNパケットを宛先アドレス30.1.1.2に送信することにより、SYNフラッド攻撃をシミュレートします。
2. ファイアウォールで、フラッド攻撃ログ情報を表示します。

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Security Logs > Flood Attack Logs** を選択します。

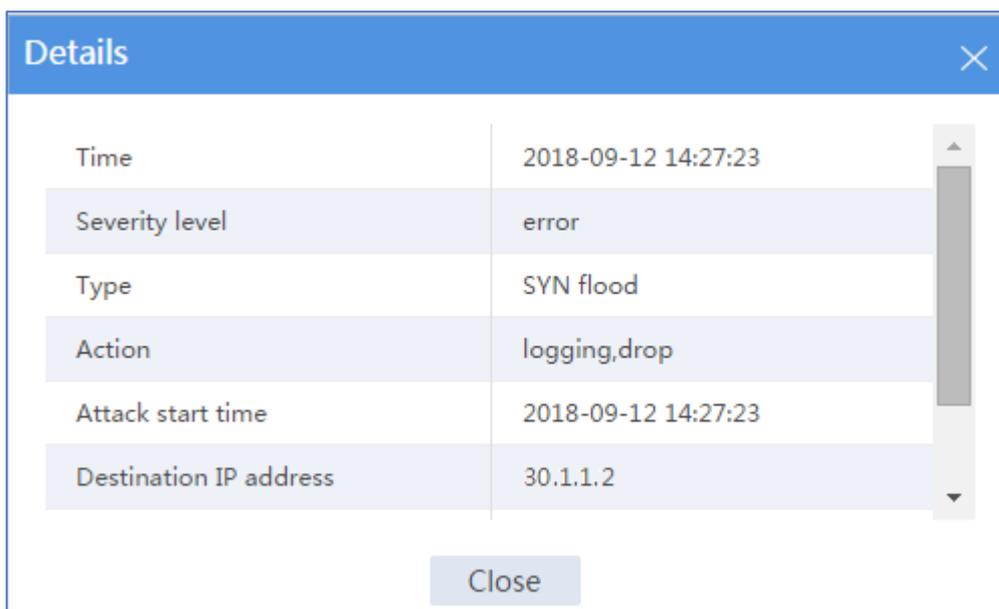
図9 フラッド攻撃ログリスト



Time	Severity level	Type	Action	VRF name	Destination IP address	Attack start time
2018-09-12 14:27:23	error	SYN flood	logging,drop		30.1.1.2	2018-09-12 14:27:23
2018-09-12 14:27:20	error	SYN flood	logging,drop		30.1.1.2	2018-09-12 14:27:20

3. フラッド攻撃ログをダブルクリックして、詳細を表示します。

図10 フラッド攻撃ログの詳細



Details	
Time	2018-09-12 14:27:23
Severity level	error
Type	SYN flood
Action	logging,drop
Attack start time	2018-09-12 14:27:23
Destination IP address	30.1.1.2

Close

4. SYNパケットがドロップされているため、SYNパケットのセッションが作成されていないことを確認します。

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Device Logs > Traffic Logs** を選択します。

# 接続制限の設定例

## はじめに

次に、接続制限の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、接続制限機能の基本的な知識があることを前提としています。

## 例:接続制限の設定

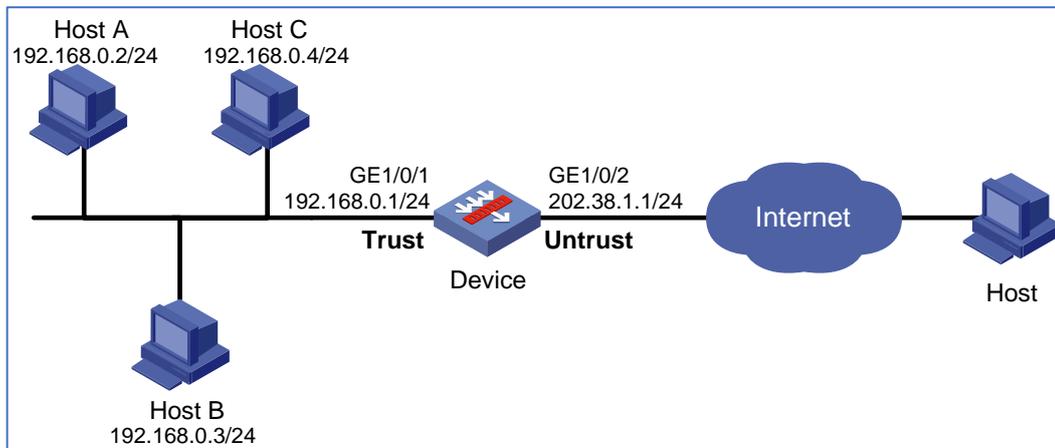
### ネットワーク構成

図1に示すように、ファイアーウォールは内部ネットワークをインターネットに接続する出力デバイスとして配置されます。

次の要件を満たすように接続制限を設定します。

- 192.168.0.0/24 上のすべてのホストは、合計で最大 100,000 のインターネット接続を確立できます。
- 192.168.0.0/24 上の各ホストは、最大 100 のインターネット接続を確立できます。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。
2. 接続制限ポリシーを設定します。
  - # トップナビゲーションバーで、Policies をクリックします。
  - # ナビゲーションペインで、Attack Defense > Connection Limit を選択します。
  - # create をクリックします。

図 2 接続制限ポリシー1 の作成

The screenshot shows a dialog box titled "Create Connection Limit Policy". The fields are as follows:

- Policy number:** A text input field containing the number "1". To the right of the field is a red asterisk and the text "(1-32)".
- IP version:** Two radio buttons are present. "IPv4" is selected with a blue dot, and "IPv6" is unselected.
- Apply to:** A dropdown menu is set to "Global". To the right of the dropdown is a "[Edit]" link.
- Description:** A large empty text area. To the right of the text area is the label "(1-127 chars)".
- Create rule:** A checkbox that is checked with a blue checkmark.

At the bottom of the dialog are two buttons: "OK" and "Cancel".

#開いたダイアログボックスで、接続制限ポリシー1 を設定します。

- ポリシー番号 1 を入力します。
- IP version は **IPv4** を選択します。
- **Apply to** フィールドで **Global** を選択します。
- **Create rule** を選択します。
- **OK** をクリックして接続制限規則を作成します。

#開いたダイアログボックスで、接続制限規則 1 を設定します。

- ルール ID1 を入力します。
- ACL2000 を選択します。この ACL は、ネットワークセグメント 192.168.0.0/24 上の送信元 IP アドレスと一致します。
- upper limit を 100000 に、lower limit を 95000 に設定します。
- **Limit by** フィールドで **Source IP** を選択します。

- Create more rule の選択を解除します。
- OK をクリックします。

図3 接続制限規則 1 の作成

Create IPv4 Connection Limit Rule

Rule ID: 1 (1-256)

ACL: 2000 \*

Connection establishment rate limit: (5-10000000)

Connection limits:

Upper limit: 100000 (1-4294967294)

Lower limit: 95000 (1-4294967294)

Limit by:

Source IP:

Destination IP:

Service port:

Action on upper limit exceeding:

Permit new connections  Deny new connections

Create more rule:

OK Cancel

#Create をクリックして、別の接続制限ポリシーを作成します。

図4 接続制限ポリシーの作成 2

Policy number 2 \*(1-32)

IP version  IPv4  IPv6

Apply to GE1/0/1 [Edit]

Description (1-127 chars)

Create rule

OK Cancel

#開いたダイアログボックスで、接続制限ポリシー2を設定します。

- ポリシー番号 2 を入力します。
- IP version は **IPv4** を選択します。
- **Apply to** フィールドで **GE1/0/1** を選択します。
- **Create rule** を選択します。
- OK をクリックして接続制限規則を作成します。

#開いたダイアログボックスで、接続制限規則 1 を設定します。

- ルール ID1 を入力します。
- ACL2000 を選択します。この ACL は、ネットワークセグメント 192.168.0.0/24 上の送信元 IP アドレスと一致します。
- upper limit を 100 に、lower limit を 95 に設定します。
- **Limit by** フィールドで **Source IP** を選択します。
- **Create more rule** の選択を解除します。

- **OK** をクリックします。

図5 接続制限規則 1 の作成

**Create IPv4 Connection Limit Rule**

Rule ID: 1 \*(1-256)

ACL: 2000 \*

Connection establishment rate limit:  (5-10000000)

Connection limits:

Upper limit: 100 (1-4294967294)

Lower limit: 95 (1-4294967294)

Limit by:

Source IP

Destination IP

Service port

Action on upper limit exceeding:  Permit new connections  Deny new connections

Create more rule

OK Cancel

設定後、接続制限ポリシーは次のように表示されます。

Policy description	IP version	Policy number	Rule count	Apply to	Edit
<input type="checkbox"/>	IPv4	1	1	Global	
<input type="checkbox"/>	IPv4	2	1	GE1/0/1	

## 設定の確認

#192.168.0.0/24 上のすべてのホストが合計 10 万までのインターネット接続を確立できること、および 192.168.0.0/24 上の各ホストが最大 100 までのインターネット接続を確立できることを確認します。

# IPS の設定例

## はじめに

次に、IPS の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、IPS 機能についての基本的な知識があることを前提します。

## 制限事項とガイドライン

IPS 機能をデバイス上で実行するには、ライセンスが必要です。ライセンスの期限が切れると、IPS はデバイス上の既存の IPS シグニチャライブラリを使用できますが、ライブラリは更新できません。

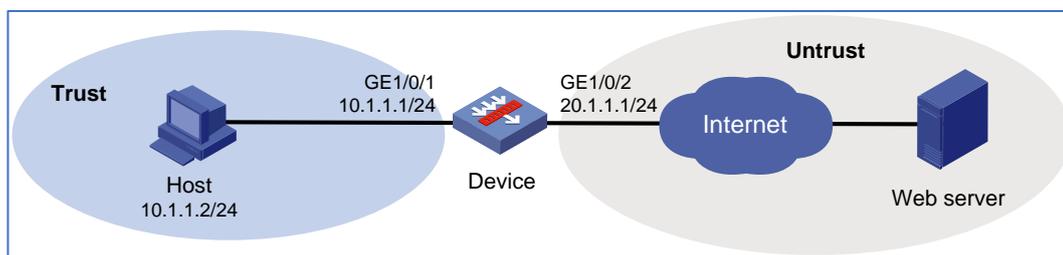
## 例:IPSの設定

### ネットワーク構成

図1に示すように、デバイスはセキュリティゲートウェイとして動作します。次の要件を満たすように IPS 機能を設定します。

- インターネットからの脆弱性およびマルウェア攻撃から内部ネットワークを保護します。
- IPS ルールに一致するアプリケーション(シグニチャ ID9 を含む)を内部ユーザーが使用できるようにします。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。  
C) **OK** をクリックします。  
#**Untrust** セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。
2. 内部IPアドレスオブジェクトグループを作成します。  
#トップナビゲーションバーで、**Object** をクリックします。  
#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。  
#**create** をクリックします。  
#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。  
A) グループ名を入力します。この例では、**private** と入力します。  
B) **add** をクリックします。  
C) 表示されるダイアログボックスで、**network segment**  
D) オブジェクトを選択し、IPv4アドレスとマスク10.1.1.0/24を入力します。

E) **OK**をクリックします。

3. IPSシグニチャライブラリを最新バージョンにアップデートします(詳細は省略)。

4. IPSプロファイルを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**APPSecurity > IPS > Profile** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、IPS プロファイルを設定します。

- **ips** という名前を入力します。
- **Signature filtering criteria** 領域で、次の設定を実行します。
  - 保護ターゲットに対して **all** を選択します。
  - 攻撃カテゴリに **Vulnerability and Malware** を選択します。
  - 方向に **To-server** と **To-client** を設定します。
  - drop、permit、reset、および blacklist のデフォルトアクションを設定します。
  - 重大度レベルを critical、high、medium、low に設定します。

図2 シグニチャフィルタリング基準の設定

**Create IPS Profile** [?] [X]

Name:  \* (1-63 chars)

---

**Signature filtering criteria**

The criteria are used to filter the signatures used by the IPS profile. By default, no criteria are configured and the IPS profile uses all enabled signatures in the system.

Protected target

- All
- OperationSystem
- NetworkDevice
- OfficeSoftware
- WebServer

Attack category

- All
- Vulnerability
- Malware
- InformationDisclosure
- ProtocolException

Direction

To-server     To-client

Default action

Drop     Permit     Reset     Blacklist

Severity level

Critical     High     Medium     Low

#Global profile action 領域で、アクションを設定します。

- アクションとして **drop** を設定
- ロギングを有効にします。

図3 グローバルプロファイルアクションコンフィギュレーション

Global profile action

Set the global profile action for traffic matching the signatures used by the profile.

Action: Drop

Logging:  Enable  Disable

Capture:  Enable  Disable

#Signature exceptions 領域で、Signature ID フィールドに 9 と入力し、Add をクリックします。

図4 シグニチャ例外の設定

Signature exceptions

To enable or disable a signature or set specific actions for the signature in the profile, configure the signature as a signature exception. The global profile action does not apply to signature exceptions.

Enter a signature ID  + Add  X Delete

<input type="checkbox"/>	Signature ID	Action	Status	Logging	Capture	Edit
<input type="checkbox"/>	9	Drop	✓	✓	⊖	

#このシグニチャの Edit アイコンをクリックします。

#開いたダイアログボックスで、アクションを permit に設定し、OK をクリックします。

図5 署名の例外編集

Edit Signature Exception

Signature ID: 9

Action: Permit

Status:  Enable  Disable

Logging:  Enable  Disable

Capture:  Enable  Disable

OK Cancel

#OK をクリックします。

5. ゾーン **Untrust** からゾーン **Trust** にセキュリティポリシーを作成し、ポリシーに IPS ファイルを使用します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **ips** を入力します。
- ソースゾーン **untrust** を選択します。
- ターゲットゾーンの **trust** を選択します。
- アクション **permit** を選択します。
- 宛先 IP アドレス **private** を選択します。
- IPS profile **ips** を選択します。

#OK をクリックします。

#**Submit** をクリックして、IPS プロファイル設定を有効にします。

## 設定の確認

IP S が内部ネットワークに対して次の保護を実装できることを確認します。

- 脆弱性およびマルウェア攻撃をログに記録し、ブロックします。
- IP S ルールに一致するアプリケーション(シグニチャ 9 を含む)を内部ユーザーが使用できるようにします。

これらのイベントに対して生成されたログを表示するには、上部ナビゲーションバーの **Monitor** をクリックし、ナビゲーションペインで **Security Logs > Threat Logs** を選択します。

# URL フィルタリングの設定例

## はじめに

次に、URL フィルタリングの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、URL フィルタリング機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

URL フィルタリング機能は、HTTP トラフィックのフィルタリングだけをサポートしています。

URL フィルタ機能をデバイス上で実行するには、ライセンスが必要です。ライセンスの期限が切れると、URL フィルタはデバイス上の既存の URL フィルタシングニチャライブラリを使用できますが、ライブラリは更新できません。

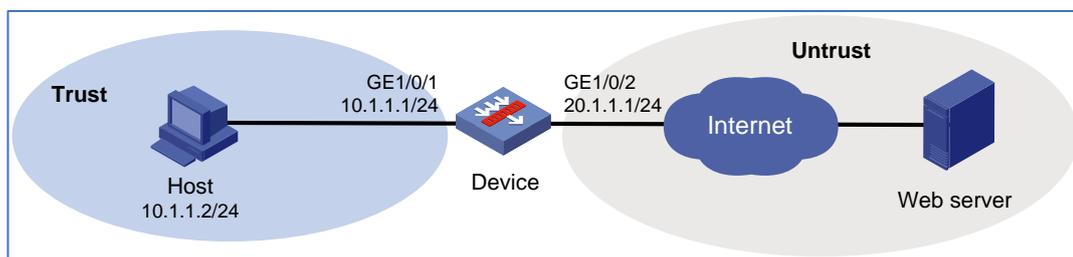
## 例:URLフィルタリングの設定

### ネットワーク構成

図1に示すように、セキュリティゲートウェイデバイスは企業ネットワークの境界に配置されます。デバイス上で URL フィルタリングを設定して、内部ユーザーの次のインターネットアクセス動作をブロックおよびログします。

- ショッピングサイトの **taobao** やアダルトサイトへのアクセス。
- **www.tudou.com** の Web サイトにアクセスします。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。
    - C) **OK** をクリックします。
  - #**Untrust** セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。
2. 内部IPアドレスオブジェクトグループを作成します。
  - #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。
    - A) グループ名を入力します。この例では、privateと入力します。
    - B) **add** をクリックします。
    - C) 表示されるダイアログボックスでネットワークセグメントオブジェクトを選択し、IPv4アドレスとマスク10.1.1.0/24を入力してOKをクリックします。

3. URLフィルタシグニチャライブラリを最新バージョンに更新します(詳細は省略)。
4. URLフィルタリングプロファイルを設定します。
  - #トップナビゲーションバーで、**object** をクリックします。
  - #ナビゲーションペインで、**APPSecurity > URL Filtering > Profiles** を選択します。
  - #create をクリックします。
  - #開いたダイアログボックスで、URL フィルタリングプロファイルを設定します。
    - A) 名前**urlfilter**を入力します。
    - B) デフォルトアクションとして**Permit**を選択します。
    - C) **Logging**オプションを選択します。
    - D) **blacklist**領域で、**add**をクリックします。
    - E) 表示されるダイアログボックスで、**Match pattern**リストから**text**を選択し、**Host name**フィールドに**www.tudou.com**と入力して**OK**をクリックします。

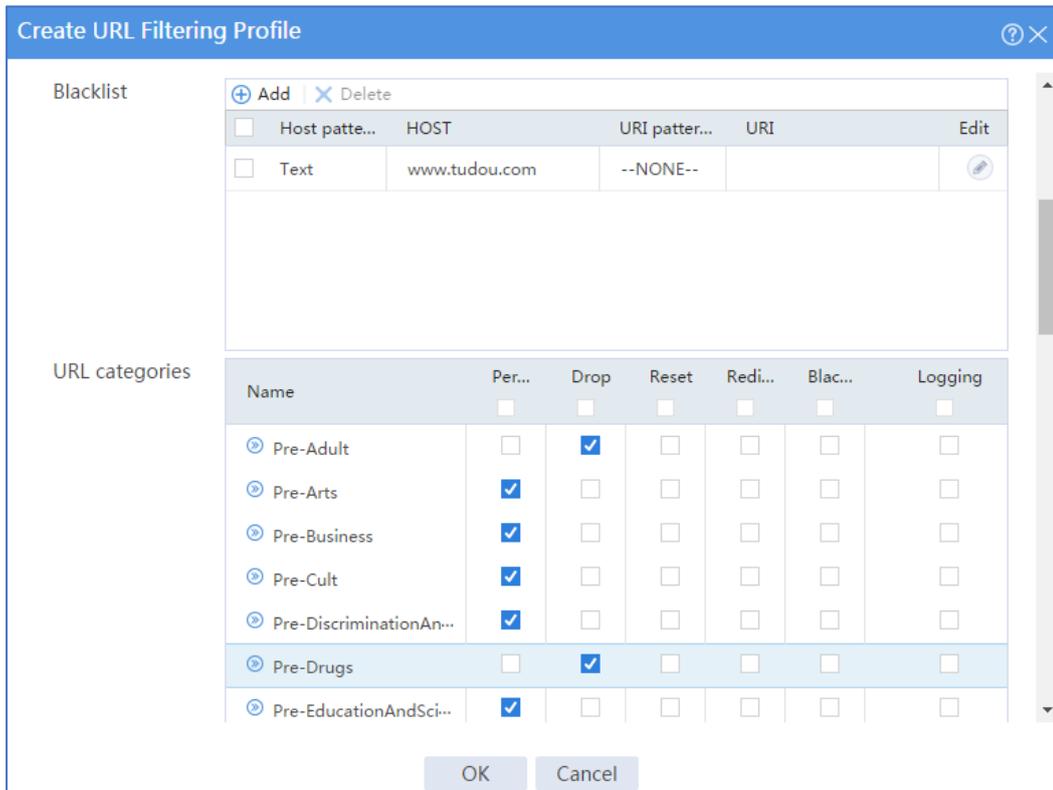
図24 Black list ルールの追加

The screenshot shows a dialog box titled "Add Blacklist Rule". It has a blue header bar with a question mark icon and a close button (X). The dialog contains the following fields and controls:

- Match pattern:** A dropdown menu with "Text" selected.
- Host name:** A text input field containing "www.tudou.com".
- Match pattern:** A second dropdown menu with "--NONE--" selected.
- URI:** An empty text input field.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

- F) **URL categories**領域で、ユーザー定義のURLカテゴリ**shopping**および事前定義のURLカテゴリ**Pre-Adult**の**Logging**アクションを選択します。
- G) **OK**をクリックします。

図3 URLフィルタリングプロファイルの設定



5. ゾーン **Untrust** からゾーン **Trust** にセキュリティポリシーを作成し、URL フィルタリングプロファイル **urlfilter** をポリシーに割り当てます。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **urlfilter** を入力します。
- ソースゾーン **Untrust** を選択します。
- ターゲットゾーンの **Trust** を選択します。
- アクション **Permit** を選択します。
- 送信元 IP アドレス **private** を選択します。
- **Content security** 領域で URL フィルタリングプロファイル **urlfilter** を選択します。

#**OK** をクリックします

#URL Filtering Profiles ページで **Submit** をクリックして、URL フィルタリングプロファイルを有効にします。

## 設定の確認

URL フィルタリングによって、内部ユーザーの次のインターネットアクセス動作がログに記録され、ブロックされることを確認します。

- ショッピングサイトのタオバオやアダルトサイトへのアクセス。
- **www.tudou.com** の Web サイトにアクセスします。

これらの動作に対して生成されたログを表示するには、トップナビゲーションバーの **Monitor** をクリックし、ナビゲーションペインで **Security Logs > URL Filtering Logs** を選択します。

# アンチウイルスの設定例

## はじめに

次に、アンチウイルスの設定例を示します。

アンチウイルス機能は、次のアプリケーションプロトコルをサポートしています。

- FTP
- HTTP
- IMAP
- NFS
- POP3
- SMB
- SMTP

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、ウイルス対策機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

アンチウイルス機能をデバイス上で実行するにはライセンスが必要です。ライセンスの期限が切れると、アンチウイルスはデバイス上の既存のウイルスシグニチャーライブラリーを使用できますが、ライブラリーは更新できません。

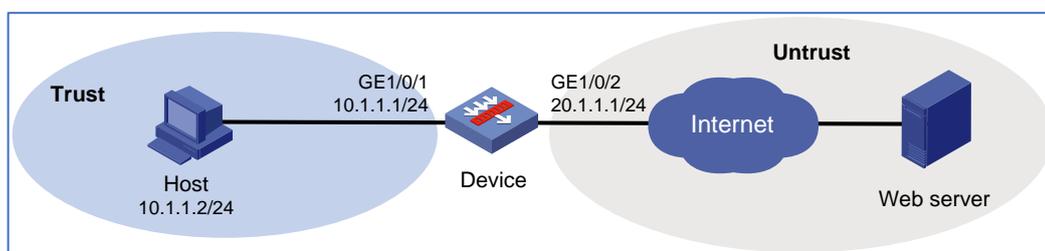
# 例:アンチウイルスの設定

## ネットワーク構成

図1に示すように、セキュリティゲートウェイデバイスは企業ネットワークの境界に配置されます。内部ユーザーは、インターネット上の Web サーバーと電子メールサーバーを使用して、ファイルと電子メールを転送する必要があります。

企業ネットワークを保護するために、内部ユーザーによって転送されたファイルおよび電子メールに対してウイルス検出を実行するように、デバイスにアンチウイルスを設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。  
C) **OK** をクリックします。

#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1./24 に設定します。

2. 内部IPアドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、**object** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。

A) グループ名を入力します。この例では、**private**と入力します。

B) **add**をクリックします。

C) 表示されるダイアログボックスで、**Network segmnet**オブジェクトを選択し、IPv4アドレスとマスク**10.1.1.0/24**を入力して、**OK**をクリックします。

3. ウイルスシグニチャーライブラリーを最新バージョンに更新します(詳細は省略)。

4. アンチウイルスプロファイルを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**APPSecurity > Anti-Virus > profile** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、アンチウイルスプロファイルを設定します。

A) 名前**antivirus**を入力します。

B) Protocols領域で、ファイル転送プロトコルおよびメールプロトコルのアンチウイルス保護を設定します(図2を参照)。

- FTP プロトコルの **Upload** および **Download** オプションのチェックボックスをオフにします。
- SMTP および POP3 メールプロトコルのアクションを **Block** に設定します。

C) **OK**をクリックします。

図 ウイルス対策プロファイルの作成

Create Anti-Virus Profile

Name: antivirus (1-63 chars)

Description: (1-255 chars)

Enable cloud query:

Protocols

File transfer protocols

Protocol	Upload	Download	Action
HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block
FTP	<input type="checkbox"/>	<input type="checkbox"/>	Block

Mail protocols

Protocol	Upload	Download	Action
SMTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Block
POP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Block
IMAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alarm

File sharing protocols

Protocol	Upload	Download	Action
NFS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block
SMB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block

Application exceptions: Please select an application

Virus exceptions: Please enter virus ID

OK Cancel

5. ゾーン **trust** からゾーン **untrust** までのセキュリティポリシーを作成し、そのポリシーにアンチウイルスプロファイル **antivirus** を割り当てます。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

(ア) ポリシー名 **anti-virus** を入力します。

(イ) ソースゾーンの **Trust** を選択します。

(ウ) 宛先ゾーン **Untrust** を選択。

(エ) アクション **permit** を選択します。

(オ) 送信元 IP アドレス **private** を選択します。

(カ) **Content security** 領域で **anti-virus profile antivirus** を選択します。

#OK をクリックします

#Anti-Virus Profile ページで、**submit** をクリックしてアンチウイルスプロファイルを有効にします。

## 設定の確認

企業ネットワークを保護するために、内部ユーザーによって送信されるウイルスに感染したファイルと電子メールをアンチウイルスが検出してブロックすることを確認します。

アンチウイルスによって生成された脅威ログを表示するには、トップナビゲーションバーの **Monitor** をクリックし、ナビゲーションペインで **Security Logs > Threat Logs** を選択します。

# データフィルタリングの設定例

## はじめに

次に、データフィルタリングの設定例を示します。

データフィルタは、アプリケーションレイヤー情報に基づいてパケットをフィルタします。データフィルタを使用すると、内部情報の漏洩、違法な情報の配布および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。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、データフィルタリング機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

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
- HTTPS
- FTP
- SMTP
- IMAP
- NFS
- Pop 3
- RTMP

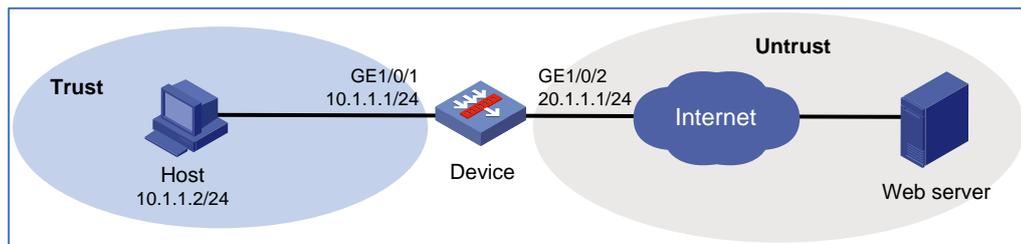
## 例:データフィルタリングの設定

### ネットワーク構成

図 1 に示すように、セキュリティゲートウェイデバイスは企業ネットワークの境界に配置されます。デバイス上でデータフィルタリングを設定して、内部ユーザーの次のインターネットアクセス動作をブロックおよび記録します。

- インターネットでの **illegal** キーワードを含む情報の閲覧、公開、またはダウンロード。
- インターネットでのみ内部使用としてマークされているファイルを転送する。

図 1 ネットワーク図



### 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、**10.1.1.1/24** と入力します。

C) **OK**をクリックします。

#**Untrust** セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1./24 に設定します。

2. 内部IPアドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、**object** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。

A) グループ名を入力します。この例では、**private**と入力します。

B) **add**をクリックします。**Create object**ダイアログボックスが開きます。

C) **Network Segment**オブジェクトを選択し、IPv4アドレスとマスク10.1.1.0/24を入力して、**OK**をクリックします。

3. キーワードグループを設定します。

#キーワードグループ **keywordgroup1** を作成します。

A) 上部のナビゲーションバーで、**object**をクリックします。

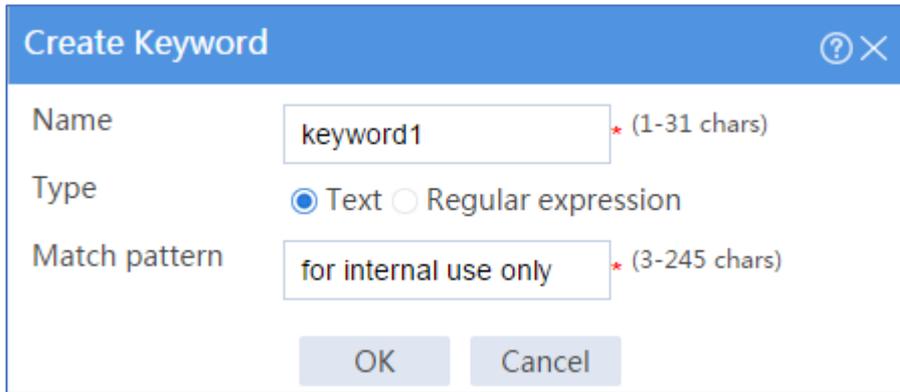
B) ナビゲーションペインで、**APPSecurity > Data Filtering > Keywork Group** を選択します。

C) **create**をクリックします。

D) 表示されるダイアログボックスで、キーワードグループを設定します。

- **name** フィールドに **keywordgroup1** と入力します。
- **User defined keyword list** 領域で、**Create** をクリックします。
- **Create keyword** ダイアログボックスで、**name** フィールドに **keyword1** と入力し、**text** タイプを選択して、**match pattern** フィールドに **for internal use only** と入力します。
- **OK** をクリックします。

図 2 キーワードの作成



The image shows a dialog box titled "Create Keyword". It has a blue header bar with the title and a close button. The main area contains three fields: "Name" with the text "keyword1" and a character limit of "(1-31 chars)", "Type" with radio buttons for "Text" (selected) and "Regular expression", and "Match pattern" with the text "for internal use only" and a character limit of "(3-245 chars)". At the bottom are "OK" and "Cancel" buttons.

新しく作成されたキーワード **keyword1** が **Create Keyword Group** ダイアログボックスに表示されます。

図 3 キーワードグループ keywordgroup1 の作成

**Create Keyword Group**

Name:  (1-31 chars)

Description:  (1-255 chars)

---

**Pre defined keyword list**

Name	Description	Enable
Phone	Phone number	<input type="checkbox"/>
Bank card	Bank card number	<input type="checkbox"/>
Credit card	Credit card number	<input type="checkbox"/>
ID card	ID card number	<input type="checkbox"/>

---

**User defined keyword list**

<input type="checkbox"/>	Name	Type	Match pattern	Edit
<input type="checkbox"/>	keyword1	Text	for internal use only	<input type="button" value="Edit"/>

Total entries: 1 undefined

E) **OK**をクリックします。

#キーワードグループ keywordgroup2 を作成します。

A) キーワードグループページで、createをクリックします。

B) 表示されるダイアログボックスで、キーワードグループを設定します。

— name フィールドに **keywordgroup2** と入力します。

— **User defined keyword list** 領域で、**Create** をクリックします。

— **Create keyword** ダイアログボックスで、name フィールドに **keyword2** と入力し、**text** タイプを選択して、**match pattern** フィールドに **illegal** と入力します。

- OK をクリックします。

図 14 キーワードの作成

The image shows a 'Create Keyword' dialog box. The title bar is blue and contains a question mark icon and a close button. The dialog has three main sections: 'Name' with a text input field containing 'keyword2' and a character count '(1-31 chars)'; 'Type' with two radio buttons, 'Text' being selected and 'Regular expression' being unselected; and 'Match pattern' with a text input field containing 'illegal' and a character count '(3-245 chars)'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

新しく作成されたキーワード **keyword2** が **Create Keyword Group** ダイアログボックスに表示されます。

図 15 キーワードグループ keywordgroup2 の作成

**Create Keyword Group**

Name:  \* (1-31 chars)

Description:  (1-255 chars)

---

**Pre defined keyword list**

Name	Description	Enable
Phone	Phone number	<input type="checkbox"/>
Bank card	Bank card number	<input type="checkbox"/>
Credit card	Credit card number	<input type="checkbox"/>
ID card	ID card number	<input type="checkbox"/>

---

**User defined keyword list**

Create  Delete

<input type="checkbox"/>	Name	Type	Match pattern	Edit
<input type="checkbox"/>	keyword2	Text	illegal	

Total entries: 1 undefined

OK Cancel

E) **OK**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設定します。  
#トップナビゲーションバーで、**object** をクリックします。  
#ナビゲーションペインで、**APPSecurity > Data Filtering > profile** を選択します。  
#**create** をクリックします。  
#開いたダイアログボックスで、データフィルタリングプロファイルを設定します。
  - A) **datafilter**という名前を入力します。
  - B) **Data filtering rules**領域で、**Create**をクリックします。
  - C) 表示されるダイアログボックスで、データフィルタリング規則**rule1**を作成し(を参照)、**OK**をクリックします。

図 6 データ規則 rule1 の作成

Create Data Filtering Rule

Name  \* (1-31 chars)

Keyword group

Applications

Direction

Action  Permit  Drop

Logging  Enable  Disable

OK Cancel

- D) データフィルタリング規則rule1を設定するのと同じ方法で、データフィルタリング規則rule2を作成します(図7を参照)

図7 データ規則 rule2 の作成

Create Data Filtering Rule

Name: rule2 \* (1-31 chars)

Keyword group: keywordgroup2

Applications: All

Direction: Both

Action:  Permit  Drop

Logging:  Enable  Disable

OK Cancel

**Create Data Filtering Profile** ダイアログボックスに、データフィルタリングルールが表示されま  
す(図8を参照)

E) **OK**をクリックします。

図8 データフィルタリングプロファイルの作成

Create Data Filtering Profile

Name: datafilter \* (1-31 chars)

Description: (1-255 chars)

Data filtering rules

<input type="checkbox"/>	Name	Keyword group	Applications	Direction	Action	Logging	Edit
<input type="checkbox"/>	rule1	keywordgroup1	All	Upload	Drop	Enable	
<input checked="" type="checkbox"/>	rule2	keywordgroup2	All	Both	Drop	Enable	

Total entries: 2undefined

OK Cancel

5. **trust** ゾーン信頼からゾーン **Untrust** にセキュリティポリシーを作成し、データフィルタリングプロフ  
ファイル **datafilter** をポリシーに割り当てます。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **datafilter** を入力します。
- ソースゾーンの **trust** を選択します。
- 宛先ゾーン **untrust** を選択。
- アクション **permit** を選択します。
- 送信元 IP アドレス **private** を選択します。
- **Content security** 領域でデータフィルタリングプロファイル **datafilter** を選択します。

#**OK** をクリックします。

#**Data Filtering Profiles** ページで、**submit** をクリックしてデータフィルタリングプロファイルを有効にします。

## 設定の確認

データフィルタリングによって、内部ユーザーの次のインターネットアクセス動作がログに記録され、ブロックされることを確認します。

- インターネットでの **illegal** キーワードを含む情報の閲覧、公開、またはダウンロード。
- インターネットでのみ内部使用としてマークされているファイルを転送する。

これらの動作に対して生成されたログを表示するには、トップナビゲーションバーの **Monitor** をクリックし、ナビゲーションペインで **Device Logs > System Logs** を選択します。

# ファイルフィルタリングの設定例

## はじめに

以下に、ファイルフィルタリングの設定例を示します。

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。ファイルフィルタを構成して、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
- HTTPS
- FTP
- SMTP
- IMAP
- NFS
- POP3
- RTMP
- SMB

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、ファイルフィルタリング機能に関する基本的な知識があることを前提としています。

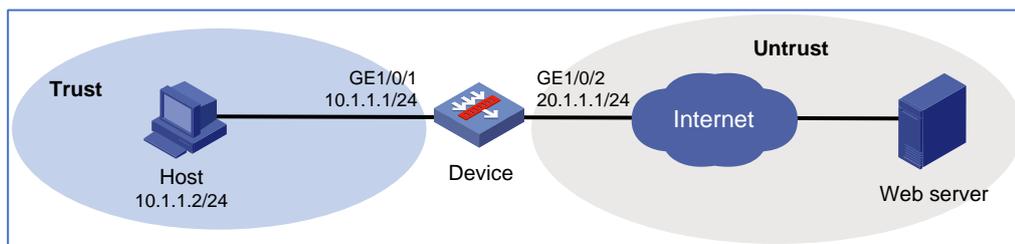
# 例:ファイルフィルタリングの設定

## ネットワーク構成

図 1 に示すように、セキュリティゲートウェイデバイスは企業ネットワークの境界に配置されます。デバイス上でファイルフィルタリングを設定して、内部ユーザーのファイル転送動作を制御します。

- 共通ファイルおよび圧縮ファイルのインターネットへのアップロードをブロックして、内部情報漏洩のリスクを軽減します。
- Web サーバーからの Windows 実行可能ファイルのダウンロードをブロックして、企業ネットワークにウイルスが侵入するリスクを軽減します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。  
C) **OK** をクリックします。

#**Untrust** セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1./24 に設定します。

2. 内部IPアドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#**create** をクリックします。**Create IPv4 Address Object Group** の作成ダイアログボックスが開きます。

#IPv4 アドレスオブジェクトグループを設定します。

A) グループ名を入力します。この例では、**private**と入力します。

B) **Add**をクリックします。**Create Object**ダイアログボックスが開きます。

C) **Network segment**オブジェクトを選択し、IPv4アドレスとマスク10.1.1.0/24を入力して、**OK** をクリックします。

3. ファイルタイプグループを設定します。

#ファイルタイプグループ **filetype1** を次のように作成します。

A) 上部のナビゲーションバーで、**Objects**をクリックします。

B) ナビゲーションペインで、**APPSecurity > File Filtering > File Type Group**を選択します。

C) **create**をクリックします。

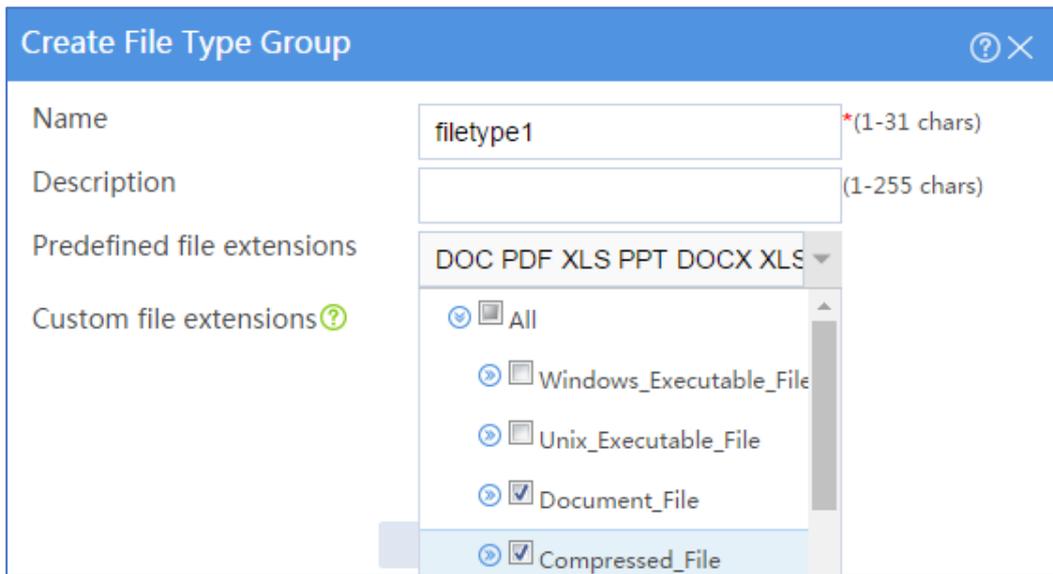
D) 表示されるダイアログボックスで、ファイルタイプグループを設定します。

— **Name** フィールドに **filetype1** と入力します。

— **Predefined file extensions** リストから、**Compressed\_File** と **Document\_File** を選択します。

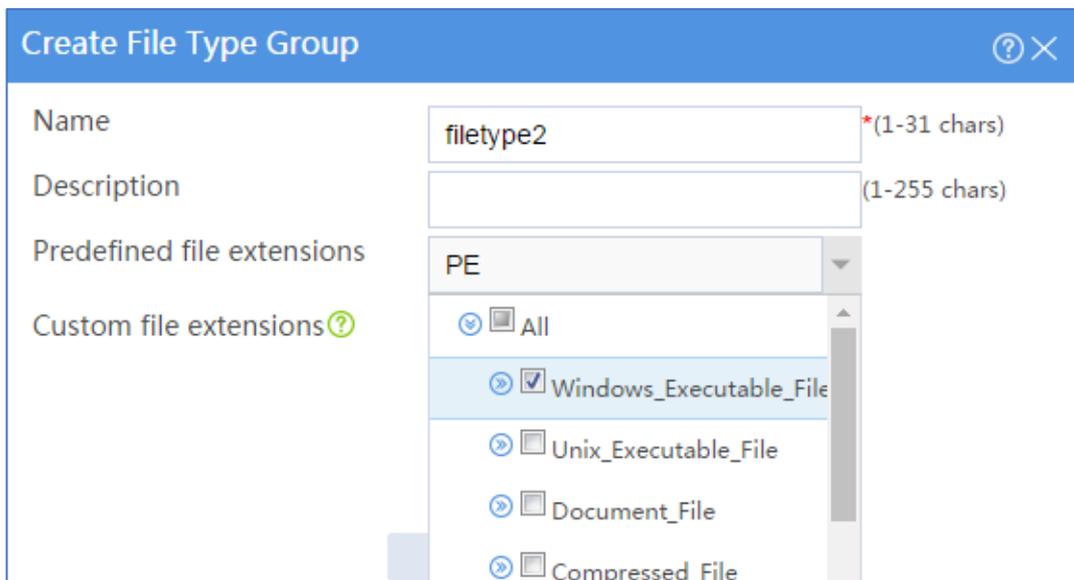
— **OK** をクリックします。

図2 ファイルタイプグループ filetype1 を作成しています



#Windows\_Executable\_File 事前定義ファイル拡張子を選択して、ファイルタイプグループ filetype2 を作成します。

図3 ファイルタイプグループ filetype2 を作成しています



4. ファイルフィルタリングプロファイルを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、APPSecurity > **file filtering** > **profile** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、ファイルフィルタリングプロファイルを設定します。

- A) 名前filefilterを入力します。
- B) **File filtering rules**領域で、**Create**をクリックします。
- C) 表示されるダイアログボックスで、ファイルフィルタリング規則rule1をに示すように設定し、**OK**をクリックします。

図4 ファイルフィルタリング規則 rule1 の作成

The screenshot shows a dialog box titled "Create File Filtering Rule". The fields are as follows:

Name	rule1	* (1-31 chars)
Applications	HTTP	
File type groups	filetype1	
Direction	Upload	
Action	<input type="radio"/> Permit	<input checked="" type="radio"/> Drop
Logging	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

Buttons: OK, Cancel

- D) ファイルフィルタリング規則rule1を設定するのと同じ方法で、ファイルフィルタリング規則rule2を作成します(図5を参照)。

図5 ファイルフィルタリング規則 rule2 の作成

**Create File Filtering Rule**

Name: rule2 (1-31 chars)

Applications: HTTP

File type groups: filetype2

Direction: Download

Action:  Permit  Drop

Logging:  Enable  Disable

OK Cancel

**Create File Filtering Profile** ダイアログボックスにファイルフィルタリングルールが表示されます (図6を参照)。

E) **OK**をクリックします。

図6 ファイルフィルタリングプロファイルの作成

**Create File Filtering Profile**

Name: filefilter (1-31 chars)

Description: (1-255 chars)

File filtering rules

<input type="checkbox"/>	Name	Applications	File type grou...	Direction	Action	Logging	Edit
<input type="checkbox"/>	rule1	HTTP	filetype1	Upload	Drop	Enable	
<input type="checkbox"/>	rule2	HTTP	filetype2	Download	Drop	Enable	

Total entries: 2

OK Cancel

- ゾーン **Trust** からゾーン **Untrust** にセキュリティポリシーを作成し、ファイルフィルタリングプロファイル **filefilter** をポリシーに割り当てます。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **filefilter** を入力します。
- ソースゾーンの **Trust** を選択します。
- 宛先ゾーンの **Untrust** を選択します。
- アクション **Permit** を選択します。
- 送信元 IP アドレス **Private** を選択します。
- **Content security** 領域でファイルフィルタリングプロファイル **filefilter** を選択します。

#**OK** をクリックします

#**File Filtering Profiles** ページで、**Submit** をクリックしてファイルフィルタリングプロファイルを有効にします。

## 設定の確認

内部ユーザーがドキュメントファイルまたは圧縮ファイルをインターネットにアップロードできないこと、または Windows 実行可能ファイルを Web サーバーからダウンロードできないことを確認します。

ファイルフィルタリングログを表示するには、トップナビゲーションバーの **Monitor** をクリックし、ナビゲーションペインで **Security Logs > File Filtering Logs** を選択します。

# APR ベースのセキュリティポリシー設定例

## はじめに

次に、APR ベースのセキュリティポリシーの設定例を示します。

セキュリティポリシーでは、転送制御と Deep Packet Inspection(DPI)に関する一連の規則を定義します。このポリシーでは、パケットを規則と照合し、照合されたパケットに対して規則で指定されたアクションを実行します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、APR およびセキュリティポリシー機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

パケットフィルタリング(設定されている場合)は、どのセキュリティポリシールールにも一致しないパケットに対してのみ実行されます。ベストプラクティスとして、セキュリティポリシーには、パケットフィルタリングよりも厳しいフィルタリング基準が設定されていることを確認してください。これにより、一致しないパケットはパケットフィルタリングによってフィルタリングできます。

セキュリティ上の理由から、APR ベースの厳密なセキュリティポリシーを設定します。

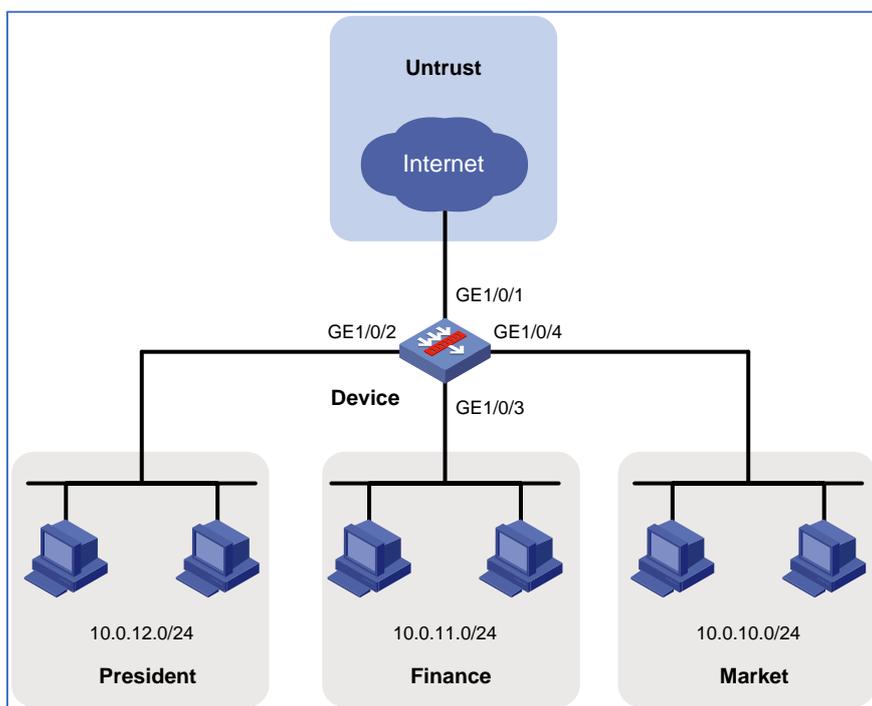
# 例:APRベースの厳密なセキュリティポリシー の設定

## ネットワーク構成

図1に示すように、次の目標を達成するようにセキュリティポリシーを設定します。

- 社長室はいつでもすべてのネットワークリソースにアクセスできます。
- 財務オフィスは、それ自体のリソースにしかアクセスできません。
- マーケティングオフィスは、勤務日の 8:00 から 18:00 まで、インターネット上のリソースにアクセスできます。
  - ゲーム、ストリーミングメディア、P2P、またはネットワークコミュニティリソースにはアクセスできませんが、YouKu にはアクセスできます。
  - WeChat だけにアクセスでき、他の IM アプリケーションにはアクセスできない。
  - MSN、DingTalk、およびセキュリティフォーラムのリソースにアクセスできます。
  - リストされているアクセスできないリソース以外のすべてのリソースにアクセスできます。
- 誰も金融オフィスにアクセスできず、金融オフィスとマーケティングオフィスは互いにアクセスできません。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

セキュリティポリシーを設定する場合は、次の制限事項およびガイドラインに従ってください。

- APR 署名ライブラリを最新バージョンに更新します。
- セキュリティポリシー内のアプリケーションを識別するには、アプリケーションの依存プロトコルを通過させる必要があります。

## 分析

- セキュリティポリシー **president\_permit** を設定して、社長室の従業員が任意のネットワークリソースに自由にアクセスできるようにします。

- セキュリティポリシー**finance\_permit**を構成して、財務オフィスの従業員が相互に通信できるようにします。
- セキュリティポリシー**market\_permit1**を構成して、マーケティングオフィスの従業員が WeChat、MSN、Dingtalk、YouKu およびセキュリティフォーラムのリソースを使用できるようにします。デフォルトでは、セキュリティポリシーは IM アプリケーションの使用を許可しません。
- 営業日の 8:00 から 18:00 まで、マーケティングオフィスのネットワークコミュニティおよびストリーミングメディアアプリケーションを拒否するように、セキュリティポリシー**market\_deny1**を設定します。このセキュリティポリシーにより、マーケティングオフィスの従業員は、営業日の 8:00 から 18:00 まで、ゲームをしたり、ビデオを見たり、ネットワークコミュニティサイトにアクセスしたりできなくなります。WeChat、MSN、Dingtalk、YouKu、およびセキュリティフォーラムアプリケーションを許可するには、**market\_deny1**の前にセキュリティポリシー**market\_permit1**を設定する必要があります。
- セキュリティポリシー**market\_permit2**を構成して、マーケティングオフィスの従業員が簡単に識別できない OA、電子メールおよびプロトコルアプリケーションを使用できるようにします。このようなアプリケーションを拒否するには、アプリケーショングループからアプリケーションを削除するか、別のセキュリティポリシーを構成して拒否します。
- セキュリティポリシー**market\_permit3**を構成して、APR でアプリケーションを正しく識別するための共通プロトコルを許可します。共通プロトコルには、TCP、UDP、DNS、HTTP、HTTPS、SMTP、IMAP および POP3 が含まれます。セキュリティポリシー**market\_permit2**は、これらのプロトコルを許可する場合があります。セキュリティポリシー**market\_permit2**の変更時にアプリケーションを正しく識別するための APR のベストプラクティスとして、これらのプロトコルを許可するようにセキュリティポリシー**market\_permit3**を構成します。
- セキュリティポリシーを次の順序で設定します。
  - A) **President\_permit**
  - B) **Finance\_permit**
  - C) **market\_permit1**

- D) market\_deny1
- E) market\_permit2
- F) market\_permit3

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、2.2.2.1/24と入力します。
    - B) **OK** をクリックします。
  - #GE1/0/2、GE1/0/3、1//2、GE1/0/3、GE1/0/4 の IP アドレスをそれぞれ 10.0.12.1/24、10.0.11.1/24、10.0.10.1/24 に設定します。
2. セキュリティゾーンを構成します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**security zones** をクリックします。
  - #セキュリティゾーンの **Untrust** の **Edit** アイコンをクリックします。
  - #開いたダイアログボックスで、セキュリティゾーンに GE1/0/1 を追加します。
  - #セキュリティゾーン名 **president** を作成し、セキュリティゾーンに GE1/0/2 を追加します。
  - #**finance** という名前のセキュリティゾーンを作成し、そのセキュリティゾーンに GE1/0/3 を追加します。
  - #**market** という名前のセキュリティゾーンを作成し、そのセキュリティゾーンに GE1/0/4 を追加します。
3. 時間範囲を設定します。
  - #トップナビゲーションバーで、**objects** をクリックします。
  - #ナビゲーションペインで、**Object Groups > Time Ranges** を選択します。
  - #**create** をクリックします。
  - #開いたダイアログボックスで、時間範囲を設定します。
    - A) 時間範囲名を入力します。この例では、**work** と入力します。
    - B) 勤務日の8:00から18:00までの期間を作成し、**OK** をクリックします。
    - C) **OK** をクリックします。
4. IPアドレスオブジェクトグループを設定します。

#トップナビゲーションバーで **Objects** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、**president** という名前の IPv4 アドレスオブジェクトグループを設定します。

A) グループ名**president**を入力します。

B) **add**をクリックします。

C) 表示されるダイアログボックスで、**network segment**オブジェクトを選択し、IPv4アドレスとマスク10.0.12.0/24を入力します。

#IPv4 アドレスオブジェクトグループ **president** を設定するのと同じ方法で、**market** という名前の IPv4 アドレスオブジェクトグループを設定します。**Network segment** オブジェクトの IPv4 アドレスとマスク 10.0.10.0/24 を入力します。

#### 5. アプリケーショングループを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**APPSecurity > APP Recognition > Application Groups** を選択します。

#**create** をクリックします。

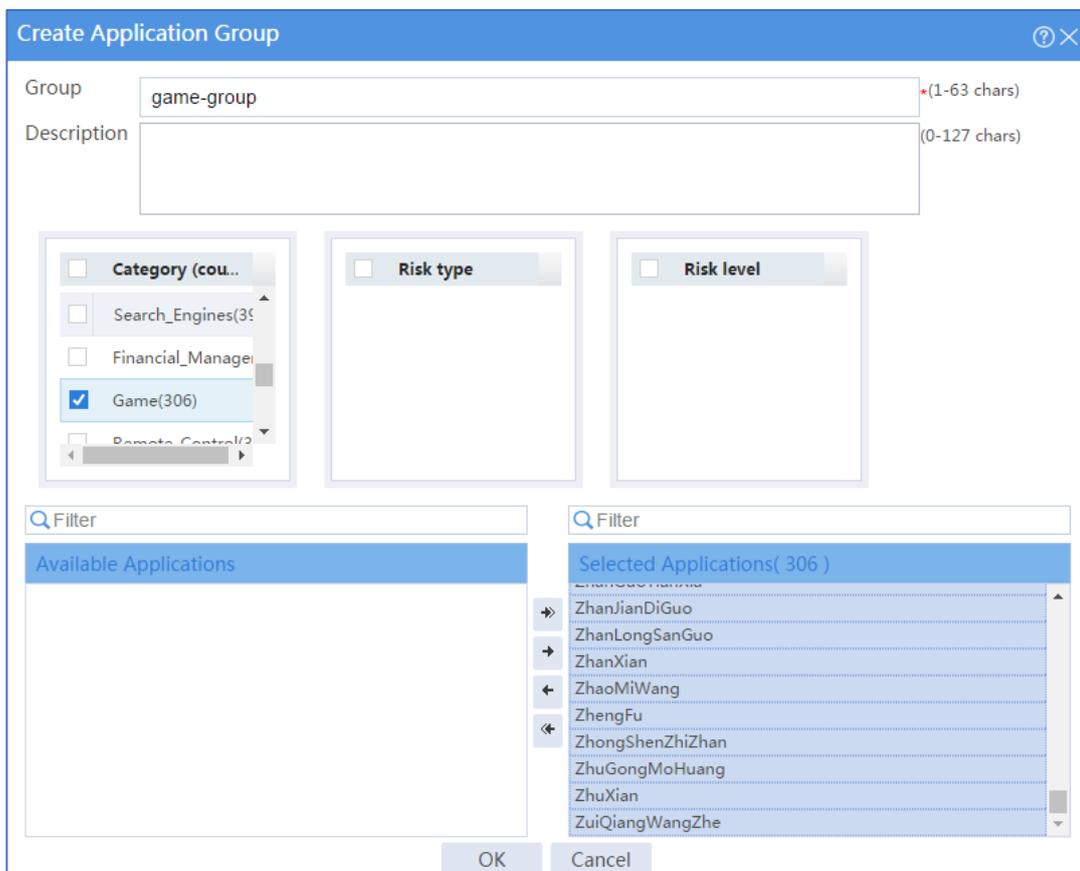
#開いたダイアログボックスで、**game-group** という名前のアプリケーショングループを設定します。

○ グループ名 **game-group** を入力します。

○ **Game** カテゴリー内のすべてのアプリケーションを **Selected Applications** ペインに追加します。

○ **OK** をクリックします。

図2 アプリケーショングループの作成



#P2P-group という名前のアプリケーショングループを作成し、P2P カテゴリー内のすべてのアプリケーションをアプリケーショングループに追加します。

#streaming-media-group という名前のアプリケーショングループを作成し、Streaming\_Media カテゴリーのすべてのアプリケーションをアプリケーショングループに追加します。

#network-community-group という名前のアプリケーショングループを作成し、Network-Community カテゴリー内のすべてのアプリケーションをアプリケーショングループに追加します。

#permit-others という名前のアプリケーショングループを作成し、E-Mail、OA、および Protocol カテゴリー内のアプリケーションの容易でないアプリケーションをアプリケーショングループに追加します。

#protocol-permit という名前のアプリケーショングループを作成し、共通プロトコル(TCP、UDP、DNS、HTTP、HTTPS、SMTP、IMAP、POP3 など)をアプリケーショングループに追加します。

6. セキュリティポリシー **president\_permit**を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies > Security Policies を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **president\_permit** を入力します。
- ソースゾーン **president** を選択します。
- ターゲットゾーンの **Untrust**、**finance**、**market** を選択します。
- ポリシータイプ **IPv4** を選択します。
- アクション **permit** を選択します。
- 送信元 IP アドレス **president** を選択します。

#**OK** をクリックします。

図3 セキュリティポリシーの作成president\_permit

The screenshot shows a 'Create Security Policy' dialog box with the following fields and values:

- Name: president\_permit
- Source zone: president
- Destination zone: Untrust, finance, market
- Type: IPv4 (selected)
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Permit (selected)
- Source IP/MAC address: president
- Destination IP: Select or enter object groups
- Service: Select or enter services
- Application: Select or enter applications
- User: Select or enter users
- Time range: Select a time range
- VRF: Select a public network
- Content security: (Section header)
- WAF profile: --NONE--

Buttons: OK, Cancel

7. **finance\_permit** という名前のセキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **finance\_permit** を入力します。
- ソースゾーン **finance** を選択します。

- 宛先ゾーン **finance** を選択します。
  - ポリシータイプ **IPv4** を選択します。
- #OK をクリックします。

図4 セキュリティポリシーfinance\_permitの作成

Create Security Policy

Name   Auto naming

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User  [Edit]

Time range

VRF

Content security

WAF profile

IPS profile

Data filtering profile

OK Cancel

8. **market\_permit1**という名前のセキュリティポリシーを設定します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。  
#**create** をクリックします。  
#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **market\_permit1** を入力します。
  - ソースゾーン **market** を選択します。
  - 宛先ゾーン **untrust** を選択。
  - ポリシータイプ **IPv4** を選択します。
  - アクション **permit** を選択します。
  - 送信元 IP アドレス **market** を選択します。
  - **WeChat、MSN、AnkAng Forum(セキュリティフォーラム)、YouKu** などのアプリケーションを選択する。
  - 時間範囲作業を選択します。
- #**OK** をクリックします。

図5 セキュリティポリシーmarket\_permit1の作成

The screenshot shows the 'Create Security Policy' dialog box with the following configuration:

- Name: market\_permit1
- Source zone: market
- Destination zone: Untrust
- Type: IPv4
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Permit
- Source IP/MAC address: market
- Destination IP: Select or enter object groups
- Service: Select or enter services
- Application: WeChat , MSN , AnFangForum , YouKu , ...
- User: Select or enter users
- Time range: work
- VRF: Select a public network

Buttons: OK, Cancel

9. **market\_deny1**という名前のセキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **market\_deny1** を入力します。
- ソースゾーン **market** を選択します。

- 宛先ゾーン **Untrust** を選択。
- ポリシータイプ **IPv4** を選択します。
- アクション **permit** を選択します。
- 送信元 IP アドレス **market** を選択します。
- アプリケーショングループ **p2p-group**、**streaming-media-group**、**network-community-group**、および **game-group** を選択します。
- 時間範囲 **work** を選択します。

#OK をクリックします。

図6 セキュリティポリシーmarket\_deny1の作成

The screenshot shows the 'Create Security Policy' dialog box with the following configuration:

- Name: market\_deny1
- Source zone: market
- Destination zone: Untrust
- Type: IPv4
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Deny
- Source IP/MAC address: market
- Destination IP: Select or enter object groups
- Service: Select or enter services
- Application: p2p-group , streaming-media-group , netw...
- User: Select or enter users
- Time range: work
- VRF: Select a public network
- Content security: WAF profile is -NONE-

10. market\_permit2という名前のセキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ・ ポリシー名 **market\_permit2** を入力します。
- ・ ソースゾーン **market** を選択します。

- ・ 宛先ゾーン **Untrust** を選択。
- ・ ポリシータイプ **IPv4** を選択します。
- ・ アクション **permit** を選択します。
- ・ 送信元 IP アドレス **market** を選択します。
- ・ アプリケーショングループ **permit-others** を選択します。
- ・ 時間範囲 **work** を選択します。

#OK をクリックします。

図7 セキュリティポリシーmarket\_permit2の作成

The screenshot shows the 'Create Security Policy' dialog box with the following configuration:

- Name: market\_permit2
- Source zone: market
- Destination zone: Untrust
- Type: IPv4
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Permit
- Source IP/MAC address: market
- Destination IP: Select or enter object groups
- Service: Select or enter services
- Application: permit-others
- User: Select or enter users
- Time range: work
- VRF: Select a public network
- Content security: WAF profile --NONE--

11. market\_permit3という名前のセキュリティポリシーを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies > Security Policies を選択します。

#create をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 market\_permit3 を入力します。
- ソースゾーン market を選択します。

- 宛先ゾーン **Untrust** を選択。
- ポリシータイプ **IPv4** を選択します。
- アクション **permit** を選択します。
- 送信元 IP アドレス **market** を選択します。
- **application group protocol-permit** を選択します。

#OK をクリックします。

図8 セキュリティポリシーmarket\_permit3の作成

**Create Security Policy**

Name  \*

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User  [Edit]

Time range

VRF

---

**Content security**

WAF profile

OK Cancel

## 設定の確認

#設定を表示します。セキュリティポリシー設定は次のとおりです。

Name	Src zone	Dst zone	Type	ID	Src address	Application	User	Action	Content ...	Enable s...	Enable	Edit
president_permit	president	Untrust finance market	IPv4	0	president	Any	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
finance_permit	finance	finance	IPv4	1	Any	Any	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
market_permit1	market	Untrust	IPv4	2	market	WeChat MSN AnFangFo... YouKu	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
market_deny1	market	Untrust	IPv4	3	market	p2p-group streaming-media-group network-community-... game-group	Any	Deny		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
market_permit2	market	Untrust	IPv4	4	market	permit-ot...	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
market_permit3	market	Untrust	IPv4	5	market	protocol-pe...	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	

#president office の従業員がネットワークリソースに自由にアクセスできることを確認します。

#financial office の従業員が相互に通信できることを確認します。

#営業日の 8:00 から 18:00 まで、マーケティングオフィスがインターネット上のリソースにアクセスできることを確認します。

- game、streaming media、P2P、または network community resouces にはアクセスできませんが、YouKu にはアクセスできます。
- WeChat だけにアクセスでき、他の IM アプリケーションにはアクセスできない。
- MSN、DingTalk、および security forumn のリソースにアクセスできます。
- リストされているアクセスできないリソース以外のすべてのリソースにアクセスできます。

#誰も財務オフィスにアクセスできないこと、および財務オフィスとマーケティングオフィスが互いにアクセスできないことを確認します。

#Monitor > Security Logs > Security Policy Logs を選択して、セキュリティポリシーが正しくヒットされることを確認します。次に、セキュリティポリシーヒットの例を示します。

図9 Xunleikankan否定

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:16:42	market	Untrust	market_deny1	1	TCP	XunLeiKanKan	10.0.10.69	49558	183.251.28.253	80	1	Deny

図10 YouKu を許可する

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 14:24:59	market	Untrust	market_permit1	3	TCP	YouKu	10.0.10.69	50013	106.11.208.145	443	1	Permit

図11 WeChatの許可

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:46:21	market	Untrust	market_permit1	5	TCP	WeChat	10.0.10.69	55493	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	market	Untrust	market_permit1	5	TCP	WeChat	10.0.10.69	55492	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	market	Untrust	market_permit1	5	TCP	WeChat	10.0.10.69	55491	117.144.245.210	80	1	Permit

図12 QQの拒否

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:48:04	market	Untrust	market_permit1	5	TCP	QQ	10.0.10.69	55792	123.151.77.194	443	1	Deny
2018-08-01 11:48:04	market	Untrust	market_permit1	5	TCP	QQ	10.0.10.69	55786	59.36.120.126	443	1	Deny
2018-08-01 11:48:04	market	Untrust	market_permit1	5	TCP	QQ	10.0.10.69	55791	163.177.94.82	443	1	Deny

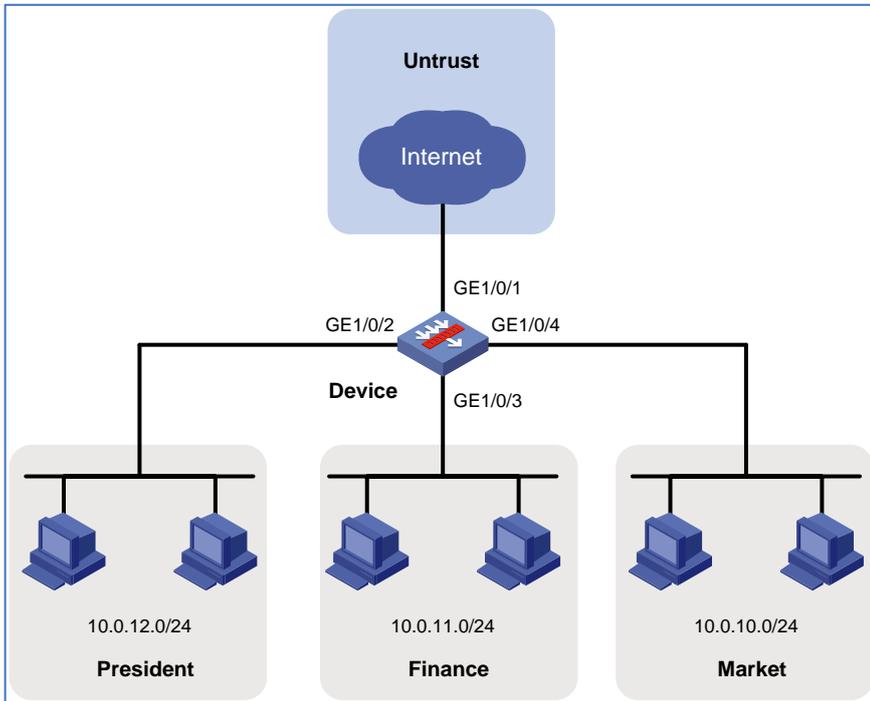
## 例:APRベースの緩いセキュリティポリシーの設定

### ネットワーク構成

図1に示すように、次の目標を達成するようにセキュリティポリシーを設定します。

- 社長室はいつでもすべてのネットワークリソースにアクセスできます。
- 財務オフィスは、それ自体のリソースにしかアクセスできません。
- マーケティングオフィスは、勤務日の 8:00 から 18:00 まで、ビデオおよびゲームアプリケーションを除くすべてのネットワークリソースにアクセスできます。また、非勤務時間中にゲームをプレイしたり、ビデオを見ることができます。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

セキュリティポリシーを設定する場合は、次の制限事項およびガイドラインに従ってください。

- APR 署名ライブラリを最新バージョンに更新します。
- セキュリティポリシー内のアプリケーションを識別するには、アプリケーションの依存プロトコルを通過させる必要があります。

## 分析

- セキュリティポリシー `finance_permit` を構成して、財務オフィスの従業員が相互に通信できるようにします。

- セキュリティポリシー **market\_deny1** を構成して、勤務日の 8:00 から 18:00 までのマーケティングオフィスのゲームおよびストリーミングビデオアプリケーションを拒否します。このセキュリティポリシーにより、勤務日の 8:00 から 18:00 までのマーケティングオフィスの従業員のゲームおよびビデオ視聴が禁止されます。
- すべてのパケットの通過を許可するようにセキュリティポリシー **permit\_all** を構成します。このセキュリティポリシーでは、前のセキュリティポリシーに一致しないすべてのパケットの通過を許可します。したがって、このセキュリティポリシーは次の要件を満たすことができます。
  - 社長室はいつでもすべてのネットワークリソースにアクセスできます。
  - マーケティングオフィスは、勤務日の 8:00 から 18:00 まで、ビデオおよびゲームアプリケーションを除くすべてのネットワークリソースにアクセスできます。また、非勤務時間中にゲームをプレイしたり、ビデオを見ることができます。
  - 共通プロトコルが許可されます。
- セキュリティポリシーを次の順序で設定します。
  - A) **Market\_permit**
  - B) **market\_deny1**
  - C) **permit\_all**

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、**2.2.2.1/24** と入力します。
    - B) **OK** をクリックします。
  - #GE1/0/2、GE1/0/3、1/2、GE1/0/3、GE1/0/4 の IP アドレスをそれぞれ 10.0.12.1/24、10.0.11.1/24、10.0.10.1/24 に設定します。

2. セキュリティゾーンを構成します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Security zone** をクリックします。

#セキュリティゾーンの **Untrust** の **Edit** アイコンをクリックします。

#開いたダイアログボックスで、セキュリティゾーンに GE1/0/1 を追加します。

#セキュリティゾーン名 **president** を作成し、セキュリティゾーンに GE1/0/2 を追加します。

#**finance** という名前のセキュリティゾーンを作成し、そのセキュリティゾーンに GE1/0/3 を追加します。

#**market** という名前のセキュリティゾーンを作成し、そのセキュリティゾーンに GE1/0/4 を追加します。

3. 時間範囲を設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Object Groups > Time Ranges** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、時間範囲を設定します。

A) 時間範囲名を入力します。この例では、**work**と入力します。

B) 勤務日の8:00から18:00までの期間を作成し、**OK**をクリックします。

C) **OK**をクリックします。

4. IPアドレスオブジェクトグループを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、**market** という名前の IPv4 アドレスオブジェクトグループを設定します。

A) グループ名**market**を入力します。

B) **add**をクリックします。

C) 表示されるダイアログボックスで、**network segment**オブジェクトを選択し、IPv4アドレスとマスク10.0.12.0/24を入力します。

5. アプリケーショングループを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

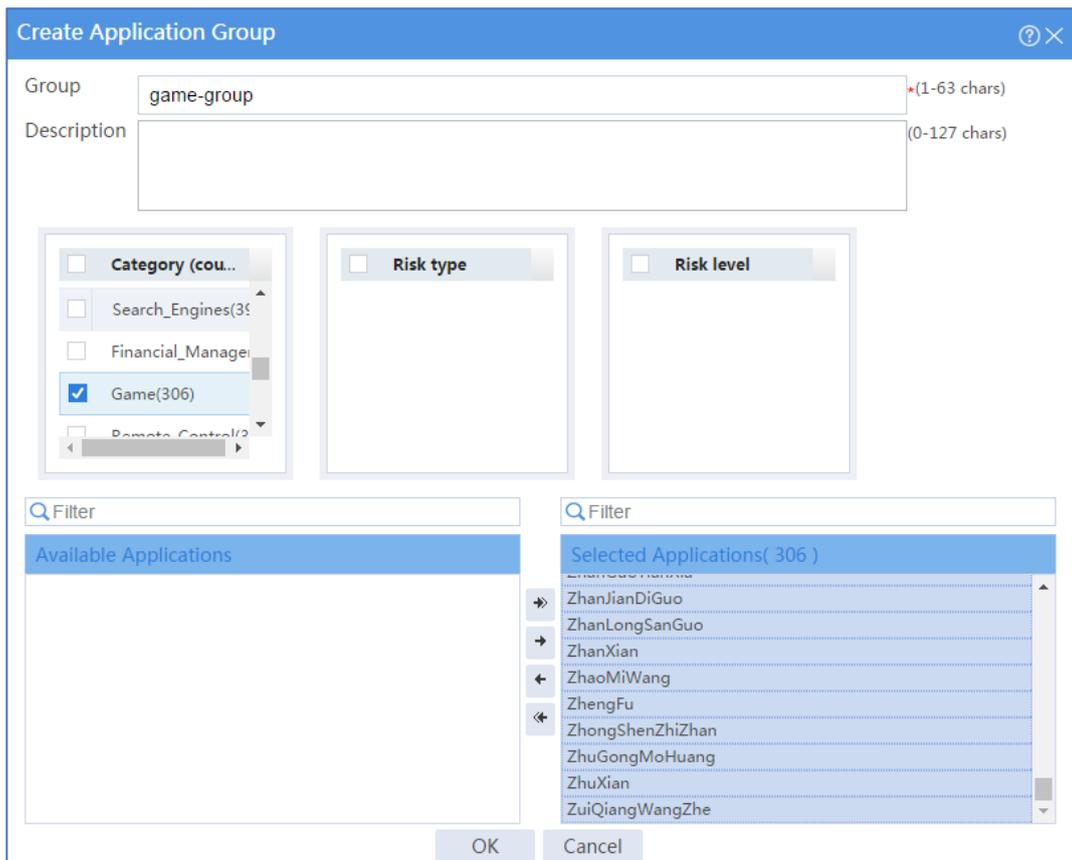
#ナビゲーションペインで、**APP Security > APP Recognition > Application Groups** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、**game-group** という名前のアプリケーショングループを設定します。

- グループ名 **game-group** を入力します。
- **game** カテゴリー内のすべてのアプリケーションを **Selected Applications** ウィンドウに追加します。
- **OK** をクリックします。

図14 アプリケーショングループgame-groupの作成



#**P2P-group** という名前のアプリケーショングループを作成し、**P2P** カテゴリー内のすべてのアプリケーションをアプリケーショングループに追加します。

#**streaming-media-group** という名前のアプリケーショングループを作成し、**Streaming\_Media** カテゴリーのすべてのアプリケーションをアプリケーショングループに追加します。

#**network-community-group** という名前のアプリケーショングループを作成し、**Network-Community** カテゴリー内のすべてのアプリケーションをアプリケーショングループに追加します。

6. **finance\_permit** という名前のセキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 `finance_permit` を入力します。
- ソースゾーン財務を選択します。
- 宛先ゾーンのファイナンスを選択します。
- ポリシータイプ `IPv4` を選択します。
- アクション許可を選択します。

#**OK** をクリックします。

図15 セキュリティポリシーfinance\_permitの作成

The screenshot shows a 'Create Security Policy' dialog box with the following fields and values:

- Name: finance\_permit
- Source zone: finance
- Destination zone: finance
- Type: IPv4 (selected)
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Permit (selected)
- Source IP/MAC address: Select or enter object groups
- Destination IP: Select or enter object groups
- Service: Select or enter services
- Application: Select or enter applications
- User: Select or enter users
- Time range: Select a time range
- VRF: Select a public network
- WAF profile: --NONE--

7. **market\_deny1**という名前のセキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#表示されるダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **market\_deny1** を入力します。
- ソースゾーン **market** を選択します。

- 宛先ゾーン **Untrust** を選択。
- ポリシータイプ **IPv4** を選択します。
- アクション **deny** アクションを選択します。
- 送信元 IP アドレス **market** を選択します。
- アプリケーショングループ **p2p-group**、**streaming-media-group**、**network-community-group**、および **game-group** を選択します。
- 時間範囲 **work** を選択します。

#OK をクリックします。

図16 セキュリティポリシーmarket\_deny1の作成

The screenshot shows a 'Create Security Policy' dialog box with the following fields and values:

- Name: markey\_deny1
- Source zone: market
- Destination zone: Untrust
- Type: IPv4 (selected)
- Policy group: Select a policy group
- Description: (1-127 chars)
- Action: Deny (selected)
- Source IP/MAC address: market
- Destination IP: Select or enter object groups
- Service: Select or enter services
- Application: p2p-group , streaming-media-group , netw...
- User: Select or enter users
- Time range: work
- VRF: Select a public network
- WAF profile: --NONE--

Buttons: OK, Cancel

8. permit\_all という名前のセキュリティポリシーを設定します。
  - #トップナビゲーションバーで、**Policies** をクリックします。
  - #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
  - #create をクリックします。
  - #表示されるダイアログボックスで、セキュリティポリシーを設定します。
    - ポリシー名 **permit\_all** を入力します。

- ポリシータイプ **IPv4** を選択します。
- アクション **permit** を選択します。

#**OK** をクリックします。

図17 セキュリティポリシーmarket\_allの作成

**Create Security Policy**

Name   Auto naming

Source zone  [Edit]

Destination zone  [Edit]

Type  IPv4  IPv6

Policy group

Description  (1-127 chars)

Action  Permit  Deny

Source IP/MAC address  [Edit]

Destination IP  [Edit]

Service  [Edit]

Application  [Edit]

User  [Edit]

Time range

VRF

**Content security**

WAF profile

OK Cancel

## 設定の確認

#設定を表示します。セキュリティポリシー設定は次のとおりです。

Name	Src zone	Dst zone	Type	ID	Src address	Application	User	Action	Content ...	Enable st...	Enable	Edit
<input type="checkbox"/> finance_permit	finance	finance	IPv4	0	Any	Any	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> market_deny1	market	Untrust	IPv4	1	market	<ul style="list-style-type: none"> <li><input type="checkbox"/> op2p-group</li> <li><input type="checkbox"/> streaming-media-group</li> <li><input type="checkbox"/> network-community-...</li> <li><input type="checkbox"/> game-group</li> </ul>	Any	Deny		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> permit_all	Any	Any	IPv4	2	Any	Any	Any	Permit		<input type="checkbox"/>	<input checked="" type="checkbox"/>	

#president office の従業員がネットワークリソースに自由にアクセスできることを確認します。

#finance office の従業員が相互に通信できることを確認します。

#marketing office が、勤務日の 8:00 から 18:00 までビデオおよびゲームアプリケーションを除くすべてのネットワークリソースにアクセスできること、および非勤務時間中にゲームをプレイしたりビデオを視聴できることを確認します。

#Monitor > Security Logs > Security Policy Logs を選択して、セキュリティポリシーが正しくヒットされることを確認します。次に、セキュリティポリシーヒットの例を示します。

図18 Xunleikankan否定

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:16:42	market	Untrust	market_deny1	1	TCP	XunLeiKanKan	10.0.10.69	49558	183.251.28.253	80	1	Deny

図19 WeChatの許可

Time	Source ...	Destina...	Security policy	Rule ID	Protocol	Application	Source IP address	Source ...	Destination IP address	Destina...	Number of ru...	Action
2018-08-01 11:46:21	Any	Any	permit_all	2	TCP	WeChat	10.0.10.69	55493	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	Any	Any	permit_all	2	TCP	WeChat	10.0.10.69	55492	117.144.245.210	80	1	Permit
2018-08-01 11:46:21	Any	Any	permit_all	2	TCP	WeChat	10.0.10.69	55491	117.144.245.210	80	1	Permit

# NAT の設定例

## はじめに

次に、NATの設定例を示します。  
次のNAT変換方式がサポートされています。

### スタティック NAT

スタティック NAT は、プライベートアドレスとパブリックアドレス間の固定マッピングを作成します。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。スタティック NAT は通常の通信に適用されます。

### ダイナミック 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。

### NAT サーバー

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ピングします。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が外部ユーザーにサービスを提供できます。

### NAT444 ポートブロック

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 は、キャリア側に NAT の第 2 レイヤを導入し、カスタマー側とアプリケーションサーバー側ではほとんど変更しません。ポートブロック割り当てにより、NAT444 はユーザートラッキングをサポートします。これは、IPv6 への移行中のキャリアにとって好ましいソリューションとなりました。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

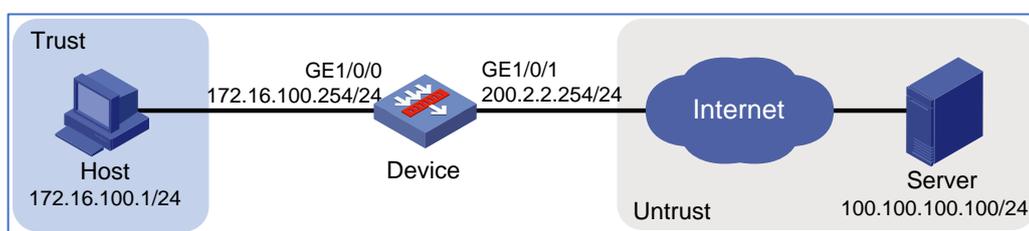
次の情報は、NAT の基本的な知識があることを前提としています。

## 例:スタティックNATの設定

### ネットワーク構成

図1に示すように、スタティック NAT を設定して、172.16.100.1/24 のホストがパブリック IP アドレス 200.2.2.254/24 を使用してインターネット上の 100.100.100.100/24 のサーバーにアクセスできるようにします。

図1ネットワーク図



### 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。

B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、200.2.2.254/24 と入力します。

C) **OK** をクリックします。

#GE1/0/0 を信頼セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 172.16.100.254/24 に設定します。

2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#パケットの通過を許可するセキュリティポリシーを作成します。

3. スタティックNATマッピングを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > Static NAT > Policy Configuration** を選択します。

#**create** をクリックします。

#スタティック NAT マッピングを作成します(図2を参照)。

図2 スタティック NAT マッピングの作成

#**OK** をクリックします。

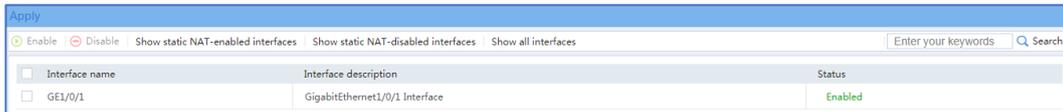
4. スタティックNATマッピングを適用します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > Static NAT > Apply Policy** を選択します。

#GE1/0/1 を選択し、Enable をクリックします。マッピングがインターフェイスに適用されています (図3を参照)。

図3スタティック NAT マッピングの適用



## 設定の確認

1. ホストが外部ネットワーク上のサーバーに正常にpingできることを確認します。

```
C:¥Users¥abc>ping 100.100.100.100
```

```
Pinging host.com [100.100.100.100] with 32 bytes of data:
```

```
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 100.100.100.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. ホストがサーバーにアクセスしたときにNATセッションが生成されることを確認します。

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Sessions** を選択します。

図4 セッションリスト

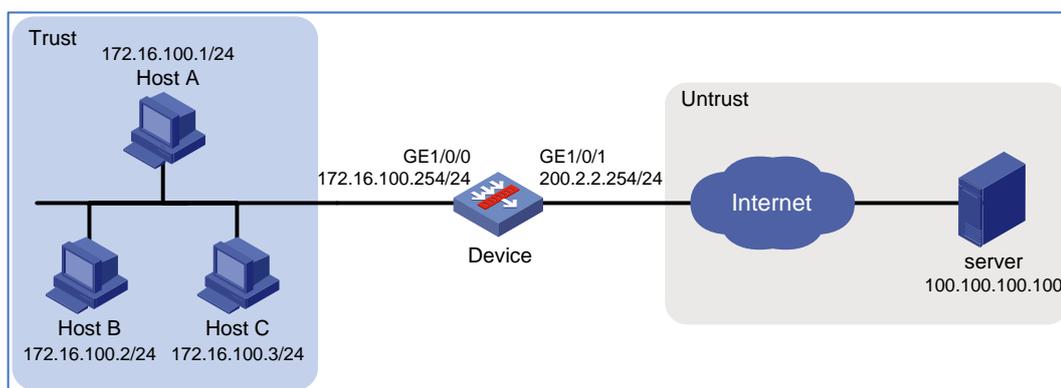
The screenshot shows a web interface titled 'Session List'. At the top, there are several controls: 'IPv4', 'Total sessions: 6', 'Delete sessions', 'Clear all filters', 'Export CLI output', 'Export this page', 'Refresh', 'Customize columns', and 'Advanced search'. Below these controls is a table with the following columns: 'Initiator source IP', 'Initiator s...', 'Initiator destination IP', 'Initiator d...', 'Initiator VRF/VLAN I...', 'Receiving secu...', 'Initiator p...', 'Application layer protocol', 'Master/B...', 'Status', and 'Security p...'. There is one row in the table with the following data: '172.16.100.1', '1', '100.100.100.100', '2048', 'VPN:Public network', 'Trust', 'ICMP', 'ICMP', 'Master', 'Normal', and 'Trust-to-Un'.

# 例:ダイナミックNATのNO-PATの設定

## ネットワーク構成

図5に示すように、この企業のパブリックアドレスは 200.2.2.1/24~200.2.2.3/24 です。内部ネットワーク内のホストがインターネット上のサーバーにアクセスできるように、NO-PAT 変換を設定します。

図5ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、200.2.2.254/24 と入力します。
    - C) **OK** をクリックします。

#GE1/0/0 を信頼セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 172.16.100.254/24 に設定します。

2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#パケットの通過を許可するセキュリティポリシーを作成します。

3. NATアドレスグループを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > NAT Advanced Settings > NAT Address Groups** を選択します。

#**create** をクリックします。

#NAT アドレスグループを作成します(図6を参照)。

図6 NAT アドレスグループの作成

Create NAT Address Group

Address group ID: 1 \*(0-65535)

Address group name: nopatpool (1-63 chars)

VRRP group: (1-255)

Port range: 1 - 65535

Port block size: (1-65535)

Number of extended port blocks: (1-5)

Address probe ?

Address group members

<input type="checkbox"/>	Start IP	End IP
<input type="checkbox"/>	200.2.2.1	200.2.2.3

OK Cancel

#OK をクリックします。

4. アウトバウンドダイナミックNAT規則を設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

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

#**Outbound Dynamic NAT**(Object Group-Based)タブで、**Create** をクリックします。

#アウトバウンドダイナミック NAT 規則を作成します(図7を参照)。

図7 アウトバウンドダイナミック NAT 規則の作成

Create Outbound Dynamic NAT

Rule name: nat\_nopat\_rule0 \*(1-63 chars)

Rule description: (1-63 chars)

Output interface: GE1/0/1 \*

Source IP: Please select an object group [Edit]

Destination IP: Please select an object group [Edit]

Service: Please select a service [Edit]

Action:  PAT  NO-PAT  Easy IP  No translation

Source address after NAT: 1 \*

Allow reverse NAT

Enable this rule

OK Cancel

#OK をクリックします。

## 設定の確認

1. ホストが外部ネットワーク上のサーバーに正常にpingできることを確認します。

```
C:¥Users¥abc>ping 100.100.100.100
```

```
Pinging host.com [100.100.100.100] with 32 bytes of data:
```

```
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 100.100.100.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

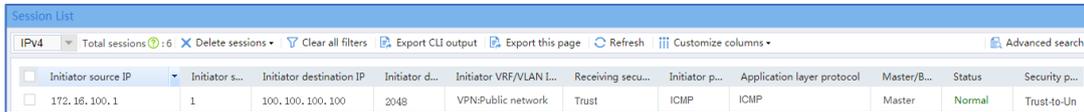
```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ホストがサーバーにアクセスしたときに NAT セッションが生成されることを確認します。

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Sessions** を選択します。

図8 セッションリスト



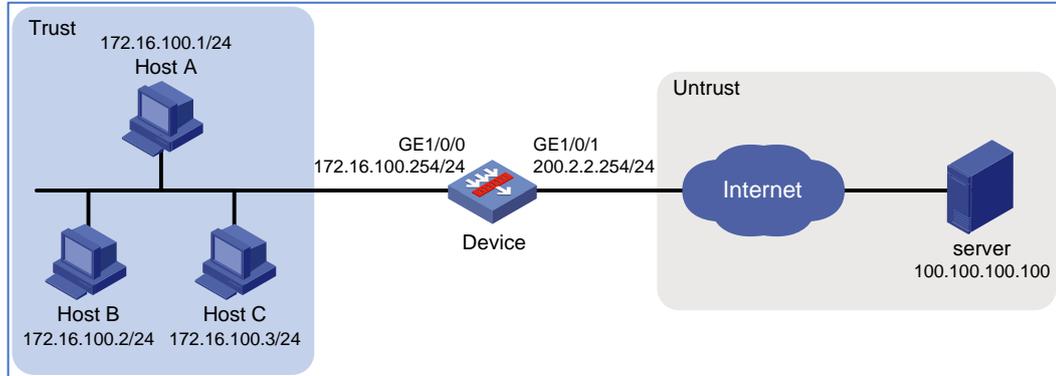
Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/VLAN I...	Receiving secu...	Initiator p...	Application layer protocol	Master/B...	Status	Security p...
172.16.100.1	1	100.100.100.100	2048	VPN:Public network	Trust	ICMP	ICMP	Master	Normal	Trust-to-Un

## 例:ダイナミックNATのPAT設定

### ネットワーク構成

図9に示すように、会社には 200.2.2.1/24 のパブリック IP アドレスが 1 つしかありません。このパブリック IP アドレスを使用して内部ホストだけがインターネットにアクセスできるように、アウトバウンドダイナミック NAT の PAT を設定してください。

図9 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。

B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、200.2.2.254/24 と入力します。

C) **OK** をクリックします。

#GE1/0/0 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 172.16.100.254/24 に設定します。

## 2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#パケットの通過を許可するセキュリティポリシーを作成します。

## 3. NATアドレスグループを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > NAT Advanced Settings > NAT Address Groups** を選択します。

#**create** をクリックします。

#NAT アドレスグループを作成します(図10を参照)。

図10 NAT アドレスグループの作成

Create NAT Address Group

Address group ID: 1 (0-65535)

Address group name: patpool (1-63 chars)

VRRP group: (1-255)

Port range: 1 - 65535

Port block size: (1-65535)

Number of extended port blocks: (1-5)

Address probe: (1-5)

Address group members:

Start IP	End IP
<input type="checkbox"/> 200.2.2.1	200.2.2.1

OK Cancel

#OK をクリックします。

4. アウトバウンドダイナミックNAT規則を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT>Dynamic NAT を選択します。

#Outbound Dynamic NAT(Object Group-Based)タブで、Create をクリックします。

#アウトバウンドダイナミック NAT 規則を作成します(図11を参照)。

図11 アウトバウンドダイナミック NAT 規則の作成

Create Outbound Dynamic NAT

Rule name: nat\_pat\_rule0 \*(1-63 chars)

Rule description: (1-63 chars)

Output interface: GE1/0/1 \*

Source IP: Please select an object group [Edit]

Destination IP: Please select an object group [Edit]

Service: Please select a service [Edit]

Action:  PAT  NO-PAT  Easy IP  No translation

Source address after NAT: 1 \*

Port reservation:  Try to preserve port number for PAT

Enable this rule:

OK Cancel

#OK をクリックします。

## 設定の確認

1. ホストが外部ネットワーク上のサーバーに正常にpingできることを確認します。

```
C:¥Users¥abc>ping 100.100.100.100
```

```
Pinging host.com [100.100.100.100] with 32 bytes of data:  
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253  
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253  
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253  
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 100.100.100.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
    Approximate round trip times in milli-seconds:
```

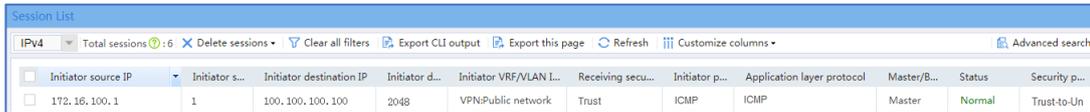
```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ホストがサーバーにアクセスしたときにNATセッションが生成されることを確認します。

#トップナビゲーションバーで **monitor** をクリックします。

#ナビゲーションペインで、**Sessions** を選択します。

図12 セッションリスト



Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/VLAN I...	Receiving secu...	Initiator p...	Application layer protocol	Master/B...	Status	Security p...
172.16.100.1	1	100.100.100.100	2048	VPN:Public network	Trust	ICMP	ICMP	Master	Normal	Trust-to-Un

## 例:NATサーバーの設定

### ネットワーク構成

図13 に示すように、外部ユーザーに Web サービスを提供する内部ネットワーク内のサーバー。

外部ユーザーがパブリックアドレス 200.2.2.1/24 を使用して内部サーバーにアクセスできるように、NAT サーバー機能を設定します。

図13 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、ネットワークをクリックします。

#ナビゲーションペインで、Interface Configuration>Interfaces を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- **Basic Configuration**タブで、**Untrust**セキュリティゾーンを選択します。
- **IPv4 Address**タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、200.2.2.254/24と入力します。
- OKをクリックします。

#GE1/0/0 を **trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 172.16.100.254/24 に設定します。

## 2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#パケットの通過を許可するセキュリティポリシーを作成します。

## 3. NATサーバー規則を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT>NAT Servers>Policy Configuration を選択します。

#create をクリックします。

#NAT サーバールールを作成します(図14を参照)。

**図14 NAT サーバー規則の作成**

The screenshot shows the 'Create NAT Server Rule' dialog box. The fields are filled as follows:

- Rule name: InnerSver0
- Interface: GE1/0/1
- Protocol type: (empty)
- Mapping: One single public address with one single or no public port
- Mapping description: (empty)
- Public IP:  Specify an IP address, 200.2.2.1
- Public port: (empty)
- Public port VRF: Public network
- Server IP: 172.16.100.1
- Server port: (empty)
- Server VRF: Public network
- ACL for packet matching: (empty)
- VRRP group: (empty)

#OK をクリックします。

## 設定の確認

1. ホストがパブリックアドレスに正常にpingできることを確認します。

```
C:¥Users¥abc>ping 200.2.2.1
```

```
Pinging host.com [200.2.2.1] with 32 bytes of data:
```

```
Reply from 200.2.2.1: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 200.2.2.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

ホストが内部サーバーにアクセスしたときにNATセッションが生成されることを確認します。

#トップナビゲーションバーで **monotor** をクリックします。

#ナビゲーションペインで、**sessions** を選択します。

図 15 セッションリスト

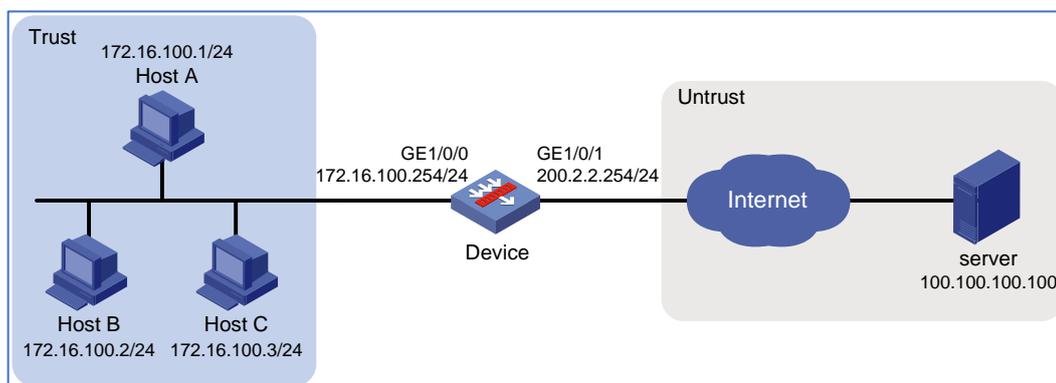
Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/VLAN I...	Receiving secu...	Initiator p...	Application layer protocol	Master/B...	Status	Security p...
100.100.100.100	1	200.2.2.1	2048	VPN:Public network	Untrust	ICMP	ICMP	Master	Normal	Untrust-Tru...

## 例:スタティックNAT444の設定

### ネットワーク構成

図 16 に示すように、企業には 1 つのパブリック IP アドレス 200.2.2.1/24 があります。内部ネットワークユーザーがこのパブリック IP アドレスを使用してインターネットにアクセスできるように、スタティック NAT444 ポートブロックマッピングを設定します。ポート範囲を 10001~15000 に設定し、ポートブロックサイズを 500 に設定します。

図16 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。
    - **IPv4 Address** タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、200.2.2.254/24 と入力します。
    - **OK** をクリックします。
  - #GE1/0/0 を **trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 172.16.100.254/24 に設定します。
2. セキュリティポリシーを設定します。
  - #トップナビゲーションバーで、**Policies** をクリックします。
  - #ナビゲーションペインで、**Security Policies > Security Policies** を選択します。
  - #**create** をクリックします。
  - #パケットの通過を許可するセキュリティポリシーを作成します。
3. ポートブロックグループを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > Static NAT444 > Port Blocks** を選択します。

#**create** をクリックします。

#ポートブロックグループを作成します(図17を参照)。

図17 ポートブロックグループの作成

Create Port Block Group

Group ID  \* ( 0-65535 )

VRRP group  (1-255)

Port range  -

Port block size  (1-65535. Default: 256.)

Add private address member |  Delete

<input type="checkbox"/>	Start IP	End IP	VRF
<input type="checkbox"/>	172.16.100.1	172.16.100.3	

Add public address member |  Delete

<input type="checkbox"/>	Start IP	End IP
<input type="checkbox"/>	200.2.2.1	200.2.2.1

OK Cancel

#OK をクリックします。

4. スタティックNAT444規則を設定します。

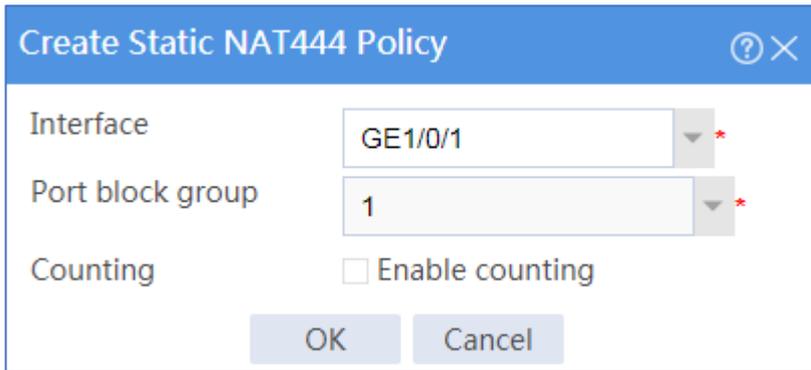
#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > Static NAT444 > Policy Configuration** を選択します。

#**create** をクリックします。

#に示すように、スタティック NAT444 規則を作成します。

図18 スタティック NAT444 規則の作成



Interface: GE1/0/1

Port block group: 1

Counting:  Enable counting

OK Cancel

#OK をクリックします。

## 設定の確認

1. ホストが外部ネットワーク上のサーバーに正常にpingできることを確認します。

```
C:¥Users¥abc>ping 100.100.100.100
```

Pinging host.com [100.100.100.100] with 32 bytes of data:

Reply from 100.100.100.100: bytes=32 time<1ms TTL=253

Ping statistics for 100.100.100.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

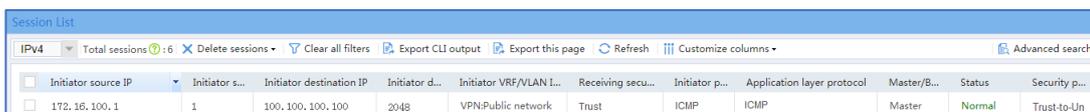
Minimum = 0ms, Maximum = 0ms, Average = 0ms

ホストがサーバーにアクセスしたときに NAT セッションが生成されることを確認します。

#トップナビゲーションバーで **monitor** をクリックします。

#ナビゲーションペインで、**sessions** を選択します。

図19 セッションリスト



Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/VLAN I...	Receiving secu...	Initiator p...	Application layer protocol	Master/B...	Status	Security p...
172.16.100.1	1	100.100.100.100	2048	VPN-Public network	Trust	ICMP	ICMP	Master	Normal	Trust-to-Un

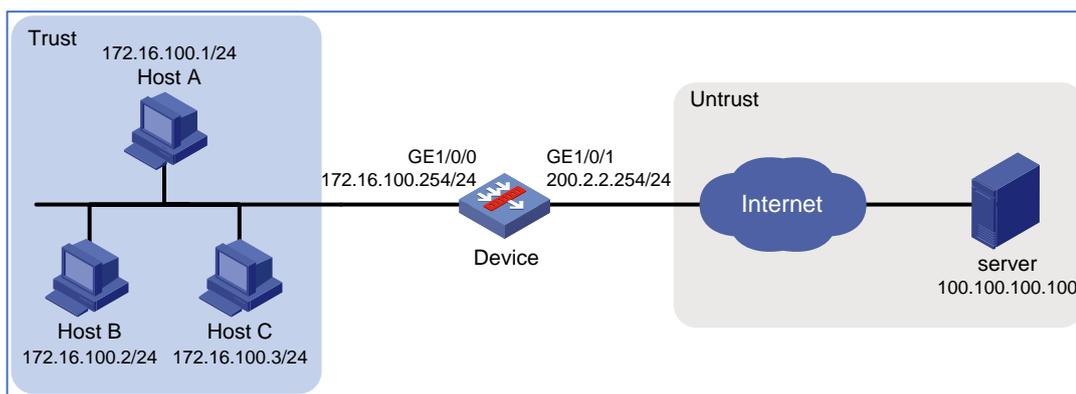
# 例:ダイナミックNAT444の設定

## ネットワーク構成

図20に示すように、企業には 200.2.2.1/24~200.2.2.3/24 のパブリック IP アドレスがあります。次の要件を満たすように、NAT444 ダイナミックポートブロックマッピングを設定します。

- 内部ネットワークユーザーは、パブリック IP アドレスを使用してインターネットにアクセスできます。
- パブリック IP アドレスのポート範囲は 1024~65535 です。
- ポートブロックサイズは 500 です。
- 割り当てられた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は、別のポートブロックをユーザー用に拡張します。

図20 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- Basic Configurationタブで、Untrustセキュリティゾーンを選択します。
- IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、200.2.2.254/24と入力します。
- OKをクリックします。

#GE1/0/0 を **trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 172.16.100.254/24 に設定します。

## 2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**create** をクリックします。

#パケットの通過を許可するセキュリティポリシーを作成します。

## 3. NATアドレスグループを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > NAT Advanced Settings > NAT Address Groups** を選択します。

#**create** をクリックします。

#NAT アドレスグループを作成します(図21を参照)。

図21 NAT アドレスグループの作成

Create NAT Address Group

Address group ID: 1 (0-65535)

Address group name: (1-63 chars)

VRRP group: (1-255)

Port range: 1024 - 65535

Port block size: 500 (1-65535)

Number of extended port blocks: 1 (1-5)

Address probe: (1-5)

Address group members

Start IP	End IP
<input type="checkbox"/> 200.2.2.1	<input type="checkbox"/> 200.2.2.3

OK Cancel

#OK をクリックします。

4. アウトバウンドダイナミックNAT444規則を設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > Dynamic NAT444** を選択します。

#**Outbound Dynamic NAT444(Object Group-Based)**タブで、**Create** をクリックします。

#アウトバウンドダイナミック NAT444 規則を作成します(図22を参照)。

図22 ダイナミック NAT444 規則の設定

Create Outbound Dynamic NAT444

Rule name: nat\_nat444\_dynamic\_rule0 \*(1-63 chars)

Rule description: (1-63 chars)

Interface: GE1/0/1 \*

Source IP: Please select an object group [Edit]

Destination IP: Please select an object group [Edit]

Service: Please select a service [Edit]

Action:  PAT  NO-PAT

Source address after NAT: 1 \*

OK Cancel

#OK をクリックします。

## 設定の確認

1. ホストが外部ネットワーク上のサーバーに正常にpingできることを確認します。

```
C:¥Users¥abc>ping 100.100.100.100
```

```
Pinging host.com [100.100.100.100] with 32 bytes of data:
```

```
Reply from 100.100.100.100: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 100.100.100.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. ホストがサーバーにアクセスしたときにNATセッションが生成されることを確認します。

#トップナビゲーションバーで **monitor** をクリックします。

#ナビゲーションペインで、**sessions** を選択します。

図23セッションリスト

Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/VLAN L...	Receiving secu...	Initiator p...	Application layer protocol	Master/B...	Status	Security p...
172.16.100.1	1	100.100.100.100	2048	VPN:Public network	Trust	ICMP	ICMP	Master	Normal	Trust-to-Un

# IPsec VPN 設定例

## はじめに

次に、IPSec VPNの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、IPSec VPN 機能の基本的な知識があることを前提としています。

## 制限事項とガイドライン

- IPsec ポリシーでリモートホスト名を指定する場合は、次の制限事項およびガイドラインに従ってください。
  - リモートホスト名が DNS サーバーによって解決された場合、ローカルデバイスは、キャッシュされた DNS エントリ期限切れになると、DNS サーバーにクエリを送信することによって、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。
  - リモートホスト名がローカルに設定されたスタティック DNS エントリによって解決され、エントリ内の IP アドレスが変更された場合、新しい IP アドレスを取得するには、IPSec ポリシーでリモートホスト名を再指定する必要があります。
- 2つの IPsec ピア間で SA 保護されたトラフィックを2つの IPsec ピア間で正しく処理できるようにするには、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 規則が相互のミラーイメージを形成しない場合、SA は次の両方の要件が満たされている場合にのみ設定できます。

- 一方のピアの ACL ルールによって指定された範囲は、もう一方のピアの対応する ACL ルールによってカバーされます。
- 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 ルールを使用している場合、一致するトラフィックが応答側の範囲外であるため、ネゴシエーション要求が拒否される可能性があります。
  - IP Sec ポリシーでローカル ID を設定しない場合、ポリシーは詳細設定で設定されたグローバルローカル ID 設定を使用します。
- IP Sec 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
  - IP Sec SA ライフタイム
  - IP Sec SA アイドルタイムアウト

既存の IPSec SA に変更を適用するには、IPSec SA をリセットする必要があります。
- IP Sec 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。

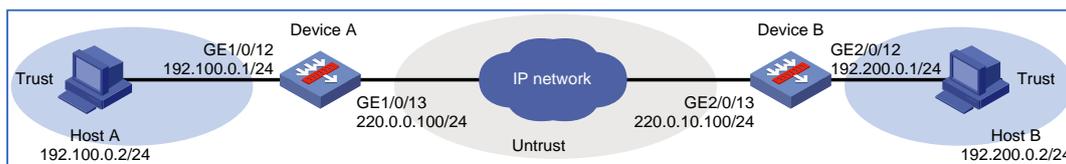
# 例:IPv4サブネット用のIPSecトンネルの設定

## ネットワーク構成

図1に示すように、デバイス A とデバイス B の間に IPSec トンネルを確立して、ホスト A とホスト B のサブネット間のデータフローを保護します。次のようにトンネルを設定します。

- IKE ネゴシエーションを介して SA を設定します。
- 3DES-CBC 暗号化アルゴリズム、SHA256 認証アルゴリズム、および事前共有キー認証方式を使用するように IKE を設定します。
- IP IPSec カプセル化モードを指定し、ESP としてセキュリティプロトコルを指定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイス A の設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/13 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。  
B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、220.0.0.100/24 と入力します。  
C) **OK** をクリックします。

#GE1/0/12 を **Trust** セキュリティゾーンに追加し、GE1/0/13 の設定と同じ方法で IP アドレスを 192.100.0.1/24 に設定します。

2. **Trust**セキュリティゾーンと**Untrust**セキュリティゾーンの間にセキュリティポリシーを構成します。**Trust**セキュリティゾーンと**Untrust**セキュリティゾーンが相互に通信できることを確認してください。

3. IKE プロポーザルを作成します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**VPN > IPSec > IKE Proposals** を選択します。

#**create** をクリックします。

- プライオリティを 1 に設定します。
- 事前共有キー認証方式を選択します。
- SHA256 認証アルゴリズムを選択します。
- 3DES-CBC 暗号化アルゴリズムを選択します。

#**OK** をクリックします。

図2 IKE プロポーザルの作成

Priority	1	*(1-65535)
Authentication method	Preshared key	
Authentication algorithm	SHA256	
Encryption algorithm	3DES-CBC	
DH	DH group 1	
IKE SA lifetime	86400	seconds (60-604800)

4. IP Sec ポリシーを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**VPN > IPSec > IPSec Policies** を選択します。

#**create** をクリックします。

#次のように基本設定を行います。

- ポリシー名を **policy1** に設定します。
- プライオリティを 1 に設定します。
- デバイスタイプを **Peer/branch gateway** に設定します。
- IP バージョンを **IPv4** に設定します。
- インターフェイス GE1/0/13 を選択します。
- ローカルアドレスを 220.0.0.100 に設定します。
- リモートアドレス/ホスト名を 220.0.10.100 に設定します。

図3 基本設定

Basic settings	
Policy name	policy1 <small>*(1-46 chars)</small>
Priority	1 <small>*(1-65535)</small>
Device type	<input checked="" type="radio"/> Peer/branch gateway <input type="radio"/> Headquarters gateway
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Smart link selection	<input type="checkbox"/> Enable
Interface	GE1/0/13 <small>*</small> <a href="#">Edit</a>
Local address	220.0.0.100
Remote IP/hostname	220.0.10.100 <small>*(1-253 chars)</small>
Description	<small>(1-80 chars)</small>

#IKE プロファイルを次のように設定します。

- ネゴシエーションモードを **Main** に設定します。
- 認証方式を **Preshared key** に設定します。
- 事前共有キースtringを入力し、キーを確認します。
- IKE proposal 1 ( **Preshared key; SHA256; 3DES-CBC; DH group1** ) を選択します。
- ローカル ID を IPv4 アドレス 220.0.0.100 に設定します。

- ピア ID を IPv4 アドレス 220.0.10.100 に設定します。

図4 IKE プロファイル設定

The screenshot shows the 'IKE profile settings' window with the following configurations:

- Negotiation mode:  Main,  Aggressive,  GM main
- Authentication method:  Preshared key,  Digital signature authentication
- Preshared key: [Redacted] (1-128 chars)
- Confirm preshared key: [Redacted]
- IKE proposal: 1 (Preshared key ; SHA256 ; 3DES-CBC ; DH group 1)
- Local ID: IPv4 address 220.0.0.100
- Peer ID: IPv4 address 220.0.10.100

#データフローフィルタ規則を次のように設定します。

- **create** をクリックします。
- 送信元 IP アドレスを 192.100.0.0/24 に設定します。
- 宛先 IP アドレスを 192.200.0.0/24 に設定します。

#OK をクリックします。

図5 データフローフィルタールの作成

The screenshot shows the 'Create Data Flow Filter Rule' dialog box with the following configurations:

- VRF: Public network
- Src IP address: 192.100.0.0/24
- Dest IP address: 192.200.0.0/24
- Protocol: any (0-255)
- Action: Protect

Buttons: OK, Cancel

#IPSec の詳細設定を次のように構成します。

- トンネルカプセル化モードを選択します。
- ESP セキュリティプロトコルを選択します。

#OK をクリックします。

## デバイス B の設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE2/0/13 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- **Basic Configuration** タブで、**Untrust** セキュリティゾーンを選択します。
- **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、220.0.10.100/24 と入力します。
- **OK** をクリックします。

#GE2/0/ge2//12 を追加し、GE2/0/13 と同じ方法で IP アドレスを 192.200.0.2/24 に設定します。

2. 信頼するセキュリティゾーンと信頼しないセキュリティゾーンの間セキュリティポリシーを構成します。信頼するセキュリティゾーンと信頼しないセキュリティゾーンが相互に通信できることを確認してください。
3. IKE プロポーザルを作成します。

#トップナビゲーションバーで、**ネットワーク** をクリックします。

#ナビゲーションペインで、**VPN > IPSec > IKE Proposals** を選択します。

#create をクリックします。

- プライオリティを 1 に設定します。
- 事前共有キー認証方式を選択します。
- SHA256 認証アルゴリズムを選択します。
- 3DES-CBC 暗号化アルゴリズムを選択します。

#OK をクリックします。

図6 IKE プロポーザルの作成

Field	Value	Range/Unit
Priority	1	*(1-65535)
Authentication method	Preshared key	
Authentication algorithm	SHA256	
Encryption algorithm	3DES-CBC	
DH	DH group 1	
IKE SA lifetime	86400	seconds (60-604800)

4. IP Sec ポリシーを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**VPN > IPSec > IPSec Policies** を選択します。

#**create** をクリックします。

#次のように基本設定を行います。

- ポリシー名を **policy1** に設定します。
- プライオリティを **1** に設定します。
- デバイスタイプを **Peer/branch gateway** に設定します。
- IP バージョンを **IPv4** に設定します。
- インターフェイス **GE2/0/13** を選択します。
- ローカルアドレスを **220.0.10.100** に設定します。
- リモートアドレス/ホスト名を **220.0.0.100** に設定します。

図7 基本設定

Basic settings	
Policy name	<input type="text" value="policy1"/> *(1-46 chars)
Priority	<input type="text" value="1"/> *(1-65535)
Device type	<input checked="" type="radio"/> Peer/branch gateway <input type="radio"/> Headquarters gateway
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Smart link selection	<input type="checkbox"/> Enable
Interface	<input type="text" value="GE2/0/13"/> * <input type="button" value="Edit"/>
Local address	<input type="text" value="220.0.10.100"/>
Remote IP/hostname	<input type="text" value="220.0.0.100"/> *(1-253 chars)
Description	<input type="text"/> (1-80 chars)

#IKE プロファイルを次のように設定します。

- ネゴシエーションモードを **Main** に設定します。
- 認証方式を **Preshared key** に設定します。
- 事前共有キースtringを入力し、キーを確認します。
- IKE proposal 1 ( **Preshared key; SHA256; 3DES-CBC; DH group1**)を選択します。
- ローカル ID を IPv4 アドレス 220.0.10.100 に設定します。
- ピア ID を IPv4 アドレス 220.0.0.100 に設定します。

図8 IKE プロファイル設定

The screenshot shows the 'IKE profile settings' window. It contains the following fields and options:

- Negotiation mode:** Radio buttons for Main (selected), Aggressive, and GM main.
- Authentication method:** Radio buttons for Preshared key (selected) and Digital signature authentication.
- Preshared key:** Text input field with three dots and a red asterisk, with '(1-128 chars)' to its right.
- Confirm preshared key:** Text input field with three dots.
- IKE proposal:** Dropdown menu showing '1 (Preshared key ; SHA256 ; 3DES-CBC ; DH group 1)'. A green question mark icon is to the left.
- Local ID:** Dropdown menu for 'IPv4 address' with the value '220.0.10.100'.
- Peer ID:** Dropdown menu for 'IPv4 address' with the value '220.0.0.100' and a red asterisk to its right.

#データフローフィルタ規則を次のように設定します。

- **create** をクリックします。
- 送信元 IP アドレスを 192.200.0.0/24 に設定します。
- 宛先 IP アドレスを 192.100.0.0/24 に設定します。

#OK をクリックします。

図8 データフローフィルタールの作成

The screenshot shows the 'Create Data Flow Filter Rule' dialog box with the following settings:

- VRF:** Public network
- Src IP address:** 192.200.0.0/24
- Dest IP address:** 192.100.0.0/24
- Protocol:** any (with '(0-255)' to the right)
- Action:** Protect

Buttons for 'OK' and 'Cancel' are at the bottom.

#IPSec の詳細設定を次のように構成します。

- **Tunnel** カプセル化モードを選択します。
- **ESP** セキュリティプロトコルを選択します。

#OK をクリックします。

## 設定の確認

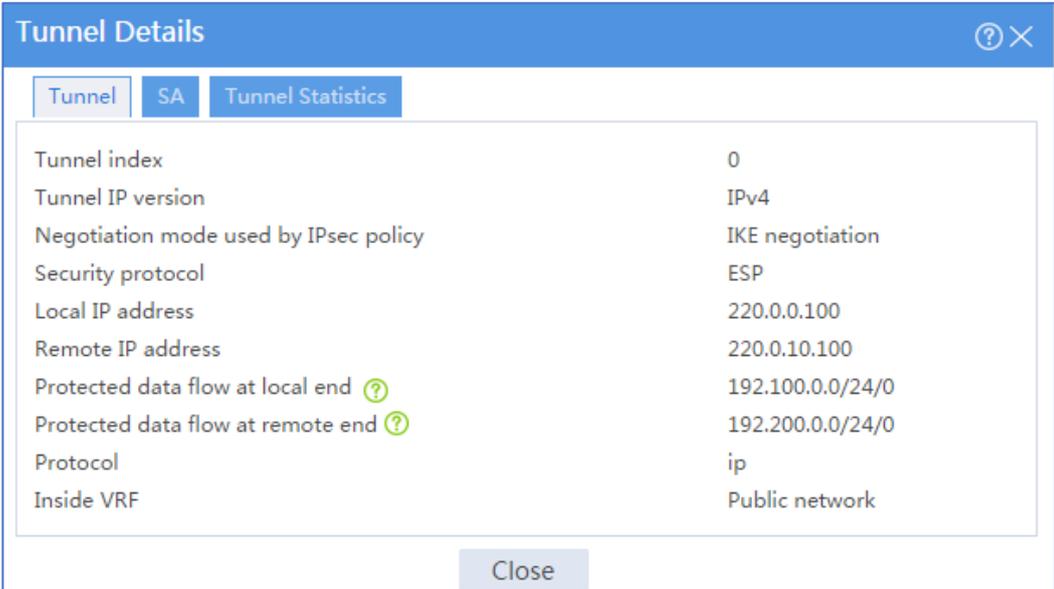
1. デバイス A とデバイス B が相互に通信できることを確認します。
2. デバイス A で、IPSecトンネル情報を表示します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**VPN > IPSec > IPSec Tunnels** を選択します。確立された IPSec トンネルが表示されます。

#IPSecトンネルの **Details** アイコンをクリックします。**Tunnel Details** ページには、トンネル情報、SA 情報、およびトンネル統計情報が表示されます。

図10 デバイス A 上の IPSec トンネルの詳細



The screenshot shows a 'Tunnel Details' window with three tabs: 'Tunnel', 'SA', and 'Tunnel Statistics'. The 'Tunnel' tab is active. The window displays the following information:

Tunnel index	0
Tunnel IP version	IPv4
Negotiation mode used by IPsec policy	IKE negotiation
Security protocol	ESP
Local IP address	220.0.0.100
Remote IP address	220.0.10.100
Protected data flow at local end ?	192.100.0.0/24/0
Protected data flow at remote end ?	192.200.0.0/24/0
Protocol	ip
Inside VRF	Public network

A 'Close' button is located at the bottom center of the window.

3. デバイス B で、IPSecトンネル情報を表示します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**VPN > IPSec > IPSec Tunnels** を選択します。確立された IPSec トンネルが表示されます。

#IPSecトンネルの **Details** アイコンをクリックします。**Tunnel Details** ページには、トンネル情報、SA 情報、およびトンネル統計情報が表示されます。

図11 デバイス B 上の IPsec トンネルの詳細

Tunnel	SA	Tunnel Statistics
Tunnel index		0
Tunnel IP version		IPv4
Negotiation mode used by IPsec policy		IKE negotiation
Security protocol		ESP
Local IP address		220.0.10.100
Remote IP address		220.0.0.100
Protected data flow at local end ?		192.200.0.0/24/0
Protected data flow at remote end ?		192.100.0.0/24/0
Protocol		ip
Inside VRF		Public network

Close

# SSL VPN 設定例

## はじめに

次に、SSL VPN の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、SSL VPN の基本的な知識があることを前提としています。

## 例:自己署名サーバー証明書によるWebアクセスの設定

### ネットワーク構成

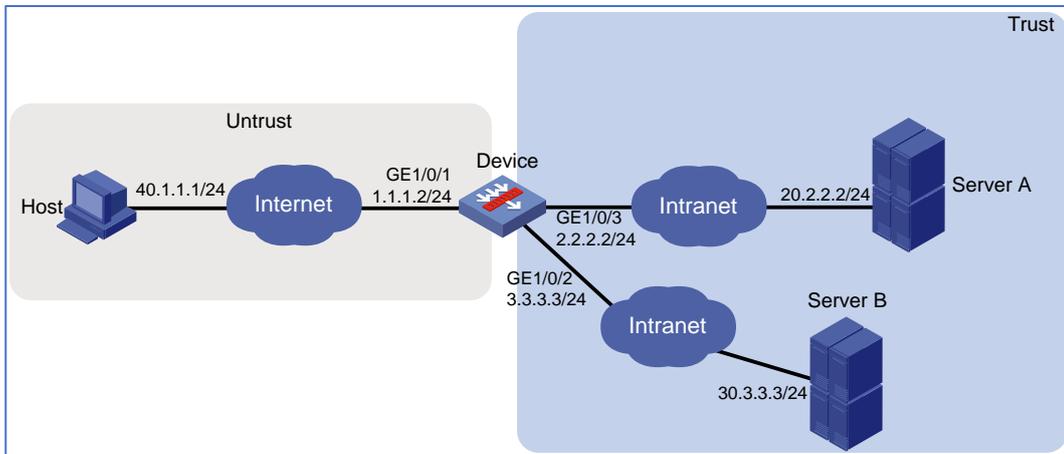
図1に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。ユーザーは、内部 Web サーバーであるサーバーA とサーバーB のリソースにアクセスする必要があります。両方のサーバーがポート 80 で HTTP を使用します。

ユーザーが Web アクセスモードでサーバーA およびサーバーB にアクセスできるように、デバイス上で SSL VPN Web アクセスサービスを設定します。

Web アクセスユーザーに対してローカル認証および認可を実行するようにデバイスを設定します。

デバイスは自己署名 SSL サーバー証明書を使用します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) 基本basic configurationタブで、**Trust**セキュリティゾーンを選択します。

B) **IPv4 Address**タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。

C) **OK**をクリックします。

#GE1/0/ge1//2 を **Trust** に追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 3.3.3.3/24 に設定します。

#GE1/0/ge1//3 を **Trust** に追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。

- Trust セキュリティゾーンと Untrust セキュリティゾーンの間にセキュリティポリシーを構成します。Trust セキュリティゾーンと Untrust セキュリティゾーンが相互に通信できることを確認してください。
- SSL VPNゲートウェイを設定します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。  
# **create** をクリックします。  
#図2に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。

図2 SSL VPN ゲートウェイの作成

Create Gateway

Gateway  \* (1-31 chars)

IP address  IPv4  IPv6

(Default: 0.0.0.0)

HTTPS port  (1025-65535, Default: 443.)

HTTP redirection

HTTP port  (1025-65535, Default: 80.)

SSL server policy

VRF

Enable

OK Cancel

- SSL VPNコンテキストを設定します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**SSL VPN > SSL VPN Contexts** を選択します。  
# **create** をクリックします。  
#図3に示すように、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。

図3 SSL VPN コンテキストの基本設定

The screenshot shows the 'Create SSL VPN Context' configuration window. The 'Basic settings' tab is selected. The configuration includes:

- Context name:** ctxweb (1-31 chars)
- Associated gateways:** A table with columns Gateway, Access..., Domain, Virtu..., and Edit. It contains one entry: sslvpngw, Domain..., domainweb.
- VRF:** Public network
- ISP domain:** (empty dropdown)
- Code verification:**
- Certificate auth:**
- Enable password:**
- Certificate and pwd authN:**  Use all methods,  Use any method
- IMC SMS verification:**
- Max sessions:** 1048575 (1-1048575)

Buttons at the bottom: Previous, Next, Cancel.

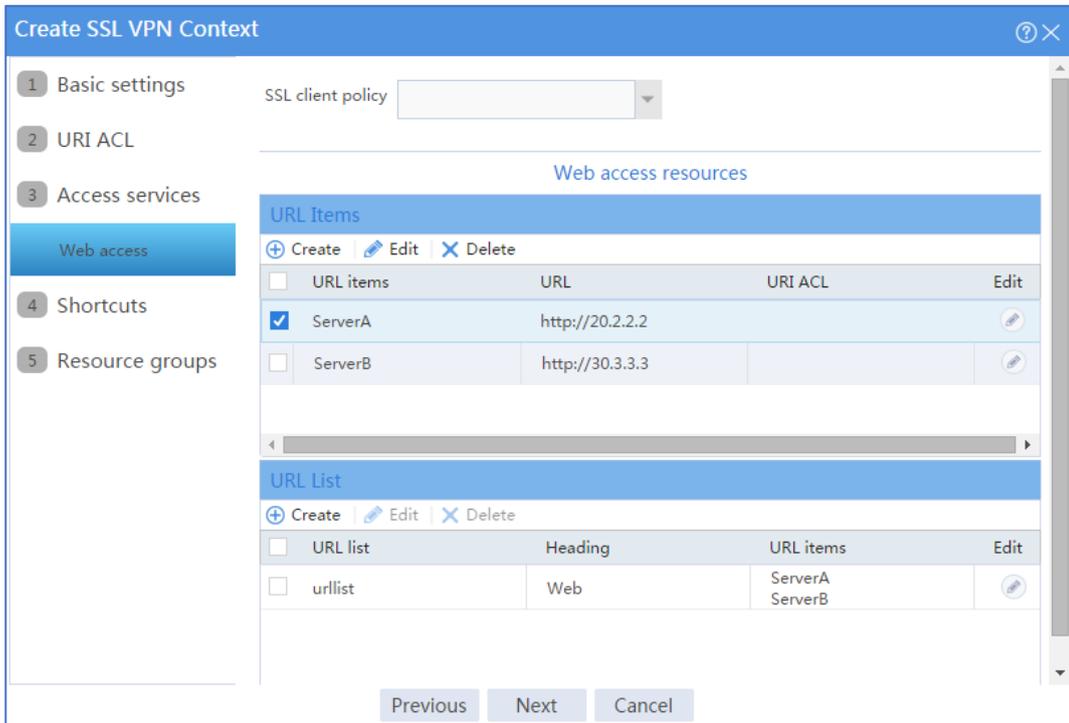
# **URI ACL** ページで、**Next** をクリックします。

# **Access services** ページで **Web Access** を選択し、**Next** をクリックします。

#**Web access** ページで、Web アクセスサービスを次のように設定します。

- A) サーバーAとサーバーBをそれぞれ指す2つのURL項目を設定します。
- B) 2つのURL項目をURLリストurllistに追加します。
- C) **next**をクリックします。

図4 Web access services の設定



# **Shortcut** ページで **next** をクリックします。

# **resource group** ページで、**create** をクリックします。

# **resourcegrp** という名前のリソースグループを作成し、アクセス可能な Web リソースとして URL リスト **urllist** を選択します(図5を参照)。

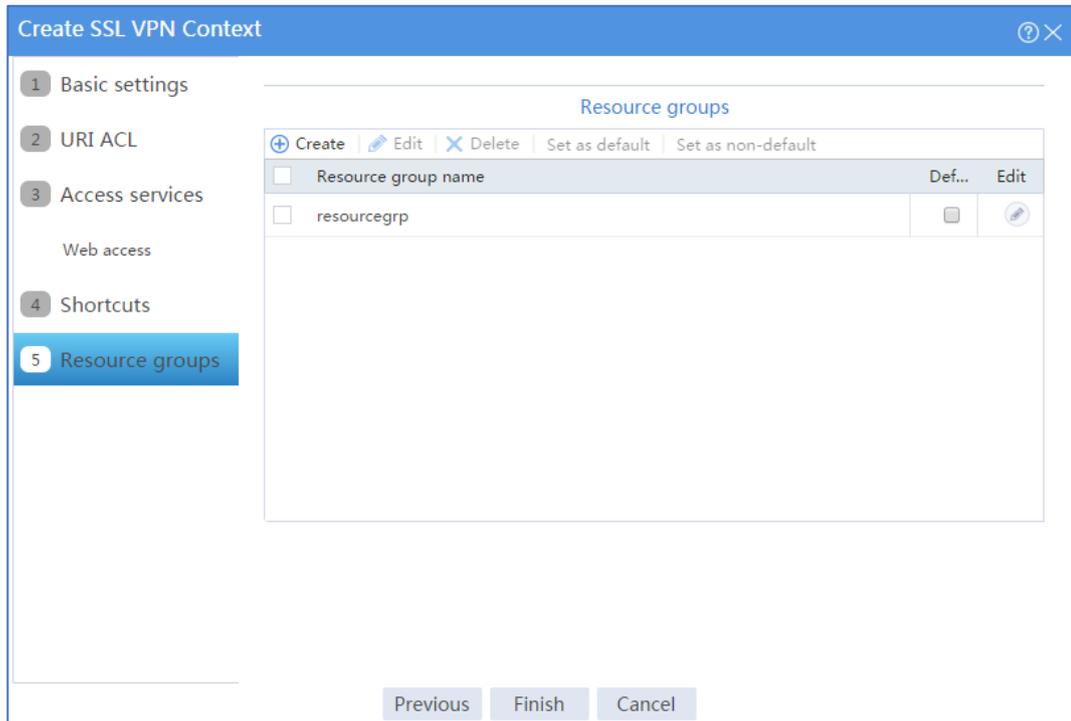
図5 SSL VPN リソースグループの作成

The image shows a 'Create Resource Group' dialog box. At the top, the title bar says 'Create Resource Group' with a help icon and a close button. Below the title bar, there is a 'Resource group' text input field containing the text 'resourcegrp'. To the right of this field is a red asterisk and the text '(1-31 chars)'. Below the 'Resource group' field is a 'Shortcut List' dropdown menu. A horizontal line separates this section from the 'Web access' section. The 'Web access' section has a title 'Web access' centered above two panes. The left pane is titled 'Web resources' and contains a search box labeled 'Filter' and a list titled 'Available URL Lists'. The right pane is titled 'Selected URL Lists(1)' and contains a search box labeled 'Filter' and a list with one item, 'urllist'. Between the two panes are four arrow buttons: a double right arrow, a single right arrow, a single left arrow, and a double left arrow. Below the panes are three dropdown menus labeled 'IPv4 ACL', 'IPv6 ACL', and 'URI ACL'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

#OK をクリックします。

Resource groups ページに、新しく作成されたリソースグループが表示されます(図6を参照)。

図6 リソースグループ設定ページ



# **finish** をクリックします。

# **Enable** チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図7を参照)。

図7 SSL VPNコンテキストのイネーブル化



Context name	Status	Gateway	Gateway access method	VRF	Enable	Edit
ctxweb	Enable	sslvpngw	Domain name:domainweb	Public network	<input checked="" type="checkbox"/>	

5. SSL VPNユーザーを作成します。

#トップナビゲーションバーで、**Objects** をクリックします。

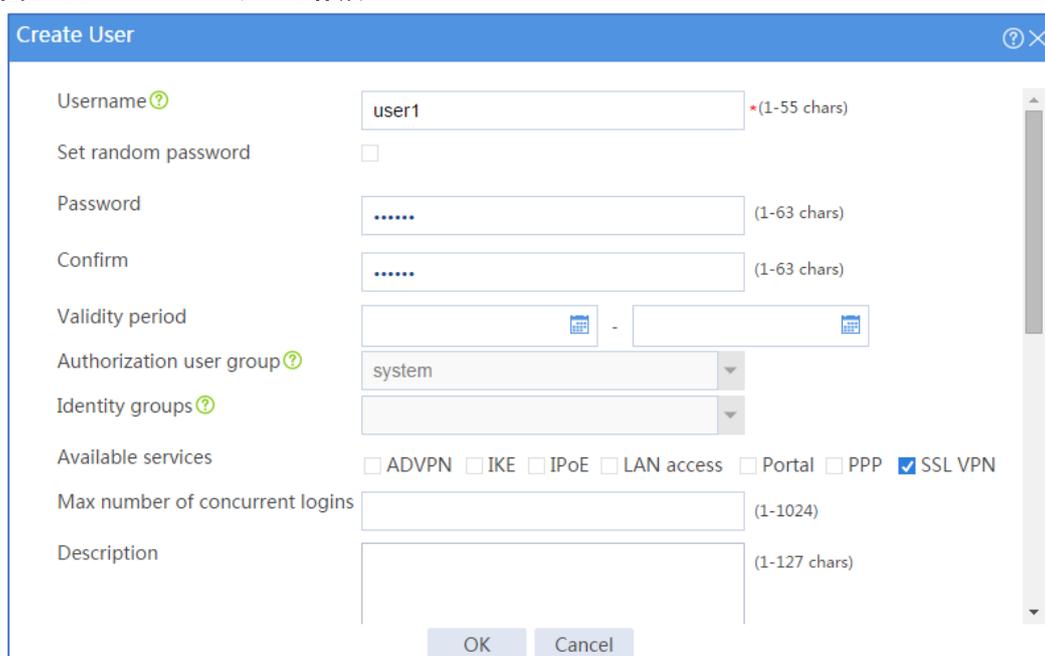
#ナビゲーションペインで、**User > User Management > Local Users** を選択します。

# **create** をクリックします。

#SSL VPN ユーザーを作成します。

A) ユーザー名を**user1**、パスワードを**123456**に設定し、使用可能なサービスとして**SSL VPN**を選択します(図8を参照)。

図8 SSL VPN ユーザーの作成



**Create User**

Username  \* (1-55 chars)

Set random password

Password  (1-63 chars)

Confirm  (1-63 chars)

Validity period  -

Authorization user group

Identity groups

Available services  ADVPN  IKE  IPoE  LAN access  Portal  PPP  SSL VPN

Max number of concurrent logins  (1-1024)

Description  (1-127 chars)

OK Cancel

B) Authorization Attributes領域で、ユーザーがSSL VPNリソースグループ resourcegrpを使用できるように許可します(図9を参照)。

図9 SSL VPN ユーザーの認可アトリビュートの設定

Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout  minutes(1-120)

Authorization VLAN  (1-4094)

SSL VPN policy group

A) OKをクリックします。

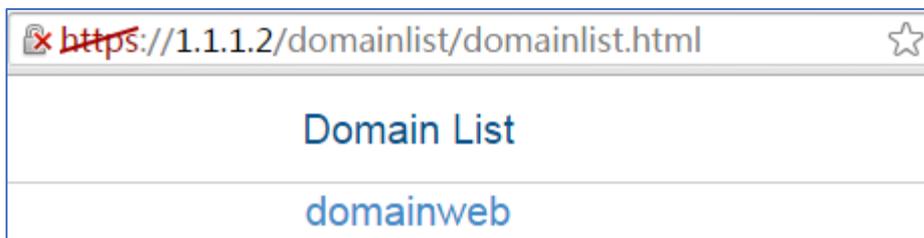
## ホストの構成

#ホストの IP アドレスとゲートウェイアドレスを設定し、SSL VPN ゲートウェイに到達できることを確認します。

## 設定の確認

1. ホストのブラウザアドレスバーに `https://1.1.1.2` と入力し、Enter キーを押してドメインリストページを開きます。

図10 ドメインリストページ



2. domainweb を選択してログインページにアクセスします。
3. ログインページで、username user1 と password123456 を入力し、Login をクリックします。

図11 ログインページ

Welcome to SSL VPN

Username

Password

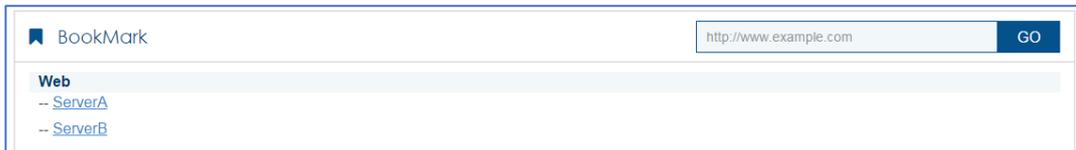
Login

Other login mode: [Certification login](#)

IP access client: [Download](#)

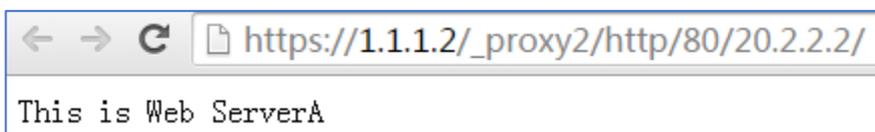
SSL VPN ホームページが開き、ユーザーがアクセスできる Web リソースが BookMark 領域に表示されます。

図12 アクセス可能な Web リソース



4. ServerA をクリックして、サーバーA 上の Web リソースにアクセスします。

図13 サーバーA へのアクセス



5. ServerB をクリックして、サーバーB 上の Web リソースにアクセスします。

図14 サーバーB へのアクセス



## 例:相互証明書認証によるWebアクセスの設定

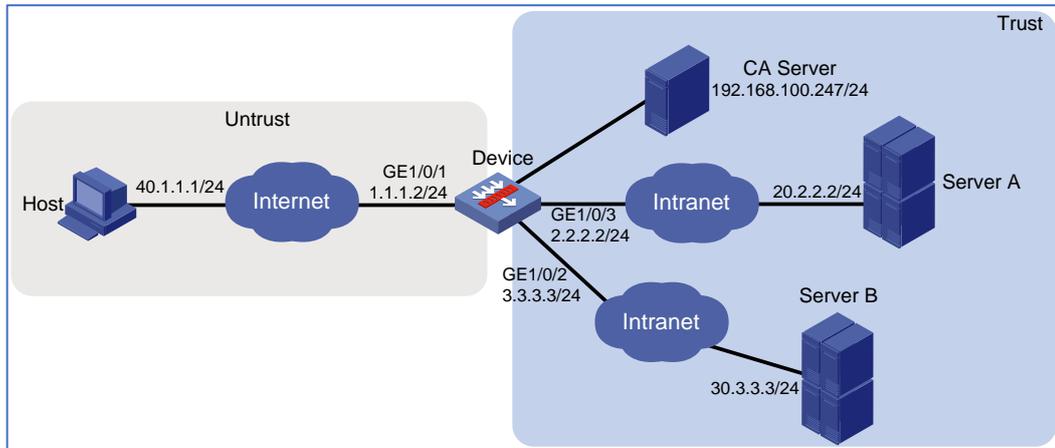
### ネットワーク構成

図1に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。Windows Server2008R2CA サーバーがプライベートネットワークに配置されています。ユーザーは内部 Web サーバーサーバーA とサーバーB のリソースにアクセスする必要があります。両方の Web サーバーはポート 80 で HTTP を使用します。

ユーザーが Web アクセスモードでサーバーA およびサーバーB にアクセスできるように、デバイス上で SSL VPN Web アクセスサービスを設定します。

Web アクセスユーザーに対してローカル認証と認可を実行するようにデバイスを構成します。ユーザーに Web アクセス用のパスワード認証と証明書認証の両方を渡すように要求します。セキュリティを強化するには、デフォルトの証明書を使用するのではなく、CA サーバーからデバイスの SSL サーバー証明書を要求します。

図15ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** タブをクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。
    - B) IPv4 Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。
    - C) OKをクリックします。
  - #GE1/0/ge1//2 を Trust セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 3.3.3.3/24 に設定します。
  - #GE1/0/ge1//3 を Trust セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。

2. **Trust** セキュリティゾーンと **Untrust** セキュリティゾーンの間にセキュリティポリシーを構成します。**Trust** セキュリティゾーンと **Untrust** セキュリティゾーンが相互に通信できることを確認してください。
3. デバイスのサーバー証明書を要求します。
  - A) 証明書のサブジェクトを作成します。
    - # トップナビゲーションバーで、**Object** をクリックします。
    - # ナビゲーションペインで、**PKI > Certificate Subject** を選択します。
    - # **create** をクリックします。
    - # 図16に示すように、証明書のサブジェクトを作成し、OK をクリックします。

図16 証明書サブジェクトの作成

Create Certificate Subject

Certificate subject name  \*(1-31 chars)

Common name  (1-63 chars)

Country code  (2 chars, case sensitive)

State or province name  (1-63 chars)

Locality  (1-63 chars)

Organization name  (1-63 chars)

Organization unit name  (1-63 chars)

FQDN  (1-255 chars)

IP address  IPv4 address  Use interface's primary IP address

OK Cancel

- B) PKIドメインを作成します。
  - # Certificate ページで、Create PKI domain をクリックします。
  - # 図17に示すように PKI ドメインを作成し、OK をクリックします。

図17 PKIドメインの作成

Create PKI Domain

Domain name  \*(1-31 chars)

Certificate subject

Key pairs for certificate request

Algorithm

Use different key pairs for encryption and signing

Key pair name  (1-64 chars)

Key length  (512-2048)

CRL checking  Check if a certificate has been revoked by the CA

Certificate usage extensions  IKE  SSL server  SSL client

Encryption algorithm for PKCS#7 cert files

OK Cancel

- C) 証明書要求を作成します。
- # **certificate** ページで、**Submit Cert Request** をクリックします。
  - #図18に示すように、証明書要求の設定を行います。

図18 証明書要求の作成

Submit Cert Request

PKI domain sslvpndomain \* [Edit]

Certificate subject <sup>?</sup> sslvpncert \* [Edit]

---

Algorithm <sup>?</sup> RSA \*

Use different key pairs for encryption and signing

Key pair name sslvpnrsa \*

Key length 1024

---

Password for cert revocation (1-31 chars)

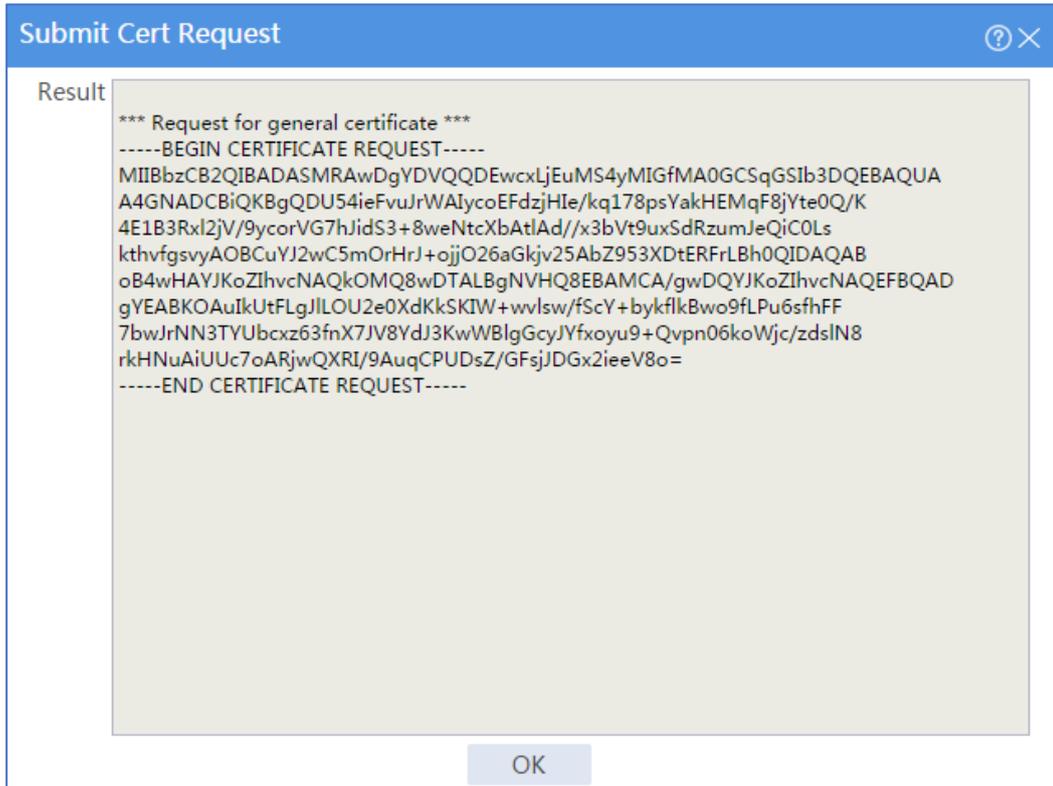
Confirm password

OK Cancel

#OK をクリックします。

証明書要求の内容が表示されます(図19を参照)。

図19 証明書要求の内容



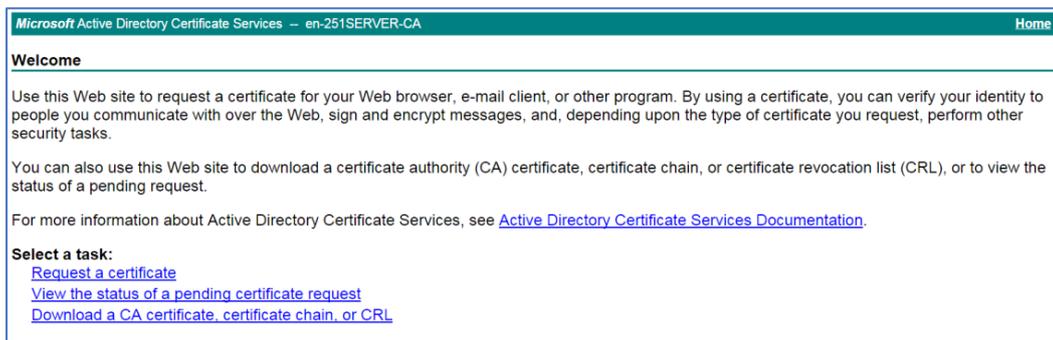
#証明書要求の内容をコピーし、OK をクリックします。

D) CAにサーバー証明書を要求する:

#ブラウザのアドレスバーに `http://192.168.100.247/certsrv` と入力します。

#図20に示す証明書サービスのホームページで、Request a certificate をクリックします。

図20 証明書サービスのホームページ



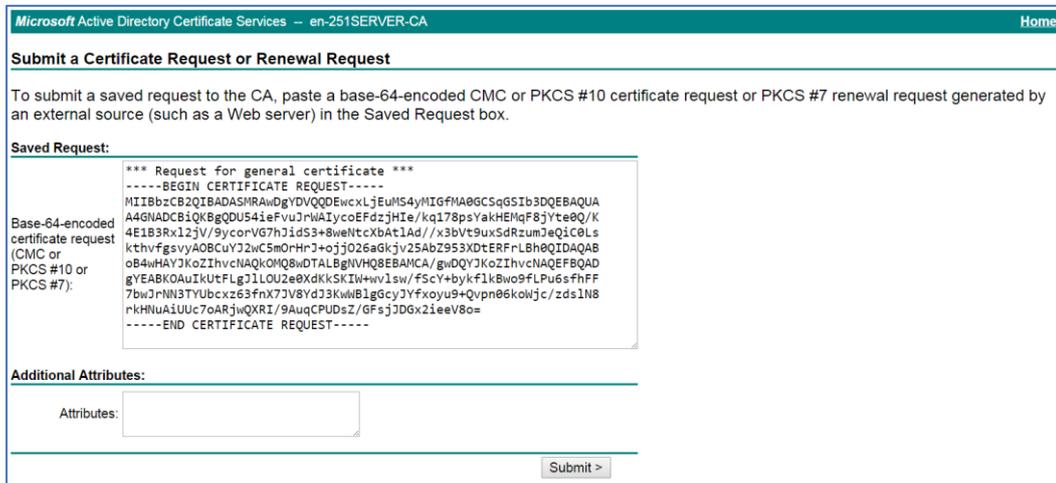
#図21に示す Request a Certificate ページで、Advanced Certificate Request をクリックします。

図21 証明書の要求ページ



#以前にコピーした証明書要求の内容を Base-64-encoded certificate request CMC or PKCS#10or PKCS#7 フィールドに貼り付けます(図22を参照)。

図22 証明書要求の内容の貼り付け

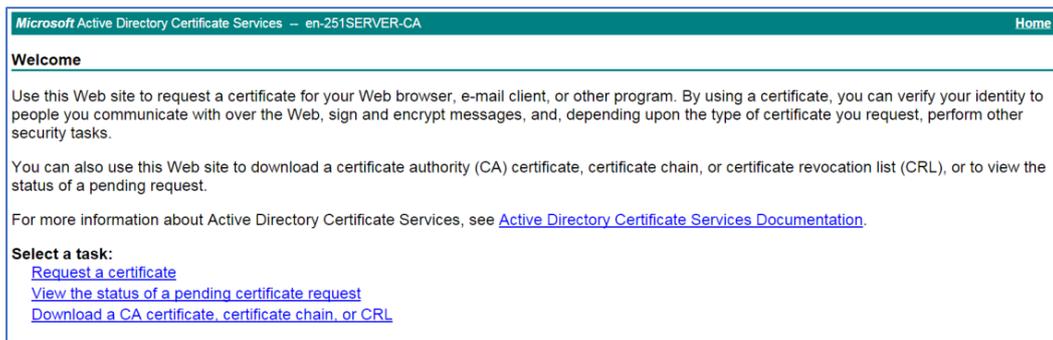


#Submit をクリックします。

証明書要求が CA 管理者によって承認されたら、ブラウザのアドレスバーに http://192.168.100.247/certsrv と入力します。

#に示す証明書サービスのホームページで、View the status of a pending certificate request をクリックします。

図23 証明書サービスのホームページ



#表示する証明書要求を選択します。

図24 Status of a Pending Certificate Request ページの表示



Certificate Issued ページが開き、要求されたサーバー証明書が発行されたことが示されます(図25を参照)。

図25 証明書発行ページ



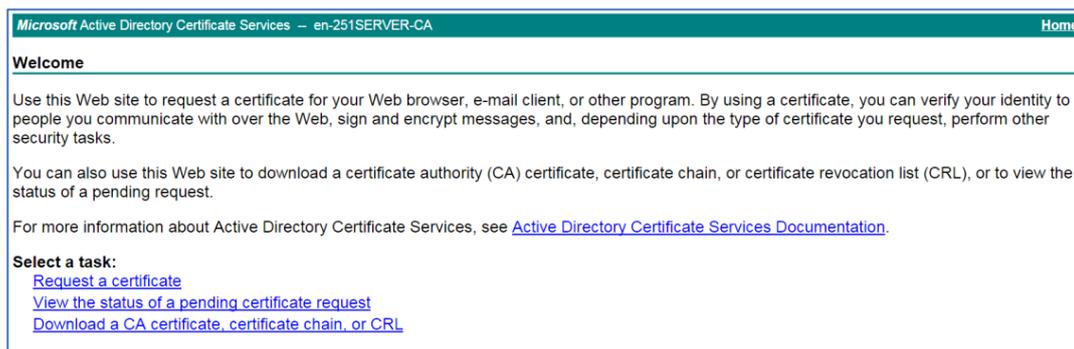
#Download certificate をクリックしてサーバー証明書をダウンロードし、ローカルに保存します。

4. CA証明書をダウンロードします。

#ブラウザのアドレスバーに <http://192.168.100.247/certsrv> と入力します。

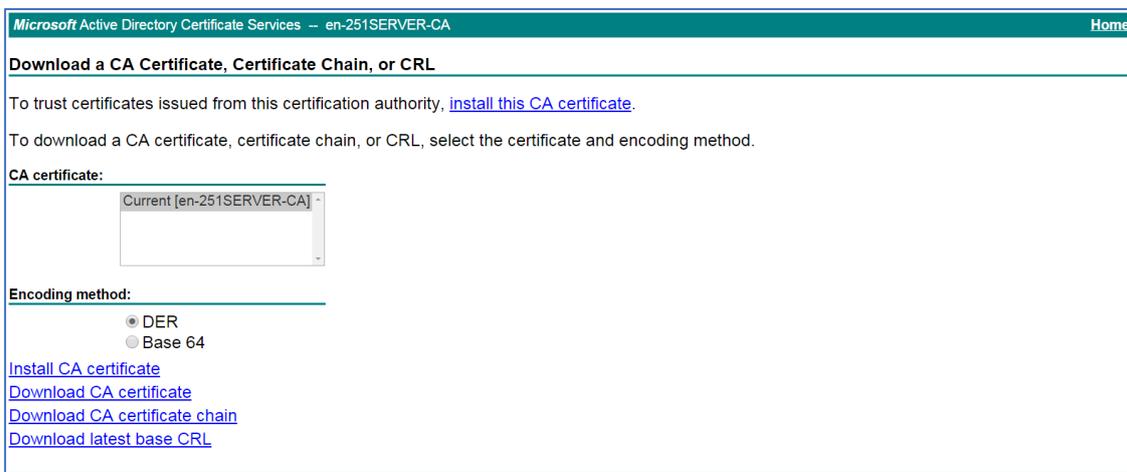
#図26に示す証明書サービスのホームページで、Download a CA certificate,certificate chain,or CRL をクリックします。

図26 証明書サービスのホームページ



#図27の Download a CA certificate,certificate chain,or CRL ページで、Download CA certificate をクリックします。

図27 CA 証明書、証明書チェーン、または CRL ページのダウンロード



#ダウンロードした CA 証明書をローカルに保存します。

5. CA証明書とサーバー証明書をPKIドメインにインポートします。

A) CA証明書をインポートします。

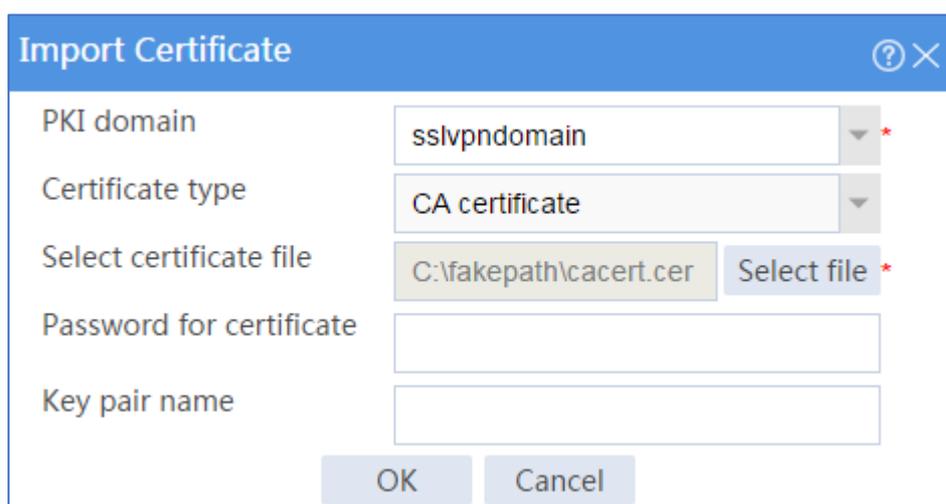
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**PKI > Certificate** を選択します。

# **import certificate** をクリックします。

#ローカルに保存された CA 証明書をインポートし(を参照)、OK をクリックします。

図28 CA 証明書のインポート



B) サーバー証明書をインポートします。

# **certificate** ページで、**import certificate** をクリックします。

#ローカルに保存されたサーバー証明書をインポートし(図29を参照)、OK をクリックします。

図29 サーバー証明書のインポート

The screenshot shows a dialog box titled "Import Certificate". It has a blue header bar with a question mark icon and a close button. The dialog contains the following fields and controls:

- PKI domain:** A dropdown menu with "sslvpnomain" selected and a red asterisk to its right.
- Certificate type:** A dropdown menu with "Local certificate" selected.
- Select certificate file:** A text box containing "C:\fakepath\localcert.cer" and a "Select file" button with a red asterisk to its right.
- Password for certificate:** An empty text box.
- Key pair name:** An empty text box.

At the bottom of the dialog are two buttons: "OK" and "Cancel".

6. SSLサーバーポリシーを設定します。

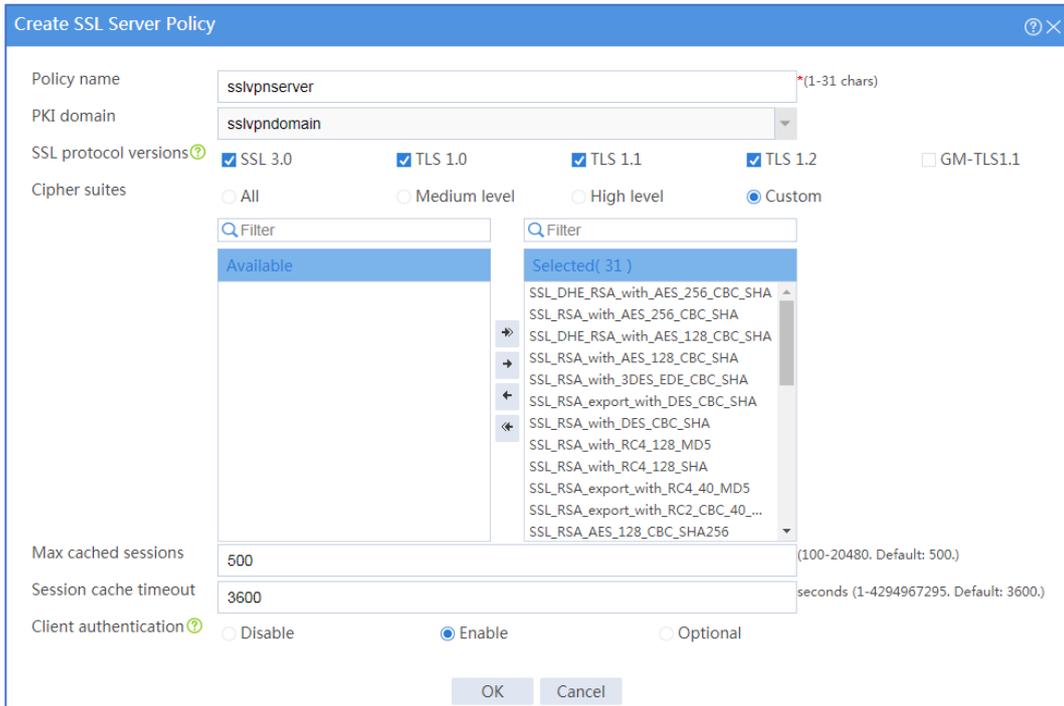
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、SSL>SSL Server Policies を選択します。

# **create** をクリックします。

#図30に示すように SSL サーバーポリシーを設定し、OK をクリックします。

図30 SSL サーバーポリシーの作成



7. SSLクライアントポリシーを構成します。

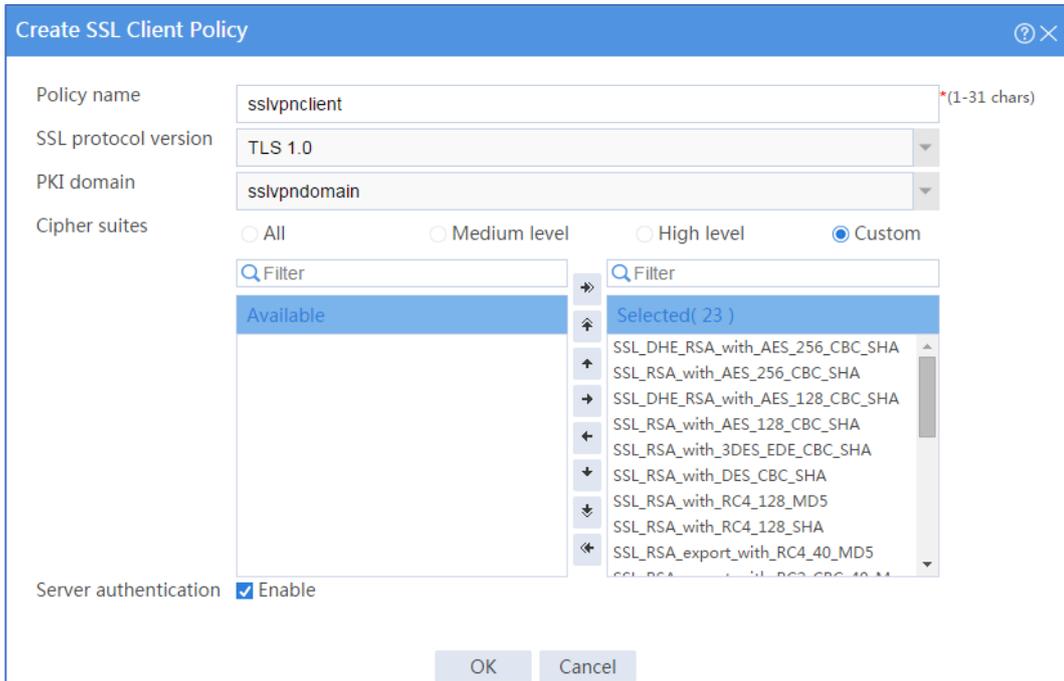
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**SSL > SSL Client Policies** を選択します。

# **create** をクリックします。

#図31 に示すように SSL クライアントポリシーを設定し、OK をクリックします。

図31 SSL クライアントポリシーの作成



8. SSL VPNゲートウェイを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。

# **create** をクリックします。

#図32に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。

図32 SSL VPN ゲートウェイの作成

Create Gateway

Gateway? sslvpngw \*(1-31 chars)

IP address?  IPv4  IPv6

1.1.1.2 (Default: 0.0.0.0)

HTTPS port 443 (1025-65535. Default: 443.)

HTTP redirection

HTTP port 80 (1025-65535. Default: 80.)

SSL server policy sslvpnsrvr

VRF Public network

Enable

OK Cancel

9. SSL VPNコンテキストを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Contexts** を選択します。

# **create** をクリックします。

#図33に示すように、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。

図33 SSL VPN コンテキストの基本設定

Create SSL VPN Context

1 Basic settings

Context name  (1-31 chars)

2 URI ACL

Associated gateways

	Gate...	Access me...	Domain	Virtual ...	Edit
<input type="checkbox"/>	sslvp...	Domain n...	domain...		

3 Access services

4 Shortcuts

5 Resource groups

VRF

ISP domain

Code verification

Certificate auth

Enable password

Certificate and pwd authN  Use all methods  Use any method

IMC SMS verification

Max sessions  (1-1048575)

Previous Next Cancel

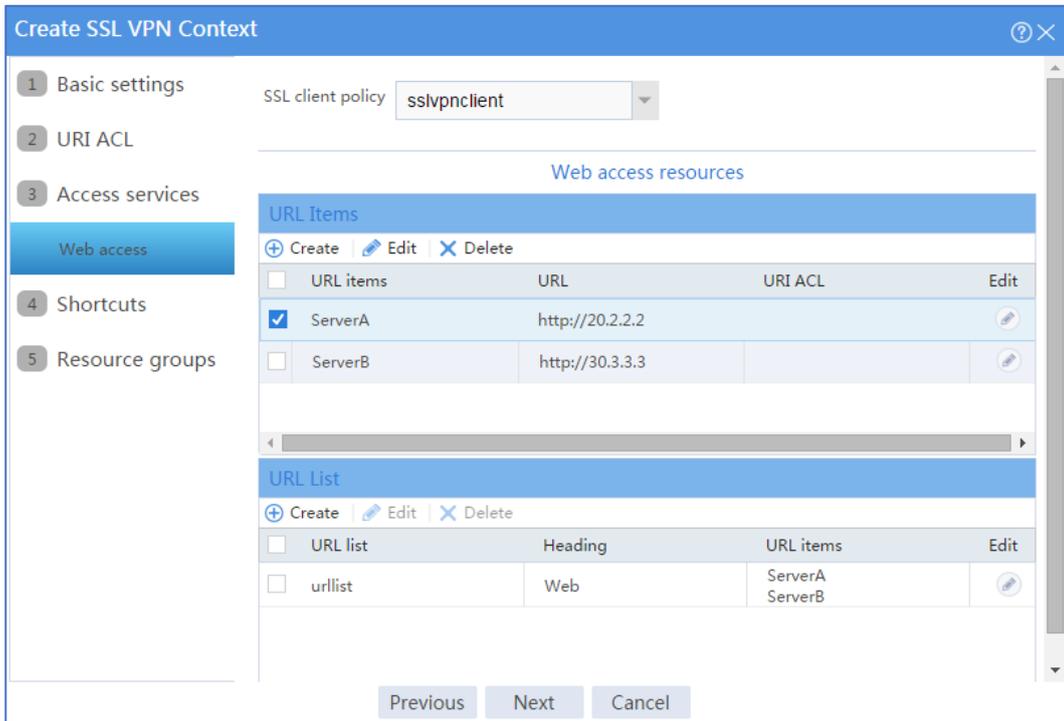
#URI ACL ページで、Next をクリックします。

# Access Services ページで Web access を選択し、Next をクリックします。

#Web access ページで、Web アクセスサービスを次のように設定します。

- SSLクライアントポリシーリストからsslvpnclientを選択します。
- サーバーAとサーバーBをそれぞれ指す2つのURL項目を設定します。
- 2つのURL項目をURLリストurllistに追加します。
- Nextをクリックします。

図34 Web アクセスサービスの構成



# Short cut ページで next をクリックします。

# Resource groups ページで、Create をクリックします。

# resourcegrp という名前のリソースグループを作成し、アクセス可能な Web リソースとして URL リスト urllist を選択します(図35を参照)。

#OK をクリックします。

図35 SSL VPN リソースグループの作成

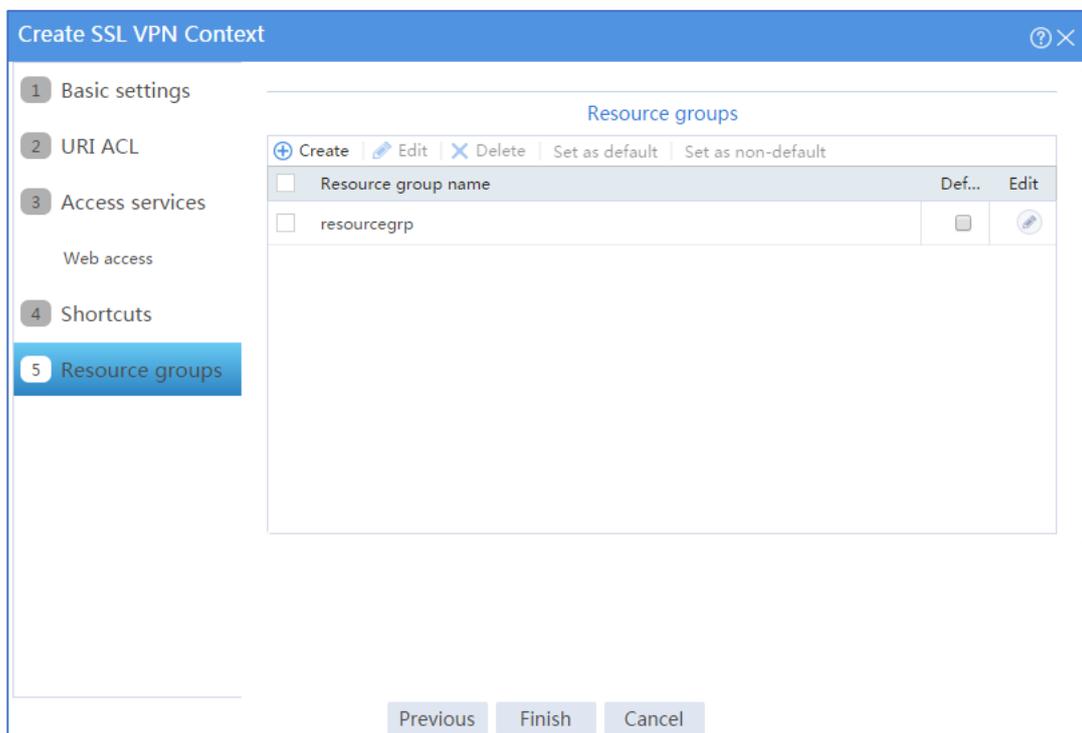
The image shows a 'Create Resource Group' dialog box. At the top, the title bar reads 'Create Resource Group' with a help icon and a close button. Below the title bar, there are several input fields and sections:

- Resource group:** A text input field containing 'resourcegrp' with a red asterisk and '(1-31 chars)' to its right.
- Shortcut List:** A dropdown menu that is currently empty.
- Web access:** A section with a blue header. It contains two panes:
  - Available URL Lists:** A list box with a search filter 'Filter' above it. It is currently empty.
  - Selected URL Lists( 1 ):** A list box with a search filter 'Filter' above it. It contains one item, 'urllist'.
  - Between the panes are four arrow buttons: a right-pointing arrow, a right-pointing arrow, a left-pointing arrow, and a double left-pointing arrow.
- IPv4 ACL:** A dropdown menu that is empty.
- IPv6 ACL:** A dropdown menu that is empty.
- URI ACL:** A dropdown menu that is empty.

At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

Resource groups ページに、新しく作成されたリソースグループが表示されます(図36を参照)。

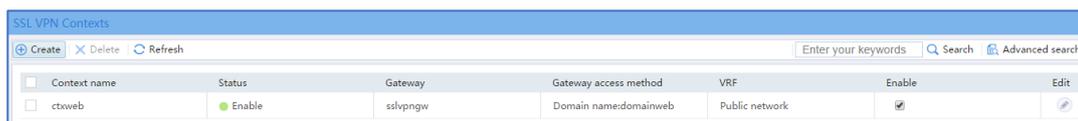
図36 リソースグループ設定ページ



# **Finish** をクリックします。

# **Enable** チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図37を参照)。

図37 SSL VPN コンテキストのイネーブル化



10. SSL VPNユーザーを作成します。

# トップナビゲーションバーで、**Objects** 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。

# **create** をクリックします。

# SSL VPN ユーザーを作成します。

A) ユーザー名をuser1、パスワードを123456に設定し、使用可能なサービスとしてSSL VPNを選択します(図38を参照)。

図38 SSL VPN ユーザーの作成

Create User

Username <sup>?</sup> user1 \* (1-55 chars)

Set random password

Password ..... (1-63 chars)

Confirm ..... (1-63 chars)

Validity period [calendar] - [calendar]

Authorization user group <sup>?</sup> system

Identity groups <sup>?</sup>

Available services  ADVPN  IKE  IPoE  LAN access  Portal  PPP  SSL VPN

Max number of concurrent logins (1-1024)

Description (1-127 chars)

OK Cancel

Authorization Attributes 領域で、ユーザーが SSL VPN リソースグループ resourcegrp を使用できるように許可します(図39を参照)。

図39 SSL VPN ユーザーの認可アトリビュートの設定

Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout minutes (1-120)

Authorization VLAN (1-4094)

SSL VPN policy group resourcegrp (1-31 chars)

OK をクリックします。

## ホストの構成

1. ホストのIPアドレスとゲートウェイアドレスを設定し、SSL VPNゲートウェイおよびCAサーバーに到達できることを確認します。
2. クライアント証明書要求をCAサーバーに送信します。
  - A) ブラウザのアドレスバーに<http://192.168.100.247/certsrv>と入力します。

- B) 図40に示す証明書サービスのホームページで、**Request a certificate**をクリックします。

図40 証明書サービスのホームページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- C) Request a Certificateページ(図41を参照)で、Advanced Certificate Requestをクリックします。

図41 証明書の要求ページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

**Request a Certificate**

Select the certificate type:

- [Web Browser Certificate](#)
- [E-Mail Protection Certificate](#)

Or, submit an [advanced certificate request](#).

- D) クライアント証明書要求を作成します(図42を参照)。

図42 クライアント証明書要求の作成

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

**Advanced Certificate Request**

**Identifying Information:**

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

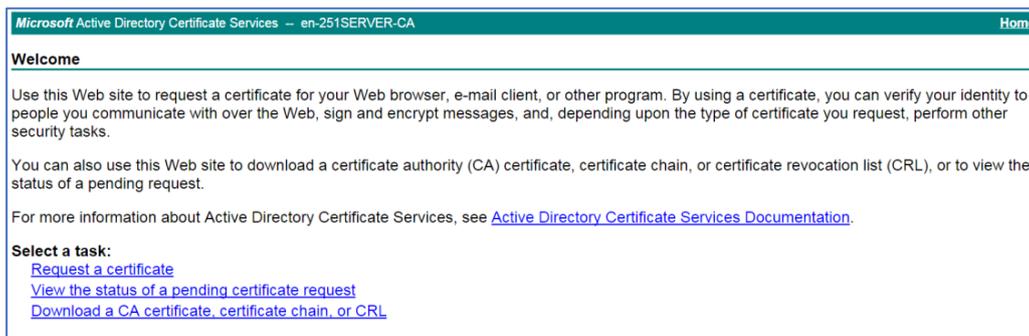
**Type of Certificate Needed:**

- E) submitをクリックします。

3. クライアント証明書をホストにインストールします。

- A) 証明書要求がCA管理者によって承認されたら、ブラウザのアドレスバーに <http://192.168.100.247/certsrv>と入力します。
- B) 図43に示す証明書サービスのホームページで、View the status of a pending certificate requestをクリックします。

**図43 証明書サービスのホームページ**



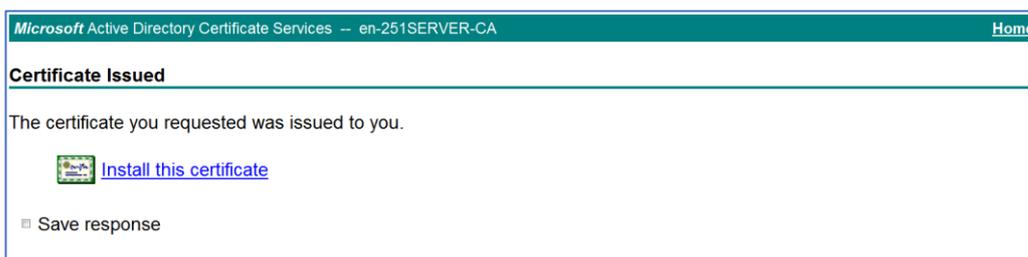
View the Status of a Pending Certificate Request ページが開きます(図44を参照)。

**図44 Status of a Pending Certificate Request ページの表示**



- C) ステータスを表示するクライアント証明書をクリックします。
- D) Certificate Issuedページ(図45を参照)で、Install this certificateをクリックしてクライアント証明書をインストールします。

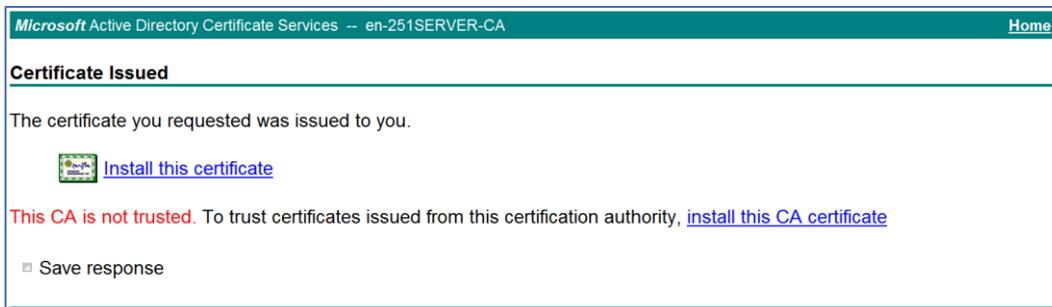
**図45 クライアント証明書のインストール**



ホストに CA 証明書がない場合、に示すページが開きます。最初に CA 証明書をインストールする必要があります。

- E) **install this CA certificate**をクリックしてCA証明書をインストールし、**Install this certificate**をクリックしてクライアント証明書をインストールします。

図46 CA 証明書とクライアント証明書のインストール



クライアント証明書をインストールすると、に示す Certificate Installed ページが開きます。

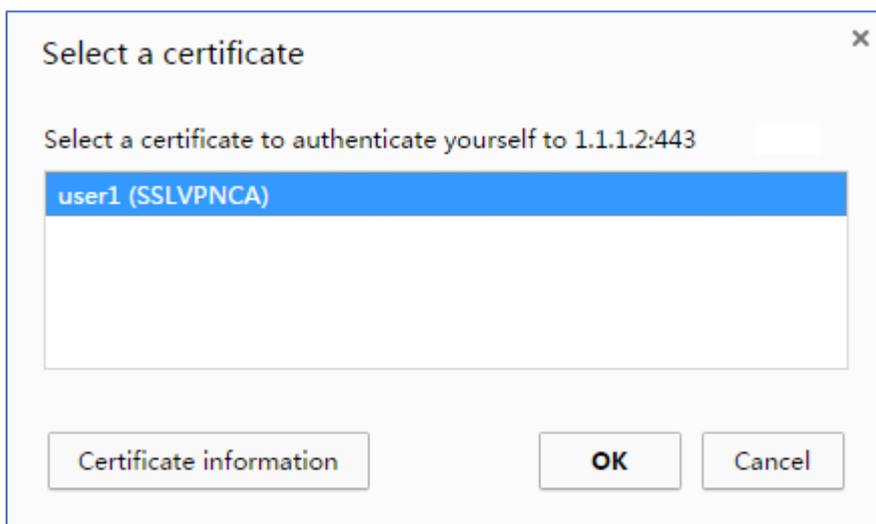
図47 Certificate Installed ページ



## 設定の確認

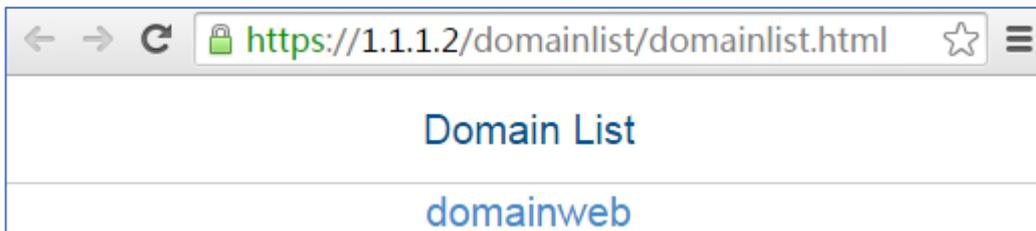
1. ホストのブラウザアドレスバーに https://1.1.1.2 と入力し、Enter を押します。
2. Select a certificate ページで、認証用のクライアント証明書を選択します(図48を参照)。

図48 証明書の選択ページ



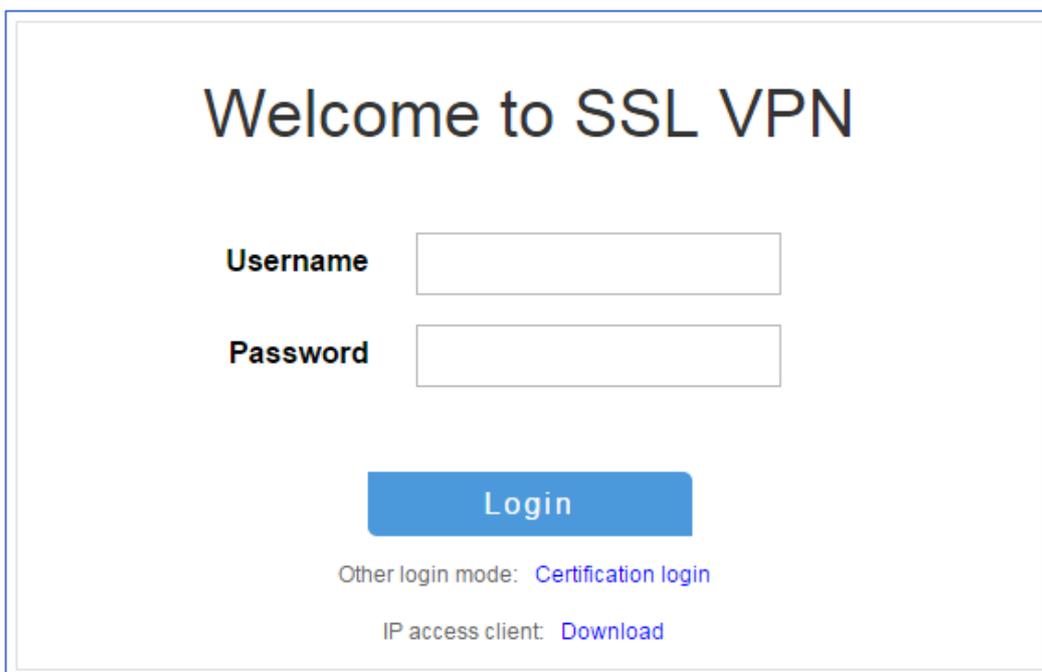
3. OK をクリックします。
4. Domain List ページ(図49を参照)で、domainweb をクリックします。

図49 Domain Listページ



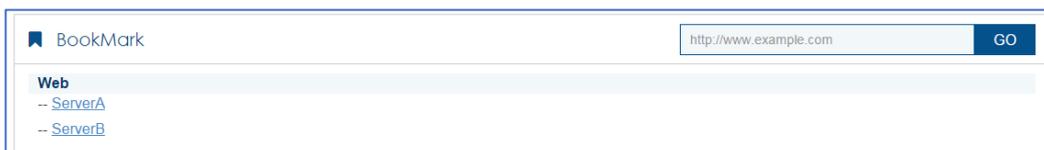
5. 図50に示す SSL VPN ログインページで、username user1 と password および 123456 を入力し、Login をクリックします。

図50 SSL VPN ログインページ



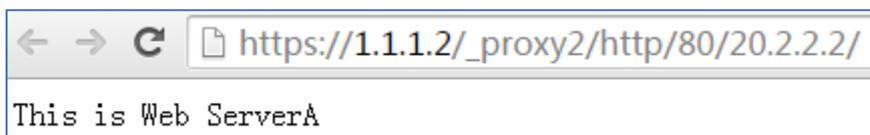
SSL VPN ホームページが開き、ユーザーがアクセスできる Web リソースが BookMark 領域に表示されます(図51を参照)。

図51 アクセス可能な Web リソース



6. **ServerA** をクリックして、サーバーA 上の Web リソースにアクセスします。

図52 ServerA へのアクセス



7. **ServerB** をクリックして、サーバーB 上の Web リソースにアクセスします。

図53 ServerB へのアクセス



## 例:自己署名サーバー証明書によるTCPアクセスの設定

### ネットワーク構成

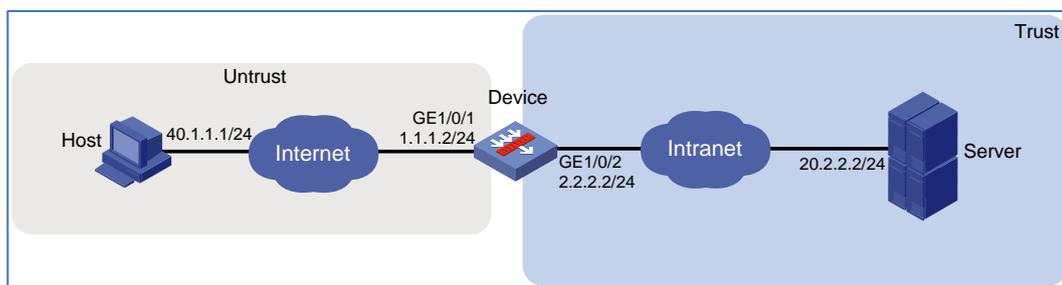
図54に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。ユーザーは、TCP アクセスモードで内部 Telnet サーバーにセキュアにアクセスする必要があります。

ユーザーがTCPアクセスモードでサーバーにアクセスできるように、デバイス上でSSL VPN TCP アクセスサービスを設定します。

TCP アクセスユーザーに対してローカル認証および認可を実行するようにデバイスを設定します。

デバイスは自己署名 SSL サーバー証明書を使用します。

図54 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

自己署名サーバー証明書を使用して TCP アクセスを設定する場合は、次の制限事項およびガイドラインに従ってください。

- 証明書ベースのクライアント認証は、TCP アクセスモードでは使用できません。
- Web インターフェイスから TCP クライアントを起動するには、Java Runtime Environment バージョン 1.7(JRE1.7)以降がクライアントホストにインストールされていることを確認してください。
- ホストから TCP アクセスモードで内部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な場合があります。管理者権限でホストにログインしてください。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - # トップナビゲーションバーで、**Network** タブをクリックします。
  - # ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - # GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- A) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。
- B) IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。
- C) OKをクリックします。

#GE1/0/ge1//2を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。

- 2. trust セキュリティゾーンと untrust セキュリティゾーンの間にセキュリティポリシーを構成します。Trust するセキュリティゾーンと Untrust セキュリティゾーンが相互に通信できることを確認してください。
- 3. SSL VPNゲートウェイを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。

#**create** をクリックします。

#図55に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。

図55 SSL VPN ゲートウェイの作成

Create Gateway

Gateway  \*(1-31 chars)

IP address  IPv4  IPv6

(Default: 0.0.0.0)

HTTPS port  (1025-65535. Default: 443.)

HTTP redirection

HTTP port  (1025-65535. Default: 80.)

SSL server policy

VRF

Enable

OK Cancel

- 4. **SSL VPN**コンテキストを設定します。  
#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Contexts** を選択します。

#**create** をクリックします。

#図56に示すように、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。

#### 図56 SSL VPN コンテキストの作成

The screenshot shows the 'Create SSL VPN Context' dialog box with the following settings:

- Context name:** ctxtcp (1-31 chars)
- Associated gateways:** A table with columns Gateway, Access..., Domain, Virtua..., and Edit. One entry is visible: sslvpngw, Domain..., domaintcp.
- VRF:** Public network
- ISP domain:** (empty)
- Code verification:**
- Certificate auth:**
- Enable password:**
- Certificate and pwd authN:**  Use all methods,  Use any method
- IMC SMS verification:**
- Max sessions:** 1048575 (1-1048575)

Buttons: Previous, Next, Cancel

#URI ACL ページで、Next をクリックします。

#**Access services** ページで **TCP access** を選択し、**Next** をクリックします。

#**TCP access** ページで、**Port Forwarding Item** 領域の **Create** をクリックします。

#**pfitem** という名前のポート転送アイテムを作成し(図57を参照)、OK をクリックします。

図57 ポート転送アイテムの作成

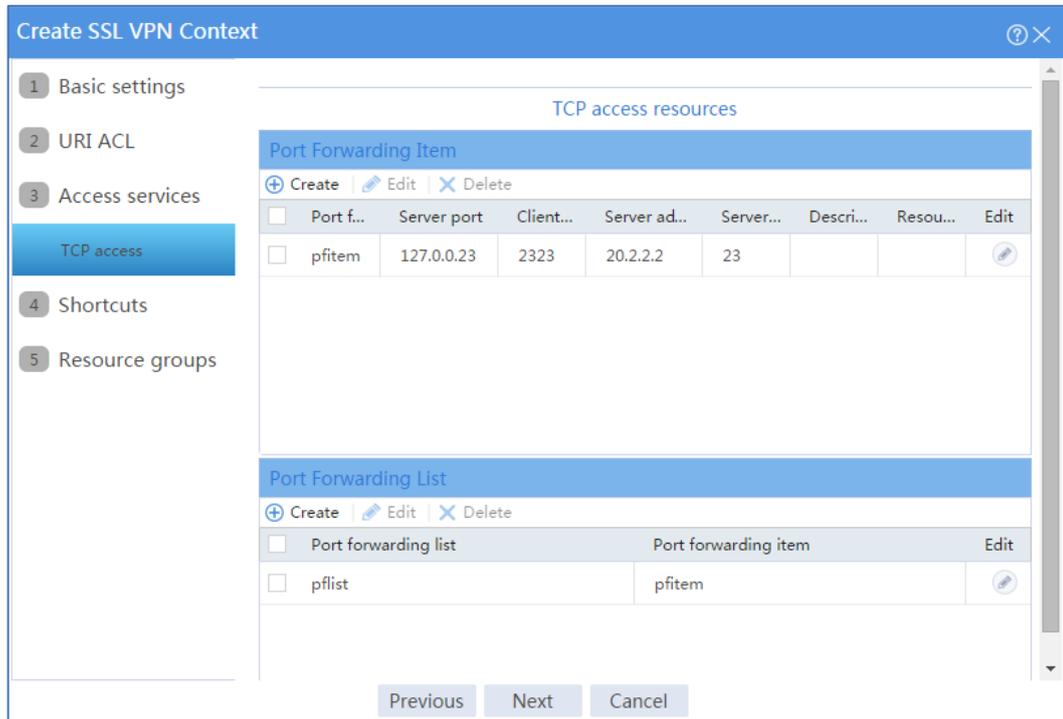
Name	<input type="text" value="pfitem"/>	* (1-31 chars)
Client host <span>?</span>	<input type="text" value="127.0.0.23"/>	* (1-253 chars)
Client port	<input type="text" value="2323"/>	* (1-65535)
Server address <span>?</span>	<input type="text" value="20.2.2.2"/>	* (1-253)
Server port	<input type="text" value="23"/>	* (1-65535)
Description	<input type="text"/>	(1-63 chars)
Resource link <span>?</span>	<input type="text" value="url('http://10.0.0.1:8080/cmd')"/>	(1-255 chars)

OK Cancel

#Port Forwarding List 領域で Create をクリックします。

#pflist という名前のポート転送リストを作成し、ポート転送アイテム pfitem を割り当てます(図58を参照)。

図58 TCP アクセスリソースの設定

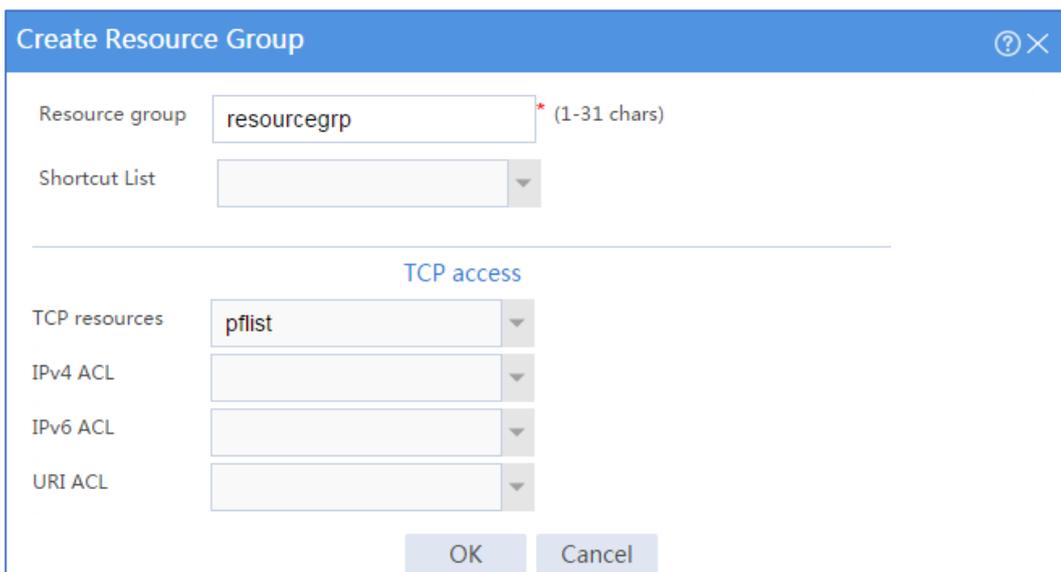


# Shortcuts ページで next をクリックします。

# Resource groups ページで、create をクリックします。

# resourcegrp という名前のリソースグループを作成し、図59に示すように、TCP resources リストからポート転送リスト pflist を選択します。

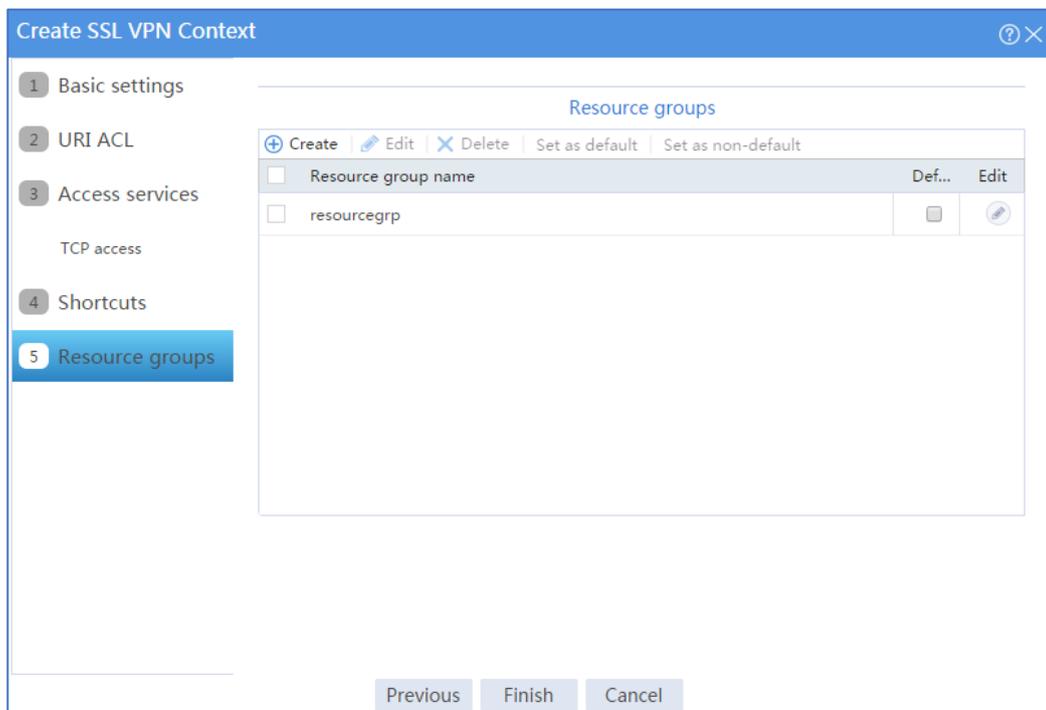
図59 SSL VPN リソースグループの作成



#OK をクリックします。

Resource groups ページに、新しく作成されたリソースグループが表示されます(を参照)。

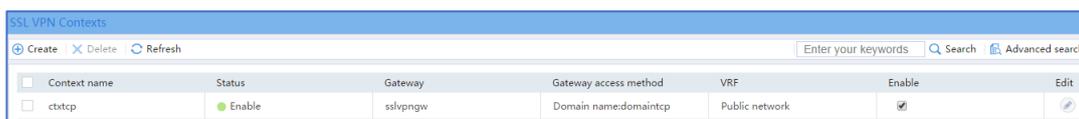
図60 リソースグループ設定ページ



#完了をクリックします。

#Enable チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図61を参照)。

図61 SSL VPN コンテキストのイネーブル化



## 5. SSL VPNユーザーを作成します。

#トップナビゲーションバーで、**Objects** 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。

# **create** をクリックします。

#SSL VPN ユーザーを作成します。

A) ユーザー名をuser1、パスワードを123456に設定し、使用可能なサービスとしてSSL VPNを選択します(図62を参照)。

図62 SSL VPN ユーザーの作成

Create User

Username <sup>?</sup> user1 \* (1-55 chars)

Set random password

Password ..... (1-63 chars)

Confirm ..... (1-63 chars)

Validity period [calendar] - [calendar]

Authorization user group <sup>?</sup> system

Identity groups <sup>?</sup>

Available services  ADVPN  IKE  IPoE  LAN access  Portal  PPP  SSL VPN

Max number of concurrent logins (1-1024)

Description (1-127 chars)

OK Cancel

B) Authorization Attributes領域で、ユーザーがSSL VPNリソースグループ resourcegrpを使用できるように許可します(図63を参照)。

図63 SSL VPN ユーザーの認可アトリビュートの設定

Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout minutes (1-120)

Authorization VLAN (1-4094)

SSL VPN policy group resourcegrp

C) OKをクリックします。

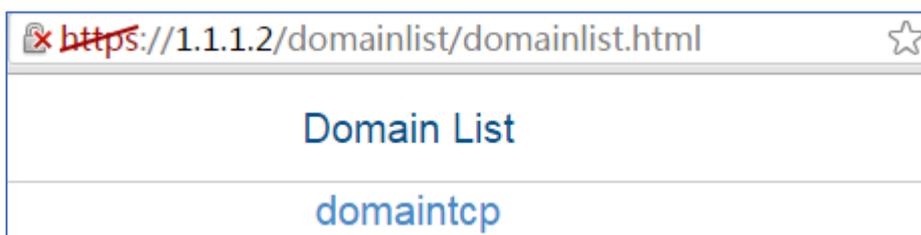
## ホストの構成

#ホストの IP アドレスとゲートウェイアドレスを設定し、SSL VPN ゲートウェイに到達できることを確認します。

## 設定の確認

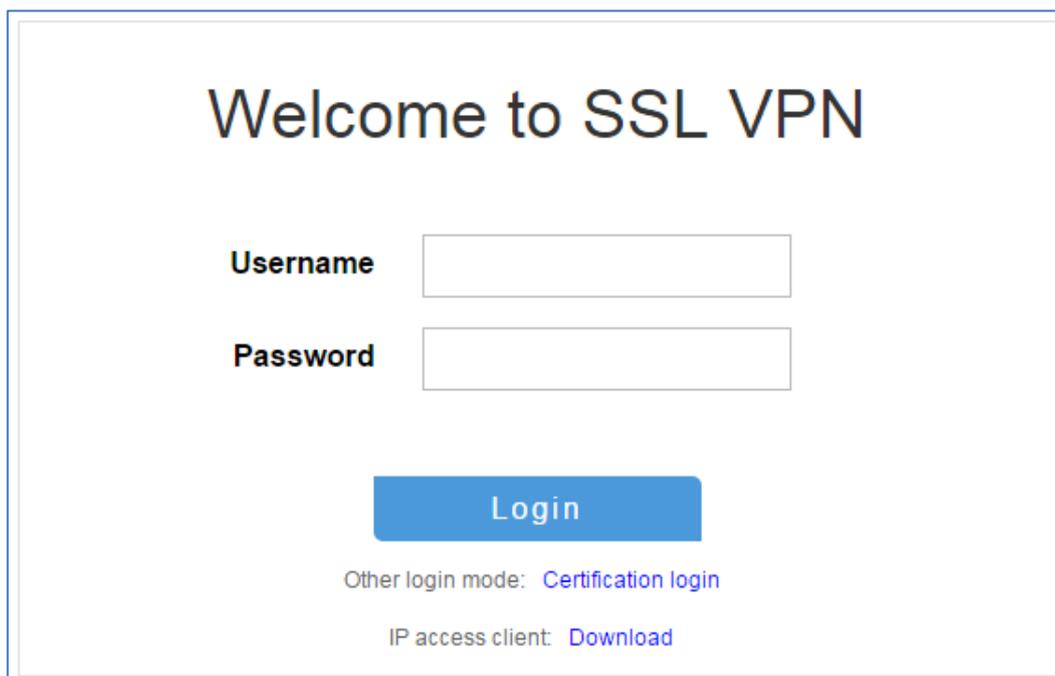
1. ホストのブラウザアドレスバーに `https://1.1.1.2` と入力し、Enter キーを押してドメインリストページを開きます。

図64 ドメインリストページ



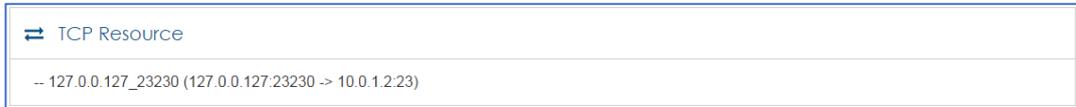
2. `domaintcp` を選択してログインページにアクセスします。
3. ログインページで、`username` に `user1` と `password` に `123456` を入力し、`Login` をクリックします。

図65 ログインページ



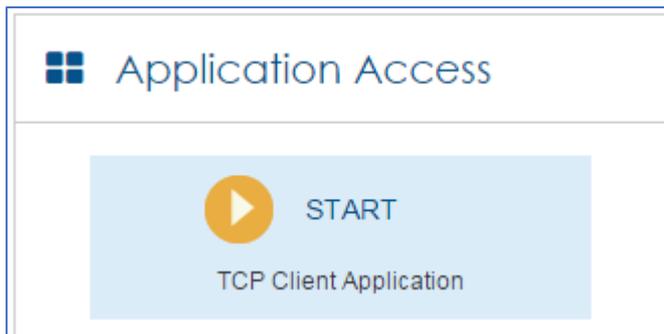
SSL VPN ホームページが開き、ユーザーがアクセスできる TCP リソースが TCP Resource 領域に表示されます。

図66 アクセス可能な TCP リソース



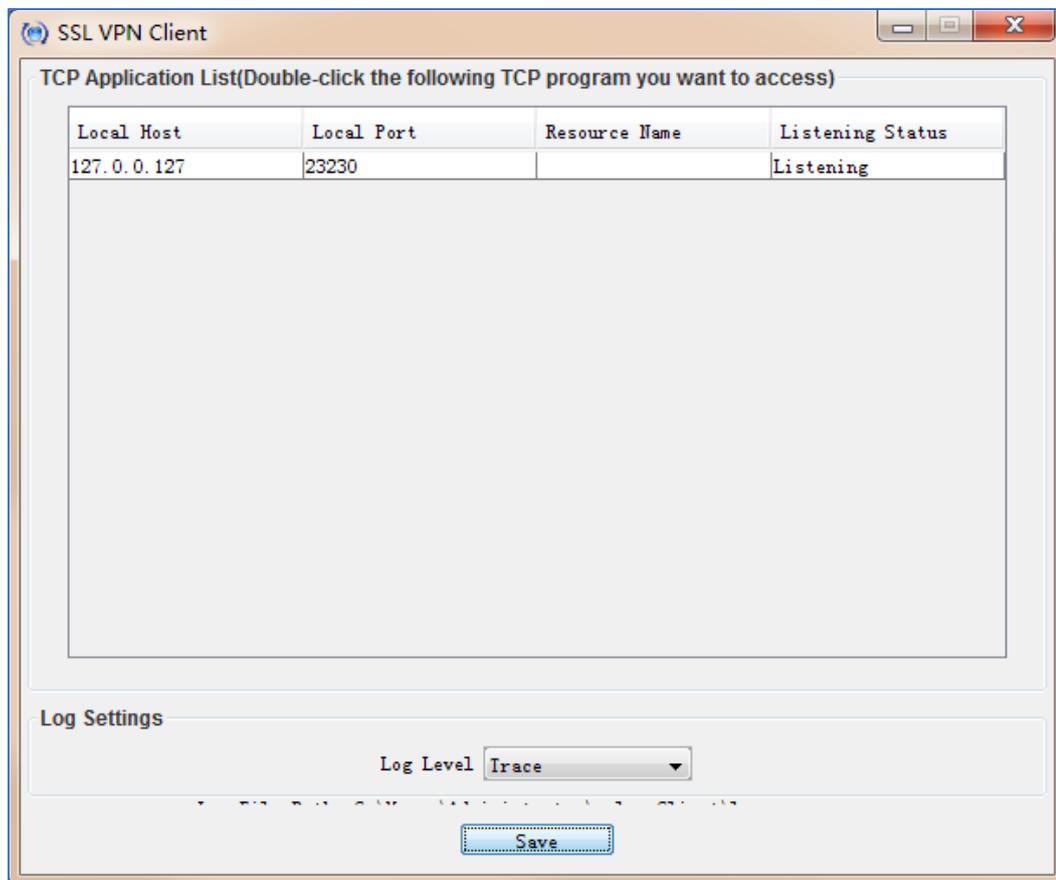
4. START をクリックして、TCP クライアントアプリケーションを起動します(を参照)。

図67 TCP クライアントアプリケーションの起動



TCP クライアントアプリケーションが起動します(図68 を参照)。

図68 TCPクライアントアプリケーション



---

❗ **重要:**

ダブルクリックでTCPアプリケーションプログラムにアクセスすることはできません。

---

- ローカルアドレス127.0.0.1およびローカルポート2323にTelnet接続し、サーバーにアクセスします。

# 例:CA署名付きサーバー証明書によるTCPアクセスの設定

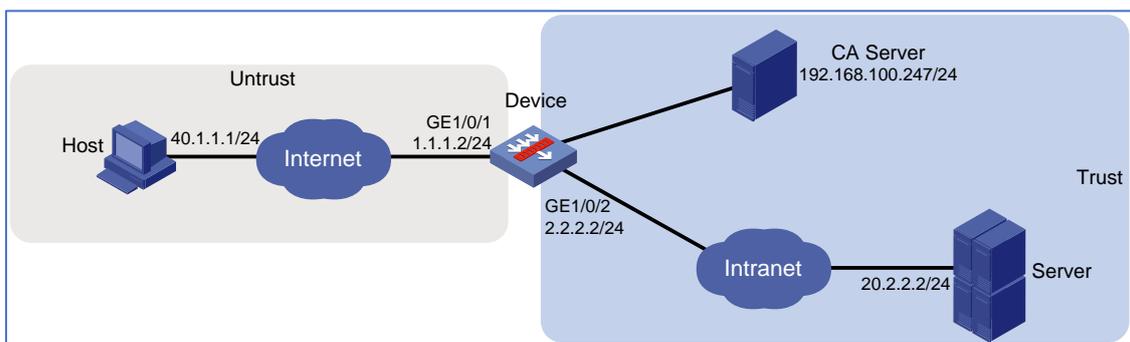
## ネットワーク構成

図69に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。Windows Server2008R2CA サーバーがプライベートネットワークに配置されています。ユーザーは、TCP アクセスモードで内部 Telnet サーバーにセキュアにアクセスする必要があります。

以下のタスクを実行してください。

- CA サーバーからデバイスのサーバー証明書を要求します。
- ユーザーが TCP アクセスモードでサーバーにアクセスできるように、デバイス上で SSL VPN TCP アクセスサービスを設定します。
- TCP アクセスユーザーに対してローカル認証および認可を実行するようにデバイスを設定します。

図69 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

# 制限事項とガイドライン

15. 証明書ベースのクライアント認証は、TCP アクセスモードでは使用できません。
16. Web インターフェイスから TCP クライアントを起動するには、Java Runtime Environment バージョン 1.7(JRE1.7)以降がクライアントホストにインストールされていることを確認してください。
17. ホストから TCP アクセスモードで内部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な場合があります。管理者権限でホストにログインしてください。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、Network タブをクリックします。
  - #ナビゲーションペインで、Interface Configuration > Interfaces を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。
    - B) **IPv 4Address**タブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。
    - C) OKをクリックします。
  - #GE1/0/ge1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。
2. 信頼するセキュリティゾーンと信頼しないセキュリティゾーンの間にセキュリティポリシーを構成します。信頼するセキュリティゾーンと信頼しないセキュリティゾーンが相互に通信できることを確認してください。
3. デバイスのサーバー証明書を要求します。
  - A) 証明書のサブジェクトを作成します。
    - #トップナビゲーションバーで、**Objects** をクリックします。
    - #ナビゲーションペインで、**PKI > Certificate Subject** を選択します。
    - #**create** をクリックします。
    - #図70に示すように、証明書のサブジェクトを作成し、OK をクリックします。

図70 証明書サブジェクトの作成

Create Certificate Subject

Certificate subject name  \*(1-31 chars)

Common name  (1-63 chars)

Country code  (2 chars, case sensitive)

State or province name  (1-63 chars)

Locality  (1-63 chars)

Organization name  (1-63 chars)

Organization unit name  (1-63 chars)

FQDN  (1-255 chars)

IP address  IPv4 address  Use interface's primary IP address

OK Cancel

B) PKIドメインを作成します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**PKI > Certificate** を選択します。

# **Create PKI domain** をクリックします。

#図71に示すように PKI ドメインを作成し、OK をクリックします。

図71 PKIドメインの作成

Create PKI Domain

Domain name  \*(1-31 chars)

Certificate subject

Key pairs for certificate request

Algorithm

Use different key pairs for encryption and signing

Key pair name  (1-64 chars)

Key length  (512-2048)

CRL checking  Check if a certificate has been revoked by the CA

Certificate usage extensions  IKE  SSL server  SSL client

Encryption algorithm for PKCS#7 cert files

OK Cancel

C) 証明書要求を作成します。

#証明書 certificate ページで、Submit Cert Request をクリックします。

#図72に示すように、証明書要求の設定を行います。

図72 証明書要求の作成

Submit Cert Request

PKI domain: sslvndomain \* [Edit]

Certificate subject: sslvncert \* [Edit]

Algorithm: RSA \* [Edit]

Key pair name: sslvnrrsa \*

Key length: 1024

Use different key pairs for encryption and signing:

Password for cert revocation: (1-31 chars)

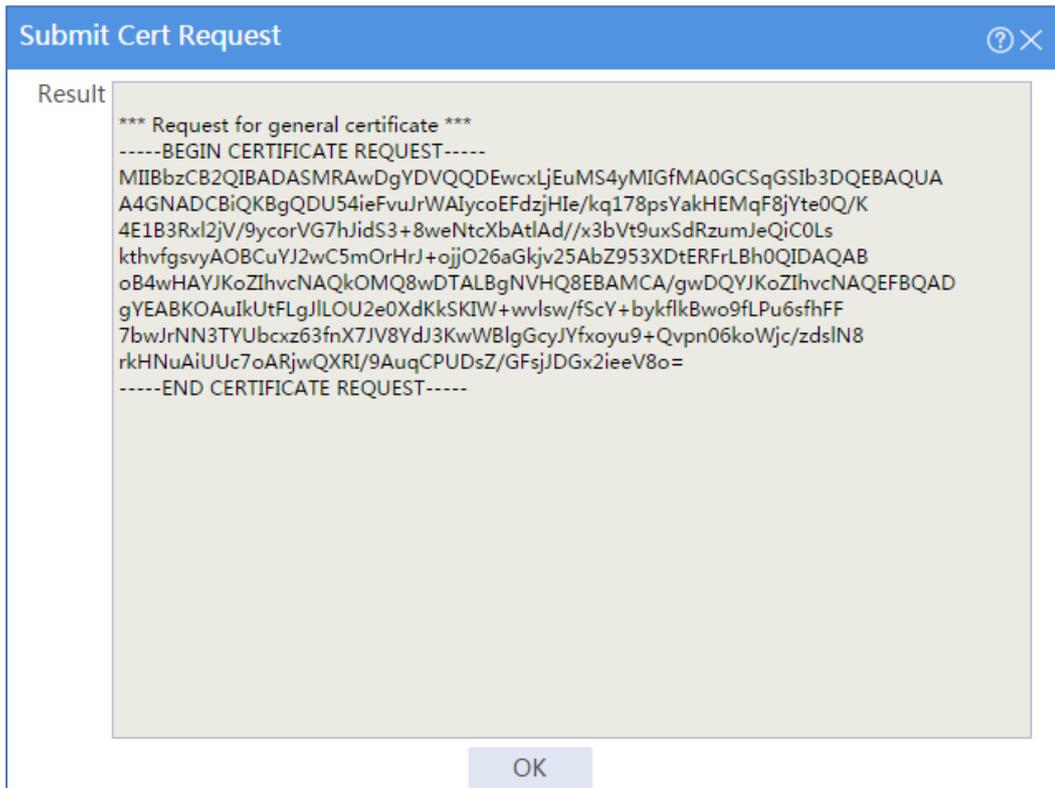
Confirm password:

OK Cancel

#OK をクリックします。

証明書要求の内容が表示されます(図73を参照)。

図73 証明書要求の内容



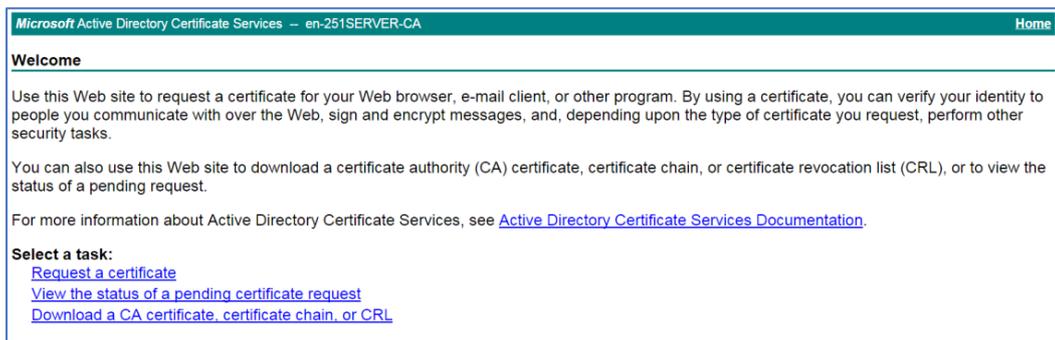
#証明書要求の内容をコピーし、OK をクリックします。

D) CAにサーバー証明書を要求する:

#ブラウザのアドレスバーに `http://192.168.100.247/certsrv` と入力します。

#図74に示す証明書サービスのホームページで、Request a certificate をクリックします。

図74 証明書サービスのホームページ



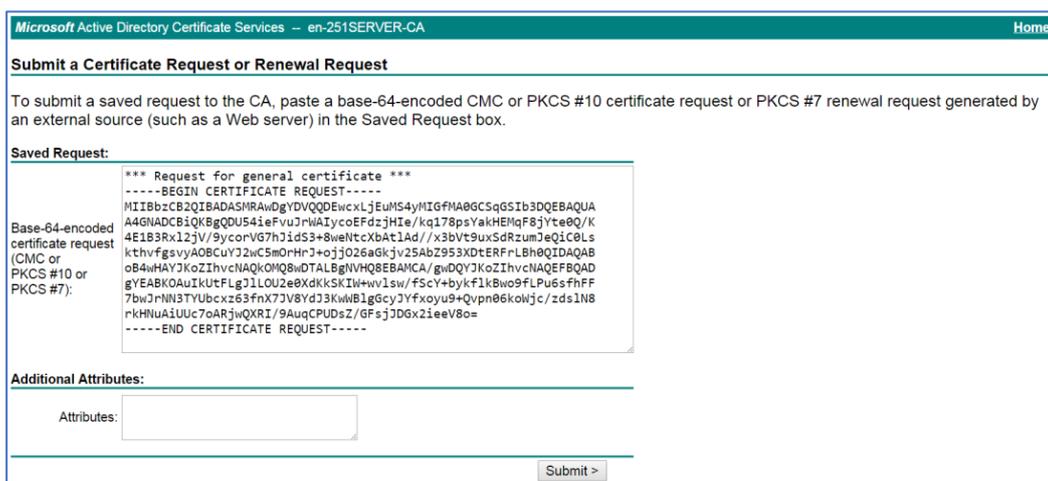
#図75に示す Request a Certificate ページで、Advanced Certificate Request をクリックします。

図75 証明書の要求ページ



#以前にコピーした証明書要求の内容を Base-64-encoded certificate request CMC or PKCS#10 or PKCS#7 フィールドに貼り付けます(図76を参照)。

図76 証明書要求の内容の貼り付け

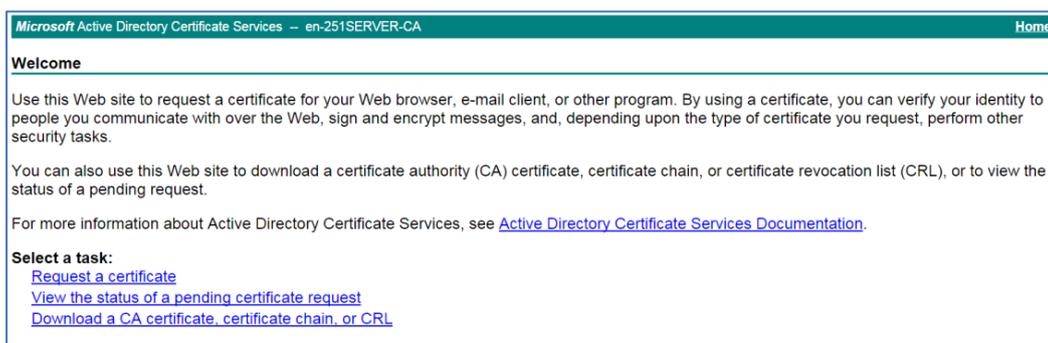


# **submit** をクリックします。

証明書要求が CA 管理者によって承認されたら、ブラウザのアドレスバーに `http://192.168.100.247/certsrv` と入力します。

#図77に示す証明書サービスのホームページで、View the status of a pending certificate request をクリックします。

図77 証明書サービスのホームページ



#表示する証明書要求を選択します。この例では、図78に示すように、Saved-Request Certificate(9/24/2018 9:53:57AM)を選択します。

図78 Status of a Pending Certificate Request ページの表示



Certificate Issued ページが開き、要求されたサーバー証明書が発行されたことが示されます(図79を参照)。

図79 証明書発行ページ



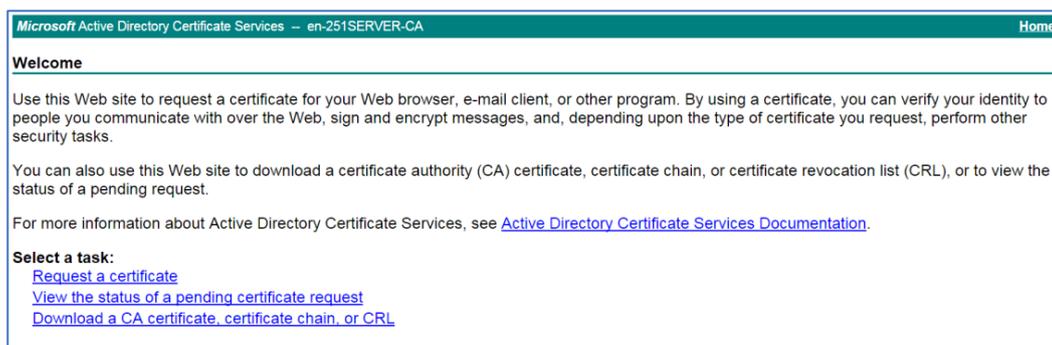
#Download certificate をクリックしてサーバー証明書をダウンロードし、ローカルに保存します。

4. CA証明書をダウンロードします。

#ブラウザのアドレスバーに http://192.168.100.247/certsrv と入力します。

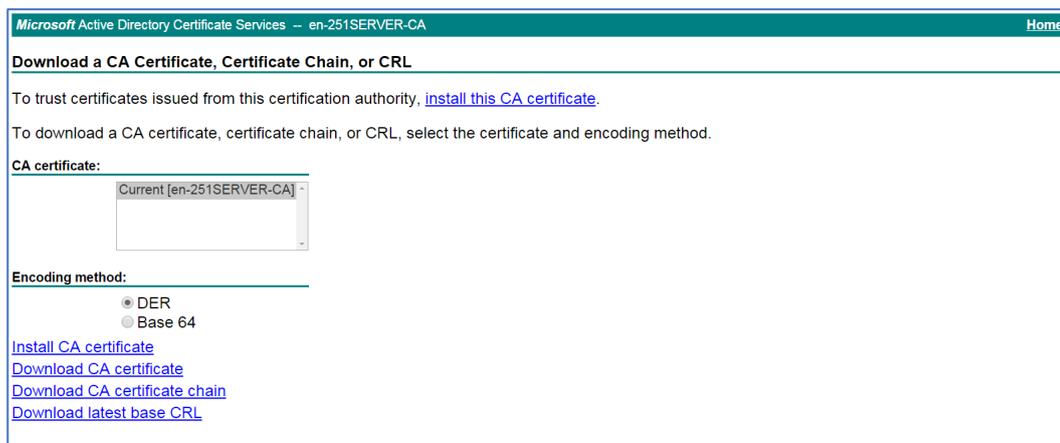
#図80に示す証明書サービスのホームページで、Download a CA certificate,certificate chain,or CRL をクリックします。

図80 証明書サービスのホームページ



#Download a CA certificate,certificate chain,or CRL ページで、Download CA certificate をクリックします。

図81 CA 証明書、証明書チェーン、または CRL ページのダウンロード



#ダウンロードした CA 証明書をローカルに保存します。

5. CA証明書とサーバー証明書をインポートします。

A) CA証明書をインポートします。

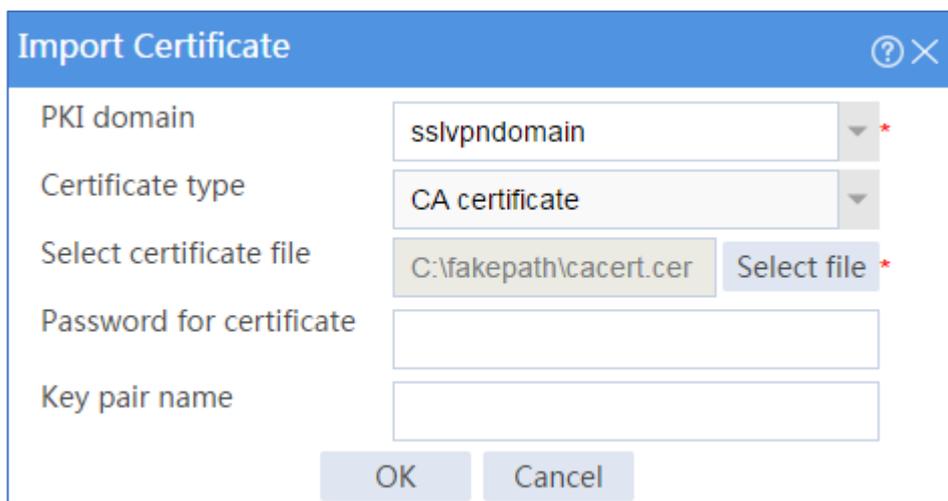
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**PKI > Certificate** を選択します。

# **Import certificate** をクリックします。

#ローカルに保存された CA 証明書をインポートし(図82を参照)、OK をクリックします。

図82 CA 証明書のインポート

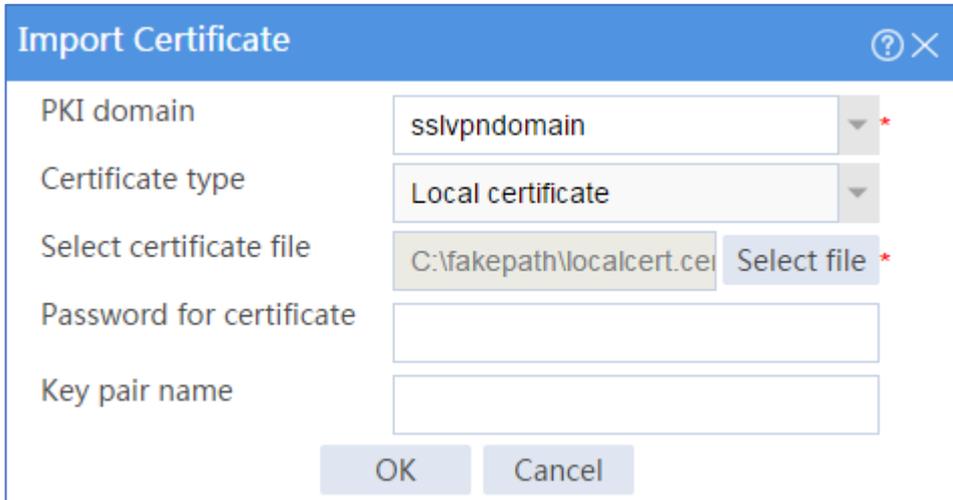


B) サーバー証明書をインポートします。

# **Certificate** ページで、**Import certificate** をクリックします。

#ローカルに保存されたサーバー証明書をインポートし(図83を参照)、OK をクリックします。

図83 サーバー証明書のインポート



The 'Import Certificate' dialog box contains the following fields and controls:

- PKI domain:** A dropdown menu with 'sslvpnomain' selected.
- Certificate type:** A dropdown menu with 'Local certificate' selected.
- Select certificate file:** A text field containing 'C:\fakepath\localcert.cer' and a 'Select file' button.
- Password for certificate:** An empty text input field.
- Key pair name:** An empty text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

6. SSLサーバーポリシーを設定します。

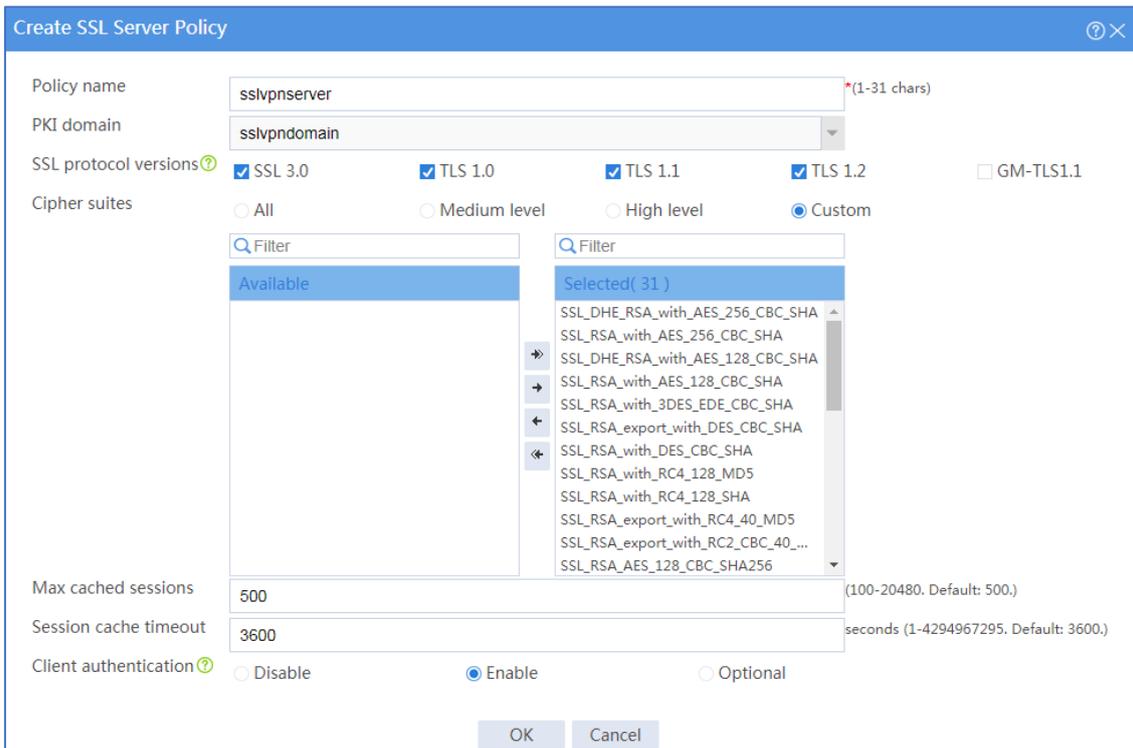
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**SSL > SSL Server Policies** を選択します。

#create をクリックします。

#図84に示すように SSL サーバーポリシーを設定し、OK をクリックします。

図84 SSL サーバーポリシーの作成



The 'Create SSL Server Policy' dialog box contains the following fields and controls:

- Policy name:** A text field with 'sslvpnserver' and a character count '(1-31 chars)'.
- PKI domain:** A dropdown menu with 'sslvpnomain' selected.
- SSL protocol versions:** Checkboxes for 'SSL 3.0', 'TLS 1.0', 'TLS 1.1', 'TLS 1.2', and 'GM-TLS1.1'.
- Cipher suites:** Radio buttons for 'All', 'Medium level', 'High level', and 'Custom' (selected).
- Cipher suites lists:** Two lists, 'Available' and 'Selected( 31 )', with a search filter and navigation arrows between them.
- Max cached sessions:** A text field with '500' and a range '(100-20480. Default: 500.)'.
- Session cache timeout:** A text field with '3600' and a unit 'seconds (1-4294967295, Default: 3600)'.
- Client authentication:** Radio buttons for 'Disable', 'Enable' (selected), and 'Optional'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

7. SSL VPNゲートウェイを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。

# **create** をクリックします。

#図85に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。0

図85 SSL VPN ゲートウェイの作成

Create Gateway

Gateway ?  \*(1-31 chars)

IP address ?  IPv4  IPv6

(Default: 0.0.0.0)

HTTPS port  (1025-65535, Default: 443.)

HTTP redirection

HTTP port  (1025-65535, Default: 80.)

SSL server policy  ▼

VRF  ▼

Enable

OK Cancel

8. SSL VPNコンテキストを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Contexts** を選択します。

# **create** をクリックします。

#に示すように、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。

図86 SSL VPN コンテキストの作成

Create SSL VPN Context

1 Basic settings

Context name <sup>?</sup> ctxtcp \* (1-31 chars)

2 URI ACL

Associated gateways

+ Create Edit X Delete \*

<input type="checkbox"/>	Gateway	Access ...	Domain	Virtua...	Edit
<input checked="" type="checkbox"/>	sslvpngw	Domain ...	domaintcp		

3 Access services

4 Shortcuts

5 Resource groups

VRF Public network

ISP domain

Code verification <sup>?</sup>

Certificate auth <sup>?</sup>

Enable password

Certificate and pwd authN  Use all methods  Use any method

IMC SMS verification <sup>?</sup>

Max sessions 1048575 (1-1048575)

Previous Next Cancel

# URI ACL ページで、**Next** をクリックします。

# Access services ページで **TCP access** を選択し、**Next** をクリックします。

# TCP access ページで、**Port Forwarding Item** 領域の **Create** をクリックします。

#pfitem という名前のポート転送アイテムを作成し(図87を参照)、OK をクリックします。

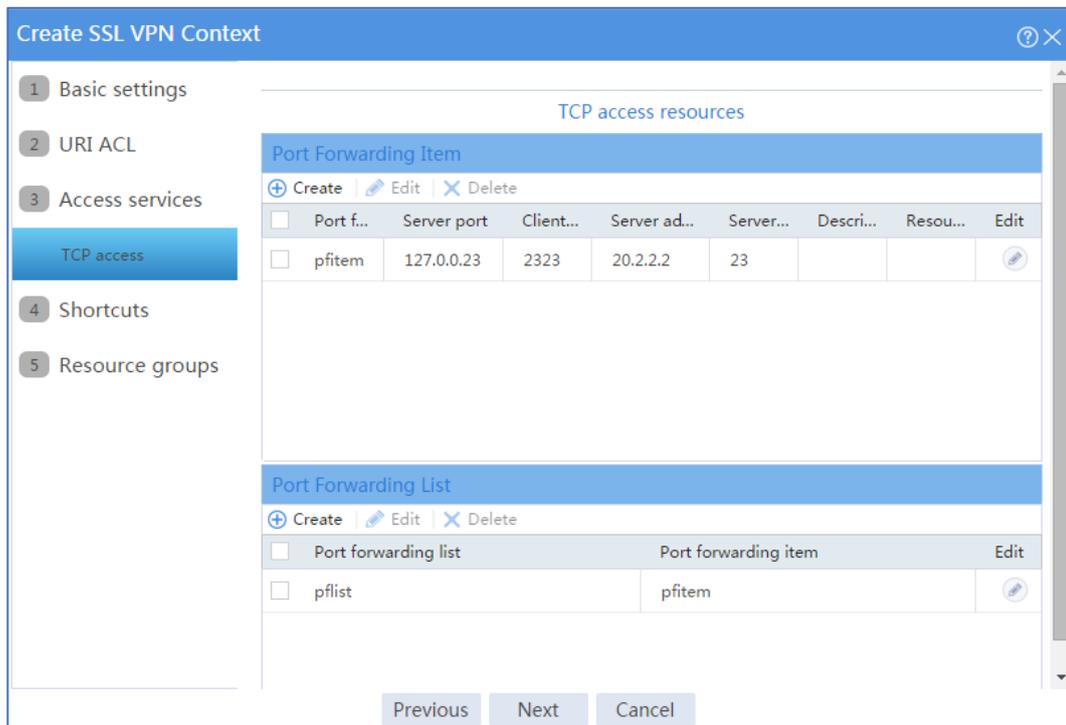
図87 ポート転送アイテムの作成

The screenshot shows a dialog box titled "Add Port Forwarding Item". It contains the following fields and values:

Field	Value	Character Limit
Name	pfitem	1-31 chars
Client host	127.0.0.23	1-253 chars
Client port	2323	1-65535
Server address	20.2.2.2	1-253
Server port	23	1-65535
Description		1-63 chars
Resource link	url('http://10.0.0.1:8080/cmd')	1-255 chars

#pflist という名前のポート転送リストを作成し、ポート転送アイテム pfitem を割り当てます(図88を参照)。

図88 TCP アクセスリソースの設定



# **Shortcuts** ページで **next** をクリックします。

# **Resource groups** ページで、**create** をクリックします。

# resourcegrp という名前のリソースグループを作成し、図88に示すように、**TCP resources** リストからポート転送リスト pflist を選択します。

図88 SSL VPN リソースグループの作成

Create Resource Group

Resource group  \* (1-31 chars)

Shortcut List

---

TCP access

TCP resources

IPv4 ACL

IPv6 ACL

URI ACL

OK Cancel

#OK をクリックします。

Resource groups ページに、新しく作成されたリソースグループが表示されます(図90を参照)。

図90 リソースグループ設定ページ

Create SSL VPN Context

1 Basic settings

2 URI ACL

3 Access services

4 Shortcuts

5 Resource groups

Resource groups

+ Create Edit Delete Set as default Set as non-default

<input type="checkbox"/>	Resource group name	Def...	Edit
<input type="checkbox"/>	resourcegrp		

Previous Finish Cancel

# **finish** をクリックします。

#Enable チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図91を参照)。

図91 SSL VPN コンテキストのイネーブル化



Context name	Status	Gateway	Gateway access method	VRF	Enable	Edit
ctxtcp	Enable	sslvpngw	Domain namedomaintcp	Public network	<input checked="" type="checkbox"/>	

9. SSL VPNユーザーを作成します。

#トップナビゲーションバーで、**Objects** をクリックします。

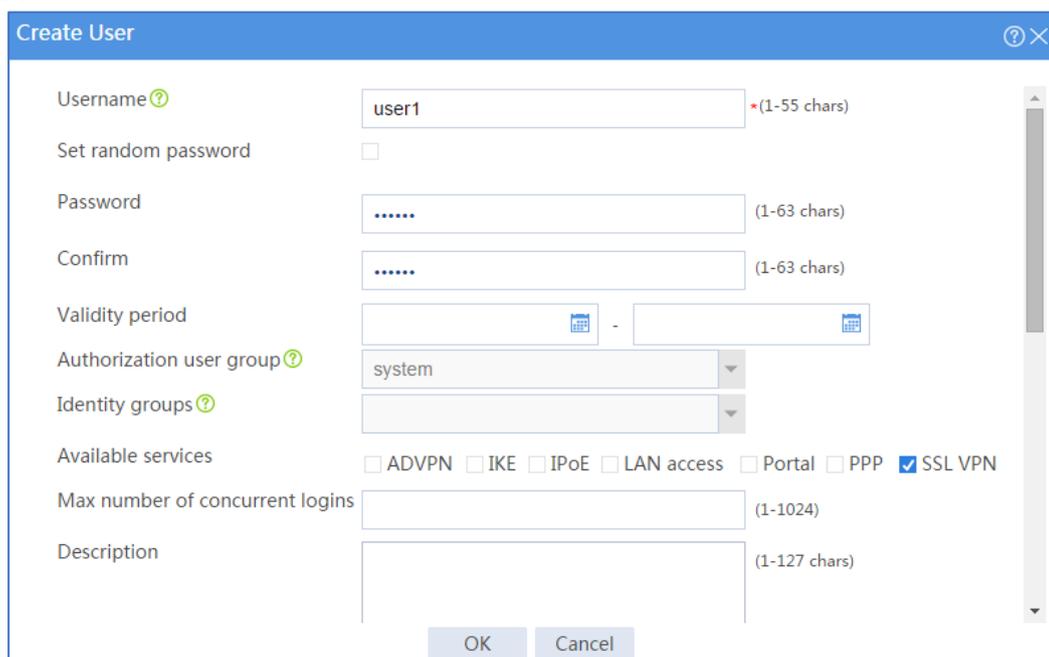
#ナビゲーションペインで、**User > User Management > Local Users** を選択します。

# **create** をクリックします。

#SSL VPN ユーザーを作成します。

A) ユーザー名をuser1、パスワードを123456に設定し、使用可能なサービスとしてSSL VPNを選択します(図92を参照)。

図92 SSL VPN ユーザーの作成



**Create User**

Username  \* (1-55 chars)

Set random password

Password  (1-63 chars)

Confirm  (1-63 chars)

Validity period  -

Authorization user group

Identity groups

Available services  ADVPN  IKE  IPoE  LAN access  Portal  PPP  SSL VPN

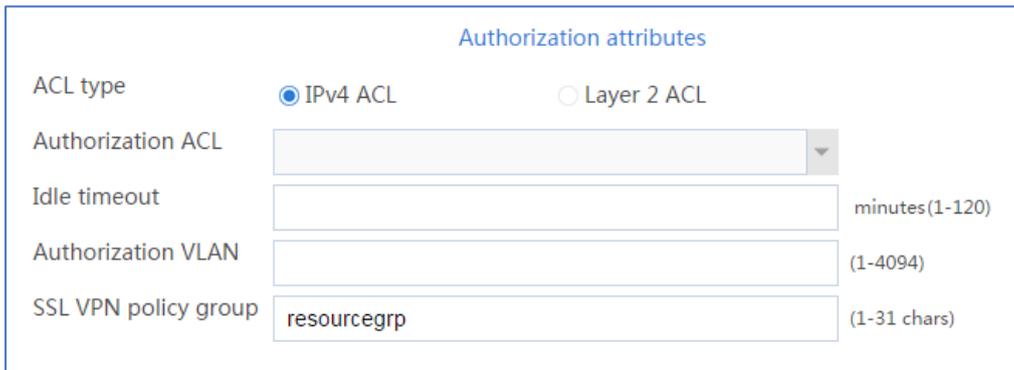
Max number of concurrent logins  (1-1024)

Description  (1-127 chars)

OK Cancel

B) Authorization Attributes領域で、ユーザーがSSL VPNリソースグループ resourcegrpを使用できるように許可します(図93を参照)。

図93 SSL VPN ユーザーの認可アトリビュートの設定



Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout  minutes(1-120)

Authorization VLAN  (1-4094)

SSL VPN policy group  (1-31 chars)

C) OKをクリックします。

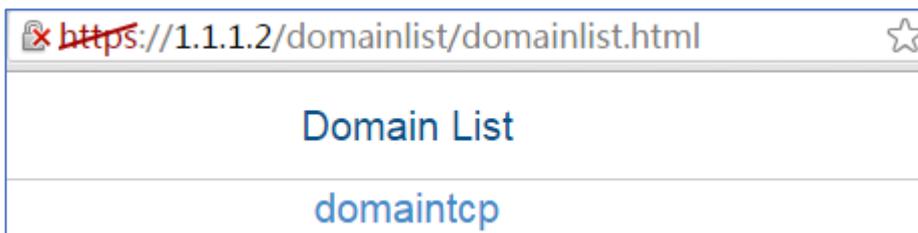
## ホストの構成

#ホストの IP アドレスとゲートウェイアドレスを設定し、SSL VPN ゲートウェイに到達できることを確認します。

## 設定の確認

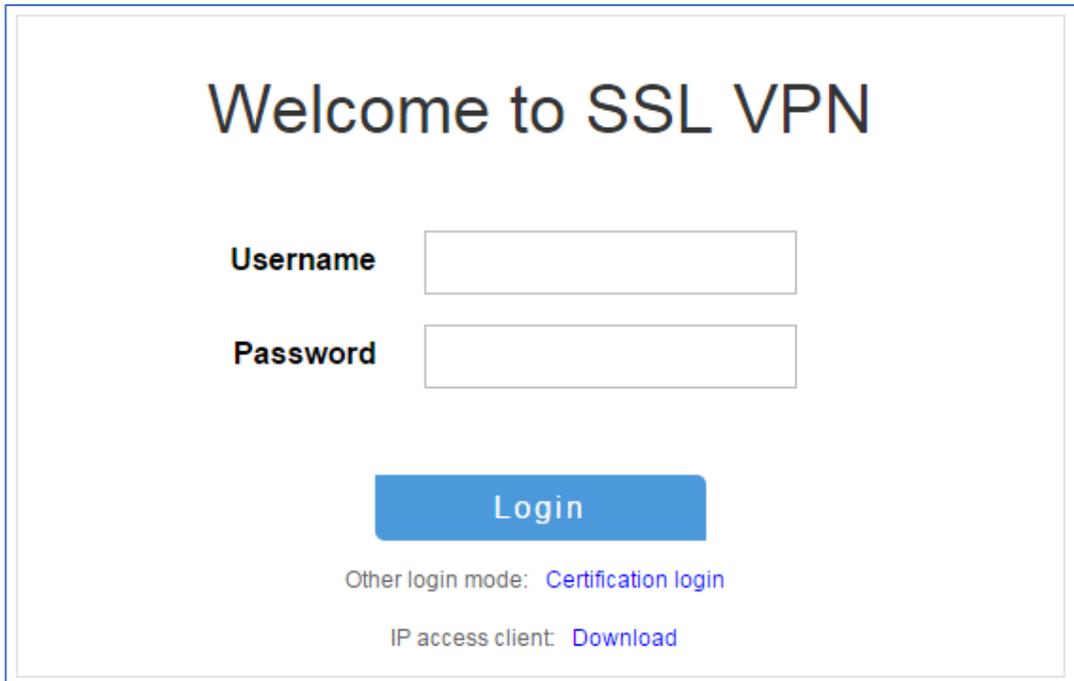
1. ホストのブラウザアドレスバーに `https://1.1.1.2` と入力し、Enter キーを押してドメインリストページを開きます。

図94 ドメインリストページ



2. `domaintcp` を選択してログインページにアクセスします。
3. ログインページで、`username user1` と `password123456` を入力し、Login をクリックします。

図95 ログインページ



Welcome to SSL VPN

Username

Password

Login

Other login mode: [Certification login](#)

IP access client: [Download](#)

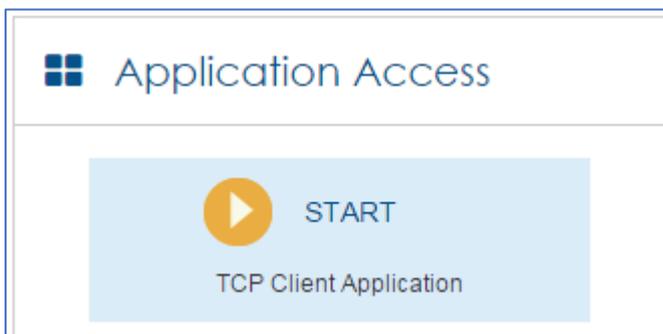
SSL VPN ホームページが開き、ユーザーがアクセスできる TCP リソースが TCP Resource 領域に表示されます。

図96 アクセス可能な TCP リソース

<a href="#">TCP Resource</a>
- 127.0.0.127_23230 (127.0.0.127:23230 -> 10.0.1.2:23)

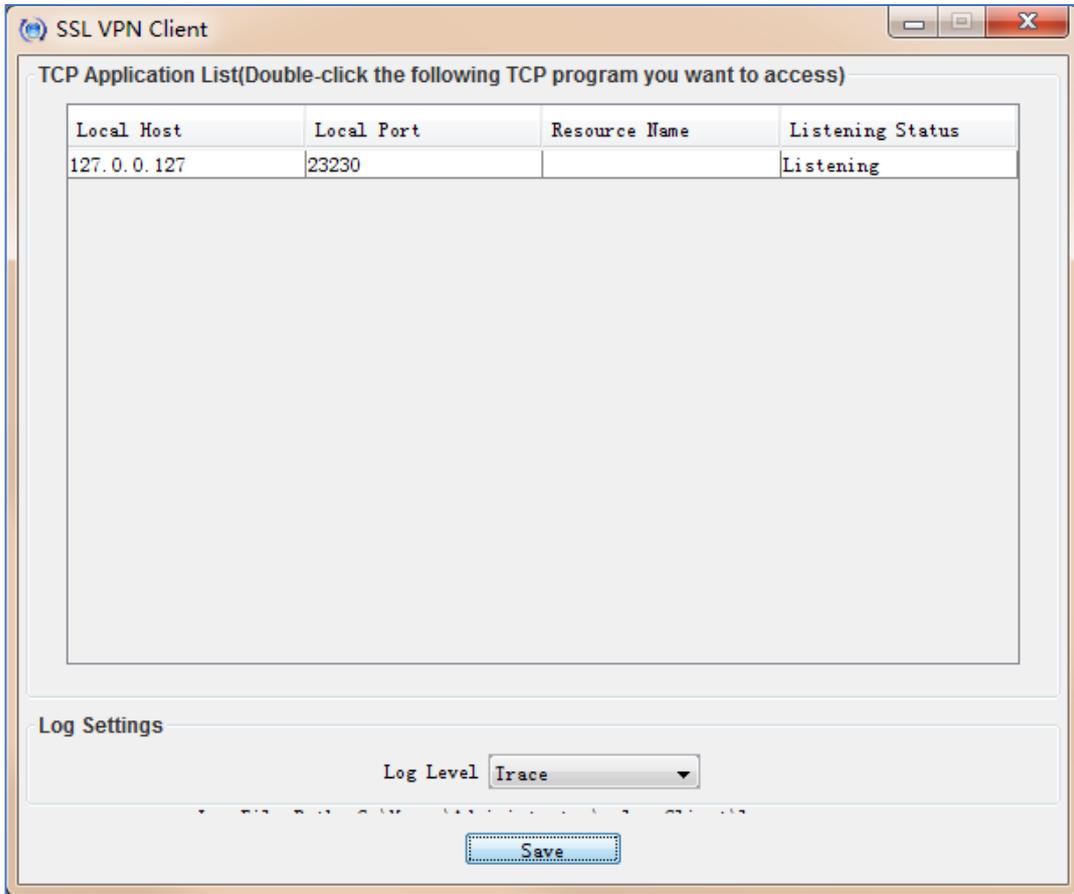
4. START をクリックして、TCP クライアントアプリケーションを起動します(を参照)。

図97 TCP クライアントアプリケーションの起動



TCP クライアントアプリケーションが起動します(図98を参照)。

図98 TCP クライアントアプリケーション



❗ 重要:

ダブルクリックでTCPアプリケーションプログラムにアクセスすることはできません。

- ローカルアドレス127.0.0.1にTelnet接続し、ローカルポート2323でサーバーにアクセスします。

## 例:ローカル認証と自己署名証明書によるIPアクセスの設定

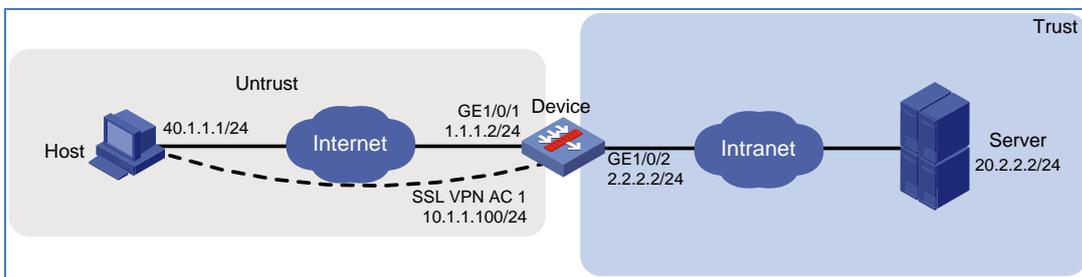
### ネットワーク構成

図99に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。ユーザーは、IP アクセスモードで内部サーバーにセキュアにアクセスする必要があります。

デバイスは自己署名サーバー証明書を使用します。  
以下のタスクを実行してください。

- ユーザーが IP アクセスモードで内部サーバーにアクセスできるように、デバイス上で SSL VPN IP アクセスサービスを設定します。
- IP アクセスユーザーに対してローカル認証および認可を実行するようにデバイスを設定します。

図99ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

- Web インターフェイスから IP クライアントを起動するには、Java Runtime Environment バージョン 1.7(JRE1.7)以降がクライアントホストにインストールされていることを確認してください。
- クライアントアドレス割り当て用に設定された IP アドレスプールは、次の要件を満たす必要があります。
  - アドレスプールのアドレス範囲は、クライアントホストで使用される IP アドレスと同じサブネット上にはできません。
  - アドレスプールの IP アドレスは、デバイスで使用される IP アドレスと競合しません。

- アドレスプールのアドレス範囲は、内部サーバーの IP アドレスと同じサブネット上にはできません。
- SSL VPN AC インターフェイスを正しいセキュリティゾーン(この例では Untrust)に追加する必要があります。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、**Network** タブをクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。  
B) IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。  
C) OKをクリックします。  
#GE1/0/2 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。  
#GE1/0/3 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 3.3.3.1/24 に設定します。
2. 信頼するセキュリティゾーンと信頼しないセキュリティゾーンの間にセキュリティポリシーを構成します。信頼するセキュリティゾーンと信頼しないセキュリティゾーンが相互に通信できることを確認してください。
3. SSL VPNゲートウェイを設定します。  
#トップナビゲーションバーで、**network** をクリックします。  
#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。  
# **create** をクリックします。  
#図100に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。

図100 SSL VPN ゲートウェイの作成

Create Gateway

Gateway ?  \*(1-31 chars)

IP address ?  IPv4  IPv6

(Default: 0.0.0.0)

HTTPS port  (1025-65535. Default: 443.)

HTTP redirection

HTTP port  (1025-65535. Default: 80.)

SSL server policy

VRF

Enable

OK Cancel

4. SSL VPN ACインターフェイスを作成します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN AC Interfaces** を選択します。

# **create** をクリックします。

#開いた Create Interfaces ダイアログボックスで、Interface number フィールドに 1 と入力し、OK をクリックします。

#Modify Interface Settings ダイアログボックスで、SSL VPN AC インターフェイスの基本設定を行います(図101を参照)。

図101 SSL VPN AC インターフェイスの基本設定

Modify Interface Settings

Name: SSLVPN-AC1

Link status: **Down**  Shut down

Description: SSLVPN-AC1 Interface

Basic Configuration | IPv4 Address

Add an interface to a security zone: Untrust

VRF: Public network

MAC address: 00-00-00-FF-F6-D3

MTU: 1500 (100-64000)

Expected bandwidth: <1-400000000> (kbps)

Apply OK Cancel

#IPv4Address タブをクリックし、SSL VPN AC インターフェイスの IPv4 アドレスを設定します(図 102を参照)。

#OK をクリックします。

図102 SSL VPN AC インターフェイスのIPv4アドレス設定

Modify Interface Settings

Name: SSLVPN-AC1

Link status: **Down**  Shut down

Description: SSLVPN-AC1 Interface

Basic Configuration | IPv4 Address

IP address:  Manual assignment

IP address/mask length:  /

Assign secondary IP  Delete secondary IP

<input type="checkbox"/>	Secondary IP addr...	Mask length	Edit
--------------------------	----------------------	-------------	------

Apply OK Cancel

5. IPアクセスユーザーのアドレスプールを作成します。  
#トップナビゲーションバーで、ネットワークをクリックします。  
#ナビゲーションペインで、SSL VPN>IP Access Address Pools を選択します。  
#create をクリックします。  
#IP アクセスアドレスプールを作成し(図103を参照)、OK をクリックします。

図103 IP アクセスアドレスプールの作成

Create IP Access Address Pool

Address pool name  \*(1-31 chars)

Start IP address  \*

End IP address  \*

OK Cancel

6. SSL VPNコンテキストを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Contexts** を選択します。

# **create** をクリックします。

#図104に示すように、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。

図104 SSL VPN コンテキストの基本設定

Create SSL VPN Context

1 Basic settings

Context name  \*(1-31 chars)

2 URI ACL

Associated gateways

Gateway	Access m...	Domain	Virtual...	Edit
<input type="checkbox"/>	sslvpngw	Domain ...	domainip	<input type="text"/>

3 Access services

4 Shortcuts

5 Resource groups

VRF

ISP domain

Code verification

Certificate auth

Enable password

Certificate and pwd authN  Use all methods  Use any method

IMC SMS verification

Max sessions  (1-1048575)

Previous Next Cancel

#URI ACL ページで、Next をクリックします。

#アクセスサービスページで IP アクセスを選択し、next をクリックします。

# IP access ページで、IP アクセスサービスを次のように設定します。

A) IPアクセスパラメータを設定し(図105を参照)、Nextをクリックします。

図105 IP アクセスサービスの IP アクセスパラメータの設定

The screenshot shows the 'Create SSL VPN Context' configuration window with the 'IP access' tab selected. The settings are as follows:

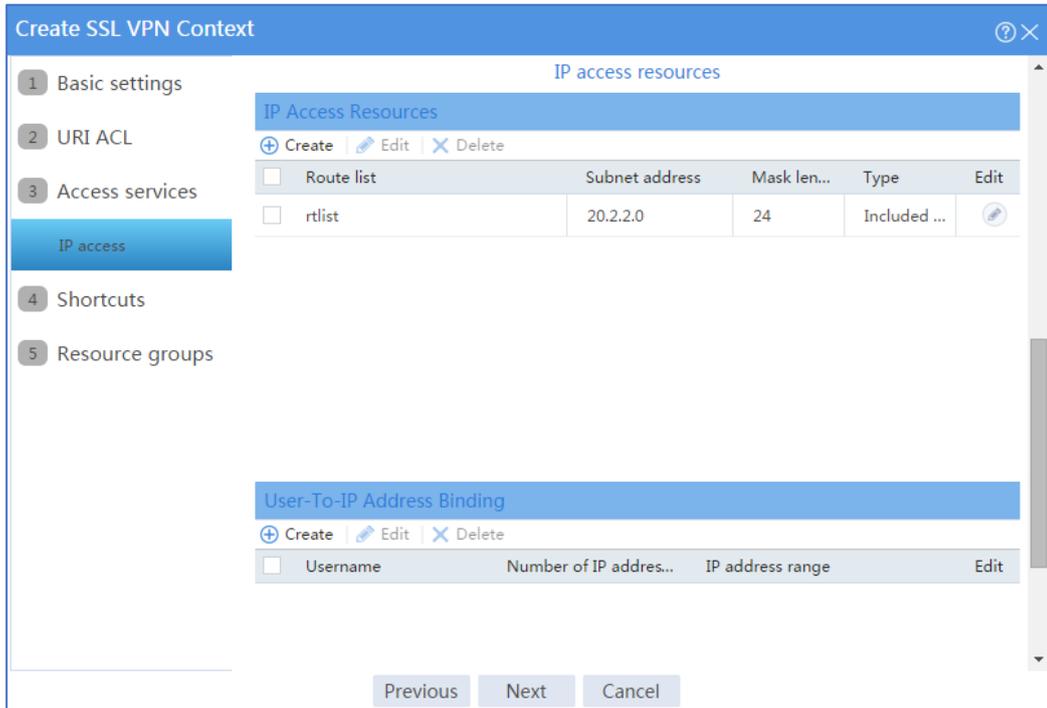
- SSL VPN AC interface: SSLVPN-AC1
- IP access address pool: sslvpnpool
- Mask length: 24 (range 1-30)
- Primary DNS server: X.X.X.X
- Secondary DNS server: X.X.X.X
- Primary WINS server: X.X.X.X
- Secondary WINS server: X.X.X.X
- Keepalive interval: 30 seconds (range 0-600)
- Start IP access client:
- Push Web resources:
- Rate limit: Upstream traffic (empty) Kbps (range 1000-1000000000)
- Downstream traffic (empty) Kbps (range 1000-1000000000)

Buttons at the bottom: Previous, Next, Cancel.

A) IP access resources領域で、図106に示すように、20.2.2.0/24のルートエントリを含むルートルストlistを設定します。

B) nextをクリックします。

図106 IP アクセスサービス用の IP アクセスリソースの設定



# **Shortcuts** ページで **next** をクリックします。

# **Resource groups** ページで、**create** をクリックします。

#resourcegrp という名前のリソースグループを作成します(図107を参照)。この例では、アクセス可能な IP リソースとしてルートリスト rtlist を選択し、IP アクセス要求フィルタリングに IPv4 ACL 3999(すべてのトラフィックを許可)を使用します。

図107 SSL VPN リソースグループの作成

Create Resource Group

Resource group \* (1-31 chars)

Shortcut List

---

IP access

Force all traffic to SSL VPN

Issue routes to client

Route list \*

IP access address pool

Mask length  (1-30)

IPv4 ACL

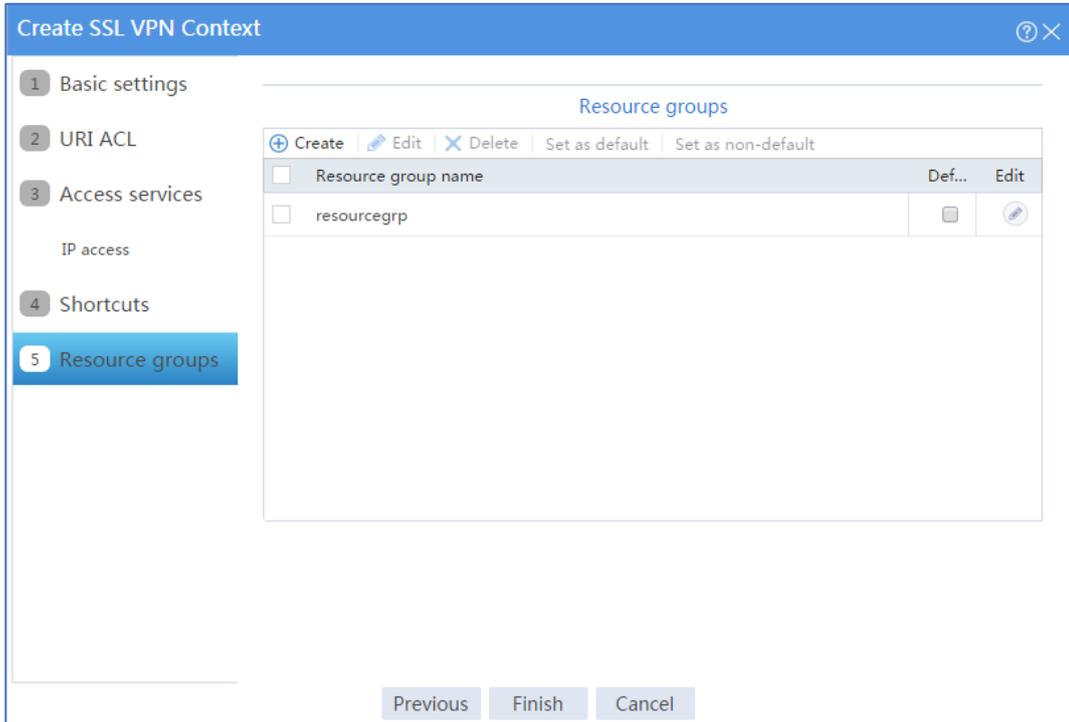
IPv6 ACL

URI ACL

#OK をクリックします。

Resource groups ページに、新しく作成されたリソースグループが表示されます(図108を参照)。

図108 Resource groups 設定ページ



# **finish** をクリックします。

#Enable チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図109を参照)。

図109 SSL VPN コンテキストのイネーブル化



7. SSL VPNユーザーを作成します。

#トップナビゲーションバーで、**Objects** 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。

# **create** をクリックします。

#SSL VPN ユーザーを作成します。

ユーザー名を user1、パスワードを 123456 に設定し、使用可能なサービスとして SSL VPN を選択します(図110を参照)。

図110 SSL VPN ユーザーの作成

Create User

Username <sup>?</sup> user1 (1-55 chars)

Set random password

Password ..... (1-63 chars)

Confirm ..... (1-63 chars)

Validity period [ ] - [ ]

Authorization user group <sup>?</sup> system

Identity groups <sup>?</sup>

Available services  ADVPN  IKE  IPoE  LAN access  Portal  PPP  SSL VPN

Max number of concurrent logins (1-1024)

Description (1-127 chars)

OK Cancel

Authorization Attributes 領域で、ユーザーが SSL VPN リソースグループ resourcegrp を使用できるように許可します(図111を参照)。

図111 SSL VPN ユーザーの認可アトリビュートの設定

Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout minutes(1-120)

Authorization VLAN (1-4094)

SSL VPN policy group resourcegrp (1-31 chars)

C) OKをクリックします。

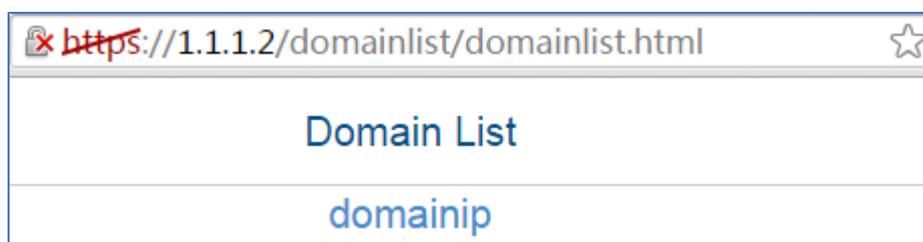
## ホストの構成

#ホストの IP アドレスとゲートウェイアドレスを設定し、SSL VPN ゲートウェイに到達できることを確認します。

## 設定の確認

1. ホストのブラウザアドレスバーに `https://1.1.1.2` と入力し、Enter キーを押してドメインリストページを開きます。

図112 ドメインリストページ



2. ログインページにアクセスするには、`domainip` を選択します。
3. ログインページで、`username user1` と `password123456` を入力し、`Login` をクリックします。

図113 ログインページ

Welcome to SSL VPN

Username

Password

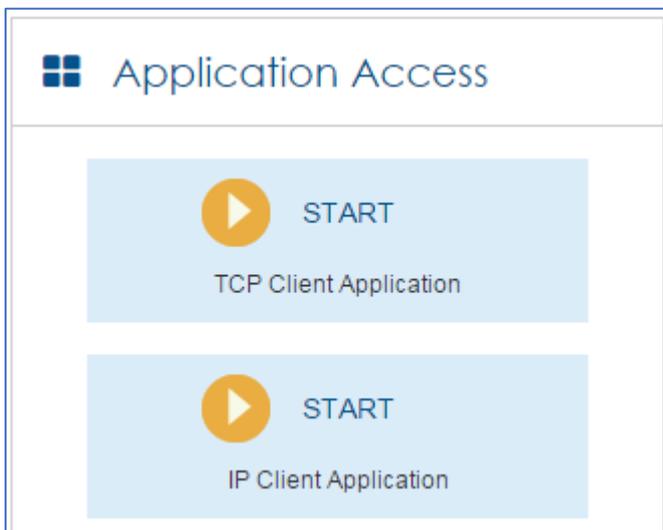
Login

Other login mode: [Certification login](#)

IP access client: [Download](#)

4. START をクリックして、IP クライアントアプリケーションを起動します(図114を参照)。

図114 IP クライアントアプリケーションの起動

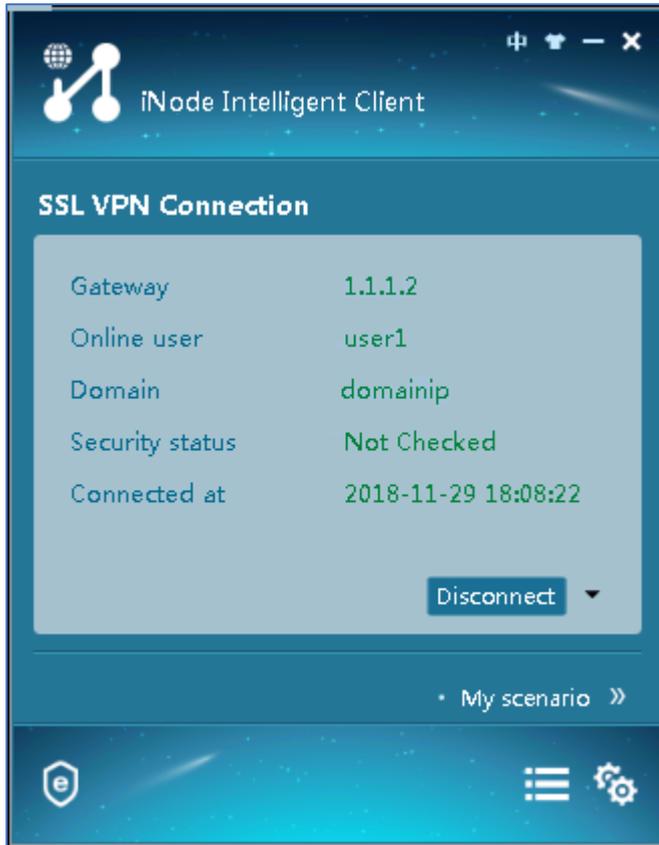


ホストに INode クライアントがインストールされていない場合、システムは INode クライアントをインストールし、INode クライアントを SSL VPN ゲートウェイに接続します。

ホストにすでに INode クライアントがインストールされている場合、システムは INode クライアントを起動し、SSL VPN ゲートウェイに直接接続します。

図115に INode クライアントが SSL VPN ゲートウェイに正常に接続されたことを示します。

図115 iNode クライアントの SSL VPN ゲートウェイへの接続



## 例:RADIUS認証によるIPアクセスの設定

### ネットワーク構成

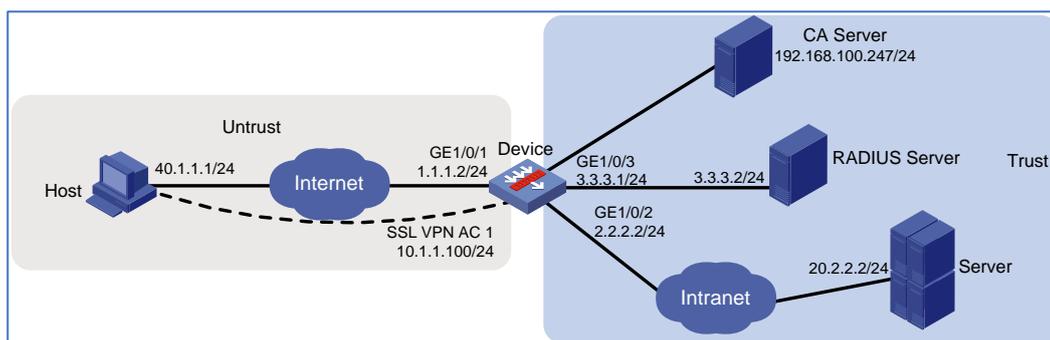
図1に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。プライベートネットワークには、Windows Server2008R2CA サーバーと、IMC PLAT7.3(E0504)を実行する RADIUS サーバーが配置されます。ユーザーは、IP アクセスモードで内部サーバー(20.2.2.2/24)にセキュアにアクセスする必要があります。

以下のタスクを実行してください。

- CA サーバーからデバイスの SSL サーバー証明書を要求します。
- ユーザーが IP アクセスの証明書認証を通過するようにデバイスを設定します。

- RADIUS サーバーを使用して IP アクセスユーザーのリモート認証および認可を実行するようにデバイスを設定します。
- ユーザーが IP アクセスモードで内部サーバーにアクセスできるように、デバイス上で SSL VPN IP アクセスサービスを設定します。

図 116 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

- Web インターフェイスから IP クライアントを起動するには、Java Runtime Environment バージョン 1.7(JRE1.7)以降がクライアントホストにインストールされていることを確認してください。
- クライアントアドレス割り当て用に設定された IP アドレスプールは、次の要件を満たす必要があります。
  - アドレスプールのアドレス範囲は、クライアントホストで使用される IP アドレスと同じサブネット上にはできません。
  - アドレスプールの IP アドレスは、デバイスで使用される IP アドレスと競合しません。

- アドレスプールのアドレス範囲は、内部サーバーの IP アドレスと同じサブネット上にはできません。
- SSL VPN AC インターフェイスを正しいセキュリティゾーン(この例では Untrust)に追加する必要があります。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** タブをクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。
    - B) IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。
    - C) OKをクリックします。
  - # GE1/0/2 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。
  - #GE1/0/3 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 3.3.3.1/24 に設定します。
2. trust セキュリティゾーンと untrust セキュリティゾーンの間にセキュリティポリシーを構成します。trust セキュリティゾーンと untrust セキュリティゾーンが相互に通信できることを確認してください。
3. デバイスのサーバー証明書を要求します。
  - A) 証明書のサブジェクトを作成します。
    - #トップナビゲーションバーで、**Objects** をクリックします。
    - #ナビゲーションペインで、**PKI > Certificate Subject** を選択します。
    - # **create** をクリックします。
    - # 図117に示すように、証明書のサブジェクトを作成し、OK をクリックします。

図117 証明書サブジェクトの作成

Create Certificate Subject

Certificate subject name  \*(1-31 chars)

Common name  (1-63 chars)

Country code  (2 chars, case sensitive)

State or province name  (1-63 chars)

Locality  (1-63 chars)

Organization name  (1-63 chars)

Organization unit name  (1-63 chars)

FQDN  (1-255 chars)

IP address  IPv4 address  Use interface's primary IP address

OK Cancel

B) PKIドメインを作成します。

# Certificate ページで、Create PKI domain をクリックします。

#図118に示すように PKIドメインを作成し、OK をクリックします。

図118 PKIドメインの作成

Create PKI Domain

Domain name  \*(1-31 chars)

Certificate subject

---

Key pairs for certificate request

Algorithm

Use different key pairs for encryption and signing

Key pair name  (1-64 chars)

Key length  (512-2048)

---

CRL checking  Check if a certificate has been revoked by the CA

Certificate usage extensions  IKE  SSL server  SSL client

Encryption algorithm for PKCS#7 cert files

OK Cancel

C) 証明書要求を作成します。

#certificate ページで、Submit Cert Request をクリックします。

#図119に示すように、証明書要求の設定を行います。

図119 証明書要求の作成

Submit Cert Request

PKI domain: sslvpndomain \* [Edit]

Certificate subject: sslvpncert \* [Edit]

Algorithm: RSA \*  
 Use different key pairs for encryption and signing

Key pair name: sslvpnrna \*

Key length: 1024

Password for cert revocation: (1-31 chars)

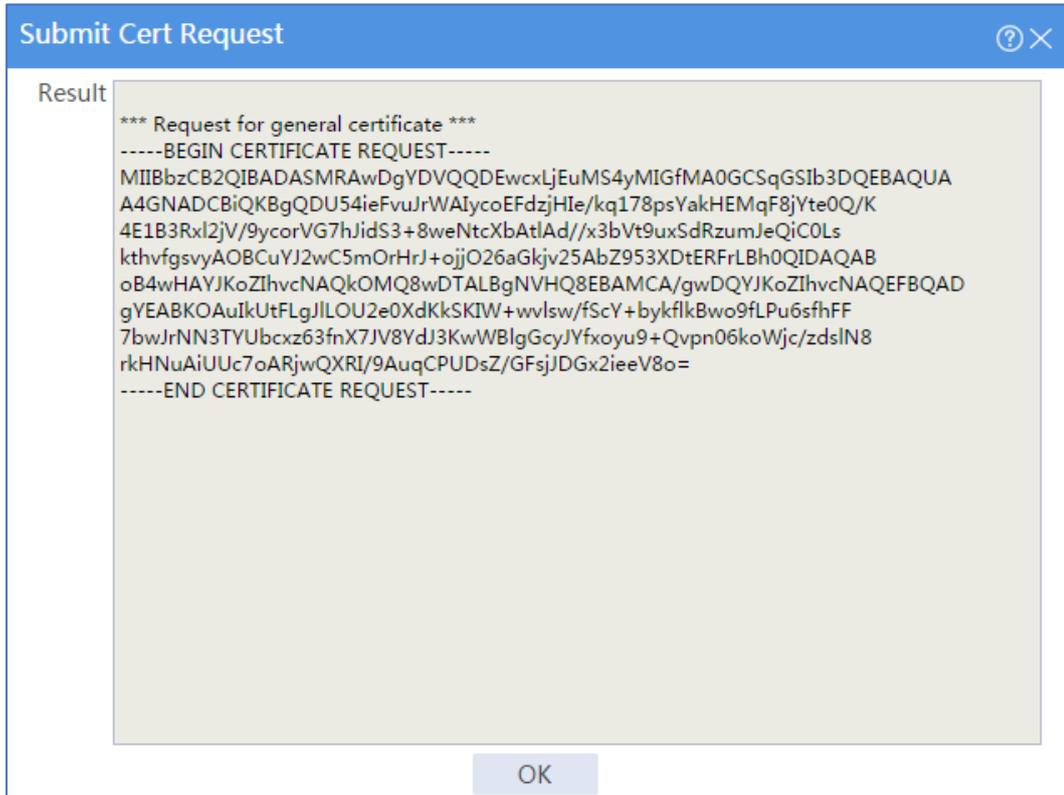
Confirm password:

OK Cancel

#OK をクリックします。

証明書要求の内容が表示されます(図 120 を参照)。

図120 証明書要求の内容



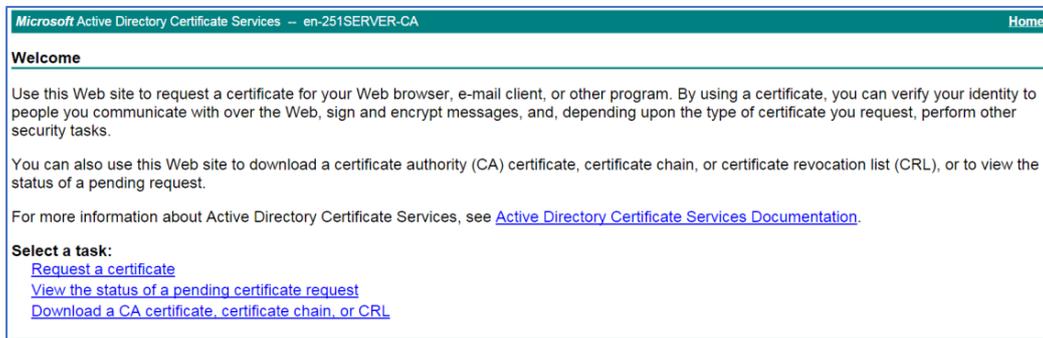
#証明書要求の内容をコピーし、OK をクリックします。

D) CAにサーバー証明書を要求する:

#ブラウザのアドレスバーに `http://192.168.100.247/certsrv` と入力します。

#図121に示す証明書サービスのホームページで、Request a certificate をクリックします。

図121 証明書サービスのホームページ



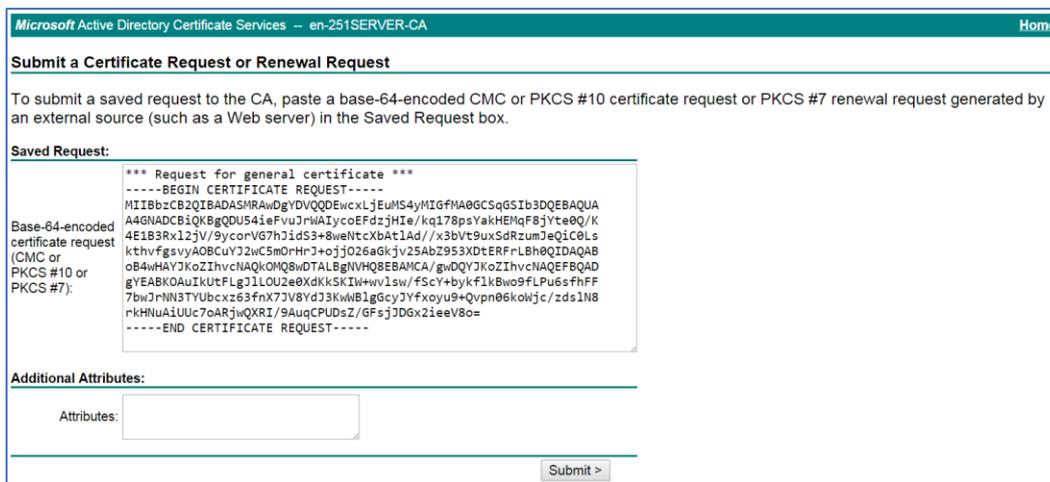
# 図122に示す Request a Certificate ページで、Advanced Certificate Request をクリックします。

図122 証明書の要求ページ



#以前にコピーした証明書要求の内容を Base-64-encoded certificate request CMC or PKCS#10or PKCS#7 フィールドに貼り付けます(図123を参照)。

図123 証明書要求の内容の貼り付け

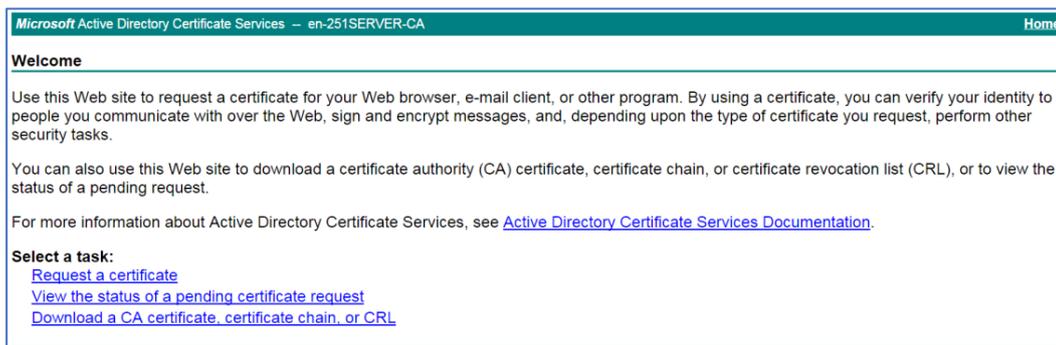


# submit をクリックします。

証明書要求が CA 管理者によって承認されたら、ブラウザのアドレスバーに http://192.168.100.247/certsrv と入力します。

#図124に示す証明書サービスのホームページで、View the status of a pending certificate request をクリックします。

図124 証明書サービスのホームページ



#表示する証明書要求を選択します。

図125 Status of a Pending Certificate Request ページの表示



Certificate Issued ページが開き、要求されたサーバー証明書が発行されたことが示されます(図126を参照)。

図126 証明書発行ページ



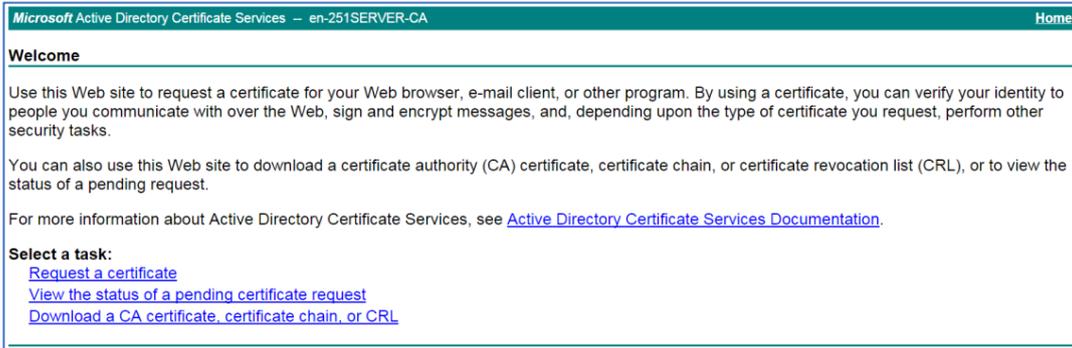
#Download certificate をクリックしてサーバー証明書をダウンロードし、ローカルに保存します。

4. CA証明書をダウンロードします。

#ブラウザのアドレスバーに <http://192.168.100.247/certsrv> と入力します。

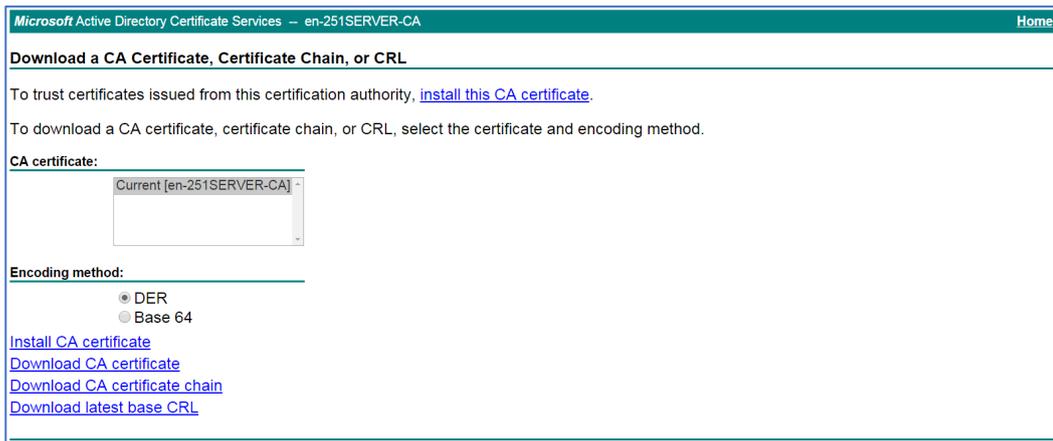
#図127に示す証明書サービスのホームページで、Download a CA certificate,certificate chain,or CRL をクリックします。

図127 証明書サービスのホームページ



# 図128の Download a CA certificate の certificate chain, or CRL ページで、Download CA certificate をクリックします。

図128 CA 証明書、証明書チェーン、または CRL ページのダウンロード



#ダウンロードした CA 証明書をローカルに保存します。

5. CA証明書とサーバー証明書をPKIドメインにインポートします。

A) CA証明書をインポートします。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**PKI > Certificate** を選択します。

# **Import certificate** をクリックします。

#ローカルに保存された CA 証明書をインポートし(図129を参照)、OK をクリックします。

図129 CA 証明書のインポート

The screenshot shows a dialog box titled "Import Certificate". It has a blue header bar with a question mark icon and a close button. The dialog contains the following fields and controls:

- PKI domain:** A dropdown menu with "sslvpnomain" selected. A red asterisk is to the right.
- Certificate type:** A dropdown menu with "CA certificate" selected.
- Select certificate file:** A text box containing "C:\fakepath\cacert.cer" and a "Select file" button. A red asterisk is to the right.
- Password for certificate:** An empty text box.
- Key pair name:** An empty text box.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

B) サーバー証明書をインポートします。

# **Certificate** ページで、**Import certificate** をクリックします。

#ローカルに保存されたサーバー証明書をインポートし(図130を参照)、OK をクリックします。

図130 サーバー証明書のインポート

The screenshot shows a dialog box titled "Import Certificate". It has a blue header bar with a question mark icon and a close button. The dialog contains the following fields and controls:

- PKI domain:** A dropdown menu with "sslvpnomain" selected. A red asterisk is to the right.
- Certificate type:** A dropdown menu with "Local certificate" selected.
- Select certificate file:** A text box containing "C:\fakepath\localcert.cer" and a "Select file" button. A red asterisk is to the right.
- Password for certificate:** An empty text box.
- Key pair name:** An empty text box.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

6. SSLサーバーポリシーを設定します。

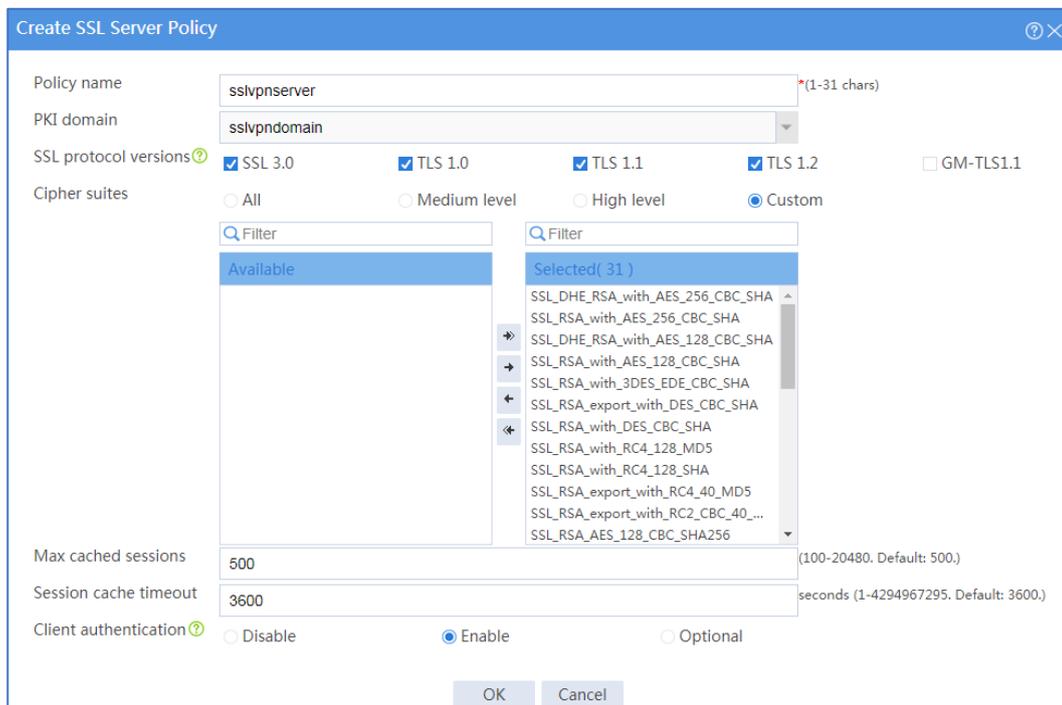
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**SSL > SSL Server Policies** を選択します。

# **create** をクリックします。

# 図131に示すように SSL サーバーポリシーを設定し、OK をクリックします。

図131 SSL サーバーポリシーの作成



7. SSLクライアントポリシーを構成します。

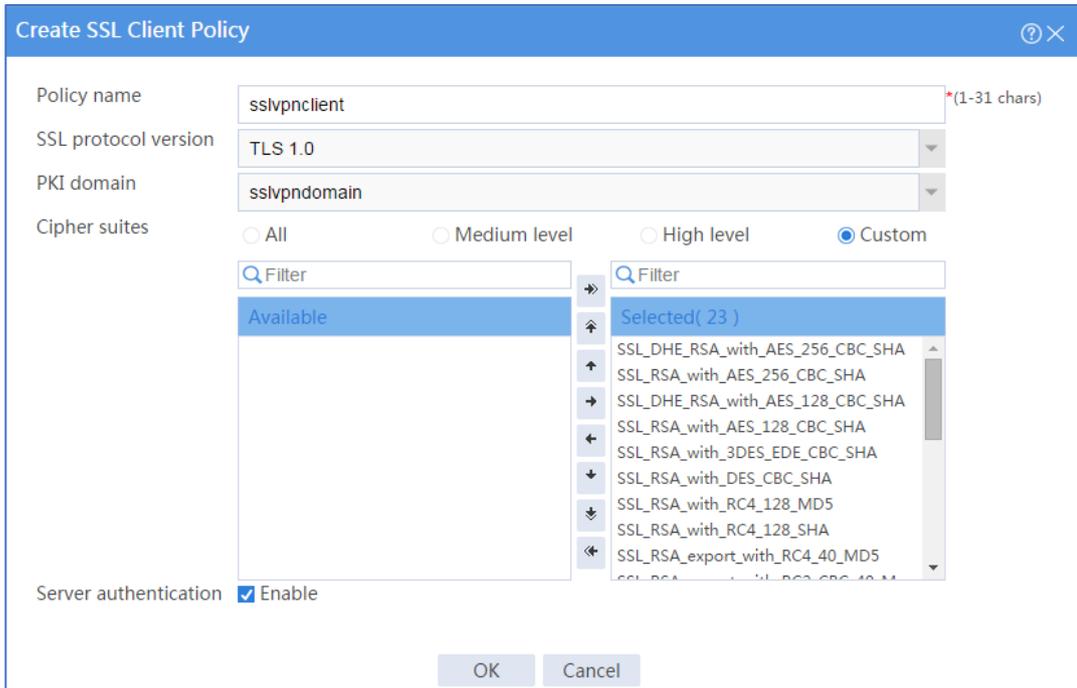
# トップナビゲーションバーで、**Objects** をクリックします。

# ナビゲーションペインで、**SSL > SSL Client Policies** を選択します。

# **create** をクリックします。

# 図 132 に示すように SSL クライアントポリシーを設定し、OK をクリックします。

図132 SSL クライアントポリシーの作成



8. RADIUSスキームを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**User > Authentication > RADIUS** を選択します。

# **create** をクリックします。

#radius という名前の RADIUS スキームを設定します。

- 認証サーバーを設定します(図133を参照)。
- 認証用のグローバル共有キーを 123456 に設定します。

図133 RADIUS スキームの設定

Create RADIUS Scheme

Scheme name  \* (1-32 chars)

Authentication servers

Primary server

Create  Delete

<input type="checkbox"/> VRF	IP version	IP address	Port	Shared key	Status	Edit
<input type="checkbox"/> Public netw	IPv4 address	3.3.3.3	1812		Active	

Secondary servers

Create  Delete

<input type="checkbox"/> VRF	IP version	IP address	Port	Shared key	Status	Edit
------------------------------	------------	------------	------	------------	--------	------

Global shared key for authentication  (1-64 chars)

Accounting servers

OK Cancel

#Advanced settings 領域で RADIUS スキームの詳細設定を行います図134(を参照)。

図134RADIUS スキームの詳細設定

Create RADIUS Scheme

Advanced settings

Source IPv4 address for outgoing RADIUS packets  3.3.3.1

Source IPv6 address for outgoing RADIUS packets  Example: 1:1::1:1

Server response timeout  3 seconds (1-10. Default: 3.)

Max RADIUS packet transmission attempts  3 (1-20. Default: 3.)

Server quiet timer  5 minutes (1-255. Default: 5.)

Real-time accounting timer  12  minutes (0-71582. Default: 720.)

Max real-time accounting attempts  5 (1-255. Default: 5.)

Format of usernames sent to servers  Without domain name

Data flow measurement unit  Byte

Packet measurement unit  One-packet

Online user password change  Enable

OK Cancel

#OK をクリックします。

9. CLI で、ISP ドメイン sslvpn を作成し、認証および認可方式に RADIUS スキーム radius を指定し、アカウントング方式を none に設定します。

```
<Device> system-view
[Device] domain sslvpn
[Device-isp-sslvpn] authentication sslvpn radius-scheme radius
[Device-isp-sslvpn] authorization sslvpn radius-scheme radius
[Device-isp-sslvpn] accounting sslvpn none
[Device-isp-sslvpn] quit
```

10. ユーザーグループを作成します。

#トップナビゲーションバーで、**Objects** 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。

#User Group タブをクリックします。

# **create** をクリックします。

#sslvpn\_usergroup という名前のユーザーグループを作成し、ユーザーグループに SSL VPN リソースグループ resourcegrp を指定します(図135を参照)。

#OK をクリックします。

図135 ユーザーグループの作成

Group name  (1-32 chars)

Identity members ?

Identity users ?

Identity groups

Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout  minutes ( 1-120 )

Authorization VLAN  ( 1-4094 )

SSLVPNPolicy

OK Cancel

11. SSL VPNゲートウェイを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。

# **create** をクリックします。

#図136に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。

図136 SSL VPN ゲートウェイの作成

Create Gateway

Gateway  \*(1-31 chars)

IP address  IPv4  IPv6

(Default: 0.0.0.0)

HTTPS port  (1025-65535. Default: 443.)

HTTP redirection

HTTP port  (1025-65535. Default: 80.)

SSL server policy

VRF

Enable

OK Cancel

12. SSL VPN ACインターフェイスを作成します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN AC Interfaces** を選択します。

# **create** をクリックします。

#開いた Create Interfaces ダイアログボックスで、Interface number フィールドに 1 と入力し、OK をクリックします。

#Modify Interface Settings ダイアログボックスで、SSL VPN AC インターフェイスの基本設定を行います(図137を参照)。

図137 SSL VPN AC インターフェイスの基本設定

Modify Interface Settings

Name: SSLVPN-AC1

Link status: **Down**  Shut down

Description: SSLVPN-AC1 Interface

Basic Configuration | IPv4 Address

Add an interface to a security zone: Untrust

VRF: Public network

MAC address: 00-00-00-FF-F6-D3

MTU: 1500 (100-64000)

Expected bandwidth: <1-400000000> (kbps)

Apply OK Cancel

#IPv4Address タブをクリックし、SSL VPN AC インターフェイスの IPv4 アドレスを設定します(図 138を参照)。

#OK をクリックします。

図138 SSL VPN AC インターフェイスのIPv4アドレス設定

**Modify Interface Settings**

Name: SSLVPN-AC1

Link status: **Down**  Shut down

Description: SSLVPN-AC1 Interface

**Basic Configuration** | IPv4 Address

IP address:  Manual assignment

IP address/mask length:  /

<input type="checkbox"/>	Secondary IP addr...	Mask length	Edit
--------------------------	----------------------	-------------	------

13. IPアクセスユーザーのアドレスプールを作成します。  
#トップナビゲーションバーで、ネットワークをクリックします。  
#ナビゲーションペインで、SSL VPN>IP Access Address Pools を選択します。  
#create をクリックします。  
#IP アクセスアドレスプールを作成し(図139を参照)、OK をクリックします。

図139 IP アクセスアドレスプールの作成

Create IP Access Address Pool

Address pool name  \*(1-31 chars)

Start IP address  \*

End IP address  \*

OK Cancel

14. SSL VPNコンテキストを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Contexts** を選択します。

# **create** をクリックします。

#図140に示すように、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。

図140 SSL VPN コンテキストの基本設定

1 Basic settings

Context name <sup>?</sup> ctxip (1-31 chars)

2 URI ACL

Associated gateways

	Gateway	Access m...	Domain	Virtual...	Edit
<input checked="" type="checkbox"/>	sslvpngw	Domain ...	domainip		

3 Access services

4 Shortcuts

5 Resource groups

VRF Public network

ISP domain

Code verification <sup>?</sup>

Certificate auth <sup>?</sup>

Enable password

Certificate and pwd authN  Use all methods  Use any method

IMC SMS verification <sup>?</sup>

Max sessions 1048575 (1-1048575)

Previous Next Cancel

#URI ACL ページで、Next をクリックします。

#アクセスサービスページで IP アクセスを選択し、next をクリックします。

#IP アクセスページで、IP アクセスサービスを次のように設定します。

A) IPアクセスパラメータを設定し(図141を参照)、Nextをクリックします。

図141 IP アクセスサービスの IP アクセスパラメータの設定

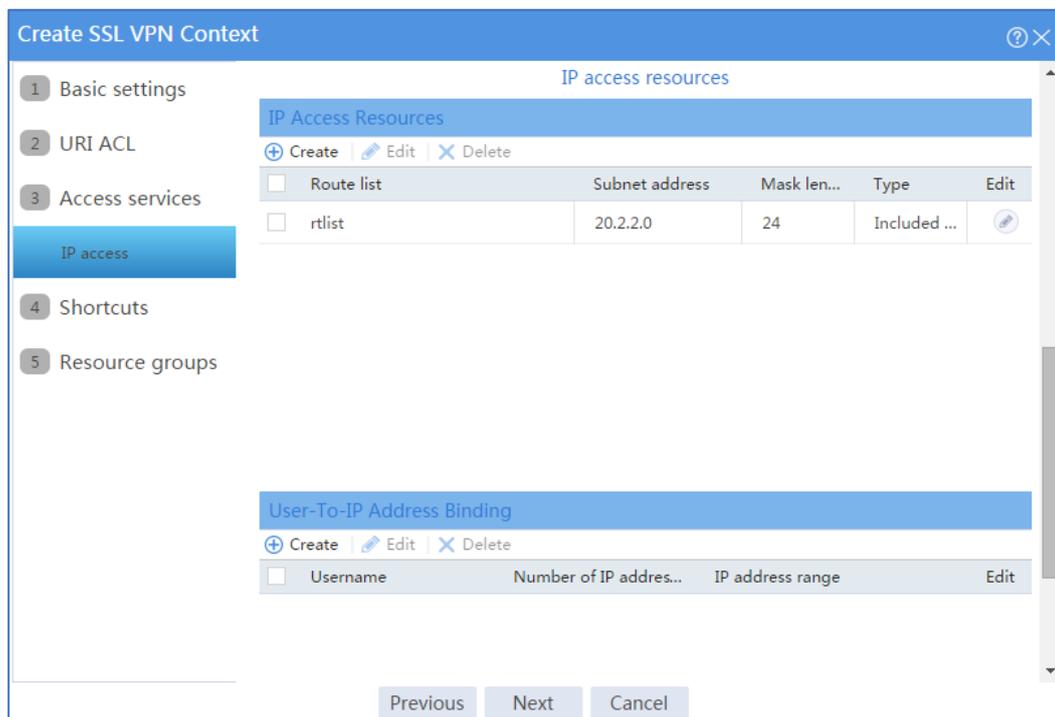
The screenshot shows the 'Create SSL VPN Context' configuration window with the 'IP access' tab selected. The configuration is as follows:

Section	Field	Value	Unit/Range
Basic settings	SSL VPN AC interface	SSLVPN-AC1	
	IP access address pool	sslvpnpool	
Access services	Mask length	24	(1-30)
	Primary DNS server	X.X.X.X	
Shortcuts	Secondary DNS server	X.X.X.X	
	Primary WINS server	X.X.X.X	
Resource groups	Secondary WINS server	X.X.X.X	
	Keepalive interval	30	seconds (0-600)
IP access	Start IP access client	<input type="checkbox"/>	
	Push Web resources	<input type="checkbox"/>	
	Rate limit (Upstream traffic)		Kbps (1000-100000000)
	Rate limit (Downstream traffic)		Kbps (1000-100000000)

Navigation buttons: Previous, Next, Cancel

- B) IP access resources領域で、図142に示すように、20.2.2.0/24のルートエントリを含むルートリストrtlistを設定します。
- C) **next**をクリックします。

図142 IP アクセスサービス用の IP アクセスリソースの設定



# **Shortcuts** ページで **next** をクリックします。

# **Resource groups** ページで、**create** をクリックします。

#resourcegrp という名前のリソースグループを作成します(図143を参照)。この例では、アクセス可能な IP リソースとしてルートリスト rtlist を選択し、IP アクセス要求フィルタリングに IPv4ACL3999(すべてのトラフィックを許可)を使用します。

図143 SSL VPN リソースグループの作成

Create Resource Group

Resource group  \* (1-31 chars)

Shortcut List

---

IP access

Force all traffic to SSL VPN

Issue routes to client

Route list  \*

IP access address pool

Mask length  (1-30)

IPv4 ACL

IPv6 ACL

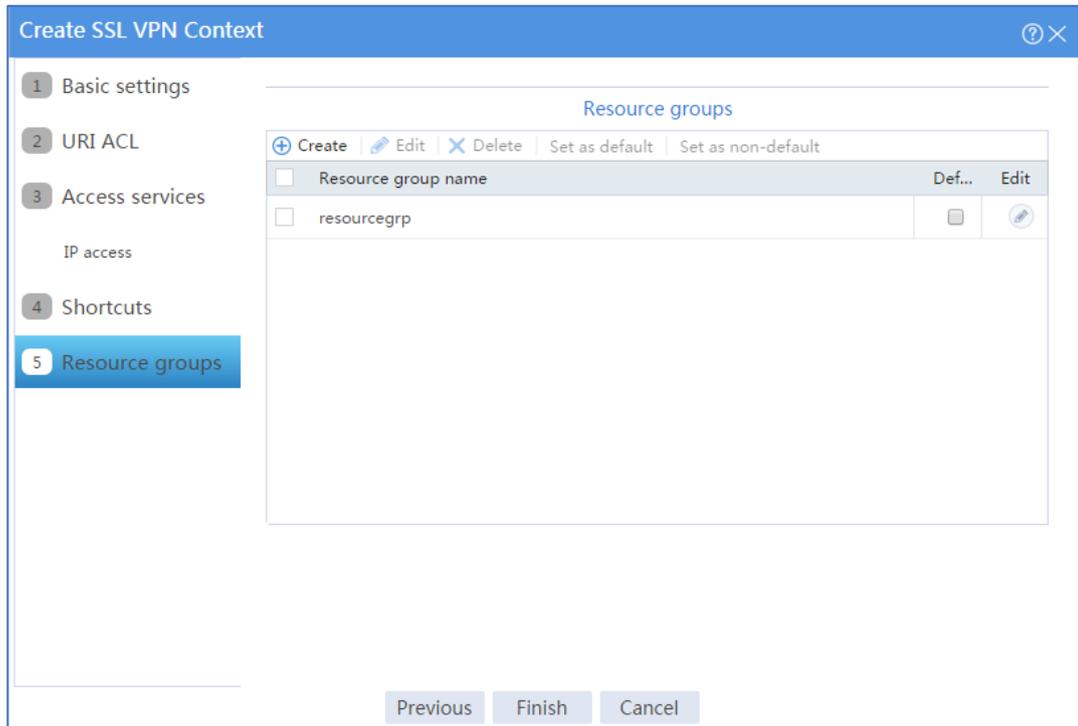
URI ACL

OK Cancel

#OK をクリックします。

Resource groups ページに、新しく作成されたリソースグループが表示されます(図144を参照)。

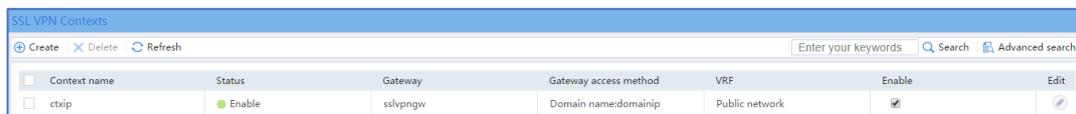
図144 リソースグループ設定ページ



# **finish** をクリックします。

#Enable チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図145を参照)。

図145 SSL VPN コンテキストのイネーブル化



Context name	Status	Gateway	Gateway access method	VRF	Enable	Edit
ctxip	Enable	sslvpngw	Domain name:domainip	Public network	<input checked="" type="checkbox"/>	

## RADIUSサーバーを構成する

1. resourcegrpという名前のアクセスポリシーを設定します。

#IMC にログインします。

#トップナビゲーションバーで、**user** をクリックします。

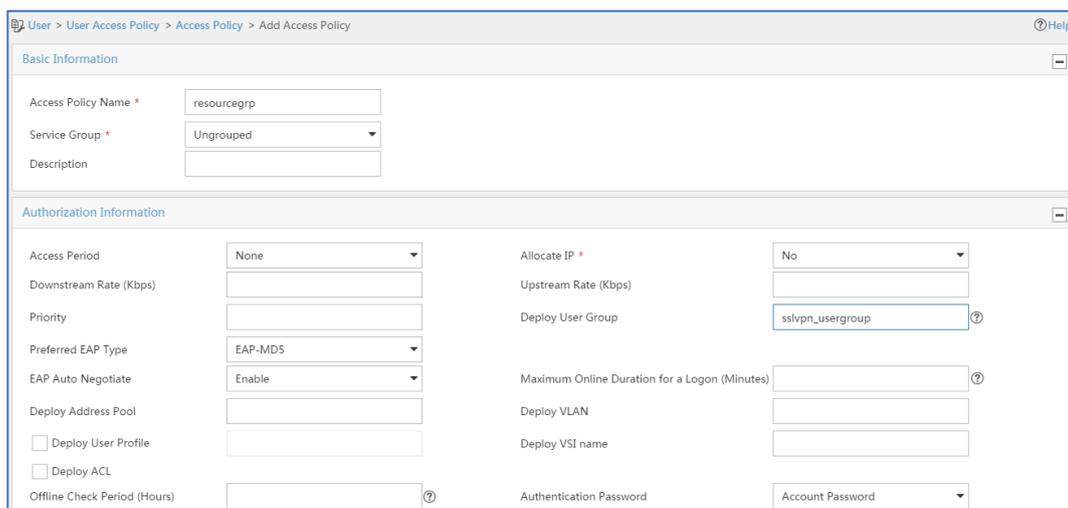
#ナビゲーションペインで、**User Access Policy > Access Policy** を選択します。

# **add** をクリックします。

#アクセスポリシーを追加します(図146を参照)。

#OK をクリックします。

図146 アクセスポリシーの作成



User > User Access Policy > Access Policy > Add Access Policy

Basic Information

Access Policy Name \* resourcegrp

Service Group \* Ungrouped

Description

Authorization Information

Access Period None

Allocate IP \* No

Downstream Rate (Kbps)

Upstream Rate (Kbps)

Priority

Deploy User Group sslvpn\_usergroup

Preferred EAP Type EAP-MD5

EAP Auto Negotiate Enable

Maximum Online Duration for a Logon (Minutes)

Deploy Address Pool

Deploy VLAN

Deploy VSI name

Deploy User Profile

Deploy ACL

Offline Check Period (Hours)

Authentication Password Account Password

2. sslvpnservice という名前のアクセスサービスを設定します。

#トップナビゲーションバーで、**user** をクリックします。

#ナビゲーションペインで、**User Access Policy > Access Service** を選択します。

# **add** をクリックします。

#アクセスサービスを追加します(図147を参照)。この例では、デフォルトのアクセスポリシーとしてアクセスポリシー-resourcegrp を指定します。

#OK をクリックします。

図147 アクセスサービスの作成

3. アクセスデバイスを設定します。

#トップナビゲーションバーで、**user** をクリックします。

#ナビゲーションペインで、**User Access Policy > Access Device Management > Access Device** を選択します。

# **add** をクリックします。

#アクセスデバイスを追加します(図148を参照)。この例では、共有キーを 123456 に設定します。

#OK をクリックします。

図148アクセスデバイスの設定

4. アクセスマユーザーを設定します。

# **User > Add User** ページにアクセスします。

#プラットフォームユーザーを追加します(図149を参照)。

#OK をクリックします。

図149 プラットフォームユーザーの追加

User > Add User

Add User

Basic Information

User Name \* zhagsan Identity Number \* none Check Availability

Contact Address Telephone

Email User Group \* Ungrouped

Open Account

OK Cancel

#ナビゲーションペインで、**Access User > All Access Users** を選択します。

# add をクリックします。

#アクセスユーザーを追加し、そのユーザーにアクセスサービス sslvpnservice を割り当てます(図150を参照)。

#OK をクリックします。

図150 アクセスユーザーの追加

User > All Access Users > Add Access User

Add Access User

Access Information

User Name \* zhagsan Select Add User

Account Name \* user1

Trial Account  Default BYOD User  MAC Authentication User  Computer User  Fast Access User

Password \* Password Confirm Password \* Password

Allow User to Change Password  Enable Password Strategy  Modify Password at Next Login

Start Time 2018-09-05 00:00 End Time 2020-09-24 00:00

Max. Idle Time (Minutes) Max. Concurrent Logins 1

Login Message

Access Service

Service Name	Service Suffix	Status	Allocate IP
<input type="checkbox"/> Portal		Available	
<input checked="" type="checkbox"/> sslvpnservice		Available	

OK Cancel

## ホストの構成

1. ホストのIPアドレスとゲートウェイアドレスを設定し、SSL VPNゲートウェイおよびCAサーバーに到達できることを確認します。
2. クライアント証明書要求をCAサーバーに送信します。
  - A) ブラウザのアドレスバーにhttp://192.168.100.247/certsrvと入力します。

- B) 図151に示す証明書サービスのホームページで、Request a certificateをクリックします。

図151 証明書サービスのホームページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA [Home](#)

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- C) Request a Certificateページ(図152を参照)で、Advanced Certificate Requestをクリックします。

図152証明書の要求ページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA [Home](#)

**Request a Certificate**

Select the certificate type:

- [Web Browser Certificate](#)
- [E-Mail Protection Certificate](#)

Or, submit an [advanced certificate request](#).

- D) クライアント証明書要求を作成します(図153を参照)。

図153 クライアント証明書要求の作成

Microsoft Active Directory Certificate Services -- en-251SERVER-CA [Home](#)

**Advanced Certificate Request**

**Identifying Information:**

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

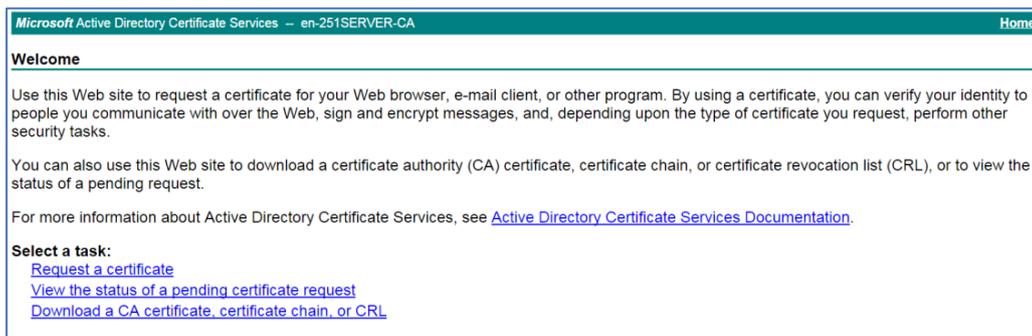
**Type of Certificate Needed:**

- E) **submit**をクリックします。

3. クライアント証明書をホストにインストールします。

- A) 証明書要求がCA管理者によって承認されたら、ブラウザのアドレスバーに <http://192.168.100.247/certsrv> と入力します。
- B) 図154に示す証明書サービスのホームページで、View the status of a pending certificate request をクリックします。

図154 証明書サービスのホームページ



View the Status of a Pending Certificate Request ページが開きます(図155を参照)。

図155 Status of a Pending Certificate Request ページの表示



- C) ステータスを表示するクライアント証明書をクリックします。
- D) Certificate Issuedページ(図156を参照)で、Install this certificate をクリックしてクライアント証明書をインストールします。

図156 クライアント証明書のインストール

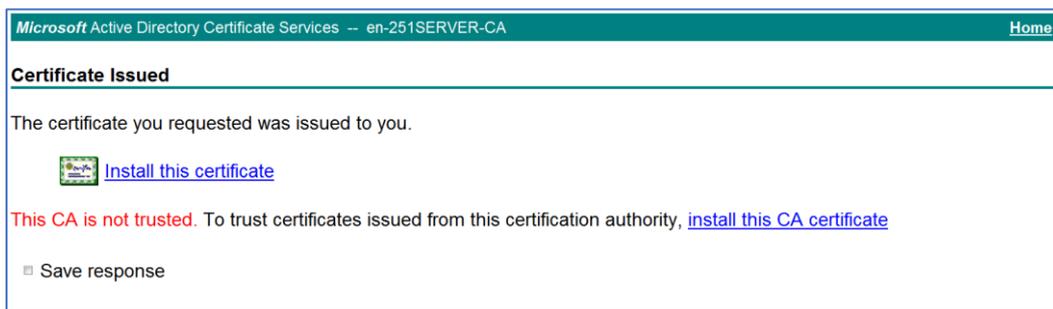


ホストに CA 証明書がない場合、図157に示すページが開きます。最初に CA 証明書をインストールする必要があります。

- E) **install this CA certificate** をクリックしてCA証明書をインストールし、**Install this**

**certificate**をクリックしてクライアント証明書をインストールします。

図157 CA 証明書とクライアント証明書のインストール



クライアント証明書をインストールすると、図158に示す Certificate Installed ページが開きます。

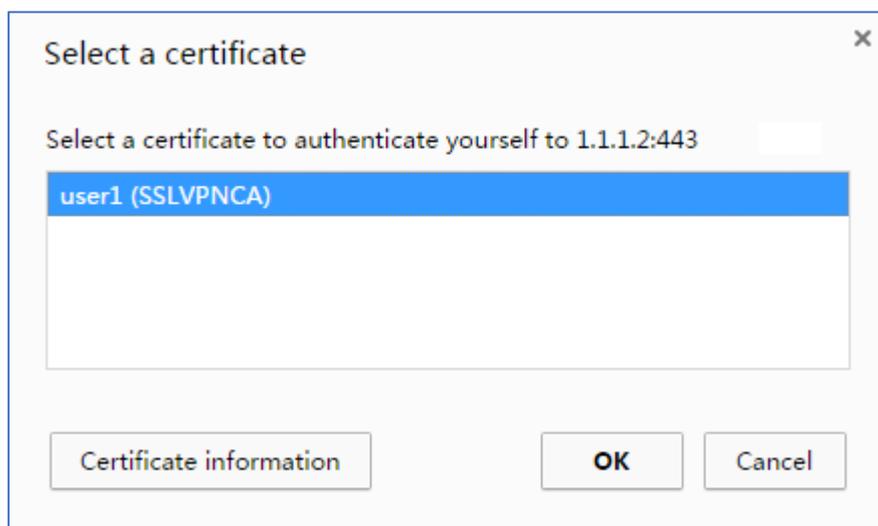
図158 Certificate Installed ページ



## 設定の確認

1. ホストのブラウザアドレスバーに https://1.1.1.2 と入力し、Enter を押します。
2. Select a certificate ページで、認証用のクライアント証明書を選択します(図159を参照)。

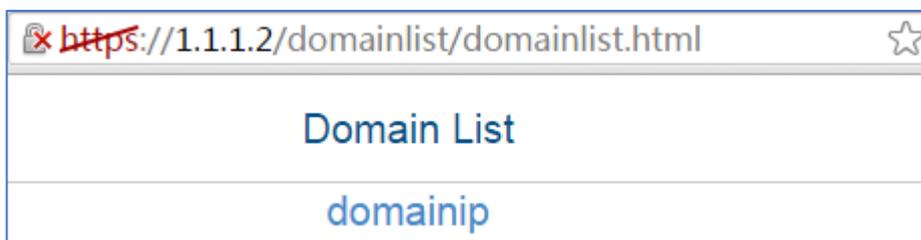
図159 証明書の選択ページ



3. OK をクリックします。

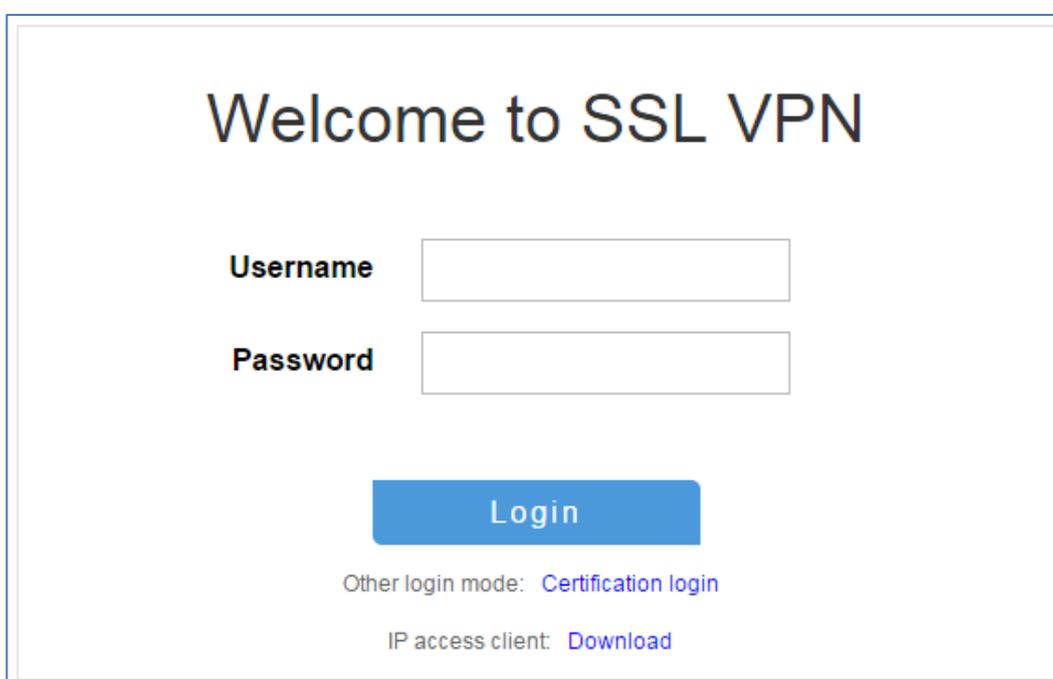
4. 図160に示す Domain List ページで、domainip を選択してログインページにアクセスします。

図160 ドメインリストページ



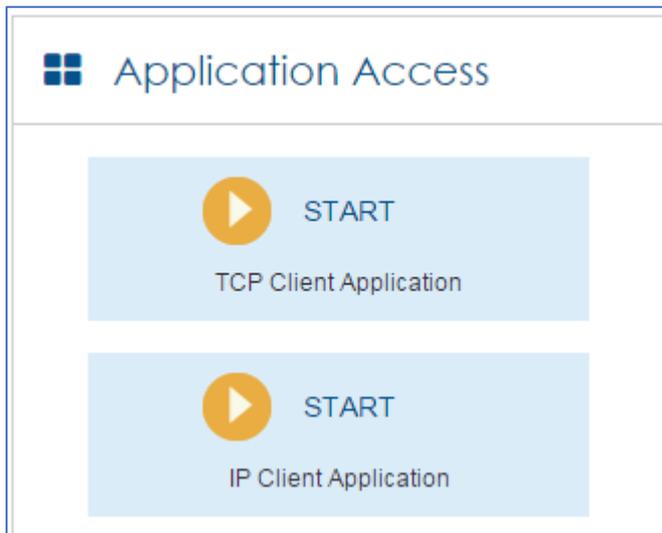
5. ログインページで、username に user1 と password に 123456 を入力し、Login をクリックします。

図161 ログインページ



6. START をクリックして、IP クライアントアプリケーションを起動します(図162を参照)。

図162 IP クライアントアプリケーションの起動

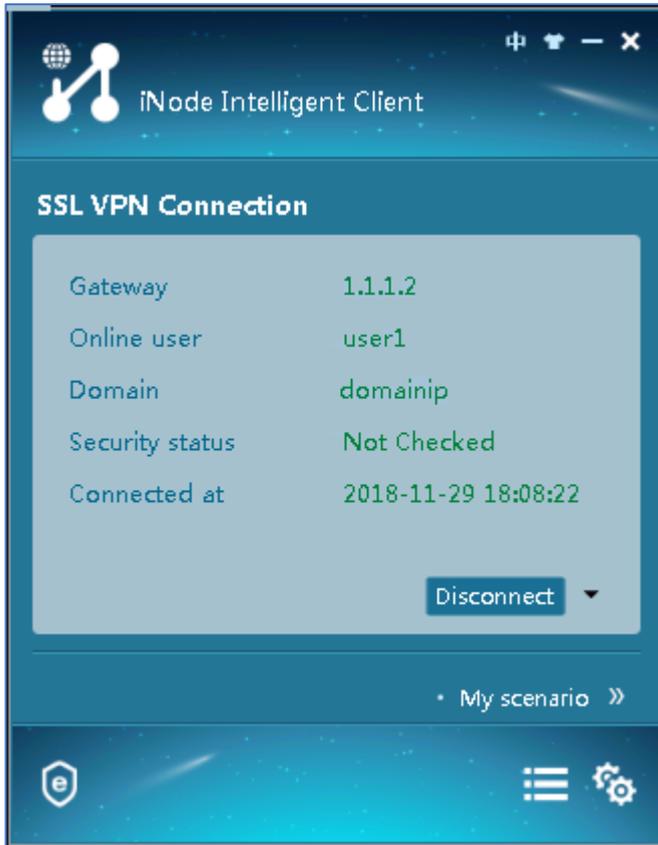


ホストに INode クライアントがインストールされていない場合、システムは INode クライアントをインストールし、INode クライアントを起動して SSL VPN ゲートウェイに接続します。

ホストにすでに INode クライアントがインストールされている場合、システムは INode クライアントを起動し、SSL VPN ゲートウェイに直接接続します。

図163に、INode クライアントが SSL VPN ゲートウェイに正常に接続されたことを示します。

図163 INode クライアントの SSL VPN ゲートウェイへの接続



## 例:LDAP認証によるIPアクセスの設定

### ネットワーク構成

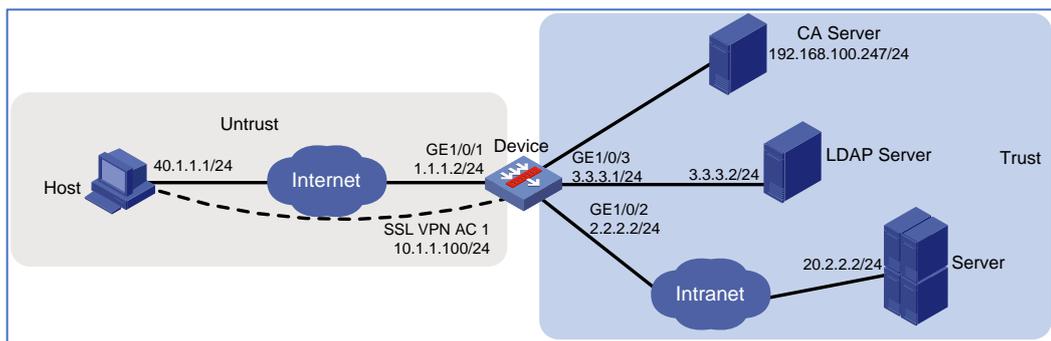
図164に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続する SSL VPN ゲートウェイとして動作します。プライベートネットワークでは、CA サーバーと LDAP サーバーが展開され、両方のサーバーで Windows Server2008R2 オペレーティングシステムが実行されます。ユーザーは、IP アクセスモードで内部サーバー(20.2.2.2/24)にセキュアにアクセスする必要があります。

以下のタスクを実行してください。

- CA サーバーからデバイスの SSL サーバー証明書を要求します。
- ユーザーが IP アクセスのパスワード認証と証明書認証の両方を通過するようにデバイスを設定します。

- LDAP サーバーを使用して IP アクセスユーザーのリモート認証と認可を実行するようにデバイスを設定します。
- ユーザーが IP アクセスモードで内部サーバーにアクセスできるように、デバイス上で SSL VPN IP アクセスサービスを設定します。

図164 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

- Web インターフェイスから IP クライアントを起動するには、Java Runtime Environment バージョン 1.7(JRE1.7)以降がクライアントホストにインストールされていることを確認してください。
- クライアントアドレス割り当て用に設定された IP アドレスプールは、次の要件を満たす必要があります。
  - アドレスプールのアドレス範囲は、クライアントホストで使用される IP アドレスと同じサブネット上にはできません。
  - アドレスプールの IP アドレスは、デバイスで使用される IP アドレスと競合しません。

- アドレスプールのアドレス範囲は、内部サーバーの IP アドレスと同じサブネット上にはできません。
- SSL VPN AC インターフェイスを正しいセキュリティゾーン(この例では Untrust)に追加する必要があります。

## 手順

### デバイスの設定

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、Network タブをクリックします。  
#ナビゲーションペインで、Interface Configuration > Interfaces を選択します。  
#GE1/0/1 の **edit** アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
A) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。  
B) IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、1.1.1.2/24と入力します。  
C) OKをクリックします。  
#GE1/0/ge1//2 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 2.2.2.2/24 に設定します。  
#GE1/0/ge1//3 を **Trust** セキュリティゾーンに追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 3.3.3.1/24 に設定します。
2. trust セキュリティゾーンと untrust セキュリティゾーンの間にセキュリティポリシーを構成します。  
trust セキュリティゾーンと untrust セキュリティゾーンが相互に通信できることを確認してください。
3. デバイスのサーバー証明書を要求します。  
A) 証明書のサブジェクトを作成します。  
#トップナビゲーションバーで、**Objects** をクリックします。  
#ナビゲーションペインで、**PKI > Certificate Subject** を選択します。  
# **create** をクリックします。  
#図165に示すように、証明書のサブジェクトを作成し、OK をクリックします。

図165 証明書サブジェクトの作成

Create Certificate Subject

Certificate subject name  \*(1-31 chars)

Common name  (1-63 chars)

Country code  (2 chars, case sensitive)

State or province name  (1-63 chars)

Locality  (1-63 chars)

Organization name  (1-63 chars)

Organization unit name  (1-63 chars)

FQDN  (1-255 chars)

IP address  IPv4 address  Use interface's primary IP address

OK Cancel

B) PKIドメインを作成します。

#Certificate ページで、Create PKI domain をクリックします。

#図166に示すように PKIドメインを作成し、OK をクリックします。

図166 PKIドメインの作成

Create PKI Domain

Domain name  \*(1-31 chars)

Certificate subject

---

Key pairs for certificate request

Algorithm

Use different key pairs for encryption and signing

Key pair name  (1-64 chars)

Key length  (512-2048)

---

CRL checking  Check if a certificate has been revoked by the CA

Certificate usage extensions  IKE  SSL server  SSL client

Encryption algorithm for PKCS#7 cert files

OK Cancel

C) 証明書要求を作成します。

#証明書 certificate ページで、Submit Cert Request をクリックします。

#図167に示すように、証明書要求の設定を行います。

図167 証明書要求の作成

Create PKI Domain

Domain name  \*(1-31 chars)

Certificate subject

Key pairs for certificate request

Algorithm

Use different key pairs for encryption and signing

Key pair name  (1-64 chars)

Key length  (512-2048)

CRL checking  Check if a certificate has been revoked by the CA

Certificate usage extensions  IKE  SSL server  SSL client

Encryption algorithm for PKCS#7 cert files

OK Cancel

#OK をクリックします。

証明書要求の内容が表示されます(図168を参照)。

図168 証明書要求の内容

Create PKI Domain

Domain name: sslvndomain \*(1-31 chars)

Certificate subject: sslvncert

Key pairs for certificate request

Algorithm: RSA

Use different key pairs for encryption and signing

Key pair name: sslvnrsa (1-64 chars)

Key length: 1024 (512-2048)

CRL checking:  Check if a certificate has been revoked by the CA

Certificate usage extensions:  IKE  SSL server  SSL client

Encryption algorithm for PKCS#7 cert files: DES-CBC

OK Cancel

#証明書要求の内容をコピーし、OK をクリックします。

D) CAにサーバー証明書を要求する:

#ブラウザのアドレスバーに http://192.168.100.247/certsrv と入力します。

#図169に示す証明書サービスのホームページで、Request a certificate をクリックします。

図169 証明書サービスのホームページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

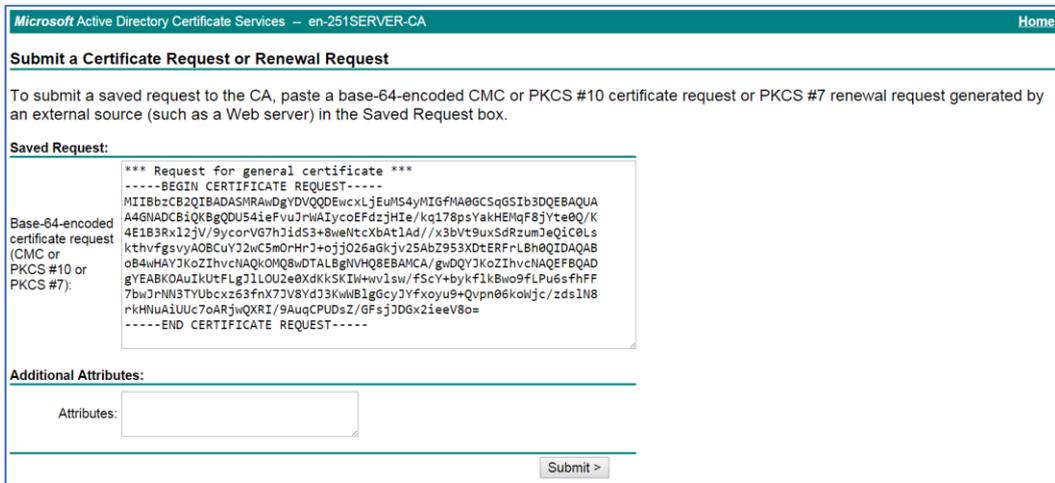
#図170に示す Request a Certificate ページで、Advanced Certificate Request をクリックします。

図170 証明書の要求ページ



#以前にコピーした証明書要求の内容を Base-64-encoded certificate request CMC or PKCS#10 or PKCS#7 フィールドに貼り付けます(図171を参照)。

図171 証明書要求の内容の貼り付け

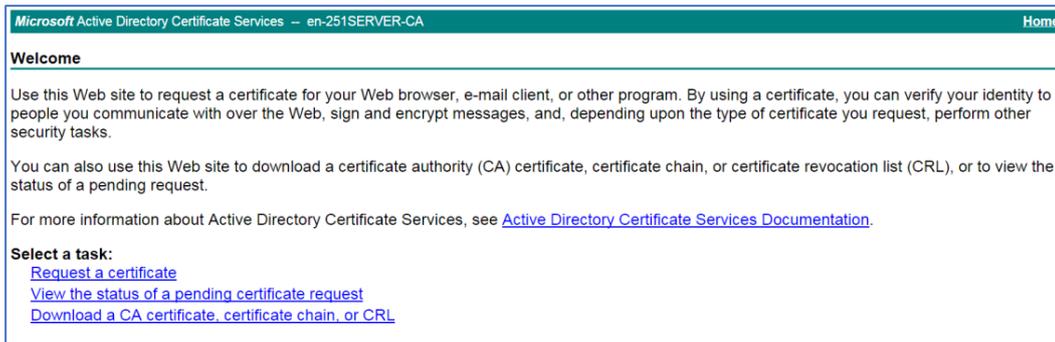


#submit をクリックします。

証明書要求が CA 管理者によって承認されたら、ブラウザのアドレスバーに <http://192.168.100.247/certsrv> と入力します。

#図172に示す証明書サービスのホームページで、View the status of a pending certificate request をクリックします。

図172 証明書サービスのホームページ



#表示する証明書要求を選択します。

図173 Status of a Pending Certificate Request ページの表示



Certificate Issued ページが開き、要求されたサーバー証明書が発行されたことが示されます(図174を参照)。

図174 証明書発行ページ



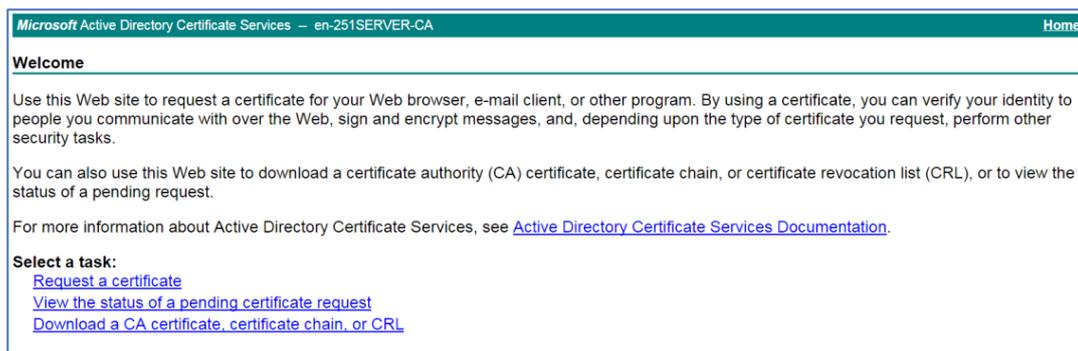
#Download certificate をクリックしてサーバー証明書をダウンロードし、ローカルに保存します。

4. CA証明書をダウンロードします。

#ブラウザのアドレスバーに http://192.168.100.247/certsrv と入力します。

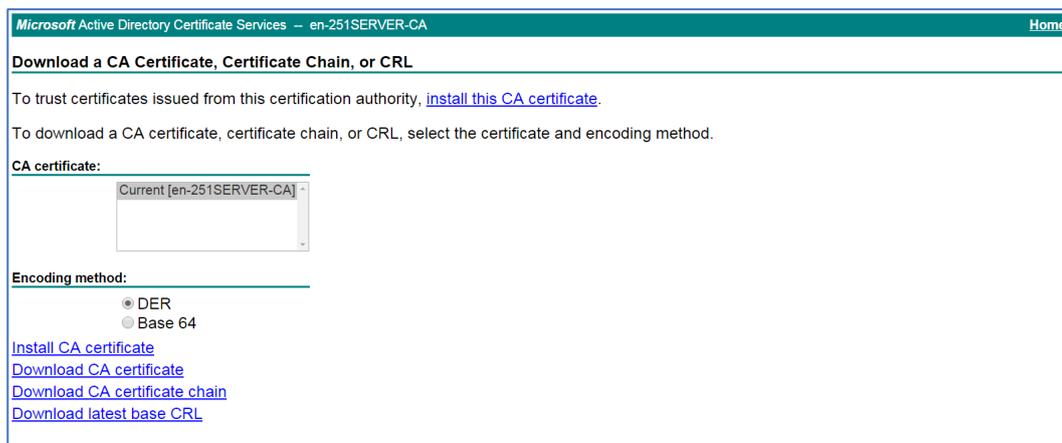
#図175に示す証明書サービスのホームページで、Download a CA certificate,certificate chain,or CRL をクリックします。

図175 証明書サービスのホームページ



#図176の Download a CA certificate,certificate chain,or CRL ページで、Download CA certificate をクリックします。

図176 CA 証明書、証明書チェーン、または CRL ページのダウンロード



#ダウンロードした CA 証明書をローカルに保存します。

5. CA証明書とサーバー証明書をPKIドメインにインポートします。

A) CA証明書をインポートします。

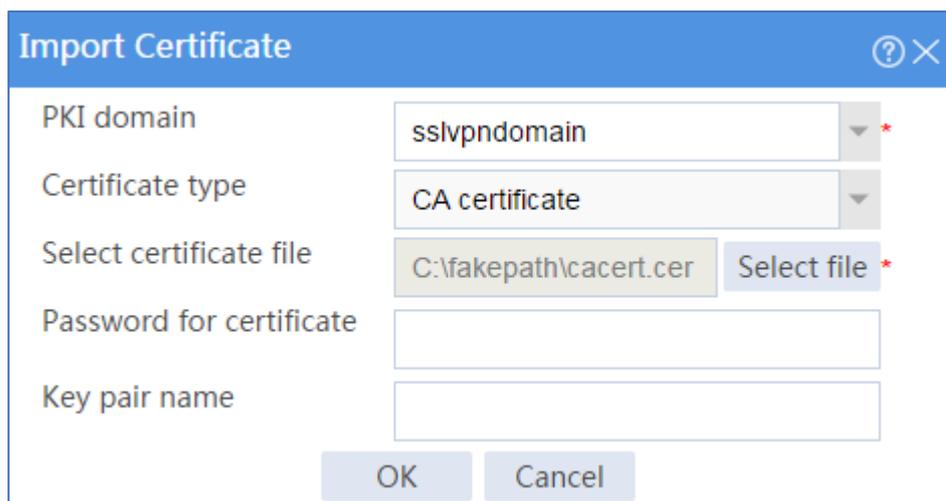
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**PKI > Certificate** を選択します。

# **Import certificate** をクリックします。

#ローカルに保存された CA 証明書をインポートし(図177を参照)、OK をクリックします。

図177 CA 証明書のインポート

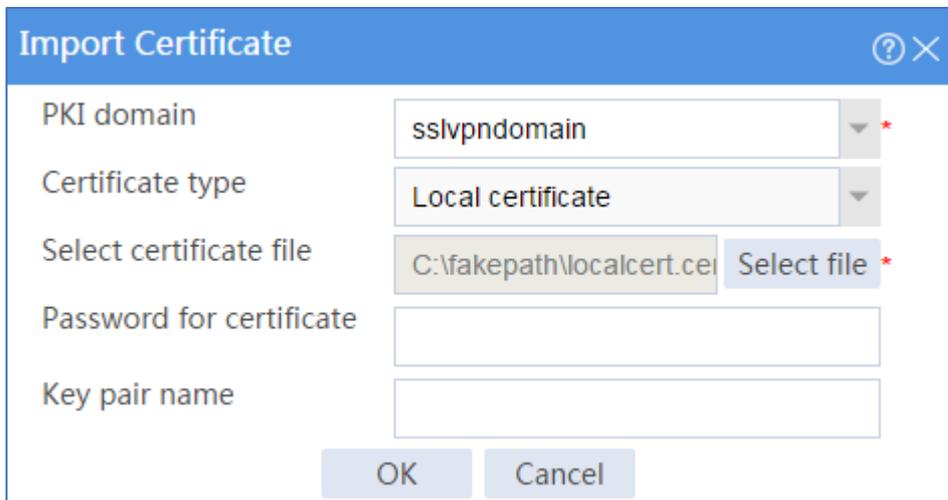


B) サーバー証明書をインポートします。

# **Certificate** ページで、**Import certificate** をクリックします。

#ローカルに保存されたサーバー証明書をインポートし(図178を参照)、OK をクリックします。

図178 サーバー証明書のインポート



Import Certificate

PKI domain: sslvpnomain \*

Certificate type: Local certificate \*

Select certificate file: C:\fakepath\localcert.cer Select file \*

Password for certificate: [Empty]

Key pair name: [Empty]

OK Cancel

6. SSLサーバーポリシーを設定します。

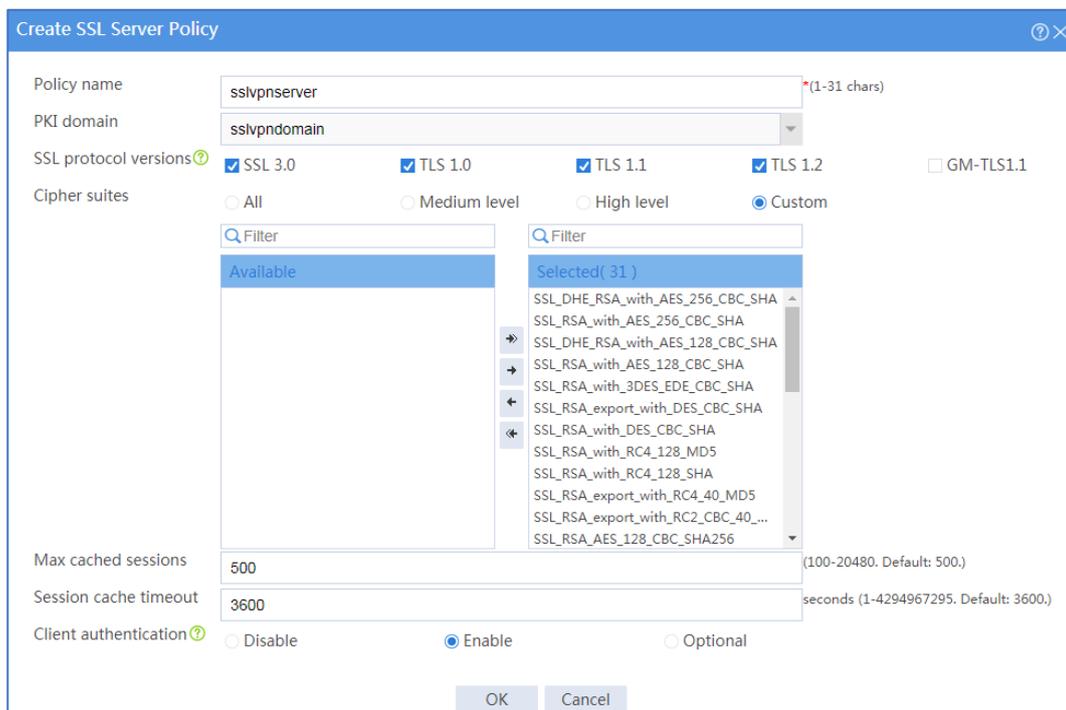
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、SSL > SSL Server Policies を選択します。

# **create** をクリックします。

#図179に示すように SSL サーバーポリシーを設定し、OK をクリックします。

図179 SSL サーバーポリシーの作成



7. SSLクライアントポリシーを構成します。

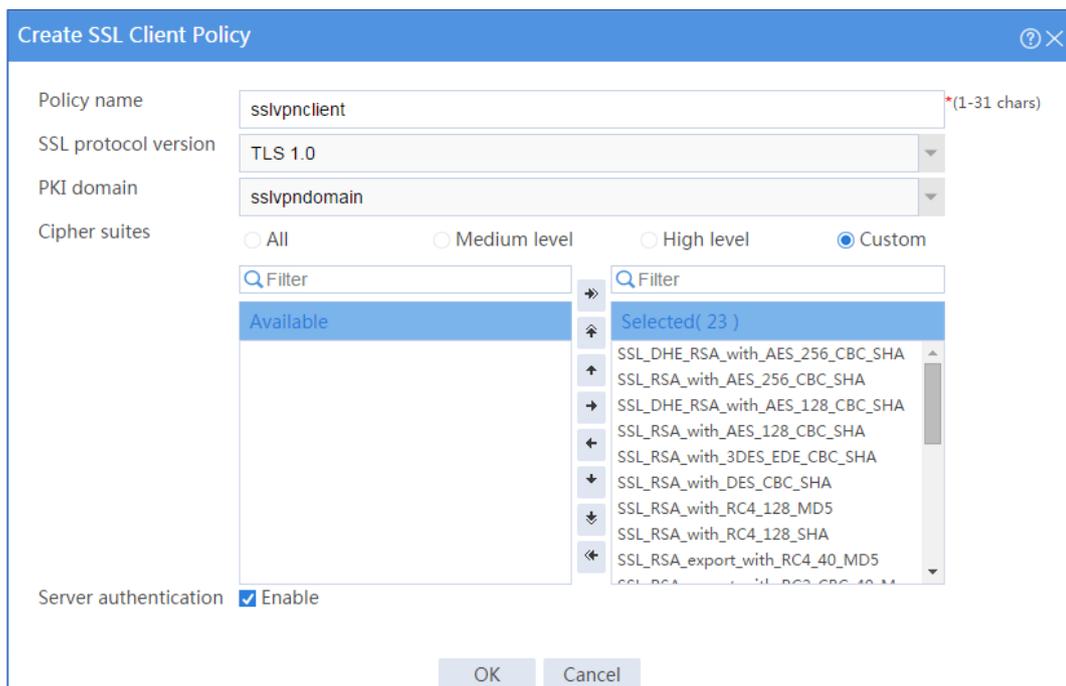
#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**SSL > SSL Client Policies** を選択します。

# **create** をクリックします。

#図180に示すように SSL クライアントポリシーを設定し、OK をクリックします。

図180 SSL クライアントポリシーの作成



8. CLIでLDAP設定を構成します。

```
# Configure LDAP server ldap1.
```

```
<Device> system-view
```

```
[Device] ldap server ldap1
```

```
[Device-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ldap,dc=com
```

```
[Device-ldap-server-ldap1] search-base-dn ou=sslvpn_usergroup,dc=ldap,dc=com
```

```
[Device-ldap-server-ldap1] ip 3.3.3.3
```

```
[Device-ldap-server-ldap1] login-password simple 123456
```

```
[Device-ldap-server-ldap1] quit
```

```
# Configure LDAP attribute map test.
```

```
[Device] ldap attribute-map test
```

```
[Device-ldap-attr-map-test] map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
```

```
[Device-ldap-attr-map-test] quit
```

```
# Configure LDAP scheme shm1.
```

```
[Device] ldap scheme shm1
```

```
[Device-ldap-shm1] authentication-server ldap1
[Device-ldap-shm1] authorization-server ldap1
[Device-ldap-shm1] attribute-map test
[Device-ldap-shm1] quit
# Configure ISP domain sslvpn.
[Device] domain sslvpn
[Device-isp-sslvpn] state active
[Device-isp-sslvpn] authentication sslvpn ldap-scheme shm1
[Device-isp-sslvpn] authorization sslvpn ldap-scheme shm1
[Device-isp-sslvpn] accounting sslvpn none
[Device-isp-sslvpn] quit
```

9. ユーザーグループを作成します。

#トップナビゲーションバーで、**Objects** 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。

#User Group タブをクリックします。

# creat をクリックします。

#sslvpn\_usergroup という名前のユーザーグループを作成し、ユーザーグループに SSL VPN リソースグループ resourcegrp を指定します(図181を参照)。

#OK をクリックします。

図181 ユーザーグループの作成

Create User Group

Group name  \* (1-32 chars)

Identity members ?

Identity users ?

Identity groups

Authorization attributes

ACL type  IPv4 ACL  Layer 2 ACL

Authorization ACL

Idle timeout  minutes ( 1-120 )

Authorization VLAN  ( 1-4094 )

SSLVPNPolicy

OK Cancel

10. SSL VPNゲートウェイを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN Gateways** を選択します。

# **create** をクリックします。

#図182に示すように SSL VPN ゲートウェイを作成し、OK をクリックします。

図182 SSL VPN ゲートウェイの作成

Create Gateway

Gateway  \*(1-31 chars)

IP address  IPv4  IPv6

(Default: 0.0.0.0)

HTTPS port  (1025-65535. Default: 443.)

HTTP redirection

HTTP port  (1025-65535. Default: 80.)

SSL server policy

VRF

Enable

OK Cancel

11. SSL VPN ACインターフェイスを作成します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > SSL VPN AC Interfaces** を選択します。

# **create** をクリックします。

#開いた Create Interfaces ダイアログボックスで、Interface number フィールドに 1 と入力し、OK をクリックします。

#Modify Interface Settings ダイアログボックスで、SSL VPN AC インターフェイスの基本設定を行います(図183を参照)。

図183 SSL VPN AC インターフェイスの基本設定

**Modify Interface Settings** [?] [X]

Name: SSLVPN-AC1

Link status: **Down**  Shut down

Description: SSLVPN-AC1 Interface

Basic Configuration | **IPv4 Address**

Add an interface to a security zone: Untrust

VRF: Public network

MAC address: 00-00-00-FF-F6-D3

MTU: 1500 (100-64000)

Expected bandwidth: <1-400000000> (kbps)

Apply OK Cancel

#IPv4 Address タブをクリックし、SSL VPN AC インターフェイスの IPv4 アドレスを設定します(図 184を参照)。

#OK をクリックします。

図184 SSL VPN AC インターフェイスのIPv4アドレス設定

The screenshot shows a 'Modify Interface Settings' window for the 'SSLVPN-AC1' interface. The window has a blue header with a question mark and a close button. The main content area is divided into two tabs: 'Basic Configuration' and 'IPv4 Address'. The 'IPv4 Address' tab is selected. Under 'IP address', the 'Manual assignment' radio button is selected. The 'IP address/mask length' field is filled with '10.1.1.100 / 255.255.255.0'. Below this, there are two buttons: '+ Assign secondary IP' and 'X Delete secondary IP'. A table below these buttons has columns for 'Secondary IP addr...', 'Mask length', and 'Edit', but it is currently empty. At the bottom of the window are three buttons: 'Apply', 'OK', and 'Cancel'.

12. IPアクセスユーザーのアドレスプールを作成します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**SSL VPN > IP Access Address Pools** を選択します。

# **create** をクリックします。

#IP アクセスアドレスプールを作成し(図185を参照)、OK をクリックします。

図185 IP アクセスアドレスプールの作成

Create IP Access Address Pool

Address pool name  \*(1-31 chars)

Start IP address  \*

End IP address  \*

OK Cancel

13. SSL VPNコンテキストを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、SSL VPN > SSL VPN Contexts を選択します。

# **create** をクリックします。

#図186に示すように、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。

図186 SSL VPN コンテキストの基本設定

Create SSL VPN Context

1 Basic settings

Context name  (1-31 chars)

2 URI ACL

3 Access services

4 Shortcuts

5 Resource groups

Associated gateways

<input checked="" type="checkbox"/>	Gateway	Access m...	Domain	Virtual...	Edit
<input checked="" type="checkbox"/>	sslvpngw	Domain ...	domainip		<input type="text"/>

VRF

ISP domain

Code verification

Certificate auth

Enable password

Certificate and pwd authN  Use all methods  Use any method

IMC SMS verification

Max sessions  (1-1048575)

Previous Next Cancel

#URI ACL ページで、Next をクリックします。

# Access services ページで IP access を選択し、next をクリックします。

# IP access ページで、IP アクセスサービスを次のように設定します。

A) IPアクセスパラメータを設定し(図187を参照)、Nextをクリックします。

図187 IP アクセスサービスの IP アクセスパラメータの設定

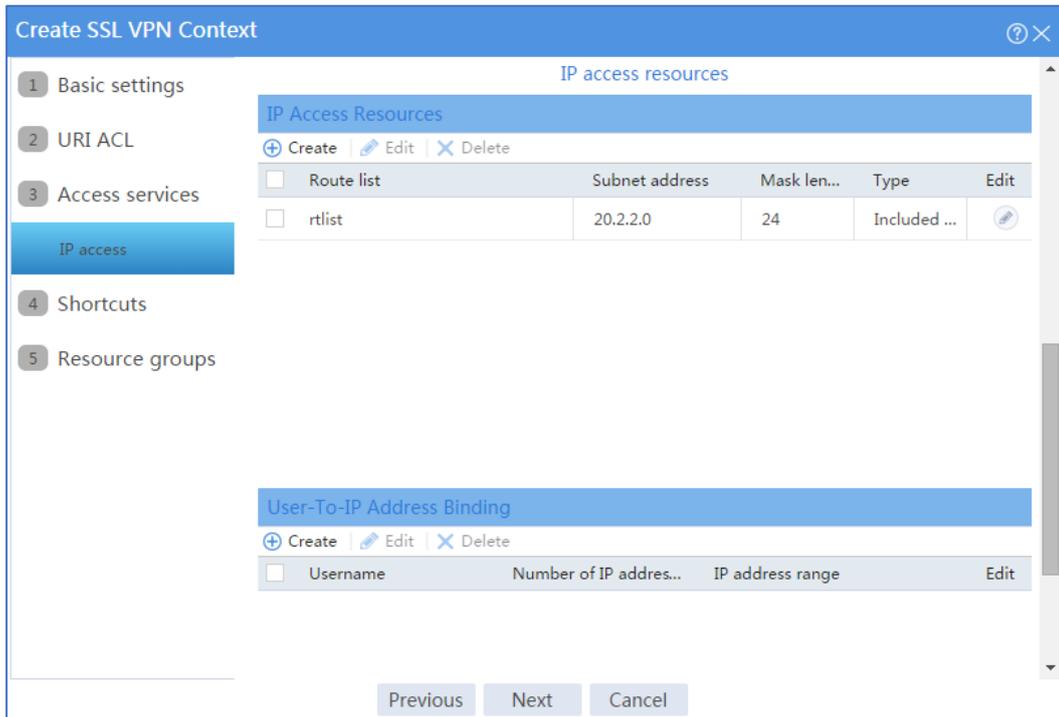
The screenshot shows the 'Create SSL VPN Context' configuration window with the 'IP access' tab selected. The configuration is as follows:

Section	Parameter	Value	Unit/Range
Basic settings	SSL VPN AC interface	SSLVPN-AC1	
	IP access address pool	sslvpnpool	
Access services	Mask length	24	(1-30)
	Primary DNS server	X.X.X.X	
Shortcuts	Secondary DNS server	X.X.X.X	
	Primary WINS server	X.X.X.X	
Resource groups	Secondary WINS server	X.X.X.X	
	Keepalive interval	30	seconds (0-600)
IP access	Start IP access client	<input type="checkbox"/>	
	Push Web resources	<input type="checkbox"/>	
Rate limit	Upstream traffic		Kbps (1000-100000000)
	Downstream traffic		Kbps (1000-100000000)

Buttons at the bottom: Previous, Next, Cancel

- B) IP access resources領域で、図188に示すように、20.2.2.0/24のルートエントリを含むルートリストrtlistを設定します。
- C) nextをクリックします。

図188 IP アクセスサービス用の IP アクセスリソースの設定



# **Shortcuts** ページで next をクリックします。

#**Resource group** ページで、create をクリックします。

#resourcegrp という名前のリソースグループを作成します(図189を参照)。この例では、アクセス可能な IP リソースとしてルートリスト rtlist を選択し、IP アクセス要求フィルタリングに IPv4 ACL 3999(すべてのトラフィックを許可)を使用します。

図189 SSL VPN リソースグループの作成

Create Resource Group

Resource group  \* (1-31 chars)

Shortcut List

---

IP access

Force all traffic to SSL VPN

Issue routes to client

Route list  \*

IP access address pool

Mask length  (1-30)

IPv4 ACL

IPv6 ACL

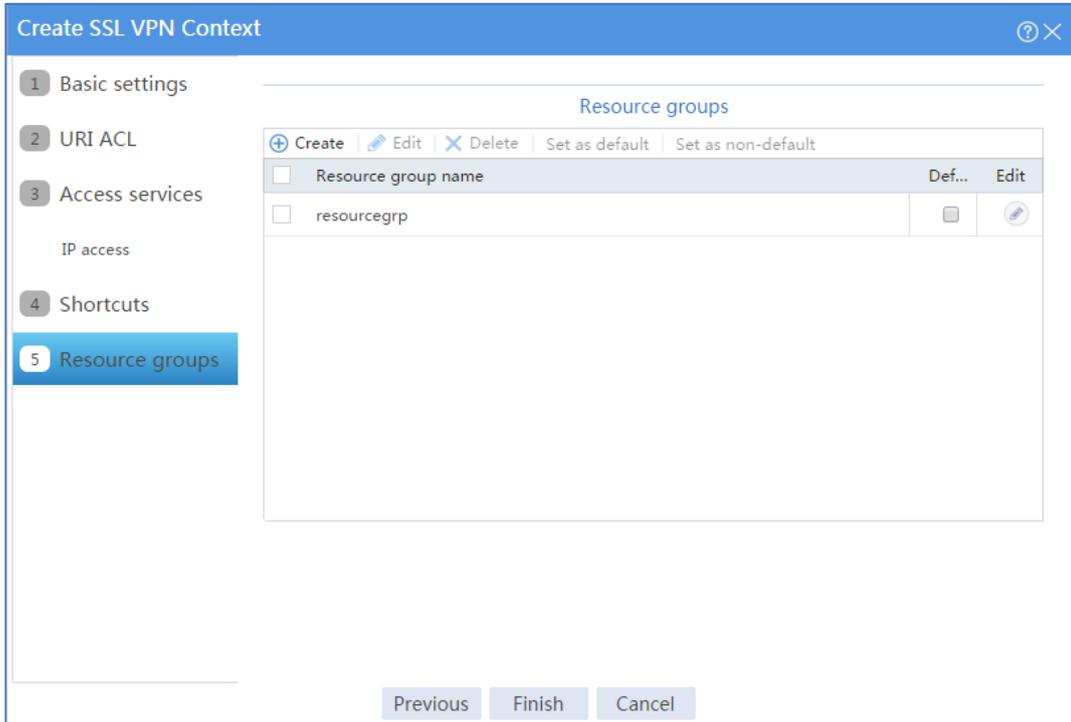
URI ACL

OK Cancel

#OK をクリックします。

Resource groups ページに、新しく作成されたリソースグループが表示されます(図190を参照)。

図190 リソースグループ設定ページ



# finish をクリックします。

#Enable チェックボックスをオンにして、SSL VPN コンテキストをイネーブルにします(図191を参照)。

図191 SSL VPN コンテキストのイネーブル化



## LDAPサーバーを構成する

1. ユーザーグループ **sslvpn\_usergroup** を作成します。

#LDAP サーバーで、**Start > Administrative Tools > Server Manager** を選択してサーバーマネージャを起動します。

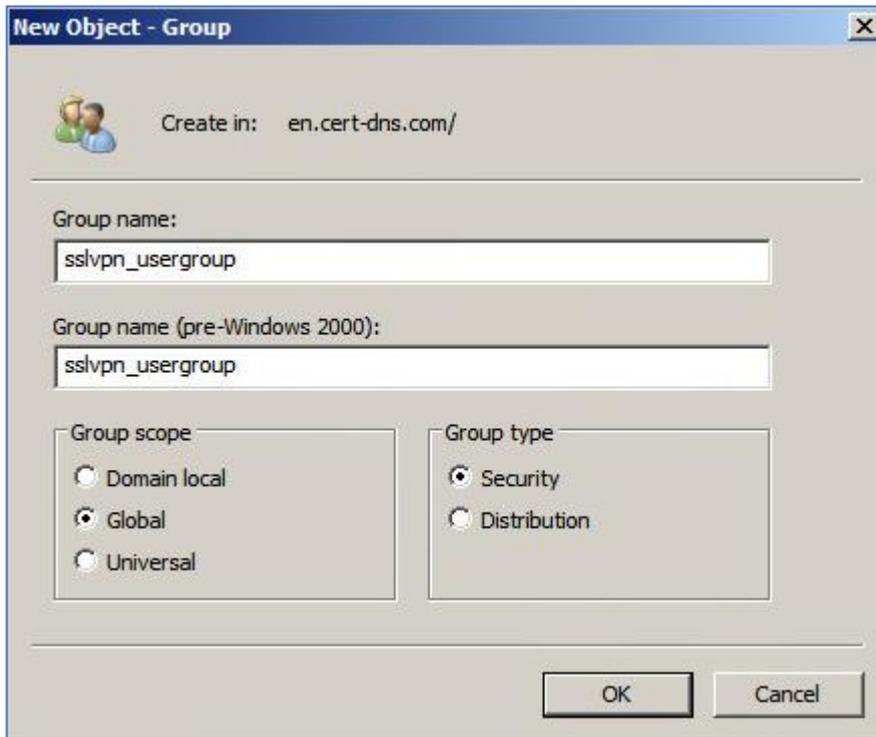
#ナビゲーションペインで、**Roles > Active Directory Domain Services > Active Directory Users and Computers** を選択します。

# **en.cert-dns.com** ノードの下にある **Users** を右クリックし、ショートカットメニューから **New > Group** を選択します。

#ユーザーグループ **sslvpn\_usergroup** を作成します(図192を参照)。

#OK をクリックします。

図192 ユーザーグループの作成



2. ユーザーuser1 を作成し、ユーザーグループ sslvpn\_usergroup に追加します。  
# LDAP サーバーで、**Start > Administrative Tools > Server Manager** を選択してサーバーマネージャを起動します。  
#ナビゲーションペインで、**Roles > Active Directory Domain Services > Active Directory Users and Computers** を選択します。  
# en.cert-dns.com ノードを右クリックし、ショートカットメニューから **New > Organizational Unit** を選択します。  
#組織単位 **sslvpn\_usergroup** を作成します(図193を参照)。  
#OK をクリックします。

図193 組織単位の作成

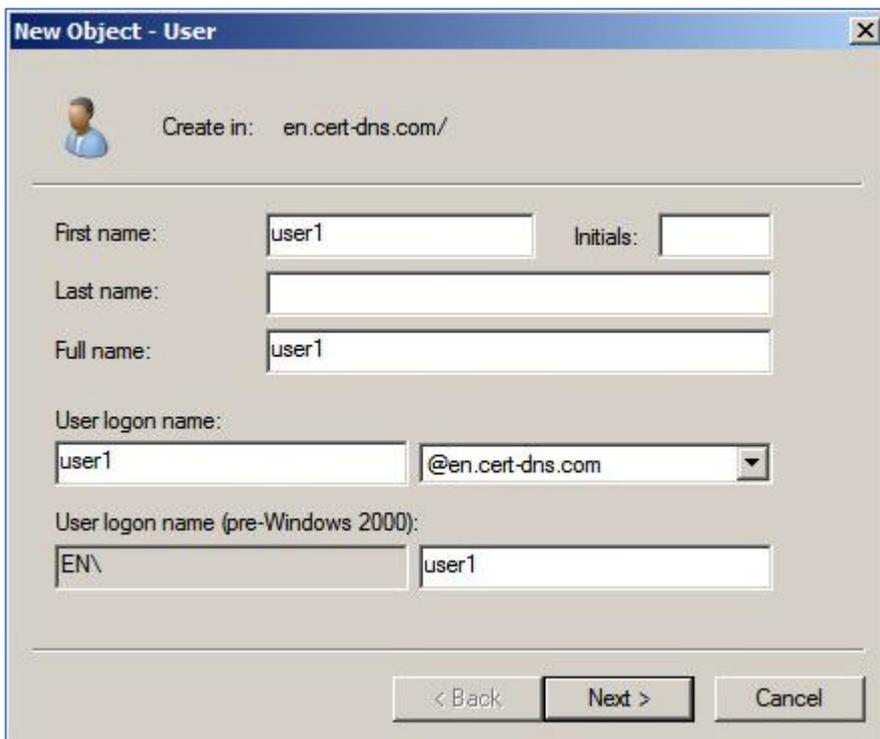


# **sslvpn\_usergroup** を右クリックし、ショートカットメニューから **New > User** を選択します。

# ユーザー **user1** を追加します(図194を参照)。

# **next** をクリックします。

図194 LDAP ユーザー **user1** の追加



# 図195に示すページで、password に **123456** と入力し、必要に応じてオプションを選択し、**Next** をクリックします。

図195 ユーザーのパスワードの設定

New Object - User

Create in: en.cert-dns.com/

Password: [password field]

Confirm password: [password field]

User must change password at next logon

User cannot change password

Password never expires

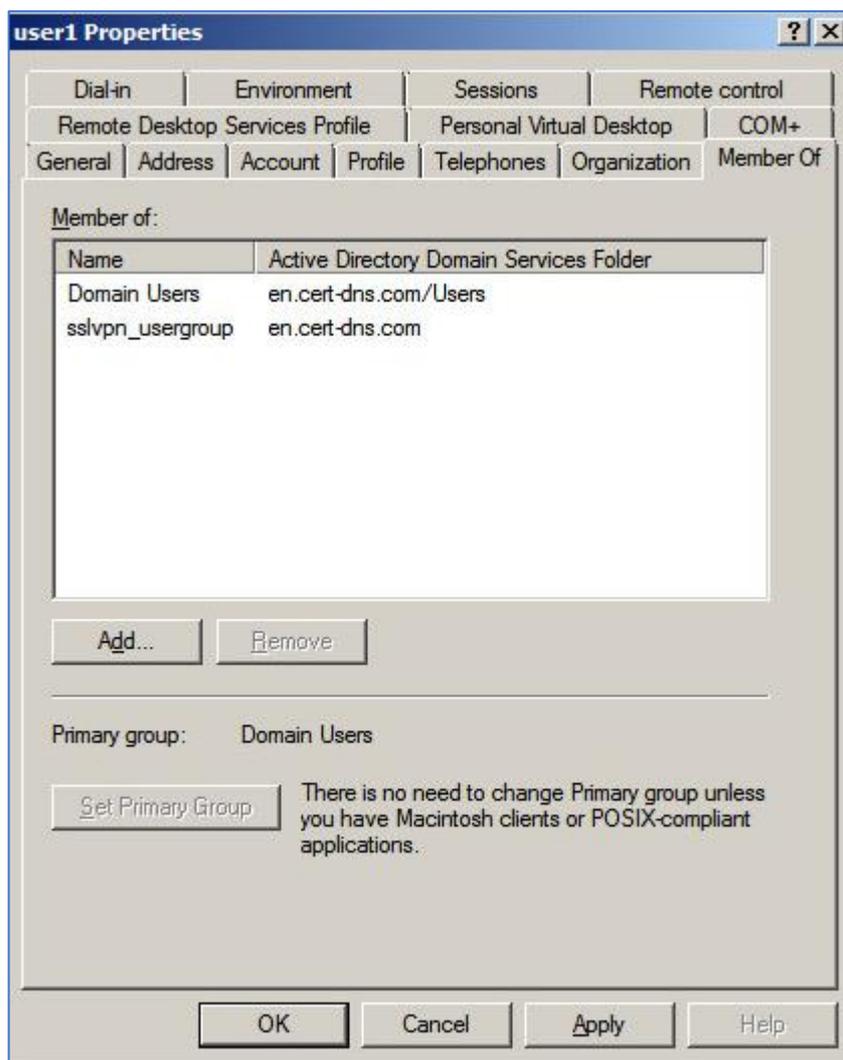
Account is disabled

< Back   Next >   Cancel

# ユーザーuser1 を右クリックし、**Properties** を選択します。

#開いたダイアログボックスで、**Member Of** タブをクリックし、ユーザーグループ **sslvpn\_usergroup** に **user1** を追加します(図196を参照)。

図196 ユーザープロパティの変更



#OK をクリックします。

## ホストの構成

1. ホストのIPアドレスとゲートウェイアドレスを設定し、SSL VPNゲートウェイおよびCAサーバーに到達できることを確認します。
2. クライアント証明書要求をCAサーバーに送信します。
  - A) ブラウザのアドレスバーに<http://192.168.100.247/certsrv>と入力します。
  - B) 図197に示す証明書サービスのホームページで、**Request a certificate**をクリックします。

図197 証明書サービスのホームページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

C) Request a Certificateページ(図198を参照)で、Advanced Certificate Requestをクリックします。

図198 証明書の要求ページ

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

**Request a Certificate**

Select the certificate type:

- [Web Browser Certificate](#)
- [E-Mail Protection Certificate](#)

Or, submit an [advanced certificate request](#).

D) クライアント証明書要求を作成します(図199を参照)。

図199 クライアント証明書要求の作成

Microsoft Active Directory Certificate Services -- en-251SERVER-CA Home

**Advanced Certificate Request**

**Identifying Information:**

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

**Type of Certificate Needed:**

Client Authentication Certificate

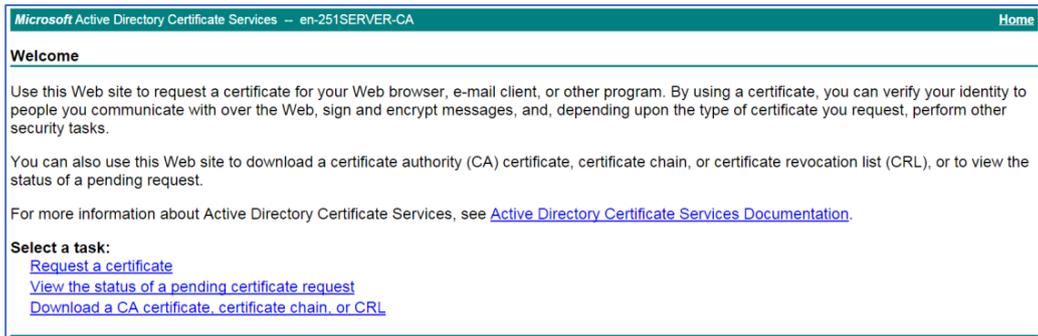
E) **Submit**をクリックします。

3. クライアント証明書をホストにインストールします。

A) 証明書要求がCA管理者によって承認されたら、ブラウザのアドレスバーに <http://192.168.100.247/certsrv> と入力します。

B) 図200に示す証明書サービスのホームページで、View the status of a pending certificate requestをクリックします。

図200 証明書サービスのホームページ



View the Status of a Pending Certificate Request ページが開きます(図201を参照)。

### 図201 Status of a Pending Certificate Request ページの表示



- C) ステータスを表示するクライアント証明書をクリックします。
- D) Certificate Issuedページ(図202を参照)で、Install this certificateをクリックしてクライアント証明書をインストールします。

### 図202 クライアント証明書のインストール



ホストに CA 証明書がない場合、に示すページが開きます。最初に CA 証明書をインストールする必要があります。

- E) この **install this CA certificate** をクリックして CA 証明書をインストールし、**Install this certificate** をクリックしてクライアント証明書をインストールします。

図203 CA 証明書とクライアント証明書のインストール



クライアント証明書をインストールすると、に示す Certificate Installed ページが開きます。

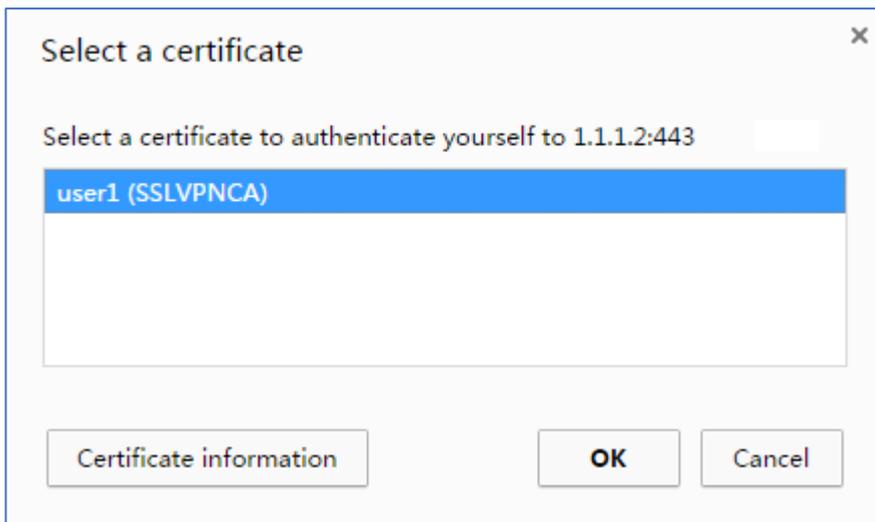
図204 Certificate Installed ページ



## 設定の確認

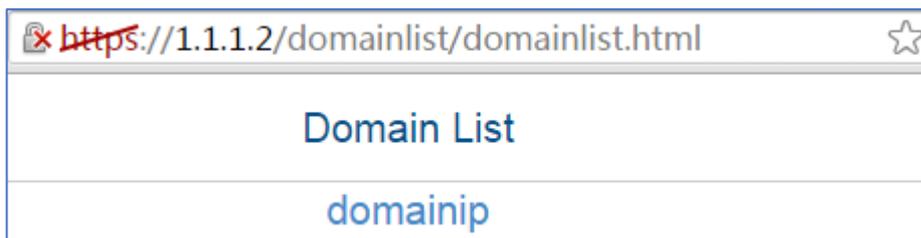
1. ホストのブラウザアドレスバーに **https://1.1.1.2** と入力し、**Enter** を押します。
2. **Select a certificate** ページで、認証用のクライアント証明書を選択します(図205を参照)。

図205 証明書の選択ページ



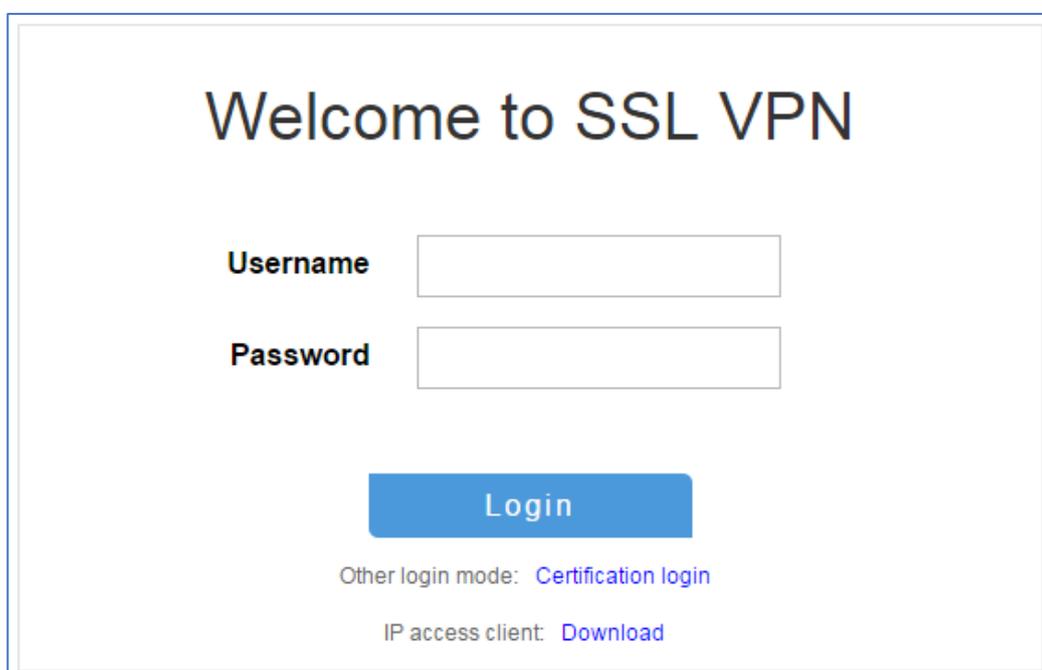
3. **OK** をクリックします。
4. 図206に示す Domain List ページで、**domainip** を選択してログインページにアクセスします。

図206 ドメインリストページ



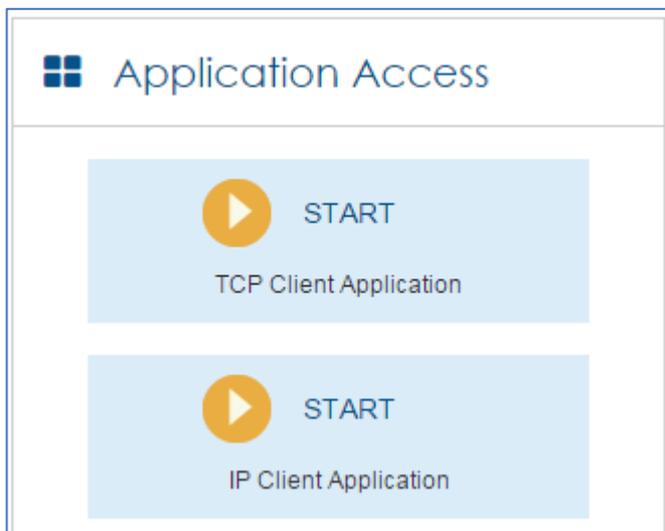
5. ログインページにアクセスするには、domainip を選択します。
6. ログインページで、username に user1 と password に 123456 を入力し、Login をクリックします。

図207 ログインページ



7. START をクリックして、IP クライアントアプリケーションを起動します(図208を参照)。

図208 IP クライアントアプリケーションの起動

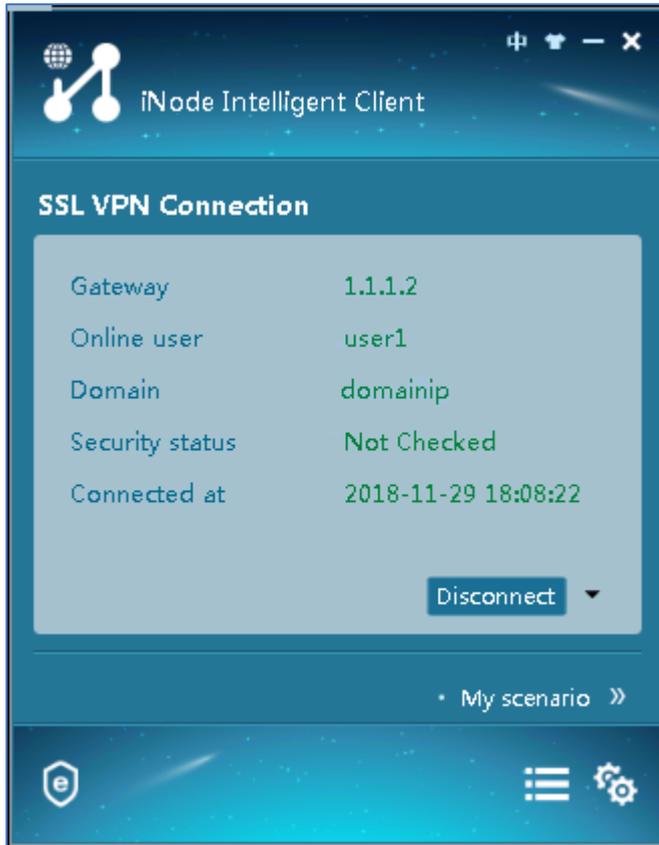


ホストに INode クライアントがインストールされていない場合、システムは INode クライアントをインストールし、INode クライアントを起動して SSL VPN ゲートウェイに接続します。

ホストにすでに INode クライアントがインストールされている場合、システムは INode クライアントを起動し、SSL VPN ゲートウェイに直接接続します。

図209に INode クライアントが SSL VPN ゲートウェイに正常に接続されたことを示します。

図209 INodeクライアントのSSL VPNゲートウェイへの接続



# 透過的 DNS プロキシの設定例

## はじめに

次に、透過的DNSプロキシの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、透過的 DNS プロキシ機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

この機能を使用するには、企業の内部ネットワークに DNS サーバーを配置しないでください。内部ネットワークに DNS サーバーを配置すると、DNS 要求はこの機能によって処理されるのではなく、DNS サーバーに転送されます。

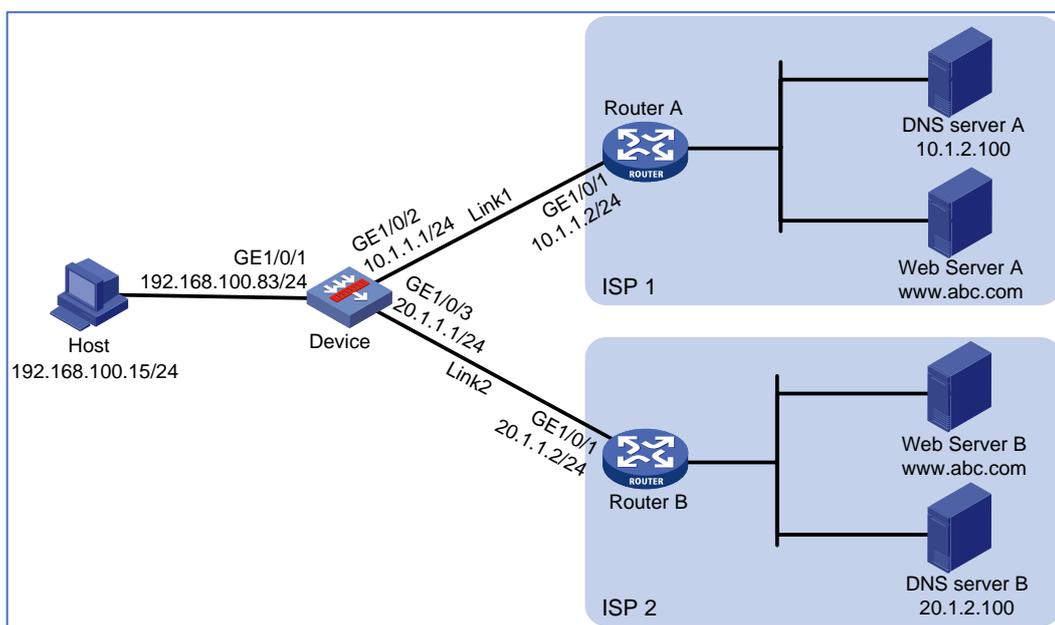
## 例:透過DNSプロキシの設定

### ネットワーク構成

図1に示すように、ISP1 と ISP2 は、同じ帯域幅を持つ 2 つのリンク(リンク 1 とリンク 2)を企業に提供します。ISP1 の DNS サーバーIP アドレスは 10.1.2.100 です。ISP2 の DNS サーバーIP アドレスは 20.1.2.100 です。イントラネットユーザーはドメイン名 `www.abc.com` を使用して Web サーバーA と Web サーバーB にアクセスします。

ユーザートラフィックをリンク 1 とリンク 2 に均等に分配するように、デバイスに透過的 DNS プロキシを設定します。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**Network** タブをクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。

B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスク長を入力します。この例では、192.168.100.83/24 と入力します。

C) **OK** をクリックします。

#GE1/0/GE1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 10.1.1.1/24 に設定します。

#Untrust セキュリティゾーンに GE1/0/3 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。

2. ゾーン **Untrust** からゾーン **Trust** へのセキュリティポリシーを作成します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。  
#**Create > Create a policy** を選択します。  
#開いたダイアログボックスで、セキュリティポリシーを設定します。
  - ソースゾーン **Untrust** を選択します。
  - ターゲットゾーンの **Trust** を選択します。
  - アクション **permit** を選択します。
  - **OK** をクリックします。
3. ICMP プローブテンプレートを設定します。  
#トップナビゲーションバーで、**Object** をクリックします。  
#ナビゲーションペインで、**Health Monitoring** をクリックします。  
#**create** をクリックします。  
#開いたダイアログボックスで、ICMP プローブテンプレートを設定します。
  - A) テンプレート名 **t1** を入力します。
  - B) **ICMP** タイプを選択します。
  - C) **Length of data to pad** フィールドに 100 と入力します。
  - D) **Probe interval** フィールドに 5000 と入力します。
  - E) **Probe timeout** フィールドに 3000 と入力します。
  - F) **OK** をクリックします。

図2 ICMP プローブテンプレートの作成

Basic configuration

Template name	<input type="text" value="t1"/>	*(1-32 chars)
Type	<input type="text" value="ICMP"/>	
Destination IP address	<input type="text"/>	(IPv4/IPv6 address)
Data to pad	<input type="text"/>	(0-200 chars)
Length of data to pad	<input type="text" value="100"/>	(20-65507)
Next hop IP address	<input type="text"/>	(IPv4/IPv6 address)
Outgoing interface	<input type="text"/>	
Probe interval <span>?</span>	<input type="text" value="5000"/>	ms(0-604800000)
Probe timeout <span>?</span>	<input type="text" value="3000"/>	ms(10-3600000)
Description	<input type="text"/>	(0-200 chars)

OK Cancel

4. リンクを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Common Configuration > Links** を選択します。

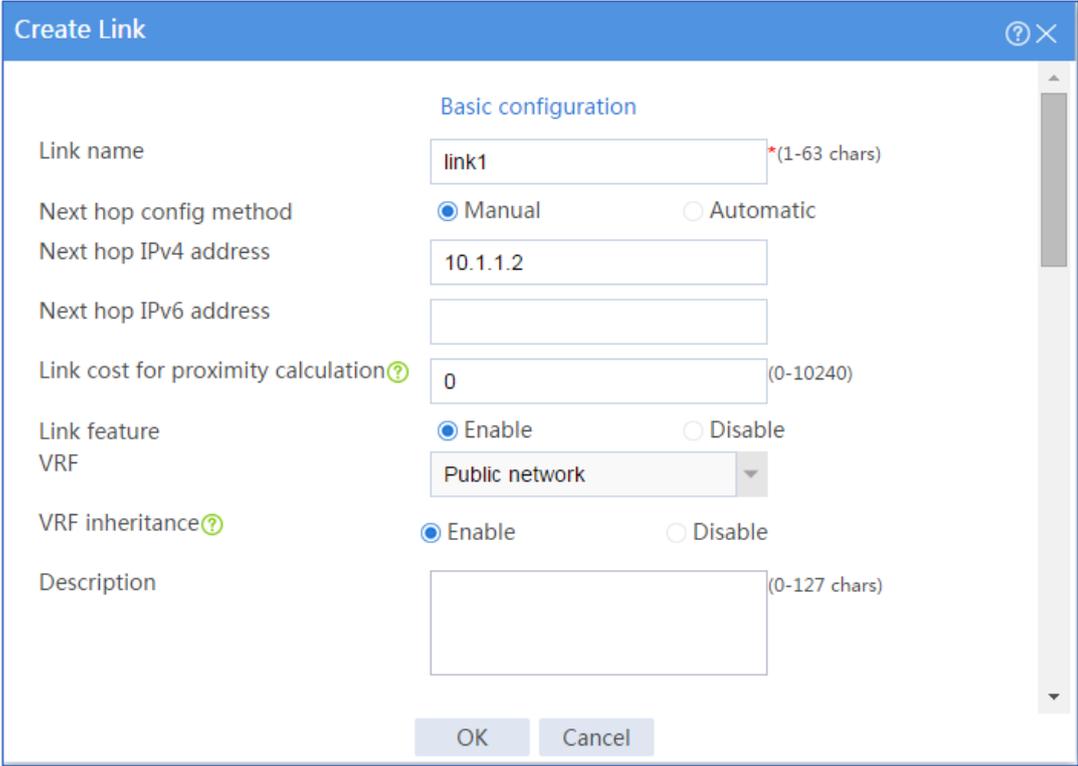
#**create** をクリックします。

#開いたダイアログボックスで、**link1** という名前のリンクを設定します。

- リンク名 **link1** を入力してください
- **Next hop config method** フィールドで **Manual** を選択します。
- ネクストホップ IPv4 アドレス 10.1.1.2 を入力します。
- 近接計算のリンクコストを 0 に設定します。

- リンク機能を有効にします。
- VRF 継承をイネーブルにします。
- OK をクリックします。

図3 リンク link1 を作成しています



The screenshot shows a 'Create Link' dialog box with the following configuration:

- Link name:** link1 (1-63 chars)
- Next hop config method:** Manual (selected), Automatic
- Next hop IPv4 address:** 10.1.1.2
- Next hop IPv6 address:** (empty)
- Link cost for proximity calculation:** 0 (0-10240)
- Link feature:** Enable (selected), Disable
- VRF:** Public network
- VRF inheritance:** Enable (selected), Disable
- Description:** (empty) (0-127 chars)

Buttons: OK, Cancel

#リンク link1 を設定するのと同じ方法でリンク link2 を設定します。

図4 リンク link2 の作成

The screenshot shows a 'Create Link' dialog box with the following fields and values:

- Link name: link2 (1-63 chars)
- Next hop config method:  Manual,  Automatic
- Next hop IPv4 address: 20.1.1.2
- Next hop IPv6 address: (empty)
- Link cost for proximity calculation: 0 (0-10240)
- Link feature:  Enable,  Disable
- VRF: Public network (dropdown)
- VRF inheritance:  Enable,  Disable
- Description: (empty) (0-127 chars)

Buttons: OK, Cancel

5. DNS サーバーを構成します。

#トップナビゲーションバーで、**Polices** をクリックします。

#ナビゲーションペインで、**Load Balancing > Link Load Balancing > DNS Proxy** を選択します。

#DNS サーバータブで、**create** をクリックします。

#開いたダイアログボックスで、**dns\_a** という名前の DNS サーバーを設定します。

- DNS サーバー名 **dns\_a** を入力します。
- **IP address config method** フィールドで **Manual** を選択します。
- IPv4 アドレス 10.1.2.100 を入力します。
- ポート番号 0 を入力します。
- weight100 と入力します。
- 優先順位 4 を入力します。
- プローブ方法 **t1** を選択します。

- 成功基準を **At least 1** に設定します。
- リンク **link1** を選択します。
- **OK** をクリックします。

図5 DNS サーバーdns\_a の作成

The screenshot shows the 'Create DNS Server' dialog box with the following configuration:

- DNS server name:** dns\_a (required, 1-63 chars)
- IP address config method:** Manual (selected)
- IPv4 address:** 10.1.2.100
- IPv6 address:** (empty)
- Port number:** 0 (0-65535)
- Weight:** 100 (1-255)
- Priority:** 4 (1-8)
- Probe method:** t1 (dropdown, [Edit] link)
- Success criteria:** At least 1 probes succeed (1-4294967295)
- Link:** link1 (dropdown, required)
- Description:** (empty text box, 0-127 chars)

Buttons: OK, Cancel

#DNS サーバーdns\_a を構成するのと同じ方法で DNS サーバーdns\_b を構成します。

図6 DNS サーバーdns\_bの作成

Create DNS Server

DNS server name  \*(1-63 chars)

IP address config method  Manual  Automatic

IPv4 address

IPv6 address

Port number  (0-65535)

Weight  (1-255)

Priority  (1-8)

Probe method  [Edit]

Success criteria   probes succeed(1-4294967295)

Link  \*

Description  (0-127 chars)

OK Cancel

6. DNS サーバープールを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Link Load Balancing > DNS Proxy** を選択します。

#DNS サーバープールタブで、**create** をクリックします。

#開いたダイアログボックスで、**dsp** という名前の DNS サーバープールを設定します。

- DNS サーバープール名 **dsp** を入力します。
- スケジュールアルゴリズム **Round robin** を選択します。
- 成功基準を **At least 1** に設定します。

- DNS サーバー `dns_a` および `dns_b` を DNS サーバープールに追加します。
- **OK** をクリックします。

図7 DNS サーバープール dsp の作成

The screenshot shows the 'Create DNS Server Pool' dialog box with the following configuration:

- Pool name:** dsp (1-63 chars)
- Scheduling algorithm:** Round robin
- Priority:**  Limit the number of DNS servers to be scheduled
- Minimum number:** (1-1000)
- Maximum number:** (1-1000)
- Probe method:** Select a probe method (Edit)
- Success criteria:** At least 1 probes succeed (1-4294967295)
- DNS server list:**

<input type="checkbox"/>	Na...	Sta...	IPv4 ...	IPv6 ...	Por...	Edit
<input type="checkbox"/>	dns...		10.1...		0	
<input type="checkbox"/>	dns...		20.1...		0	
- Description:** (0-127 chars)

Buttons: OK, Cancel

7. IPv4 ルーティングポリシーを設定します。

#トップナビゲーションバーで、**Polices** をクリックします。

#ナビゲーションペインで、**Load Balancing > Link Load Balancing > DNS Proxy** を選択します。

#**IPv4 Routing Policy** タブの **Common configuration** 領域で、Transparent DNS proxy オプションを選択し、**Apply** をクリックします。

図8 共通の構成

The screenshot shows a configuration window with tabs for 'Class', 'DNS Server Pool', 'DNS Server', 'IPv4 Proxy Policy', and 'IPv6 Proxy Policy'. The 'IPv4 Proxy Policy' tab is active, displaying a 'Common Configuration' section. This section contains several settings: 'Status' is checked with a green checkmark; 'Transparent DNS proxy' is checked with a blue checkmark; 'Session extension information' is unchecked; 'Proxy port' is set to '53' with a red asterisk and '(1-65535)' next to it; 'Link protection' is unchecked; and 'Sticky entry synchronization' is unchecked. An 'Apply' button is located at the bottom left of the configuration area.

#IPv4 Routing Policy タブの Policy 領域で、Default という名前のデフォルト IPv4 ルーティングポリシーの Edit アイコンをクリックします。

#開いたダイアログボックスで、デフォルトの IPv4 ルーティングポリシーを設定します。

- 転送モード **Load balance** を選択します。
- DNS server pool **dsp** を選択します。
- **OK** をクリックします。

図9 デフォルト IPv4 ルーティングポリシーの編集

The screenshot shows the 'Edit Policy' dialog box with a blue header and a close button. The 'Class' is set to 'Default'. The 'Forwarding mode' is a dropdown menu set to 'Load balance' with a red asterisk. The 'ToS' is a text input field with '(0-255)' to its right. The 'DNS server pool' is a dropdown menu set to 'dsp' with a red asterisk. The 'Sticky group' is a dropdown menu. At the bottom, there are 'OK' and 'Cancel' buttons.

# 設定の確認

ホスト上のブラウザから <http://www.abc.com> にアクセスし、デバイスが DNS サーバー dns\_a および dns\_b に DNS 要求を配布していることを確認します。

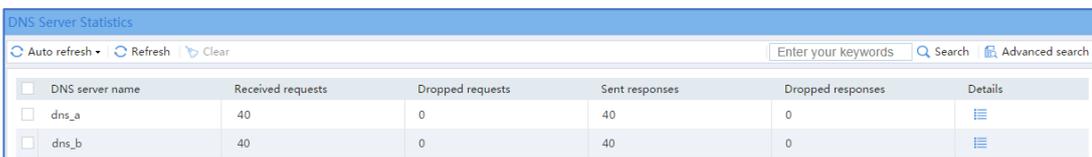
1. **DNS Server Statistics** ページを表示します。

#トップナビゲーションバーで、モニタータブをクリックします。

#ナビゲーションペインで、Statistics>DNS Proxy Statistics>DNS Servers を選択します。

DNS Server Statistics ページは次のとおりです。

図10 DNS サーバー統計



<input type="checkbox"/>	DNS server name	Received requests	Dropped requests	Sent responses	Dropped responses	Details
<input type="checkbox"/>	dns_a	40	0	40	0	
<input type="checkbox"/>	dns_b	40	0	40	0	

2. **DNS Server Pool Statistics** ページを表示します。

#ナビゲーションペインで、Statistics > DNS Proxy Statistics > DNS Server Pools を選択します。

DNS Server Pool Statistics ページは次のとおりです。

図11 DNS サーバープール統計



<input type="checkbox"/>	DNS server pool statistics	Slot number	Received requests	Dropped requests	Sent responses	Dropped responses	Details
<input type="checkbox"/>	dsp	1	80	0	80	0	

# コンテキストの設定例

## はじめに

次に、コンテキストコンフィギュレーションの例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、コンテキスト機能の基本的な知識があることを前提としています。

## 制限事項とガイドライン

コンテキストに VLAN を割り当てる場合は、次の制限事項およびガイドラインに従ってください。

- VLAN-unshared 属性のないコンテキストに対しては、VLAN を割り当てるだけで、**vlan** コマンドを使用して VLAN を作成することはできません。割り当ての前に、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。
- VLAN-unshared、VLAN-unshared の VLAN を割り当てることはできません。
  - VLAN1
  - インターフェイスのデフォルト VLAN。
  - VLAN インターフェイスを作成した VLAN。

インターフェイスをコンテキストに割り当てる場合は、次の制限事項およびガイドラインに従ってください。

- サブインターフェイス、VLAN インターフェイス、および集約インターフェイスは、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。
- コンテキストにサブインターフェイスを割り当てた後、そのプライマリインターフェイスをコンテキストに割り当てることはできません。コンテキストにプライマリインターフェイスを割り当てた後、そのサブインターフェイスをコンテキストに割り当てることはできません。

- 共有モードのコンテキストには、集約インターフェイスのメンバーインターフェイスを割り当てないでください。
- インターフェイスを共有モードのコンテキストに割り当てた後、インターフェイスを再生成する前に、インターフェイスを排他モードのコンテキストに割り当ててはできません。
- IRF 物理インターフェイ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。
- レイヤ3 インターフェイスのサブインターフェイスが Reth インターフェイスのメンバーインターフェイスである場合は、レイヤ3 インターフェイ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。

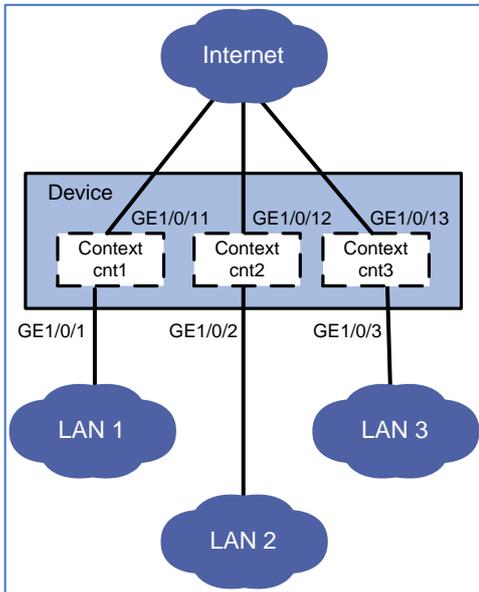
## 例:コンテキストの設定

### ネットワーク構成

図1に示すように、LAN のコンテキストを次のように設定します。

- コンテキスト **cnt1** を LAN1 用にします。コンテキストに 60%のディスク領域と 60%のメモリ領域を割り当て、CPU の重みを 8 に設定します。
- コンテキスト **cnt2** を LAN2 用に構成します。デフォルトのディスクスペース量とデフォルトのメモリースペース量を使用するようにコンテキストを残します。
- LAN3 にコンテキスト **cnt3** を設定します。CPU の重みを 2 に設定します。
- GigabitEthernet1/0/1 および GigabitEthernet1/0/11 をコンテキスト **cnt1** に割り当てます。GigabitEthernet1/0/2 および GigabitEthernet1/0/12 をコンテキスト **cnt2** に割り当てます。GigabitEthernet1/0/3 および GigabitEthernet1/0/13 をコンテキスト **cnt3** に割り当てます。

図1 ネットワーク図



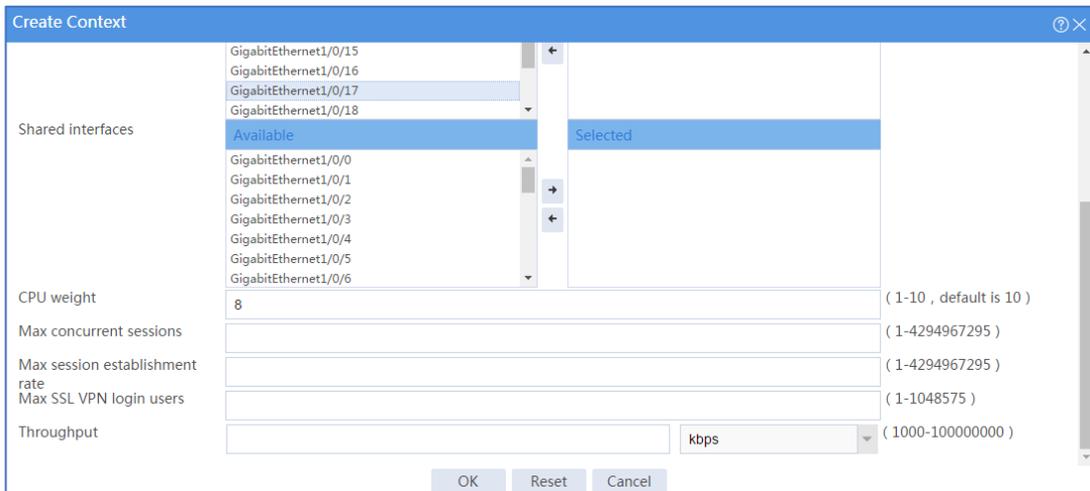
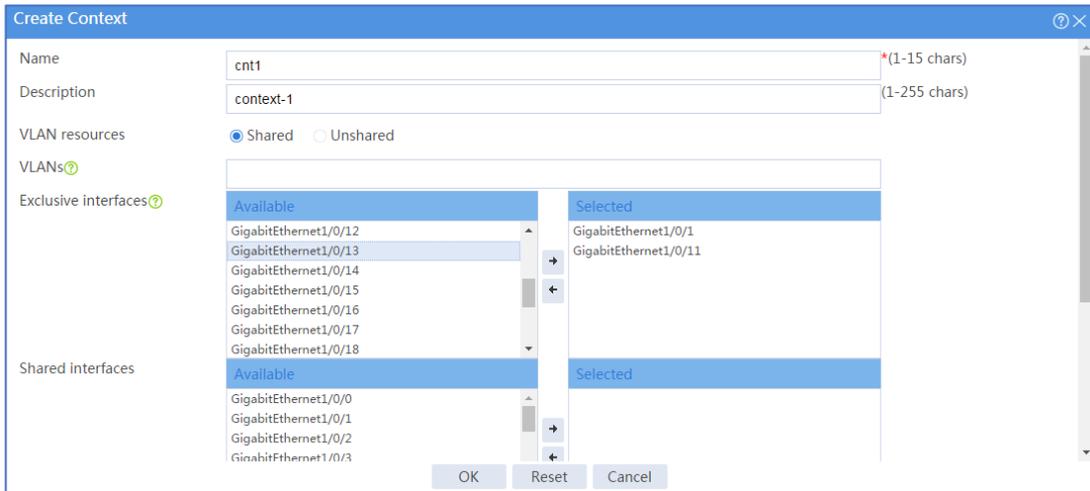
## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの Ess9345 で作成および確認されています。

## 手順

1. コンテキストcnt1を設定します。
  - #トップナビゲーションバーで、**system** をクリックします。
  - #ナビゲーションペインで、**Virtualization > Contexts > Contexts** を選択します。
  - #**create** をクリックします。
  - #コンテキスト cnt1 を設定します(図2を参照)。
  - #**OK** をクリックします。

図2 コンテキストの作成



#コンテキストリストからコンテキスト cnt1 を選択し、**Start** をクリックします。

図3 開始コンテキストcnt1



#ナビゲーションペインで、**Virtualization > Contexts > Resource Allocation** を選択します。

#コンテキスト **cnt1** をクリックし、コンテキストのリソース割り当てスキームを編集します(図4を参照)。

#**OK** をクリックします。

図4 リソース割り当てスキームの編集

Context: cnt1

Memory usage (%): 60 (1-100)%

Maximum disk space usage (%): 60 (1-100)%

Buttons: OK, Cancel

2. コンテキストcnt2とcnt3は、コンテキストcnt1と同じ方法で設定します。

## 設定の確認

1. 上部のナビゲーションバーで、**system**をクリックします。
2. ナビゲーションペインで、**Virtualization > Contexts > Contexts**を選択します。
3. コンテキストがリストされ、その設定が設定されていることを確認します。

図5 コンテキストの表示

Context	Status	VLANs	Numb...	Number of e...	Exclusive int...	Number of s...	Shared interf...	CPU w...	Max c...	Max s...	Max S...	Throughput	Description	Edit
<input type="checkbox"/> cnt1	Started	Shared	2	Exclusive interf...	GigabitEtherne GigabitEtherne			8					context-1	
<input type="checkbox"/> cn2	Started	Shared	2	Exclusive interf...	GigabitEtherne GigabitEtherne			10					context-2	
<input type="checkbox"/> cn3	Started	Shared	2	Exclusive interf...	GigabitEtherne GigabitEtherne			2					context-3	

4. ナビゲーションペインで、**Virtualization>Contexts>Resource Allocation**を選択して、コンテキストに割り当てられているメモリおよびディスクリソースの量を表示します。

図6 コンテキストリソース割り当ての表示

Engine	Number of contexts	Contexts	Total memory	Total disk space
<input type="checkbox"/> Slot1	3	cnt1 cnt2 cnt3	19680192KB 32800316KB 32800316KB	2453084KB 4088468KB 4088468KB

5. ナビゲーションペインで、**Virtualization > Contexts > Resource Usage**を選択して、コンテキストのリソース使用状況を表示します。

図7 コンテキストのリソース使用状況の表示

The screenshot shows a web-based interface for monitoring resource usage. At the top, there is a blue header with the text 'View Resource Usage' and a 'Refresh' button. Below the header is a table with the following columns: 'Name', 'CPU', 'Memory', and 'De...'. The table lists several contexts: 'Slot1', 'Admin', 'cnt1', 'cn2', and 'cn3'. Each context has a corresponding CPU and Memory usage bar chart and a percentage value. 'Slot1' is selected, indicated by a blue circle next to its name. The 'De...' column contains menu icons for each row.

Name	CPU	Memory	De...
Slot1	1%	16%	☰
Admin	4%	1%	☰
cnt1	0%	0%	☰
cn2	0%	0%	☰
cn3	0%	0%	☰

# IRF 設定例

## はじめに

次に、IRFの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

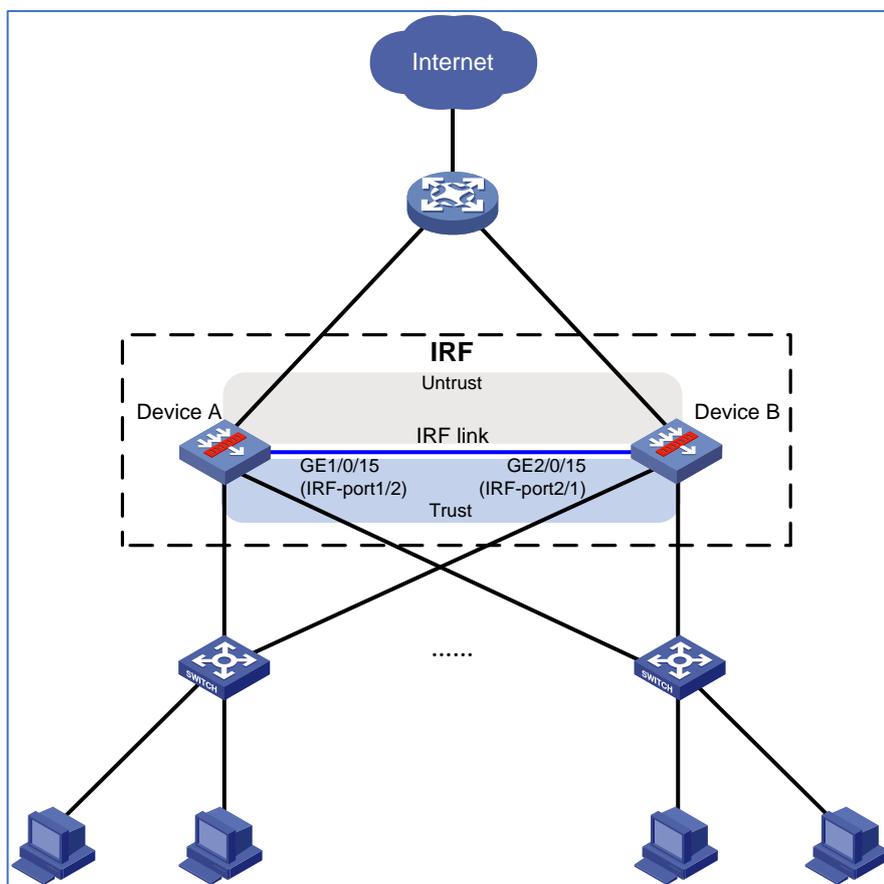
次の情報は、IRF 機能に関する基本的な知識があることを前提としています。

## 例:IRFファブリックの設定

### ネットワーク構成

図1に示すように、デバイス A とデバイス B を使用して IRF ファブリックを設定します。デバイス A にデバイス B より高いプライオリティを割り当て、デバイス A をマスターデバイスにできるようにします。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

### デバイス A の設定

#トップナビゲーションバーで、システムをクリックします。

#ナビゲーションペインで、Virtualization > IRF を選択します。

#IRF-port2 の設定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、IRF パラメータを設定します(図2を参照)。

図2デバイス A での IRF の設定

Configure IRF

Domain ID 0 (0-4294967295)

Member ID 1 \*(1-2)

Priority 32 (1-32)

IRF bridge MAC persistence  6 minutes  Always  Not retain

IRF software auto-update

Description (1-127 chars)

IRF port 2 (1-2)

IRF physical interfaces GigabitEthernet1/0/15 +

OK Cancel

#OK をクリックします。

### デバイス B の設定

#トップナビゲーションバーで、システムをクリックします。

#ナビゲーションペインで、Virtualization > IRF を選択します。

#IRF-port1 の設定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、IRF パラメータを設定します(図3を参照)。

図3 デバイス B での IRF の設定

Configure IRF

Domain ID: 0 (0-4294967295)

Member ID: 2 \*(1-2)

Priority: 1 (1-32)

IRF bridge MAC persistence:  6 minutes  Always  Not retain

IRF software auto-update:

Description: (1-127 chars)

IRF port: 1 (1-2)

IRF physical interfaces: GigabitEthernet1/0/15

OK Cancel

#OK をクリックします。

デバイス B は自動的にリブートして、デバイス A と IRF ファブリックを形成します。

## 設定の確認

#マスター(デバイス A)の管理アドレスを使用して、IRF ファブリックの Web インターフェイスにログインします。

#トップナビゲーションバーで、システムをクリックします。

#ナビゲーションペインで、Virtualization > IRF を選択します。

#デバイス A およびデバイス B が IRF メンバーデバイスであり、それらの IRF ポートが動作していることを確認します。

図4 IRF 情報

Member ID	IRF port	IRF physical interfaces	IRF port status	Settings
1	1		Disabled	⚙️
1	2	GigabitEthernet1/0/15	Up	⚙️
2	1	GigabitEthernet2/0/15	Up	⚙️
2	2		Disabled	⚙️

# ホットバックアップの設定例

## はじめに

次に、ホットバックアップの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、IRF、RBM、VRRP、冗長グループ、およびトラック機能に関する基本的な知識があることを前提としています。

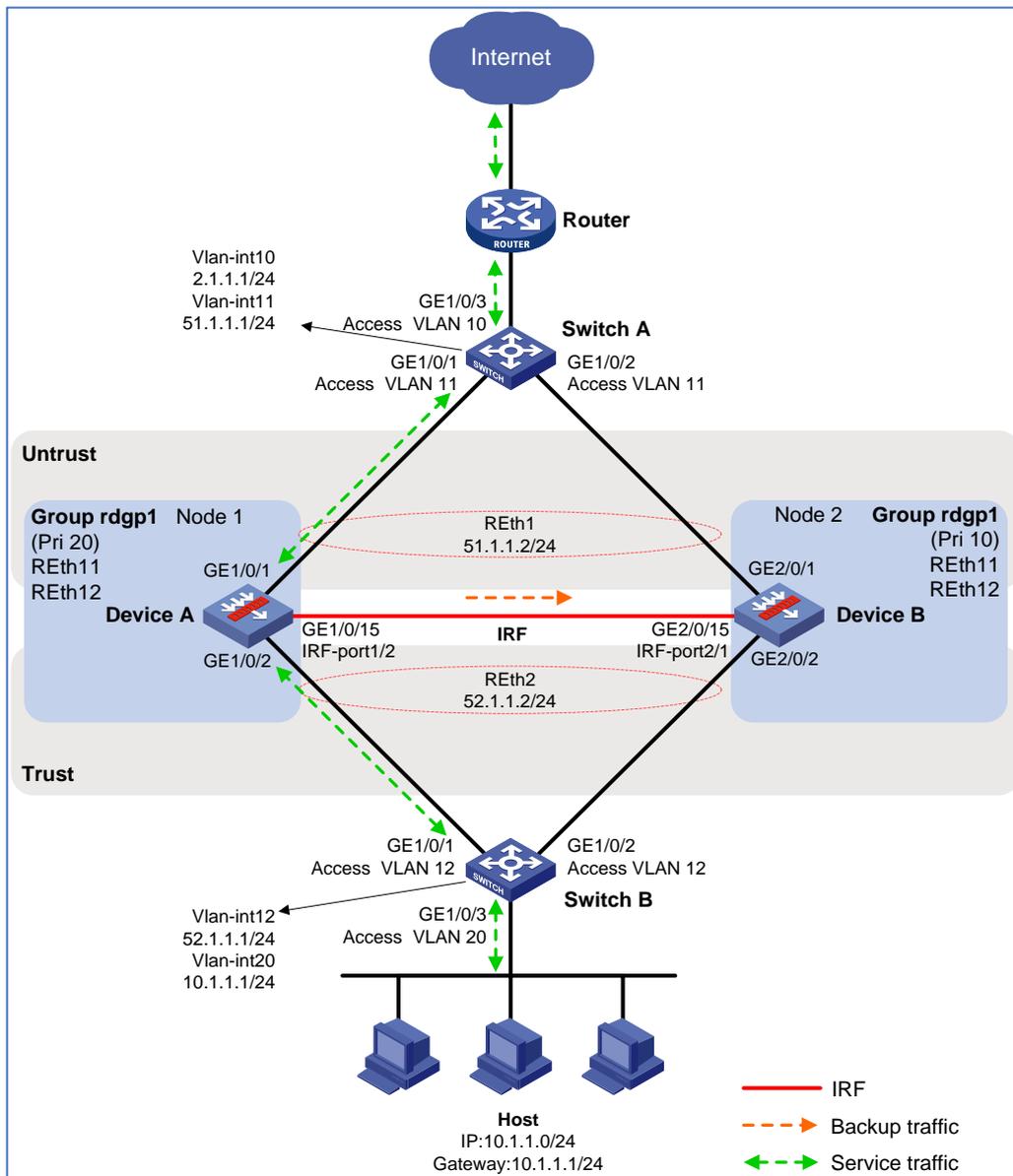
## 例:1つの冗長グループによるアクティブ/スタンバイモードでのIRFホットバックアップシステムの設定

### ネットワーク構成

図1に示すように、サービスの継続性を確保するために、インターネットと企業の内部ネットワークの境界にIRFホットバックアップシステムをセットアップします。0

- アクティブ/スタンバイモードで動作するようにホットバックアップシステムを設定します。
- デバイス A をプライマリデバイスとして設定し、デバイス B をセカンダリデバイスとして設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 前提条件

IRFホットバックアップを設定する前に、IRFホットバックアップシステムのメンバーデバイスで、次のハードウェアおよびソフトウェア設定が同じであることを確認してください。

- デバイスモデル
- ソフトウェアバージョン
- サービスモジュールの場所、数、およびタイプ
- インターフェイスモジュールの場所、数、およびタイプ

## 手順

### デバイス A およびデバイス B の設定

#### IRF の設定

##### 1. デバイスAの構成:

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**Virtualization > IRF** を選択します。

#デバイス A を設定します(図2を参照)。

#OK をクリックします。

#### 図2 デバイスAのIRF設定

The screenshot shows the 'Configure IRF' dialog box with the following settings:

- Domain ID: 0 (range: 0-4294967295)
- Member ID: 1 (range: \*(1-2))
- Priority: 32 (range: (1-32))
- IRF bridge MAC persistence:  6 minutes,  Always,  Not retain
- IRF software auto-update:
- Description: (1-127 chars)
- IRF port: 2 (range: (1-2))
- IRF physical interfaces: GigabitEthernet1/0/15

Buttons: OK, Cancel

## 2. デバイスBの設定:

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**Virtualization > IRF** を選択します。

#デバイス B を設定します(図3を参照)。

#**OK** をクリックします。

デバイス B は自動的にリポートして、デバイス A と IRF ファブリックを形成します。

図3 デバイスBのIRF設定

Configure IRF

Domain ID	0	(0-4294967295)
Member ID ?	2	* (1-2)
Priority ?	1	(1-32)
IRF bridge MAC persistence	<input checked="" type="radio"/> 6 minutes	<input type="radio"/> Always <input type="radio"/> Not retain
IRF software auto-update	<input checked="" type="checkbox"/>	
Description		(1-127 chars)
IRF port ?	1	(1-2)
IRF physical interfaces ?	GigabitEthernet2/0/15	X
		+

OK Cancel

## ホットバックアップの構成

#トップナビゲーションバーで、**System** 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。

#IRF ホットバックアップを設定します(図4を参照)。

図4 IRF ホットバックアップの設定

IRF hot backup

Operating mode ?  Active/standby  Dual-active

Session state machine mode ?  Strict  Loose  Compact

Backup

Back up NAT444 port blocks

Back up sessions

Back up DNS

Back up HTTP

Back up IPsec SAs

#他のパラメータのデフォルト設定を使用します。

#**Apply** をクリックします。

#**Redundancy Group** をクリックします。

図5 冗長グループコンフィギュレーション

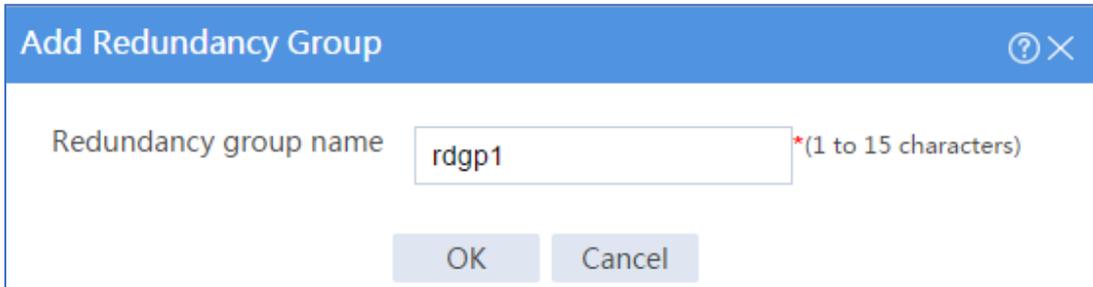
Redundancy Group

Redundancy group

#**create** をクリックします。

#表示されるダイアログボックスで、冗長グループ **rdgp1** を設定します(図6を参照)。

図6 冗長グループの作成



Add Redundancy Group

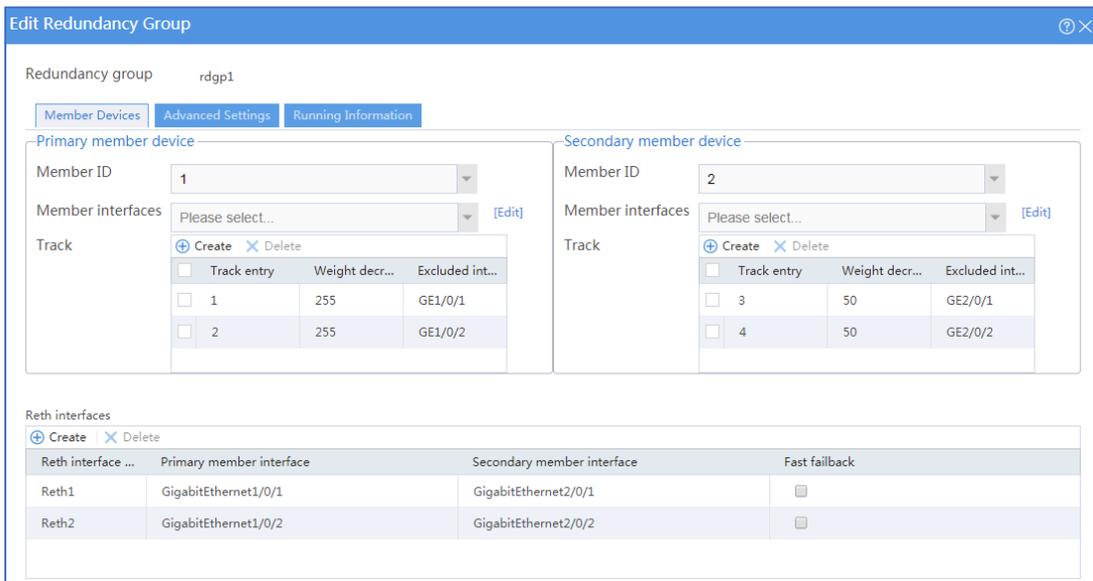
Redundancy group name  \*(1 to 15 characters)

OK Cancel

#OK をクリックします。

#冗長グループを設定します(図7を参照)。

図7 冗長グループの設定



Edit Redundancy Group

Redundancy group rdgp1

Member Devices Advanced Settings Running Information

Primary member device

Member ID 1

Member interfaces Please select... [Edit]

Track

Track entry	Weight decr...	Excluded int...
<input type="checkbox"/> 1	255	GE1/0/1
<input type="checkbox"/> 2	255	GE1/0/2

Secondary member device

Member ID 2

Member interfaces Please select... [Edit]

Track

Track entry	Weight decr...	Excluded int...
<input type="checkbox"/> 3	50	GE2/0/1
<input type="checkbox"/> 4	50	GE2/0/2

Reth interfaces

Reth interface ...	Primary member interface	Secondary member interface	Fast fallback
Reth1	GigabitEthernet1/0/1	GigabitEthernet2/0/1	<input type="checkbox"/>
Reth2	GigabitEthernet1/0/2	GigabitEthernet2/0/2	<input type="checkbox"/>

#OK をクリックします。

#インターフェイスに IP アドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。

#Reth1 をセキュリティゾーン **Untrust** に割り当て、Reth2 をセキュリティゾーン **Trust** に割り当てます(詳細は省略)。

## スイッチ A の設定

この例では、簡単な設定手順のみを示しています。

1. VLAN10およびVLAN11を作成します。
2. GigabitEthernet1/0/1およびGigabitEthernet1/0/2をレイヤー2モードで動作するように設定し、これらをアクセスインターフェイスとしてVLAN11に割り当てます。
3. GigabitEthernet1/0/3をレイヤー2モードで動作するように設定し、アクセスインターフェイスとしてVLAN10に割り当てます。
4. VLAN-interface11およびVLAN-interface10にそれぞれ51.1.1.1/24および2.1.1.1/24を割り当てます。
5. 内部ネットワークへのルートのネクストホップとして51.1.1.2(Reth1のIPアドレス)を指定し、インターネットへのルートのネクストホップとして2.1.1.2(ルーター上のIPアドレス)を指定します。

## スイッチ B の設定

この例では、簡単な設定手順のみを示しています。

1. VLAN12およびVLAN20を作成します。
2. GigabitEthernet1/0/1およびGigabitEthernet1/0/2をレイヤー2モードで動作するように設定し、これらをアクセスインターフェイスとしてVLAN12に割り当てます。
3. GigabitEthernet1/0/3をレイヤー2モードで動作するように設定し、アクセスインターフェイスとしてVLAN20に割り当てます。
4. VLAN-interface12およびVLAN-interface20にそれぞれ52.1.1.1/24および10.1.1.1/24を割り当てます。
5. インターネットへのルートのネクストホップとして52.1.1.2(Reth2のIPアドレス)を指定します。

## ホストの構成

#ホストで、デフォルトゲートウェイとして10.1.1.1(スイッチBのVLANインターフェイス20のIPアドレス)を指定します。

# 設定の確認

デバイスAまたはデバイスBの設定を確認します。

1. 上部のナビゲーションバーで、**System** をクリックします。
2. ナビゲーションペインで、**High Availability > Hot Backup** を選択します。
3. 冗長グループ **rdgp1** の編集アイコンをクリックします。
4. **Running Information** をクリックします。

図8 デバイス A が正常に動作している場合の冗長グループ情報

The screenshot shows the 'Edit Redundancy Group' window for 'rdgp1'. It has three tabs: 'Member Devices', 'Advanced Settings', and 'Running Information'. The 'Running Information' tab is active, showing a 'Refresh' button and a summary box with the following details:

Redundancy group	rdgp1
Remaining preemption delay time	0(sec)
Remaining hold-down time	0(sec)

Below this is a table for 'Redundancy group' members:

Member devices	Status	Weight
1	Primary	255
2	Secondary	255

Next is a 'Track' table:

Member devices	Track entry	Status	Excluded interface
1	1	Active	GigabitEthernet1/0/1
	2	Active	GigabitEthernet1/0/2
2	3	Active	GigabitEthernet2/0/1
	4	Active	GigabitEthernet2/0/2

Finally, there is a 'Reth interface' table:

Name	Member interfaces	Member interface forwarding status	Member interface presence status
Reth1	GigabitEthernet1/0/1	Active	Present
	GigabitEthernet2/0/1	Inactive	Present
Reth2	GigabitEthernet1/0/2	Active	Present
	GigabitEthernet2/0/2	Inactive	Present

At the bottom of the window are 'OK' and 'Cancel' buttons.

5. デバイス A の GE1/0/1 をシャットダウンし、冗長グループでスイッチオーバーが発生することを確認します(図9を参照)。

図9 デバイス A に障害が発生した場合の冗長グループ情報

Redundancy group rdgp1

Member Devices | **Advanced Settings** | Running Information

Refresh

Redundancy group rdgp1  
 Remaining preemption delay time 0(sec)  
 Remaining hold-down time 0(sec)

Redundancy group

Member devices	Status	Weight
1	Secondary	-255
2	Primary	255

Track

Member devices	Track entry	Status	Excluded interface
1	1	Inactive	GigabitEthernet1/0/1(Failure)
	2	Inactive	GigabitEthernet1/0/2
2	3	Active	GigabitEthernet2/0/1
	4	Active	GigabitEthernet2/0/2

Reth interface

Name	Member interfaces	Member interface forwarding status	Member interface presence status
Reth1	GigabitEthernet1/0/1	Inactive	Present
	GigabitEthernet2/0/1	Active	Present
Reth2	GigabitEthernet1/0/2	Inactive	Present
	GigabitEthernet2/0/2	Active	Present

OK Cancel

6. デバイス A で GE1/0/1 を起動し、トラフィックが 60 秒以内にデバイス A に切り替わることを確認します(図10を参照)。

図10 スイッチオーバー後の冗長グループ情報

Redundancy group rdgp1

Member Devices | **Advanced Settings** | Running Information

Refresh

Redundancy group rdgp1

Remaining preemption delay time 0(sec)

Remaining hold-down time 0(sec)

Redundancy group

Member devices	Status	Weight
1	Primary	255
2	Secondary	255

Track

Member devices	Track entry	Status	Excluded interface
1	1	Active	GigabitEthernet1/0/1
	2	Active	GigabitEthernet1/0/2
2	3	Active	GigabitEthernet2/0/1
	4	Active	GigabitEthernet2/0/2

Reth interface

Name	Member interfaces	Member interface forwarding status	Member interface presence status
Reth1	GigabitEthernet1/0/1	Active	Present
	GigabitEthernet2/0/1	Inactive	Present
Reth2	GigabitEthernet1/0/2	Active	Present
	GigabitEthernet2/0/2	Inactive	Present

OK Cancel

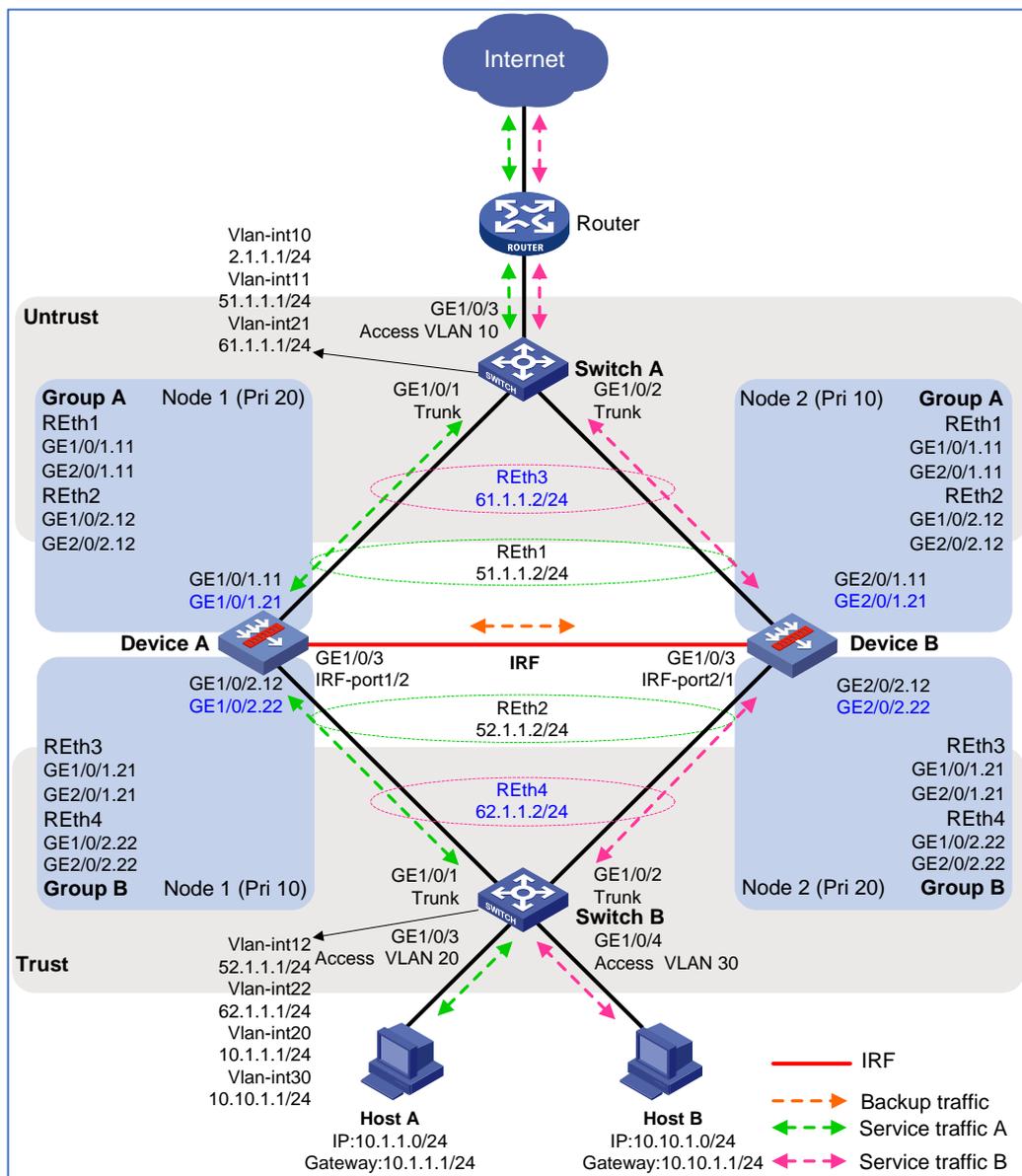
例:2つの冗長グループがあるデュアルアクティブモードでのIRFホットバックアップシステムの設定

## ネットワーク構成

図1に示すように、サービスの継続性を確保するために、インターネットと企業の内部ネットワークの境界にIRFホットバックアップシステムをセットアップします。

- ホットバックアップシステムをデュアルアクティブモードで動作するように設定します。
- ホストAとホストBのトラフィックをそれぞれ処理するように、デバイスAとデバイスBを設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 前提条件

IRFホットバックアップを設定する前に、IRFホットバックアップシステムのメンバーデバイスで、次のハードウェアおよびソフトウェア設定が同じであることを確認してください。

- デバイスマデル

- ソフトウェアバージョン
- サービスモジュールの場所、数、およびタイプ
- インターフェイスモジュールの場所、数、およびタイプ

## 手順

### デバイス A およびデバイス B の設定

#### IRF の設定

“例:1 つの冗長グループによるアクティブ/スタンバイモードでの IRF ホットバックアップシステムの設定”の説明に従って IRF を設定します。

#### レイヤー3 イーサネットサブインターフェイスの設定

1. 最も外側の VLAN ID11 のパケットを終端するように GE1/0/1.11 を設定します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
#**Create Interface** をクリックし、次のようにサブインターフェイスを設定します。
  - ◇ **Type** を **Physical subinterface** に設定します。
  - ◇ メインインターフェイスとして GE1/0/1 を選択します。
  - ◇ インターフェイス番号を 11 に設定します。
2. ネットワークダイアグラム内の他のレイヤー3イーサネットサブインターフェイスを、GE1/0/1.11 と同じ方法で設定します(詳細は省略)。

#### ホットバックアップの構成

#トップナビゲーションバーで、システムをクリックします。  
#ナビゲーションペインで、High Availability > Hot Backup を選択します。  
#IRF ホットバックアップを設定します(図 12 を参照)。

#### 図12 IRF ホットバックアップの設定

IRF hot backup

Operating mode ?  Active/standby  Dual-active

Session creation mode  Local-based ?  Hash-based ?

Transparent transmission for UDP packets ?  Enable  Disable

Session state machine mode ?  Strict  Loose  Compact

Backup

Back up NAT444 port blocks

Back up sessions

Back up DNS

Back up HTTP

Back up IPsec SAs

#他のパラメータのデフォルト設定を使用します。

#**Apply** をクリックします。

#**Redundancy Group** をクリックします。

図13 冗長グループコンフィギュレーション

Redundancy Group

Redundancy group

#**create** をクリックします。

#表示されるダイアログボックスで、冗長グループ **a** を作成します(図14を参照)。

図 14 冗長グループ a の作成

Add Redundancy Group

Redundancy group name  \*(1 to 15 characters)

OK Cancel

#OK をクリックします。

#冗長グループを設定します(図15を参照)。

図 15 冗長グループ a の設定

Edit Redundancy Group

Redundancy group a

Member Devices Advanced Settings Running Information

Primary member device

Member ID 1

Member interfaces Please select... [Edit]

Track

<input type="checkbox"/>	Track entry	Weight decr...	Excluded int...
<input type="checkbox"/>	1	255	GE1/0/1.11
<input type="checkbox"/>	3	255	GE1/0/2.12

Secondary member device

Member ID 2

Member interfaces Please select... [Edit]

Track

<input type="checkbox"/>	Track entry	Weight decr...	Excluded int...
<input type="checkbox"/>	5	50	GE2/0/1.11
<input type="checkbox"/>	7	50	GE2/0/2.12

Reth interfaces

Reth interface ...	Primary member interface	Secondary member interface	Fast fallback
Reth1	GigabitEthernet1/0/1.11	GigabitEthernet2/0/1.11	<input type="checkbox"/>
Reth2	GigabitEthernet1/0/2.12	GigabitEthernet2/0/2.12	<input type="checkbox"/>

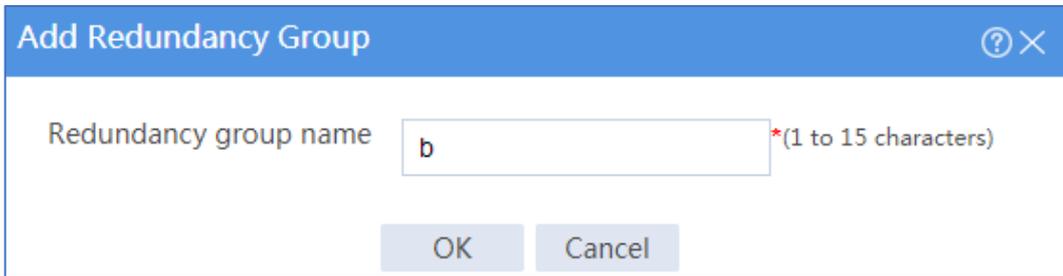
OK Cancel

#OK をクリックします。

#create をクリックします。

#表示されるダイアログボックスで、冗長グループ b を作成します(図 16 を参照)。

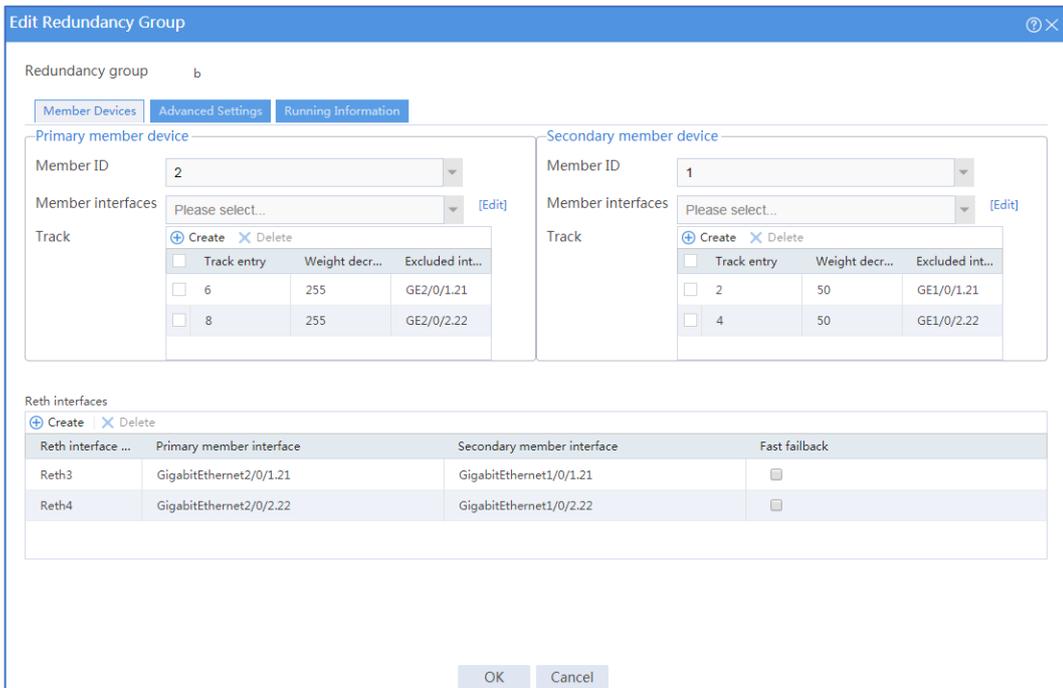
図 16 冗長グループ b の作成



#OK をクリックします。

#冗長グループを設定します(図 17 を参照)。

図 17 冗長グループ b の設定



Track entry	Weight decr...	Excluded int...	
<input type="checkbox"/>	6	255	GE2/0/1.21
<input type="checkbox"/>	8	255	GE2/0/2.22

Track entry	Weight decr...	Excluded int...	
<input type="checkbox"/>	2	50	GE1/0/1.21
<input type="checkbox"/>	4	50	GE1/0/2.22

Reth interface ...	Primary member interface	Secondary member interface	Fast fallback
Reth3	GigabitEthernet2/0/1.21	GigabitEthernet1/0/1.21	<input type="checkbox"/>
Reth4	GigabitEthernet2/0/2.22	GigabitEthernet1/0/2.22	<input type="checkbox"/>

#OK をクリックします。

#インターフェイスに IP アドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。

#Reth1 と Reth3 をセキュリティゾーン **Untrust** に割り当て、Reth2 と Reth4 をセキュリティゾーン **Trust** に割り当てます(詳細は省略)。

## 外部ネットワークへのスタティックルートの設定

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > Static Routing** を選択します。

#10.1.1.0/24へのルートのネクストホップを52.1.1.1(スイッチBのVLANインターフェイス12のIPアドレス)として指定します。10.10.1.0/24へのルートのネクストホップを62.1.1.1(スイッチBのVLANインターフェイス22のIPアドレス)として指定します。(詳細は省略。)

## インターネットに到達するために内部ネットワークから送信されるトラフィックに対する PBR ポリシーの設定

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > Policy-Based Routing > IPv4PBR** を選択します。

#次のようにPBRポリシーを設定します。

- 10.1.1.0/24 からインターネットに送信されるトラフィックのネクストホップを 51.1.1.1(スイッチ A の VLAN インターフェイス 11 の IP アドレス)に指定します。
- 10.10.1.0/24 からインターネットに送信されるトラフィックのネクストホップを 61.1.1.1(スイッチ A の VLAN インターフェイス 21 の IP アドレス)に指定します。

## スイッチ A の設定

この例では、簡単な設定手順のみを示しています。

1. VLAN10、VLAN11、およびVLAN21を作成します。
  2. GigabitEthernet1/0/1およびGigabitEthernet1/0/2をレイヤー2モードで動作するように設定し、これらをトランクインターフェイスとしてVLAN11およびVLAN12に割り当てます。
  3. GigabitEthernet1/0/3をレイヤー2モードで動作するように設定し、アクセスインターフェイスとしてVLAN10に割り当てます。
- A) VLANインターフェイス11、VLANインターフェイス21、およびVLANインターフェイス10にそれぞれ51.1.1.1/24、61.1.1.1/24、および2.1.1.1/24を割り当てます。
- B) 次のようにルートを設定します。

- 10.1.1.0/24 へのルートのネクストホップとして 51.1.1.2(Reth1 の IP アドレス)を指定します。
- 10.10.1.0/24 へのルートのネクストホップとして 61.1.1.2(Reth3 の IP アドレス)を指定します。
- インターネットへのルートのネクストホップとして 2.1.1.2(VLAN-interface10 のピアインターフェイスの IP アドレス)を指定します。

## スイッチ B の設定

この例では、簡単な設定手順のみを示しています。

1. VLAN12、VLAN20、VLAN22、および VLAN30 を作成します。
2. レイヤー2 モードで動作するように GigabitEthernet1/0/1 および GigabitEthernet1/0/2 を設定し、これらをトランクインターフェイスとして VLAN12 および VLAN22 に割り当てます。
3. GigabitEthernet1/0/3 をレイヤー2 モードで動作するように設定し、アクセスインターフェイスとして VLAN20 に割り当てます。
4. GigabitEthernet1/0/4 をレイヤー2 モードで動作するように設定し、アクセスインターフェイスとして VLAN30 に割り当てます。
5. VLANインターフェイス12、VLANインターフェイス22、VLANインターフェイス20、およびVLANインターフェイス30に、それぞれ52.1.1.1/24、62.1.1.1/24、10.1.1.1/24、および10.10.1.1/24を割り当てます。
6. PBRポリシーを次のように設定します。
  - 52.1.1.2(Reth2 の IP アドレス)を 10.1.1.0/24 からのパケットのネクストホップとして指定します。
  - 10.10.1.0/24 からのパケットのネクストホップとして 62.1.1.2(Reth4 の IP アドレス)を指定します。

## ホストの構成

#ホストAで、デフォルトゲートウェイとして10.1.1.1(スイッチBのVLANインターフェイス20のIPアドレス)を指定します。ホストBで、デフォルトゲートウェイとして10.10.1.1(スイッチBのVLANインターフェイス30のIPアドレス)を指定します。

## 設定の確認

デバイスAまたはデバイスBの設定を確認します。

1. 上部のナビゲーションバーで、**System** をクリックします。
2. ナビゲーションペインで、**High Availability > Hot Backup** を選択します。
3. 冗長グループ a の **edit** アイコンをクリックします。
4. **Running Information** をクリックします。

図 18 デバイス A が正常に動作している場合の冗長グループ a の情報

Redundancy group a

Member Devices | Advanced Settings | Running Information

Refresh

Redundancy group a

Remaining preemption delay time 0(sec)

Remaining hold-down time 0(sec)

Member devices	Status	Weight
1	Primary	255
2	Secondary	255

Reth interface

Name	Member interfaces	Member interface forwarding status	Member interface presence status
Reth1	GigabitEthernet1/0/1.11	Active	Present
	GigabitEthernet2/0/1.11	Inactive	Present
Reth2	GigabitEthernet1/0/2.12	Active	Present
	GigabitEthernet2/0/2.12	Inactive	Present

図 19 デバイス A が正常に動作している場合の冗長グループ b の情報

Redundancy group b

Member Devices | Advanced Settings | Running Information

Refresh

Redundancy group b

Remaining preemption delay time 0(sec)

Remaining hold-down time 0(sec)

Member devices	Status	Weight
2	Primary	255
1	Secondary	255

Redundancy group

Name	Member interfaces	Member interface forwarding status	Member interface presence status
Reth3	GigabitEthernet2/0/1.21	Active	Present
	GigabitEthernet1/0/1.21	Inactive	Present
Reth4	GigabitEthernet2/0/2.22	Active	Present
	GigabitEthernet1/0/2.22	Inactive	Present

Reth interface

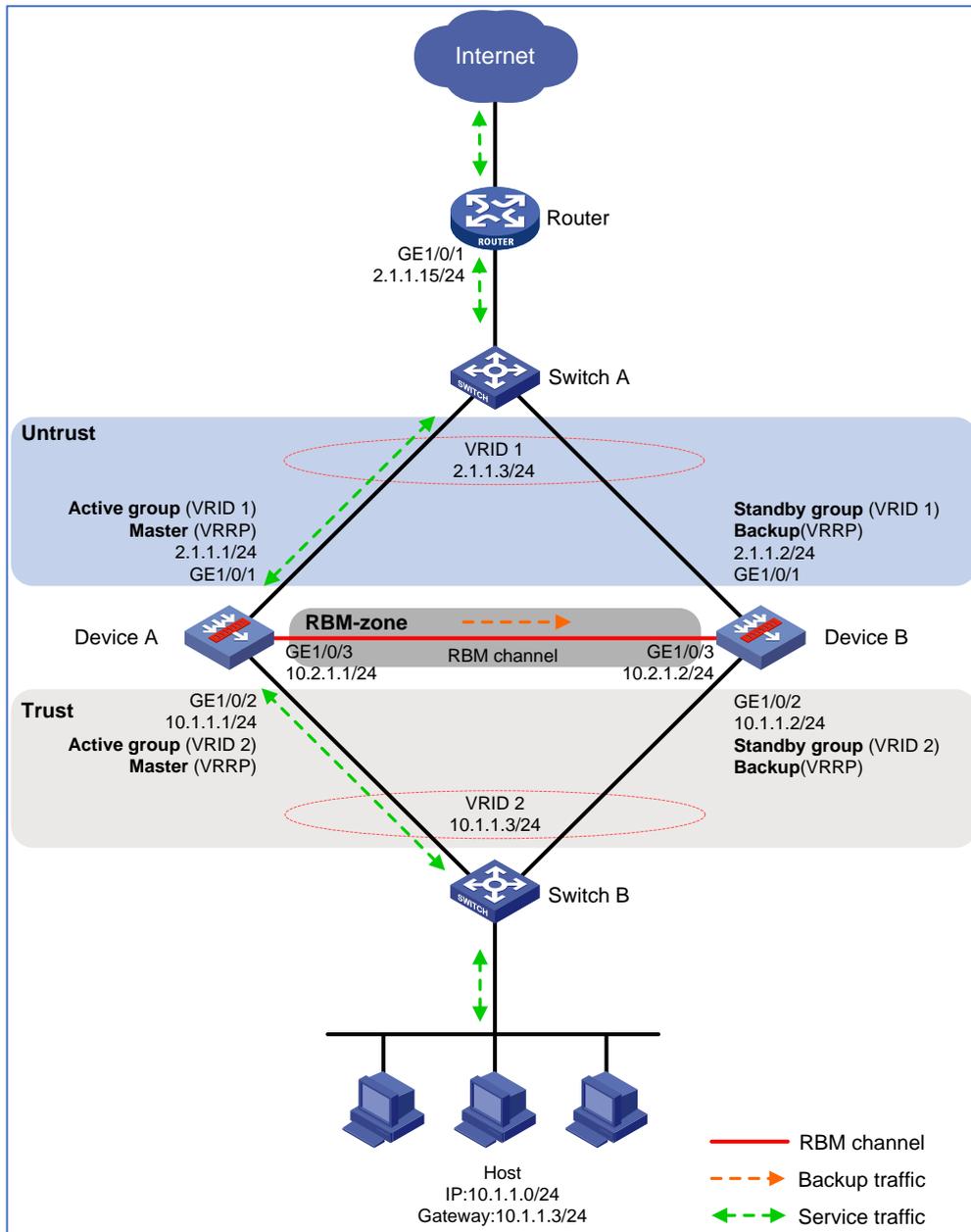
## 例:アクティブ/スタンバイモードでのVRRPホットバックアップシステムの設定

### ネットワーク構成

図 20 に示すように、インターネットと企業の内部ネットワーク間の境界に VRRP ホットバックアップシステムを設定して、サービスの継続性を確保します。

- アクティブ/スタンバイモードで動作するようにホットバックアップシステムを設定します。
- デバイス A をプライマリデバイスとして設定し、デバイス B をセカンダリデバイスとして設定します。

図 20 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

# 前提条件

VRRPホットバックアップを設定する前に、VRRPホットバックアップシステムのメンバーデバイスで、次のハードウェアおよびソフトウェア設定が同じであることを確認してください。

- デバイスモデル
- ソフトウェアバージョン
- IRF メンバーID
- コントロールチャネルを設定するためのインターフェイス
- データチャネルを設定するためのインターフェイス
- 同じスロット番号を持つインターフェイス上のセキュリティゾーン設定
- サービスモジュールの場所、数、およびタイプ
- インターフェイスモジュールの場所、数、およびタイプ

インターフェイスやルーティング機能など、VRRPホットバックアップが設定を同期しない機能の設定を完了してください。

# 手順

この例では、VRRP ホットバックアップ設定は CLI の RBM に属しています。

## デバイス A の設定

### 基本的なネットワーク設定

#インターフェイスに IP アドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **RBM-zone** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B が RBM チャネルを設定できます(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **Untrust** と **Local** 間およびセキュリティゾーン **Trust** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B は VRRP パケットを交換し、RBM チャネルが使用できないときにマスターを選択できます(詳細は省略)。

## VRRP ホットバックアップの設定

#トップナビゲーションバーで、**System** 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。

#VRRP ホットバックアップを設定します(図 21 を参照)。

図 21 VRRP ホットバックアップの設定

VRRP hot backup

VRRP hot backup  Enable  Disable

Operating mode  Active/standby  Dual-active

Device role  Active  Standby

Service entry hot backup  Enable  Disable

Data channel GE1/0/3

Local IP 10.2.1.1

Peer IP 10.2.1.2

Peer port 60064 (1024-65535. Default: 60064.)

VRRP preemption delay 1 minutes (1-50. Default: 1.)

Configuration consistency check  Enable  Disable

Interval 12 hours (1-168. Default: 24.)

Automatic configuration synchronization  Enable  Disable

Apply Synchronize configuration

#**Apply** をクリックします。

## RBM と VRRP グループの関連付け

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**High Availability > VRRP** を選択します。

#**create** をクリックします。

#VRRPグループ1を設定し、VRRPアクティブグループに関連付けます。

図 22 VRRP グループ 1 の作成

Interface GE1/0/1 \*

VRID 1 \* ( 1-255 )

IP type  IPv4  IPv6

VRRP hot backup Associate and ad

Virtual IP 2.1.1.3 \*(Separate multiple addresses with commas)

Priority 100 ( 1-254 )

Preemption mode Preemptive

Preemption delay 0 centiseconds ( 0-180000 )

Advertisement interval 100 centiseconds ( 10-4095 )

OK Cancel

#OK をクリックします。

#create をクリックします。

#VRRPグループ2を設定し、VRRPアクティブグループに関連付けます。

図 23 VRRP グループ 2 の作成

Interface	GE1/0/2	*
VRID	2	*( 1-255 )
IP type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
VRRP hot backup	Associate and ad	
Virtual IP ?	10.1.1.3	*(Separate multiple addresses with commas)
Priority	100	( 1-254 )
Preemption mode	Preemptive	
Preemption delay	0	centiseconds ( 0-180000 )
Advertisement interval	100	centiseconds ( 10-4095 )

OK Cancel

#OK をクリックします。

## デバイス B の設定

### 基本的なネットワーク設定

#インターフェイスに IP アドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **RBM-zone** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B が RBM チャネルを設定できます(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **Untrust** と **Local** 間およびセキュリティゾーン **Trust** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B は VRRP パケットを交換し、RBM チャネルが使用できないときにマスターを選択できます(詳細は省略)。

## VRRP ホットバックアップの設定

#トップナビゲーションバーで、**System** 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。

#VRRP ホットバックアップを設定します(図 24 を参照)。0

図 24 VRRP ホットバックアップの設定

VRRP hot backup

VRRP hot backup  Enable  Disable

Operating mode  Active/standby  Dual-active

Device role  Active  Standby

Service entry hot backup  Enable  Disable

Data channel  \*

Local IP  \*

Peer IP  \*

Peer port  (1024-65535. Default: 60064.)

VRRP preemption delay  minutes (1-50. Default: 1.)

Configuration consistency check  Enable  Disable

Interval  hours (1-168. Default: 24.)

Automatic configuration synchronization  Enable  Disable

#**Apply** をクリックします。

## RBM と VRRP グループの関連付け

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**High Availability > VRRP** を選択します。

#**create** をクリックします。

#VRRPグループ1を設定し、VRRPスタンバイグループに関連付けます。

図 25 VRRP グループ 1 の作成

Interface: GE1/0/1 \*

VRID: 1 \* ( 1-255 )

IP type:  IPv4  IPv6

VRRP hot backup: Associate and ad

Virtual IP <sup>?</sup>: 2.1.1.3 \*(Separate multiple addresses with commas)

Priority: 100 ( 1-254 )

Preemption mode: Preemptive

Preemption delay: 0 centiseconds ( 0-180000 )

Advertisement interval: 100 centiseconds ( 10-4095 )

OK Cancel

#OK をクリックします。

#create をクリックします。

#VRRPグループ2を設定し、VRRPスタンバイグループに関連付けます。

図 26 VRRP グループ 2 の作成

Interface	GE1/0/2	*
VRID	2	*( 1-255 )
IP type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
VRRP hot backup	Associate and ad	
Virtual IP ?	10.1.1.3	*(Separate multiple addresses with commas)
Priority	100	( 1-254 )
Preemption mode	Preemptive	
Preemption delay	0	centiseconds ( 0-180000 )
Advertisement interval	100	centiseconds ( 10-4095 )

OK Cancel

#OK をクリックします。

## スイッチ A の設定

この例では、簡単な設定手順のみを示しています。

#VLAN10 を作成します。

#ホットバックアップシステムおよびルーターに接続されたインターフェイスをレイヤー2 モードで動作するように設定します。これらのインターフェイスをアクセスインターフェイスとして VLAN10 に割り当てます。

## スイッチ B の設定

この例では、簡単な設定手順のみを示しています。

#VLAN10を作成します。

#ホットバックアップシステムとホストに接続されたインターフェイスをレイヤー2モードで動作するように設定します。これらのインターフェイスをアクセスインターフェイスとして VLAN10 に割り当てます。

## ルーターの設定

この例では、簡単な設定手順のみを示しています。

#IP アドレス 2.1.1.15/24 を GigabitEthernet1/0/1 に割り当てます。

#次のようにルートを設定します。

- 内部ネットワークへのルートのネクストホップとして 2.1.1.3(VRRP グループ 1 の仮想 IP アドレス)を指定します。
- トラフィック発信インターフェイスに接続されたピアインターフェイスの IP アドレスを、インターネットへのルートのネクストホップとして指定します。

## セキュリティサービスの設定

#デバイス A(プライマリ)で RBM によってバックアップできるセキュリティサービスを設定します。RBM によってバックアップできるセキュリティサービスの詳細は、High Availability Configuration Guide を参照してください。

## ホストの構成

#ホストで、デフォルトゲートウェイとして10.1.1.3(VRRPグループ2の仮想IPアドレス)を指定します(詳細は省略)。

## 設定の確認

#セキュリティゾーン **Trust** と **Untrust** 間の通信を許可するゾーン間ポリシーのロギングをイネーブルにします。ホストがデバイス A を介してインターネットと通信するときに、デバイス B がログメッセージを生成しないことを確認します(詳細は省略)。

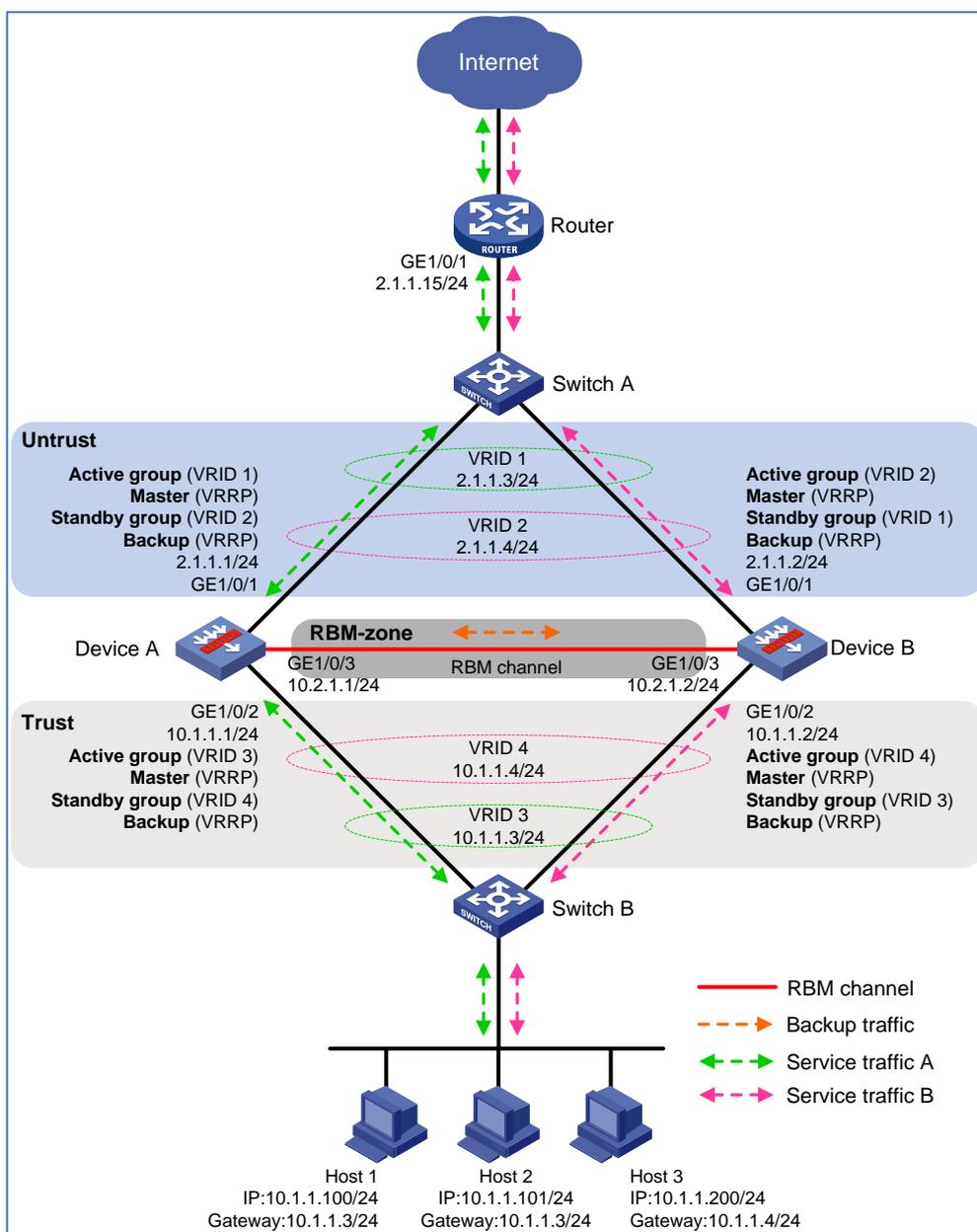
# 例:デュアルアクティブモードでのVRRPホットバックアップシステムの設定

## ネットワーク構成

図 27 に示すように、インターネットと企業の内部ネットワーク間の境界に VRRP ホットバックアップシステムを設定して、サービスの継続性を確保します。

- ホットバックアップシステムをデュアルアクティブモードで動作するように設定します。
- デバイス A とデバイス B がトラフィックをロードシェアリングするように設定します。

図 27 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 前提条件

VRRPホットバックアップを設定する前に、VRRPホットバックアップシステムのメンバーデバイスで、次のハー

ドウェアおよびソフトウェア設定が同じであることを確認してください。

- デバイスモデル
- ソフトウェアバージョン
- IRF メンバーID
- コントロールチャネルを設定するためのインターフェイス
- データチャネルを設定するためのインターフェイス
- 同じスロット番号を持つインターフェイス上のセキュリティゾーン設定
- サービスモジュールの場所、数、およびタイプ
- インターフェイスモジュールの場所、数、およびタイプ

インターフェイスやルーティング機能など、VRRPホットバックアップが設定を同期しない機能の設定を完了してください

## 手順

### デバイス A の設定

#### 基本的なネットワーク設定

#インターフェイスに IP アドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **RBM-zone** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B が RBM チャネルを設定できます(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **Untrust** と **Local** 間およびセキュリティゾーン **Trust** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B は VRRP パケットを交換し、RBM チャネルが使用できないときにマスターを選択できます(詳細は省略)。

#### VRRP ホットバックアップの設定

#トップナビゲーションバーで、**System** 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。

#VRRP ホットバックアップを設定します(図 28 を参照)。

図 28 VRRP ホットバックアップの設定

VRRP hot backup

VRRP hot backup  Enable  Disable

Operating mode  Active/standby  Dual-active

Device role  Active  Standby

Service entry hot backup  Enable  Disable

Data channel GE1/0/3 \*

Local IP 10.2.1.1 \*

Peer IP 10.2.1.2 \*

Peer port 60064 (1024-65535, Default: 60064,)

VRRP preemption delay 1 minutes (1-50, Default: 1,)

Configuration consistency check  Enable  Disable

Interval 12 hours (1-168, Default: 24,)

Automatic configuration synchronization  Enable  Disable

Apply Synchronize configuration

#Apply をクリックします。

## RBM と VRRP グループの関連付け

この例では、簡単な設定手順だけを示しています。RBM と VRRP グループの関連付けの詳細については、“例:アクティブ/スタンバイモードでの VRRP ホットバックアップシステムの設定”を参照してください。

#GigabitEthernet1/0/1 上に VRRP グループ 1 を作成し、その仮想 IP アドレスを 2.1.1.3 に設定して、VRRP アクティブグループに関連付けます。

#GigabitEthernet1/0/1 上に VRRP グループ 2 を作成し、その仮想 IP アドレスを 2.1.1.4 に設定して、VRRP スタンバイグループに関連付けます。

#GigabitEthernet1/0/2 上に VRRP グループ 3 を作成し、その仮想 IP アドレスを 10.1.1.3 に設定して、VRRP アクティブグループに関連付けます。

#GigabitEthernet1/0/2 上に VRRP グループ 4 を作成し、その仮想 IP アドレスを 10.1.1.4 に設定して、VRRP スタンバイグループに関連付けます。

## デバイス B の設定

### 基本的なネットワーク設定

#インターフェイスに IP アドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。ネットワーク接続が使用可能であることを確認します(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **RBM-zone** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B が RBM チャネルを設定できます(詳細は省略)。

#ゾーン間ポリシーを設定して、セキュリティゾーン **Untrust** と **Local** 間およびセキュリティゾーン **Trust** と **Local** 間の通信を許可します。これにより、デバイス A とデバイス B は VRRP パケットを交換し、RBM チャネルが使用できないときにマスターを選択できます(詳細は省略)。

### VRRP ホットバックアップの設定

#トップナビゲーションバーで、**System** 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。

#VRRP ホットバックアップを設定します(図 29 を参照)。

図 29 VRRP ホットバックアップの設定

VRRP hot backup	
VRRP hot backup	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Operating mode	<input type="radio"/> Active/standby <input checked="" type="radio"/> Dual-active
Device role	<input type="radio"/> Active <input checked="" type="radio"/> Standby
Service entry hot backup	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Data channel	GE1/0/3 *
Local IP	10.2.1.2 *
Peer IP	10.2.1.1 *
Peer port	60064 (1024-65535. Default: 60064.)
VRRP preemption delay	1 minutes (1-50. Default: 1.)
Configuration consistency check	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Interval	12 hours (1-168. Default: 24.)
Automatic configuration synchronization	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Synchronize configuration"/>	

#Apply をクリックします。

### RBM と VRRP グループの関連付け

この例では、簡単な設定手順だけを示しています。RBM と VRRP グループの関連付けの詳細については、「」を参照してください。

#GigabitEthernet1/0/1 に VRRP グループ 1 を作成し、その仮想 IP アドレスを 2.1.1.3 に設定して、VRRP スタンバイグループに関連付けます。

#GigabitEthernet1/0/1 上に VRRP グループ 2 を作成し、その仮想 IP アドレスを 2.1.1.4 に設定して、VRRP アクティブグループに関連付けます。

#GigabitEthernet1/0/2 上に VRRP グループ 3 を作成し、その仮想 IP アドレスを 10.1.1.3 に設定して、VRRP スタンバイグループに関連付けます。

#GigabitEthernet1/0/2 上に VRRP グループ 4 を作成し、その仮想 IP アドレスを 10.1.1.4 に設定して、VRRP アクティブグループに関連付けます。

## スイッチ A の設定

この例では、簡単な設定手順のみを示しています。

#VLAN10 を作成します。

#ホットバックアップシステムおよびルーターに接続されたインターフェイスをレイヤー2 モードで動作するように設定します。これらのインターフェイスをアクセスインターフェイスとして VLAN10 に割り当てます。

## スイッチ B の設定

この例では、簡単な設定手順のみを示しています。

#VLAN10 を作成します。

#ホットバックアップシステムとホストに接続されたインターフェイスをレイヤー2 モードで動作するように設定します。これらのインターフェイスをアクセスインターフェイスとして VLAN10 に割り当てます。

## ルーターの設定

この例では、簡単な設定手順のみを示しています。

#IP アドレス 2.1.1.15/24 を GigabitEthernet1/0/1 に割り当てます。

#次のようにルートを設定します。

- 内部ネットワークの他のサブネットへのルートのネクストホップとして 2.1.1.3(VRRP グループ 1 の仮想 IP アドレス)を指定します。内部ネットワークの他のサブネットへのルートのネクストホップとして 2.1.1.4(VRRP グループ 2 の仮想 IP アドレス)を指定します。
- トラフィック発信インターフェイスに接続されているピアインターフェイスの IP アドレスを、インターネットへのルートのネクストホップとして指定します。

## セキュリティサービスの設定

#デバイス A(プライマリ)で RBM によってバックアップできるセキュリティサービスを設定します。RBM によってバックアップできるセキュリティサービスの詳細は、High Availability Configuration Guide を参照してください。

## ホストの構成

#一部のホストでは、デフォルトゲートウェイとして 10.1.1.3(VRRP グループ 3 の仮想 IP アドレス)を指定します。その他のホストでは、デフォルトゲートウェイとして 10.1.1.4(VRRP グループ 4 の仮想 IP アドレス)を指定します(詳細は省略)。

## 設定の確認

#セキュリティゾーン **Trust** と **Untrust** 間の通信を許可するゾーン間ポリシーのロギングをイネーブルにします。デバイス B がトラフィックを転送するホストがインターネットと通信するときに、デバイス B がログメッセージを生成しないこと。デバイス B がトラフィックを転送するホストがインターネットと通信するときに、デバイス B がログメッセージを生成しないこと。(詳細は省略)

# ユーザーID の設定例

## はじめに

次に、ユーザーID の設定例を示します。

ユーザー識別機能は、IP アドレスでユーザーを識別します。この機能は、他のセキュリティ機能と連携して、ユーザーごとにネットワークアクセスを制御します。

この機能により、デバイスは次のタスクを実行できます。

- セキュリティポリシーをユーザーごとに実装して、ポリシーの使いやすさを向上させます。
- ネットワーク攻撃動作とトラフィックフローの統計情報と分析をユーザー単位で収集し、ユーザーネットワークアクセス動作をリアルタイムで追跡します。
- ユーザーIP アドレスの変更に関係なく、ポリシー制御を実装します。

RADIUS シングルサインオンサービスを使用すると、RADIUS サーバーはユーザーID 情報(ユーザー名や IP アドレスなど)をセキュリティデバイス(ファイアウォールなど)に同期させることができます。これにより、ユーザーは RADIUS サーバーでの認証に合格した後、デバイスで認証することなくネットワークにアクセスできます。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、ポータル、AAA、ユーザーID、およびセキュリティポリシー機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

セキュリティポリシーおよびパケットフィルタポリシーを構成する場合は、それらが期待どおりに有効になるようにしてください。セキュリティポリシーは、パケットフィルタポリシーの前にパケットを処理します。パケットフィルタポリシーは、セキュリティポリシーと一致するパケットを処理しません。

## 例:RADIUS認証(RADIUSシングルサインオン)を通過するポータルユーザーのユーザーIDの設定

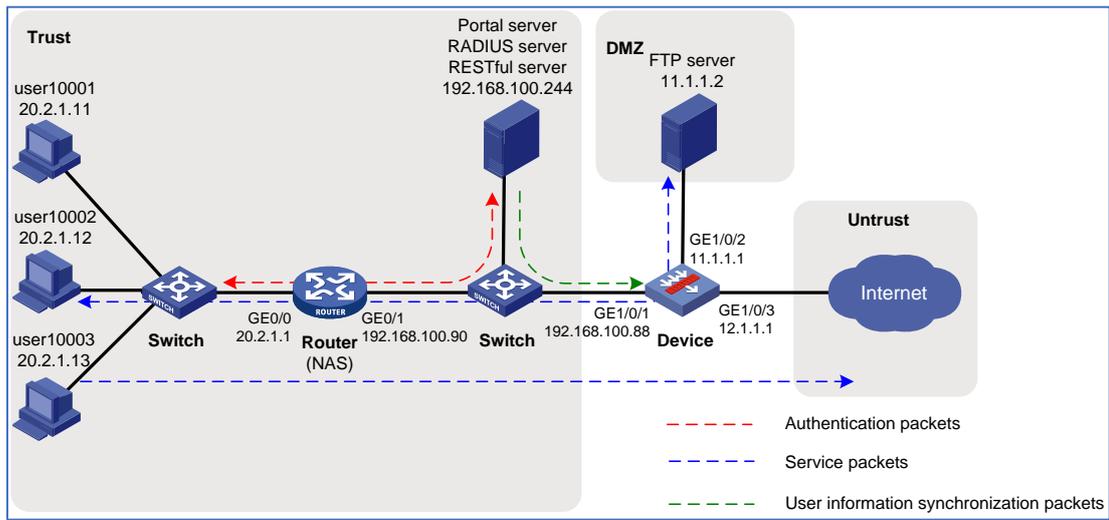
### ネットワーク構成

図1に示すように:

- ユーザー **user10001**、**user10002**、および **user10003** は静的 IP アドレスを使用し、ネットワークにアクセスするにはポータル認証に合格する必要があります。
- ルーターは、ユーザーがネットワークにアクセスするための NAS として機能します。NAS は RADIUS サーバーを使用してユーザーを認証します。
- RADIUS サーバーは IMC コンポーネントとともにインストールされます。ポータル認証の場合、サーバーはポータル認証サーバーとポータル Web サーバーの両方として機能します。

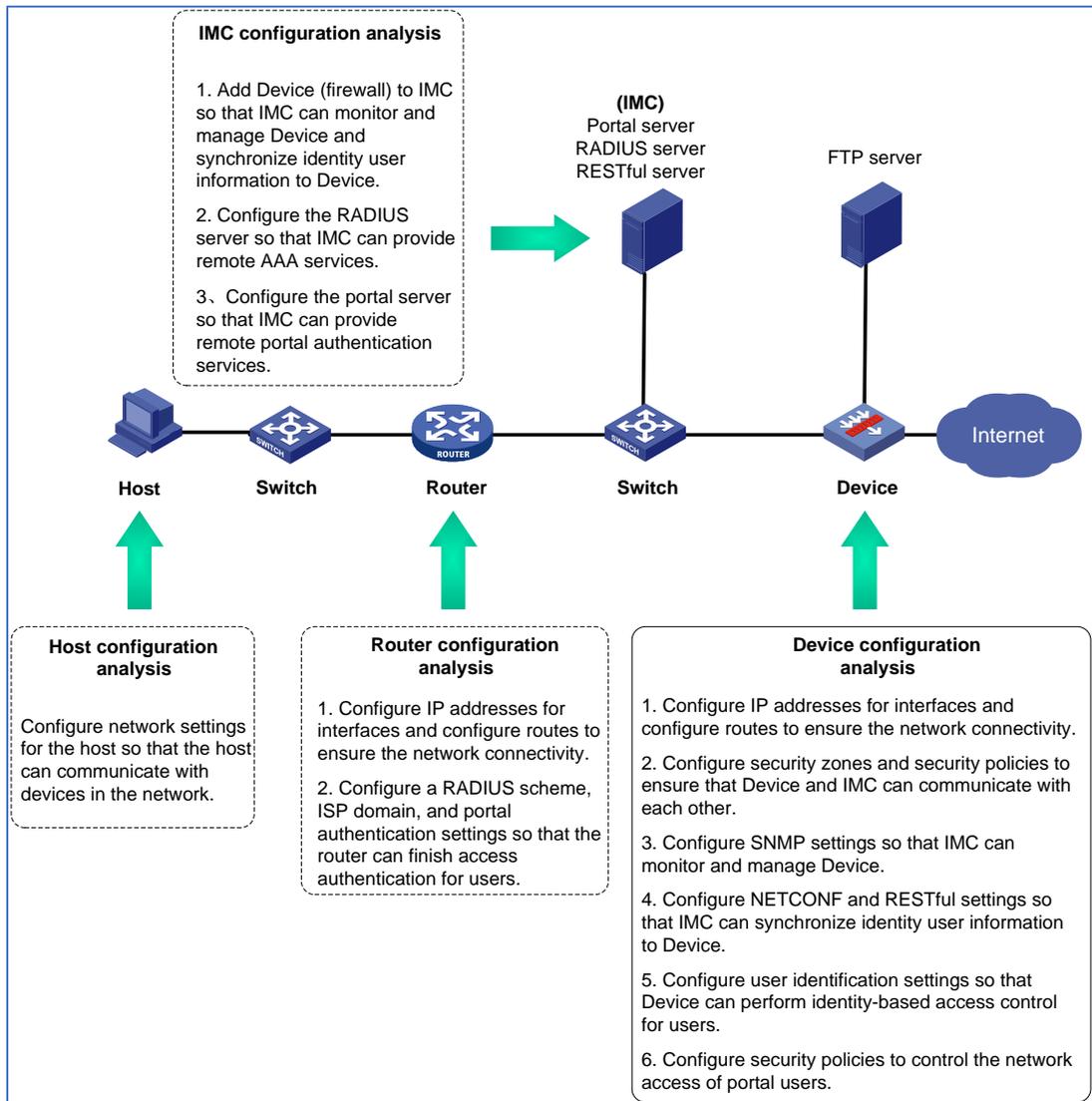
- RESTful サーバーはユーザーカウント情報を保存します。サーバーはユーザーID 情報をデバイスに同期できます。
- デバイスはファイアウォールです。ユーザーは、RADIUS サーバーでの認証に合格した後、ファイアウォールで認証することなくネットワークにアクセスできます。
- ファイアウォールは、ポータル認証に合格したユーザーに対して次の ID ベースのアクセスコントロールを実行します。
  - ユーザー **user10001** は FTP サーバーまたはインターネットにアクセスできません。
  - ユーザー **user10002** は FTP サーバーにアクセスできますが、インターネットにはアクセスできません。
  - ユーザー **user10003** はインターネットにアクセスできますが、FTP サーバーにはアクセスできません。
  - インターネットからのユーザーは、**Trust** および **DMZ** セキュリティゾーン内のホストにアクセスできません。

図1 ネットワーク図



# 分析

図2 分析図



## 使用するソフトウェアバージョン

この設定例は、次のソフトウェアバージョンで作成および確認されています。

- F1060 デバイスの E9345

- バージョン 7.1.064、MSR26-30 ルーターの ESS0701。

RADIUS およびポータルサーバーは、IMC PLAT7.3(E0506)、IMC UAM7.3(E0503)、IMMC CAMS7.3(E0501)、および IMMC SSM7.3(E0501)とともにインストールされます。

## 制限事項とガイドライン

IMC サーバーがオンラインユーザーをログオフするのは、そのユーザーに対する会計停止要求を受信した後のみです。NAS が会計停止要求をサーバーに送信するには、NAS 上のユーザーの認証ドメインで会計設定を構成する必要があります。ただし、会計は必要ないため、IMC サーバーで会計パラメータを構成する必要はありません。

## 手順

### ルーターの設定

ルーターのネットワーク接続を保証するためのインターフェイスおよびデフォルトルートの IP アドレスの設定

#IP アドレス 20.2.1.1 を GigabitEthernet0/0 に割り当てます。

```
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ip address 20.2.1.1 255.255.255.0
[Router-GigabitEthernet0/0] quit
```

#IP アドレス 192.168.100.90 を GigabitEthernet0/1 に割り当てます。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ip address 192.168.100.90 255.255.255.0
[Router-GigabitEthernet0/1] quit
```

#ルーターが FTP サーバーとインターネットに到達できるようにデフォルトルートを設定します。

```
Routerip route-static0.0.0.0 0.0.0.0 192.168.100.88
```

## ルーターを監視および管理するための IMC サーバーの SNMP の設定

#SNMP エージェントを有効にします。

```
[Router] snmp-agent
```

#すべての SNMP バージョンを有効にし、読み取り専用コミュニティ **public** と読み取りおよび書き込みコミュニティ **private** を作成します。

```
[Router] snmp-agent sys-info version all
```

```
[Router] snmp-agent community read public
```

```
[Router] snmp-agent community write private
```

## RADIUS スキームの設定

#**rs1** という名前の RADIUS スキームを作成し、そのビューを入力します。

```
[Router] radius scheme rs1
```

#192.168.100.244 のサーバーをプライマリ認証サーバーおよびプライマリアカウンティングサーバーとして指定し、認証共有キーをプレーンテキスト形式の **admin** に設定して、セキュアな RADIUS 通信を実現します。

```
[Router-radius-rs1] primary authentication 192.168.100.244
```

```
[Router-radius-rs1] primary accounting.192.168.100.244
```

```
[Router-radius-rs1,] key authentication simple admin
```

#RADIUS サーバーに送信されるユーザー名からドメイン名を除外します。

```
[Router-radius-rs1] user-name-format without-domain
```

```
[Router-radius-rs1] quit
```

## 認証ドメインの構成

#**dm1** という名前の ISP ドメインを作成し、そのビューを入力します。

```
[Router] domain dm1
```

#ポータルユーザーの認証、認可、アカウントングに RADIUS スキーム **rs1** を使用するように ISP ドメインを設定します。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
```

```
[Router-isp-dm1] authorization portal radius-scheme rs1
```

```
[Router-isp-dm1] accounting portal radius-scheme rs1
```

```
[Router-isp-dm1] quit
```

## ポータル認証の設定

```
#ポータル認証サーバーを構成します。
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.100.244 key simple admin
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit

#ポータル Web サーバーを構成します。

[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.100.244:8080/portal
[Router-portal-websvr-newpt] quit
#GigabitEthernet0/0 で直接ポータル認証をイネーブルにします。
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] portal enable method direct
#GigabitEthernet0/0 でポータル Web サーバーnewpt を指定します。
[Router-GigabitEthernet0/0] portal apply web-server newpt
#ドメイン dm1 を GigabitEthernet0/0 上のポータル認証ドメインとして指定します。
[Router-GigabitEthernet0/0] portal domain dm1
[Router-GigabitEthernet0/0] quit
```

## デバイス(ファイアウォール)の設定

ファイアウォールを監視および管理するための IMC サーバーの

### SNMP の設定

```
#SNMP エージェントを有効にします。
<Device> system-view
[Device] snmp-agent

#すべての SNMP バージョンを有効にし、読み取り専用コミュニティ public と読み取りおよび書き込みコミュニティ private を作成します。
[Device] snmp-agent sys-info version all
[Device] snmp-agent community read public
[Device] snmp-agent community write private
```

## ファイアウォールに設定を発行するための IMC サーバーの NETCONF over SOAP の設定

#NETCONF over SOAP over HTTP を有効にします。

```
[Device] netconf soap http enable
```

#NETCONF over SOAP over HTTPS を有効にします。

## ファイアウォールが IMC RESTful サーバーと通信するための RESTful の有効化

#RESTful over HTTP を有効にします。

```
[Device] restful http enable
```

#HTTPS 経由の RESTful を有効にします。

```
[Device] restful https enable
```

## インターフェイスへの IP アドレスの割り当ておよびインターフェイスのセキュリティゾーンへの追加

1. IPアドレス192.168.100.88をGigabitEthernet1/0/1に割り当て、インターフェイスをゾーンTrustに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **basic configuration** タブで、Trustセキュリティゾーンを選択します。

B) **IPv4Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、192.168.100.88/24と入力します。

図3 セキュリティゾーン Trust へのインターフェイスの追加

**Modify Interface Settings** [?] [X]

Name: GE1/0/1

Link status: **Up**  Shut down

Description: GigabitEthernet1/0/1 Interface

Link mode: Layer 3 mode

**Basic Configuration** | IPv4 Address | IPv6 Address | Physical Interface Configuration

Add an interface to a security zone: Trust

VRF: Public network

Speed: autonegotiation

Duplex mode: autonegotiation

MAC address: 74-1F-4A-80-DA-69

MTU: 1500 (46-1560)

Expected bandwidth: <1-400000000> (kbps)

Apply OK Cancel

図4 インターフェイスの IP アドレスとマスクの設定

The screenshot shows the 'Modify Interface Settings' window for interface GE1/0/1. The 'IPv4 Address' tab is selected. The 'IP address' is set to 'Manual assignment' with the value '192.168.100.88' and a mask length of '255.255.255.0'. Below this, there is a table for secondary IP addresses:

Secondary IP ad...	Mask length	Edit

Buttons at the bottom include 'Apply', 'OK', and 'Cancel'.

#OK をクリックします。

2. GigabitEthernet1/0/1を設定するのと同じ方法で、次の作業を実行します。
  - IP アドレス 11.1.1.1 を GigabitEthernet1/0/2 に割り当て、インターフェイスをゾーン DMZ に追加します。
  - IP アドレス 12.1.1.1 を GigabitEthernet1/0/3 に割り当て、インターフェイスをゾーン Untrust に追加します。

## ファイアウォールのネットワーク接続を保証するための IP ルーティングの設定

1. ファイアウォールとユーザーが互いに到達できるように、スタティックルートを設定します。  
#トップナビゲーションバーで、**Network** をクリックします。  
#ナビゲーションペインで、**Routing > Static Routing** を選択します。  
#IPv4 Static Routing タブで、**Create** をクリックします。  
#開いたダイアログボックスで、IPv4 スタティックルートを設定します。
  - **Destination address** フィールドに 20.2.1.0 と入力します。
  - **Mask length** フィールドに 24 と入力します。
  - **Next hop** フィールドにネクストホップアドレスとして 192.168.100.90 を入力します。

図5 IPv4 スタティックルートの作成

The screenshot shows a 'Create IPv4 Static Route' dialog box with the following fields and values:

- VPN instance: Public network
- Destination address: 20.2.1.0
- Mask length: 24
- Next hop:  Next hop VRF instance,  Output interface, Next hop address: 192.168.100.90
- Preference: 60
- Route tag: 0
- Description: (empty)

Buttons: OK, Cancel

#OK をクリックします。

2. ファイアウォールがインターネットに到達できるように、デフォルトルートを設定します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Routing > Static Routing** を選択します。

#IPv4 Static Routing タブで、**Create** をクリックします。

#開いたダイアログボックスで、IPv4 スタティックルートを設定します。

- **Destination address** フィールドに 0.0.0.0 と入力します。
- **Mask length** フィールドに 0 と入力します。
- **Next hop** フィールドにネクストホップアドレスとして 12.1.1.2 を入力します。

インターネットのファイアウォールに接続するデバイスの IP アドレスをネクストホップアドレスとして指定します。この例では、ネクストホップアドレスは 12.1.1.2 です。

図6 IPv4 スタティックルートの作成

The screenshot shows a dialog box titled "Create IPv4 Static Route". It contains the following fields and values:

- VPN instance: Public network
- Destination address: 0.0.0.0
- Mask length: 0
- Next hop:  Next hop VRF instance,  Output interface, Next hop address: 12.1.1.2
- Preference: 60
- Route tag: 0
- Description: (empty)

Buttons: OK, Cancel

#OK をクリックします。

## 管理者 admin への HTTP サービスの割り当て

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**Administrators > Administrators** を選択します。

#管理者 **admin** 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、HTTP サービスを選択します(図7を参照)。

図7 管理者情報の変更

Username: admin (1-55 chars)

Password: (1-63 chars)

Confirm: (1-63 chars)

User role: network-admin (1-55 chars)

User group: system

Services:  Terminal  SSH  HTTPS  FTP  
 Telnet  PAD  HTTP

Max concurrent logins: (1-1024)

FTP directory: cfa0:

Advanced settings ⓘ

OK Cancel

#OK をクリックします。

## ユーザーID の構成

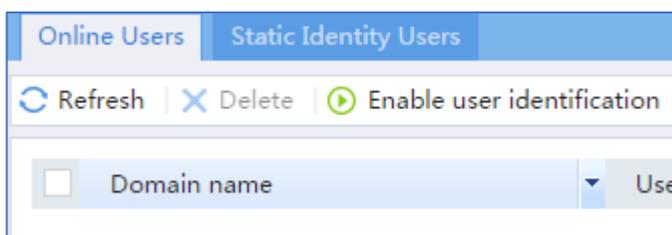
1. ユーザーIDを有効にする:

#トップナビゲーションバーで、**Objects** 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。

#Online Users タブで、**Enable user identification** をクリックします。

図8 ユーザーIDの有効化



2. RESTfulサーバーrest1の作成:

#トップナビゲーションバーで、**Objects** 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 サーバーの次のパラメータを構成します。

- サーバー名を rest1 に、ユーザー名を admin に、パスワードを admin に設定します。
- Get-user-account URI を  
http://192.168.100.244:8080/imcrs/ssm/imcuser/accessUser に設定します。
- Get-online-user URI を http://192.168.100.244:8080/imcrs/ssm/imcuser/onlineUser  
に設定します。
- Get-user-group URI を  
http://192.168.100.244:8080/imcrs/ssm/imcuser/accessUserGroup に設定します。
- Put-online-user URI を  
http://192.168.100.244:8080/imcrs/ssm/imcuser/uploadOnlineUser に設定します。
- Put-offline-user URI を  
http://192.168.100.244:8080/imcrs/ssm/imcuser/uploadOfflineUser に設定します。



IMC RESTfulサーバーの場合、URIは固定形式です。IPアドレス以外の上記のURIのパラメータは変更できません。

図9 RESTful サーバーの作成

Name	rest1	*(1-31 chars)
Username	admin	*(1-55 chars)
Password	.....	*(1-63 chars)
Get-user-account URI	http://192.168.100.244:8080/imcrs/ssm/imcuse	(1-255 chars)
Get-online-user URI	http://192.168.100.244:8080/imcrs/ssm/imcuse	(1-255 chars)
Get-user-group URI	http://192.168.100.244:8080/imcrs/ssm/imcuse	(1-255 chars)
Put-online-user URI	http://192.168.100.244:8080/imcrs/ssm/imcuse	(1-255 chars)
Put-offline-user URI	http://192.168.100.244:8080/imcrs/ssm/imcuse	(1-255 chars)
VRF	Public network	
Enable server detection	<input type="checkbox"/>	

#OK をクリックします。

3. ユーザーインポートポリシーimcの作成:

#トップナビゲーションバーで、**Objects** 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。

#ユーザーインポートポリシーのパラメータを設定します(図10を参照)。

図10 ユーザーインポートポリシーの作成

#OK をクリックします。

#ファイアウォールと IMC サーバーが相互に通信できるようになったら、User Import Policies ページに移動し、ポリシーリストから imc を選択します。次に、Manually import identity users アイコンと Manually import online users アイコンをクリックして、IMC サーバーのユーザーカウントとオンラインユーザーをファイアウォールにインポートします。

図11 ユーザーカウントとオンラインユーザーのインポート

Policy name	RESTful server	LDAP schemes	Import types	Auto import interval	Auto import	Manually import iden...	Manually import onli...	Edit
<input type="checkbox"/> imc	rest1		User and user group	1	Enabled			

## ファイアウォールと IMC サーバー間のネットワーク接続を確保するためのセキュリティポリシーの設定

ファイアウォールが IMC サーバーから ID ユーザー情報をインポートできるようにするには、この項の作業を実行します。

1. セキュリティポリシー trust-local を作成して、ゾーン Trust からゾーン Local へのトラフィックを許可します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Create > Create a policy** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを次のように設定します。

- セキュリティポリシー名を **trust-local** に設定します。
- **Source zone** フィールドから **security zone Trust** を選択します。
- **Destination zone** フィールドから **security zone Local** を選択します。
- アクションを **permit** に設定します。

#OK をクリックします。

2. セキュリティポリシーlocal-trustを作成して、セキュリティポリシーtrust-localを作成する場合と同じ方法で、ゾーン Local からゾーン Trust へのトラフィックを許可します。

## ユーザーのアクセス権を制御するセキュリティポリシーの構成

1. ユーザーuser10002がFTPサーバーにアクセスできるようにし、他のユーザーがFTPサーバーにアクセスできないようにするには、セキュリティポリシーuser10002を作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Create > Create a policy** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを次のように設定します。

- セキュリティポリシー名を user10002 に設定します。
- **Source zone** フィールドからセキュリティゾーン Trust および DMZ を選択します。
- **Destination zone** フィールドからセキュリティゾーン Trust および DMZ を選択します。
- アクションを **permit** に設定します。
- user user10002 を選択します。

#OK をクリックします。

2. セキュリティポリシーuser10003を作成して、ユーザーuser10003がインターネットにアクセスできるようにしますが、インターネットからのユーザーが内部ネットワークにアクセスできないようにします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Create > Create a policy** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを次のように設定します。

- セキュリティポリシー名を **user10003** に設定します。
- **Source zone** フィールドから **security zone Trust** を選択します。
- **Destination zone** フィールドから **security zone Untrust** を選択します。
- アクションを **permit** に設定します。
- ユーザー **user10003** を選択します。

#OK をクリックします。

## 管理対象デバイスの IMC への追加

IMC がデバイスを監視および管理できるように、ルーターとファイアウォールを IMC に追加します。

### 1. IMCにログインします。

#Web ブラウザのアドレスバーに IMC の URL を入力します。この例では、URL は `http://192.168.100.244:8080/imc/` です。

#username に **admin** と password に **admin** を入力します。

### 2. ファイアウォールをIMCに追加します。

#**Resource** タブをクリックします。

#ナビゲーションツリーで、**Resource Management > Add Device** を選択します。

#開いたページで、図12に示すようにパラメータを設定します。

- Telnet Settings 領域で、username と password を **admin** に設定します。
- 他のパラメータにはデフォルト値を使用します。

デフォルトでは、読み取り専用 SNMP コミュニティストリングは `public`、読み取りおよび書き込み SNMP コミュニティストリングは `private` です。

図12 IMC へのファイアウォールの追加

Resource > Add Device

Basic Information

Host Name/IP \* 192.168.100.88

Device Label

Mask

Device Group

Login Type Telnet

Automatically register to receive SNMP traps from supported devices

Support Ping Operation

Add the device regardless of the ping result

Use the loopback address as the management IP

+ SNMP Settings

- Telnet Settings

Configure

Authentication Mode	Username + Password
Username	admin
Password	*****
Timeout (seconds)	4

+ SSH Settings

OK Cancel

#OK をクリックします。

#ファイアウォールを IMC に追加するのと同じ方法で、ルーター(192.168.100.90)を IMC に追加します。

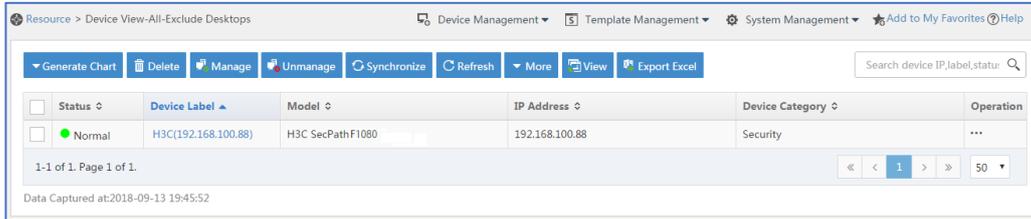
3. NETCONF設定の変更:

#Resource タブをクリックします。

#ナビゲーションツリーで、**View Management > Device View** を選択します。

#ターゲットデバイスの **Device Label** 列のリンクをクリックします。

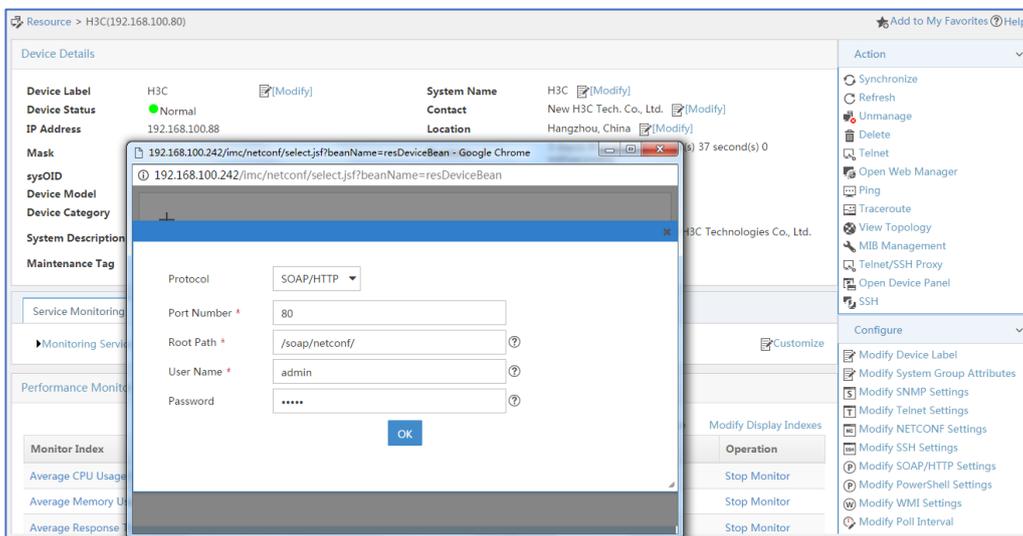
図13 デバイスリスト



#右ペインで、**Configure > Modify NETCONF Settings** をクリックします。

#表示されるダイアログボックスで、プラス記号(+)をクリックしてプロトコルを追加します(図14を参照)。この例では、ユーザー名とパスワードを **admin** に設定します。

図14 NETCONF 設定の変更



#OK をクリックします。

## セキュリティサービス(IMC)の設定

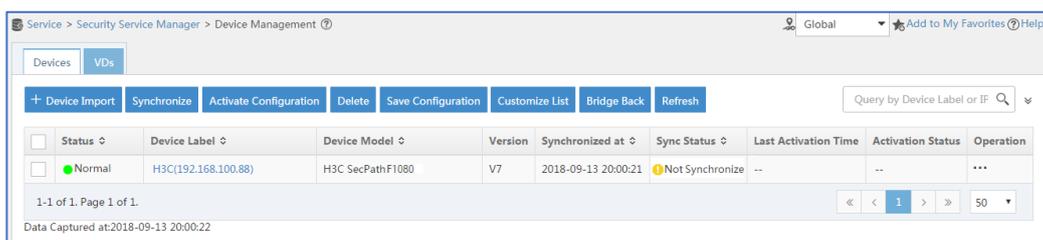
1. ファイアウォールからIMCサーバーへのセキュリティサービスを同期して、ファイアウォールとIMCサーバーの間で設定とユーザー情報が一貫していることを確認します。

#**Service** タブをクリックします。

#ナビゲーションツリーで、**Security Service Manager > Device Management** を選択します。

#**Devices** タブのデバイスリストにファイアウォールが表示されます(図15を参照)。

図15 セキュリティデバイス管理ページ(非同期)



#デバイスリストでファイアウォールを選択し、**Synchronize** をクリックします。**Sync Status** 列から同期ステータスを表示できます(図16および図17を参照)。

同期処理に時間がかかる場合があります。しばらくお待ちください。

図16 セキュリティデバイス管理(同期化)ページ

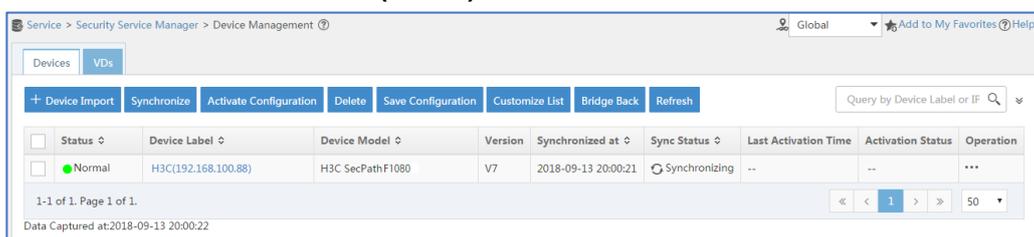
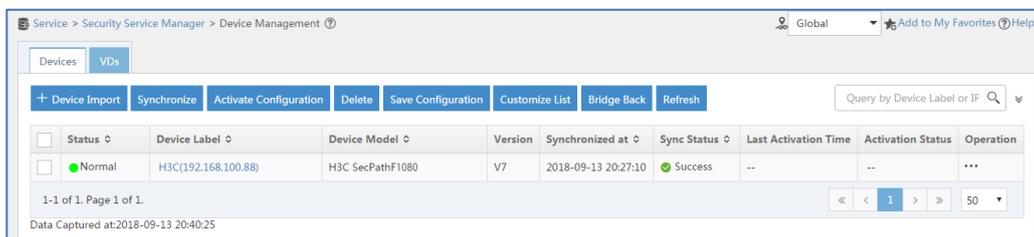


図17 セキュリティデバイス管理ページ(同期成功)



2. ユーザー認証システムパラメータおよびユーザー通知パラメータを設定して、IMCサーバーがユーザーのオンラインおよびオフライン情報をファイアウォールにリアルタイムで同期できるようにします。

#**Service** タブをクリックします。

#ナビゲーションツリーで、**Security Service Manager > Global Parameters** を選択します。

#ユーザー認証システムパラメータを設定します(図18を参照)。

ポータル認証サーバーのプロトコルに応じてプロトコルを選択します。ユーザー名とパスワードが IMC サーバーへのログインに使用したのと同じであることを確認してください。

図18 ユーザー認証システムパラメーターの構成

Enable *	<input type="radio"/> No <input checked="" type="radio"/> Yes
Access Type *	EIA
Protocol *	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
Authentication System Address *	127.0.0.1
Port Number *	8080
Username *	admin
Password *	*****

#OK をクリックします。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy > Service Parameters>System Settings** を選択します。

#ユーザー通知 **user notification parameters** の **Configure** アイコンをクリックします。

#開いたページで、**add** をクリックします。

#**Add User Notification** ページで、図19に示すようにパラメータを設定します。この例では、共有キーをランダムに入力できます。

図19 ユーザー通知パラメーターの構成

Notification Type	<input type="radio"/> RADIUS <input type="radio"/> SYSLOG <input type="radio"/> UDP <input checked="" type="radio"/> Proprietary <input type="radio"/> Custom
Server IP Address *	127.0.0.1
Server Port *	11812
Share Key *	•
Confirm Shared Key *	•

#OK をクリックします。

## RADIUS サーバー(IMC)の設定

1. ルーターをアクセスデバイスとしてサーバーに追加します。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy > Access Device Management>Access Device** を選択します。

#add をクリックします。

#共有キーを **admin** に設定します(図20を参照)。

#**Device List** 領域で、**Select** または **Add Manually** をクリックして、192.168.100.90 のデバイスをアクセスデバイスとして追加します。

サーバー上のアクセスデバイスの IP アドレスとして、ルーター上の発信 RADIUS パケットの送信元 IP アドレスを指定する必要があります。

ルーターでは、送信元 IP アドレスは nas-ip または radius nas-ip コマンドを使用して設定されます。nas-ip コマンドを使用して設定された IP アドレスは、radius nas-ip コマンドを使用して設定された IP アドレスよりも優先順位が高くなります。送信元 IP アドレスとして IP アドレスが指定されていない場合、パケット送信インターフェイスの IP アドレスが送信元 IP アドレスとして使用されます。この例では、パケット送信インターフェイスの IP アドレス 192.168.100.90 が使用されます。

## 図20 アクセスデバイスの追加

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port \* 1812 Accounting Port \* 1813

Service Type Unlimited Forcible Logout Type Disconnect user

Access Device Type H3C (General) Service Group Ungrouped

Shared Key \* \*\*\*\*\* Confirm Shared Key \* \*\*\*\*\*

Access Device Group --

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
Router	192.168.100.90			

Total Items: 1.

OK Cancel

#OK をクリックします。

## 2. アクセスポリシーを追加します。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy > Access Policy** を選択します。

#add をクリックします。

#アクセスポリシー名を **Portal** に設定します(図21を参照)。

図21 アクセスポリシーの追加

User > User Access Policy > Access Policy > Add Access Policy

Basic Information

Access Policy Name \* Portal

Service Group \* Ungrouped

Description

Authorization Information

Authentication Binding Information

User Client Configuration

OK Cancel

#OK をクリックします。

3. アクセスサービスを追加します。

#user タブを選択します。

#ナビゲーションツリーから、**User Access Policy > Access Service** を選択します。

#add をクリックします。

#Add Access Service ページで、次のパラメータを設定します。

- portal にサービス名を入力します。
- **Default Access Policy** リストから **Portal** を選択します。

図22 アクセスサービスの追加

User > User Access Policy > Access Service > Add Access Service

Basic Information

Service Name \* Portal

Service Group \* Ungrouped

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Devices for Single Account \* 0

Daily Max. Online Duration \* 0

Description

Available

Service Suffix

Default Access Policy \* Portal

Default Max. Number of Online Endpoints \* 0

Transparent Authentication

Access Scenario List

OK Cancel

#OK をクリックします。

#### 4. アクセスマユーザーの追加

#user タブをクリックします。

#ナビゲーションツリーから、**Access User > All Access Users** を選択します。

#add をクリックします。

#Add Access User ページで、パラメータを設定します(図23を参照)。

- **User Name** フィールドに **user** と入力します。
- **Account Name** フィールドに **user10001** と入力します。
- **Password** フィールドと **Confirm Password** フィールドに **admin** と入力します。
- Access Service 領域で Portal を選択します。

図23 アクセスマユーザーの追加

User > All Access Users > Add Access User

Access Information

User Name \*

Account Name \*  ⓘ

Trial Account  Default BYOD User  MAC Authentication User  Computer User  Fast Access User

Password \*  Confirm Password \*

Allow User to Change Password  Enable Password Strategy  Modify Password at Next Login

Start Time  End Time

Max. Idle Time (Minutes)  Max. Concurrent Logins

Login Message

Access Service

<input type="checkbox"/>	Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/>	Portal		Available	

Binding Information

#OK をクリックします。

#ユーザーカウント **user10002** と **user10003** を、ユーザーカウント **user10001** を追加するのと同じ方法で追加します。

## ポータルサーバー(IMC)の設定

ポータルサーバーを構成します。

#**user** タブをクリックします。

#ナビゲーションツリーから、User Access Policy > Portal Service > Server を選択します。

#ネットワークの状態に応じて図24のようにパラメータを設定します。この例では、デフォルト値が使用されています。

図24 ポータルサーバーの構成

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level \* Info

Bind IP Group to Port Groups Deny

Portal Server

Request Timeout (Seconds) \* 4

Server Heartbeat Interval (Seconds) \* 20

User Heartbeat Interval (Minutes) \* 5

LB Device Address

Portal Web

Request Timeout (Seconds) \* 15

Packet Code

Verify Endpoint Requests Yes

Use Cache No

HTTP Heartbeat Display New Page

HTTPS Heartbeat Display Original Page

Portal Page

https://192.168.100.244:8080/portal/  
https://192.168.100.244:8443/portal/

#OK をクリックします。

2. IPグループを追加します。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy > Portal Service > IP Group** を選択します。

#add をクリックします。

#パラメータを設定します(図25を参照)。

**図25 IPグループの追加**

User > User Access Policy > Portal Service > IP Group > Add IP Group

Help

Add IP Group

IP Group Name \* Portal-user

Start IP \* 20.2.1.10

End IP \* 20.2.1.100

Service Group Ungrouped

Action \* Normal

OK Cancel

#OK をクリックします。

3. ポータルデバイスを追加します。

#user タブをクリックします。

#ナビゲーションツリーで、**User Access Policy > Portal Service > Device** を選択します。

#add をクリックします。

#共有キーを admin に設定し、その他のパラメータを設定します(図26を参照)。

**図26 ポータルデバイスの追加**

The screenshot shows a web interface for adding a device. The breadcrumb navigation is 'User > User Access Policy > Portal Service > Device > Add Device'. The page title is 'Add Device'. There are two main sections: 'Device Information' and 'Advanced Information'. The 'Device Information' section contains: Device Name (Router), IP Address (192.168.100.90), Key (\*\*\*\*\*), and Confirm Key (\*\*\*\*\*). The 'Advanced Information' section contains: Listening Port (2000), Local Challenge (No), Authentication Retries (0), Logout Retries (1), Support Server Heartbeat (No), Support User Heartbeat (No), Version (Portal 2.0), Service Group (Ungrouped), Access Method (Directly Conne...), and Device Description (empty field). At the bottom, there are 'OK' and 'Cancel' buttons.

#OK をクリックします。

4. ポータルデバイスをIPグループに関連付けます。

#user タブをクリックします。

#ナビゲーションツリーで、**User Access Policy > Portal Service > Device** を選択します。

#ルーターの **Operation** カラムで **Port Group** アイコンをクリックします。

図27 デバイスリスト

#開いたページで、**add** をクリックします。

#開いたページで、ポートグループを設定します(を参照)。

図28 ポートグループの追加

#OK をクリックします。

## ホストの構成

#各ホストの IP アドレス、ネットワークマスクおよびデフォルトゲートウェイ設定を構成します。ホストがネットワーク内のデバイスと通信できることを確認します(詳細は省略)。

# 設定の確認

1. ホスト上で、ユーザーがポータル認証を通過できることを確認します。

#ポータル認証ページにログインするために、Web ブラウザのアドレスバーにポータル Web サーバーの URL を入力します。この例では、URL は `http://192.168.100.244:8080/portal` です。

#ユーザー名とパスワードを入力します。

#**Login** をクリックします。

#ユーザーがポータル認証に合格したことを確認します。

図29 ポータル認証成功ページ



2. IMC サーバーで、ユーザー `user10001`、`user10002` および `user10003` がポータル認証に合格した後、オンラインユーザーリストにあることを確認します。オンラインユーザーリストを表示するには、**user** タブをクリックし、ナビゲーションツリーから **Access user > Online Users** を選択します。
3. ファイアウォールで、IDユーザー情報を表示します。

#すべての ID ユーザーに関する情報を表示します。

```
[Device] display user-identity all user
```

User ID	Username
0x2	user10001
0x3	user10002
0x4	user10003

#オンライン ID ユーザー `user10001` に関する情報を表示します。

```
[Device] display user-identity online-user null-domain name user10001
```

```
User name: user10001
```

IP : 20.2.1.11

MAC : 0011-95e4-4aa9

Type: Dynamic

Total 1 records matched.

#オンライン ID ユーザーuser10002 に関する情報を表示します。

[Device] display user-identity online-user null-domain name user10002

User name: user10002

IP : 20.2.1.12

MAC : 0011-95e4-4aa3

Type: Dynamic

Total 1 records matched.

#オンライン ID ユーザーuser10003 に関する情報を表示します。

[Device] display user-identity online-user null-domain name user10003

User name: user10003

IP : 20.2.1.13

MAC : 0011-95e4-4aa2

Type: Dynamic

Total 1 records matched.

4. ファイアウォールがユーザーに対してIDベースのアクセスコントロールを実行できることを確認します。

# ユーザー **user10001** が FTP サーバーに ping できないことを確認しなさい

C:¥>ping 11.1.1.2

Pinging 11.1.1.2 with 32 bytes of data:

Request time out.

Request time out.

Request time out.

Request time out.

Ping statistics for 11.1.1.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

#ユーザーuser10002 が FTP サーバーに ping を実行するときに、ファイアウォールが次のメッセージを生成することを確認します。

```
[Device]%Nov  6 10:19:53:920 2017 H3C FILTER/6/FILTER_ZONE_EXECUTION_ICMP: -Context=1; SrcZoneName(1025)=Trust;DstZoneName(1035)=DMZ;Type(1067)=ACL;SecurityPolicy(1072)=user10002;RuleID(1078)=2;Protocol(1001)=ICMP;SrcIPAddr(1003)=20.2.1.12;SrcMacAddr(1021)=7425-8a37-b5f6;DstIPAddr(1007)=11.1.1.2;IcmpType(1062)=ECHO(8);IcmpCode(1063)=0;MatchCount(1069)=1;Event(1048)=Permit;
```

#ユーザーuser10003 がインターネットのホストに ping できることを確認します。この例では、ユーザーは 12.1.1.2 でホストに ping します。

```
C:¥>ping 12.1.1.2
```

Pinging 12.1.1.2 with 32 bytes of data:

```
Reply from 12.1.1.2: bytes=32 time=37ms TTL=253
```

```
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
```

```
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
```

```
Reply from 12.1.1.2: bytes=32 time<1ms TTL=253
```

Ping statistics for 12.1.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 36ms, Average = 9ms

#ユーザーuser10003 がインターネットのホストに ping を実行するときに、ファイアウォールが次のメッセージを生成することを確認します。

```
[Device]%Nov  6 10:19:53:920 2017 H3C FILTER/6/FILTER_ZONE_EXECUTION_ICMP: -Context=1; SrcZoneName(1025)=Trust;DstZoneName(1035)=Untrust;Type(1067)=ACL;SecurityPolicy(1072)=user10003;RuleID(1078)=3;Protocol(1001)=ICMP;SrcIPAddr(1003)=20.2.1.13;SrcMacAddr(1021)=7425-8a37-b5f6;DstIPAddr(1007)=12.1.1.2;IcmpType(1062)=ECHO(8);IcmpCode(1063)=0;MatchCount(1069)=1;Event(1048)=Permit;
```

## 構成ファイル

### ルーター

```
[Router] display current-configuration
```

```
#
```

```
interface GigabitEthernet0/0
```

```
port link-mode route
ip address 20.2.1.1 255.255.255.0
portal enable method direct
portal domain dm1
portal apply web-server newpt
#
interface GigabitEthernet0/1
port link-mode route
ip address 192.168.100.90 255.255.255.0
#
interface GigabitEthernet3/0
port link-mode route
combo enable copper
#
ip route-static 0.0.0.0 0 192.168.100.88
#
snmp-agent
snmp-agent local-engineid 800063A28074258A37B5F500000001
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
#
radius scheme rs1
primary authentication 192.168.100.244
primary accounting 192.168.100.244
key authentication cipher $c$3$hhbEbD5Ycvw7VWqljAoMoU7hQRgcUjtg
user-name-format without-domain
```

```

#
domain dm1
    authentication portal radius-scheme rs1
    authorization portal radius-scheme rs1
    accounting portal radius-scheme rs1
#
domain system
#
    domain default enable system
#
local-user admin class manage
    password                                     hash
    $h$6$UblhNnPevyKUwfpm$LqR3+yg1ljNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
    bablIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
    service-type telnet http
    authorization-attribute user-role network-admin
#
portal web-server newpt
    url http://192.168.100.244:8080/portal
#
portal server newpt
    ip 192.168.100.244 key cipher $c$3$+UmaGOco7eHsjOqlrp8ll4eYe0A8NpYU
#
return

```

## デバイス

```

[Device] display current-configuration
#

```

```
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.100.88 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 12.1.1.1 255.255.255.0
#
security-zone name Trust
  import interface GigabitEthernet1/0/1
#
security-zone name DMZ
  import interface GigabitEthernet1/0/2
#
security-zone name Untrust
  import interface GigabitEthernet1/0/3
#
line vty 0 63
  authentication-mode scheme
  user-role network-admin
#
ip route-static 0.0.0.0 0 12.1.1.2
ip route-static 20.2.1.0 24 192.168.100.90
```

```

#
snmp-agent
snmp-agent local-engineid 800063A280487ADA9593B700000001
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 192.168.100.244 params securityn
ame public v2c
#
local-user admin class manage
password hash
$h$6$UblhNnPevyKUwfpm$LqR3+yg1ljNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babllFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
service-type ssh telnet terminal http https
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
netconf soap http enable
netconf soap https enable
restful http enable
restful https enable
#
user-identity enable
user-identity user-account auto-import policy imc
#
user-identity restful-server rest1
login-name admin password cipher $c$3$phGy00HA6OP6pIpGI0KOKZEOPuLVbtt/

```

```
uri get-user-database http://192.168.100.244:8080/imcrs/ssm/imcuser/accessUser
uri get-user-group-database http://192.168.100.244:8080/imcrs/ssm/imcuser/acces
sUserGroup
uri get-online-user http://192.168.100.244:8080/imcrs/ssm/imcuser/onlineUser
uri put-online-user http://192.168.100.244:8080/imcrs/ssm/imcuser/uploadOnlineU
ser
uri put-offline-user http://192.168.100.244:8080/imcrs/ssm/imcuser/uploadOfflin
eUser
#
user-identity user-import-policy imc
account-update-interval 1
restful-server rest1
#
security-policy ip
rule 0 name trust-local
action pass
source-zone trust
destination-zone local
rule 1 name local-trust
action pass
source-zone local
destination-zone trust
rule 2 name user10002
action pass
logging enable
source-zone trust
source-zone dmz
```

```
destination-zone dmz
destination-zone trust
user user10002
rule 3 name user10003
action pass
logging enable
source-zone trust
destination-zone untrust
user user10003
#
Return
```

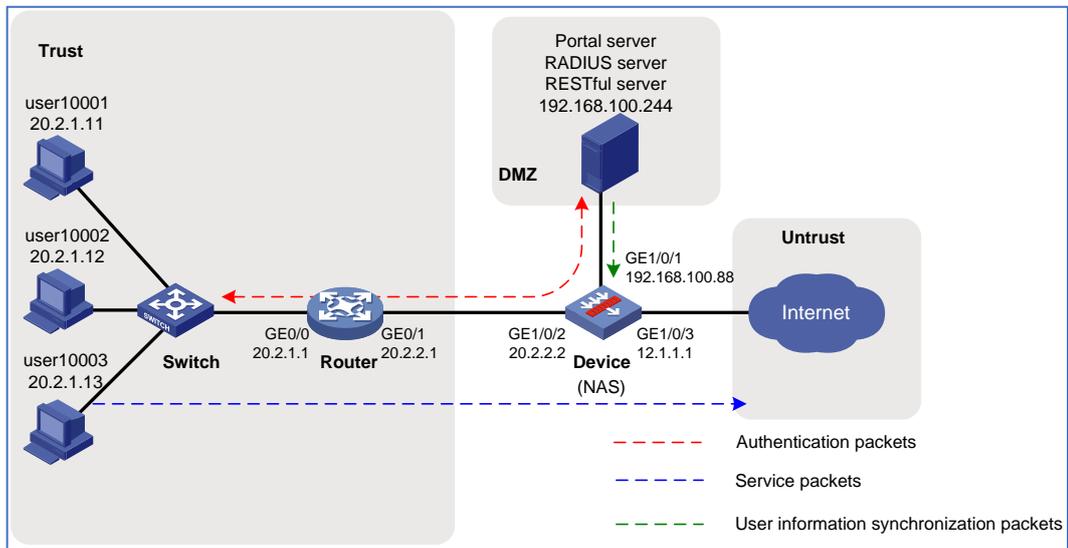
# 例:RADIUS認証(非RADIUSシングルサインオン)をパスするポータルユーザーのユーザーIDの設定

## ネットワーク構成

図30に示すように

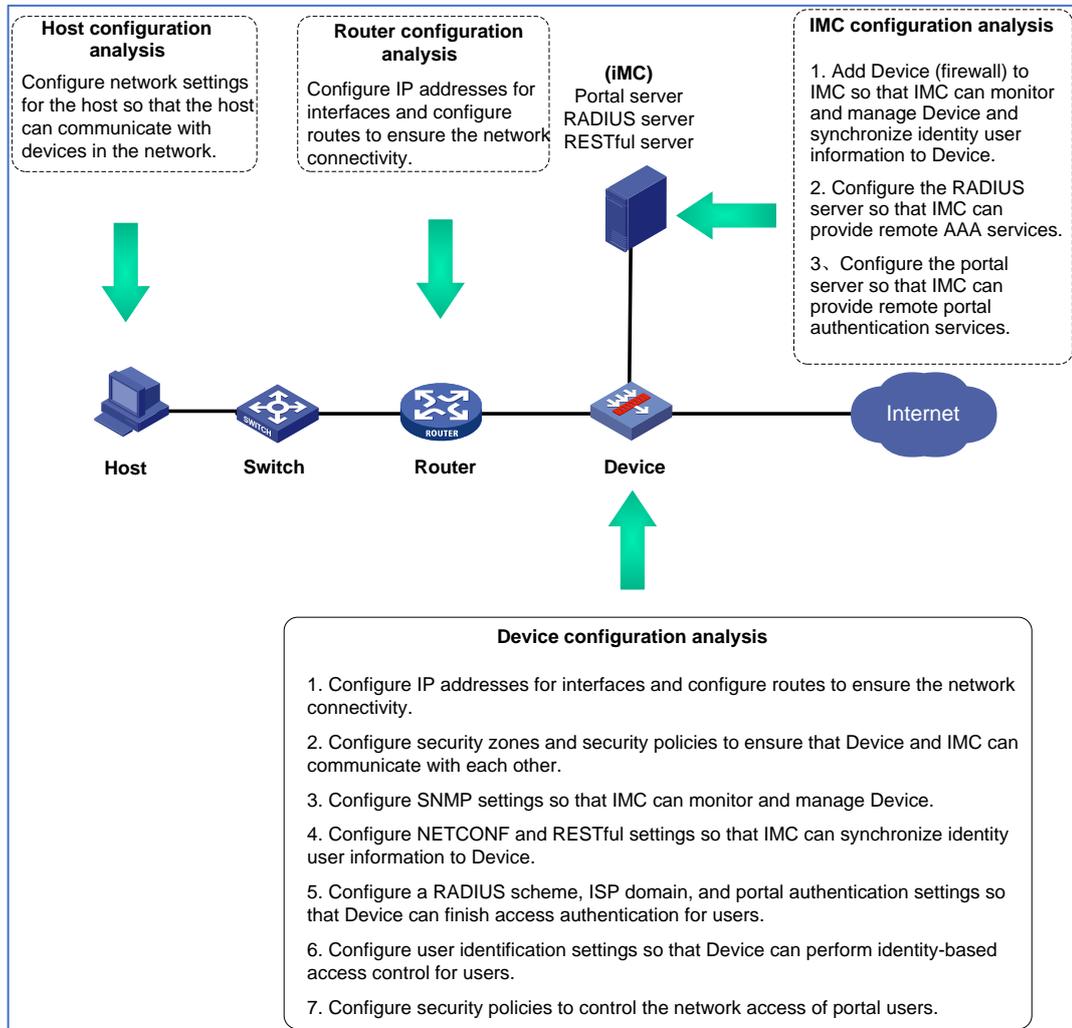
- ユーザーuser10001、user10002、および user10003 は静的 IP アドレスを使用し、ネットワークにアクセスするにはポータル認証に合格する必要があります。
- デバイスはファイアウォールであり、ユーザーがネットワークにアクセスするための NAS として機能します。NAS は RADIUS サーバーを使用してユーザーを認証します。
- RADIUS サーバーは IMC コンポーネントとともにインストールされます。ポータル認証の場合、サーバーはポータル認証サーバーとポータル Web サーバーの両方として機能します。
- RESTful サーバーはユーザーカウント情報を保存します。サーバーはユーザーID 情報をデバイス(ファイアウォール)に同期できます。
- ファイアウォールは、ポータル認証に合格したユーザーに対して次の ID ベースのアクセスコントロールを実行します。
  - ユーザーuser10001 および user10002 はインターネットにアクセスできません。
  - ユーザーuser10003 はインターネットにアクセスすることができる。
  - インターネットからのユーザーは、trust および DMZ セキュリティゾーン内のホストにアクセスできません。

図30 ネットワーク図



# 分析

図31 分析図



## 使用するソフトウェアバージョン

この設定例は、次のソフトウェアバージョンで作成および確認されています。

- F1060 デバイスの E9345
- バージョン 7.1.064、MSR26-30 ルーターの ESS0701。

RADIUS およびポータルサーバーは、IMC PLAT7.3(E0506)、IMC UAM7.3(E0503)、IMMC CAMS7.3(E0501)、および IMMC SSM7.3(E0501)とともにインストールされます。

## 制限事項とガイドライン

IMC サーバーがオンラインユーザーをログオフするのは、そのユーザーに対する会計停止要求を受信した後のみです。NAS が会計停止要求をサーバーに送信するには、NAS 上のユーザーの認証ドメインで会計設定を構成する必要があります。ただし、会計は必要ないため、IMC サーバーで会計パラメータを構成する必要はありません。

## 手順

### ルーターの設定

ルーターのネットワーク接続を確認するには、この項の作業を実行します。

#IP アドレス 20.2.1.1 を GigabitEthernet0/0 に割り当てます。

```
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ip address 20.2.1.1 255.255.255.0
[Router-GigabitEthernet0/0] quit
```

#IP アドレス 20.2.2.1 を GigabitEthernet0/1 に割り当てます。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ip address 20.2.2.1 255.255.255.0
[Router-GigabitEthernet0/1] quit
```

#ルーターがインターネットに到達できるようにデフォルトルートを設定します。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 20.2.2.2
```

### デバイス(ファイアウォール)の設定

ファイアウォールを監視および管理するための IMC サーバーの SNMP の設定

#SNMP エージェントを有効にします。

```
<Device> system-view
```

```
[Device] snmp-agent
```

#すべての SNMP バージョンを有効にし、読み取り専用コミュニティ public と読み取りおよび書き込みコミュニティ private を作成します。

```
[Device] snmp-agent sys-info version all
```

```
[Device] snmp-agent community read public
```

```
[Device] snmp-agent community write private
```

## ファイアウォールに設定を発行するための IMC サーバーの NETCONF over SOAP の設定

#NETCONF over SOAP over HTTP を有効にします。

```
[Device] netconf soap http enable
```

#NETCONF over SOAP over HTTPS を有効にします。

```
[Device] netconf soap https enable
```

## ファイアウォールが IMC RESTful サーバーと通信するための RESTful の有効化

#RESTful over HTTP を有効にします。

```
[Device] restful http の有効化
```

#HTTPS 経由の RESTful を有効にします。

```
[Device] restful https 有効
```

## インターフェイスへの IP アドレスの割り当ておよびインターフェイスのセキュリティゾーンへの追加

1. IP アドレス 192.168.100.88 を GigabitEthernet1/0/1 に割り当て、インターフェイスをゾーン DMZ に追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

A) **Basic Configuration** タブで、**DMZ**セキュリティゾーンを選択します。

B) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。  
この例では、**192.168.100.88/24**と入力します。

**図32 セキュリティゾーン DMZ へのインターフェイスの追加**

**Modify Interface Settings** [?] [X]

Name: GE1/0/1

Link status:  Up  Shut down

Description: GigabitEthernet1/0/1 Interface

Link mode: Layer 3 mode

Basic Configuration | **IPv4 Address** | IPv6 Address | Physical Interface Configuration

Add an interface to a security zone: DMZ

VRF: Public network

Speed: autonegotiation

Duplex mode: autonegotiation

MAC address: 74-1F-4A-80-DA-69

MTU: 1500 (46-1560)

Expected bandwidth: <1-400000000> (kbps)

Apply OK Cancel

図33 インターフェイスの IP アドレスとマスクの設定

The screenshot shows the 'Modify Interface Settings' window for interface GE1/0/1. The 'IPv4 Address' tab is selected. The 'IP address' is set to 192.168.100.88 with a mask of 255.255.255.0. The 'Link status' is 'Up'. The 'Last hop holding' is set to 'Disable'. The 'IP address' is set to 'Manual assignment'. The 'Gateway' field is empty. A secondary IP configuration table is visible with columns for 'Secondary IP ad...', 'Mask length', and 'Edit'. The 'Apply', 'OK', and 'Cancel' buttons are at the bottom.

#OK をクリックします。

2. GigabitEthernet1/0/2およびGigabitEthernet1/0/3は、GigabitEthernet1/0/1と同じ方法で設定します。
  - IP アドレス 20.2.2.2 を GigabitEthernet1/0/2 に割り当て、インターフェイスをゾーン Trust に追加します。
  - IP アドレス 12.1.1.1 を GigabitEthernet1/0/3 に割り当て、インターフェイスをゾーン Untrust に追加します。

## ファイアウォールのネットワーク接続を保証するための IP ルーティングの設定

1. ファイアウォールとユーザーが互いに到達できるように、スタティックルートを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > Static Routing** を選択します。

#**IPv4 Static Routing** タブで、**Create** をクリックします。

#開いたダイアログボックスで、IPv4 スタティックルートを設定します。

- **Destination address** フィールドに **20.2.1.0** と入力します。
- **Mask length** フィールドに **24** と入力します。
- **Next hop** フィールドにネクストホップアドレスとして 20.2.2.1 を入力します。

図34 IPv4スタティックルートの作成

The screenshot shows a dialog box titled "Create IPv4 Static Route". It contains the following fields and values:

- VPN instance: Public network
- Destination address: 20.2.1.0
- Mask length: 24
- Next hop:  Next hop VRF instance,  Output interface, Next hop address: 20.2.2.1
- Preference: 60
- Route tag: 0
- Description: (empty)

Buttons: OK, Cancel

#OK をクリックします。

2. ファイアウォールがインターネットに到達できるように、デフォルトルートを設定します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Routing > Static Routing** を選択します。

#IPv4 Static Routing タブで、**Create** をクリックします。

#開いたダイアログボックスで、IPv4 スタティックルートを設定します。

- **Destination address** フィールドに 0.0.0.0 と入力します。
- **Mask length** フィールドに 0 と入力します。
- **Next hop** フィールドにネクストホップアドレスとして 12.1.1.2 を入力します。

インターネットのファイアウォールに接続するデバイスの IP アドレスをネクストホップアドレス

として指定します。この例では、ネクストホップアドレスは 12.1.1.2 です。

図35 IPv4 スタティックルートの作成

Create IPv4 Static Route

VPN instance: Public network

Destination address: 0.0.0.0 \*

Mask length: 0 \*(0-32)

Next hop ?

Next hop VRF instance

Output interface

Next hop address: 12.1.1.2 \*

Preference ? : 60 (1-255. Default: 60.)

Route tag ? : 0 (0-4294967295. Default: 0.)

Description: (1-60 chars)

OK Cancel

#OK をクリックします。

## 管理者 admin への HTTP サービスの割り当て

#トップナビゲーションバーで、**System** をクリックします。

#ナビゲーションペインで、**Administrators > Administrators** を選択します。

#管理者 admin 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、HTTP サービスを選択します(図36を参照)。

図36 管理者情報の変更

Username: admin (1-55 chars)

Password: (1-63 chars)

Confirm: (1-63 chars)

User role: network-admin

User group: system

Services:  Terminal  SSH  HTTPS  FTP  
 Telnet  PAD  HTTP

Max concurrent logins: (1-1024)

FTP directory: cfa0:

Advanced settings ?

OK Cancel

#OK をクリックします。

## ファイアウォールと IMC サーバー間のネットワーク接続を確保するためのセキュリティポリシーの設定

ファイアウォールが IMC サーバーから ID ユーザー情報をインポートできるようにするには、この項の作業を実行します。

1. ゾーン DMZ からゾーン Local へのトラフィックを許可するセキュリティポリシー dmz-local を作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

#**Create > Create a policy** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを次のように設定します。

- セキュリティポリシー名を dmz-local に設定します。
- Source zone フィールドからセキュリティゾーン DMZ を選択します。
- Destination zone フィールドから security zone Local を選択します。
- アクションを **permit** に設定します。

#OK をクリックします。

2. セキュリティポリシー dmz-local を作成するのと同じ方法で、ゾーン Local からゾーン DMZ へのトラフィックを許可するには、セキュリティポリシー local-dmz を作成します。

## ゾーン信頼とゾーン DMZ 間のトラフィックを許可するセキュリティポリシーの設定

ポータルユーザーはゾーン信頼に属し、IMC RADIUS サーバーはゾーン DMZ に属しています。NAS がユーザーおよび IMC サーバーの AAA およびポータル認証パケットを送受信できるようにするには、セキュリティポリシー trust-dmz を作成して、ゾーン信頼とゾーン DMZ 間のトラフィックを許可します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#Create>Create a policy をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを次のように設定します。

- セキュリティポリシー名を trust-dmz に設定します。
- Source zone フィールドからセキュリティゾーン Trust および DMZ を選択します。
- Destination zone フィールドからセキュリティゾーン Trust および DMZ を選択します。
- アクションを **permit** に設定します。

#OK をクリックします。

## RADIUS スキーム rs1 の設定

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**User > Authentication > RADIUS** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、RADIUS 認証サーバーと RADIUS アカウンティングサーバーを作成し、詳細設定を行います(図37および図38を参照)。

図37 RADIUS スキームの作成(認証サーバー)

Scheme name  \* (1-32 chars)

**Authentication servers**

Primary server

<input type="checkbox"/>	VRF	IP version	IP address	Port	Shared key	Status	Edit
<input type="checkbox"/>	Public netw	IPv4 address	192.168.100.244	1812	admin	Active	<input type="button" value="Edit"/>

Secondary servers

<input type="checkbox"/>	VRF	IP version	IP address	Port	Shared key	Status	Edit
<input type="checkbox"/>							

Global shared key for authentication  (1-64 chars)

図38 RADIUSスキームの作成(アカウンティングサーバー)

**Accounting servers**

Primary server

[+](#) Create [X](#) Delete

<input type="checkbox"/>	VRF	IP version	IP address	Port	Shared key	Status	Edit
<input type="checkbox"/>	Public netw	IPv4 address	192.168.100.244	1813	admin	Active	

Secondary servers

[+](#) Create [X](#) Delete

<input type="checkbox"/>	VRF	IP version	IP address	Port	Shared key	Status	Edit
--------------------------	-----	------------	------------	------	------------	--------	------

Global shared key for accounting [?](#)  (1-64 chars)

**図39 RADIUSスキームの作成(詳細設定)**

**Advanced settings**

Source IPv4 address for outgoing RADIUS packets  [?](#)

Source IPv6 address for outgoing RADIUS packets  [?](#)

Server response timeout  seconds (1-10. Default: 3.)

Max RADIUS packet transmission attempts  (1-20. Default: 3.)

Server quiet timer  minutes (1-255. Default: 5.)

Real-time accounting timer   (0-71582. Default: 720.)

Max real-time accounting attempts  (1-255. Default: 5.)

Format of usernames sent to servers  [?](#)

Data flow measurement unit  [?](#)

Packet measurement unit  [?](#)

Online user password change  Enable [?](#)

#OK をクリックします。

## 認証ドメイン dm1 の構成

#トップナビゲーションバーで、**Objects** 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。

#開いたダイアログボックスで、ポータルユーザーのアクセスタイプと AAA 方式を設定します(図40および図41を参照)。

図40 ISPドメイン dm1(アクセスタイプ)の追加

Add ISP Domain

Domain name  \* (1-255 chars)

Status

Access types  Login  LAN access  Portal  ADVPN

図41 ISPドメイン dm1 の追加(ポータルユーザー用の AAA 方式)

Add ISP Domain

RADIUS scheme

Accounting methods  RADIUS  Local  None

RADIUS scheme

AAA methods for portal users

Authentication methods  RADIUS  Local  None

RADIUS scheme

Authorization methods  RADIUS  Local  None

RADIUS scheme

Accounting methods  RADIUS  Local  None

RADIUS scheme

AAA methods for ADVPN users

Authentication methods  RADIUS  Local  None

RADIUS scheme

Authorization methods  RADIUS  Local  None

OK Cancel

#OK をクリックします。

## ポータル認証の設定

### 1. ポータル認証サーバーの構成:

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**User > Access Control > Portal** を選択します。

#**Portal Authentication Servers** タブで、**Create** をクリックします。

#開いたダイアログボックスで、ポータル認証サーバーを設定します。

- サーバー名 newpt を入力します。
- IP アドレスを 192.168.100.244 に設定します。
- key を admin と入力します。
- ポートを 50100 に設定します。

図42 ポータル認証サーバーの作成

Create Portal Authentication Server

Server name: newpt \*(1-32 chars)

IP address: 192.168.100.244 (Example: 192.168.0.1 or 1::1:1:1)

VRF: (1-31 chars)

Key: admin (1-64 chars)

Port: 50100 (1-65534, Default: 50100)

Server detection  Enable  Disable

Timeout: 60 seconds (10-3600, Default: 60)

Action\*  Log  Trap

User synchronization  Enable  Disable

User sync interval: 1200 seconds (60-18000, Default: 1200)

Apply Cancel

#OK をクリックします。

2. ポータルWebサーバーを構成します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**User > Access Control > Portal** を選択します。

#Portal Web Servers タブをクリックします。

#**create** をクリックします。

#表示されるダイアログボックスで、サーバー名と URL を設定します(図43を参照)。この例では、URL は `http://192.168.100.244:8080/portal` です。

図43 ポータル Web サーバーの作成

Server name: newpt (1-32 chars)

URL: http://192.168.100.244:8080/portal (1-256 chars)

VRF: (1-31 chars)

Server detection:  Enable  Disable

Detection interval: 5 seconds (1-1200. Default: 5)

Max detection attempts: 3 (1-10. Default: 3)

Action:  Log  Trap

**Parameters added to URL**

The device adds the parameters to the portal Web server redirection URL to send the related information to the portal Web server.

Create  Delete

Type	Parameter name	Custom parameter
------	----------------	------------------

OK Cancel

#OK をクリックします。

3. インターフェイスポータルポリシーを設定し、GE1/0/2でIPv4ポータルをイネーブルにします。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**User > Access Control > Portal** を選択します。

#**Interface Portal Policies** タブをクリックします。

#**create** をクリックします。

#表示されるダイアログボックスで、インターフェイスポータルポリシーを設定します(図44を参照)。

図44 インターフェイスポータルポリシーの作成

Interface: GE1/0/2

IPv4 portal

Portal authentication:  Enable  Disable

Authentication mode: Cross-subnet

Portal Web server: newpt

Authentication domain: dm1

Max number of users: (1-4294967295)

Fail-permit feature:  Enable  Disable

Portal Web server fail-permit:  Enable  Disable

Portal authentication server fail-permit: None

BAS-IP: (Example: 192.168.32.2)

Pre-auth address pool: (1-63 chars)

Online user detection:  ARP detection  ICMP detection  Disable

Max detect attempts: 3 (1-10. Default: 3)

Detection interval: 3 seconds (1-1200. Default: 3)

OK Cancel

#OK をクリックします。

## ユーザーID の構成

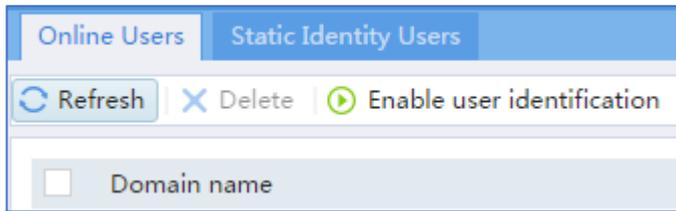
1. ユーザーIDを有効にする:

#トップナビゲーションバーで、**Objects** 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。

#**Online Users** タブで、**Enable user identification** をクリックします。

図45 ユーザーIDの有効化



## 2. RESTful サーバーrest1 の作成:

#トップナビゲーションバーで、**Objects** 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。

#開いたダイアログボックスで、RESTful サーバーの次のパラメータを設定します。

- サーバー名 rest1 を入力します。
- username admin と入力します。
- password admin と入力します。
- Get-user-account URI を `http://192.168.100.244:8080/imcrs/ssm/imcuser/accessUser` に設定します。
- Get-user-group URI を `http://192.168.100.244:8080/imcrs/ssm/imcuser/accessUserGroup` に設定します。



IMC RESTfulサーバーの場合、URIは固定形式です。IPアドレス以外の上記のURIのパラメータは変更できません。

図46 RESTful サーバーの作成

Name	rest1	(1-31 chars)
Username	admin	(1-55 chars)
Password	.....	(1-63 chars)
Get-user-account URI	URI: http://192.168.100.244:8080/imcrs/ssm/ir	(1-255 chars)
Get-online-user URI		(1-255 chars)
Get-user-group URI	http://192.168.100.244:8080/imcrs/ssm/imcuse	(1-255 chars)
Put-online-user URI		(1-255 chars)
Put-offline-user URI		(1-255 chars)
VRF	Public network	
Enable server detection	<input type="checkbox"/>	

OK Cancel

#OK をクリックします。

3. ユーザーインポートポリシーimc の作成:

#トップナビゲーションバーで、**Objects** 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。

#表示されるダイアログボックスで、ユーザーインポートポリシーのパラメータを設定します(図47を参照)。

図47 ユーザーインポートポリシーimcの作成

Create User Import Policy

Name: imc \* (1-31 chars)

RESTful server: rest1

LDAP schemes: Select LDAP schemes [Edit]

Import types: User and user group

Enable auto import:

Import interval: 1 hours (1-65535)

OK Cancel

#OK をクリックします。

#ファイアウォールと IMC サーバーが相互に通信できるようになったら、User Import Policies ページに移動し、ポリシーimc の Manually import identity users アイコンをクリックして、IMC サーバーのユーザーカウントをファイアウォールにインポートします。

図48 ユーザーカウントのインポート

<input checked="" type="checkbox"/>	Policy name	RESTful server	LDAP schemes	Import types	Auto import interval	Auto import	Manually import iden...	Manually import onli...	Edit
<input checked="" type="checkbox"/>	imc	rest1		User and user group	1	Enabled			

## ユーザーuser10003 がインターネットにアクセスできるようにセキュリティポリシーを設定する

セキュリティポリシーuser10003 を作成して、ユーザーuser10003 がインターネットにアクセスできるようにし、インターネットからのユーザーが内部ネットワークにアクセスできないようにします。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#Create>Create a policy をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを次のように設定します。

- セキュリティポリシー名を user10003 に設定します。

- Source zone フィールドから security zone Trust を選択します。
- Destination zone フィールドから security zone Untrust を選択します。
- アクションを許可に設定します。
- user user10003 を選択します。

#OK をクリックします。

## IMC へのファイアウォールの追加

#ファイアウォールを IMC に追加して、IMC がファイアウォールを監視および管理できるようにします。

1. IMCにログインします。

#Web ブラウザのアドレスバーに IMC の URL を入力します。この例では、URL は http://192.168.100.244:8080/imc/です。

#username admin と password admin を入力します。

2. ファイアウォールをIMCに追加します。

#Resource タブをクリックします。

#ナビゲーションツリーで、**Resource Management > Add Device** を選択します。

#開いたページで、に示すようにパラメータを設定します。

- Telnet Settings 領域で、ユーザー名とパスワードを admin に設定します。
- 他のパラメータにはデフォルト値を使用します。
- デフォルトでは、読み取り専用 SNMP コミュニティストリングは public、読み取りおよび書き込み SNMP コミュニティストリングは private です。

図49 IMC へのファイアウォールの追加

Resource > Add Device

Basic Information

Host Name/IP \* 192.168.100.88

Device Label

Mask ?

Device Group ?

Login Type Telnet ?

Automatically register to receive SNMP traps from supported devices

Support Ping Operation ?

Add the device regardless of the ping result ?

Use the loopback address as the management IP

+ SNMP Settings

- Telnet Settings

Configure

Authentication Mode	Username + Password
Username	admin
Password	*****
Timeout (seconds)	4

+ SSH Settings

OK Cancel

#OK をクリックします。

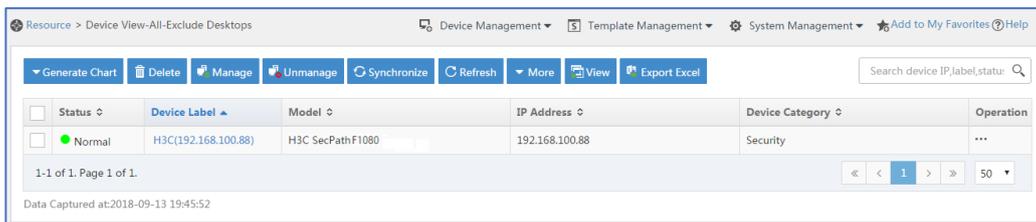
3. NETCONF設定の変更:

#Resource タブをクリックします。

#ナビゲーションツリーで、View Management > Device View を選択します。

#ターゲットデバイスの Device label 列のリンクをクリックします。

図50 デバイスリスト

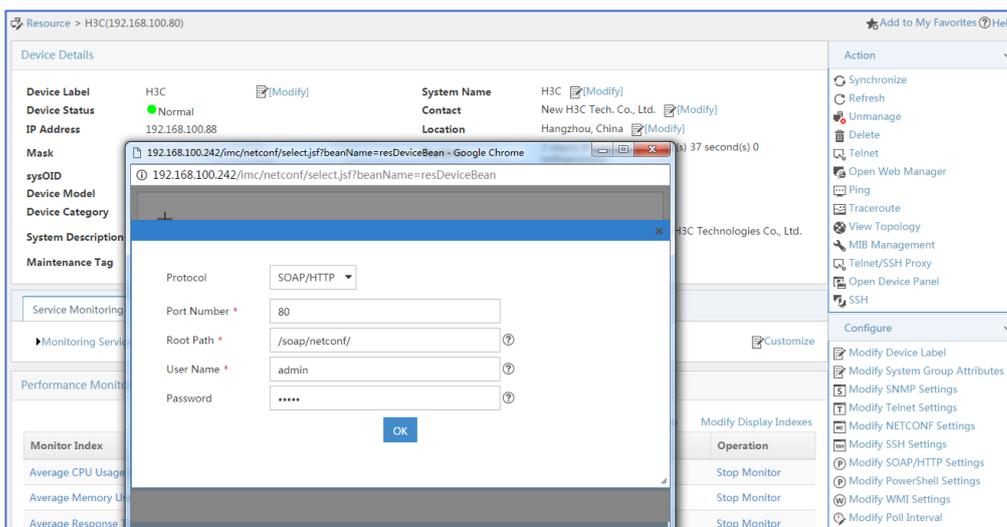


#右ペインで、**Configure > Modify NETCONF Settings** をクリックします。

#表示されるダイアログボックスで、プラス記号(+)をクリックしてプロトコルを追加します(図51を参照)。

この例では、ユーザー名とパスワードを admin に設定します。

図51 NETCONF 設定の変更



#OK をクリックします。

## セキュリティサービス(IMC)の設定

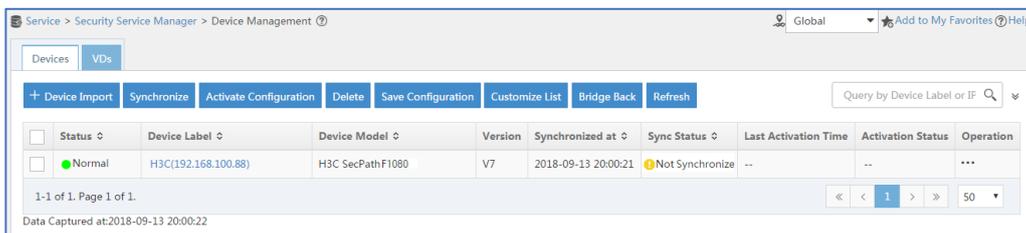
1. ファイアウォールからIMCサーバーへのセキュリティサービスを同期して、ファイアウォールとIMCサーバーの間で設定とユーザー情報が一貫していることを確認します。

#service タブをクリックします。

#ナビゲーションツリーで、**Security Service Manager > Device Management** を選択します。

#Devices タブのデバイスリストにファイアウォールが表示されます(図52を参照)。

図52 セキュリティデバイス管理ページ(非同期)



#デバイスリストでファイアウォールを選択し、Synchronize をクリックします。Sync Status 列から同期ステータスを表示できます(図53および図54を参照)。

同期処理に時間がかかる場合があります。しばらくお待ちください。

図53 セキュリティデバイス管理(同期化)ページ

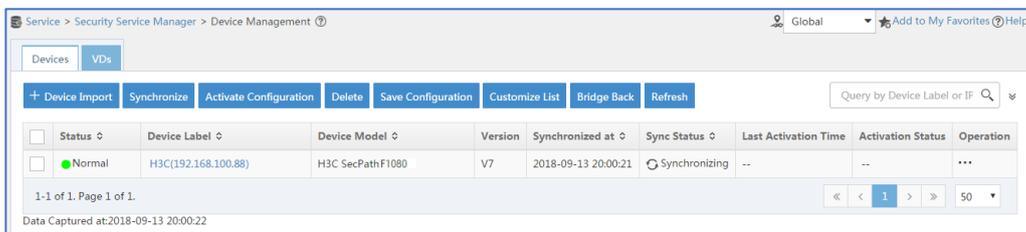
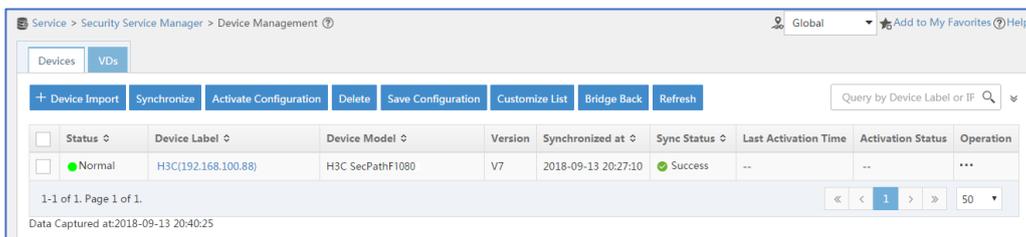


図54 セキュリティデバイス管理ページ(同期成功)



2. ユーザー認証システムパラメータおよびユーザー通知パラメータを設定して、IMCサーバーがユーザーのオンラインおよびオフライン情報をファイアウォールにリアルタイムで同期できるようにします。

#service タブをクリックします。

#ナビゲーションツリーで、Security Service Manager>Global Parameters を選択します。

#ユーザー認証システムパラメータを設定します(図55を参照)。

ポータル認証サーバーのプロトコルに応じてプロトコルを選択します。ユーザー名とパスワードがIMCサーバーへのログインに使用したのと同じであることを確認してください。

図55 ユーザー認証システムパラメーターの構成

User Authentication System Parameters

Enable \*  No  Yes

Access Type \* EIA

Protocol \*  HTTP  HTTPS

Authentication System Address \* 127.0.0.1

Port Number \* 8080

Username \* admin

Password \* .....

#OK をクリックします。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy > Service Parameters>System Settings** を選択します。

#ユーザー通知 user notification parameters の Configure アイコンをクリックします。

#開いたページで、**add** をクリックします。

#Add User Notification ページで、図56に示すようにパラメータを設定します。この例では、共有キーをランダムに入力できます。

図56 ユーザー通知パラメーターの構成

User > User Access Policy > Service Parameters > System Settings > User Notification Parameters > Add User Notification

Add User Notification

Notification Type  RADIUS  SYSLOG  UDP  Proprietary  Custom

Server IP Address \* 127.0.0.1

Server Port \* 11812

Share Key \* .

Confirm Shared Key \* .

#OK をクリックします。

## RADIUS サーバー(IMC)の設定

1. ファイアウォールをアクセスデバイスとしてIMCサーバーに追加します。

#**user** タブをクリックします。

#ナビゲーションツリーから、User Access Policy>Access Device Management>Access Device を選択します。

#**add** をクリックします。

#Access Configuration 領域で、共有キーを admin に設定します(を参照)。

#Device List 領域で、Select または Add Manually をクリックして、192.168.100.88 のデバイスをアクセスデバイスとして追加します。

サーバー上のアクセスデバイスの IP アドレスとして、ファイアウォール上の発信 RADIUS パケットの送信元 IP アドレスを指定する必要があります。

ファイアウォールでは、送信元 IP アドレスは nas-ip または radius nas-ip コマンドを使用して構成されます。nas-ip コマンドを使用して構成された IP アドレスは、radius nas-ip コマンドを使用して構成された IP アドレスよりも優先順位が高くなります。送信元 IP アドレスとして IP アドレスが指定されていない場合、パケット送信インターフェイスの IP アドレスが送信元 IP アドレスとして使用されます。この例では、パケット送信インターフェイスの IP アドレス 192.168.100.88 が使用されます。

図57 アクセスデバイスの追加

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port \* 1812      Accounting Port \* 1813

Service Type Unlimited      Forcible Logout Type Disconnect user

Access Device Type H3C (General)      Service Group Ungrouped

Shared Key \* \*\*\*\*\*      Confirm Shared Key \* \*\*\*\*\*

Access Device Group --

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
Device	192.168.100.88			🗑️

Total Items: 1.

OK Cancel

#OK をクリックします。

2. アクセスポリシーを追加します。

#**user** タブをクリックします。

#ナビゲーションツリーから、User Access Policy>Access Policy を選択します。

#追加をクリックします。

#Add Access Policy ページで、アクセスポリシー名を Portal に設定します(図58を参照)。

図58 アクセスポリシーの追加

User > User Access Policy > Access Policy > Add Access Policy Help

Basic Information -

Access Policy Name \* Portal

Service Group \* Ungrouped

Description

Authorization Information +

Authentication Binding Information +

User Client Configuration +

OK Cancel

#OK をクリックします。

3. アクセスサービスを追加します。

#user タブを選択します。

#ナビゲーションツリーから、User Access Policy>Access Service を選択します。

#追加をクリックします。

#Add Access Service ページで、サービス名を Portal に設定し、Default Access Policy リストから Portal を選択します。

図59 アクセスサービスの追加

User > User Access Policy > Access Service > Add Access Service Help

Basic Information -

Service Name \* Portal

Service Group \* Ungrouped

Default Proprietary Attribute Assignment Policy \* Do not use ?

Default Max. Devices for Single Account \* 0 ?

Daily Max. Online Duration \* 0 ?

Description

Available ?

Service Suffix

Default Access Policy \* Portal

Default Max. Number of Online Endpoints \* 0 ?

Transparent Authentication ?

Access Scenario List +

OK Cancel

#OK をクリックします。

#### 4. アクセスユーザーの追加:

#user タブをクリックします。

#ナビゲーションツリーから、Access User>All Access Users を選択します。

#追加をクリックします。

#Add Access User ページで、パラメータを設定します(を参照)。

- User Name フィールドに user と入力します。
- Account Name フィールドに user10001 と入力します。
- Password フィールドと Confirm Password フィールドに admin と入力します。
- Access Service 領域で Portal を選択します。

図60 アクセスユーザーの追加

Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/> Portal		Available	

#OK をクリックします。

#ユーザーカウント user10002 と user10003 を、ユーザーカウント user10001 を追加するのと同じ方法で追加します。

## ポータルサーバー(IMC)の設定

### 1. ポータルサーバーを構成します。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy > Portal Service>Server** を選択します。

#図61でネットワークの状態に応じてパラメータを設定します。この例では、デフォルト値が使用されています。

**図61 ポータルサーバー構成**

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level \* Info

Bind IP Group to Port Groups Deny

Portal Server

Request Timeout (Seconds) \* 4 Server Heartbeat Interval (Seconds) \* 20

User Heartbeat Interval (Minutes) \* 5 LB Device Address

Portal Web

Request Timeout (Seconds) \* 15 Packet Code

Verify Endpoint Requests Yes Use Cache No

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://192.168.100.244:8080/portal/  
https://192.168.100.244:8443/portal/

#OK をクリックします。

## 2. IPグループを追加します。

#user タブをクリックします。

#ナビゲーションツリーから、**User Access Policy>Portal Service>IP Group** を選択します。

#add をクリックします。

#Add IP Group ページで、IP グループパラメータを設定します(図62を参照)。

**図62 IP グループの追加**

User > User Access Policy > Portal Service > IP Group > Add IP Group ? Help

### Add IP Group

IP Group Name \*

Start IP \*

End IP \*

Service Group

Action \*

#OK をクリックします。

- ポータルデバイスを追加します。

#user タブをクリックします。

#ナビゲーションツリーで、**User Access Policy > Portal Service>Device** を選択します。

#add をクリックします。

#Add Device ページで、キーを admin に設定し、その他のパラメータを設定します(図63を参照)。

**図63 ポータルデバイス構成の追加**

User > User Access Policy > Portal Service > Device > Add Device

### Add Device

Device Information

Device Name \*  IP Address \*

Key \*  Confirm Key \*

Advanced Information

Listening Port \*  Local Challenge \*

Authentication Retries \*  Logout Retries \*

Support Server Heartbeat \*  Support User Heartbeat \*

Version \*  Service Group \*

Access Method \*

Device Description

#OK をクリックします。

- ポータルデバイスをIPグループに関連付けます。

#user タブをクリックします。

#ナビゲーションツリーで、**User Access Policy > Portal Service > Device** を選択します。

#ファイアウォールの Operation 列で Port Group アイコンをクリックします。

図64 デバイスリスト

The screenshot shows the 'Query Devices' interface. At the top, there is a breadcrumb trail: 'User > User Access Policy > Portal Service > Device'. Below this is a search area with fields for 'Device Name', 'Version', 'Deploy Result', 'Service Group', 'Device IP Address Range From', and 'To'. There are 'Query' and 'Reset' buttons. Below the search area is an 'Add' button. The main part of the interface is a table with the following columns: 'Device Name', 'Version', 'Service Group', 'IP Address', 'Last Deployed at', 'Deploy Result', and 'Operation'. The table contains one row with the following data: 'Device', 'Portal 2.0', 'Ungrouped', '192.168.100.88', an empty cell, 'Not Deployed', and an 'Operation' column containing three icons (a red square icon, a refresh icon, and a delete icon). At the bottom of the table, there is a pagination control showing '1-1 of 1. Page 1 of 1.' and a dropdown menu set to '50'.

#開いたページで、**add** をクリックします。

#開いたページで、ポートグループを設定します(図65を参照)。

図65 ポートグループの追加

The screenshot shows the 'Add Port Group' configuration form. The breadcrumb trail is 'User > User Access Policy > Portal Service > Device > Configure Port Group > Add Port Group'. The form is divided into two sections: 'Basic Information' and 'Advanced Information'. In the 'Basic Information' section, there are fields for 'Port Group Name' (Portal-user), 'Authentication Type' (PAP), 'Transparent Authentication' (Not Supported), 'IP Group' (Portal-user), 'Page Push Policy', and 'Default Authentication Page' (PC - Default Web Login(PC)). There is an 'Add' button next to the 'IP Group' field. In the 'Advanced Information' section, there are fields for 'Protocol' (HTTP), 'NAT or Not' (No), 'Language' (English), 'Heartbeat Interval (Minutes)' (0), 'User Domain', 'Quick Authentication' (No), 'Error Transparent Transmission' (Yes), 'Client Protection Against Cracks' (No), and 'Heartbeat Timeout (Minutes)' (0). There is also a 'Port Group Description' field. At the bottom of the form, there are 'OK' and 'Cancel' buttons.

#OK をクリックします。

## ホストの構成

#各ホストの IP アドレス、ネットワークマスクおよびデフォルトゲートウェイ設定を構成します。

ホストがネットワーク内のデバイスと通信できることを確認します(詳細は省略)。

## 設定の確認

1. ホスト上で、ユーザーがポータル認証を通過できることを確認します。

#ポータル認証ページにログインするために、Web ブラウザのアドレスバーにポータル Web サーバーの URL を入力します。この例では、URL は `http://192.168.100.244:8080/portal` です。

#ユーザー名とパスワードを入力します。

#Log in をクリックします。

#ユーザーがポータル認証に合格したことを確認します。

図66 ポータル認証成功ページ



2. IMC サーバーで、ユーザー `user10001`、`user10002` および `user10003` がポータル認証に合格した後、オンラインユーザーリストにあることを確認します。オンラインユーザーリストを表示するには、`user` タブをクリックし、ナビゲーションツリーから `Access User > Online user` を選択します。
3. ファイアウォールで、すべてのポータルユーザーに関する情報を表示します。

```
[Device] display portal user all
```

```
Total portal users: 3
```

```
Username: user10001
```

```
Portal server: newpt
```

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0011-95e4-4aa9	20.2.1.13	--	GigabitEthernet1/0/2

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

Username: user10002

Portal server: newpt

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0011-95e4-4aa3	20.2.1.13	--	GigabitEthernet1/0/2

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

Username: user10003

Portal server: newpt

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0011-95e4-4aa2	20.2.1.13	--	GigabitEthernet1/0/2

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A  
Inbound CAR: N/A  
Outbound CAR: N/A

4. ファイアウォールで、IDユーザー情報を表示します。

#すべての ID ユーザーに関する情報を表示します。

```
[Device] display user-identity all user
```

User ID	Username
0x2	user10001
0x3	user10002
0x4	user10003

#オンライン ID ユーザーuser10001 に関する情報を表示します。

```
[Device] display user-identity online-user null-domain name user10001
```

```
User name: user10001  
IP : 20.2.1.11  
MAC : 0011-95e4-4aa9  
Type: Dynamic
```

Total 1 records matched.

#オンライン ID ユーザーuser10002 に関する情報を表示します。

```
[Device] display user-identity online-user null-domain name user10002
```

```
User name: user10002  
IP : 20.2.1.12  
MAC : 0011-95e4-4aa3  
Type: Dynamic
```

Total 1 records matched.

#オンライン ID ユーザーuser10003 に関する情報を表示します。

```
[Device] display user-identity online-user null-domain name user10003
```

```
User name: user10003  
IP : 20.2.1.13  
MAC : 0011-95e4-4aa2  
Type: Dynamic
```

Total 1 records matched.

5. ファイアウォールがユーザーに対してIDベースのアクセスコントロールを実行できることを確認します。

#ユーザーuser10001 がインターネットのどのホストにも ping できないことを確認します。この例では、ユーザーは 12.1.1.2 のホストに ping します。

```
C:¥>ping 12.1.1.2
```

Pinging 12.1.1.2 with 32 bytes of data:

Request time out.

Request time out.

Request time out.

Request time out.

Ping statistics for 12.1.1.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

#ユーザーuser10003 がインターネットのホストに ping できることを確認します。この例では、ユーザーは 12.1.1.2 でホストに ping します。

C:¥>ping 12.1.1.2

Pinging 12.1.1.2 with 32 bytes of data:

Reply from 12.1.1.2: bytes=32 time=36ms TTL=253

Reply from 12.1.1.2: bytes=32 time<1ms TTL=253

Reply from 12.1.1.2: bytes=32 time<1ms TTL=253

Reply from 12.1.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 12.1.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 36ms, Average = 9ms

#ユーザーuser10003 がインターネットのホストに ping を実行すると、ファイアウォールは次のメッセージを生成します。

[Device]%Nov 6 10:19:53:920 2017 H3C FILTER/6/FILTER\_ZONE\_EXECUTION\_ICMP:

-Context

=1;

SrcZoneName(1025)=Trust;DstZoneName(1035)=Untrust;Type(1067)=ACL;SecurityPolicy(1072)=user10003;RuleID(1078)=3;Protocol(1001)=ICMP;SrcIPAddr(1003)=20.2.1.13;Src

```
MacAddr(1021)=7425-8a37-  
b5f6;DstIPAddr(1007)=12.1.1.2;IcmpType(1062)=ECHO(8);Icm  
pCode(1063)=0;MatchCount(1069)=1;Event(1048)=Permit;
```

## 構成ファイル

### ルーター

```
Router  
[Router] display current-configuration  
#  
interface GigabitEthernet0/0  
port link-mode route  
ip address 20.2.1.1 255.255.255.0  
#  
interface GigabitEthernet0/1  
port link-mode route  
ip address 20.2.2.1 255.255.255.0  
#  
interface GigabitEthernet3/0  
port link-mode route  
combo enable copper  
#  
ip route-static 0.0.0.0 0 20.2.2.2  
#  
snmp-agent  
snmp-agent local-engineid 800063A28074258A37B5F500000001  
snmp-agent community write private  
snmp-agent community read public  
snmp-agent sys-info version all  
#  
local-user admin class manage  
password hash $h$6$UblhNnPeVyKUwfpml$Qr3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh  
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==  
service-type telnet http  
authorization-attribute user-role network-admin  
#  
return
```

### デバイス

```
[Device] display current-configuration
```

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.100.88 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.2.2.2 255.255.255.0
 portal enable method direct
 portal domain dm1
 portal apply web-server newpt
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name DMZ
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/3
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
ip route-static 0.0.0.0 0 12.1.1.2
ip route-static 20.2.1.0 24 20.2.2.1
#
snmp-agent
snmp-agent local-engineid 800063A280487ADA9593B700000001
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 192.168.100.244 params securityn
ame public v2c
#
radius scheme rs1
 primary authentication 192.168.100.244
 primary accounting 192.168.100.244
 key authentication cipher $c$3$hhbEbD5Ycvw7VWqIjAoMoU7hQRgcUjtg
 user-name-format without-domain
#
domain dm1

```

```

authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
domain system
#
domain default enable system
#
local-user admin class manage
password hash $h$6$UblhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
service-type ssh telnet terminal http https
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
portal web-server newpt
url http://192.168.100.244:8080/portal
#
portal server newpt
ip 192.168.100.244 key cipher $c$3$+UmaGOco7eHsjOqlrp8II4eYe0A8NpYU
#
netconf soap http enable
netconf soap https enable
restful http enable
restful https enable
#
user-identity enable
user-identity user-account auto-import policy imc
#
user-identity restful-server rest1
login-name admin password cipher $c$3$phGy00HA6OP6pIpGI0KOKZEOPuLVbtt/
uri get-user-database http://192.168.100.244:8080/imcrs/ssp/imcuser/accessUser
uri get-user-group-database http://192.168.100.244:8080/imcrs/ssp/imcuser/acces
sUserGroup
uri get-online-user http://192.168.100.244:8080/imcrs/ssp/imcuser/onlineUser
uri put-online-user http://192.168.100.244:8080/imcrs/ssp/imcuser/uploadOnlineU
ser
uri put-offline-user http://192.168.100.244:8080/imcrs/ssp/imcuser/uploadOfflin
eUser
#
user-identity user-import-policy imc
account-update-interval 1
restful-server rest1
#
security-policy ip
rule 0 name dmz-local

```

```
action pass
source-zone dmz
destination-zone local
rule 1 name local-dmz
action pass
source-zone local
destination-zone dmz
rule 2 name trust-dmz
action pass
source-zone trust
source-zone dmz
destination-zone dmz
destination-zone trust
rule 3 name user10003
action pass
logging enable
source-zone trust
destination-zone untrust
user user10003
#
return
```

# SSL 復号化の設定例

## はじめに

次に、SSL 復号化の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

以下の情報は、SSL 復号化に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

SSL 復号化を設定する場合は、セキュリティポリシーでセキュリティゾーンとローカルセキュリティゾーン間の通信が許可されていることを確認してください。

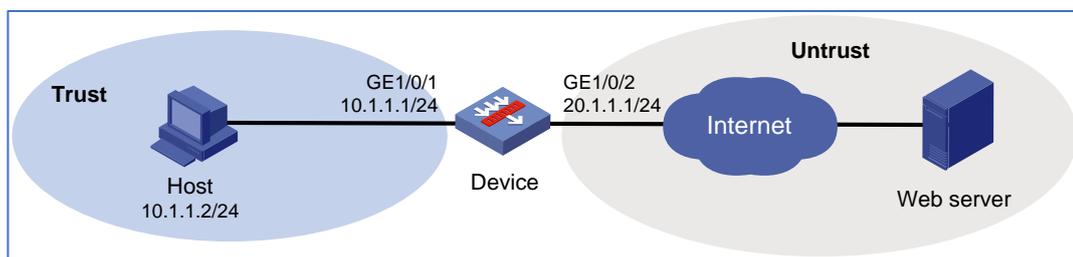
SSL 復号化を設定すると、IPS キャプチャアクションは無効になります。

## 例:SSL復号化の設定

### ネットワーク構成

図1に示すように、デバイスは企業のセキュリティゲートウェイとして動作します。デバイスは SSL 暗号化パケット(HTTPS パケットなど)を検査できず、パケット内のセキュリティ脅威をマスクします。内部ネットワークセキュリティを向上させるには、デバイス上で SSL 復号化を設定して HTTPS パケットを復号化し、ディープパケットインスペクションを実行します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

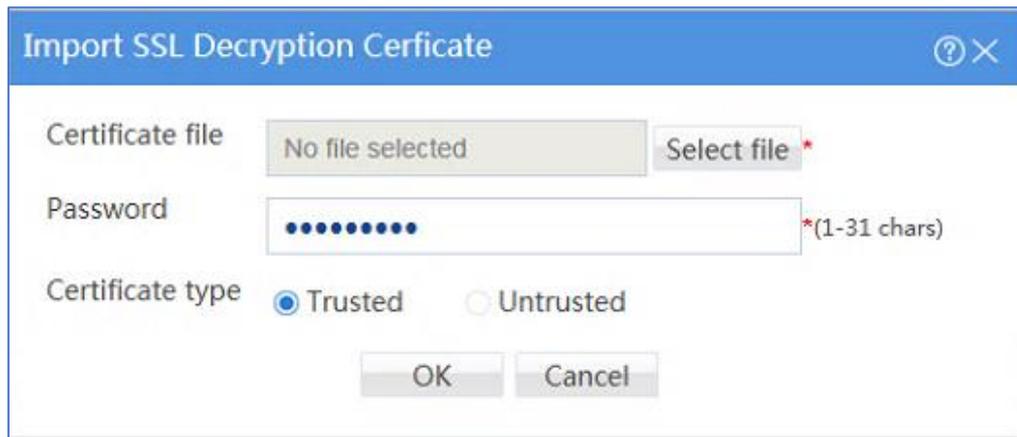
## 手順

### デバイスを設定する

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで **network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - A) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
    - B) **IPv4 Address** タブで、インターフェイスの IP アドレスとマスクを入力します。この例では、10.1.1.2/24 と入力します。
    - C) **OK** をクリックします。
  - #GE1/0/GE1//2 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。
2. 信頼できるSSL復号化証明書をインポートします。
  - #トップナビゲーションバーで、**Policies** をクリックします。
  - #ナビゲーションペインで、**Application Proxy > SSL Decryption Certificates** を選択します。
  - #**import** をクリックします。
  - #開いたダイアログボックスで、次の設定を行います(図2を参照)。
    - A) ファイル **trust.pem** を選択します。
    - B) ファイルのパスワードを入力します。
    - C) 証明書の種類を **Trusted** に設定します。

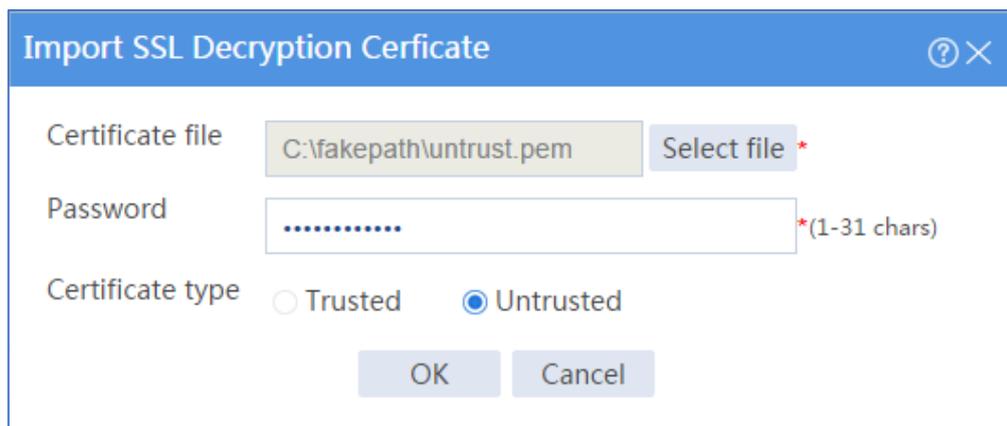
#OK をクリックします。

図2 信頼できるSSL復号化証明書のインポート



#信頼できる SSL 復号化証明書をインポートするのと同じ方法で、信頼できない SSL 復号化証明書をインポートします(図3を参照)。

図3 信頼できないSSL復号化証明書のインポート



3. 信頼できるSSL復号化証明書を内部ネットワークからブラウザにインストールして信頼します(詳細は省略)。
4. プロキシポリシーを設定します。  
#トップナビゲーションバーで、**Policies** をクリックします。  
#ナビゲーションペインで、**Application Proxy > Proxy Policy** を選択します。  
#create をクリックします。  
#開いたダイアログボックスで、プロキシポリシーを設定します。
  - policy name policy1 と入力します。
  - ソースセキュリティゾーンの信頼と信頼解除を選択します。

- ターゲットセキュリティゾーンの信頼と信頼解除を選択します。
- service https を選択します。
- アクション SSL 復号化を選択します。
- ポリシーを有効にします。

#OK をクリックします。

図4 プロキシポリシーの作成

5. セキュリティポリシーを構成し、コンテンツセキュリティ設定をセキュリティポリシーに適用します。信頼および信頼解除のセキュリティゾーンがローカルセキュリティゾーンと相互通信できることを確認します(詳細は省略)。

## 設定の確認

デバイスが、プロキシポリシーと一致する HTTPS パケットに対して SSL 復号化を実行できることを確認し、復号化されたパケットに対してディープパケットインスペクションを実行します。

# 帯域幅管理の設定例

## はじめに

次に、帯域幅管理の設定例を示します。

帯域幅管理では、次の情報を使用して、デバイスを通るトラフィックを細かく制御できます。

- 送信元および宛先セキュリティゾーン。
- 送信元および宛先 IP アドレス。
- ユーザーおよびユーザーグループ。
- アプリケーションおよびアプリケーショングループ。
- DSCP プライオリティ。
- 時間範囲

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、帯域幅管理の基本的な知識があることを前提としています。

## 制限事項とガイドライン

帯域幅管理を設定する場合は、次の制限事項およびガイドラインに従ってください。

- トラフィックポリシーはネストをサポートしており、最大 4 つのレベルでネストできます。
- 子トラフィックポリシーの最大帯域幅は、その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、その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、子トラフィックポリシーと親トラフィックポリシーで同じにすることはできません。
- デフォルトの予想帯域幅が小さいインターフェイスでは、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。
  - インターフェイスに大量のトラフィックがある。
  - インターフェイ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イスに対して、予期される帯域幅を暗黙的に大きな値に設定します。たとえば、インターフェイス上に大量のトラフィックがある場合、トンネルインターフェイスの予期される帯域幅を 64kbps(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、親トラフィックポリシーだけがコピーされます。

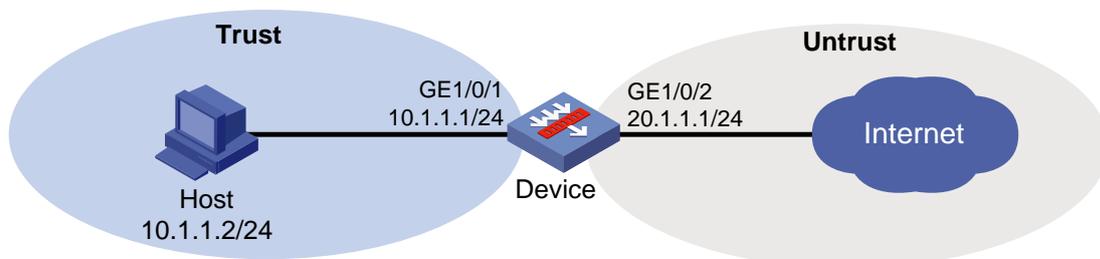
## 例:単一のトラフィックプロファイルの設定

### ネットワーク構成

図1に示すように、次の要件を満たすようにデバイスの帯域幅管理を設定します。

- イントラネット内のホストのアップストリームおよびダウンストリーム iQiYiPPS アプリケーショントラフィックの最大帯域幅は、30Mbps に制限されています。
- 保証帯域幅は、ホストのアップストリームとダウンストリームの両方の FTP トラフィックに対して 30Mbps です。
- インターネットへのインターフェイスの帯域幅は 100Mbps に制限されています。

図1 ネットワーク図



# 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **Edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
- b) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24 と入力します。
- c) **OK** をクリックします。

#**Untrust** セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。

2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- o ポリシー名 **Trust-Untrust** を入力します。
- o ソースゾーンは **trust** を選択します。
- o 宛先ゾーンは **untrust** を選択します。
- o アクション **permit** を選択します。

#OK をクリックします。

3. トラフィックプロファイルを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management > Traffic Profiles** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、aiqiyi という名前のトラフィックプロファイルを作成します(図2を参照)。

図2 aiqiyiという名前のトラフィックプロファイルの作成

The screenshot shows a 'Create Traffic Profile' dialog box with the following settings:

- Name: aiqiyi (1-63 chars)
- Bandwidth Limit:
  - Bandwidth limit mode:  Limit uplink and downlink separately,  Limit uplink and downlink as a whole
  - Total bandwidth Reference mode:  Exclusive,  Shared
  - Uplink bandwidth:
    - Maximum: 30 Mbps (1-100000)
    - Guaranteed: (empty) Mbps (1-100000)
  - Downlink bandwidth:
    - Maximum: 30 Mbps (1-100000)
    - Guaranteed: (empty) Mbps (1-100000)
- Forwarding priority: 1 (lowest)
- Per-IP/Per-user bandwidth:
  - Limit by:  IP address,  User
  - Bandwidth allocation among IP addresses:  Allocated dynamically and evenly
  - Uplink bandwidth:
    - Maximum: (empty) Mbps (1-100000)
    - Guaranteed: (empty) Mbps (1-100000)

Buttons: OK, Cancel

#OK をクリックします。

#トラフィックプロファイル aiqiyi を作成するのと同じ方法で、profileFTP という名前のトラフィックプロファイルを作成します(図3を参照)。

図3 profileFTPという名前のトラフィックプロファイルの作成

Create Traffic Profile

Name: profileFTP (1-63 chars)

**Bandwidth Limit**

Bandwidth limit mode:  Limit uplink and downlink separately  Limit uplink and downlink as a whole

Total bandwidth Reference mode:  Exclusive  Shared

Uplink bandwidth: Maximum: [ ] Mbps (1-100000) Guaranteed: 30 Mbps (1-100000)

Downlink bandwidth: Maximum: [ ] Mbps (1-100000) Guaranteed: 30 Mbps (1-100000)

Forwarding priority: 1 (lowest)

Per-IP/Per-user bandwidth Limit by:  IP address  User

Bandwidth allocation among IP addresses:  Allocated dynamically and evenly

Uplink bandwidth: Maximum: [ ] Mbps (1-100000) Guaranteed: [ ] Mbps (1-100000)

OK Cancel

#OK をクリックします。

4. トラフィックポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management > Traffic Policies** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、aiqiyi という名前のトラフィックポリシーを作成します(図4を参照)。

図4 aiqiyiという名前のトラフィックポリシーの作成

Field	Value	Action
Parent policy	Select a parent policy	
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	Select or enter users	
Service	Select or enter services	[Edit]
Application	iQIYIPPS	[Edit]
Time range	Select a time range	
DSCP priority	Select or enter DSCP values	[Edit]
Traffic profile	aiqiyi	[Edit]

#OK をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、Enable をクリックしてポリシーを有効にします。

#トラフィックポリシーaiqiyi を作成するのと同じ方法で、トラフィックポリシーFTP を作成します(図5を参照)。

図5 FTP という名前のトラフィックポリシーの作成

Parent policy	Select a parent policy	[Edit]
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	Select or enter users	
Service	Select or enter services	[Edit]
Application	ftp, ftp-data	[Edit]
Time range	Select a time range	
DSCP priority	Select or enter DSCP values	[Edit]
Traffic profile	profileFTP	[Edit]

#OK をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、Enable をクリックしてポリシーを有効にします。

5. インターフェイス帯域幅を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Bandwidth Management > Interface Bandwidth を選択します。

# **create** をクリックします。

# 図6表示されるダイアログボックスで、に示すようにインターフェイス帯域幅を設定します。

図6 インターフェイス帯域幅の設定



#OK をクリックします。

## 設定の確認

#GigabitEthernet1/0/2 の合計トラフィックレートが 100Mbps に達したときに、iQiYiPPS アプリケーショントラフィックレートが 30Mbps を超えることができず、FTP トラフィックレートが最低 30Mbps に達することができることを確認します。

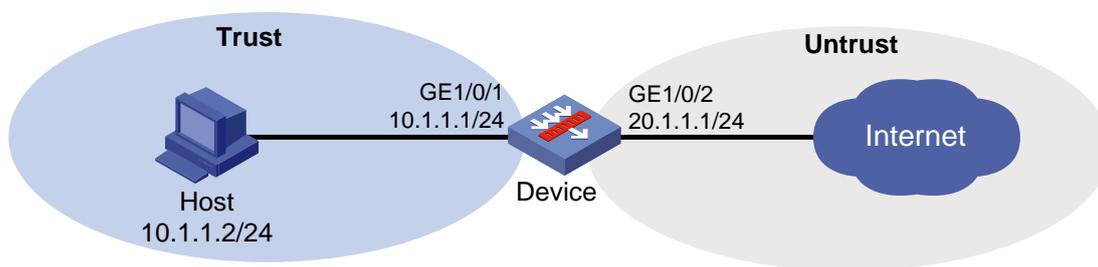
## 例:親/子トラフィックプロファイルの設定

### ネットワーク構成

図7に示すように、次の要件を満たすようにデバイスの帯域幅管理を設定します。

- イントラネット内のホストのアップストリームおよびダウンストリーム iQiYiPPS アプリケーショントラフィックの最大帯域幅は、30Mbps に制限されています。
- 保証帯域幅は、ホストのアップストリームとダウンストリームの両方の FTP トラフィックに対して 30Mbps です。
- ホストの合計トラフィックレートは 50Mbps に制限されています。

図7 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **Edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) **basic configuration** タブで、**Trust** セキュリティゾーンを選択します。
- b) **IPv4 Address** タブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24 と入力します。
- c) **OK** をクリックします。

#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1./24 に設定します。

2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies > Security Policies** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 **Trust-Untrust** を入力します。
- ソースゾーンの **trust** を選択します。

- 宛先ゾーンの **untrust** を選択します。
- アクション **permit** を選択します。

#OK をクリックします。

3. トラフィックプロファイルを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management > Traffic Profiles** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、トラフィックプロファイルを設定します(図8を参照)。

図8 profileという名前のトラフィックプロファイルの作成

The screenshot shows the 'Create Traffic Profile' dialog box with the following settings:

- Name:** profile (1-63 chars)
- Bandwidth Limit:**
  - Bandwidth limit mode:  Limit uplink and downlink separately,  Limit uplink and downlink as a whole
  - Total bandwidth Reference mode:  Exclusive,  Shared
  - Uplink bandwidth: Maximum: 50 Mbps (1-100000), Guaranteed: (empty) Mbps (1-100000)
  - Downlink bandwidth: Maximum: 50 Mbps (1-100000), Guaranteed: (empty) Mbps (1-100000)
- Forwarding priority:** 1 (lowest)
- Per-IP/Per-user bandwidth:**
  - Limit by:  IP address,  User
  - Bandwidth allocation among IP addresses:  Allocated dynamically and evenly
  - Uplink bandwidth: Maximum: (empty) Mbps (1-100000), Guaranteed: (empty) Mbps (1-100000)

Buttons: OK, Cancel

#OK をクリックします。

#profile という名前のトラフィックプロファイルを作成するのと同じ方法で、aiqiyi という名前のトラフィックプロファイルを作成します(図9を参照)。

図9 aiqiyiという名前のトラフィックプロファイルの作成

Create Traffic Profile

Name  (1-63 chars)

**Bandwidth Limit**

Bandwidth limit mode  Limit uplink and downlink separately  Limit uplink and downlink as a whole

Total bandwidth Reference mode  Exclusive  Shared

Uplink bandwidth Maximum:  Mbps (1-100000)  
Guaranteed:  Mbps (1-100000)

Downlink bandwidth Maximum:  Mbps (1-100000)  
Guaranteed:  Mbps (1-100000)

Forwarding priority

Per-IP/Per-user bandwidth Limit by  IP address  User

Bandwidth allocation among IP addresses  Allocated dynamically and evenly

Uplink bandwidth Maximum:  Mbps (1-100000)  
Guaranteed:  Mbps (1-100000)

OK Cancel

#OK をクリックします。

#profile という名前のトラフィックプロファイルを作成するのと同じ方法で、profileFTP という名前のトラフィックプロファイルを作成します(図10を参照)。

図10 profileFTPという名前のトラフィックプロファイルの作成

The screenshot shows the 'Create Traffic Profile' dialog box with the following settings:

- Name: profileFTP (1-63 chars)
- Bandwidth Limit:
  - Bandwidth limit mode:  Limit uplink and downlink separately,  Limit uplink and downlink as a whole
  - Total bandwidth Reference mode:  Exclusive,  Shared
  - Uplink bandwidth:
    - Maximum: [ ] Mbps (1-100000)
    - Guaranteed: 30 Mbps (1-100000)
  - Downlink bandwidth:
    - Maximum: [ ] Mbps (1-100000)
    - Guaranteed: 30 Mbps (1-100000)
- Forwarding priority: 1 (lowest)
- Per-IP/Per-user bandwidth:
  - Limit by:  IP address,  User
  - Bandwidth allocation among IP addresses:  Allocated dynamically and evenly
  - Uplink bandwidth:
    - Maximum: [ ] Mbps (1-100000)
    - Guaranteed: [ ] Mbps (1-100000)

Buttons: OK, Cancel

#OK をクリックします。

4. 親トラフィックポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management > Traffic Policies** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、policy という名前のトラフィックポリシーを作成します(図11を参照)。

図11 policyという名前のトラフィックポリシーの作成

parent policy	Select a parent policy	[Edit]
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	Select or enter users	
Service	Select or enter services	[Edit]
Application	Select or enter applications	[Edit]
Time range	Select a time range	
DSCP priority?	Select or enter DSCP values	[Edit]
Traffic profile	profile	[Edit]

OK Cancel

# **OK** をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、**Enable** をクリックしてポリシーを有効にします。

5. 子トラフィックポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management > Traffic Policies** を選択します。

# **create** をクリックします。

#開いたダイアログボックスで、aiqiyl という名前のトラフィックポリシーを作成します(図12を参照)。

図12 aiqiyiという名前のトラフィックポリシーの作成

Parent policy	policy	[Edit]
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	Select or enter users	
Service	Select or enter services	[Edit]
Application	iQIYIPPS	[Edit]
Time range	Select a time range	
DSCP priority	Select or enter DSCP values	[Edit]
Traffic profile	aiqiyi	[Edit]

OK Cancel

#OK をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、**Enable** をクリックしてポリシーを有効にします。

# policy という名前のトラフィックポリシーを作成するのと同じ方法で、FTP という名前のトラフィックポリシーを作成します (図13を参照)。

図13 FTPという名前のトラフィックポリシーの作成

Parent policy	policy	[Edit]
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	Select or enter users	
Service	Select or enter services	[Edit]
Application	ftp, ftp-data	[Edit]
Time range	Select a time range	
DSCP priority	Select or enter DSCP values	[Edit]
Traffic profile	profileFTP	[Edit]

#OK をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、Enable をクリックしてポリシーを有効にします。

## 設定の確認

#ホストの合計トラフィックレートが 50Mbps に制限されていること、および iQiYiPPS アプリケーションのトラフィックレートが 30Mbps に制限されていることを確認します。輻輳が発生すると、FTP トラフィックに対して 30Mbps の帯域幅が保証されます。

# 例:ユーザーベースのトラフィックプロファイルの設定

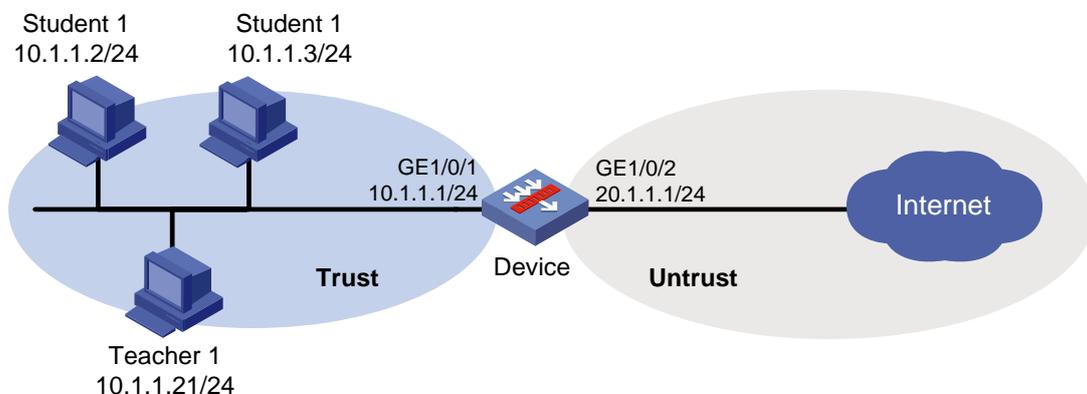
## ネットワーク構成

図1に示すように、イントラネットには2つのユーザーグループがあります。2人の教師がいる教師グループと5人の生徒がいる生徒グループです。

次の要件を満たすように、デバイス上でユーザー単位の帯域幅管理を設定します。

- 帯域幅は、アップストリーム方向とダウンストリーム方向の両方で各教師に対して 10Mbps に制限され、アップストリーム方向とダウンストリーム方向の両方で各生徒に対して 2Mbps に制限されます。
- 合計接続数の制限は、教師の場合は 100000 に制限されています。合計接続数の制限は、生徒の場合は 40000 に制限されています。また、接続数の制限は、各生徒の場合は 10000 に制限されています。
- 教師は生徒よりもインターネットへのアクセスの優先順位が高い。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、**Network** をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **Edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) basic configurationタブで、Trustセキュリティゾーンを選択します。
- b) IPv4Addressタブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。
- c) OKをクリックします。

#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1./24 に設定します。

## 2. セキュリティポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Security Policies>Security Policies** を選択します。

#create をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 Trust-Untrust を入力します。
- ソースゾーンの信頼を選択します。
- 宛先ゾーンを選択信頼解除。
- アクション許可を選択します。

#OK をクリックします。

## 3. IDユーザーを作成します。

#トップナビゲーションバーで、**Objects** 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。

#ユーザータブで、create をクリックします。

#開いたダイアログボックスで、ユーザー名を student1 に設定します。

#OK をクリックします。

#ユーザーstudent2、student3、student4、student5、teacher1、および teacher2 を、ユーザー student1 の作成と同じ方法で作成します。

#トップナビゲーションバーで、**Objects** 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。

#ユーザーグループタブで、create をクリックします。

#開いたダイアログボックスで、グループ名を student に設定し、グループに対して identity users student1、student2、student3、student4、および student5 を設定します。

#OK をクリックします。

#teacher という名前のグループを作成し、グループ student の設定と同じ方法で、グループに対して ID ユーザー teacher1 と teacher2 を設定します。

#トップナビゲーションバーで、**Objects** 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。

#Static Identity Users タブで、Create をクリックします。

#開いたダイアログボックスで、ユーザー名を student1、IP アドレスタイプを IPv4、IP アドレスを 10.1.1.11 に設定します。

#OK をクリックします。

#static identity user student1 の設定と同じ方法で、static identity users student2、student3、student4、student5、teacher1、および teacher2 を作成します。

#トップナビゲーションバーで、**Objects** 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。

#Online Users タブで、Enable user identification をクリックします。

#### 4. トラフィックプロファイルを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management>Traffic Profiles** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、profile-teacher という名前のトラフィックプロファイルを作成します (図2及び図3を参照)。

図2 profile-teacher(l)という名前のトラフィックプロファイルの作成

**Create Traffic Profile** [?] [X]

Name:  \* (1-63 chars)

---

**Bandwidth Limit**

Bandwidth limit mode:  Limit uplink and downlink separately  Limit uplink and downlink as a whole

Total bandwidth Reference mode [?]:  Exclusive  Shared

Uplink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

Downlink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

Forwarding priority:

Per-IP/Per-user bandwidth

Limit by:  IP address  User

Bandwidth allocation among IP addresses [?]:  Allocated dynamically and evenly

Uplink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

[OK] [Cancel]

図3 profile-teacher(II)という名前のトラフィックプロファイルの作成

Create Traffic Profile

Bandwidth allocation among IP addresses  Allocated dynamically and evenly

Uplink bandwidth

Maximum: 10 Mbps (1-100000)

Guaranteed: Mbps (1-100000)

Downlink bandwidth

Maximum: 10 Mbps (1-100000)

Guaranteed: Mbps (1-100000)

---

Connection Count Limit

Total connections 100000 (1-12000000)

Limit by  IP address  User

Per-IP/Per-user connection count (1-12000000)

---

Connection Rate Limit

Total connection rate (1-12000000)

Limit by  IP address  User

OK Cancel

#OK をクリックします。

#およびに示すように、profile-student という名前のトラフィックプロファイルを作成します(図17, 図18)。

図17 profile-student(l)という名前のトラフィックプロファイルの作成

**Create Traffic Profile** [?] [X]

Name:  (1-63 chars)

---

**Bandwidth Limit**

Bandwidth limit mode:  Limit uplink and downlink separately  Limit uplink and downlink as a whole

Total bandwidth Reference mode <sup>?</sup>:  Exclusive  Shared

Uplink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

Downlink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

Forwarding priority:  ▾

Per-IP/Per-user bandwidth

Limit by:  IP address  User

Bandwidth allocation among IP addresses <sup>?</sup>:  Allocated dynamically and evenly

Uplink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

OK Cancel

図18 profile-student(II)という名前のトラフィックプロファイルの作成

Create Traffic Profile

Bandwidth allocation among  Allocated dynamically and evenly  
IP addresses ?

Uplink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

Downlink bandwidth

Maximum:  Mbps (1-100000)

Guaranteed:  Mbps (1-100000)

---

Connection Count Limit

Total connections  (1-12000000)

Limit by  IP address  User

Per-IP/Per-user connection count  (1-12000000)

---

Connection Rate Limit

Total connection rate  (1-12000000)

Limit by  IP address  User

OK Cancel

#OK をクリックします。

5. トラフィックポリシーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Bandwidth Management > Traffic Policies** を選択します。

#create をクリックします。

#開いたダイアログボックスで、policy-teacher という名前のトラフィックポリシーを作成します(図19を参照)。

図19 policy-teacherという名前のトラフィックポリシーの作成

Parent policy	Select a parent policy	[Edit]
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	teacher	
Service	Select or enter services	[Edit]
Application	Select or enter applications	[Edit]
Time range	Select a time range	
DSCP priority	Select or enter DSCP values	[Edit]
Traffic profile	profile-teacher	[Edit]

OK Cancel

#OK をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、Enable をクリックしてポリシーを有効にします。

#policy-student という名前のトラフィックポリシーを、policy-teacher という名前のトラフィックポリシーを作成するのと同じ方法で作成します(図20を参照)。

図20 policy-studentという名前のトラフィックポリシーの作成

Parent policy	Select a parent policy	
Source security zone	Trust	[Edit]
Destination security zone	Untrust	[Edit]
Source IP address	Select or enter source IP addresses	[Edit]
Destination IP address	Select or enter destination IP addresses	[Edit]
User	student	
Service	Select or enter services	[Edit]
Application	Select or enter applications	[Edit]
Time range	Select a time range	
DSCP priority	Select or enter DSCP values	[Edit]
Traffic profile	profile-student	[Edit]

#OK をクリックします。

#トラフィックポリシーの作成後、ポリシーを選択し、Enable をクリックしてポリシーを有効にします。

## 設定の確認

#各教師の帯域幅が 10Mbps に制限されていることと、各生徒の帯域幅が 2Mbps に制限されていることを確認します。

#接続数が生徒と教師の両方に制限されていることを確認します。

# NAT ヘアピンの設定例

## はじめに

次に、NATヘアピンの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

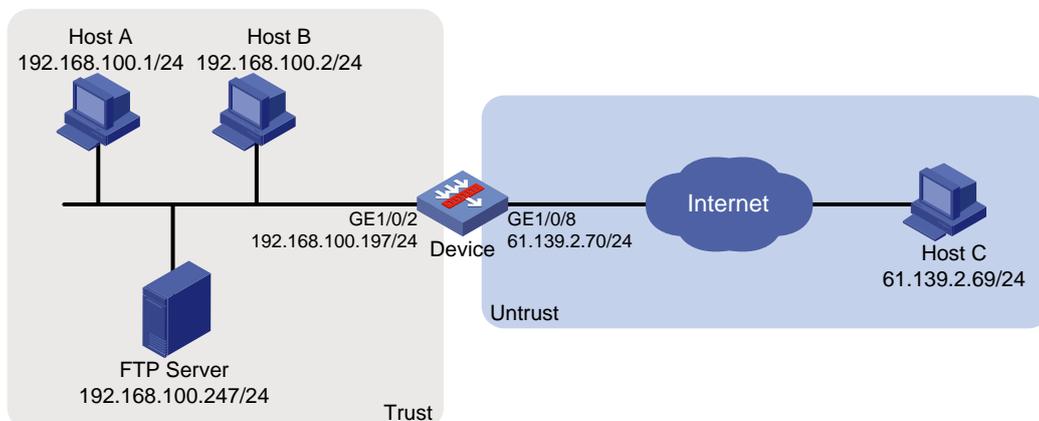
次の情報は、NAT の基本的な知識があることを前提としています。

## 例:NATヘアピンの設定

### ネットワーク構成

図1に示すように、192.168.100.247/24 の内部 FTP サーバーは、内部ユーザーと外部ユーザーにサービスを提供します。外部ユーザーと内部ユーザーがパブリック IP アドレス 61.139.2.70/24 を使用して内部 FTP サーバーにアクセスできるように、C/S モードで NAT ヘアピンを設定します。

図1ネットワーク図



## 分析

次に、C/S モードでの NAT ヘアピンの一般的な使用例を示します。ネットワーク要件を満たすには、次の作業を実行します。

- 内部ホストがパブリック IP アドレスを使用して内部 FTP サーバーにアクセスできるようにするには、内部ネットワークに接続されているインターフェイス上で NAT ヘアピンをイネーブルにします。NAT サーバーマッピングが設定されているインターフェイス上でアウトバウンド NAT を設定します。宛先アドレスは、NAT サーバーマッピングと一致させることによって変換されます。送信元アドレスは、アウトバウンド NAT と一致させることによって変換されます。
- 外部ホストがパブリック IP アドレスを使用して内部 FTP サーバーにアクセスできるようにするには、外部ネットワークに接続されたインターフェイス上で NAT サーバーを設定します。

# 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

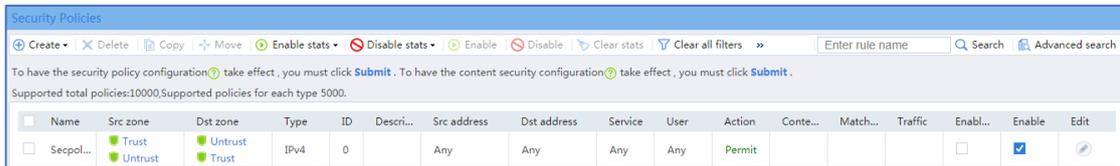
## 手順

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
# トップナビゲーションバーで、**Network** をクリックします。  
# ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。  
# GE1/0/2 の編集アイコンをクリックします。  
# 開いたダイアログボックスで、インターフェイスを設定します。
  - a) 基本 basic configuration タブで、Trust セキュリティゾーンを選択します。
  - b) IPv4Address タブで、インターフェイスの IP アドレスとマスク長を入力します。この例では、192.168.100.197/24 と入力します。
  - c) OK をクリックします。  
# GE1/0/GE1//8 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 61.139.2.70/24 に設定します。
2. セキュリティポリシーを設定します。  
# トップナビゲーションバーで、Policies をクリックします。  
# ナビゲーションペインで、Security Policies > Security Policies を選択します。

# create をクリックします。

#Untrust セキュリティゾーンと Trust セキュリティゾーン間の通信を許可するセキュリティポリシーを設定します。

図2セキュリティポリシーの設定



### 3. NATを設定します。

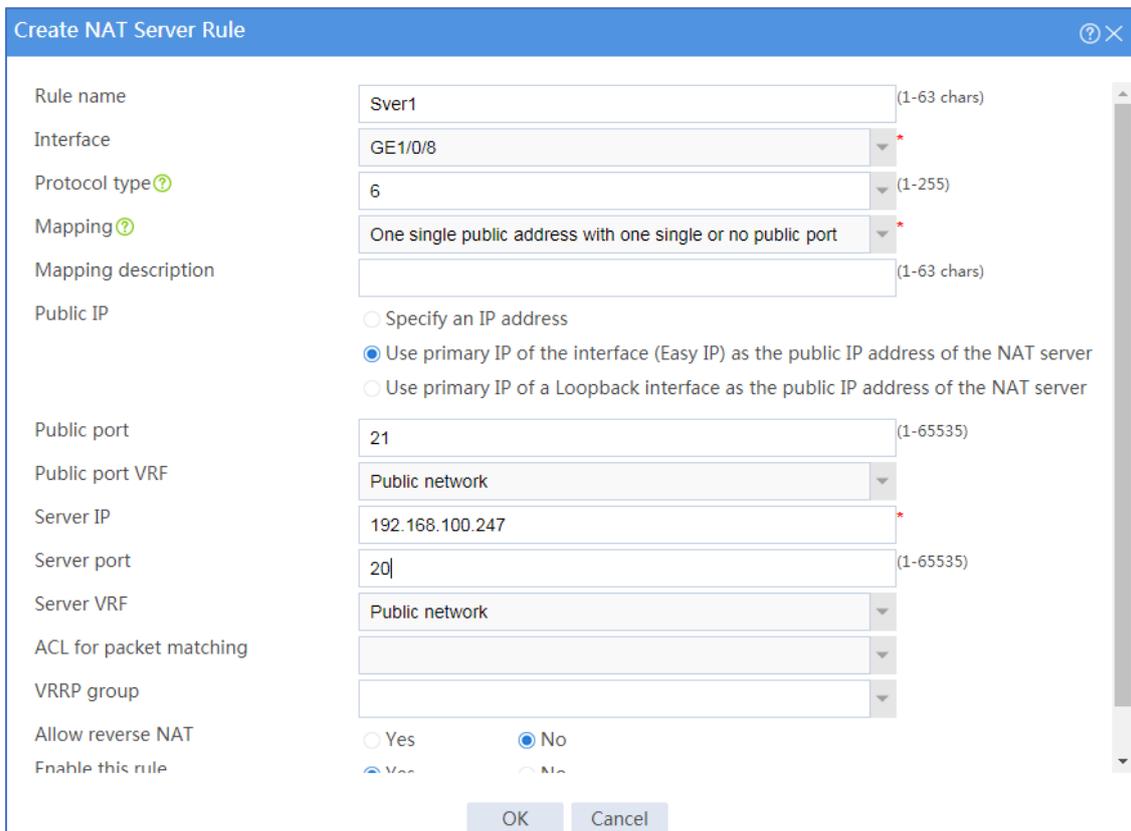
#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT>NAT Servers>Policy Configuration を選択します。

#create をクリックします。

#表示されるダイアログボックスで、NAT サーバー規則を作成します(図3を参照)。

図3NAT サーバー規則の作成



#OK をクリックします。

#トップナビゲーションバーで、Policies をクリックします。

- #ナビゲーションペインで、NAT > Dynamic NAT を選択します。
- #Outbound Dynamic NAT(ACL-Based)タブで、Create をクリックします。
- #アウトバウンドダイナミック NAT 規則を作成します(図4を参照)。

図4 アウトバウンドダイナミック NAT 規則の作成

The screenshot shows a configuration window titled "Create Outbound Dynamic NAT". The fields are as follows:

- Interface: GE1/0/8
- ACL: (empty)
- Source address after NAT:  NAT address group  Easy IP
- VRF: Public network
- Translation mode:  PAT
- Port preservation:  Try to preserve port number for PAT
- Enable this rule:
- Counting:

Buttons: OK, Cancel

- #OK をクリックします。
- #トップナビゲーションバーで、Policies をクリックします。
- #ナビゲーションペインで、NAT > NAT Advanced Settings > NAT Hairpin を選択します。
- #GE1/0/2 を選択し、Enable をクリックします。GE1/0/2 は NAT ヘアピンでイネーブルになります(図5を参照)。

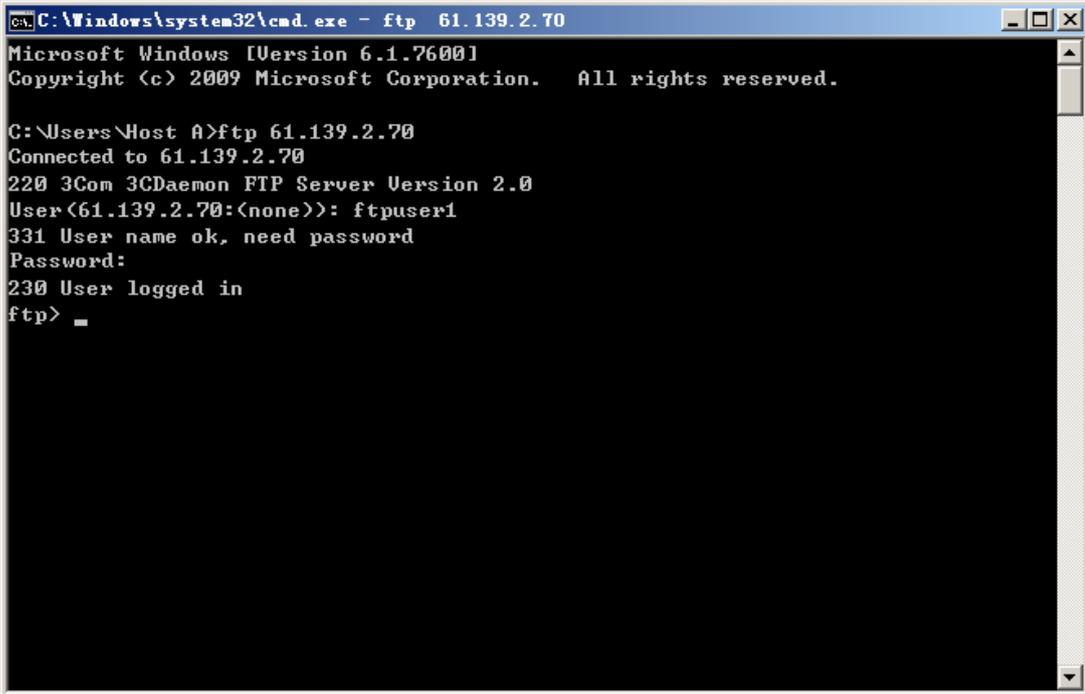
図5 NAT ヘアピンのイネーブル化

Interface name	Interface description	NAT hairpin status
<input type="checkbox"/> GE1/0/2	GigabitEthernet1/0/2 Interface	Enabled

## 設定の確認

1. 内部ホストがパブリックアドレスを使用してFTPサーバーにアクセスできることを確認します(図6を参照)。

図6 内部ホストからFTPサーバーへの接続

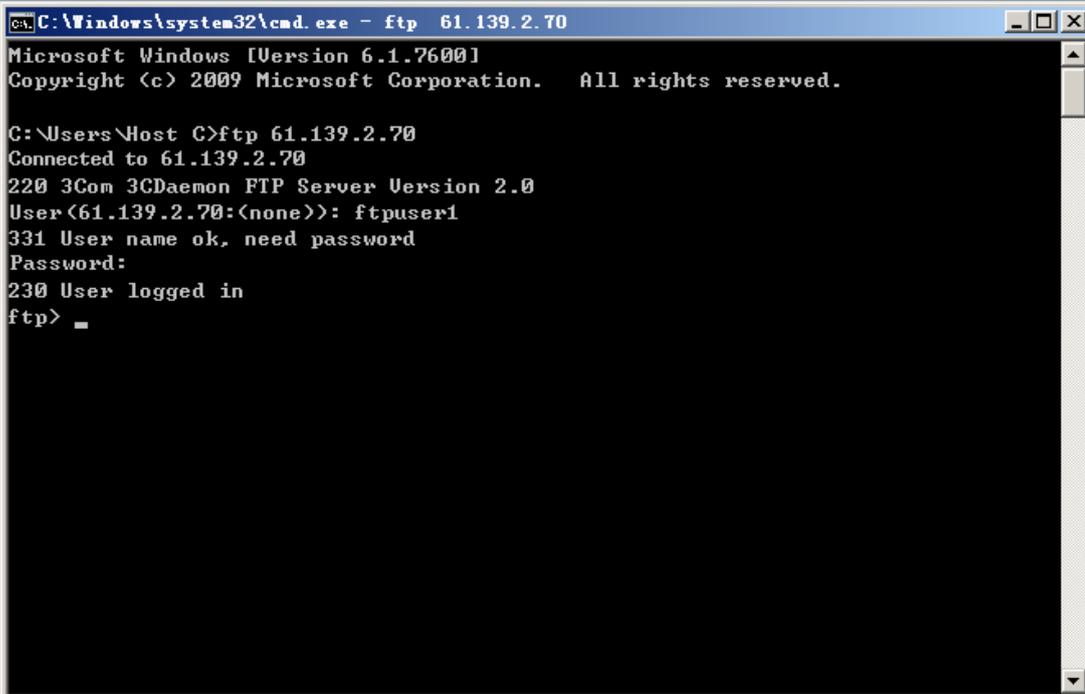


```
C:\Windows\system32\cmd.exe - ftp 61.139.2.70
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Host A>ftp 61.139.2.70
Connected to 61.139.2.70
220 3Com 3CDaemon FTP Server Version 2.0
User (61.139.2.70:(none)): ftpuser1
331 User name ok, need password
Password:
230 User logged in
ftp> _
```

2. 外部ホストがパブリックアドレスを使用してFTPサーバーにアクセスできることを確認します(図7を参照)。

図7 外部ホストからFTPサーバーへの接続



```
C:\Windows\system32\cmd.exe - ftp 61.139.2.70
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Host C>ftp 61.139.2.70
Connected to 61.139.2.70
220 3Com 3CDaemon FTP Server Version 2.0
User (61.139.2.70:(none)): ftpuser1
331 User name ok, need password
Password:
230 User logged in
ftp> _
```

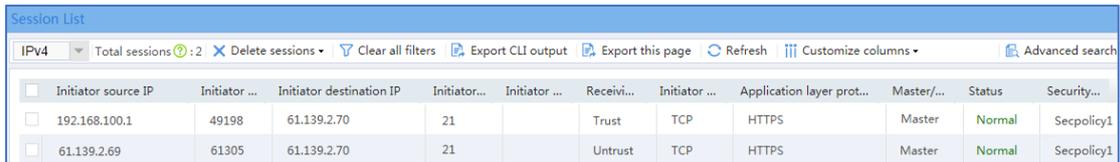
3. 内部ホストと外部ホストがFTPサーバーにアクセスするときに、それらのセッションが作

成されていることを確認します。

#トップナビゲーションバーでモニターをクリックします。

#ナビゲーションペインで、Session を選択します。

図8 セッションリスト



The screenshot shows a web interface titled "Session List". At the top, there is a navigation bar with "IPv4" selected, "Total sessions: 2", and buttons for "Delete sessions", "Clear all filters", "Export CLI output", "Export this page", "Refresh", "Customize columns", and "Advanced search". Below the navigation bar is a table with the following columns: "Initiator source IP", "Initiator ...", "Initiator destination IP", "Initiator...", "Initiator ...", "Receivi...", "Initiator ...", "Application layer prot...", "Master/...", "Status", and "Security...". The table contains two rows of session data.

<input type="checkbox"/>	Initiator source IP	Initiator ...	Initiator destination IP	Initiator...	Initiator ...	Receivi...	Initiator ...	Application layer prot...	Master/...	Status	Security...
<input type="checkbox"/>	192.168.100.1	49198	61.139.2.70	21		Trust	TCP	HTTPS	Master	Normal	Secpolicy1
<input type="checkbox"/>	61.139.2.69	61305	61.139.2.70	21		Untrust	TCP	HTTPS	Master	Normal	Secpolicy1

# サーバーロードバランシングの設定例

## はじめに

次に、サーバーロードバランシングの設定例を示します。

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。

- レイヤー4 サーバーロードバランシング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布します。レイヤー4 サーバー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 サービスを配布できません。
- レイヤー7 サーバーロードバランシング内容に基づいて実装されます。パケットの内容を分析し、内容に基づいてパケットを1つずつ配布し、事前定義されたポリシーに従って指定されたサーバーに接続を配布します。レイヤー7 サーバーロードバランシングは、広い範囲にロードバランシングサービスを適用します。

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、IPv4 から IPv6 または IPv6 から IPv4 への変換はサポートしません。

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、HTTP、パフォーマンス(HTTP)、HTTPS、および HTTP リダイレクションがあります。IP、TCP、および UDP はレイヤー4 サーバーロードバランシングと呼ばれます。HTTP、パフォーマンス(HTTP)、HTTPS、および HTTP リダイレクションはレイヤー7 サーバーロードバランシングと呼ばれます。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

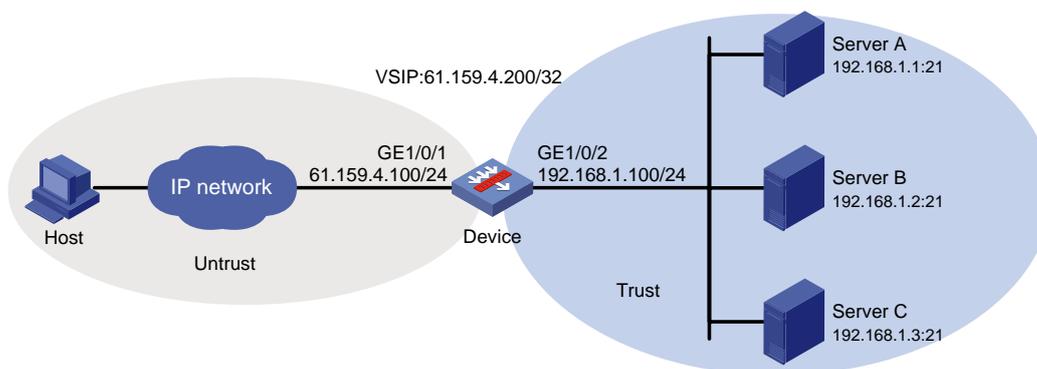
次の情報は、サーバーロードバランシング機能の基本的な知識があることを前提としています。

# 例:レイヤー4サーバーロードバランシングの設定

## ネットワーク構成

図1に示すように、企業はサーバーA、サーバーB およびサーバーC を使用して FTP サービスを提供します。サーバーのロードバランシングを構成して、ソースアドレスに基づいてホストからの FTP 要求をサーバー間でロードバランシングします。たとえば、デバイスが 62.159.4.0/24 および 63.159.4.0/24 からの FTP 要求をそれぞれサーバーA およびサーバーB に割り当てることを有効にし、デバイスが他のソースアドレスを持つ FTP 要求をサーバーC に割り当てることを有効にします。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、networkをクリックします。  
#ナビゲーションペインで、Interface Configuration > Interfaces を選択します。  
#GE1/0/1 の edit アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。  
a) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。

b) IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、61.159.4.100/24と入力します。

c) OKをクリックします。

#GE1/0/ge1//2を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 192.168.1.100/24 に設定します。ゾーン Untrust からゾーン Trust へのセキュリティポリシーを作成します(詳細は省略)。

3. #トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Health Monitoring** を選択します。

#Create をクリックして、プローブテンプレート t1 を設定します(図2を参照)。

図2プローブテンプレートt1の作成

Basic configuration

Template name	<input type="text" value="t1"/> *	(1-32 chars)
Type	<input type="text" value="ICMP"/>	
Destination IP address	<input type="text"/>	(IPv4/IPv6 address)
Data to pad	<input type="text"/>	(0-200 chars)
Length of data to pad	<input type="text" value="100"/>	(20-65507)
Next hop IP address	<input type="text"/>	(IPv4/IPv6 address)
Outgoing interface	<input type="text"/>	
Probe interval?	<input type="text" value="5000"/>	ms(0-604800000)
Probe timeout?	<input type="text" value="3000"/>	ms(10-3600000)
Description	<input type="text"/>	(0-200 chars)

OK Cancel

#OK をクリックします。

4. アドレスタイプおよびポートタイプのスティッキグループを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Common Configuration>Sticky Groups を選択します。

#Create をクリックして、スティッキグループ sticky\_group を設定します(を参照)。

図3スティッキグループの作成sticky\_group

Create Sticky Group

Sticky group name  \*(1-63 chars)

Type  \*

Aging time  sec (10-604800)

Override limits  Enable  Disable

Stickiness-over-busyness  Enable  Disable

Description  (0-127 chars)

Address/port stickiness

IPv4

Mask length  (0-32)

OK Cancel

#OK をクリックします。

5. 実サーバーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing > Server Load Balancing > Real Servers を選択します。

#Create をクリックして実サーバーrs\_a を設定します(図4を参照)。

図4実サーバーrs\_aの作成

Basic configuration

Real server name: rs\_a (1-63 chars)

IPv4 address: 192.168.1.1

IPv6 address: |

Port number: 0 (0-65535)

VPN instance: Public network

VPN instance inheritance:  Enable  Disable

Real server feature:  Enable  Disable

Description: (0-127 chars)

Advanced configuration

OK Cancel

#OK をクリックします。

#実サーバーrs\_bを設定し、その方法で、実サーバーrs\_bを設定し、その IP アドレスを 192.168.1.2 に設定します。

#実サーバーrs\_aを設定するのと同じ方法で、実サーバーrs\_cを設定し、その IP アドレスを 192.168.1.3 に設定します。

#設定されている実サーバーを表示します(図5を参照)。

図5設定された実サーバーの表示

Real server name	Status	VRF	IPv4 address	Port number	Priority	Weight	Server farm	Real server f...	Edit
<input checked="" type="checkbox"/> rs_a	●	Public network	192.168.1.1	0	4	100		Enable	ⓘ
<input checked="" type="checkbox"/> rs_b	●	Public network	192.168.1.2	0	4	100		Enable	ⓘ
<input checked="" type="checkbox"/> rs_c	●	Public network	192.168.1.3	0	4	100		Enable	ⓘ

## 6. サーバーファームを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing > Server Load Balancing > Server Farms を選択します。

#Create をクリックして、サーバーファーム sf1 を設定します(図6および図7を参照)。

図6サーバーファームsf1(l)の作成

Create Server Farm ? ×

Basic configuration

Server farm name  \*(1-63 chars)

Scheduling algorithm ?

Mask length  (0-32)

Prefix length  (0-128)

Priority scheduling ?  Limit real servers to participate in scheduling

Minimum number  \*(1-1000)

Maximum number  \*(1-1000)

Real server

+ Add | × Delete

<input type="checkbox"/>	Name	St...	O...	IPv4...	IPv6...	Port	Edit
<input type="checkbox"/>	rs_a		-	192...		0	

Probe method

+ Add | × Delete

OK Cancel

図7サーバーファームsf1の作成(II)

#OK をクリックします。

#サーバーファーム sf2 を設定し、サーバーファーム sf1 と同じ方法で実サーバーrs\_b を指定します。

#サーバーファーム sf3 を設定し、サーバーファーム sf1 と同じ方法で実サーバーrs\_c を指定します。

#設定されたサーバーファームを表示します(図8を参照)。

図8 設定されたサーバーファームの表示

Server farm name	Status	Scheduling algorithm	Total real servers	Available real servers	Edit
<input type="checkbox"/> sf1	●	Hash source IP address	1	1	
<input type="checkbox"/> sf2	●	Hash source IP address	1	1	
<input type="checkbox"/> sf3	●	Hash source IP address	1	1	

7. クラスを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Advanced Policies を  
選択します。

#クラスタブをクリックします。

#Create をクリックして、クラス cls\_1 を設定します(図9を参照)。

図9 クラスcls\_1の作成

Class name: cls\_1 (1-63 chars)

Type: Generic

Match type:  Match all  Match any

Match rule:

Rule ID	Type	Rule content
<input type="checkbox"/> 1	Source IPv4 ...	62.159.4.0/24

Description: (0-127 chars)

Buttons: OK, Cancel

#OK をクリックします。

#Create をクリックして、クラス cls\_2 を設定します(図10を参照)。

図10 クラスcls\_2の作成

Class name: cls\_2 (1-63 chars)

Type: Generic

Match type:  Match all  Match any

Match rule:

Rule ID	Type	Rule content
<input type="checkbox"/> 1	Source IPv4 ...	61.159.4.0/24

Description: (0-127 chars)

Buttons: OK, Cancel

#OK をクリックします。

8. アクションを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Advanced Policies を選択します。

#Action タブをクリックします。

#Create をクリックして、action act\_1 を設定します(図11を参照)。

図11 action act\_1の作成

**Create Action**

Basic configuration

Action name: act\_1 \* (1-63 chars)

Type: Generic

Forwarding mode: Load balance

Fallback action: Match next rule

ToS: (0-255)

Description: (0-127 chars)

Server farms

Primary server farm: sf1 \*

Backup server farm:

Sticky group: sticky\_group

OK Cancel

#OK をクリックします。

#action act\_2 を設定し、action act\_1 と同じ方法でプライマリサーバーファーム sf2 を指定します。

#action act\_3 を設定し、action act\_1 を設定するのと同じ方法でプライマリサーバーファーム sf3 を指定します。

#設定されたアクションを表示します(図12を参照)。

図12 設定済みアクションの表示

Action name	Type	Forwarding action	Effective server farm	Edit
<input type="checkbox"/> act_1	Generic	Load balance		
<input type="checkbox"/> act_2	Generic	Load balance		
<input type="checkbox"/> act_3	Generic	Load balance		

9. ロードバランシングポリシーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Advanced Policies を選択します。

#Load Balancing Policy タブをクリックします。

#Create をクリックして、ロードバランシングポリシーloadbalance\_policy を設定します(図13を参照)。

図13 ロードバランシングポリシーの作成loadbalance\_policy

Create Load Balancing Policy

Name: loadbalance\_policy (1-63 chars)

Type: Generic

Default action: act\_3

Rule

Class	Action
cls_1	act_1
cls_2	act_2

Description: (0-127 chars)

OK Cancel

#OK をクリックします。

#### 10. 仮想サーバーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Virtual Servers を選択します。

#Create をクリックして、仮想サーバーを設定します(図14および図15参照)。

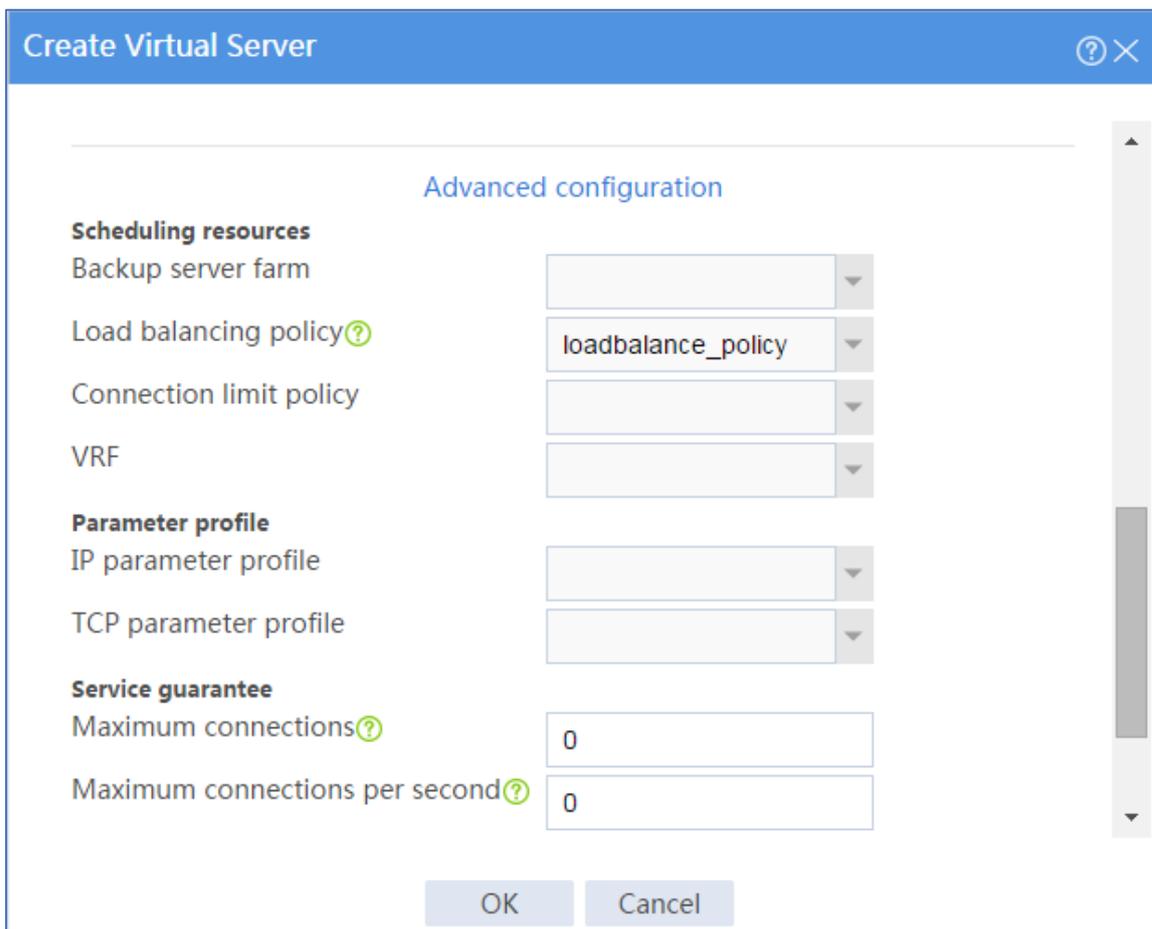
図14 仮想サーバーの作成と(基本設定)

The image shows a 'Create Virtual Server' dialog box with a blue title bar. The main area is titled 'Basic configuration' and contains several fields and options:

- Virtual server name:** A text input field containing 'vs' with a red asterisk and '(1-63 chars)' to its right.
- Type:** A dropdown menu showing 'TCP'.
- IPv4 address:** Two input fields containing '61.159.4.21' and '32' separated by a slash.
- IPv6 address:** Two empty input fields separated by a slash.
- Port number:** An input field containing '21' with '(0-65535)' to its right.
- SSL server policy:** A dropdown menu.
- Server farm:** A dropdown menu.
- Sticky group:** A dropdown menu.
- Interfaces for sending gratuitous ARP/ND packets:** A dropdown menu with a blue '[Edit]' link to its right.
- Operation mode:** Two radio buttons: 'four-layer' (selected) and 'seven-layer'.
- IP address advertisement:** Two radio buttons: 'Enable' and 'Disable' (selected).

At the bottom of the dialog are 'OK' and 'Cancel' buttons. A vertical scrollbar is visible on the right side of the configuration area.

図15仮想サーバーの作成と(高度な構成)



#OK をクリックします。

## 設定の確認

1. ホストIPアドレス62.159.4.1から仮想サーバーIPアドレス61.159.4.100に送信されるFTP要求が、デバイスによってサーバーAに割り当てられることを確認します。  
#IP アドレス 62.159.4.1 のホスト上の仮想サーバーIP アドレス 61.159.4.100 にアクセスします。  
C:¥Users¥system>ftp 61.159.4.200  
Connected to 61.159.4.200.  
220 FTP service ready.  
User (61.159.4.200:(none)): admin  
331 Password required for admin.  
Password:  
230 User logged in.

ftp>

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Virtual Servers** を選択します。

図16 仮想サーバー統計情報の表示

Virtual server name	Slot No.	Packet count			Connection count		Details	
		Received	Sent	Dropped	Maximum	Active		Total
vs	1	30	30	0	2	0	3	

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Servers Farms** を選択します。

Device が 62.159.4.1 から送信された FTP 要求をサーバーファーム sf1 にていることがわかります。

図17サーバーファーム統計情報の表示

Server farm name	Slot No.	Packet count			Connection count		Details
		Received	Sent	Dropped	Active	Total	
sf1	1	30	30	0	0	3	
sf2	1	0	0	0	0	0	
sf3	1	0	0	0	0	0	

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Real Servers** を選択します。

Device が 62.159.4.1 から送信される FTP 要求を実サーバーrs\_a に割り当てることがわかります。

図18 実サーバーの統計情報の表示

Real server name	Slot No.	Packet count			Connection count		Details	
		Received	Sent	Dropped	Maximum	Active		Total
rs_a	1	30	30	0	2	0	3	
rs_b	1	0	0	0	0	0	0	
rs_c	1	0	0	0	0	0	0	

2. ホストIPアドレス63.159.4.1から仮想サーバーIPアドレス61.159.4.200に送信される FTP要求が、デバイスによってサーバーBに割り当てられることを確認します。

#IP アドレス 63.159.4.1 のホスト上の仮想サーバーIP アドレス 61.159.4.200 にアクセスします。

```
C:¥Users¥system>ftp 61.159.4.200
```

```
Connected to 61.159.4.200.
```

```
220 FTP service ready.
```

```
User (61.159.4.200:(none)): admin
```

331 Password required for admin.

Password:

230 User logged in.

ftp>

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Virtual Servers** を選択します。

図19 仮想サーバー統計情報の表示

Virtual server name	Slot No.	Packet count			Connection count		Details	
		Received	Sent	Dropped	Maximum	Active		Total
<input type="checkbox"/> vs	1	13	14	0	2	0	1	

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Servers Farms** を選択します。  
Device が 63.159.4.1 から送信された FTP 要求をサーバーファーム sf2 に割り当てていることがわかります。

図20サーバーファーム統計情報の表示

Server farm name	Slot No.	Packet count			Connection count		Details
		Received	Sent	Dropped	Active	Total	
<input type="checkbox"/> sf1	1	0	0	0	0	0	
<input type="checkbox"/> sf2	1	13	14	0	1	1	
<input type="checkbox"/> sf3	1	0	0	0	0	0	

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Real Servers** を選択します。  
Device が 63.159.4.1 からの FTP 要求を実サーバーrs\_b に割り当てていることがわかります。

図21 実サーバーの統計情報の表示

Real server name	Slot No.	Packet count				Connection count		Details
		Received	Sent	Dropped	Maximum	Active	Total	
<input type="checkbox"/> rs_a	1	0	0	0	0	0	0	
<input type="checkbox"/> rs_b	1	13	14	0	2	0	1	
<input type="checkbox"/> rs_c	1	0	0	0	0	0	0	

- デバイスが、ホストIPアドレス64.159.4.1から送信され、仮想サーバーIPアドレス61.159.4.200を宛先とするFTP要求をサーバーCに割り当ててることを確認します。

#IP アドレス 64.159.4.1 のホスト上の仮想サーバーIP アドレス 61.159.4.200 にアクセスします。

```
C:¥Users¥system>ftp 61.159.4.200
```

```
Connected to 61.159.4.200.
```

```
220 FTP service ready.
```

```
User (61.159.4.200:(none)): admin
```

```
331 Password required for admin.
```

```
Password:
```

```
230 User logged in.
```

```
ftp>
```

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Virtual Servers** を選択します。

図22 仮想サーバー統計情報の表示

Virtual server name	Slot No.	Packet count				Connection count		Details
		Received	Sent	Dropped	Maximum	Active	Total	
<input type="checkbox"/> vs	1	28	29	0	1	0	2	

- #トップナビゲーションバーで **Monitor** をクリックします。
- #ナビゲーションペインで、**Statistics > Server LB Statistics > Servers Farms** を選択します。
- Device が 64.159.4.1 から送信された FTP 要求をサーバーファーム sf3 に割り当てていることがわかります。

図23サーバーファーム統計情報の表示

Server farm name	Slot No.	Packet count			Connection count		Details
		Received	Sent	Dropped	Active	Total	
<input type="checkbox"/> sf1	1	0	0	0	0	0	
<input type="checkbox"/> sf2	1	0	0	0	0	0	
<input type="checkbox"/> sf3	1	28	29	0	0	2	

#トップナビゲーションバーで **Monitor** をクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Real Servers** を選択します。  
Device が 64.159.4.1 から送信された FTP 要求を実サーバーrs\_cに割り当てていることがわかります。

図24実サーバーの統計情報の表示

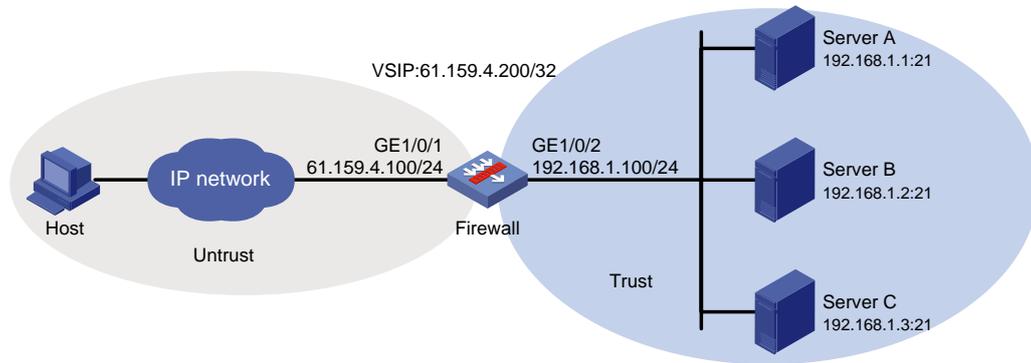
Real server name	Slot No.	Packet count				Connection count		Details
		Received	Sent	Dropped	Maximum	Active	Total	
<input type="checkbox"/> rs_a	1	0	0	0	0	0	0	
<input type="checkbox"/> rs_b	1	0	0	0	0	0	0	
<input type="checkbox"/> rs_c	1	28	29	1	0	0	2	

## 例:レイヤー7サーバーロードバランシングの設定

### ネットワーク構成

図1に示すように、企業はサーバーA、サーバーB およびサーバーC を使用して HTTP サービスを提供します。ホストからの HTTP 要求をロードバランシングするようにサーバーロードバランシングを構成します。デバイスは、URL にスポーツ、政府およびニュースが含まれる要求をサーバーAに割り当て、URL に財務、技術およびショッピングが含まれる要求をサーバーBに割り当て、その他の要求をサーバーCに割り当てます。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、**Network** をクリックします。
  - #ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。
  - #GE1/0/1 の **edit** アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - a) Basic Configurationタブで、Untrustセキュリティゾーンを選択します。
    - b) IPv4Addressタブで、インターフェイスのIPアドレスとマスク長を入力します。この例では、61.159.4.100/24と入力します。
    - c) OKをクリックします。
  - #GE1/0/ge1//2を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 192.168.1.100/24 に設定します。
2. セキュリティポリシーを作成します(詳細は省略)。
3. ICM Pタイプのプローブテンプレートを作成します。
  - #トップナビゲーションバーで、**Objects** をクリックします。
  - #ナビゲーションペインで、**Health Monitoring** を選択します。
  - #**Create** をクリックして、プローブテンプレート **t1** を設定します(図2を参照)。

図2 プロブテンプレートt1の作成

Basic configuration

Template name	<input type="text" value="t1"/>	*(1-32 chars)
Type	<input type="text" value="ICMP"/>	
Destination IP address	<input type="text"/>	(IPv4/IPv6 address)
Data to pad	<input type="text"/>	(0-200 chars)
Length of data to pad	<input type="text" value="100"/>	(20-65507)
Next hop IP address	<input type="text"/>	(IPv4/IPv6 address)
Outgoing interface	<input type="text"/>	
Probe interval <sup>?</sup>	<input type="text" value="5000"/>	ms(0-604800000)
Probe timeout <sup>?</sup>	<input type="text" value="3000"/>	ms(10-3600000)
Description	<input type="text"/>	(0-200 chars)

OK Cancel

#OK をクリックします。

4. HTTP cookie スティックグループを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Common Configuration > Sticky Groups** を選択します。

#**Create** をクリックして、スティックグループ **sticky\_group** を設定します(図3を参照)。

図3 スティックグループの作成sticky\_group

Create Sticky Group

Sticky group name  \*(1-63 chars)

Type  \*

Aging time  sec (0-31536000)

Override limits  Enable  Disable

Stickiness-over-busyness  Enable  Disable

Description  (0-127 chars)

Cookie stickiness

Cookie name  (0-63 chars. Default is X-I)

OK Cancel

#OK をクリックします。

5. 実サーバーを作成します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Server Load Balancing > Real Servers** を選択します。

#Create をクリックして実サーバーrs\_a を設定します(図4を参照)。

図4 実サーバーrs\_aの作成

Basic configuration

Real server name: rs\_a (1-63 chars)

IPv4 address: 192.168.1.1

IPv6 address: |

Port number: 0 (0-65535)

VPN instance: Public network

VPN instance inheritance:  Enable  Disable

Real server feature:  Enable  Disable

Description: (0-127 chars)

Advanced configuration

OK Cancel

#OK をクリックします。

#実サーバーrs\_bを設定し、その方法で、実サーバーrs\_bを設定し、その IP アドレスを 192.168.1.2 に設定します。

#実サーバーrs\_aを設定するのと同じ方法で、実サーバーrs\_cを設定し、その IP アドレスを 192.168.1.3 に設定します。

#設定されている実サーバーを表示します(図5を参照)。

図5 設定された実サーバーの表示

Real server name	Status	VRF	IP Address	Port number	Priority	Weight	Server farm	Real server f...	Edit
rs_a	●	Public network	192.168.1.1	0	4	100		Enable	
rs_b	●	Public network	192.168.1.2	0	4	100		Enable	
rs_c	●	Public network	192.168.1.3	0	4	100		Enable	

## 6. サーバーファームを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Server Farms を選択します。

#Create をクリックして、サーバーファーム sf1 を設定します(図6および図7を参照)。

図6サーバーファームsf1(l)の作成

The screenshot shows a 'Create Server Farm' dialog box with the following configuration:

- Server farm name:** sf1 (1-63 chars)
- Scheduling algorithm:** Hash source\_IP\_address
- Mask length:** 32 (0-32)
- Prefix length:** 128 (0-128)
- Priority scheduling:**  Limit real servers to participate in scheduling
- Minimum number:** (1-1000)
- Maximum number:** (1-1000)
- Real server:** A table with one entry: rs\_a, -, 192..., 0.
- Probe method:** (Add/Delete buttons)

Name	St...	O...	IPv4...	IPv6...	Port	Edit
rs_a		-	192...		0	

Buttons: OK, Cancel

図7サーバーファームsf1の作成(II)

#OK をクリックします。

#サーバーファーム sf2 を設定し、サーバーファーム sf1 と同じ方法で実サーバーrs\_bを指定します。

#サーバーファーム sf3 を設定し、サーバーファーム sf1 と同じ方法で実サーバーrs\_cを指定します。

#設定されたサーバーファームを表示します(図8を参照)。

図8設定されたサーバーファームの表示

Server farm name	Status	Scheduling algorithm	Total real servers	Available real servers	Edit
<input type="checkbox"/> sf1	●	Hash source IP address	1	1	
<input type="checkbox"/> sf2	●	Hash source IP address	1	1	
<input type="checkbox"/> sf3	●	Hash source IP address	1	1	

7. クラスを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Advanced Policies を  
選択します。

#クラスタブをクリックします。

#Create をクリックして、クラス cls\_1 を設定します(図9を参照)。

図9クラスcls\_1の作成

Class name: cls\_1 (1-63 chars)

Type: HTTP

Match type:  Match all  Match any

Match rule:

Rule ID	Type	Rule content
<input type="checkbox"/> 1	URL	sports
<input type="checkbox"/> 2	URL	government
<input type="checkbox"/> 3	URL	news

Description: (0-127 chars)

Buttons: OK, Cancel

#OK をクリックします。

#Create をクリックして、クラス cls\_2 を設定します(図10を参照)。

図10クラスcls\_2の作成

Class name: cls\_2 (1-63 chars)

Type: HTTP

Match type:  Match all  Match any

Match rule:

<input type="checkbox"/>	Rule ID	Type	Rule content
<input type="checkbox"/>	1	URL	finance
<input type="checkbox"/>	2	URL	technology
<input type="checkbox"/>	3	URL	shopping

Description: (0-127 chars)

OK Cancel

#OK をクリックします。

8. アクションを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Advanced Policies を選択します。

#Action タブをクリックします。

#Create をクリックして、action act\_1 を設定します(図11を参照)。

図11 action act\_1の作成

The screenshot shows the 'Create Action' dialog box with the following configuration:

- Basic configuration**
  - Action name: act\_1 (1-63 chars)
  - Type: HTTP
  - Forwarding mode: Load balance
  - Fallback action: Match next rule
  - ToS: (0-255)
  - Description: (0-127 chars)
- Server farms**
  - Primary server farm: sf1
  - Backup server farm: (empty)
  - Sticky group: sticky\_group
- Advanced configuration**
  - Response content rewrite:

Buttons: OK, Cancel

#OK をクリックします。

#action act\_2 を設定し、action act\_1 と同じ方法でプライマリサーバーファーム sf2 を指定します。

#action act\_3 を設定し、action act\_1 を設定するのと同じ方法でプライマリサーバーファーム sf3 を指定します。

#設定されたアクションを表示します(図12を参照)。

図12設定済みアクションの表示

Action name	Type	Forwarding action	Effective server farm	Edit
<input type="checkbox"/> act_1	HTTP	Load balance		
<input type="checkbox"/> act_2	HTTP	Load balance		
<input type="checkbox"/> act_3	HTTP	Load balance		

## 9. ロードバランシングポリシーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Advanced Policies を選択します。

#Load Balancing Policy タブをクリックします。

#Create をクリックして、ロードバランシングポリシーloadbalance\_policy を設定します(図13を参照)。

図13ロードバランシングポリシーの作成loadbalance\_policy

Class	Action
<input type="checkbox"/> cls_1	act_1
<input type="checkbox"/> cls_2	act_2

#OK をクリックします。

10. HTTPタイプのパラメータプロファイルを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Parameter Profiles を選択します。

#Create をクリックしてパラメータプロファイル loadbalance\_profile を設定します(図14を参照)。

図14パラメータプロファイルloadbalance\_profileの作成

Parameter profile name: loadbalance\_profile (1-63 chars)

Type: HTTP

Description: (0-127 chars)

HTTP-type parameters

Max header parse length: 4096 (1-65535)

Max content parse length: 4096 (1-65535)

Secondary cookie delimiter: /&#+ (1-4 chars)

Secondary cookie start delimiter: ? (1-2 chars)

Action on max-header-length exceeded packets:  Permit  Drop

Per-packet load balancing:  Enable  Disable

Connection reuse:  Enable  Disable

OK Cancel

#OKをクリックします。

11. 仮想サーバーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Virtual Servers を選択します。

#Create をクリックして、仮想サーバーを設定します(図15および図16を参照)。

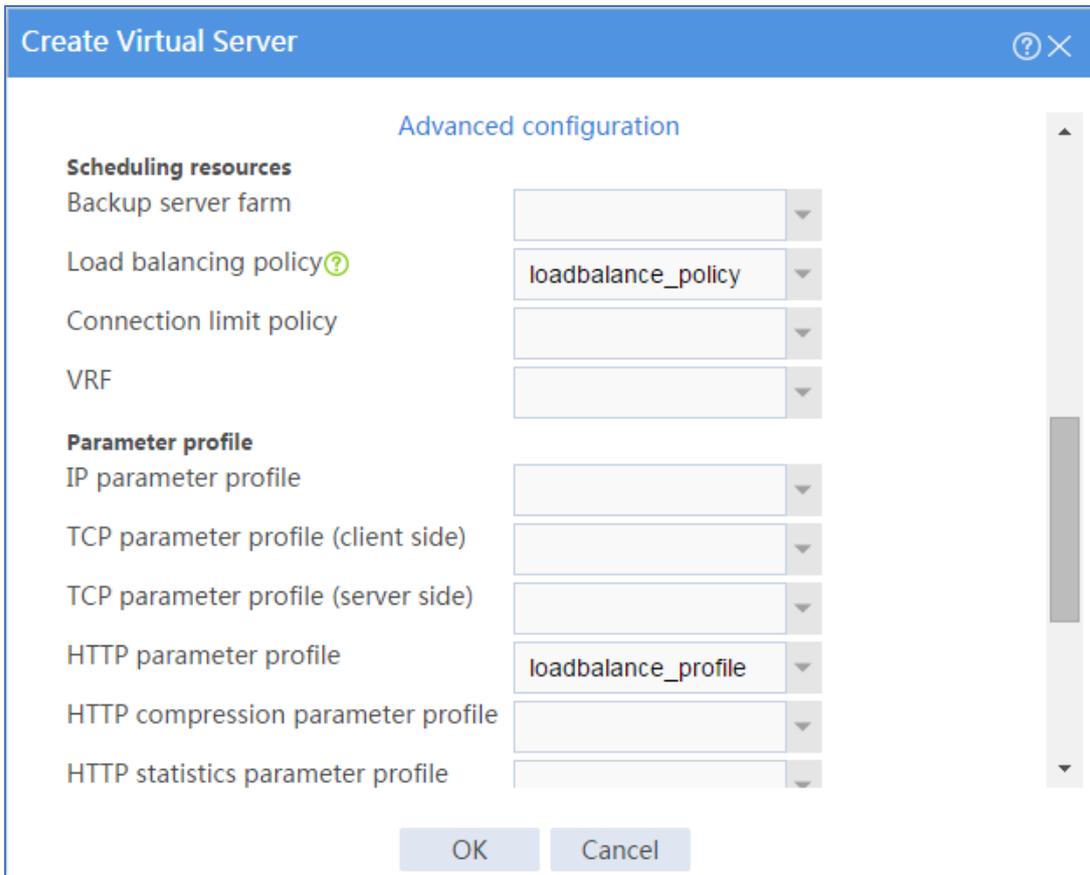
図15仮想サーバーの作成と(基本設定)

The image shows a 'Create Virtual Server' dialog box with a blue header bar containing a question mark icon and a close button. The main area is titled 'Basic configuration' and contains several fields and options:

- Virtual server name:** A text input field containing 'vs' with a red asterisk and '(1-63 chars)' to its right.
- Type:** A dropdown menu with 'HTTP' selected.
- IPv4 address:** A text input field containing '61.159.4.200'.
- IPv6 address:** An empty text input field.
- Port number:** A text input field containing '80' with '(1-65535)' to its right.
- Server farm:** A dropdown menu.
- Sticky group:** A dropdown menu.
- Interfaces for sending gratuitous ARP/ND packets IP address advertisement:** A dropdown menu with '[Edit]' to its right.
- Virtual server feature:** A section with three radio button options:
  - Enable  Disable
  - Enable  Disable
  - Enable  Disable

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

図16仮想サーバーの作成と(高度な構成)



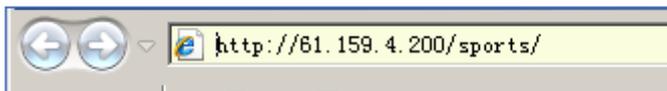
#OK をクリックします。

## 設定の確認

1. デバイスがサーバーAにURL <http://61.159.4.200/sports/> 付きのHTTP要求を割り当てることを確認します。

#ホスト上の <http://61.159.4.200/sports/> にアクセスします。

図17HTTPサービスへのアクセス



#トップナビゲーションバーで Monitor をクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Virtual Servers を選択します。

図18仮想サーバー統計情報の表示

Virtual server name	Slot No.	Packet count				Connection count		Details
		Received	Sent	Dropped	Maximum	Active	Total	
vs	1	14	9	0	3	1	3	

#トップナビゲーションバーでモニターをクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Servers Farms を選択します。デバイスが、URL <http://61.159.4.200/sports/>を含む HTTP 要求をサーバーファーム sf1 に割り当てていることがわかります。

図19サーバーファーム統計情報の表示

Server farm name	Slot No.	Packet count			Connection count		Details
		Received	Sent	Dropped	Active	Total	
sf1	1	4	3	0	1	1	
sf2	1	0	0	0	0	0	
sf3	1	0	0	0	0	0	

#トップナビゲーションバーで Monitor をクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Real Servers を選択します。デバイスが、URL <http://61.159.4.200/sports/>を含む HTTP 要求を実サーバーrs\_a に割り当てていることがわかります。

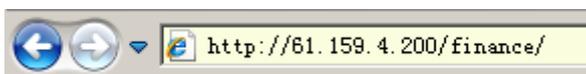
図20実サーバーの統計情報の表示

Real server name	Slot No.	Packet count				Connection count		Details
		Received	Sent	Dropped	Maximum	Active	Total	
rs_a	1	4	3	0	1	1	1	
rs_b	1	0	0	0	0	0	0	
rs_c	1	0	0	0	0	0	0	

2. デバイスがサーバーBに URL <http://61.159.4.200/finance/>付きの HTTP 要求を割り当てることを確認します。

#ホスト上の <http://61.159.4.200/finance/>にアクセスします。

図21HTTPサービスへのアクセス



#トップナビゲーションバーで Monitor をクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Virtual Servers を選択します。

図22仮想サーバー統計情報の表示

Virtual server name	Slot No.	Packet count			Connection count			Details
		Received	Sent	Dropped	Maximum	Active	Total	
<input type="checkbox"/> vs	1	6	5	0	0	1	0	

#トップナビゲーションバーで Monitor をクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Servers Farms を選択します。デバイスが、URL http://61.159.4.200/finance/を含む HTTP 要求をサーバーファーム sf2 に割り当てていることがわかります。

図23サーバーファーム統計情報の表示

Server farm name	Slot No.	Packet count			Connection count		Details
		Received	Sent	Dropped	Active	Total	
<input type="checkbox"/> sf1	1	0	0	0	0	0	
<input checked="" type="checkbox"/> sf2	1	6	5	0	1	1	
<input type="checkbox"/> sf3	1	0	0	0	0	0	

#トップナビゲーションバーで Monitor をクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Real Servers を選択します。デバイスが、URL http://61.159.4.200/finance/を含む HTTP 要求を実サーバーrs\_b に割り当てていることがわかります。

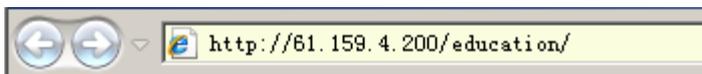
図24実サーバーの統計情報の表示

Real server name	Slot No.	Packet count			Connection count			Details
		Received	Sent	Dropped	Maximum	Active	Total	
<input type="checkbox"/> rs_a	1	0	0	0	0	0	0	
<input checked="" type="checkbox"/> rs_b	1	6	5	0	1	1	1	
<input type="checkbox"/> rs_c	1	0	0	0	0	0	0	

3. デバイスがサーバーC に URL http://61.159.4.200/education/付きの HTTP 要求を割り当てることを確認します。

#ホスト上の http://61.159.4.200/education/にアクセスします。

図25 HTTPサービスへのアクセス



#トップナビゲーションバーでモニターをクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Virtual Servers を選択します。

図26 仮想サーバー統計情報の表示

Virtual Server Statistics								
Auto refresh Refresh Clear Enter your keywords Search Advanced search								
Virtual server name	Slot No.	Packet count			Connection count		Details	
		Received	Sent	Dropped	Maximum	Active		Total
<input type="checkbox"/> vs	1	12	6	0	0	1	0	

#トップナビゲーションバーでモニターをクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Servers Farms** を選択します。デバイスが、URL http://61.159.4.200/education/を含む HTTP 要求をサーバーファーム sf3 に割り当てていることがわかります。

図27 サーバーファーム統計情報の表示

Server Farm Statistics								
Auto refresh Refresh Enter your keywords Search Advanced search								
Server farm name	Slot No.	Packet count			Connection count		Details	
		Received	Sent	Dropped	Active	Total		
<input type="checkbox"/> sf1	1	0	0	0	0	0	0	
<input type="checkbox"/> sf2	1	0	0	0	0	0	0	
<input type="checkbox"/> sf3	1	12	12	0	1	0	0	

#トップナビゲーションバーで Monitor をクリックします。

#ナビゲーションペインで、Statistics>Server LB Statistics>Real Servers を選択します。デバイスが、URL http://61.159.4.200/education/を含む HTTP 要求を実サーバーrs\_c に割り当てていることがわかります。

図28 実サーバーの統計情報の表示

Real Server Statistics								
Auto refresh Refresh Clear Enter your keywords Search Advanced search								
Real server name	Slot No.	Packet count			Connection count		Details	
		Received	Sent	Dropped	Maximum	Active		Total
<input type="checkbox"/> rs_a	1	0	0	0	0	0	0	
<input type="checkbox"/> rs_b	1	0	0	0	0	0	0	
<input type="checkbox"/> rs_c	1	12	12	0	0	1	0	

# アウトバウンドリンクロードバランシングの設定例

## はじめに

次に、発信リンクロードバランシングの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、発信リンクロードバランシング機能の基本的な知識があることを前提としています。

## 例:アウトバウンドリンクロードバランシングの設定

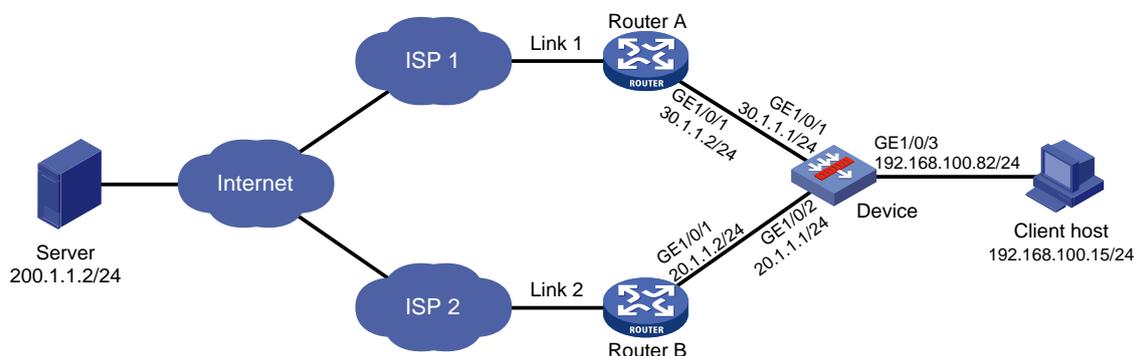
### ネットワーク構成

ISP1 と ISP2 は、2 つのリンク(リンク 1 とリンク 2)を企業に提供します。両方のリンクのルータホップカウント、帯域幅、およびコストは同じです。

次の要件を満たすようにアウトバウンドリンクロードバランシングを設定します。

- SoHu ビデオアプリケーションのトラフィックは、リンク Link1 に配信されます。
- 他のすべてのアプリケーションのトラフィックは、リンク Link2 に配信されます。

図1ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。
  - #トップナビゲーションバーで、Network タブをクリックします。
  - #ナビゲーションペインで、Interface Configuration>Interfaces を選択します。
  - #GE1/0/1 の編集アイコンをクリックします。
  - #開いたダイアログボックスで、インターフェイスを設定します。
    - a) Basic Configuration タブで、Untrust セキュリティゾーンを選択します。
    - b) IPv4Address タブで、インターフェイスの IP アドレスとマスク長を入力します。この例では、30.1.1.1/24 と入力します。
    - c) OK をクリックします。
  - #Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。
  - #GE1/0/ge1//3 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 192.168.100.82/24 に設定します。
2. ゾーンUntrustからゾーンTrustへのセキュリティポリシーを作成します。
  - #トップナビゲーションバーで、Policies をクリックします。
  - #ナビゲーションペインで、Security Policies>Security Policies を選択します。
  - #Create>Create a policy を選択します。
  - #開いたダイアログボックスで、セキュリティポリシーを設定します。

- ソースゾーン **Untrust** を選択します。
  - ターゲットゾーンの **trust** を選択します。
  - アクション許可を選択します。
  - OK をクリックします。
3. ICMPプローブテンプレートを設定します。
- #トップナビゲーションバーで、**Objects** をクリックします。
- #ナビゲーションペインで、Health Monitoring をクリックします。
- #create をクリックします。
- #開いたダイアログボックスで、ICMP プローブテンプレートを設定します。
- a) テンプレート名 t1 を入力します。
  - b) ICMP タイプを選択します。
  - c) Length of data to pad フィールドに 100 と入力します。
  - d) Probe interval フィールドに 5000 と入力します。
  - e) Probe timeout フィールドに 3000 と入力します。
  - f) OK をクリックします。

図 2 ICMP プローブテンプレートの作成

Basic configuration

Template name	<input type="text" value="t1"/>	*(1-32 chars)
Type	<input type="text" value="ICMP"/>	
Destination IP address	<input type="text"/>	(IPv4/IPv6 address)
Data to pad	<input type="text"/>	(0-200 chars)
Length of data to pad	<input type="text" value="100"/>	(20-65507)
Next hop IP address	<input type="text"/>	(IPv4/IPv6 address)
Outgoing interface	<input type="text"/>	
Probe interval <sup>?</sup>	<input type="text" value="5000"/>	ms(0-604800000)
Probe timeout <sup>?</sup>	<input type="text" value="3000"/>	ms(10-3600000)
Description	<input type="text"/>	(0-200 chars)

OK Cancel

4. アプリケーショングループを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

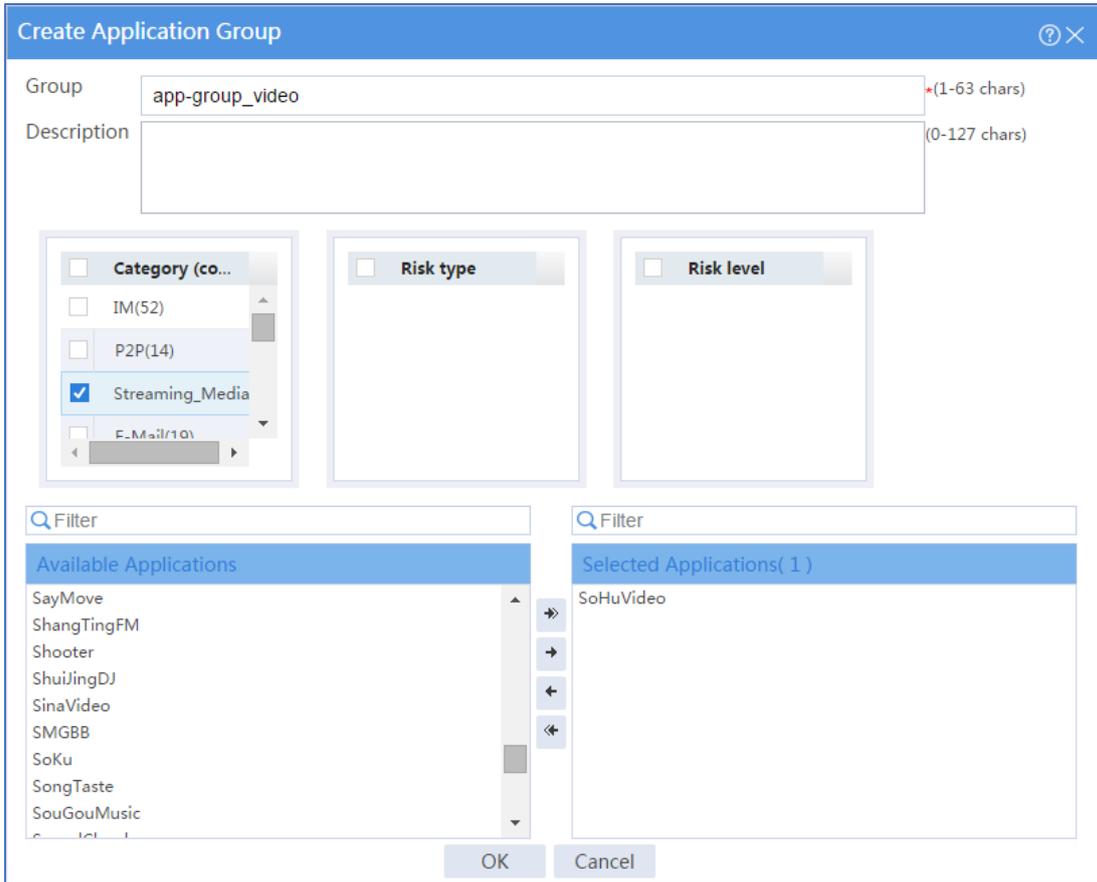
#ナビゲーションペインで、APPSecurity>APP Recognition>Application Groups を選択します。

#create をクリックします。

#開いたダイアログボックスで、app-group\_video という名前のアプリケーショングループを設定します。

- グループ名 app-group\_video を入力します。
- Streaming\_Media カテゴリ内のアプリケーション SoHuVideo を Selected Applications ペインに追加します。
- OK をクリックします。

図 3 アプリケーショングループの作成



5. リンクを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、Load Balancing>Common Configuration>Links を選択します。

#create をクリックします。

#開いたダイアログボックスで、link1 という名前のリンクを設定します。

- リンク名 link1 を入力してください
- Next hop config method フィールドで Manual を選択します。
- ネクストホップ IPv4 アドレス 30.1.1.2 を入力します。
- 近接計算のリンクコストを 0 に設定します。
- リンク機能を有効にします。
- VRF 継承をイネーブルにします。

- OK をクリックします。

図 4 リンク link1 を作成しています

The image shows a 'Create Link' dialog box with a blue header and a white body. The title bar contains a question mark icon and a close button. The main content area is titled 'Basic configuration' and contains the following fields and options:

- Link name:** A text input field containing 'link1' with a red asterisk and '(1-63 chars)' to its right.
- Next hop config method:** Two radio buttons: 'Manual' (selected) and 'Automatic'.
- Next hop IPv4 address:** A text input field containing '30.1.1.2'.
- Next hop IPv6 address:** An empty text input field.
- Link cost for proximity calculation:** A text input field containing '0' with a green question mark icon and '(0-10240)' to its right.
- Link feature:** Two radio buttons: 'Enable' (selected) and 'Disable'.
- VRF:** A dropdown menu showing 'Public network'.
- VRF inheritance:** Two radio buttons: 'Enable' (selected) and 'Disable', with a green question mark icon to the left.
- Description:** A large text input field with '(0-127 chars)' to its right.

At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

#link link1 を設定するのと同じ方法で link link2 を設定します。

図 5 リンク link2 の作成

The screenshot shows a 'Create Link' dialog box with the following fields and options:

- Link name:** link2 (1-63 chars)
- Next hop config method:** Manual (selected), Automatic
- Next hop IPv4 address:** 20.1.1.2
- Next hop IPv6 address:** (empty)
- Link cost for proximity calculation:** 0 (0-10240)
- Link feature:** Enable (selected), Disable
- VRF:** Public network (dropdown)
- VRF inheritance:** Enable (selected), Disable
- Description:** (0-127 chars)

Buttons: OK, Cancel

6. リンクグループを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、Load Balancing>Link Load Balancing>Outbound Link LB を選択します。

#リンクグループタブで、create をクリックします。

#開いたダイアログボックスで、Link\_group1 という名前のリンクグループを設定します。

- リンクグループ名 Link\_group1 を入力します。
- 動的近接を無効にします。
- スケジュールアルゴリズムラウンドロビンを選択します。
- プローブ方法 t1 を選択します。
- 成功基準を少なくとも 1 に設定します。
- link link1 をリンクグループに追加します。
- OK をクリックします。

図 6 リンクグループ Link\_group1 の作成

Link group name: Link\_group1 \*(1-63 chars)

Dynamic proximity:  Enable  Disable

Scheduling algorithm: Round robin

Lower percentage: (1-99)

Upper percentage: (1-99)

Priority scheduling  Limit links to participate in scheduling

Minimum number: \*(1-1000)

Maximum number: \*(1-1000)

Probe method: t1 [Edit]

Success criteria: At least 1 probes succeed(1-4294967295)

Member list

+ Add | X Delete

<input type="checkbox"/>	Name	Status	Next hop IPv4...	Next hop IPv6...	Edit
<input type="checkbox"/>	link1		30.1.1.2		

OK Cancel

#リンクグループ Link\_group1 を設定するのと同じ方法で、リンクグループ Link\_group2 を設定します。

図 7 リンクグループ Link\_group2 の作成

Link group name: Link\_group2 \*(1-63 chars)

Dynamic proximity:  Enable  Disable

Scheduling algorithm: Round robin

Lower percentage: (1-99)

Upper percentage: (1-99)

Priority scheduling  Limit links to participate in scheduling

Minimum number: \*(1-1000)

Maximum number: \*(1-1000)

Probe method: t1 [Edit]

Success criteria: At least 1 probes succeed(1-4294967295)

Member list: + Add - Delete

<input type="checkbox"/>	Name	Status	Next hop IPv4...	Next hop IPv6...	Edit
<input type="checkbox"/>	link2		20.1.1.2		

OK Cancel

## 7. クラスを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Link Load Balancing>Outbound Link LB を選択します。

#クラスタブで、create をクリックします。

#開いたダイアログボックスで、class\_app という名前のクラスを設定します。

- クラス名 class\_app を入力します。
- Match type フィールドで Match any を選択します。
- 一致ルールとしてアプリケーショングループ app-group\_video を追加します。
- OK をクリックします。

図 8 クラス class\_app の作成

Class name: class\_app \*(1-48 chars)

Match type:  Match all  Match any

Match rule:

<input type="checkbox"/>	Match ID	Type	HTTP entity
<input type="checkbox"/>	1	Applicati...	app-group_video

Description: (0-127 chars)

OK Cancel

8. IPv4ルーティングポリシーを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Link Load Balancing>Outbound Link LB を選択します。

#IPv4Routing Policy タブの Global configuration 領域で、LB サービスとリンク保護を有効にします。

図 9 グローバル構成

Global configuration

LB service	<input checked="" type="checkbox"/>	Link protection	<input checked="" type="checkbox"/>
Session extension information synchronization	<input type="checkbox"/>	Sticky entry synchronization	<input type="checkbox"/>

#IPv4Routing Policy タブの Policy 領域で、Create をクリックします。

#開いたダイアログボックスで、IPv4 ルーティングポリシーを設定します。

- class-app という名前を選択します。
- 転送モードロードバランスを選択します。
- プライマリリンクグループ link\_group1 を選択します。
- Fallback action フィールドで Match next rule を選択します。
- OK をクリックします。

図 10 クラス class-app の作成

#IPv4Routing Policy タブの Policy 領域で、Default という名前のデフォルト IPv4 ルーティングポリシーの Edit アイコンをクリックします。

#開いたダイアログボックスで、デフォルトの IPv4 ルーティングポリシーを設定します。

- 転送モードロードバランスを選択します。
- プライマリリンクグループ link\_group2 を選択します。

- OK をクリックします。

図 11 デフォルト IPv4 ルーティングポリシーの編集

IPv4 ルーティングポリシーの設定は次のとおりです。

図 12 IPv4 ルーティングポリシーの設定

Class	Forwarding mode	Primary link group	Backup link group	Sticky group	Edit
class_app	Load balance	link_group1			
Default	Load balance	link_group2			

## 設定の確認

1. SoHuビデオクライアントを開き、再生するムービーを選択します。
2. SoHuビデオクライアントのトラフィックがリンクlink1を介して送信されることを確認します。

#トップナビゲーションバーで、Monitor タブをクリックします。

#ナビゲーションペインで、Statistics>Outbound Link LB Statistics>Links を選択します。

Link Statistics ページは次のとおりです。

図 13 リンク統計情報

The screenshot shows the 'Link Statistics' page with a table of data. The table has the following structure:

Link name	Output interface rate (Bps)		Slot No.	Bandwidth (KBps)	Connection rate	Connection count		Details
	Inbound	Outbound				Active	Total	
<input type="checkbox"/> link1	31	49	1	0	3	1	629	
<input type="checkbox"/> link2	50	471	1	0	0	1	1	

# インバウンドリンクロードバランシングの設定例

## はじめに

次に、インバウンドリンクロードバランシングの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、インバウンドリンクロードバランシング機能の基本的な知識があることを前提としています。

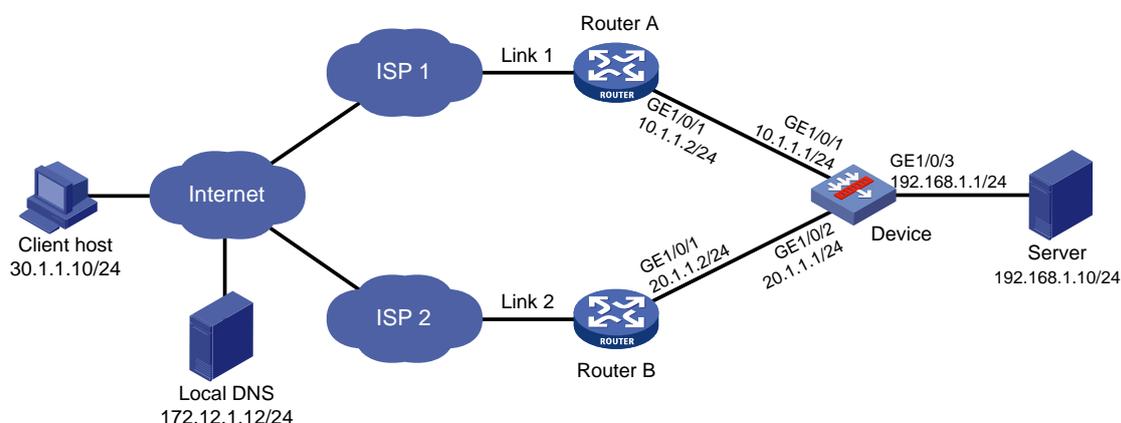
## 例:インバウンドリンクロードバランシングの設定

### ネットワーク構成

図1に示すように、ISP1 と ISP2 は、2 つのリンク(リンク 1 とリンク 2)を企業に提供します。両方のリンクのルータホップカウント、帯域幅、およびコストは同じです。

クライアントホストからサーバーへのトラフィックに最適なリンクを選択するように、デバイスのインバウンドリンクロードバランシングを設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

着信リンクロードバランシングを設定する場合は、次の制限事項およびガイドラインに従ってください。

- サーバーのロードバランシングも有効になっている場合に、インバウンドリンクのロードバランシングが正しく動作するように、仮想サーバーの IP アドレスを DNS リスナーの IP アドレスとして指定しないでください。
- インバウンドリンクロードバランシングのための仮想サーバーの IPv4 アドレスは、32 ビットのマスク長を持つユニキャストアドレスである必要があります。IPv4 アドレスのアドレスにすることはできません。
- LB デバイスをオーソリテティブ DNS サーバーとして指定するために、ローカル DNS サーバー上に委任ドメインを構成するには、ISP に問い合わせる必要があります。

## 手順

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、Network タブをクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の **edit** アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) Basic Configuration タブで、Untrust セキュリティゾーンを選択します。
- b) IPv4Address タブで、インターフェイスの IP アドレスとマスク長を入力します。この例では、10.1.1.1/24 と入力します。
- c) OK をクリックします。

#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1./24 に設定します。

#GE1/0/ge1//3 を追加し、GE1/0/1 の設定と同じ方法で IP アドレスを 192.168.1.1/24 に設定します。

## 2. ゾーンUntrustからゾーンTrustへのセキュリティポリシーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#Create>Create a policy を選択します。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ソースゾーン **Untrust** を選択します。
- ターゲットゾーンの **trust** を選択します。
- アクション許可を選択します。
- OK をクリックします。

## 3. ICMPプローブテンプレートを設定します。

#トップナビゲーションバーで、**Objects** をクリックします。

#ナビゲーションペインで、**Health Monitoring** をクリックします。

#**create** をクリックします。

#開いたダイアログボックスで、ICMP プローブテンプレートを設定します。

- a) テンプレート名 t1 を入力します。
- b) ICMP タイプを選択します。
- c) Length of data to pad フィールドに 100 と入力します。
- d) Probe interval フィールドに 5000 と入力します。
- e) Probe timeout フィールドに 3000 と入力します。
- f) OK をクリックします。

図2ICMP プローブテンプレートの作成

Basic configuration

Template name	t1	(1-32 chars)
Type	ICMP	
Destination IP address		(IPv4/IPv6 address)
Data to pad		(0-200 chars)
Length of data to pad	100	(20-65507)
Next hop IP address		(IPv4/IPv6 address)
Outgoing interface		
Probe interval?	5000	ms(0-604800000)
Probe timeout?	3000	ms(10-3600000)
Description		(0-200 chars)

OK Cancel

4. リンクを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Common Configuration > Links** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、link1 という名前のリンクを設定します。

**基本構成:**

- リンク名 link1 を入力してください
- Next hop config method フィールドで Manual を選択します。
- ネクストホップ IPv4 アドレス 10.1.1.2 を入力します。
- リンク機能を有効にします。
- VRF 継承をイネーブルにします。

図 3 link link1 の作成(基本設定)

The screenshot shows a 'Create Link' dialog box with the following fields and options:

- Link name:** link1 (1-63 chars)
- Next hop config method:** Manual (selected), Automatic
- Next hop IPv4 address:** 10.1.1.2
- Next hop IPv6 address:** (empty)
- Link cost for proximity calculation:** 0 (0-10240)
- Link feature:** Enable (selected), Disable
- VRF:** Public network
- VRF inheritance:** Enable (selected), Disable
- Description:** (empty) (0-127 chars)

Buttons: OK, Cancel

**高度な構成:**

- weight100 と入力します。
- 優先順位 4 を入力します。
- プローブ方法 t1 を選択します。
- 成功基準を少なくとも 1 に設定します。
- 合計帯域幅比率 70%を入力します。
- 帯域幅回復率 60%を入力します。
- インバウンド帯域幅比率 70%を入力します。
- OK をクリックします。

図 4 link link1 の作成(詳細設定)

The screenshot shows a 'Create Link' dialog box with a blue header and a white body. The title bar contains a question mark icon and a close button. The main area is titled 'Advanced configuration' and contains several settings:

- Weight**: Input field with '100' and '(1-255)' range.
- Priority**: Input field with '4' and '(1-8)' range.
- Link group**: A dropdown menu that is currently empty.
- Probe method**: A dropdown menu with 't1' selected and an '[Edit]' link to its right.
- Success criteria**: A dropdown menu with 'At least' selected and an input field with '1' and 'probes succeed (1-4294967295)' range.
- Bandwidth ratio** (Total bandwidth): Input field with '70' and '% (1-100)' range.
- Bandwidth recovery ratio**: Input field with '60' and '% (1-100)' range.
- Inbound bandwidth**: Input field with '70' and '% (1-100)' range.

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

#link link1 を設定するのと同じ方法で link link2 を設定します。

図5 link link2 の作成(基本設定)

The screenshot shows the 'Create Link' dialog box with the 'Basic configuration' tab selected. The fields are as follows:

Field	Value	Constraint
Link name	link2	*(1-63 chars)
Next hop config method	Manual	Manual (selected), Automatic
Next hop IPv4 address	20.1.1.2	
Next hop IPv6 address		
Link cost for proximity calculation	0	(0-10240)
Link feature	Enable	Enable (selected), Disable
VRF	Public network	Public network (selected)
VRF inheritance	Enable	Enable (selected), Disable
Description		(0-127 chars)

Buttons: OK, Cancel

図6 link link2 の作成(詳細設定)

The screenshot shows the 'Create Link' dialog box with the 'Advanced configuration' tab selected. The fields are as follows:

Field	Value	Constraint
Weight	100	(1-255)
Priority	4	(1-8)
Link group		
Probe method	t1	[Edit]
Success criteria	At least 1	probes succeed (1-4294967295)
<b>Bandwidth ratio</b>		
<b>Total bandwidth</b>		
Bandwidth ratio	70	% (1-100)
Bandwidth recovery ratio	60	% (1-100)
<b>Inbound bandwidth</b>		
Bandwidth ratio	70	% (1-100)

Buttons: OK, Cancel

5. 実サーバーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Server Load Balancing > Real Servers** を選択します。

#**creste** をクリックします。

#開いたダイアログボックスで、rs という名前の実サーバーを設定します。

- サーバー名 rs を入力します。
- IPv4 アドレス 192.168.1.10 を入力します。
- ポート番号 0 を入力します。
- VRF 継承をイネーブルにします。
- 実サーバーを有効にします。
- OK をクリックします。

図7実サーバーrs の作成

The screenshot shows a 'Create Real Server' dialog box with a blue header and a white body. The title bar contains a question mark icon and a close icon. The main content is titled 'Basic configuration' and includes the following fields and options:

- Real server name: Text input field containing 'rs', with a red asterisk and '(1-63 chars)' to the right.
- IPv4 address: Text input field containing '192.168.1.10'.
- IPv6 address: Empty text input field.
- Port number: Text input field containing '0', with '(0-65535)' to the right.
- VPN instance: Dropdown menu showing 'Public network'.
- VPN instance inheritance: Radio buttons for 'Enable' (selected) and 'Disable'.
- Real server feature: Radio buttons for 'Enable' (selected) and 'Disable'.
- Description: Text area, empty, with '(0-127 chars)' to the right.

Below the 'Basic configuration' section is a section titled 'Advanced configuration' which is currently collapsed. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

6. サーバーファームを構成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Server Load Balancing>Server Farms を選択します。

#create をクリックします。

#開いたダイアログボックスで、sf:という名前のサーバーファームを設定します。

- サーバーファーム名 sf を入力します。
- スケジューリングアルゴリズム Hash source\_IP\_address を選択します。
- マスク長 32 とプレフィクス長 128 を入力します。
- 実サーバーrs をサーバーファームに追加します。
- プロブ方法 t1 を選択します。
- OK をクリックします。

図8サーバーファーム sf の作成

The screenshot shows the 'Create Server Farm' dialog box with the following configuration:

- Server farm name:** sf (1-63 chars)
- Scheduling algorithm:** Hash source\_IP\_address
- Mask length:** 32 (0-32)
- Prefix length:** 128 (0-128)
- Priority scheduling:**  Limit real servers to participate in scheduling
- Minimum number:** (1-1000)
- Maximum number:** (1-1000)
- Real server:** A table with one entry: rs, with IP 192... and Port 0.
- Probe method:** (partially visible)

Buttons: OK, Cancel

7. 仮想サーバーを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Server Load Balancing > Virtual Servers** を選択します。

#**create** をクリックします。

#開いたダイアログボックスで、vs1 という名前の仮想サーバーを設定します。

- サーバー名 vs1 を入力します。
- タイプ HTTP を選択します。
- IPv4 アドレス 10.1.1.3 を入力します。
- ポート番号 80 を入力します。
- サーバーファーム sf を選択します。
- IP アドレスアダプタサイズメントをディセーブルにします。
- ステックエントリの同期化をイネーブルにします。
- 仮想サーバーを有効にします。
- OK をクリックします。

図9仮想サーバーの作成 vs1

The screenshot shows a 'Create Virtual Server' dialog box with a blue header. The title bar contains a question mark icon and a close icon. The main area is titled 'Basic configuration' and contains the following fields and options:

Virtual server name	vs1	*(1-63 chars)
Type	HTTP	
IPv4 address	10.1.1.3	
IPv6 address		
Port number	80	(1-65535)
Server farm	sf	
Sticky group		
Interfaces for sending gratuitous ARP/ND packets IP address advertisement		[Edit]
	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Sticky entry synchronization	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Virtual server feature ?	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

#仮想サーバーと1を設定するのと同じ方法で、仮想サーバーと2を設定します。

図10仮想サーバーの作成 vs2

The screenshot shows a 'Create Virtual Server' dialog box with the following fields and options:

- Virtual server name: vs2 (1-63 chars)
- Type: HTTP
- IPv4 address: 20.1.1.3
- IPv6 address: (empty)
- Port number: 80 (1-65535)
- Server farm: sf
- Sticky group: (empty)
- Interfaces for sending gratuitous ARP/ND packets IP address advertisement: (empty) [Edit]
- Virtual server feature: Enable (selected), Disable
- Sticky entry synchronization: Enable (selected), Disable

Buttons: OK, Cancel

8. 仮想IPプールを設定します。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**Load Balancing > Link Load Balancing > Inbound Link LB** を選択します。

#Virtual IP Pool タブで、Create をクリックします。

#開いたダイアログボックスで、vsp という名前の仮想 IP プールを設定します。

- プール名 vsp を入力します。
- 優先予測子の選択加重ラウンドロビン。
- 仮想 IP プールに仮想サーバー-vs1 および vs2 を追加します。
- リンク保護を無効にします。
- OK をクリックします。

図11 仮想 IP プール vsp の作成

Virtual IP pool name: vsp (1-63 chars)

Preferred predictor: Weighted round robin

Backup predictor:

Alternative predictor:

Virtual IP list

<input type="checkbox"/>	Virtual IP address	Link	Weight
<input type="checkbox"/>	vs1 (10.1.1.3)	link1	100
<input type="checkbox"/>	vs2 (20.1.1.3)	link2	100

Link protection:  Enable  Disable

OK Cancel

9. DNSマッピングを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Link Load Balancing>Inbound Link LB を選択します。

#DNS Mapping タブで Create をクリックします。

#開いたダイアログボックスで、dm:という名前の DNS マッピングを設定します。

- DNS マッピング名 dm を入力します。
- 仮想 IP プール vsp を選択します。
- ドメイン名リストにドメイン名 www.aaa.com を追加します。
- TTL を 3600 秒に設定します。
- DNS マッピングを有効にします。

- OK をクリックします。

図12 DNS マッピング dm の作成

Create DNS Mapping

DNS mapping name  \*(1-63 chars)

Virtual IP pool  \*

Domain name list  + Add X Delete \*(1-253 chars)

<input type="checkbox"/>	Domain name
<input type="checkbox"/>	www.aaa.com

TTL  seconds(0-4294967295)

DNS mapping  Enable  Disable

OK Cancel

#### 10. DNSリスナーを構成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Load Balancing>Link Load Balancing>Inbound Link LB を選択します。

#DNS Listener タブで、Create をクリックします。

#開いたダイアログボックスで、dl1 という名前の DNS リスナーを設定します。

- DNS リスナー名 dl1 を入力します。
- IPv4 アドレス 10.1.1.1 を入力します。
- ポート番号 53 を入力します。
- DNS リスニングを有効にします。
- 存在しないドメインの処理フィールドで DNS 拒否で応答するを選択します。
- OK をクリックします。

図13DNSリスナ d1 の作成

Create DNS Listener

DNS listener name  \*(1-63 chars)

IPv4 address

IPv6 address

Port number  (1-65535)

VRF

DNS listening  Enable  Disable

Processing for nonexistent domain  Do not respond  Respond with a DNS reject  Respond through a DNS proxy

OK Cancel

#DNS リスナ dl1 を構成するのと同じ方法で DNS リスナ dl2 を構成します。

図14DNS リスナーdl2 の作成

Create DNS Listener

DNS listener name: dl2 (1-63 chars)

IPv4 address: 20.1.1.1

IPv6 address:

Port number: 53 (1-65535)

VRF: Public network

DNS listening:  Enable  Disable

Processing for nonexistent domain:  Do not respond  Respond with a DNS reject  Respond through a DNS proxy

OK Cancel

## 設定の確認

1. ホストのブラウザからhttp://www.aaa.comにアクセスし、デバイスがHTTP要求をリンク link1およびlink2に配布することを確認します。

#トップナビゲーションバーで、**Monitor** タブをクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Virtual Servers** を選択します。

Virtual Server Statistics ページは次のとおりです。

図15仮想サーバー統計情報

Virtual server name	Slot No.	Packet count			Connection count			Details
		Received	Sent	Dropped	Maximum	Active	Total	
<input type="checkbox"/> vs1	1	372	692	0	6	6	6	<a href="#">Details</a>
<input type="checkbox"/> vs2	1	410	621	0	6	0	13	<a href="#">Details</a>

2. 仮想サーバーvs1をディセーブルにし、ホストのブラウザからhttp://www.aaa.comにアク

セスして、デバイスがHTTP要求をlink link2だけに配信することを確認します。

#トップナビゲーションバーで、**Monitor** タブをクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Virtual Servers** を選択します。

Virtual Server Statistics ページは次のとおりです。

図16仮想サーバー統計情報

Virtual server name	Slot No.	Packet count			Connection count			Details
		Received	Sent	Dropped	Maximum	Active	Total	
vs1	1	372	692	0	6	6	6	
vs2	1	410	621	0	6	0	13	

3. 仮想サーバーvs2をディセーブルにし、ホストのブラウザからhttp://www.aaa.comにアクセスして、デバイスがHTTP要求をlink link1だけに配信することを確認します。

#トップナビゲーションバーで、**Monitor** タブをクリックします。

#ナビゲーションペインで、**Statistics > Server LB Statistics > Virtual Servers** を選択します。

Virtual Server Statistics ページは次のとおりです。

図17仮想サーバー統計情報

Virtual server name	Slot No.	Packet count			Connection count			Details
		Received	Sent	Dropped	Maximum	Active	Total	
vs1	1	372	692	0	6	6	6	
vs2	1	410	621	0	6	0	13	

# NAT フローロギングの設定例

## はじめに

次に、NAT フローロギングの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

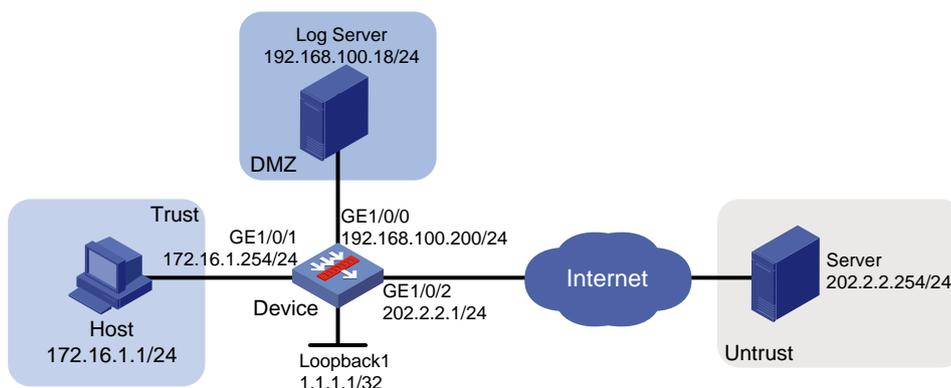
次の情報は、フローロギング、NAT ロギング、および NAT に関する基本的な知識があることを前提としています。

## 例:NATフローロギングの設定

### ネットワーク構成

図1に示すように、NAT セッション情報をログサーバーに送信してユーザーのトレース情報をログサーバーに送信し、ユーザーのトレースおよび分析を可能にします。内部ホストがパブリックネットワーク上のサーバーにアクセスすると、次のログ情報が記録されます。NAT 変換前後の送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、および宛先ポート番号。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 制限事項とガイドライン

- 変換後に IP アドレスとポート番号を記録するには、ログバージョン 3.0 を使用します。
- NAT フローロギングを有効にするには、NAT ロギングをイネーブルにする必要があります。
- ログは、ログホストとインフォメーションセンターに同時に送信できません。デフォルトでは、ログはログホストに送信されます。インフォメーションセンターがログ出力先として指定されている場合、ログはログホストに送信されません。

## 手順

### デバイスの設定

1. インターフェイスに IP アドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、Network をクリックします。

#ナビゲーションペインで、Interface Configuration>Interfaces を選択します。

#GE1/0/0 の edit アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) Basic Configuration タブで、DMZ セキュリティゾーンを選択します。
- b) IPv4Address タブで、インターフェイスの IP アドレスとマスク長を入力します。この例では、192.168.100.200/24 と入力します。
- c) OKをクリックします。

#GE1/0/1 を信頼セキュリティゾーンに追加し、GE1/0/0 と同じ方法で IP アドレスを 172.16.1.1/24 に設定します。#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/0 と同じ方法で IP アドレスを 202.2.2.1/24 に設定します。

## 2. セキュリティポリシーSecPolicy1を作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 SecPolicy1 を入力します。
- ソースゾーンの信頼を選択します。
- 宛先ゾーンを選択信頼解除。
- アクション許可を選択します。

#OK をクリックします。

## 3. セキュリティポリシーSecPolicy2を作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

#OK をクリックします。

## 4. NATを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT > Static NAT > Policy Configuration を選択します。

#create をクリックします。

#発信スタティック NAT マッピングを作成します(図2を参照)。

図2発信スタティック NAT マッピングの作成

Create Outbound Static NAT
?
✕

Translation method  One-to-one  Net-to-net  Address object group

Private address  \*

Public VRF  ▼

Private VRF  ▼

Public address  \*

ACL  ▼

Enable this rule

Counting

Important: This rule takes effect after you enable it on an interface in policy application page.

#OK をクリックします。

#トップナビゲーションバーで、**Policies** をクリックします。

#ナビゲーションペインで、**NAT > Static NAT > Apply Policy** を選択します。

#GE1/0/2 を選択し Enable をクリックします。マッピングがインターフェイスに適用されています (図3を参照)。

図3スタティック NAT マッピングの適用

Interface name	Interface description	Status
<input type="checkbox"/> GE1/0/18	GigabitEthernet1/0/18 Interface	Disabled
<input type="checkbox"/> GE1/0/2	GigabitEthernet1/0/2 Interface	Enabled

5. フローロギングを設定します。

#トップナビゲーションバーで、system をクリックします。

#ナビゲーションペインで、Log Settings>Basic Settings を選択します。

#Flow Log タブで、フローロギングを設定します(図4を参照)。

図4フローロギングの設定

Log version  1.0  3.0  5.0

Load balancing

Source IP for log packets

Apply

<input type="checkbox"/>	Log host address	Port number	VRF	Edit
<input type="checkbox"/>	192.168.100.18	514	Public network	

6. NATロギングを設定します。

#トップナビゲーションバーで、system をクリックします。

#ナビゲーションペインで、Log Settings>NAT Log Settings を選択します。

#NAT ロギングを設定します(図5を参照)。

図5 NAT ログिंगの設定

NAT Log Settings

Enable NAT logging

Fast log output ?

Advanced configuration

NAT session logging

NAT session establishment logging

NAT session removal logging

Active NAT session logging ?

Logging interval  \*minutes (10-120)

ACL ?

NAT444 logging

NAT444 port block assignment logging

NAT444 port block withdrawal logging

NAT resource exhaustion logging

Apply

#適用をクリックします。

### ログサーバーの設定

#ログサーバーを設定します(詳細は省略)。

## 設定の確認

ホストがパブリックネットワーク上のサーバーにアクセスしたときに、ログサーバー上にNATセッションログが生成されることを確認します。ログ情報には、変換前後の送信元IPアドレス、送信元ポート番号、宛先IPアドレス、および宛先ポート番号が含まれます。

# サーバー接続検出の設定例

## はじめに

次に、Server Connection Detection(SCD)の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、SCD 機能の基本的な知識があることを前提としています。

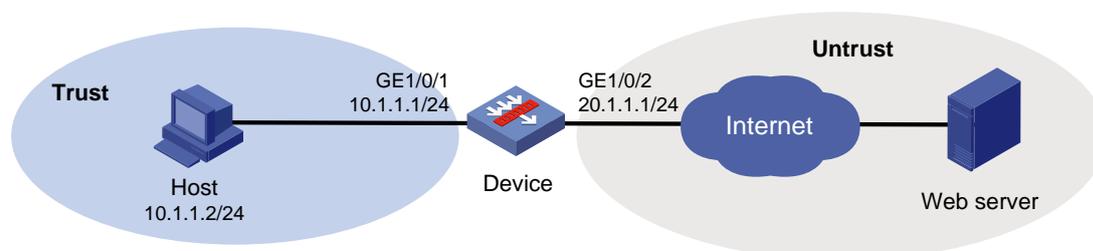
## 例:SCDの構成

## ネットワーク構成

図1に示すように、デバイス上で SCD を構成して次のタスクを実行します。0

- サブネット 2.2.1.0/24 内のサーバーによって開始された接続を 1 日間監視します。
- ホスト 2.2.3.2/24 上の TCP ポート 80 および 443 宛ての TCP 接続を除く、サーバーによって開始されたすべての接続をログに記録します。

図1 ネットワーク図



# 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、ルート、セキュリティゾーン、ゾーンペア、およびゾーン間ポリシーを設定します。ホストとWebサーバーが到達可能であることを確認します(詳細は省略)。

2. 内部IPアドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、Objects をクリックします。

#ナビゲーションペインで、Object Groups>IPv4Address Object Groups を選択します。

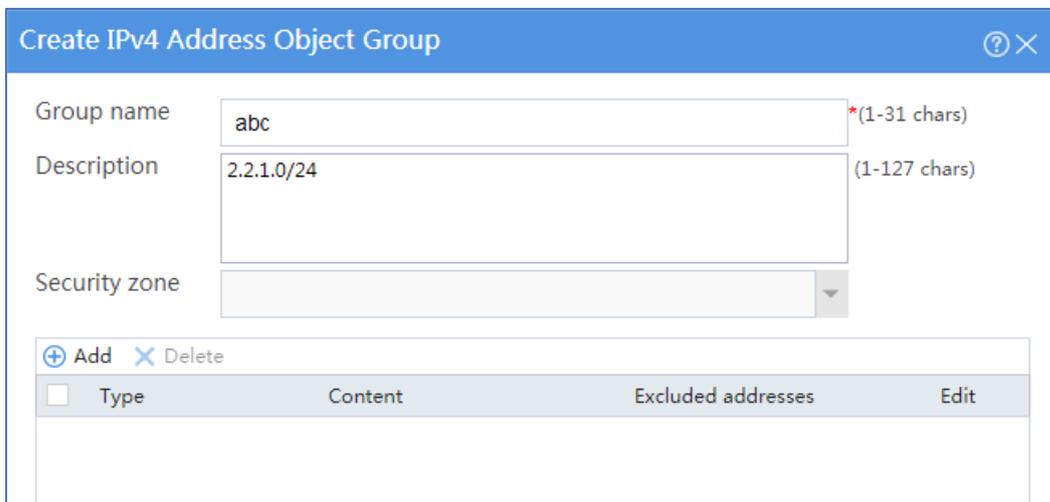
#create をクリックします。

#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。

a) グループ名を入力します。この例では、**abc**と入力します。

b) 説明を入力します。この例では、**2.2.1.0/24**と入力します。

図2IPv4アドレスオブジェクトグループの作成



Create IPv4 Address Object Group

Group name: abc (1-31 chars)

Description: 2.2.1.0/24 (1-127 chars)

Security zone: [Dropdown]

+ Add X Delete

Type	Content	Excluded addresses	Edit
------	---------	--------------------	------

c) addをクリックします。

d) 表示されるダイアログボックスで、ネットワークセグメントオブジェクトを選択し、IPv4アドレスとマスク**2.2.1.0/24**を入力します。

図3オブジェクトの作成

Create Object

Object Network segment

2.2.1.0 / 255.255.255.0 \* (IPv4 address/mask length (0-32))

Excluded addresses

OK Cancel

e) OKをクリックします。

1. サーバー接続の学習を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Server Connection Detect > SCD learning を選択します。

#サーバーのアドレスを入力します。この例では、abc と入力します。

#学習期間を選択します。この例では、24 時間を選択します。

#適用をクリックします。

図4サーバー接続ラーニングの設定

Server address abc [Edit]

Learning period 24 hours

Apply

4. SCDポリシーを構成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Server Connection Detect>SCD Policy を選択します。

#create をクリックします。

#開いたダイアログボックスで、SCD ポリシーを作成します。

a) ポリシー名を入力します。この例では、policy1 と入力します。

b) サーバーアドレスを入力します。この例では、2.2.1.2 と入力します。

- c) ポリシーを有効にします。
- d) SCDロギングを有効にします。

図5 SCD ポリシーの作成

The screenshot shows the 'Create SCD Policy' dialog box. It has a blue title bar with a question mark and a close button. The main area contains several fields and options:

- Policy name:** A text input field containing 'policy1'. A red asterisk and '(1-63 chars)' are to the right.
- Server address:** A text input field containing '2.2.1.2'. A red asterisk is to the right.
- Enable policy:** Two radio buttons, 'On' (selected) and 'Off'.
- SCD logging:** Two radio buttons, 'On' (selected) and 'Off'.
- SCD rules:** A section with a '+' icon and 'Create' button, and an 'X' icon and 'Delete' button. Below is a table with the following header:
 

ID	Destination address	Protocols and ports	Edit

- e) createをクリックします。
- f) 表示されるダイアログボックスで、宛先アドレス2.2.3.12とTCPポート80および443を入力します。

図6 SCD ルールの作成

The screenshot shows the 'Create SCD Rule' dialog box. It has a blue title bar with a question mark and a close button. The main area contains the following fields and options:

- Destination address:** A text input field containing '2.2.3.12'. A red asterisk is to the right.
- Protocols and ports:** A section with a blue header. It contains:
  - TCP:** A radio button (selected) with a question mark icon. To its right is a text input field containing '80,443' and '(1-65535)' to the right.
  - UDP:** A radio button (unselected) with a question mark icon. To its right is an empty text input field and '(1-65535)' to the right.
  - ICMP:** A radio button (unselected).
- Note:** A text box at the bottom of the section containing the text: 'Configure a minimum of one protocol. Only connections established'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom of the dialog.

- g) OKをクリックします。

図7SCDポリシーの表示

Policy name	Server address	SCD rule count	SCD logging	Enable	Edit
policy1	2.2.1.2	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

## 設定の確認

サーバー接続イベント用に生成されたログを表示するには、トップナビゲーションバーの Monitor をクリックし、ナビゲーションペインで **Device Logs > System Logs** を選択します。

図8デバイスログの表示

Time	Severity level	Module	Mnemonic	Details
2019-05-20 14:23:18	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=138;server illegal connection.
2019-05-20 14:22:59	● Informational	SCD	SCD_IPV4	Protocol(1001)=TCP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=172.8.30.41;DstPort(1008)=80;server illegal connection.
2019-05-20 14:22:32	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:21:00	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:20:59	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:20:59	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:20:32	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:18:32	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:17:54	● Informational	SCD	SCD_IPV4	Protocol(1001)=TCP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=172.8.30.41;DstPort(1008)=80;server illegal connection.
2019-05-20 14:16:32	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:14:32	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:12:49	● Informational	SCD	SCD_IPV4	Protocol(1001)=TCP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=172.8.30.41;DstPort(1008)=80;server illegal connection.
2019-05-20 14:12:32	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=10.153.0.11;DstPort(1008)=137;server illegal connection.
2019-05-20 14:11:15	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=138;server illegal connection.
2019-05-20 14:10:50	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.
2019-05-20 14:10:50	● Informational	SCD	SCD_IPV4	Protocol(1001)=UDP;ServerIPAddr(1003)=2.2.1.2;DstIPAddr(1007)=2.2.1.255;DstPort(1008)=137;server illegal connection.

# IP レピュテーションの設定例

## はじめに

次に、IP レピュテーションの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、IP レピュテーション機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

IP レピュテーションの使用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なくなります。

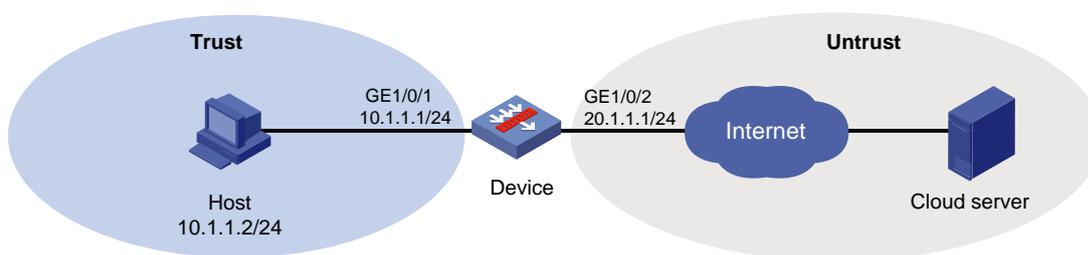
IP 評価リストの更新が 7 日間連続して失敗すると、デバイスは IP 評価リストをクリアし、IP 評価は使用できなくなります。

## 例:IPレピュテーションの設定

### ネットワーク構成

図1に示すように、デバイスはインターネット上のクラウドサーバーにアクセスできます。ネットワークトラフィックをフィルタリングするように IP レピュテーションを設定します。

図1 ネットワーク構成



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、ルート、セキュリティゾーン、およびセキュリティポリシーを設定します。内部ユーザーが外部ネットワークリソースにアクセスできることを確認します(詳細は省略)。
2. IPレピュテーションを設定します。

#Policies タブをクリックします。

#ナビゲーションペインで、**Threat Intelligence > IP Reputation** を選択します。

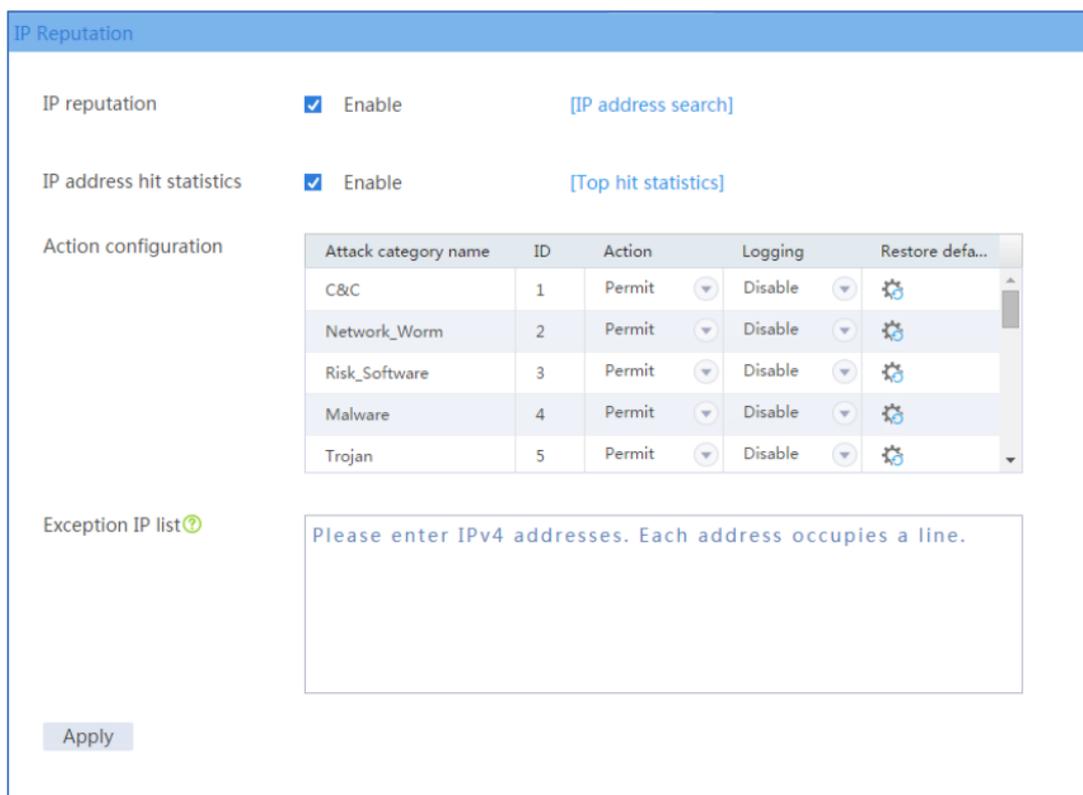
#**IP Reputation** を **Enable** にする、を選択します。

#**IP address hit statistics** を **Enable** にする、を選択します。

#**Top hit statistics** をクリックし、表示されたページで統計収集条件を設定し、**Start** をクリックします。

#**Apply** をクリックします。

図2 IPレピュテーションの設定



## 設定の確認

**Top hit statistics** をクリックして、ヒット数が最も多い IP アドレスを表示し、デバイスがパケット IP アドレスに基づいてネットワークトラフィックをフィルタリングしていることを確認します。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、ブラックリストまたは例外 IP リストから IP アドレスを削除したりできます。

ヒットした IP アドレスに関する詳細情報を表示するには、**IP address search** をクリックし、表示されるページで IP アドレスを入力します。

# NPTv6 の設定例

## はじめに

次に、NPTv6 の設定例を示します。

IPv6-to-IPv6Network Prefix Translation(NPTv6)は、NAT66 と呼ばれ、IPv6 パケットヘッダー内の内部 IPv6 プレフィクスを外部 IPv6 プレフィクスに変換し、その逆も行います。

NPTv6では、次のアドレス変換方式がサポートされています。

- 送信元アドレス変換:内部ユーザーが外部ネットワークにアクセスするときに、パケット内の送信元 IPv6 アドレスを変換します。
- 宛先アドレス変換:外部ホストが内部ネットワーク内のサーバーにアクセスする場合に、パケット内の宛先 IPv6 アドレスを変換します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

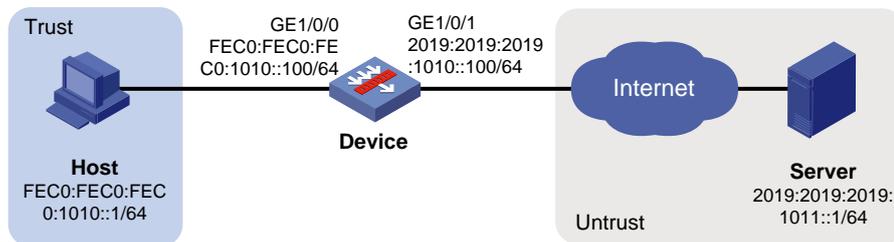
以下の情報は、NPTv6 の機能に関する基本的な知識があることを前提としています。

## 例:送信元アドレス変換の設定

### ネットワーク構成

図1に示すように、内部ユーザーが外部ネットワーク変換を設定して、内部ユーザーが外部ネットワーク内のサーバーにアクセスできるようにします。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、ネットワークをクリックします。  
#ナビゲーションペインで、Interface Configuration>Interfaces を選択します。  
#GE1/0/1 の edit アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。
  - a) Basic Configuration タブで、Untrust セキュリティゾーンを選択します。
  - b) IPv6Address タブで、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およびプレフィックスを入力します。この例では、2019:2019:2019:1010::100/64 と入力します。
  - c) OKをクリックします。#GE1/0/0 を信頼セキュリティゾーンに追加し、その IPv6 グローバルユニキャストアドレスを FEC0:FEC0:FEC0:1010::100/64 に設定します。これは、GE1/0/1 の設定と同じです。
2. セキュリティポリシーを作成します。  
#トップナビゲーションバーで、Policies をクリックします。  
#ナビゲーションペインで、Security Policies>Security Policies を選択します。  
#create をクリックします。  
#表示されるダイアログボックスで、内部ネットワークからのパケットが通過できるようにセキュリティポリシーを設定します。
3. NPTv6を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT66 > NAT66Prefix Translation を選択します。

#create をクリックします。

#プレフィクス変換マッピングを作成します(図2を参照)。

図2NAT66 プレフィクス変換マッピングの作成

Create NAT66 Prefix Translation

Interface: GE1/0/1

Translation method:  Source address translation,  Destination address translation

IPv6 prefix/prefix length before NAT: FEC0:FEC0:FEC0:: / 64 \*(Prefix length: 1-128)

IPv6 prefix/prefix length after NAT: 2019:2019:2019:10 / 64 \*(Prefix length: 1-128)

OK Cancel

#OK をクリックします。

## 設定の確認

1. ホストが外部ネットワーク内のサーバーに正常にpingできることを確認します。

```
C:¥Users¥abc>ping2019:2019:2019:1011::1
```

32バイトのデータを使用した2019:2019:2019:1011::1へのping:

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1のping統計

パケット:送信=4、受信=4、損失=0(損失0%)

おおよそのラウンドトリップ時間(ミリ秒単位):

最小=0ms、最大=0ms、平均=0ms

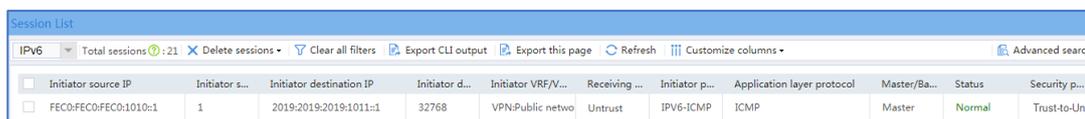
2. ホストがサーバーにアクセスしたときにセッションが生成されることを確認しま

す。

#トップナビゲーションバーでモニターをクリックします。

#ナビゲーションペインで、Sessions を選択します。

図3セッションリスト



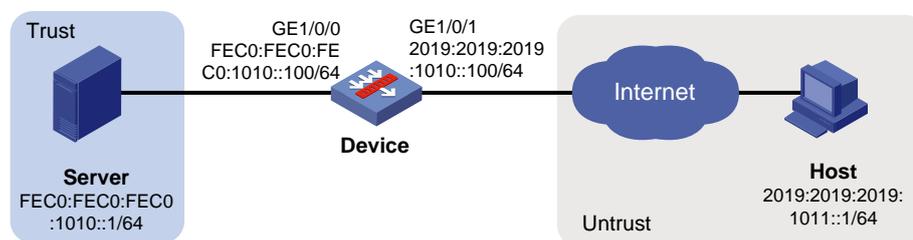
Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/V...	Receiving ...	Initiator p...	Application layer protocol	Master/Ba...	Status	Security p...
FEC0:FEC0:FEC0:1010::1	1	2019:2019:2019:1011::1	32768	VPN:Public netwo	Untrust	IPv6-ICMP	ICMP	Master	Normal	Trust-to-Un

## 例:宛先アドレス変換の設定

### ネットワーク構成

図4に示すように、外部ホストが内部 Web サーバーにアクセスできるように、デバイス上で宛先アドレス変換を設定します。

図4 ネットワーク図



### 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、Network をクリックします。

#ナビゲーションペインで、**Interface Configuration > Interfaces** を選択します。

#GE1/0/1 の edit アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) Basic Configuration タブで、Untrust セキュリティゾーンを選択します。
- b) IPv6Address タブで、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およびプレフィクスを入力します。この例では、2019:2019:2019:1010::100/64 と入力します。
- c) OKをクリックします。

#GE1/0/0 を信頼セキュリティゾーンに追加し、その IPv6 アドレスを FEC0:FEC0:FEC0:1010::100/64 に設定します。これは、GE1/0/1 の設定と同じです。

## 2. セキュリティポリシーを作成します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#表示されるダイアログボックスで、外部ホストからのパケットが通過できるようにセキュリティポリシーを設定します。

## 3. NPTv6を設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT66>NAT66Prefix Translation を選択します。

#create をクリックします。

#プレフィクス変換マッピングを作成します(図5を参照)。

図5 NAT66 プレフィクス変換マッピングの作成

The screenshot shows a dialog box titled "Create NAT66 Prefix Translation". It contains the following fields and options:

- Interface:** GE1/0/1
- Translation method:**  Source address translation,  Destination address translation
- IPv6 prefix/prefix length before NAT:** 2019:2019:2019:10 / 64
- IPv6 prefix/prefix length after NAT:** fec0:fec0:fec0:1010 / 64

Buttons: OK, Cancel

#OK をクリックします。

# 設定の確認

1. ホストが内部Webサーバーに正常にpingできることを確認します。

C:¥Users¥abc>ping2019:2019:2019:1011::1

32バイトのデータを使用した2019:2019:2019:1011::1へのping:

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1:バイト=32時間<1ms TTL=253からの応答

2019:2019:2019:1011::1のping統計

パケット:送信=4、受信=4、損失=0(損失0%)

おおよそのラウンドトリップ時間(ミリ秒単位):

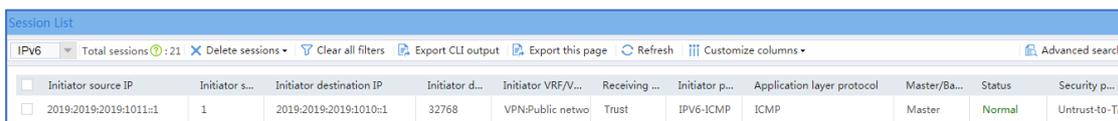
最小=0ms、最大=0ms、平均=0ms

2. ホストが内部Webサーバーにアクセスしたときにセッションが生成されることを確認します。

#トップナビゲーションバーでモニターをクリックします。

#ナビゲーションペインで、Sessions を選択します。

図6セッションリスト



Initiator source IP	Initiator s...	Initiator destination IP	Initiator d...	Initiator VRF/V...	Receiving ...	Initiator p...	Application layer protocol	Master/Ba...	Status	Security p...
2019:2019:2019:1011::1	1	2019:2019:2019:1010::1	32768	VPN:Public netwo	Trust	IPv6-ICMP	ICMP	Master	Normal	Untrust-to-Tr

# レイヤー3 デバイスによる MAC アドレス学習の設定例

## はじめに

次に、レイヤー3 デバイスを介した MAC アドレス学習の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

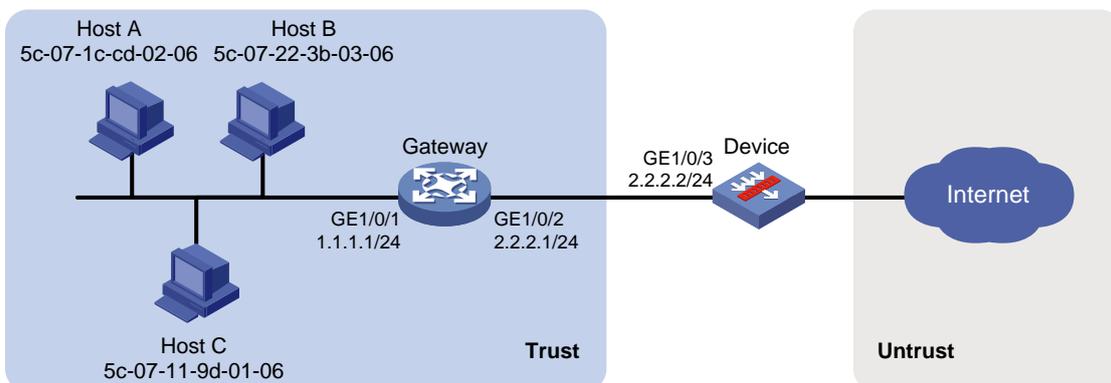
次の情報は、レイヤー3 デバイスを介した MAC アドレス学習機能の基本的な知識があることを前提としています。

## 例:レイヤー3デバイスを介したMACアドレス学習の設定

### ネットワーク構成

図1に示すように、内部ネットワーク内のホストはレイヤー3 ゲートウェイを介してデバイスに接続され、デバイスはインターネットに接続されます。デバイスがホストの MAC アドレスを学習できるように、レイヤー3 デバイスを介して MAC アドレス学習を設定します。内部ネットワーク内のホスト A とホスト B だけがネットワークにアクセスできるようにセキュリティポリシーを設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

### 手順

#### ゲートウェイの設定

1. インターフェイスにIPアドレスを割り当て、ネットワーク到達可能性を保证するようにルーティング機能を設定します(詳細は省略)。
2. SNMPv2 を指定し、プレーンテキスト形式の name public で読み取り専用コミュニティを作成します。

#### デバイスの設定

1. レイヤー3デバイスを作成します。

#トップナビゲーションバーで、system をクリックします。

#ナビゲーションペインで、Maintenance>MAC Learning Through L3Device>L3Device Access Setting を選択します。

#L3 デバイスを介した MAC 学習をイネーブルにし、SNMP 要求のポーリング間隔とアイドルタイムアウトを設定します。

#L3Devices 領域で、Add をクリックします。

#開いたダイアログで、レイヤー3 デバイスの IP アドレス 2.2.2.1 とコミュニティ名 public を入力します。

#OK をクリックします。

図2レイヤー3 デバイスの作成

The screenshot shows a dialog box titled "Add L3 Device". It has a blue header bar with a question mark icon and a close button. The main area contains three fields: "SNMP version" with radio buttons for "v2c" (selected) and "v3"; "IP address" with a text box containing "2.2.2.1" and a red asterisk; and "Community name" with a text box containing "public" and a red asterisk followed by "(1-32 chars)". At the bottom are "OK" and "Cancel" buttons.

2. IP アドレスオブジェクトグループ groupip を作成します。デバイスをゲートウェイに接続するネットワークセグメントをオブジェクトグループに追加します。  
#トップナビゲーションバーで、**Objects** をクリックします。  
#ナビゲーションペインで、**Object Groups > IPv4Address Object Groups** を選択します。  
#**create** をクリックします。  
#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。
  - a) グループ名groupipを入力します。
  - b) **add**をクリックします。
  - c) 表示されるダイアログボックスで、ネットワークセグメントオブジェクトを選択し、IPv4アドレスとマスク2.2.2.0/24を入力します。
3. MAC アドレスオブジェクトグループ groupmac を作成し、ホスト A とホスト B の MAC アドレスをオブジェクトグループに追加します。  
#トップナビゲーションバーで、**Objects** をクリックします。  
#ナビゲーションペインで、**Object Groups>MAC Address Object Groups** を選択します。  
#**create** をクリックします。  
#開いたダイアログボックスで、MAC アドレスオブジェクトグループを設定します。
  2. グループ名groupmacを入力します。
  3. **add**をクリックします。
  4. 表示されるダイアログボックスで**MAC**アドレスタイプを選択し、ホストAのMACアドレス5c-07-1c-cd-02-06を入力します。
  5. **OK**をクリックします。
  6. 手順b～dを繰り返して、ホストBのMACアドレス5c-07-22-3b-03-06をオブジェクトグ

ループに追加します。

4. ゾーンローカルからゾーン信頼にセキュリティポリシーを作成して、デバイスがゲートウェイにアクセスできるようにします。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- policy name policy1 と入力します。
- ソースゾーン Local を選択します。
- ターゲットゾーンの信頼を選択します。
- アクション許可を選択します。
- 送信元 IP/MAC アドレス groupip を選択します。
- 宛先 IP アドレス groupip を選択します。

#OK をクリックします。

5. ゾーン Trust からゾーン Untrust へのセキュリティポリシーを作成して、ホスト A とホスト B がインターネットにアクセスできるようにします。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- policy name policy2 と入力します。
- ソースゾーンの信頼を選択します。
- 宛先ゾーンを選択信頼解除。
- アクション許可を選択します。
- Source IP/MAC address groupmac を選択します。

#OK をクリックします。

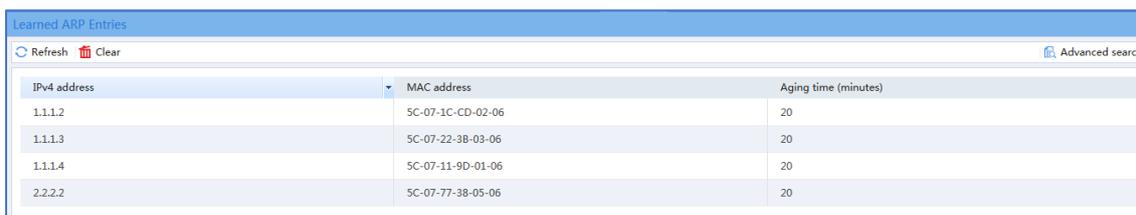
# 設定の確認

1. デバイスによって学習されたAPRエントリを表示します。

#トップナビゲーションバーで、システムをクリックします。

#ナビゲーションペインで、Maintenance>MAC Learning Through L3Device>Learned ARP entries を選択します。

図3学習された ARP エントリ



IPv4 address	MAC address	Aging time (minutes)
1.1.1.2	5C-07-1C-CD-02-06	20
1.1.1.3	5C-07-22-38-03-06	20
1.1.1.4	5C-07-11-9D-01-06	20
2.2.2.2	5C-07-77-38-05-06	20

2. ホストAとホストBはインターネットにアクセスできますが、ホストCはアクセスできないことを確認します。

# WAF の構成例

## はじめに

WAF の構成例を以下に示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

以下の情報は、WAF の機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

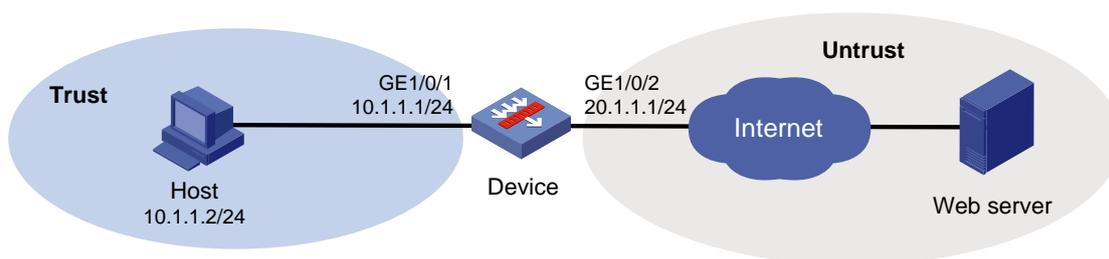
WAF の機能を利用するには、デバイス上で動作するライセンスが必要です。ライセンスの期限が切れると、WAF はデバイス上の既存の WAF シグネチャライブラリを利用できますが、そのライブラリを更新することはできません。

## 例:WAFの設定

### ネットワーク構成

図1に示すように、デバイスは内部ネットワークのセキュリティゲートウェイとして動作します。内部ネットワークをインターネットからの Web アプリケーション攻撃から保護するために、デバイスに WAF 機能を設定します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。

#トップナビゲーションバーで、Network をクリックします。

#ナビゲーションペインで、Interface Configuration>Interfaces を選択します。

#GE1/0/1 の edit アイコンをクリックします。

#開いたダイアログボックスで、インターフェイスを設定します。

- a) 基本basic configurationタブで、Trustセキュリティゾーンを選択します。
- b) IPv4Addressタブで、インターフェイスのIPアドレスとマスクを入力します。  
この例では、10.1.1.1/24と入力します。
- c) OKをクリックします。

#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。

2. 内部IPアドレスオブジェクトグループを作成します。

#トップナビゲーションバーで、Objects をクリックします。

#ナビゲーションペインで、Object Groups>IPv4Address Object Groups を選択します。

#create をクリックします。

#開いたダイアログボックスで、IPv4 アドレスオブジェクトグループを設定します。

グループ名を入力します。この例では、private と入力します。

- a) addをクリックします。

b) 表示されるダイアログボックスで、ネットワークセグメントオブジェクトを選択し、IPv4アドレスとマスク10.1.1.0/24を入力します。

c) Closeをクリックします。

#OKをクリックします。

3. WAFシグネチャライブラリを最新バージョンに更新します(詳細は省略)。

4. WAFプロファイルの設定

#トップナビゲーションバーで、Objects をクリックします。

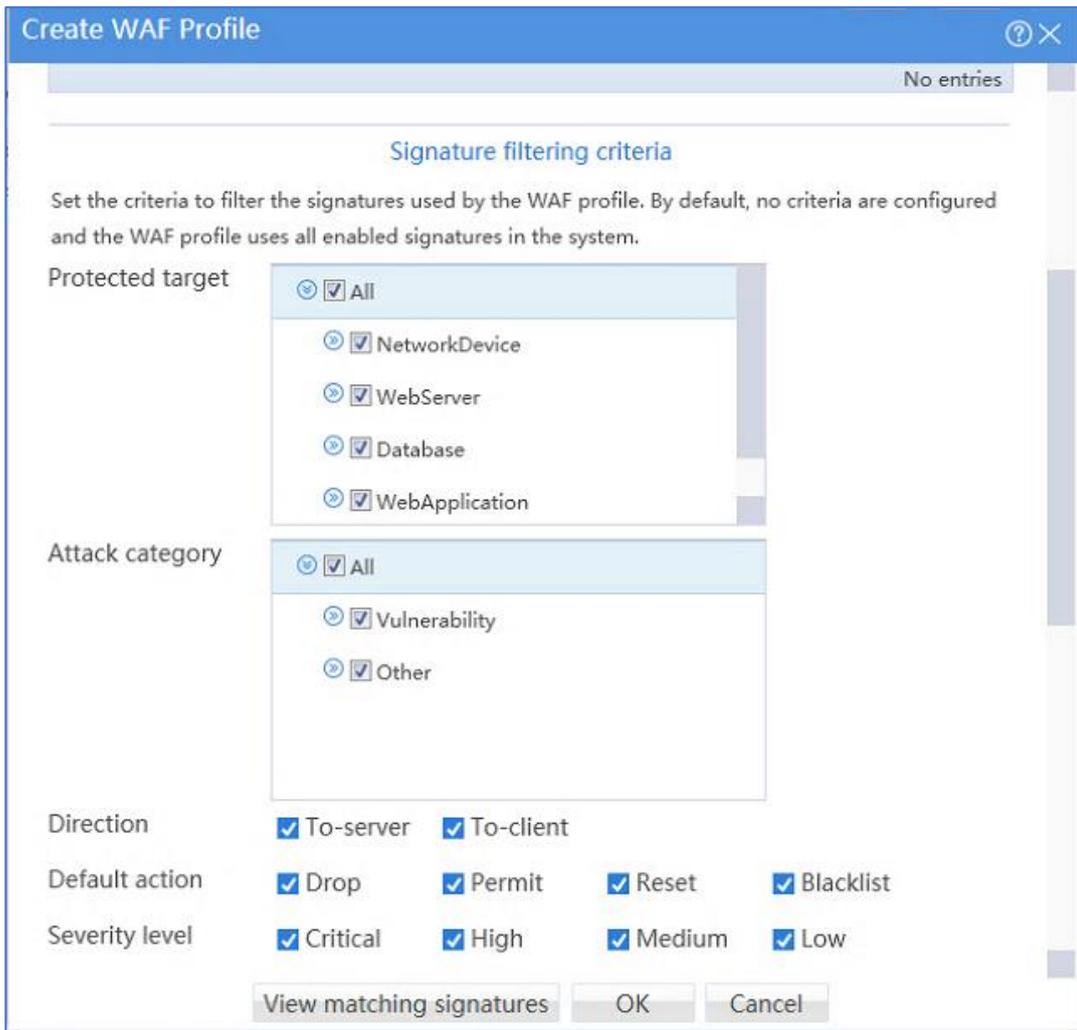
#ナビゲーションペインで、APPSecurity>WAF>プロファイルを選択します。

#create をクリックします。

#表示されるダイアログボックスで、WAF プロファイルを設定します。

- waf と入力します。
- Signature filtering criteria 領域で、次の設定を実行します。
  - 保護ターゲットに対して All を選択します。
  - 攻撃カテゴリに All を選択します。
  - 方向に To-server と To-client を設定します。
  - ドロップ、許可、リセット、およびブラックリストのデフォルトアクションを設定します。
  - 重大度レベルを critical、high、medium、low に設定します。

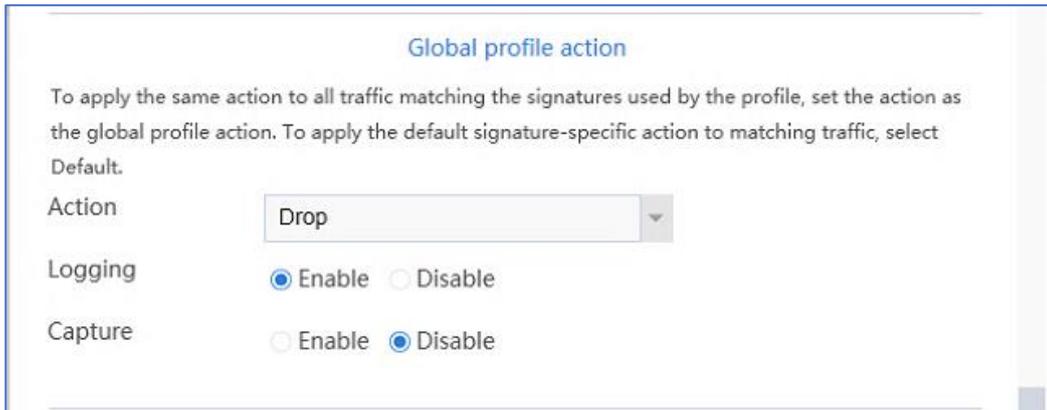
図2 シグニチャフィルタリング基準の設定



#グローバルプロファイルアクション領域で、次の設定を実行します。

- 。 アクションとして drop を設定します。
- 。 ロギングを有効にします。

図3グローバルプロファイルアクションコンフィギュレーション



Global profile action

To apply the same action to all traffic matching the signatures used by the profile, set the action as the global profile action. To apply the default signature-specific action to matching traffic, select Default.

Action

Logging  Enable  Disable

Capture  Enable  Disable

#OK をクリックします。

5. ゾーン Untrust からゾーン Trust へのセキュリティポリシーを作成し、そのポリシーに WAF ファイルを使用します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、Security Policies>Security Policies を選択します。

#create をクリックします。

#開いたダイアログボックスで、セキュリティポリシーを設定します。

- ポリシー名 Waf を入力します。
- ソースゾーン **Untrust** を選択します。
- ターゲットゾーンの **trust** を選択します。
- アクション許可を選択します。
- 宛先 IP アドレスプライベートを選択します。
- WAF プロファイル waf を選択します。

#OK をクリックします。

#Submit をクリックすると、WAF プロファイルの設定が有効になります。

## 設定の確認

WAFが既知のWebアプリケーション層攻撃から内部ネットワークを保護できることを確認します。

これらのイベントに対して生成されたログを表示するには、上部ナビゲーションバーの Monitor をクリックし、ナビゲーションペインで Security Logs>Threat Logs を選択します。

# NetShare コントロールの設定例

## はじめに

次に、NetShare コントロールの設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、NetShare の制御機能に関する基本的な知識があることを前提としています。

## 制限事項とガイドライン

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。

## 例:NetShareコントロールの設定

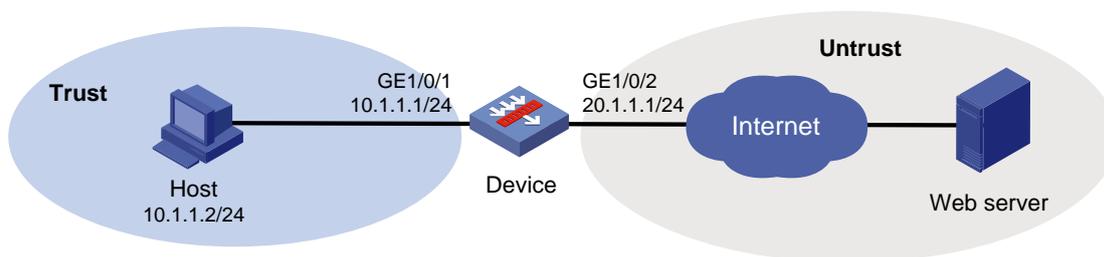
### ネットワーク構成

図 1 に示すように、デバイスは、信頼および信頼解除のセキュリティゾーンを介して、それぞれ LAN およびインターネットに接続します。

次の要件を満たすように、デバイス上で NetShare コントロールを設定します。

- APR ベースのパケット分析に基づいて、LAN 上のホストからインターネットに送信されるパケットを監視し、ネットワーク共有動作検査を行います。
- インターネットアクセス用に複数のホストで共有されている IP アドレスが検出された場合、NetShare コントロールは IP アドレスを 1 時間固定し、イベントをログに記録します。

図1 ネットワーク図



## 使用するソフトウェアバージョン

この設定例は、F1060 デバイスの E9345 で作成および確認されています。

## 手順

1. インターフェイスにIPアドレスを割り当て、インターフェイスをセキュリティゾーンに追加します。  
#トップナビゲーションバーで、Network をクリックします。  
#ナビゲーションペインで、Interface Configuration>Interfaces を選択します。  
#GE1/0/1 の edit アイコンをクリックします。  
#開いたダイアログボックスで、インターフェイスを設定します。
  - a) 基本basic configurationタブで、Trustセキュリティゾーンを選択します。
  - b) IPv4Addressタブで、インターフェイスのIPアドレスとマスクを入力します。この例では、10.1.1.1/24と入力します。
  - c) OKをクリックします。  
#Untrust セキュリティゾーンに GE1/0/2 を追加し、GE1/0/1 と同じ方法で IP アドレスを 20.1.1.1/24 に設定します。
2. APR署名ライブラリを最新バージョンに更新します(詳細は省略)。
3. NetShare制御ポリシーを設定します。  
#トップナビゲーションバーで、Policies 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。  
#create をクリックします。  
#表示されるダイアログボックスで、NetShare ポリシーを設定します。
  - ポリシー名netsharepolicyを入力します。
  - ソースセキュリティゾーンtrustを選択します。
  - 宛先のセキュリティゾーンを選択信頼解除。

- IPID追跡を無効にします。
- IPごとに最大1つの端末を許可します。
- フリーズアクションを選択します。
- フリーズ時間を60に設定します。
- ロギングを有効にします。

OKをクリックします。

図2 NetShareポリシーの作成

**Create Netshare Policy** [?] X

Name: netsharepolicy \* (1-63 chars)

Description: (1-127 chars)

Src security zones: Trust [Edit]

Dst security zones: Untrust [Edit]

Src IP addresses: Select or enter address object groups [Edit]

Dst IP addresses: Select or enter address object groups [Edit]

User: Select or enter users [Edit]

IPID trail tracking [?]  Enable  Disable

Max terminals per IP [?] 1 (1-15)

Action  Permit  Freeze

Freezing times: 60 \*minutes (5-720)

Logging  Enable  Disable

Status  Enable  Disable

OK Cancel

#Submit をクリックして、NetShare ポリシー設定を有効にします。

## 設定の確認

LAN 上のホストがプロキシ経由で共有 IP アドレスを使用してインターネットにアクセスする場合、デバイスはネットワーク共有動作を検出でき、共有 IP アドレスを 1 時間固定してイベントを記録します。

ネットワーク共有動作の IP アドレスを表示するには、トップナビゲーションバーの Policies をクリックし、ナビゲーションペインで Netshare Control>Netshare List を選択します。

# 4G 構成例

## はじめに

次に、4G の設定例を示します。

## 前提条件

このドキュメントは、特定のソフトウェアまたはハードウェアのバージョンに限定されるものではありません。この例の手順と情報は、デバイスのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解しておく必要があります。

次の情報は、4G 機能の基本的な知識があることを前提としています。

## 制限事項とガイドライン

4G 設定を構成する前に、デバイスが USB4G モデムをサポートしていることを確認し、USB4G モデムをデバイスに接続してください。

USB4G モデムは、モデムが接続されている USB インターフェイスがシャットダウンされている場合に使用できます。

データの送信中に USB4G モデムを取り外さないでください。USB4G モデムを取り外す前に、セルラーインターフェイスをシャットダウンすることをお勧めします。

USB4G モデムはホットスワップをサポートしています。

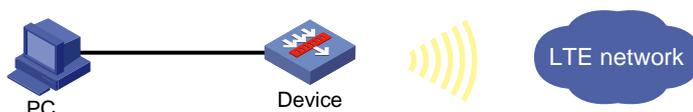
Eth チャネルインターフェイスが DHCP 経由で不正な IP アドレスを取得するのを防ぐには、4G 機能をアクティブにした直後に Eth チャネルインターフェイスを信頼解除セキュリティゾーンに追加します。これに失敗した場合は、信頼解除セキュリティゾーンにインターフェイスを追加してから、インターフェイスをリブートするか、インターフェイス上で DHCP を再度有効にする必要があります。

## 例:4Gの設定

### ネットワーク構成

図1に示すように、デバイスは USB4G モデムを提供し、PC はデバイスを介して LTE ネットワークにアクセスします。内部ユーザーがデバイスを介してインターネットにアクセスできるように、4G 設定を構成します。0

図1 ネットワーク図



### 使用するソフトウェアバージョン

この設定例は、F100-C-A6-WL デバイスの E9602 で作成および検証されました。

### 手順

1. LTEネットワークのリソースにアクセスするために、PCのインターフェイスIP、ルーティング、セキュリティゾーン、およびセキュリティポリシーを設定します (詳細は省略)。

2. 4Gを設定します。

#トップナビゲーションバーで、Network をクリックします。

#ナビゲーションペインで、Interface Configuration>4G を選択します。

#開いたページで、次のパラメータを設定します。

- サポートされているセルラーインターフェイスを選択します。
- デバイスは、セルラーインターフェイス用のEthチャンネルインターフェイス0を自動的に作成し、Ethチャンネルインターフェイスをダイヤラグループ1に追加し、インターフェイス上のすべてのIPv4パケットを許可します。デフォルトでは、EthチャンネルインターフェイスはDHCPを使用してIPアドレスを取得し、従来のDDRでイネーブルになっています。
- コールを発信するためのダイヤル番号を設定します。デバイスは自動ダイヤルアップを自動的に有効にします。
- ダイヤラオートダイヤルの間隔を設定します。DDRは、接続が確立されるま

で、その間隔でコールを試行します。

#適用をクリックします。

3. Eth-channel インターフェイスを Untrust セキュリティゾーンに追加します。

#トップナビゲーションバーで、ネットワークをクリックします。

#ナビゲーションペインで、Security Zones を選択します。

#Eth-channel インターフェイス 0 を Untrust セキュリティゾーンに追加します。

4. Eth チャンネル インターフェイスで NAT アウトバウンドを設定します。

#トップナビゲーションバーで、Policies をクリックします。

#ナビゲーションペインで、NAT>Dynamic NAT を選択します。

#create をクリックします。

#表示されるダイアログボックスで、アウトバウンドダイナミック NAT を設定します。

- Eth チャンネル インターフェイスを選択します。
- NAT 後の送信元アドレスとしてインターフェイスの IP アドレスを選択します。
- 他のフィールドのデフォルト設定を保持します。

#OK をクリックします。

## 設定の確認

PC がデバイスを介して LTE ネットワークにアクセスできること、および Web インターフェイスからデバイスの動作ステータスを表示できることを確認します。

デバイスの動作ステータスを表示するには、トップナビゲーションバーの Network をクリックし、ナビゲーションペインで Interface Configuration>4G を選択します。

図2 デバイス動作ステータスの表示

Interface

▼Dialer configuration

Dialer number  \* (1-30 chars)

Dialer autodial  seconds (1-604800. Default: 300.)

▼Running status

Link Status	Up
IP Address	10.98.228.229
Mask	255.255.255.252