H3C MSRルーター
610[810][830][1000S][2600][3600]
ACLコンフィギュレーションガイド(Comware 7)

New H3C Technologies
http://www.h3c.com

ソフトウェアバージョン:MSR-CMW710-R6728P21以降
ドキュメントバージョン:6W101-20220924

はじめに

このコンフィギュレーションガイドでは、ACLを使用してトラフィックを分類し、QoSテクノロジーを使用してネットワークリソースを割り当て、輻輳を管理して、ネットワークパフォーマンスとネットワーク使用効率を向上させる方法について説明します。ACLを使用すると、他の機能モジュール(QoSやIPルーティングなど)がトラフィックを分類またはフィルタリングするのに役立ちます。

ここでは、マニュアルに関する次の内容について説明します。

- 対象読者
- 表記規則
- ドキュメントに関するフィードバック

対象読者

このマニュアルは、次の読者を対象としています。

- 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およびサービスエンジニア。
- ネットワーク管理者。

表記規則

次の情報では、マニュアルで使用されている表記規則について説明します。

コマンドの表記規則

表記規則	説明
太字	太字のテキストは、文字どおりに入力するコマンドとキーワードを表します。
イタリック	イタリック体は、実際の値に置き換える引数を表します。
[ ]	角カッコは、省略可能な構文の選択肢(キーワードまたは引数)を囲みます。
{x | y | ... }	中かっこは、必要な構文の選択肢を縦棒で区切って囲み、その中から1つを選択します。
[x | y | ...]	角カッコは、垂直バーで区切られたオプションの構文選択肢のセットを囲み、そこから1つを選択するか、何も選択しません。
{ x | y | ....}*	アスタリスクの付いた中かっこは、必要な構文の選択肢を縦棒で区切って囲み、その中から少なくとも1つを選択します。
[x | y | ....]*	角カッコで囲まれたアスタリスクは、縦棒で区切られたオプションの構文の選択肢を囲みます。選択肢の中から、1つを選択するか、複数を選択するか、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の表記規則

表記規則	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示しています。たとえば、New Userウィンドウが開いたら、OKをクリックします。

表記規則	説明
>	マルチレベルメニューは山カッコで区切られています。たとえば、File>Create 。

記号

表記規則	説明
⚠警告!	理解または従わないと人身事故につながる可能性のある重要な情報に注意を喚起する警告。
△注意:	重要な情報に注意を喚起するアラート。この情報を理解または遵守しないと、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ります。
ⓘ重要:	重要な情報に注意を喚起する警告。
注:	追加情報または補足情報を含むアラート。
ヒント:	有用な情報を提供する警告。

ネットワークトポロジアイコン

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装置を表します。
	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装置を表します。
	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装置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する場合があります。例に記載されているポート番号、サンプル出力、スクリーンショット、およびその他の情報が、デバイス上にあるものと異なるのは正常です。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお寄せください。ご意見をお寄せいただければ幸いです。

内容

ACLの設定 1
ACLについて 1
ACLの番号付けと命名 1
ACLタイプ 1
一致の順番 1
規則の番号付け 2
ACLによるフラグメントフィルタリング 3
制約事項:ACLとのハードウェア互換性 4
制約事項および注意事項:ACLの設定 6
ACLタスクの概要 6
基本ACLの設定 7
基本的なACLについて 7
基本的なACL設定の制約事項およびガイドライン 7
IPv4基本ACLの設定 7
IPv6基本ACLの設定 8
拡張ACLの設定 9
拡張ACLについて 9
高度なACL設定の制約事項およびガイドライン 9
IPv4拡張ACLの設定 9
IPv6拡張ACLの設定 10
レイヤー2 ACLの設定 11
ACLのコピー 12
ACLアクセラレーションのイネーブル化 12
ACLを使用したパケットフィルタリングの設定 13
ACLを使用したパケットフィルタリングについて 13
パケットフィルタリングのためのインターフェイスへのACLの適用 13
パケットフィルタリングのためのゾーンペアへのACLの適用 13
パケットフィルタリング用のロギングおよびSNMP通知の設定 14
パケットフィルタリングのデフォルトアクションの設定 14
ACLの表示およびメンテナンスコマンド 14
ACLの設定例 17
例:インターフェイスベースのパケットフィルタの設定 17
例:ゾーンペアベースのパケットフィルタの設定 19

ACLの設定

ACLについて

Access Control List(ACL)は、送信元IPアドレス、宛先IPアドレス、ポート番号などの基準に基づいてトラフィックを識別するための一連の規則です。この規則は、permitステートメントまたはdenyステートメントとも呼ばれます。

ACLは、主にパケットフィルタリングに使用されます。また、QoS、セキュリティ、ルーティング、およびその他のモジュールでACLを使用して、トラフィックを識別することもできます。パケットのドロップまたは転送の決定は、ACLを使用するモジュールによって異なります。

ACLの番号付けと命名

ACLを作成するときは、識別のための番号または名前を割り当てる必要があります。既存のACLは、その番号または名前で指定できます。各ACLタイプには、一意の範囲のACL番号があります。

同じ番号の基本ACLまたは拡張ACLの場合は、ipv6キーワードを使用して区別する必要があります。同じ名前のACLの場合は、ipv6キーワードおよびmacキーワードを使用して区別する必要があります。

ACLタイプ

タイプ	ACL番号	IPバージョン	一致条件
基本ACL	2000から2999	IPv4	送信元IPv4アドレス。
		IPv6	送信元IPv6アドレス。
拡張ACL	3000から3999	IPv4	送信元IPv4アドレス、宛先IPv4アドレス、パケットプライオリティ、プロトコル番号、およびその他のレイヤー3およびレイヤー4ヘッダーフィールド。
		IPv6	送信元IPv6アドレス、宛先IPv6アドレス、パケットプライオリティ、プロトコル番号、およびその他のレイヤー3およびレイヤー4ヘッダーフィールド。
レイヤー2 ACL	4000から4999	IPv4およびIPv6	送信元および宛先MACアドレス、802.1pプライオリティ、リンクレイヤープロトコルタイプなどのレイヤー2ヘッダーフィールド。

一致の順番

ACL内のルールは、特定の順序でソートされます。パケットがルールに一致すると、デバイスは一致プロセスを停止し、ルールで定義されたアクションを実行します。ACLに重複または競合するルールが含まれている場合、一致結果と実行するアクションは、ルールの順序によって異なります。

次のACL一致順序を使用できます。

- **config**: ACLルールをルールIDの昇順にソートします。IDが小さいルールは、IDが大きいルールよりも先に一致します。この方法を使用する場合は、ルールとその順序を注意深く確認してください。
- **auto**: 深さ優先順序でACLルールをソートします。深さ優先順序では、ルールのすべてのサブセットが常にルールの前に一致します。表1は、深さ優先順序で各タイプのACLのルールをソートするために使用されるタイブレーカーのシーケンスを示しています。

表1 深さ優先順序でのACLルールのソート

ACLタイプ	タイブレーカーのシーケンス
IPv4基本ACL	1. VPNインスタンス。 2. 送信元IPv4アドレスワイルドカードの0が多い(0が多いほど、IPv4アドレス範囲が狭くなります)。 3. 以前に設定されたルール。
IPv4拡張ACL	1. VPNインスタンス。 2. 特定のプロトコル番号。 3. 送信元IPv4アドレスワイルドカードマスクに0が追加されました。 4. 宛先IPv4アドレスワイルドカードに0が追加されました。 5. より狭いTCP/UDPサービスポート番号の範囲。 6. 以前に設定されたルール。
IPv6基本ACL	1. VPNインスタンス。 2. 送信元IPv6アドレスの長いプレフィクス(長いプレフィクスは、IPv6アドレス範囲が狭いことを意味します)。 3. 以前に設定されたルール。
IPv6拡張ACL	1. VPNインスタンス。 2. 特定のプロトコル番号。 3. 送信元IPv6アドレスの長いプレフィクス。 4. 宛先IPv6アドレスの長いプレフィクス。 5. より狭いTCP/UDPサービスポート番号の範囲。 6. 以前に設定されたルール。
レイヤー2 ACL	1. 送信元MACアドレスマスクの1が多い(1が多いほど、MACアドレスが小さくなります)。 2. 宛先MACアドレスマスクに1を追加します。 3. 以前に設定されたルール。

ワイルドカードマスクは、逆マスクとも呼ばれ、ドット付き10進表記で表される32ビットの2進数です。ネットワークマスクとは対照的に、ワイルドカードマスクの0ビットは「do care」ビットを表し、1ビットは「don't care」ビットを表します。IPアドレスの「do care」ビットがIPアドレス基準の「do care」ビットと同一である場合、IPアドレスは基準と一致します。すべての「don't care」ビットは無視されます。ワイルドカードマスクの0と1は連続していなくてもかまいません。たとえば、0.255.0.255は有効なワイルドカードマスクです。

規則の番号付け

ACLルールには、手動または自動で番号を付けることができます。この項では、ACLルールの自

動番号付けの仕組みについて説明します。

ルールの番号付け手順

作成するルールにIDを割り当てない場合、ルールIDが自動的に割り当てられます。ルール採番手順では、ルールに自動的に番号を付ける増分を設定します。たとえば、デフォルトのACLルール採番手順は5です。作成するルールにIDを割り当てない場合、ルールには自動的に0、5、10、15のように番号が付けられます。採番手順の幅が広いほど、2つのルールの間に挿入できるルールの数が多くなります。

規則を連続して番号付けするのではなく、規則間にギャップを導入することで、ACLに規則を柔軟に挿入できます。この機能は、ACL規則が規則IDの昇順で照合されるconfig-order ACLで重要です。

ルール採番手順では、システムが自動的にルールに番号を付ける増分を設定します。ACLルールの作成時にルールIDを指定しない場合、システムは自動的にルールIDを割り当てます。このルールIDは、開始ルールIDから始まり、現在の最高のルールIDに最も近い採番手順の倍数です。たとえば、ルール採番手順が5で、現在の最高のルールIDが12の場合、ルールには15の番号が付けられます。

番号付けステップの幅が広いほど、2つのルールの間に挿入できるルールの数が多くなります。ステップまたは開始ルールIDが変更されるたびに、ルールの番号が開始ルールIDから振り直されます。たとえば、0、5、9、10および15の番号が付いた5つのルールがある場合、ステップを5から2に変更すると、ルールは次のようになります。
番号が0、2、4、6、および8に変更されました。

ルールの自動採番と再採番

ACLルールに自動的に割り当てられたIDは、現在の最高のルールIDに最も近い、0から始まる番号付けステップの倍数を取ります。

たとえば、ステップが5で、番号が0、5、9、10、および12の5つのルールがある場合、新しく定義されたルールの番号は15になります。ACLにルールが含まれていない場合、最初のルールの番号は0になります。

ステップが変更されるたびに、ルールの番号が0から振り直されます。たとえば、ステップを5から2に変更すると、ルール5、10、13および15の番号がルール0、2、4および6に振り直されます。

マッチの順番がautoのACLの場合、ルールは深さ順にソートされ、マッチの順番に基づいて再番号付けされます。たとえば、ルールのマッチの順番は0、10、5です。番号付けステップを2に変更すると、ルール0、10、5(0、5、10ではない)がルール0、2、4に再番号付けされます。

ACLによるフラグメントフィルタリング

従来のパケットフィルタリングでは、パケットの最初のフラグメントのみが照合され、それ以降の最初でないフラグメントはすべて通過できます。攻撃者は、最初でないフラグメントを作成してネットワークを攻撃できます。

リスクを回避するために、ACL機能は次のように設計されています。

- 先頭以外のフラグメントも含め、すべてのフラグメントをデフォルトでフィルタリングします。
- 効率的に照合基準を変更できます。たとえば、先頭以外のフラグメントだけをフィルタリングするようにACLを設定できます。

制約事項:ACLとのハードウェア互換性

次の互換性マトリクスは、WLAN関連のコマンドおよびパラメータに対するハードウェアプラットフォームのサポートを示しています。

ハードウェア	コマンドとパラメータの互換性
MSR610	有
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK MSR810-CNDE-SJK、MSR810-EI、MSR810-LM-EA、MSR810-LM-EI	有
MSR810-LMS、MSR810-LUS	無
MSR810-SI、MSR810-LM-SI	有
MSR810-LMS-EA、MSR810-LME	有
MSR1004S-5G	有
MSR2600-6-X1、MSR2600-15-X1、MSR2600-15-X1-T	有
MSR2600-10-X1	有
MSR2630	有
MSR 2630	有
MSR3600-28、MSR3600-51	有
MSR3600-28-SI、MSR3600-51-SI	無
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	有
MSR3600-28-G-DP、MSR3600-51-G-DP	有
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES、MSR3610-IE-EAD、MSR-EAD-AK770、MSR3610-I-IG、MSR3610-IE-IG	有
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC、MSR3620-X1、MSR3640-X1	有
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	有
MSR3610-G、MSR3620-G	無
MSR 3640-X1-HI	有
MSR810-W-WiNet、MSR810-LM-WiNet	有
MSR830-4LM-WiNet	有
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	有
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	有
MSR 2600-6-WiNet	有
MSR2600-10-X1-WiNet	有
MSR2630-WiNet	有
MSR 3600-28-WiNet	有

MSR3610-X1-WiNet	有
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	有
MSR860-6EI-XS	有
MSR860-6HI-XS	有
MSR2630-XS	有
MSR3600-28-XS	有
MSR3610-XS	有
MSR3620-XS	有
MSR3610-I-XS	有
MSR3610-IE-XS	有
MSR3620-X1-XS	有
MSR3640-XS	有
MSR3660-XS	有
MSR810-LM-GL	有
MSR810-W-LM-GL	有
MSR830-6EI-GL	有
MSR830-10EI-GL	有
MSR830-6HI-GL	有
MSR830-10HI-GL	有
MSR1004S-5G-GL	有
MSR2600-6-X1-GL	有
MSR3600-28-SI-GL	無

制約事項および注意事項:ACLの設定

- 番号付きACLを作成する場合は、次のコマンドを使用してACLのビューを開始できます。
  - **acl** [**ipv6**] **number** *acl-number*
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number*
- 番号と名前の両方を指定してACLを作成する場合は、次のコマンドを使用してACLのビューを入力できます。
  - **acl** [**ipv6**] **number** *acl-number* (基本と拡張ACLのみ)
  - **acl** [**ipv6**] **number** *acl-number*[**name** *acl-name*]
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*コマンドを使用して名前付きACLを作成する場合は、次のコマンドを使用してACLのビューを開始できます。
  - **acl** [**ipv6**] **name** *acl-name*
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*
- ACLルールに一致基準が含まれている場合、または次の一致基準と機能に加えて機能がイネーブルになっている場合、一致するパケットは低速転送によって転送されます。
  - 送信元および宛先IPアドレス。
  - 送信元ポートと宛先ポート。
  - トランスポート層プロトコル。
  - ICMPまたはICMPv6メッセージタイプ、メッセージコード、およびメッセージ名。
  - VPNインスタンス。
  - ロギング。
  - 時間範囲。

  低速転送では、転送エントリの計算のためにパケットをコントロールプレーンに送信する必要があります。これは、デバイスの転送パフォーマンスに影響します。

ACLタスクの概要

ACLを設定するには、次の作業を実行します。

- 一致するパケットの特性に従ってACLを設定します。
  - 基本ACLの設定
  - 拡張ACLの設定
  - レイヤー2 ACLの設定
- (任意)ACLのコピー
- (任意)ACLアクセラレーションのイネーブル化
- (任意)ACLを使用したパケットフィルタリングの設定

基本ACLの設定

基本的なACLについて

基本ACLは、送信元IPアドレスだけに基づいてパケットを照合します。

基本的なACL設定の制約事項およびガイドライン

ACLルールで指定されたloggingキーワードを使用すると、ACLモジュールはログメッセージをインフォメーションセンターに送信できます。

インフォメーションセンターでは、ログメッセージのフィルタリングと出力先を含む出力ルールを設定できます。

インフォメーションセンターでは、コンソールとモニタ端末以外の出力先にACLログを出力できますが、コンソールやモニタ端末を出力先として設定した場合、出力先の設定は有効になりません。

デバイスに保存されているACLログを表示するには、display logbufferコマンドを使用します。デフォルトでイネーブルになっているログバッファへのログ出力をディセーブルにしないようにしてください。

Information Centerの設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

IPv4基本ACLの設定

1. システムビューに入ります。

   system-view
2. IPv4基本ACLを作成し、そのビューを入力します。必要に応じて、次のいずれかのオプションを選択します。
   - ACL番号を指定して、IPv4基本ACLを作成します。

     acl number *acl-number*[**name** *acl-name*] [**match-order** { **auto** | **config** }]
   - basicキーワードを指定して、IPv4基本ACLを作成します。

     acl basic { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]
3. (任意)IPv4基本ACLの説明を設定します。

   description *text*

   デフォルトでは、IPv4基本ACLには説明がありません。
4. (任意)ルールの番号付けステップを設定します。

   step *step-value*

   デフォルトでは、ルールの番号付けステップは5で、開始ルールIDは0です。
5. 規則を作成または編集します。

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

loggingキーワードが有効になるのは、ACLを使用するモジュール(パケットフィルタリングなど)がロギングをサポートしている場合だけです。

6. (任意)ルールコメントを追加または編集します。

   rule *rule-id* **comment** *text*

   デフォルトでは、ルールコメントは設定されていません。

IPv6基本ACLの設定

1. システムビューに入ります。

   system-view

2. IPv6基本ACLビューを作成し、そのビューを入力します。必要に応じて、次のいずれかのオプションを選択します。

   - ACL番号を指定して、IPv6基本ACLを作成します。

     acl ipv6 number *acl-number*[**name** *acl-name*] [**match-order** { **auto** | **config** }]

   - basicキーワードを指定して、IPv6基本ACLを作成します。

     acl ipv6 basic { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

3. (任意)IPv6基本ACLの説明を設定します。

   description *text*

   デフォルトでは、IPv6基本ACLには説明がありません。

4. (任意)ルールの番号付けステップを設定します。

   step *step-value*

   デフォルトでは、ルールの番号付けステップは5で、開始ルールIDは0です。

5. 規則を作成または編集します。

   rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

   loggingキーワードが有効になるのは、ACLを使用するモジュール(パケットフィルタリングなど)がロギングをサポートしている場合だけです。

6. (任意)ルールコメントを追加または編集します。

   rule *rule-id* **comment** *text*

   デフォルトでは、ルールコメントは設定されていません。

拡張ACLの設定

拡張ACLについて

拡張ACLは、次の基準に基づいてパケットを照合します。

- 送信元IPアドレス。
- 宛先IPアドレス。
- パケットプライオリティ。
- ローカルQoS ID。
- プロトコルの種類。
- TCP/UDP送信元および宛先ポート番号、TCPフラグ、ICMPメッセージタイプ、およびICMPメッセージコードなど、その他のプロトコルヘッダー情報。

基本ACLと比較して、拡張ACLでは、より柔軟で正確なフィルタリングが可能です。

高度なACL設定の制約事項およびガイドライン

ACLルールで指定されたloggingキーワードを使用すると、ACLモジュールはログメッセージをインフォメーションセンターに送信できます。

インフォメーションセンターでは、ログメッセージのフィルタリングと出力先を含む出力ルールを設定できます。

インフォメーションセンターでは、コンソールとモニタ端末以外の出力先にACLログを出力できますが、コンソールやモニタ端末を出力先として設定した場合、出力先の設定は有効になりません。

デバイスに保存されているACLログを表示するには、display logbufferコマンドを使用します。デフォルトでイネーブルになっているログバッファへのログ出力をディセーブルにしないようにしてください。

Information Centerの設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

IPv4拡張ACLの設定

1. システムビューに入ります。

   system-view

2. IPv4拡張ACLを作成し、そのビューを入力します。必要に応じて、次のいずれかのオプションを選択します。

   - ACL番号を指定して、番号付きIPv4拡張ACLを作成します。

     acl number *acl-number*[**name** *acl-name*] [**match-order** { **auto** | **config** }]

   - advancedキーワードを指定して、IPv4拡張ACLを作成します。

     acl advanced { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

3. (任意)IPv4拡張ACLの説明を設定します。

   description *text*

   デフォルトでは、IPv4拡張ACLには説明がありません。

4. (任意)ルールの番号付けステップを設定します。

   step *step-value*

   デフォルトでは、ルールの番号付けステップは5で、開始ルールIDは0です。

5. 規則を作成または編集します。

   rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp1* [**to** *dscp2*] | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **ttl** *operator ttl-value1* [*ttl-value2*] | **vpn-instance** *vpn-instance-name*] *

   loggingキーワードが有効になるのは、ACLを使用するモジュール(パケットフィルタリングなど)がロギングをサポートしている場合だけです。

6. (任意)ルールコメントを追加または編集します。

   rule *rule-id* **comment** *text*

   デフォルトでは、ルールコメントは設定されていません。

IPv6拡張ACLの設定

1. システムビューに入ります。

   system-view

2. IPv6拡張ACLを作成し、そのビューを入力します。必要に応じて、次のいずれかのオプションを選択します。

   - ACL番号を指定して、番号付きIPv6拡張ACLを作成します。

     acl ipv6 number *acl-number*[**name** *acl-name*] [**match-order** { **auto** | **config** }]

   - advancedキーワードを指定して、IPv6拡張ACLを作成します。

     acl ipv6 advanced { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

3. (任意)IPv6拡張ACLの説明を設定します。

   description *text*

   デフォルトでは、IPv6拡張ACLには説明がありません。

4. (任意)ルールの番号付けステップを設定します。

   step *step-value*

   デフォルトでは、ルールの番号付けステップは5で、開始ルールIDは0です。

5. 規則を作成または編集します。

   rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination**

{ **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name*| **ttl** *operator ttl-value1* [*ttl-value2*] | **vpn-instance** *vpn-instance-name*] *

loggingキーワードが有効になるのは、ACLを使用するモジュール(パケットフィルタリングなど)がロギングをサポートしている場合だけです。

6. (任意)ルールコメントを追加または編集します。

   rule *rule-id* **comment** *text*

   デフォルトでは、ルールコメントは設定されていません。

レイヤー2 ACLの設定

このタスクについて

レイヤー2 ACLは、イーサネットフレームヘッダーACLとも呼ばれ、次のようなレイヤー2イーサネットヘッダーフィールドに基づいてパケットを照合します。

- 送信元MACアドレス。
- 宛先MACアドレス。
- 802.1pプライオリティ(VLANプライオリティ)。
- リンク層プロトコルタイプ。
- カプセル化タイプ。

手順

1. システムビューに入ります。

   system-view

2. レイヤー2 ACLを作成し、そのビューを入力します。必要に応じて、次のいずれかのオプションを選択します。

   - ACL番号を指定して、レイヤー2 ACLを作成します。

     acl number *acl-number*[**name** *acl-name*] [**match-order** { **auto** | **config** }]

   - macキーワードを指定して、レイヤー2 ACLを作成します。

     acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

3. (任意)レイヤー2 ACLの説明を設定します。

   description *text*

   デフォルトでは、レイヤー2 ACLには説明がありません。

4. (任意)ルールの番号付けステップを設定します。

   step *step-value*

デフォルトでは、ルールの番号付けステップは5で、開始ルールIDは0です。

5. 規則を作成または編集します。

   rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

6. (任意)ルールコメントを追加または編集します。

   rule *rule-id* **comment** *text*

   デフォルトでは、ルールコメントは設定されていません。

ACLのコピー

このタスクについて

既存のACL(ソースACL)をコピーして、ACLを作成できます。新しいACL(宛先ACL)は、ソースACLと同じプロパティと内容を持ちますが、ソースACLとは異なる番号または名前を使用します。

制限事項およびガイドライン

ACLを正常にコピーするには、次のことを確認します。

- 宛先ACLは、送信元ACLと同じタイプです。
- 送信元ACLはすでに存在しますが、宛先ACLは存在しません。

手順

1. システムビューに入ります。

   system-view

2. 既存のACLをコピーして、新しいACLを作成します。

   acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

ACLアクセラレーションのイネーブル化

このタスクについて

ACLアクセラレーションにより、ACLルール検索が高速化されます。アクセラレーションの効果は、ACLルールの数とともに増加します。たとえば、NATやASPFなどのセッションベースのサービスに大きなACLが使用される場合、ACLアクセラレーションにより、ACL処理の遅延によるセッションのタイムアウトを回避できます。

ACLアクセラレーションは、ACLルールが追加、削除、または変更された後、一定期間遅延されます。遅延期間中に追加のルール変更が発生した場合、遅延期間は再びカウントを開始します。ACLに含まれるルールが100以下の場合、遅延期間は2秒です。ACLに含まれるルールが100を超える場合、遅延期間は20秒です。

手順

1. システムビューに入ります。

   system-view

2. ACLを作成し、ACLビューを開始します。

acl { [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } | **mac** { *acl-number* | **name** *acl-name* } } [**match-order** { **auto** | **config** }]

3. ACLのACLアクセラレーションをイネーブルにします。

   accelerate

   デフォルトでは、ACLアクセラレーションはディセーブルです。

△注意:

多数のACLルールが存在する場合、undo accelerateコマンドを実行すると、デバイスが重大なCPU使用率アラームしきい値に達し、通常のサービス処理に影響を与える可能性があります。

ACLを使用したパケットフィルタリングの設定

ACLを使用したパケットフィルタリングについて

この項では、ACLを使用してパケットをフィルタリングする手順について説明します。たとえば、ACLをインターフェイスに適用して、着信または発信パケットをフィルタリングできます。

パケットフィルタリングのためのインターフェイスへのACLの適用

制限事項およびガイドライン

インターフェイスの同じ方向に最大32個のACLを適用できます。

手順

1. システムビューに入ります。

   system-view

2. インターフェイスビューを入力します。

   interface *interface-type interface-number*

3. ACLをインターフェイスに適用して、パケットをフィルタリングします。

   packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

   デフォルトでは、インターフェイスはパケットをフィルタリングしません。

パケットフィルタリングのためのゾーンペアへのACLの適用

制限事項およびガイドライン

最大32のACLを同じゾーンペアに適用できます。ゾーンペアの詳細については、『Security Configuration Guide』を参照してください。

手順

1. システムビューに入ります。

   system-view

2. ゾーンペアビューを開始します。

   zone-pair security source *source-zone-name* **destination** *destination-zone-name*

3. ゾーンペアにACLを適用して、パケットをフィルタリングします。

   packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

   デフォルトでは、ゾーンペアはパケットをフィルタリングしません。

パケットフィルタリング用のロギングおよびSNMP通知の設定

このタスクについて

パケットフィルタリングのログエントリまたはSNMP通知を生成し、出力間隔で情報センターまたはSNMPモジュールに出力するようにACLモジュールを設定できます。ログエントリまたは通知には、一致したパケットの数と一致したACLルールが記録されます。フローの最初のパケットがACLルールに一致すると、出力間隔が開始され、デバイスはただちにこのパケットのログエントリまたは通知を出力します。出力間隔が終了すると、デバイスはフローの後続の一致パケットのログエントリまたは通知を出力します。

インフォメーションセンターの詳細については、Network Management and Monitoring Configuration Guideを参照してください。

SNMPの詳細については、Network Management and Monitoring Configuration Guideを参照してください。

手順

1. システムビューに入ります。

   system-view

2. パケットフィルタリングのログまたは通知を出力する間隔を設定します。

   acl { **logging** | **trap** } **interval** *interval*

   デフォルト設定は0分です。デフォルトでは、デバイスはパケットフィルタリングのログエントリまたはSNMP通知を生成しません。

パケットフィルタリングのデフォルトアクションの設定

このタスクについて

デフォルトでは、パケットフィルタは、どのACLルールにも一致しないパケットの通過を許可します。どのACLルールにも一致しないパケットを拒否するには、次の作業を実行します。パケットフィルタリングのデフォルトアクションは、ゾーンペアパケットフィルタリングには影響しません。ゾーンペアパケットフィルタリングのデフォルトアクションは、常に拒否です。

手順

1. システムビューに入ります。

   system-view

2. パケットフィルタリングのデフォルトアクションをdenyに設定します。

   packet-filter default deny

   デフォルトでは、パケットフィルタはどのACLルールにも一致しないパケットの通過を許可します。

ACLの表示およびメンテナンスコマンド

任意のビューでdisplayコマンドを実行し、ユーザビューでコマンドをリセットします。

タスク	コマンド
ACLの設定と試合の統計を表示します。	**display acl** [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }
ACLアクセラレーションステータスを表示します。	スタンドアロンモードの場合: **display acl accelerate** { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } } IRFモードの場合: **display acl accelerate** { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **slot** *slot-number* }
パケットフィルタリングのACLアプリケーション情報を表示します。	スタンドアロンモードの場合: **display packet-filter** { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] } IRFモードの場合: **display packet-filter** { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] } [**slot** *slot-number*]
パケットフィルタリングACLの試合の統計を表示します。	**display packet-filter statistics** { **interface** *interface-type interface-number* { **inbound** | **outbound** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**brief**]
パケットフィルタリングACLの累積統計情報を表示します。	**display packet-filter statistics sum** { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]
詳細なACLパケットフィルタリング情報を表示します。	スタンドアロンモードの場合: **display packet-filter verbose** { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } IRFモードの場合: **display packet-filter verbose** { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**slot** *slot-number*]

ACL統計情報をクリアします。	**reset acl** [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }
パケットフィルタリングACLの試合の統計を消去します。	**reset packet-filter statistics** { **interface** [*interface-type interface-number*] { **inbound** | **outbound** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**ipv6**] { *acl-number* | **name** *acl-name* } }

ACLの設定例

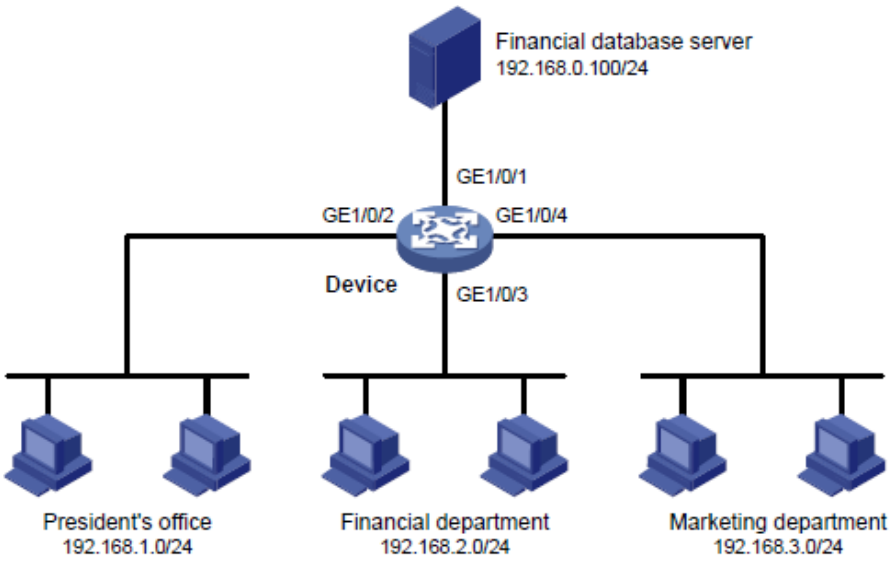
例:インターフェイスベースのパケットフィルタの設定

ネットワーク構成

企業は、デバイスを介して部門を相互接続します。パケットフィルタを次のように設定します。

- 社長室から財務データベースサーバーへのアクセスをいつでも許可します。
- 就業日の就業時間中(8:00～18:00)にのみ、財務部からデータベースサーバーへのアクセスを許可します。
- 他の部門からデータベースサーバーへのアクセスを拒否します。

図1 ネットワークダイアグラム



手順

#就業日の8:00から18:00までの定期的な時間範囲を作成します。

<Device> system-view

[Device] time-range work 08:0 to 18:00 working-day

#3000という番号のIPv4拡張ACLを作成します。

[Device] acl advanced 3000

#社長室から財務データベースサーバーへのアクセスを許可するルールを設定します。

[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0

#勤務時間中に財務部からデータベースサーバーへのアクセスを許可するルールを構成します。

[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work

#財務データベースサーバーへのアクセスを拒否するルールを設定します。

[Device-acl-ipv4-adv-3000] rule deny ip source any destination 192.168.0.100 0

[Device-acl-ipv4-adv-3000] quit

#IPv4拡張ACL 3000を適用して、インターフェイスGigabitEthernet 1/0/1上の発信パケットをフィルタリングします。

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] packet-filter 3000 outbound

[Device-GigabitEthernet1/0/1] quit

設定の確認

#財務部のPCが、勤務時間中にデータベースサーバー対してpingを実行できることを確認します(この例では、すべてのPCがWindows 10を使用しています)。

C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255

Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.100:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

#マーケティング部門のPCが、勤務時間中にデータベースサーバーに対してpingを実行できないことを確認します。

C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.0.100:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

#デバイス上のIPv4拡張ACL 3000の設定と試合の統計を表示します。

[Device] display acl 3000

Advanced IPv4 ACL 3000, 3 rules,

ACL's step is 5

rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0

rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work (4 times matched) (Active)

rule 10 deny ip destination 192.168.0.100 0 (4 times matched)

この出力は、ルール5がアクティブであることを示しています。ping操作の結果、ルール5とルール10は4回一致しました。

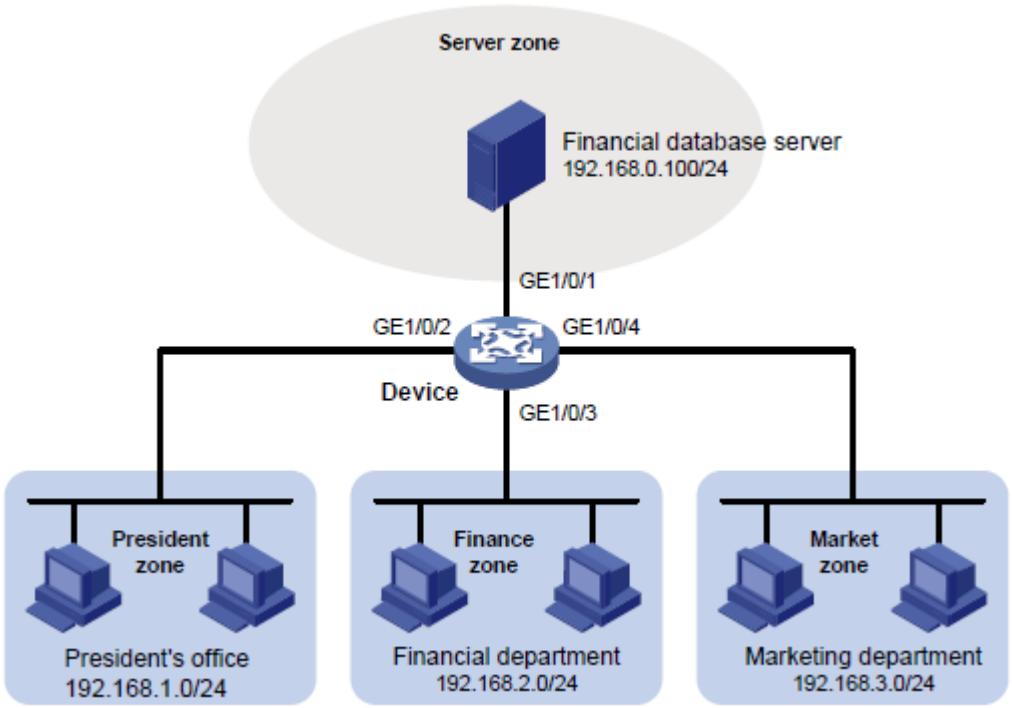
例:ゾーンペアベースのパケットフィルタの設定

ネットワーク構成

企業は、デバイスを介して部門を相互接続します。財務データベースサーバー、社長室、財務部門、およびマーケティング部門は、異なるセキュリティゾーンに属しています。次のようにパケットフィルタを設定します。

- 社長室から財務データベースサーバーへのアクセスをいつでも許可します。
- 就業日の就業時間中(8:00～18:00)にのみ、財務部から財務データベースサーバーへのアクセスを許可します。
- 他の部門から財務データベースサーバーへのアクセスを拒否します。

図2 ネットワークダイアグラム



手順

#セキュリティゾーン**Server**を作成し、インターフェイスGigabitEthernet 1/0/1をセキュリティゾーンに追加します。

<Device> system-view

[Device] security-zone name Server

[Device-security-zone-Server] import interface gigabitethernet 1/0/1

[Device-security-zone-Server] quit

#セキュリティゾーン**President**を作成し、インターフェイスGigabitEthernet 1/0/2をセキュリティゾーンに追加します。

[Device] security-zone name President

[Device-security-zone-President] import interface gigabitethernet 1/0/2

[Device-security-zone-President] quit

#セキュリティゾーン**Finance**を作成し、インターフェイスGigabitEthernet 1/0/3をセキュリティゾーンに追加します。

[Device] security-zone name Finance

[Device-security-zone-Finance] import interface gigabitethernet 1/0/3

[Device-security-zone-Finance] quit

#セキュリティゾーン**Market**を作成し、インターフェイスGigabitEthernet 1/0/4をセキュリティゾーンに追加します。

[Device] security-zone name Market

[Device-security-zone-Market] import interface gigabitethernet 1/0/4

[Device-security-zone-Market] quit

#就業日の8:00から18:00までの定期的な時間範囲を作成します。

[Device] time-range work 08:0 to 18:00 working-day

#社長室のオフィスから財務データベースサーバーへのアクセスをいつでも許可するようにACL 3000を設定します。

Device] acl advanced 3000

[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0

[Device-acl-ipv4-adv-3000] quit

#就業日の就業時間中にのみ、財務部から財務データベースサーバーへのアクセスを許可するようにACL 3001を設定します。

[Device] acl advanced 3001

[Device-acl-ipv4-adv-3001] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work

[Device-acl-ipv4-adv-3001] quit

#ACL 3002を設定して、他の部門から財務データベースサーバーへのアクセスを拒否します。

[Device] acl advanced 3002

[Device-acl-ipv4-adv-3002] rule deny ip source any destination 192.168.0.100 0

[Device-acl-ipv4-adv-3002] quit

#送信元セキュリティゾーンPresidentと宛先セキュリティゾーンServerを持つゾーンペアを作成します。パケットフィルタリングのためにACL 3000をゾーンペアに適用します。

[Device] zone-pair security source president destination server

[Device-zone-pair-security-President-Server] packet-filter 3000

[Device-zone-pair-security-President-Server] quit

#送信元セキュリティゾーンFinanceと宛先セキュリティゾーンServerを持つゾーンペアを作成します。パケットフィルタリングのためにACL 3001をゾーンペアに適用します。

[Device] zone-pair security source finance destination server

[Device-zone-pair-security-Finance-Server] packet-filter 3001

[Device-zone-pair-security-President-Server] quit

#送信元セキュリティゾーンMarketと宛先セキュリティゾーンServerを持つゾーンペアを作成します。

パケットフィルタリングのために、ACL 3002をゾーンペアに適用します。

[Device] zone-pair security source market destination server

[Device-zone-pair-security-Market-Server] packet-filter 3002

[Device-zone-pair-security-Market-Server] quit

設定の確認

#財務部のPCが、勤務時間中にデータベースサーバーに対してpingを実行できることを確認します(この例では、すべてのPCがWindows 10を使用しています)。

C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255 Reply from 192.168.0.100: bytes=32 time<1ms TTL=255 Reply from 192.168.0.100: bytes=32 time<1ms TTL=255 Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.100:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

#マーケティング部門のPCが、勤務時間中にデータベースサーバーに対してpingを実行できないことを確認します。

C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.0.100:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

#デバイス上のIPv4拡張ACL 3001および3002の設定と試合の統計を、営業時間内に表示します。

[Device] display acl 3001

Advanced IPv4 ACL 3001, 2

rules,

ACL's step is 5

rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work (4 times matched) (Active)

[Device] display acl 3002

Advanced IPv4 ACL 3002, 1 rule,

ACL's step is 5

rule 0 deny ip destination 192.168.0.100 0 (4 times matched)

この出力は、ACL 3001のルールがアクティブであることを示しています。ping操作の結果、ACL 3001とACL 3002の両方が4回一致しました。