

A decorative graphic on the left side of the text bar, consisting of a vertical stack of four squares: a red square at the top, followed by a white square, a grey square, and a white square at the bottom.

ファイアウォールテクノロジー 初心者からマスターへ

内容

01

ポリシーの設定方法

02

NATの設定方法

03

VPNの設定方法

04

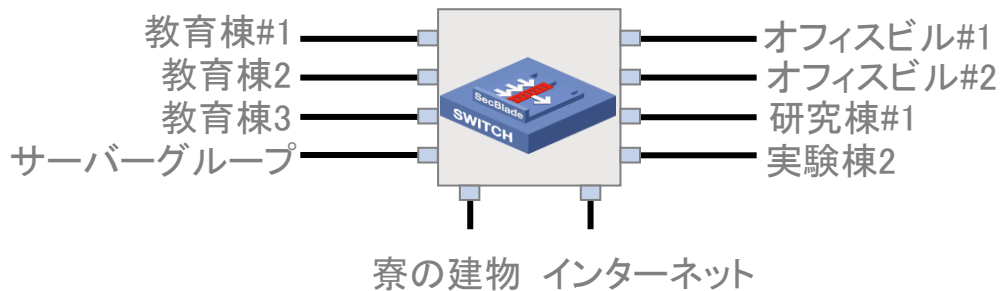
ソフトウェアを更新する方法

05

トラブルシューティング

基本概念

- デフォルトでは、V7 ファイアウォールは**すべてdisable**になっています。つまり、空の割り当ての場合、サービスは使用できません。(Managementゾーンを除く)
- セキュリティゾーンは、ファイアウォールとスイッチおよびルータを区別する基本特性の1つです。インターフェイスは、ビジネスセキュリティゾーンに追加された後にのみデータを転送します。
- セキュリティゾーンを使用して、ファイアウォールデバイス上の同じセキュリティ要件を持つ複数のインターフェイスを管理できます。また、管理者は同じセキュリティ要件を持つインターフェイスを同じセキュリティゾーンに分割できます。
- それぞれのセキュリティゾーンは、セキュリティポリシーの設定後に相互にアクセスできます。



セキュリティゾーンを構成する方法

- セキュリティゾーンにレイヤー2メンバーを追加する

注:レイヤー2メンバーをセキュリティゾーンに追加する場合は、vlanパラメータを追加する必要があります。

- セキュリティゾーンにレイヤー3メンバを追加する

注:集約ポート、vlan仮想インターフェイス、ethポートなど、セキュリティゾーンに転送する実際のインターフェイスを追加します。

Edit Security Zone

Security zone name: Trust (1-31 chars)

VLAN members: (1-4094)

Layer 2 members

Filter

Interface List

- Core2IPS
- IPS2Core
- GE1/0/2
- BAGG1
- BAGG2

Member List(0)

Layer 3 members

Filter

Interface List

- GE1/0/0
- GE1/0/1
- GE1/0/3
- GE1/0/4
- GE1/0/5
- GE1/0/6
- GE1/0/7
- GE1/0/8
- GE1/0/9
- GE1/0/10

Member List(0)

OK Cancel

セキュリティポリシーを構成する方法

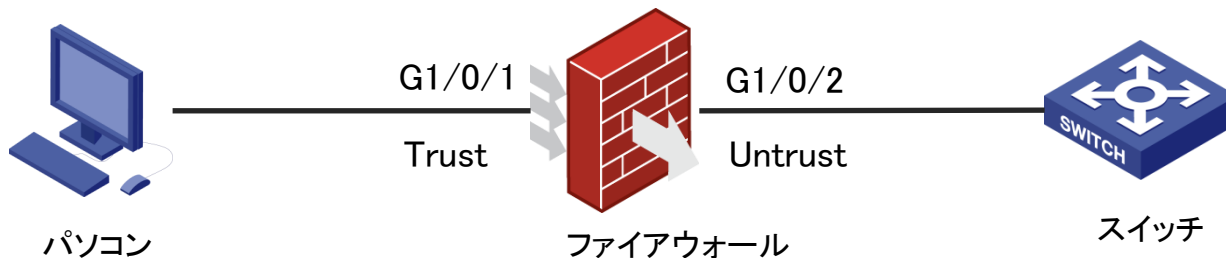
➔ セキュリティポリシーを構成する方法

- ファイアウォールに送られるメッセージは二つのタイプに分けられ、一つはローカルファイアウォールに送られるもので、もう一つはファイアウォールによって転送されるものである。

セキュリティポリシーを構成する方法

● セキュリティポリシーの設定方法 - ローカルメッセージ

- インターフェイスG1/0/1をファイアウォールにtelnet接続するには、まずインターフェイスG1/0/1をセキュリティゾーンTrustに追加してから、外部ゾーンTrustからローカルゾーンにセキュリティポリシーを設定します。
- ピアスイッチをファイアウォールからpingするには、まずスイッチと相互接続するインターフェイスG1/0/2をセキュリティゾーンUntrustに追加し、次にローカルゾーンのセキュリティポリシーをUntrustゾーンに設定します。



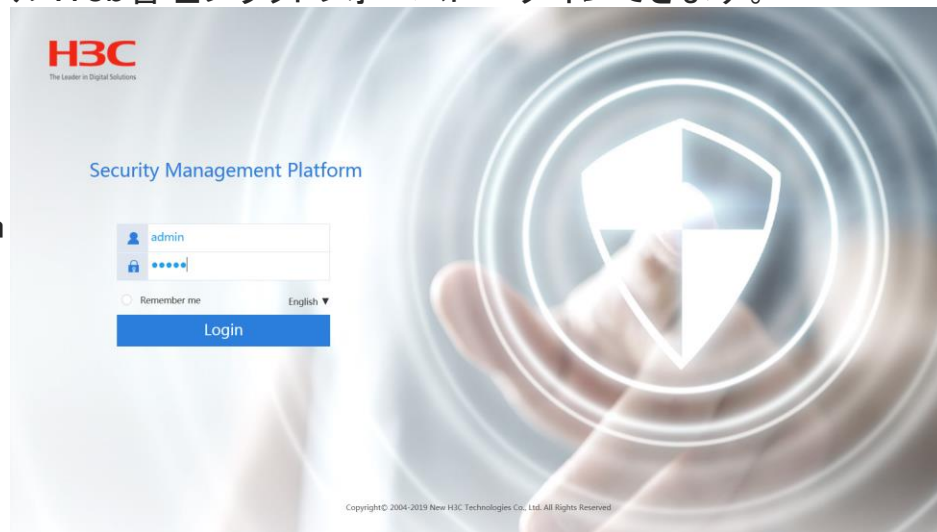
セキュリティポリシーを構成する方法

- セキュリティポリシーの設定方法 - ローカルメッセージ

- デフォルトでは、管理ポートG1/0/0は管理ゾーンに属し、管理ゾーンとローカルゾーンは相互接続されています。したがって、直接接続された管理ポートG1/0/0を介してデフォルトのアドレスとアカウント番号を入力すると、ファイアウォールWeb管理プラットフォームにログインできます。

<https://192.168.0.1/>

ユーザー名/パスワード:admin/admin



セキュリティポリシーを構成する方法

● セキュリティポリシーの設定方法 - ローカルメッセージ

- Web管理プラットフォームで、Policies > Security Policiesの下のCreateセキュリティポリシーをクリックします。
- Source Zone/Destination Zoneを選択し、ActionをPermitにします。
- さらに、ソースアドレス、宛先アドレス、およびソース/宛先ポート(サービス)などのパラメータを設定して、アクセス制御の目的を達成できます。

Security Policies

»

To have the security policy configuration take effect, you must click **Submit**. To have the content security configuration take effect, you must click **Submit**.

Supported total policies:10000,Supported policies for each type 5000.

<input type="checkbox"/>	Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matc...	Traffic	Enabl...	Enable
<input type="checkbox"/>	Trust...	Trust	Local	IPv4	0		Any	Any	telnet	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>

セキュリティポリシーを構成する方法

● セキュリティポリシーの設定方法 - ローカルメッセージ

- セキュリティポリシーの右側にあるEditをクリックして、ソースアドレス172.31.0.0/22のアドレスオブジェクトにのみローカルアクセスを許可するようにセキュリティポリシーを変更します。

The screenshot shows the configuration page for a security policy. The 'Source IP/MAC address' field is highlighted with a red box and contains the value '172.31.0.0'. Other fields include Name (Trust→Local_0_IPv4), Source zone (Trust), Destination zone (Local), Type (IPv4), Policy group (Select a policy group), Description (1-127 chars), Action (Permit), Destination IP (Any), and Service (telnet).

セキュリティポリシーを構成する方法

● セキュリティポリシーの設定方法 - Forwarding Message

アップリンクポートG1/0/4とダウンリンクポートG1/0/5をそれぞれTrustゾーンとUntrustゾーンに追加し、172.31.0.0/22の送信元アドレスだけが192.168.0.0/24の宛先アドレスにアクセスできるようにします。

- Web管理プラットフォームで、Policies>Security Policiesの下でCreateセキュリティポリシーをクリックします。
- Source Zone/Destination Zoneを選択し、172.31.0.0/22および192.168.0.0/24のIPv4オブジェクトグループを追加して、送信元アドレス/宛先アドレスを選択します。

Security Policies

⊕ Create ▾ × Delete 📄 Copy ➕ Move 🟢 Enable stats ▾ 🔴 Disable stats ▾ 🟢 Enable 🔴 Disable 🗑️ Clear stats >> Enter rule name 🔍 Search 📄 Adv...

To have the security policy configuration take effect, you must click **Submit**. To have the content security configuration take effect, you must click **Submit**.

Supported total policies:10000,Supported policies for each type 5000.

<input type="checkbox"/>	Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matc...	Traffic	Enabl...	Enable
<input type="checkbox"/>	Trust...	Trust	Local	IPv4	0		Any	Any	telnet	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Trust...	Trust	Untrust	IPv4	1		172.31.0.0	192.168.0.0	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>

セキュリティポリシーを構成する方法

- セキュリティポリシーの設定方法 - **Forwarding Message**
- このとき、172.31.0.0ネットワークセグメントのアドレスは192.168.0.0ネットワークセグメントにアクティブにアクセスできますが、192.168.0.0ネットワークセグメントは172.31.0.0ネットワークセグメントにアクセスできません。
 - これは、セキュリティポリシーが方向性を持っているためです。192.168.0.0ネットワークセグメントが他のネットワークセグメントにアクティブにアクセスできるようにするには、UntrustゾーンからTrust Zoneへのリバースセキュリティポリシーを確立する必要があります。

<input type="checkbox"/>	Name	Src zone	Dst zone	Type	ID	Descri...	Src address	Dst address	Service	User	Action	Conte...	Matc...	Traffic	Enabl...	Enable
<input type="checkbox"/>	Trust...	Trust	Local	IPv4	0		Any	Any	telnet	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Trust...	Trust	Untrust	IPv4	1		172.31.0.0	192.168.0.0	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Untru...	Untrust	Trust	IPv4	2		192.168.0.0	172.31.0.0	Any	Any	Permit				<input type="checkbox"/>	<input checked="" type="checkbox"/>

内容

01

ポリシーの設定方法

02

NATの設定方法

03

VPNの設定方法

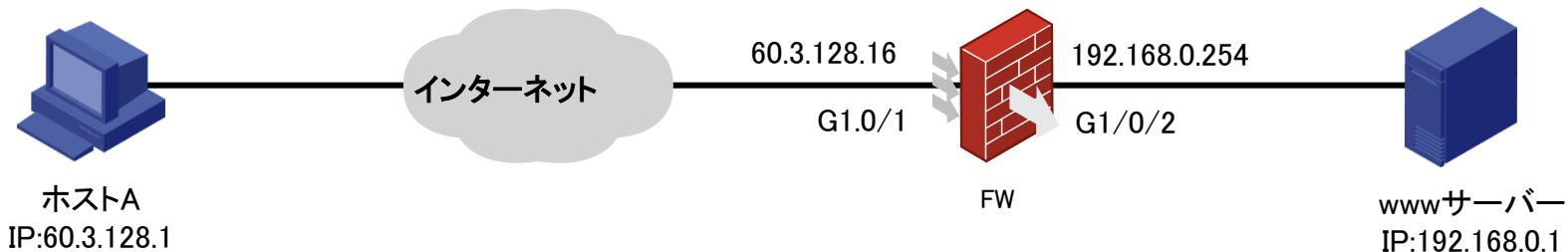
04

ソフトウェアを更新する方法

05

トラブルシューティング

NATサーバ



- 内部ネットワーク内のサーバがパブリックネットワークにサービスを提供する必要がある
- NATデバイスを使用すると、外部ネットワークユーザは指定されたNATアドレスとポートを介してこれらの内部サービスにアクセスできます。
- NAT内部サーバの設定では、NATアドレスとポート、および内部サーバアドレスとポート間のマッピング関係を定義します。

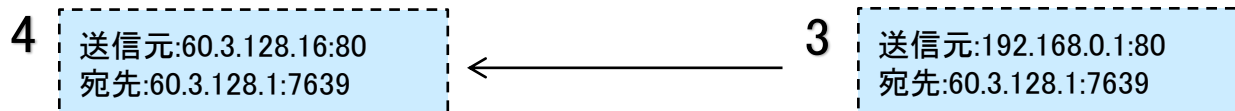
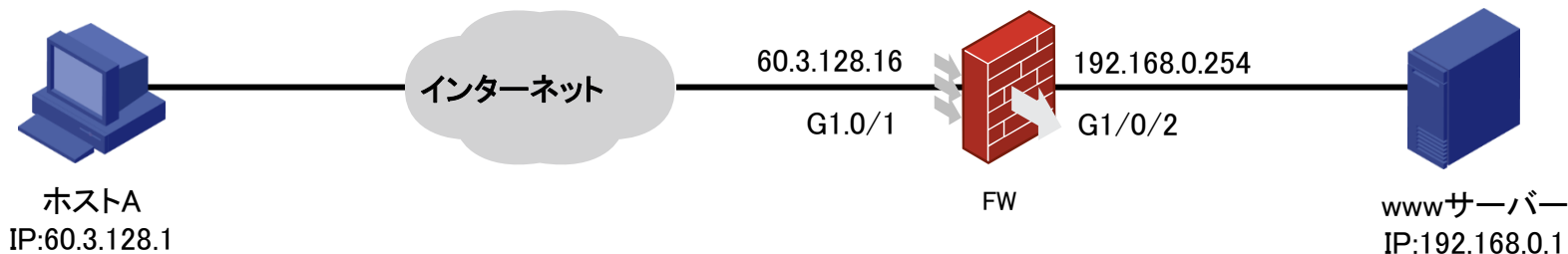
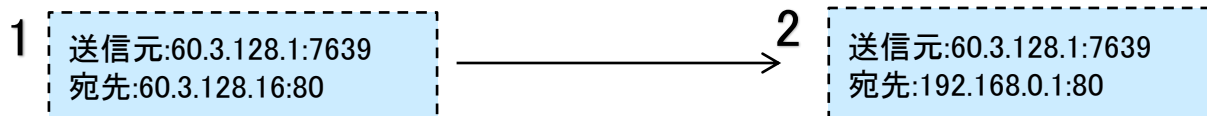
内部サーバの実装

H3C

The Leader in Digital Solutions

NATテーブル

NAT前	NAT後
60.3.128.16:80	192.168.0.1:80



内部サーバの設定

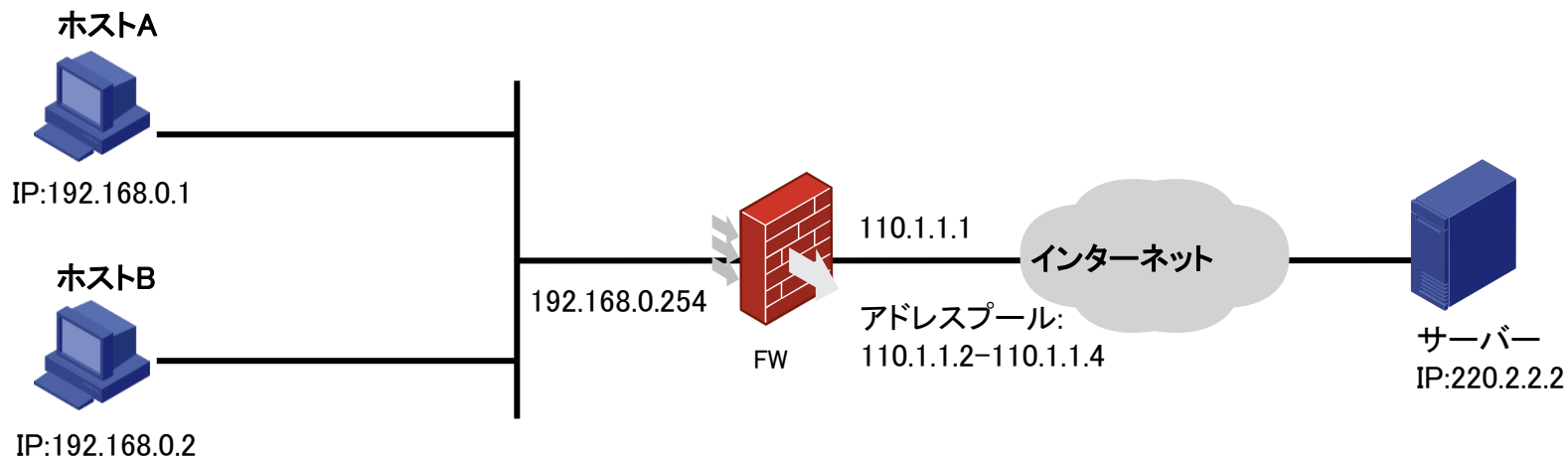
- ナビゲーションバーのPolicies>NAT>NAT Servers>Policy Configurationをクリックして、新しいNAT Server Ruleを作成します。

Create NAT Server Rule

Rule name	ServerRule_1 (1-63 chars)
Interface	GE1/0/1 *
Protocol type	(1-255)
Mapping	One single public address with one single or no public port *
Mapping description	(1-63 chars)
Public IP	<input checked="" type="radio"/> Specify an IP address 60.3.128.16 *
	<input type="radio"/> Use primary IP of the interface (Easy IP) as the public IP address of the NAT server <input type="radio"/> Use primary IP of a Loopback interface as the public IP address of the NAT server
Public port	(1-65535)
Public port VRF	Public network
Server IP	192.168.0.1 *
Server port	(1-65535)
Server VRF	Public network
ACL for packet matching	
VRRP group	

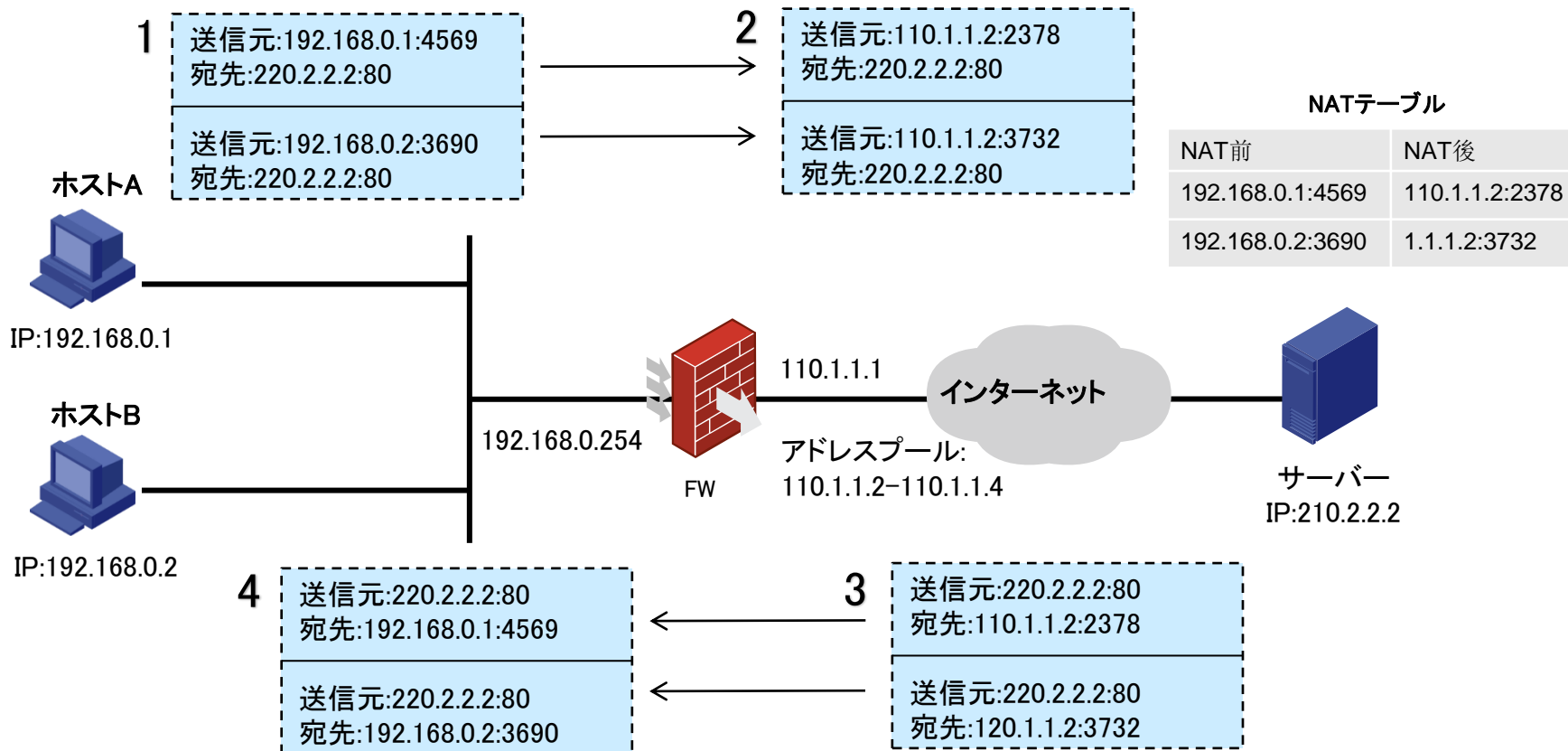
OK Cancel

NATアウトバウンド



- Outboundダイナミックアドレス変換は通常、内部プライベートネットワークアドレスを外部パブリックネットワークアドレスに変換するために、外部ネットワーク上のインターフェイスに適用されます。

NATアウトバウンドの実装



NATアウトバウンド(1)の設定

- ナビゲーションバーのPolicies>NAT>NAT Advanced Settings>NAT Address Groupsをクリックし、Createをクリックしてアドレスグループを作成し、Addをクリックしてアドレスグループメンバーをアドレスグループに追加します。

Create NAT Address Group

Address group ID: 1 (0-65535)

Address group name: (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
110.1.1.2	110.1.1.4

OK Cancel

NATアウトバウンド(2)の設定

- ナビゲーションバーのObjects > ACL > IPv4ACLをクリックし、Createをクリックして新しいACLを作成します。

The screenshot shows a dialog box titled "Create Rule For IPv4 Advanced ACL". The fields are as follows:

- ACL number: 3000 (3000-3999 or 1-63 chars)
- Rule ID: Auto numbered (0-65534)
- Description: (1-127 chars)
- Action: Permit, Deny
- IP protocol type: ip (0-256, 256 for all IP protocols)
- Match criteria: Source IPv4 address/wildcard mask (192.168.0.0 / 0.0.0.255)
- Source IPv4 address object group
- Destination IPv4 address/wildcard mask
- Destination IPv4 address object group
- Source ports in TCP/UDP packets

Buttons: OK, Cancel

NATアウトバウンドの設定(3)

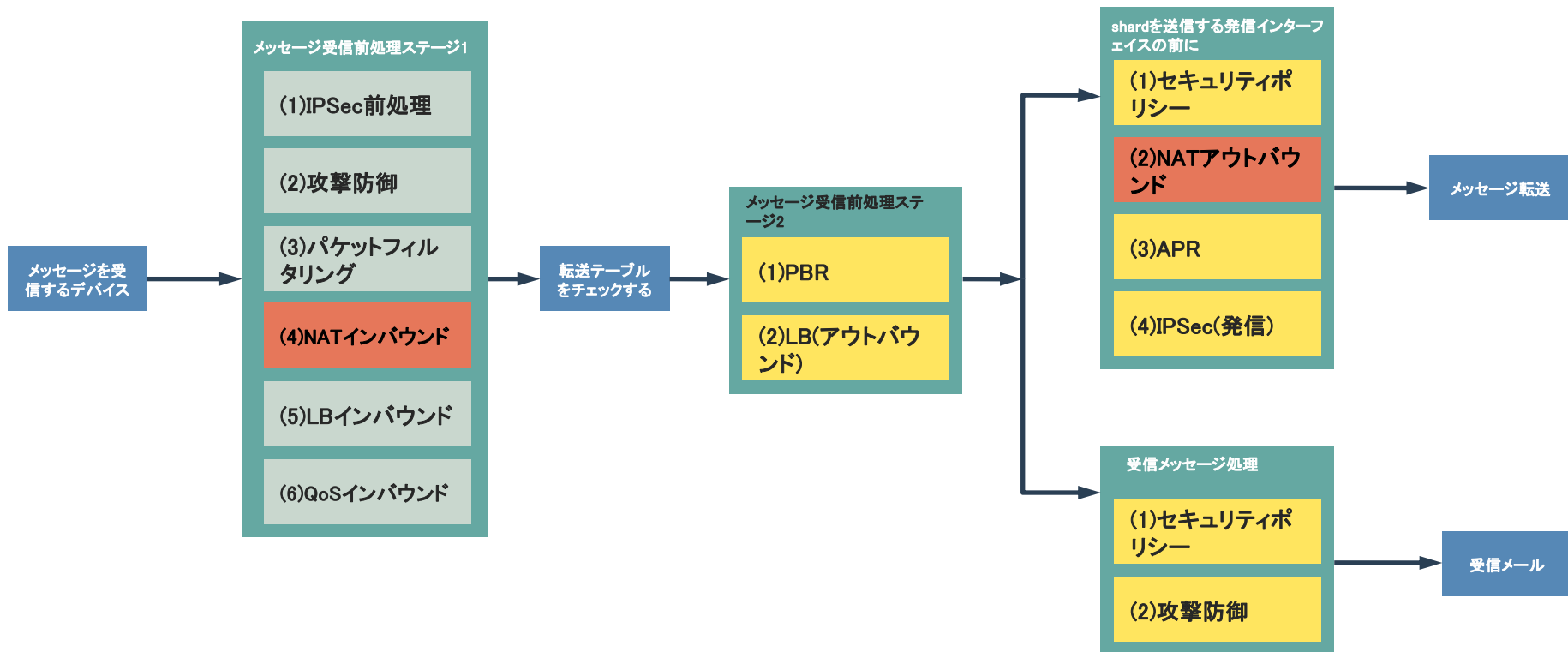
- ナビゲーションバーのPolicies > NAT > Dynamic NATをクリックして、新しいNAT規則を作成します。

The screenshot shows a configuration window titled "Create Outbound Dynamic NAT". The window contains the following fields and options:

- Interface:** GE1/0/2
- ACL:** 3000
- Source address after NAT:** NAT address group Easy IP (?)
- Source address after NAT (dropdown):** 1
- VRF:** Public network
- Translation mode:** PAT NO-PAT
- Port preservation:** Try to preserve port number for PAT
- Enable this rule:**
- Counting:**

At the bottom of the window are "OK" and "Cancel" buttons.

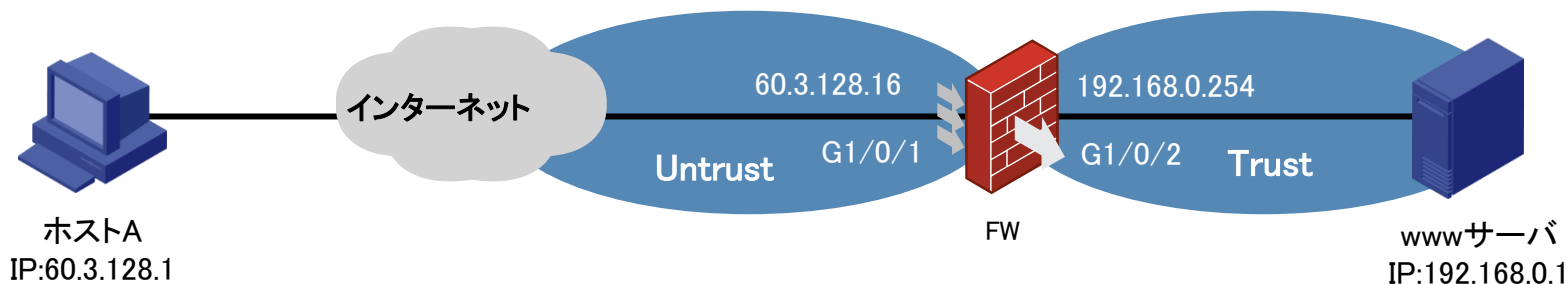
ファイアウォールを通過するメッセージの処理フロー



ファイアウォールを通過するメッセージの処理フロー

- NATサーバとセキュリティポリシー

NATサーバの規則では、TrustゾーンへのUntrustゾーンアクセスのセキュリティポリシーを作成する必要があります。また、宛先内部サーバのアドレスは**プライベートネットワークのアドレスである必要があります**。

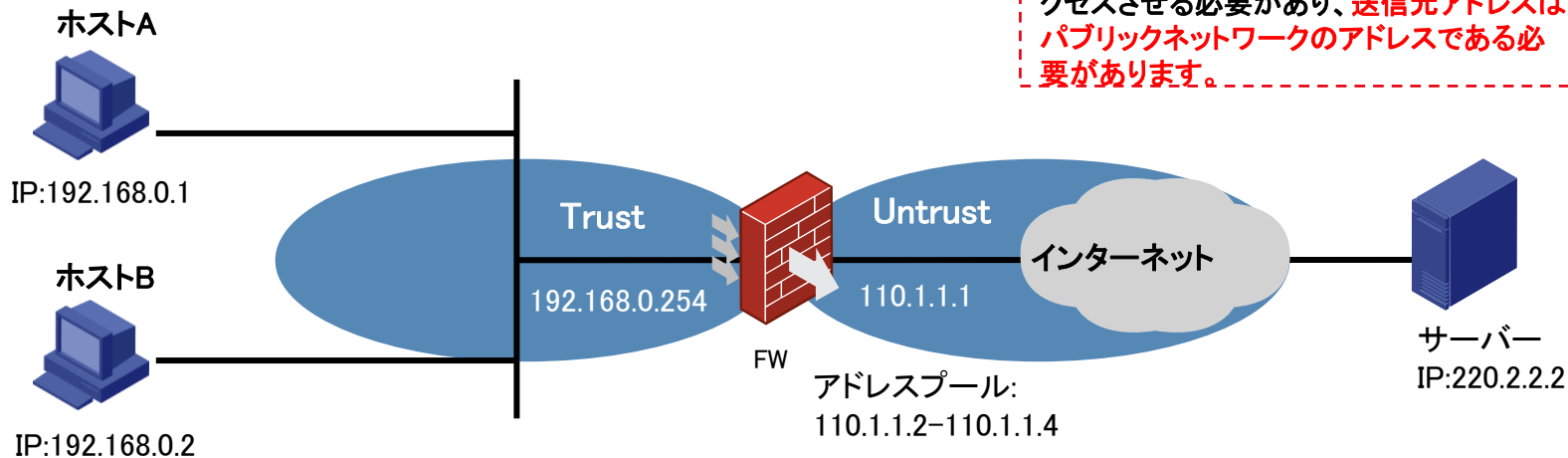


- 192.168.0.1の内部ネットワークホストの外部アドレスは60.3.128.16です。外部ゲートウェイ60.3.128.1から60.3.128.16にアクセスするためのセキュリティポリシーの規則は何ですか?

ファイアウォールを通過するメッセージの処理フロー

● NATアウトバウンドおよびセキュリティポリシー

NATアウトバウンド規則では、TrustゾーンのセキュリティポリシーをUntrustゾーンにアクセスさせる必要があります、送信元アドレスはパブリックネットワークのアドレスである必要があります。



- 192.168.0.1の内部ネットワークホストは220.2.2.2のパブリックネットワークサーバーにアクセスし、送信元アドレスをゲートウェイファイアウォールの110.1.1.2のアドレスプールのアドレスに変換します。セキュリティポリシーの規則は何ですか？

内容

01

ポリシーの設定方法

02

NATの設定方法

03

VPNの設定方法

04

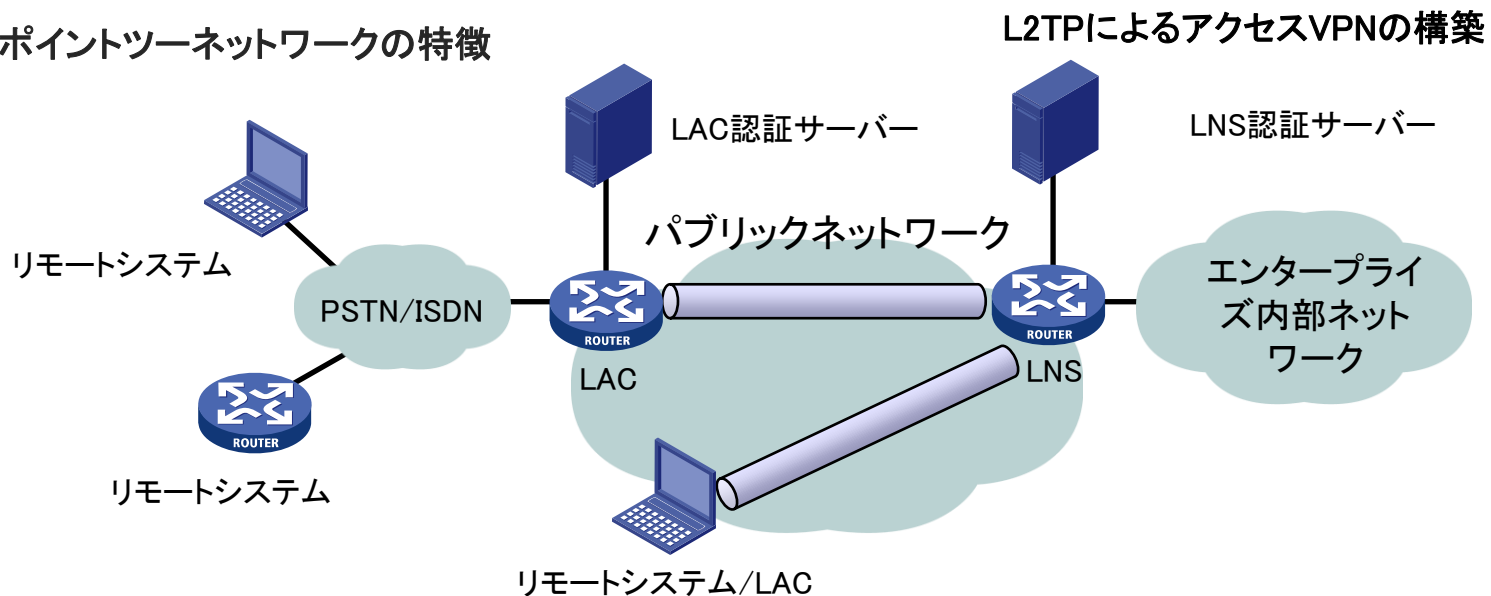
ソフトウェアを更新する方法

05

トラブルシューティング

L2TP VPNの概要

- トンネリング伝送PPP
- 認証アドレスと動的アドレス割り当て
- ポイントツーネットワークの特徴

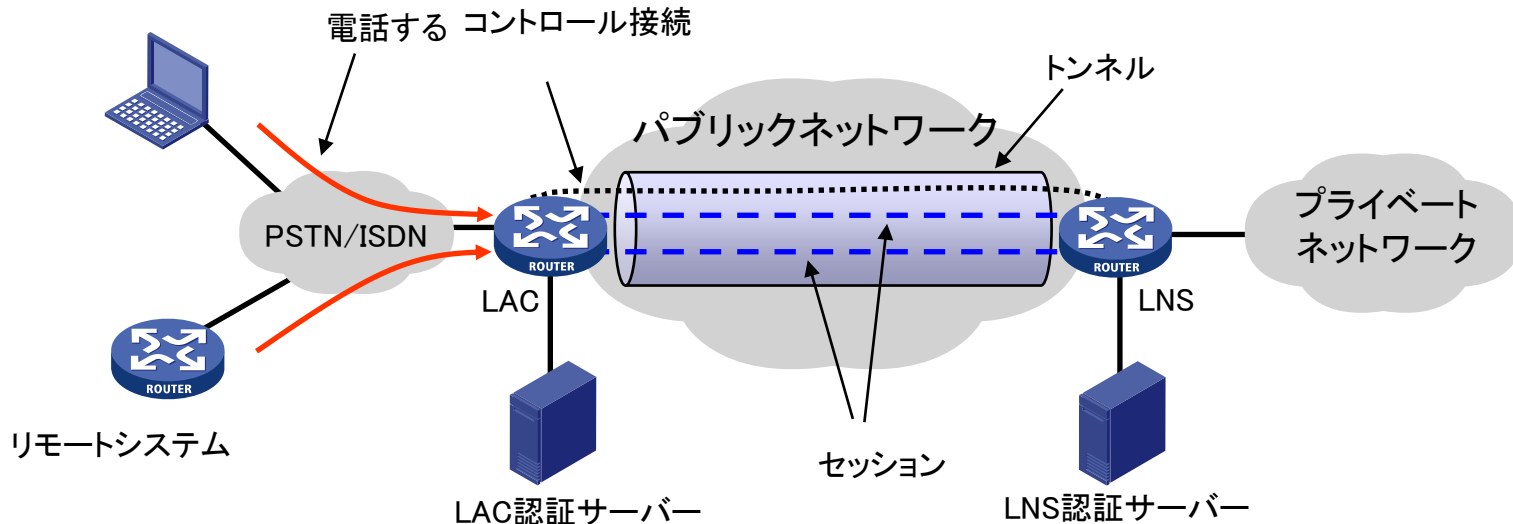


L2TPコンポーネント

- (リモートシステム)
- LAC(L2TPアクセスコンセントレータ)
- LNS(L2TPネットワークサーバー)

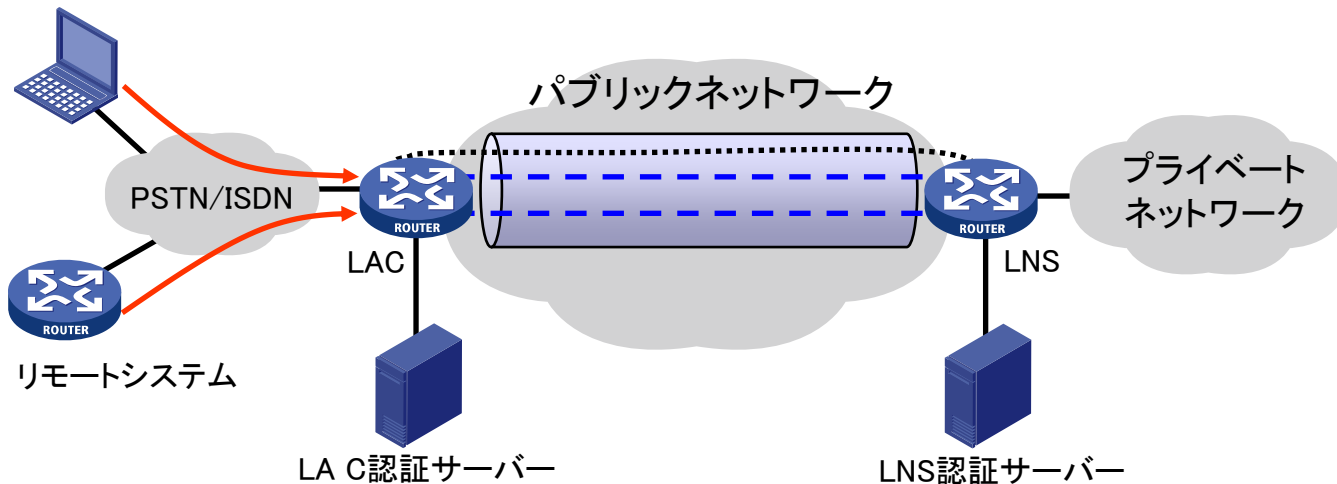
L2TPの条件

リモートシステム



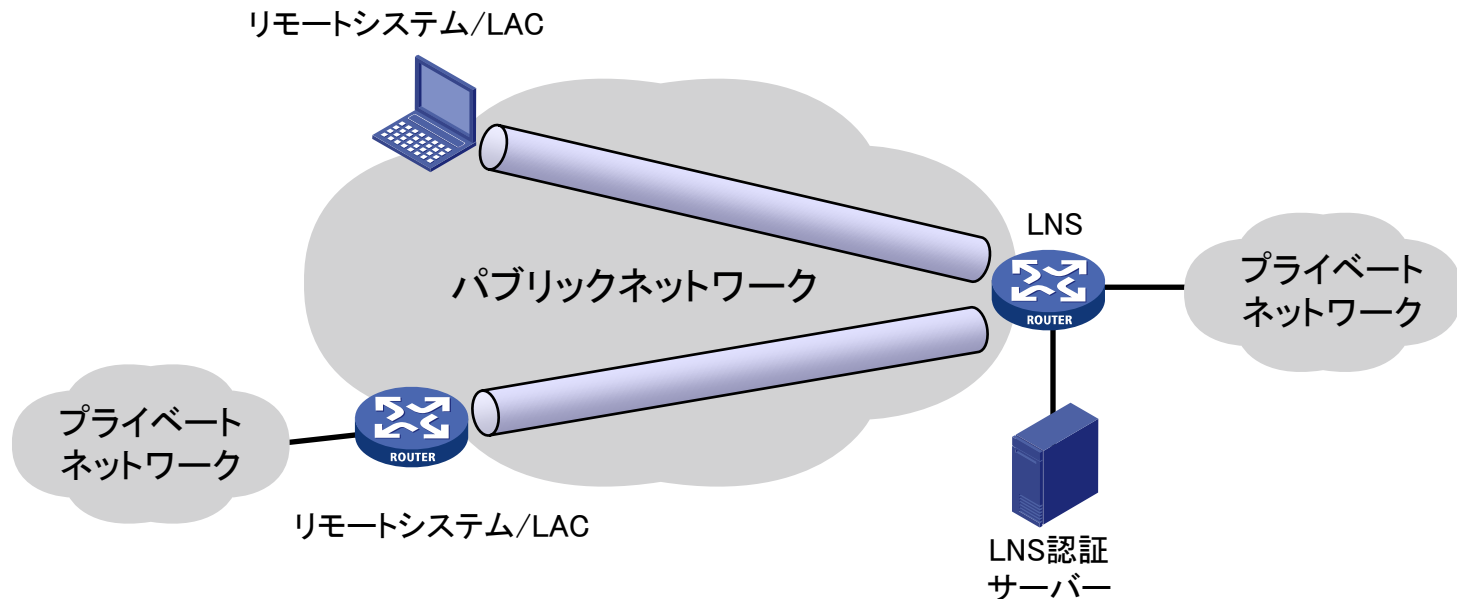
独立したLACトポロジー構造

リモートシステム



- ISPがLACデバイスを提供
- LACデバイスによる追加のユーザー制御と管理
- リモートシステムまたは支店はインターネットアクセスポイントに依存しない

カスタマーLACトポロジ構造



- 直接インターネットアクセスポイントが必要です
- 追加のLACデバイスに依存せず、柔軟性に優れています。
- 企業はインターネット上で直接VPNを構築可能

L2TPの設定作業(1)

● LAC側

- L2TPを有効にする
- L2TPグループを作成
- LNSへのトンネル確立要求を開始するLACのトリガー条件を設定します。
- LNSのIPアドレスの設定
- LAC側のVPNユーザーに対するAAA認証の設定

Enable L2TP

Create L2TP Tunnel

Group type LAC LNS

Group number *(1-65535)

Local tunnel name (1-31 chars)

Tunnel password auth

L2TP server addresses *+

PPP authentication mode --NONE--

Advanced configuration

Hello interval 60 seconds (60-1000)

AVP hiding

Flow control

OK Cancel

L2TPの設定作業(2)

● LNS側

- L2TPを有効にする
- L2TPグループを作成
- 仮想テンプレートを設定する
- L2TPトンネル確立要求を受信するLNSのトリガー条件を設定します。
- LNS側のVPNユーザーに対するAAA認証の設定

Enable L2TP

Create L2TP Tunnel

Group type: LAC LNS

Group number: *(1-65535)

Local tunnel name: (1-31 chars)

Peer tunnel name: *(1-31 chars)

Tunnel password auth:

User dialup configuration

PPP authentication mode:

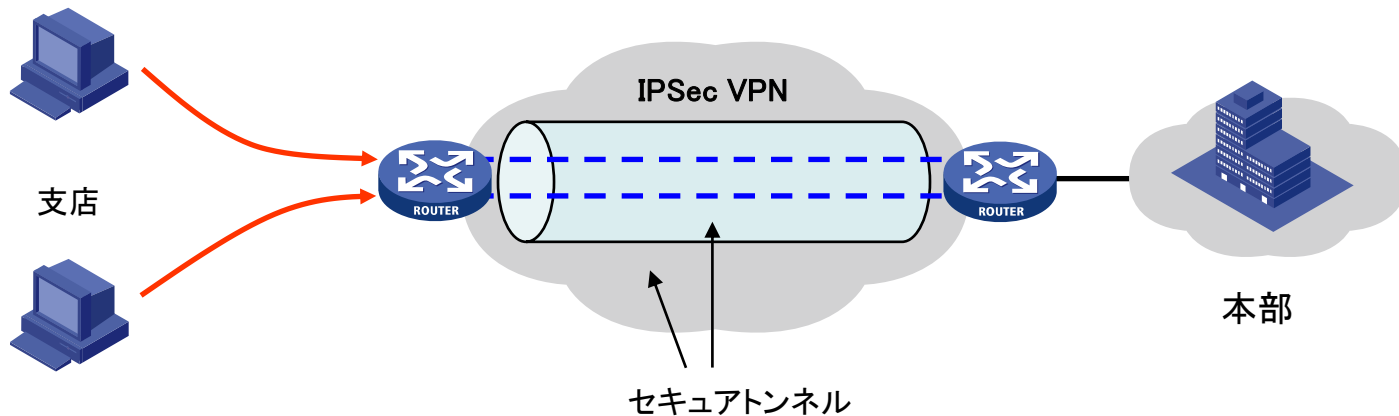
PPP server address: *

Subnet mask: *

User address pool:

OK Cancel

IPSec VPN



- IPsecは、IPネットワーク上のデータ送信のセキュリティと機密性を保証するためにIETFによって開発されたレイヤ3セキュリティプロトコルシステムです。
- IPSecは、IPLレイヤでIPメッセージのセキュリティサービスを提供します。

IPSec VPNアーキテクチャ

- **セキュリティプロトコル**

- データ保護を担当
- AH/ESP

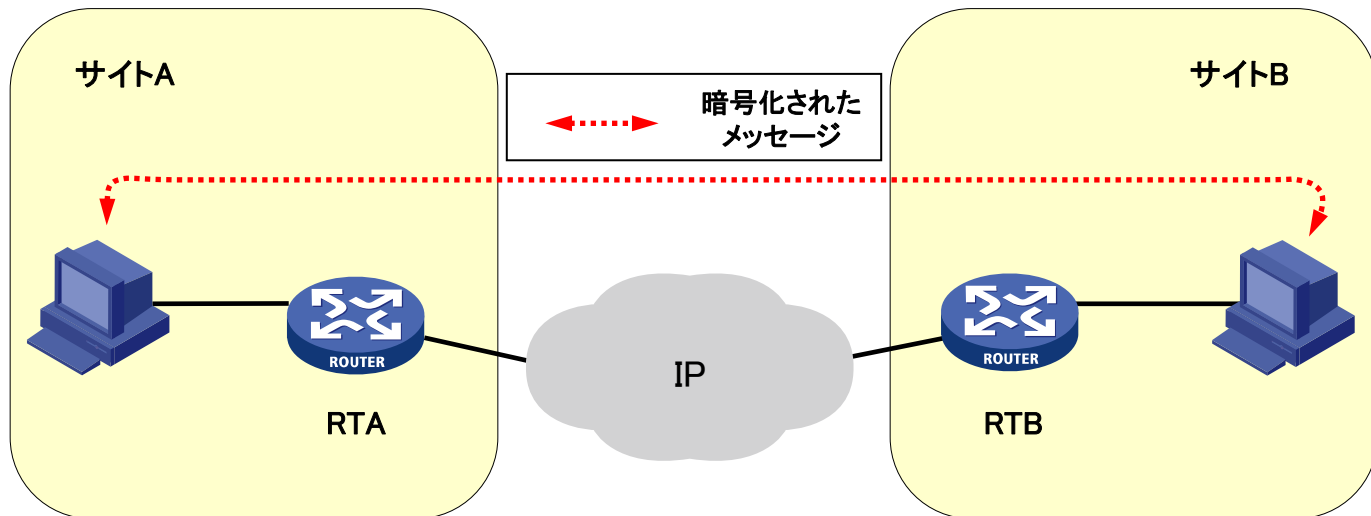
- **作業モード**

- 転送モード: エンドツーエンド保護の実現
- トンネルモード: サイト間保護の実現

- **インターネット鍵交換**

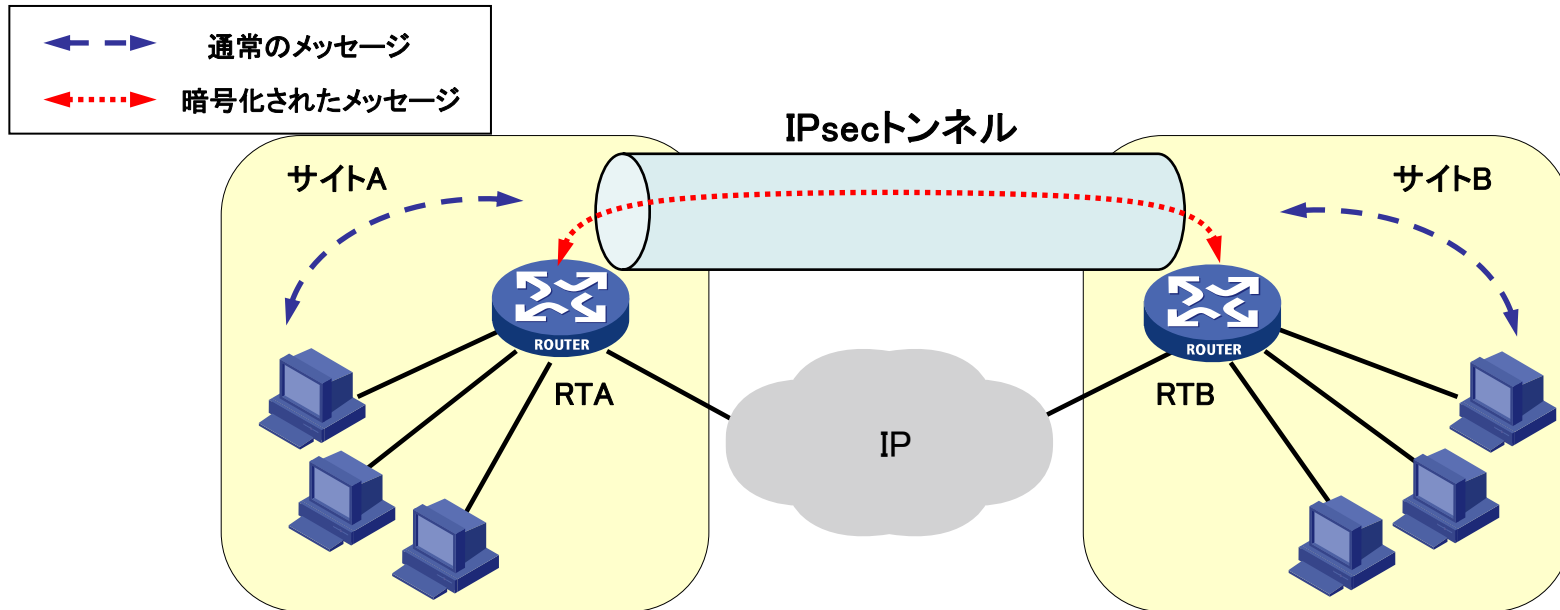
- IKE:セキュリティプロトコルのネゴシエーション

IPsecトランスポートモード



- 通信する必要がある2台の端末コンピュータは、相互間で直接IPSecプロトコルを実行します。AHとESPは、上位層プロトコル(トランスポート層プロトコル)を保護するために直接使用されます。

IPsecトンネルモード



- 2つのセキュリティゲートウェイが相互間でIPSecプロトコルを実行し、相互間で暗号化する必要があるデータについて合意し、AHまたはESPを使用してデータを保護します。

セキュリティアソシエーション

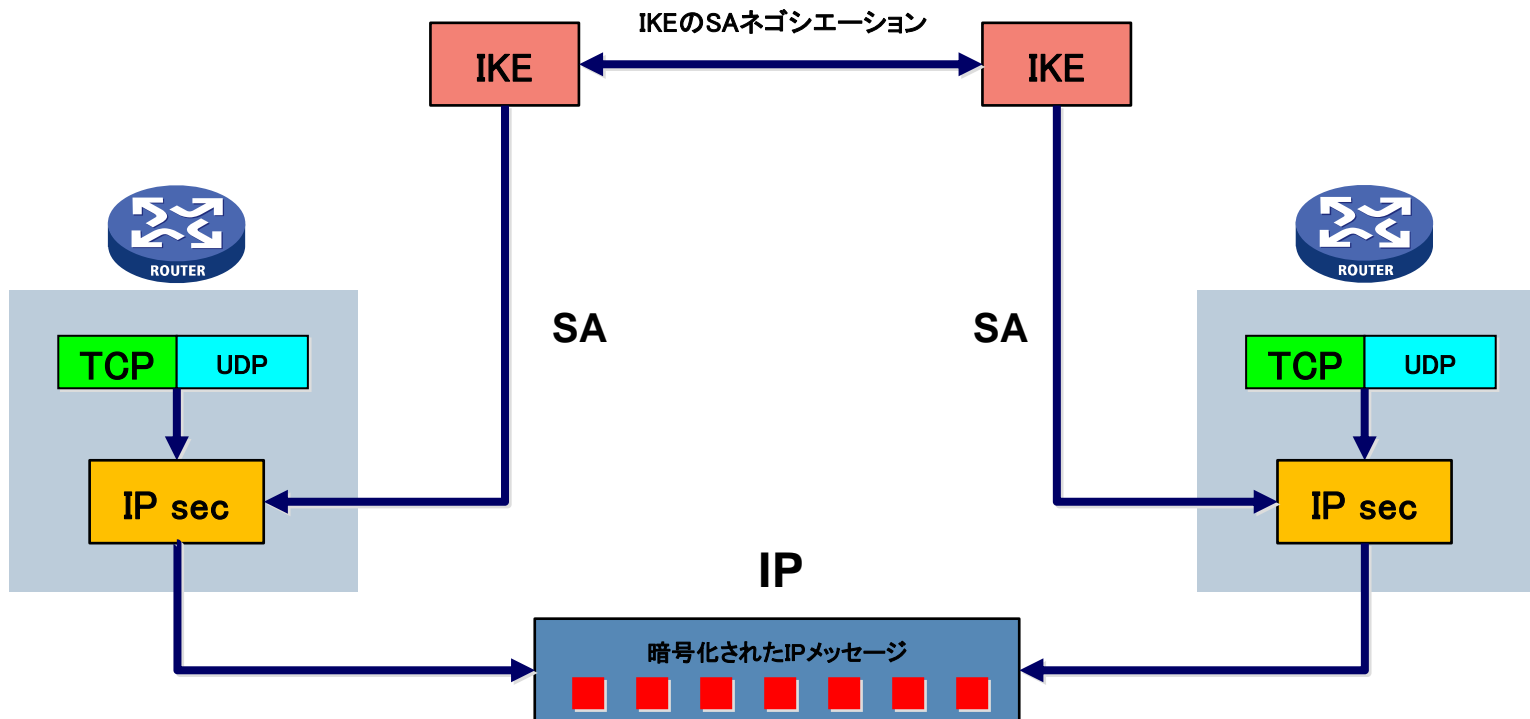
- セキュリティアソシエーション
- 一意に識別される(トリプル(SPI、IP宛先アドレス、セキュリティプロトコル識別子)によって)
- 各IPSec SAは単方向
- 手動設定/IKEネゴシエーション設定
- IP secが提供するipsecが提供するセキュリティサービスは、SAを介して実装されます。
- IKE SA

IKE

- IKE(インターネットキーエクスチェンジ)
- Diffie-Hellmanを使用した交換
- 完全転送セキュリティ
- UDPポート500

- セキュリティー保護されていないネットワーク上で鍵を配布し、IDを認証する
- 自動ネゴシエーションキー交換およびIPSec用SA確立サービスの提供
- SAを定期的に更新する
- キーを定期的に更新する
- IPSecがアンチリプレイサービスを提供できるようにします。

IKEとIPSecの関係



IKEネゴシエーションの2つの段階

- **ステージ1**

- ステージ2のネゴシエーションを保護するために、ネットワーク上にIKE SAを確立します。
- (メインモード)および(アグレッシブモード)

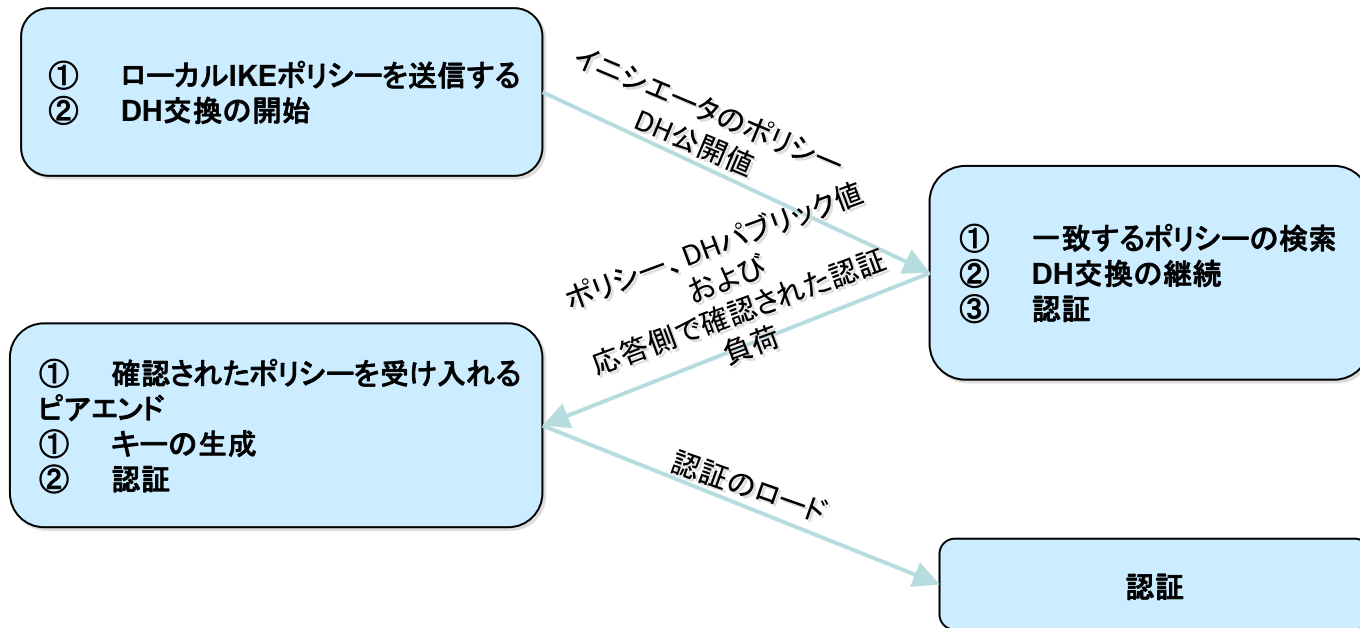
- **ステージ2**

- ステージ1で確立されたIKE SAの保護の下でIPSec SAネゴシエーションの完了
- (クイックモード)

IKEアグレッシブモード

イニシエータ

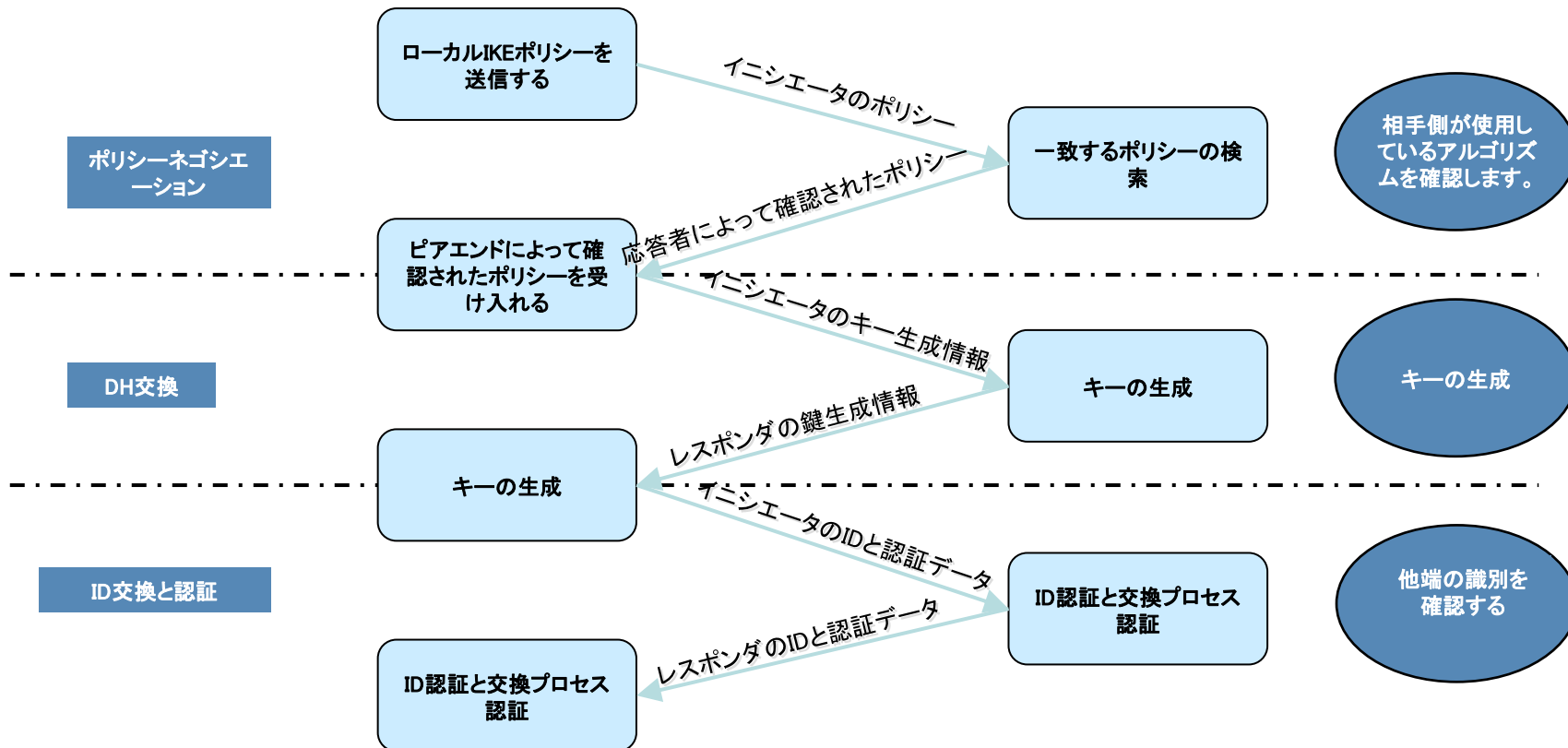
レスポンド



IKEメインモード

イニシエータ

レスポンス



IPsecの設定作業

- セキュリティACLを設定する
- セキュリティ提案の設定
 - セキュリティ提案を作成する
 - セキュリティプロトコルの選択
 - セキュリティアルゴリズムの選択
 - 作業モードを選択
- セキュリティポリシーを構成する
 - IKEを介してネゴシエートされるパラメータを持つセキュリティポリシー
- インターフェイスにセキュリティポリシーを適用する

内容

01

ポリシーの設定方法

02

NATの設定方法

03

VPNの設定方法

04

ソフトウェアを更新する方法

05

トラブルシューティング

Webからのソフトウェアのアップグレード

- ナビゲーションバーのSystem>Upgrade Center>Software Upgradeをクリックし、Upgrade immediatelyを選択します。

Software Upgrade

Software version 7.1.064,Ess 9345P05

Location

Current software image list:

flash:/f1000fw-cmw710-boot-E9345P05.bin
flash:/f1000fw-cmw710-system-E9345P05.bin

Main startup software image list:

flash:/f1000fw-cmw710-boot-E9345P05.bin
flash:/f1000fw-cmw710-system-E9345P05.bin

Webからのソフトウェアのアップグレード

- 選択をクリックして、PCに保存されている起動ファイルをロードします。
- 次にOKをクリックしてアップグレードを開始します。

The screenshot displays the 'Software Upgrade' web interface. The main window shows the current software version as '7.1.064,Ess 9345P05' and the location set to 'Slot1'. It lists two software images: 'flash:/f1000fw-cmw710-boot-E934' and 'flash:/f1000fw-cmw710-system-E934'. A modal dialog titled 'Upgrade Immediately' is open, showing the active MPU as '1024.00MB space in total, 411.82MB space free'. The startup file type is set to 'ipe'. The MPU path is 'C:\Users\y11767\Desktop\SECPATH1080F' with a 'Select *' button. The dialog includes checkboxes for 'Delete all startup files' (unchecked), 'Save running configuration' (checked), and 'Reboot the device immediately' (checked). 'OK' and 'Cancel' buttons are at the bottom.

CLIからのソフトウェアのアップグレード

- IPEファイルには2つのBINファイル(ブートおよびシステム)が含まれています。IPEファイルまたはbinファイルを使用してソフトウェアをアップグレードできます。
- 次に、設定を保存してデバイスをリブートします。

➤ 方法1:

```
<H3C> boot-loader file slot1#flash:/F1080.ipe slot 1 main
```

➤ 方法2:

```
<H3C> boot-loader file boot slot1#flash:/boot.bin system flash:/system.bin  
slot 1 main
```

CLIからのソフトウェアのアップグレード

- デバイスを再起動する前に、設定を正しく確認してください。

```
<F1080>display boot-loader
Software images on slot 1:
Current software images:
  flash:/f1000fw-cmw710-boot-E9345P05.bin
  flash:/f1000fw-cmw710-system-E9345P05.bin
Main startup software images:
  flash:/f1000fw-cmw710-boot-E9345P05.bin
  flash:/f1000fw-cmw710-system-E9345P05.bin
Backup startup software images:
None
```


BootWareからのソフトウェアのアップグレード

- CLIおよびWebが使用できない場合、コンソールポート経由でソフトウェアをアップグレードする
手順1:起動時に、Ctrl+Bを押してBootWareメニューに入り、3を押してEthernetサブメニューに入ります。

```
===== <EXTENDED-BOOTWARE MENU> =====  
|<1> Boot System  
|<2> Enter Serial SubMenu  
|<3> Enter Ethernet SubMenu  
|<4> File Control  
|<5> Restore to Factory Default Configuration  
|<6> Skip Current System Configuration  
|<7> BootWare Operation Menu  
|<8> Skip Authentication for Console Login  
|<9> Storage Device Operation  
|<0> Reboot  
=====
```

Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Ctrl+C: Display Copyright
Enter your choice(0-9): 3

BootWareからのソフトウェアのアップグレード

ステップ2:5を入力してイーサネットパラメータを設定します。

```
=====<Enter Ethernet SubMenu>=====
|Note:the operating device is cfa0
|<1> Download Image Program To SDRAM And Run
|<2> Update Main Image File
|<3> Update Backup Image File
|<4> Download Files(*.*)
|<5> Modify Ethernet Parameter
|<0> Exit To Main Menu
|<Ensure The Parameter Be Modified Before Downloading!>
=====
Enter your choice(0-5): 5
```

BootWareからのソフトウェアのアップグレード

ステップ3:FTPパラメータを入力して、FTPサーバに保存されているIPEファイルをロードします。

```
===== <ETHERNET PARAMETER SET> =====
|Note:      '.' = Clear field.
|           '-' = Go to previous field.
|           Ctrl+D = Quit.
=====
Protocol (FTP or TFTP) :ftp
Load File Name        :f5000fw-cmw710-E9330P07.ipe
                      :
Target File Name      :f5000fw-cmw710-E9330P07.ipe
                      :
Server IP Address     :192.168.0.2
Local IP Address      :192.168.0.1
Subnet Mask           :255.255.255.0
Gateway IP Address    :0.0.0.0
FTP User Name         :admin
FTP User Password     :*****
```

BootWareからのソフトウェアのアップグレード

手順4:2を入力して新しいイメージをロードします。

```
=====<Enter Ethernet SubMenu>=====
|Note:the operating device is cfa0
|<1> Download Image Program To SDRAM And Run
|<2> Update Main Image File
|<3> Update Backup Image File
|<4> Download Files(*.*)
|<5> Modify Ethernet Parameter
|<0> Exit To Main Menu
|<Ensure The Parameter Be Modified Before Downloading!>
=====
Enter your choice(0-5): 2█
```

ステップ5:0を2回入力してBootWareメニューに戻り、デバイスをリブートしてアップグレードを完了します。

ソフトウェアのアップグレード

- たとえば、CLIからソフトウェアをアップグレードします。

手順1:TFTPまたはFTPを使用して、ソフトウェアアップグレードファイル(xxxxx.ipe)をデバイスに転送します。

手順2:デバイスにファイルをロードする

アップグレード

<H3C> **boot-loader file** chassis2#slot0#flash:/xxxxx.ipe chassis 2 slot 0 main

手順3:設定を保存してデバイスをリブートします。

内容

01

ポリシーの設定方法

02

NATの設定方法

03

VPNの設定方法

04

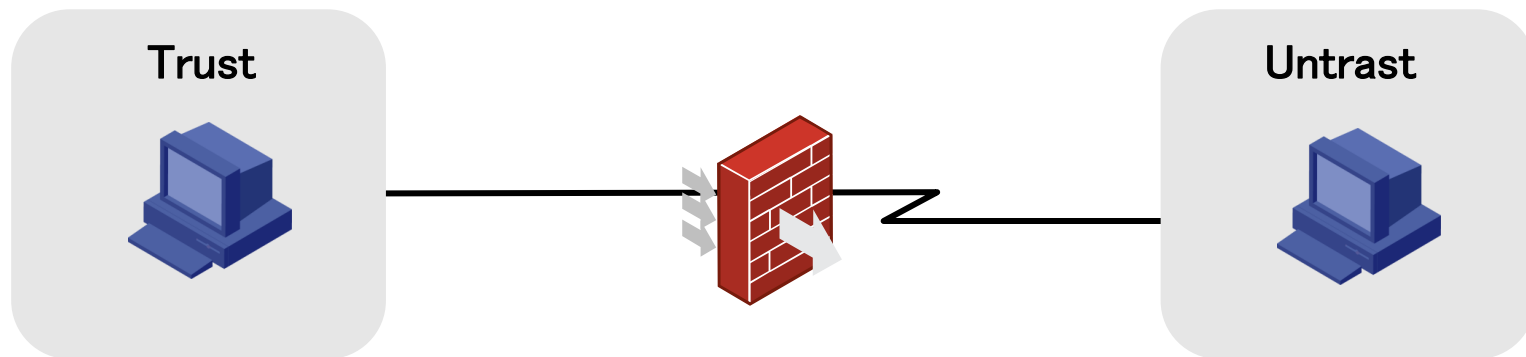
ソフトウェアを更新する方法

05

トラブルシューティング

➔ アイデアのトラブルシューティング

- メッセージはファイアウォールに届きますか？
- メッセージはファイアウォールによってブロックされていますか？



メッセージがファイアウォールに到達するかどうか

- 手順1:セッションテーブルが存在するかどうかを確認する
 - セッションの表示時に送信元アドレスと宛先アドレスを指定し、詳細情報を表示するために詳細を追加します。
 - セッションが存在する場合は、メッセージがファイアウォールに到達したことを意味します。

```
[H3C]display session table ipv4 source-ip 172.31.0.1 destination-ip 172.31.0.4 v
erbose
Slot 1:
Initiator:
  Source      IP/port: 172.31.0.1/50
  Destination IP/port: 172.31.0.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/0
  Source security zone: Management
Responder:
  Source      IP/port: 172.31.0.4/50
  Destination IP/port: 172.31.0.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: ICMP_REPLY
Application: ICMP
Start time: 2017-08-31 07:32:33  TTL: 29s
Initiator->Responder:      62 packets      5208 bytes
Responder->Initiator:      62 packets      5208 bytes
```


メッセージがファイアウォールに到達するかどうか

- ステップ2:メッセージがファイアウォールに送信されるかどうかを確認するIPパケットaclのデバッグ
 - 多数のデバッグメッセージがあります。(送信元アドレス/宛先アドレスおよびプロトコルを示す)ACL一致メッセージを指定する必要があります。

```
acl advanced 3000
```

```
rule 0 permit icmp source 172.31.0.1 0 destination 172.31.0.4 0
```

```
<H3C> debugging ip packet acl 3000
```

```
This command is CPU intensive and might affect ongoing services. Are you sure you  
want to continue? [Y/N]:Y
```

```
<H3C> terminal monitor
```

```
The current terminal is enabled to display logs.
```

```
<H3C> terminal debugging
```

メッセージがファイアウォールに到達するかどうか

- ステップ2:メッセージがファイアウォールに送信されるかどうかを確認するIPパケットaclのデバッグ
 - ACLと一致するデバッグメッセージは、メッセージがファイアウォールに到達したことを示します。到達しなかった場合、メッセージはファイアウォールに到達しません。ルーティングおよびその他のネットワーク要因のトラブルシューティングを行う必要があります。

```
*Aug 31 07:41:40:069 2017 H3C IPFW/7/IPFW_PACKET: -Context=1;
Delivering, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 51129, offset = 0, ttl = 255, protocol = 1
checksum = 39851, s = 172.31.0.1, d = 172.31.0.4
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: ICMP
type = 8, code = 0, checksum = 0xdcba.
```

```
*Aug 31 07:41:40:269 2017 H3C IPFW/7/IPFW_PACKET: -Context=1;
Delivering, interface = GigabitEthernet1/0/0
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 51131, offset = 0, ttl = 255, protocol = 1
checksum = 39849, s = 172.31.0.1, d = 172.31.0.4
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: ICMP
type = 8, code = 0, checksum = 0xdbf1.
```

メッセージがファイアウォールに到達するかどうか

- ステップ3:パケットキャプチャ

- Web管理プラットフォームで、System-Diagnosis Center-Packet Captureを選択し、Start Packet Captureをクリックしてフィルタ条件を設定し、インターフェイスを選択します。トラフィックが大きい場合は、ACLを一致させることをお勧めします。

Navigation Pane

- Virtualization
 - IRF
 - Contexts
- High Availability
- Log Settings
- Report Settings
- Session Aging Time S
- Upgrade Center
 - License Config
- Administrators
- Maintenance
- Diagnosis Center
 - Ping

Packet Capture

Start packet capture Stop packet capture Set packet capture parameters Delete all packet files

Packet Capture Status: Stopped

Set Filters

* Packet capture affects device performance.
Enable it only when necessary.

Interface GE1/0/3

IPv4 IPv6

ACL 3001

Start Cancel

No.	File name	Size (kB)
-----	-----------	-----------

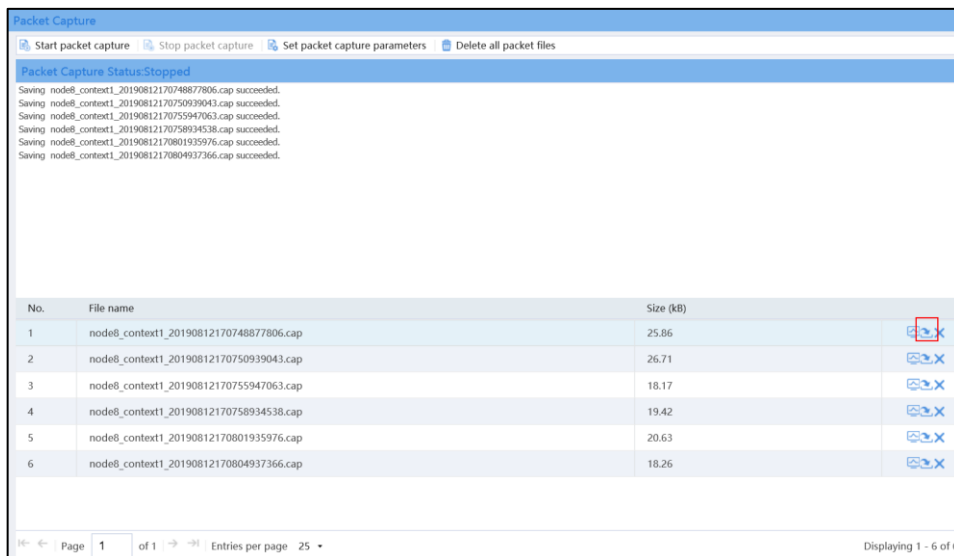
Page 0 of 0 Entries per page 25

Copyright© 2004-2019 New H3C Technologies Co., Ltd. All Rights Reserved

メッセージがファイアウォールに到達するかどうか

- ステップ3:パケットキャプチャ

- メッセージキャプチャのフィルタ条件を設定したら、Startをクリックします。
- パケットをキャプチャした後Stop Packet Captureをクリックし、キャプチャをダウンロードします。



ファイアウォールでメッセージがブロックされているかどうか **H3C**

The Leader in Digital Solutions

- ステップ1: security-policy packet ip aclのデバッグは、セキュリティポリシーがメッセージへのアクセスを許可しているかどうかをチェックします。
 - 多数のデバッグメッセージがあります。(送信元アドレス/宛先アドレスおよびプロトコルを示す)ACL一致メッセージを指定する必要があります。

```
acl advanced 3000
```

```
rule 5 permit icmp source 192.168.10.2 0 destination 192.168.10.1 0
```

```
<H3C> debugging security-policy packet ip acl 3000
```

```
This command is CPU intensive and might affect ongoing services. Are you sure you want to continue? [Y/N]:Y
```

```
<H3C> terminal monitor
```

```
The current terminal is enabled to display logs.
```

```
<H3C> terminal debugging
```

ファイアウォールでメッセージがブロックされているかどうか



The Leader in Digital Solutions

- 通常のデバッグ

```
<H3C>*Aug 31 08:24:11:380 2017 F1020 FILTER/7/PACKET: -Context=1; The packet is permitted. Src-Zone=Trust, Dst-Zone=Local;If-In=GigabitEthernet1/0/5(6), If-Out=InLoopBack0(132); Packet Info:Src-IP=192.168.10.2, Dst-IP=192.168.10.1, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=1, Rule-ID=0.
```

ファイアウォールでメッセージがブロックされているかどうか

- ブロックされたデバッグ

```
<H3C>*Aug 31 8:26:31 AM:988 2017 H3C FILTER/7/PACKET: -Context=1; The packet is denied. Src-Zone=Trust, Dst-Zone=Local;If-In=GigabitEthernet1/0/5(6), If-Out=InLoopBack0(132); Packet Info:Src-IP=192.168.10.2, Dst-IP=192.168.10.1, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=4, Rule-ID=3.
```

- 設定されたセキュリティポリシーが拒否されたファイアウォールでは、拒否されたルールを示す上記の情報が出力されます。

ファイアウォールでメッセージがブロックされているかどうか

- ブロックされたデバッグ

```
<H3C>*Aug 31 8:26:31 AM:988 2017 H3C FILTER/7/PACKET: -Context=1; The packet is denied. Src-Zone=Trust, Dst-Zone=Local;If-In=GigabitEthernet1/0/5(6), If-Out=InLoopBack0(132); Packet Info:Src-IP=192.168.10.2, Dst-IP=192.168.10.1, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), Acl=none, rule-id=none.
```

- セキュリティポリシーが設定されていないファイアウォールでは、上記の情報が出力され、一致するルールがないことが示されます。

ファイアウォールでメッセージがブロックされているかどうか **H3C**

The Leader in Digital Solutions

- ステップ2:aspf/パケット{acl}のデバッグは、ASPFポリシーがメッセージをブロックするかどうかをチェックします。
 - 状況1

```
<H3C>debugging aspf packet
This command is CPU intensive and might affect ongoing services. Are you sure you
want to continue? [Y/N]:y
<H3C>*Aug 31 08:21:38:114 2017 F1020 ASPF/7/PACKET: -Context=1; The packet was
dropped by ASPF for nonexistent zone pair. Src-Zone=-, Dst-Zone=Local;If-
In=GigabitEthernet1/0/5(6), If-Out=InLoopBack0(132); Packet Info:Src-IP=192.168.10.2,
Dst-IP=192.168.10.1, VPN-Instance=none,Src-Port=1533, Dst-Port=2048.
Protocol=ICMP(1).
```

- インターフェイスがセキュリティゾーンに追加されていません。セキュリティゾーンの設定を確認する必要があります。

ファイアウォールでメッセージがブロックされているかどうか **H3C**

The Leader in Digital Solutions

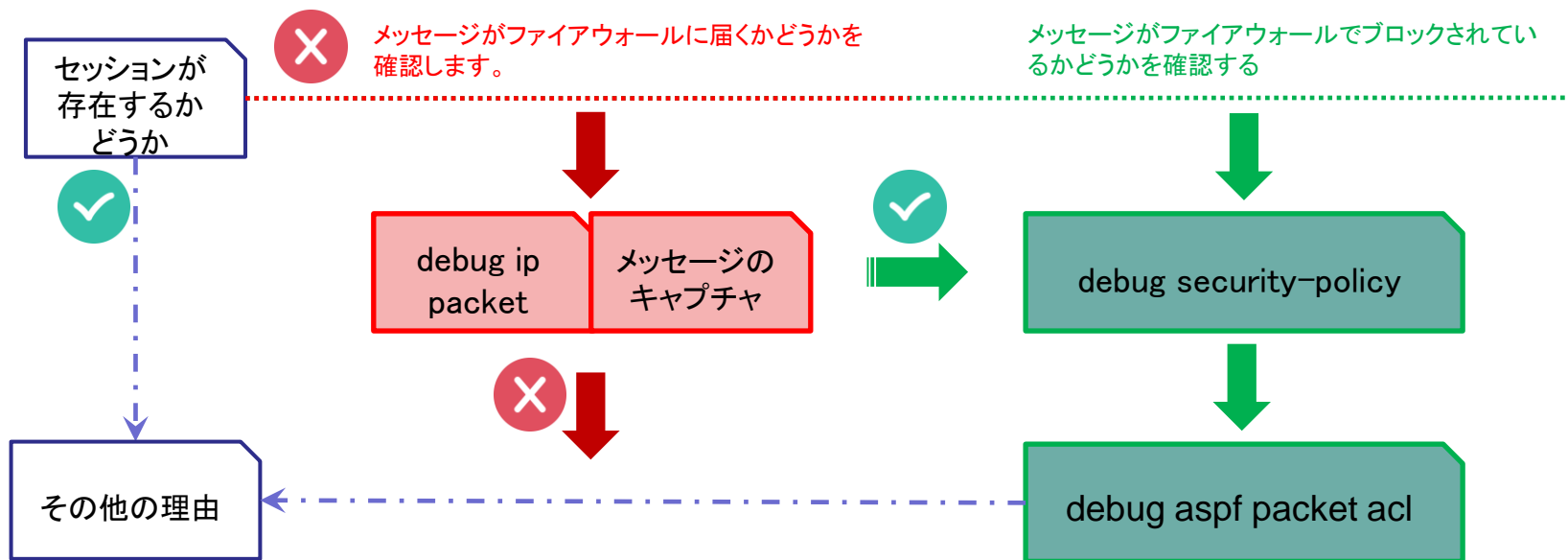
- ステップ2:aspf/パケット[ac]のデバッグは、ASPFポリシーがメッセージをブロックするかどうかをチェックします。

➤ 状況2

```
<H3C>debugging aspf packet
This command is CPU intensive and might affect ongoing services. Are you sure you
want to continue? [Y/N]:y
<H3C>*Aug 31 8:26:31 AM:988 2017 H3C ASPF/7/PACKET: -Context=1; The first packet
was dropped by packet filter or object-policy. Src-Zone=Trust, Dst-Zone=Local;If-
In=GigabitEthernet1/0/5(6), If-Out=InLoopBack0(132); Packet Info:Src-IP=192.168.10.2,
Dst-IP=192.168.10.1, VPN-Instance=none,Src-Port=1535, Dst-Port=2048.
Protocol=ICMP(1).
```

- メッセージはセキュリティポリシーによってブロックされています。適切な許可されたセキュリティポリシーがあるかどうかをチェックしてください。

ポリシー・ブロッキングのトラブルシューティング



NATセッションエントリ

```
<H3C>display session table ipv4 source-ip 60.3.128.1 destination-ip 60.3.128.16 verbose
```

```
Slot 1:
```

```
Initiator:
```

```
Source IP/port: 60.3.128.1/150  
Destination IP/port: 60.3.128.16/2048
```

```
DS-Lite tunnel peer: -
```

```
VPN instance/VLAN ID/Inline ID: -/-/
```

```
Protocol: ICMP(1)
```

```
Inbound interface: GigabitEthernet1/0/2
```

```
Source security zone: Untrust
```

```
Responder:
```

```
Source IP/port: 10.0.1.2/150
```

```
Destination IP/port: 60.3.128.1/0
```

```
DS-Lite tunnel peer: -
```

```
VPN instance/VLAN ID/Inline ID: -/-/
```

```
Protocol: ICMP(1)
```

```
Inbound interface: GigabitEthernet1/0/10
```

```
Source security zone: Trust
```

```
State: ICMP_REPLY
```

```
Application: ICMP
```

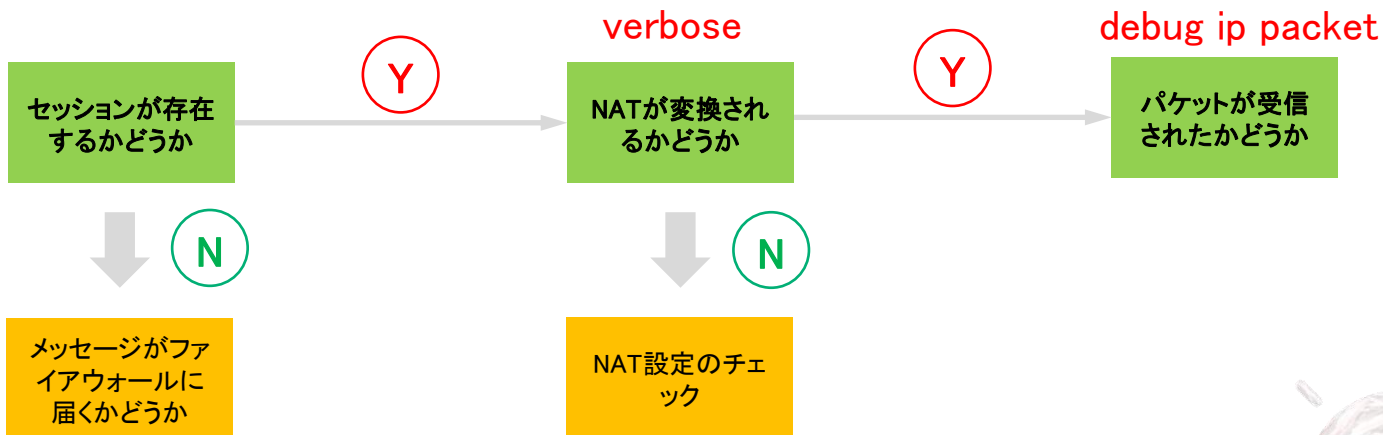
```
Start time: 2019-01-14 17:55:43 TTL: 23s
```

```
Initiator->Responder: 0 packets 0 bytes
```

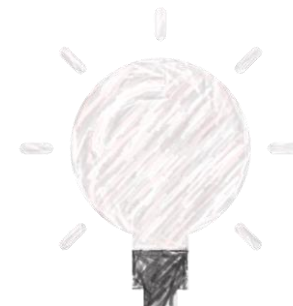
```
Responder->Initiator: 0 packets 0 bytes
```

```
Total sessions found: 1
```

NATブロッキングのトラブルシューティング



debug ip packet
debug security-policy



注

● デバッグに関する注意

- まず、デバイスのデバッグスイッチがオンになっているかどうかをコマンドで確認します。

```
<H3C>display debugging
Security-policy packet ip acl 3000 debugging switch is on
```

- デバッグが完了したら、コマンドラインまたはショートカットキーを使用してデバッグをオンにします。

```
<H3C>undo terminal debugging
The current terminal is disabled to display debugging logs.
<H3C>u t d
The current terminal is disabled to display debugging logs.
```

- ショートカットキーCTR+Cは<ユーザーモード>に戻り、CTR+Oはデバッグメッセージをオフにできます。

注

● デバッグに関するFAQ

- ・ デバッグIPパケットにメッセージがない場合は、メッセージがファイアウォールに到達しなかったことを示します。
- ・ vpn-instanceがある場合、それはACLに追加される

デバッグメッセージが表示されない場合



- ・ ACLを指定しようとする
- ・ セキュリティポリシーログの表示をオフにするinfo-center source FILTER monitor deny

デバッグメッセージが多すぎる場合





The Leader in Digital Solutions

www.h3c.com