Hillstone Networks

StoneOS Cookbook

Version 5.5R8 V9

Contact Information:

US Headquarters:

Hillstone Networks

292 Gibraltar Drive, Suite 105

Sunnyvale, CA 94089

Phone: 1-408 508 6750

https://www.hillstonenet.com/about-us/contact/

About this Guide:

This guide gives you configuration instructions of Hillstone NetworksStoneOS user scenarios.

For more information, refer to the documentation site: **https://docs.hillstonenet.com**.

To provide feedback on the documentation, please write to us at:

TechDocs@hillstonenet.com

Hillstone Networks

TWNO: TW-CBK-UNI-5.5R8-EN-V9-10/28/2020

Release Date: 10/28/2020

Contents

Overview

StoneOS Cookbook provides configuration examples for you to user Hillstone network security products. This books covers basic getting-started cases, firewall functions, and advanced user scenarios. All configuration uses graphic user interface (GUI), or also known as web user interface (WebUI), not command line interface.

Each recipe consists of two parts: scenario settings and configuration steps. Topology and screenshot are used to assist you in understanding the key information of the case.

StoneOS Cookbook is very helpful in understanding operational logic, and improving efficiency.

StoneOS Cookbook organizes its recipes into the following chapters:

This book is updated on requirement, not periodically.

The current version you are using is based on StoneOS 5.5R5.

How to Use Cookbook

Before you read the book, there are a few tips you need to know.

Target audience

Cookbook is written with new users in mind. However, if you use this book, you still are required to know how to use WebUI, connect cables and log in the system. Such information can be found in Getting Started Guide.

StoneOS Versions

This cookbook you are reading now is based on StoneOS 5.5.

With system updates, the user interface is subject to change, and WebUI layout may vary depending on hardware platforms. This cookbook may not comply with every detail on WebUI, please check your web pages for difference when you use this book.

Reading Sequence

When you open the book, it is better to read it in the sequence below:

1. Go to Table of Contents, and locate the feature you need;
2. Jump to that feature, read the scenario description and topology;
3. Go through step key points (marked as "Step1", "Step2") to understand configuration logic;
4. Read the left text and right screen shots to get the details.
5. Configure your device accordingly, but substitute with your own IP address or names.

Text vs. Screenshots

The step details are explained by combing description text and screenshots. The text on the left gives configuration details, highlights and notes; the sceenshot on the right is the exact screen capture of this step.

Getting Started and Other Chapters

In this cookbook, the chapter "Getting Started" is the prerequisite for other chapters. Other chapters deem that the protected network has already finished its basic networking settings mentioned in the Getting Started chapter. In other chapters, steps like NAT, default routes and DNS are not included. So, when you reference to user scenarios in chapters other than Getting Started, you should ensure that your protected network has already been basically established.

Interface, Name, Topology

This book explains function configuration by writing scenarios (also called "cases" or "recipes"). Interface addresses, object names, and topologies are the real laboratory settings. When you configure your own network, substitute the names and addresses with your real names and addresses.

Clicking OK or Apply

Generally, when you finish filling or editing an option, you must click **OK**, **Apply**, or **Confirm** button to make the setting take effect. This kind of operation is universal. This book will not write specifically about this operation otherwise else is needed.

Getting Started

Recipes in Getting Started chapter introduce basic networking configurations.

This chapter includes the following recipes:

Upgrading Firmware to Higher Version

This example introduces how to use WebUI and CLI to upgrade firmware to a higher version.

As an exit of the company's network, security device provides protections and services. Now, admin need upgrade firmware to optimize system's performance and get new functions.

Preparation

Before upgrading, we recommend you:

- See the system software version by using WebUI or CLI(`show version`) to get a suitable upgrading instructions.
- See the release notes of the target version to get a platform upgrading instructions.
- Get upgrade file of your target version from Hillstone.
- Do not upgrade at peak times, because you need to reboot device to make new version effective.
- Do not downgrade, because system configuration may be lost.
- Upgrade from CLI if your device's storage is low, and remember to remove the former firmware version before you upgrade.
- Make sure you have backed up the configuration file before upgrading.

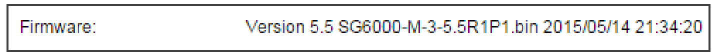
Contact us (Service Line:1-800-889-9860) first when you are in the following situations:

- Make sure whether license is out of date. If it expires, you only can upgrade system to the version whose release date is before the license expired date. If it doesn't expire, upgrading can be continued. Contact us for the release date.
- Do not cross upgrade. For example, to upgrade the versions 4.0 to 5.0, Hillstone recommends you to first upgrade to version 4.5, and then upgrade to 5.0. Contact us for cross version upgrade.
- Contact us for upgrading information if you are in HA environment.

Method 1: Upgrading from WebUI

Step 1: Logging in via WebUI with admin accout and viewing current system information.

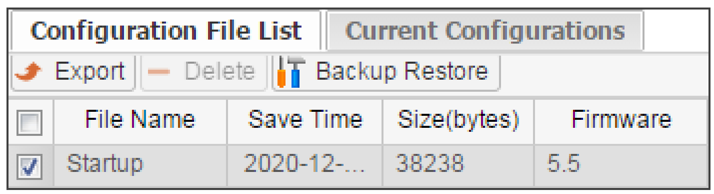
Select **System > System Information** to view the current version is 5.5R1P1.



Step 2: Exporting configuration file as a backup.

Select **System > Configuration File Management**.

In the Configuration File List tab, select **Startup** check box and click **Export**. The configuration file will be exported to your local PC.

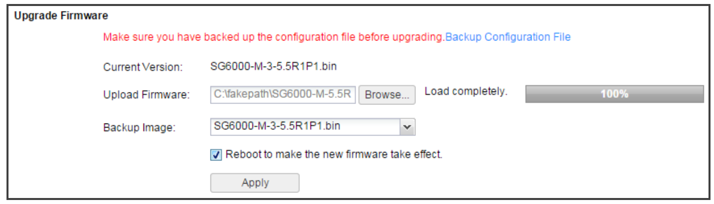


Step 3: Uploading upgrade file and rebooting system. Before uploading, make sure your upgrade file is suitable for your platform.

Select **System > Upgrade Management**.

Step 3: Uploading upgrade file and rebooting system. Before uploading, make sure your upgrade file is suitable for your platform.

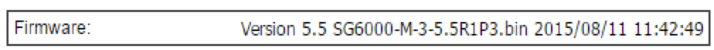
1. In the Upgrade Firmware tab, click Browse button and choose the upgrade file "SG6000-M-3-5.5R1P3.bin" in your local PC.



2. Select **Reboot to make the new firmware take effect** check box and click **Apply**. Do not select **Reboot to make the new firmware take effect** check box at traffic-peak time. Hillstone suggests you to manually reboot when you need.

Step 4: Verifying the upgrade results.

Log in via WebUI again when system finished rebooting.



1. Select **System > System Information**.

2. In the firmware part, you can see the current version is 5.5R1P3. Upgrade succeeded.

Method 2: Upgrading from CLI

Step 1: Logging in system via Telnet, and viewing the current version.

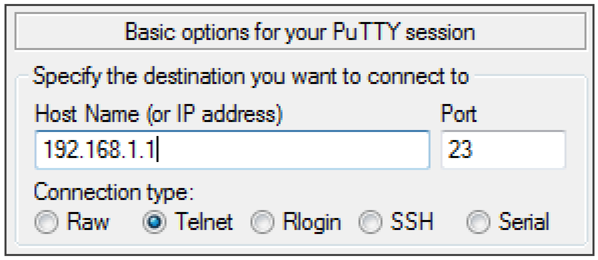
Take an example of using PuTTY.

1. Open PuTTY, and enter the followings:

   Host Name: 192.168.1.1 (manage IP of your device)

   Connetion Type: Telnet

2. Click **Open**.



Type the username and password of admin. Log in successfully.

```
login: hillstone
password:
SG-6000#
```

Type **show version** and knock the Enter key. It will show you the current system version is 5.5R1P1.

```
SG-6000# show version
Hillstone Networks StoneOS software, Version 5.5
Copyright (c) 2009-2015 by Hillstone Networks

Product name: SG-6000-E2800 S/N: 2508311140001228 Assembly number: B045
Boot file is SG6000-M-3-5.5R1P1.bin from flash
Built by buildmaster8 2015/05/14 21:34:20
```

Step 2: Upgrading your device. We upgrade with USB port in this example. Please put your upgrade file in your U-Disk, and then put it into the USB port of security device.

Type **import image from usb0 SG6000-M-3-5.5R1P3.bin** and knock the Enter key.

```
SG-6000# import image from usb0 SG6000-M-3-5.5R1P3.bin
Verified OK

SG6000-M-3-5.5R1P3.bin exists, overwrite it? [y]/n: y
Saving ............................................
Checking saved firmware ............................................ OK

Set SG6000-M-3-5.5R1P3.bin as active boot image
```

Step 2: Upgrading your device. We upgrade with USB port in this example. Please put your upgrade file in your U-Disk, and then put it into the USB port of security device.

1. Type **reboot** and knock the Enter key.
2. System prompts that "System reboot， are you sure?". Type **y** to reboot.
3. Choose a configuration file. Type **a** after "Please choose one".

```
SG-6000# reboot
System reboot, are you sure? [y]/n: y
3 configuration in system, please choose one to be loaded.
======================================================================
         Name      Version Save Time           Size (bytes)
----------------------------------------------------------------------
    [a]: Startup   5.5     2020-11-24 10:08:15 37829
    [b]: Backup 1  5.5     2015-06-18 12:14:08 35362
    [c]: Backup 0  5.5     2015-03-16 18:07:28 9327
======================================================================
Press enter to use system current setting
Please choose one: a
```

Step 3: Verifying the upgrade results.

Log in via Telnet again when system finished rebooting.

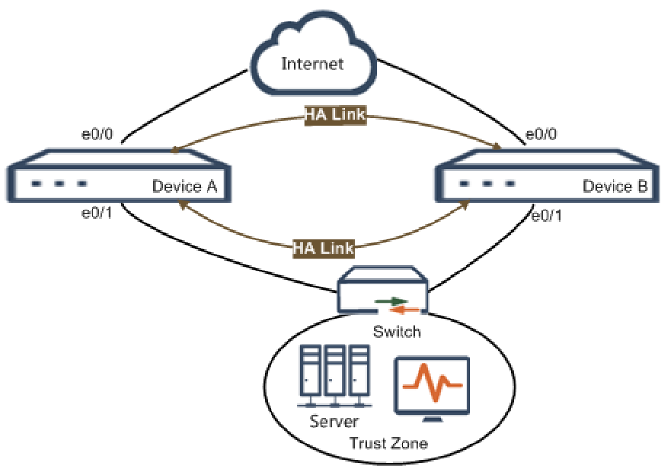
Type **show version** and knock the Enter key. It will show you the current system version is 5.5R1P3.

```
login: hillstone
password:
SG-6000# show version
Hillstone Networks StoneOS software, Version 5.5
Copyright (c) 2009-2015 by Hillstone Networks

Product name: SG-6000-E2800 S/N: 2508311140001228 Assembly number: B045
Boot file is SG6000-M-3-5.5R1P3.bin from flash
Built by buildmaster8 2015/08/11 11:42:49
```

Upgrading Firmware to Higher Version in HA mode

This example introduces how to upgrade the firmware of the device in the HA Active-Passive mode.

The topology gives a typical user scenario for HA. In the designed scenario, one (Device A)of the HA devices will be working under the active mode, while the other (Device B) is under the passive mode. The two devices use heart-beat cables to maintain communication between devices.



Preparation

Before upgrading, prepare the following first:

1. Obtained the system software version by WebUI or CLI(`show version`).

2. Obtained upgrade file of the target version from Hillstone.

3. Obtained the current configurations of the two devices by WebUI or CLI(`show configuration`), and back up the current configurations.

Note: To switch over traffic, you are recommended to upgrade the devices in HA mode through the CLI.

Upgrade Steps

Step 1: Make the backup device (Device B) go offline.

Remove the service cable and HA heartbeat cable from the backup device (Device B) to make the backup device go offline.

Note: Please remove the service cable before removing the HA heartbeat cable in case of operation errors.

Step 2: Upgrade the backup device (Device B) and restart the device.

The detailed steps for device upgrade, see "Upgrading Firmware to Higher Version" on Page 5.

Step 3: Check whether the current configurations of the backup device (Device B) is consistent with the saved configurations.

Device B

In any mode, use the following command:

show configuration

```
SG-6000(B)(config)# show configuration

Building configuration..
Running configuration:
# PREVIOUS CONFIGERATION START
# END OF PREVIOUS CONFIGERATION

!
Version 5.5R7

ip vrouter "twin-mode-vr"
exit
ip vrouter "trust-vr"
exit
ha group 0
exit
vswitch "vswitch1"
exit
zone "mgt"
exit
zone "trust"
exit
zone "untrust"
exit
zone "dmz"
exit
```

Step 4: Reconnect the service cable and HA heartbeat cable on the backup device (Device B), and transfer all service traffic to the backup device (Device B).

Reconnect the service cable and HA heartbeat cable on the backup device (Device B).

To transfer all service traffic to the backup device (Device B), in any mode, use the following command:

exec ha master switch-over

```
SG-6000(M)# exec ha master switch-over
```

Step 5: Make the master device (Device A) go offline.

Remove the service cable and HA heartbeat cable from the master device (Device A) to make the master device go offline.

Note: Please remove the service cable before removing the HA heartbeat cable in case of operation errors.

Step 6: Upgrade the master device (Device A) and restart the device.

The detailed steps for device upgrade, see "Upgrading Firmware to Higher Version" on Page 5.

Step 7: Check whether the current configurations of the master device (Device A) is consistent with the saved configurations.

Device A

In any mode, use the following command:

show configuration

```
SG-6000(B)(config)# show configuration

Building configuration..
Running configuration:
# PREVIOUS CONFIGERATION START
# END OF PREVIOUS CONFIGERATION

!
Version 5.5R7

ip vrouter "twin-mode-vr"
exit
ip vrouter "trust-vr"
exit
ha group 0
exit
vswitch "vswitch1"
exit
zone "mgt"
exit
zone "trust"
exit
zone "untrust"
exit
zone "dmz"
exit
```

Step 8: Reconnect the service cable and HA heartbeat cable on the master device (Device A), and restore all service traffic to the master device (Device A).

Reconnect the service cable and HA heartbeat cable on the master device (Device A).

To restore all service traffic to the master device (Device A), in any mode, use the following command:

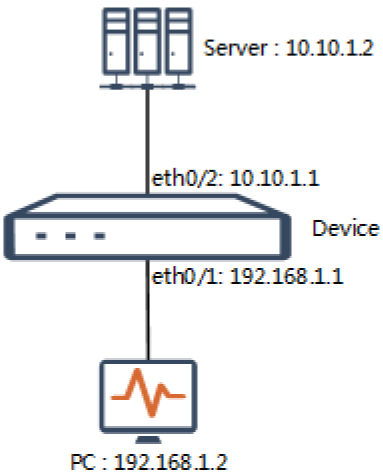
exec ha master switch-over

```
SG-6000(M)# exec ha master switch-over
```

Using Security Policy to Allow Access to Another Zone

This example introduces how to use security policies to control communication between two zones.

The scenario sets up a requirement that the private network users are not allowed to access Internet during work time. As the topology described, polices and schedules work together to allow internal users to access to server in another zone during work hour (9 a.m. to 17 p.m.). When it's not working time, the server cannot be accessed.

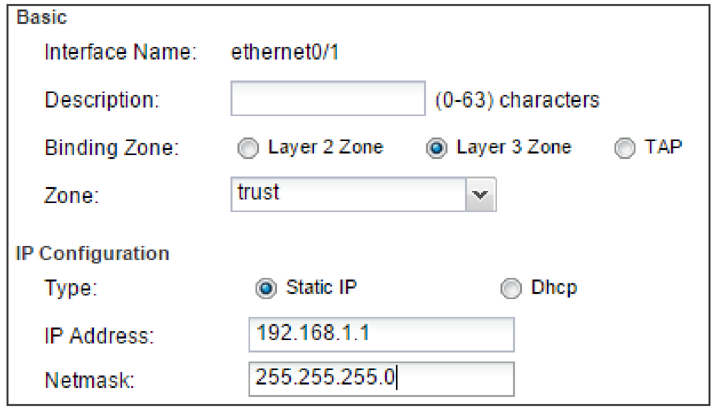


Configuration Steps

Step 1: Configuring Interface

1. Configuring the interface connected to private network

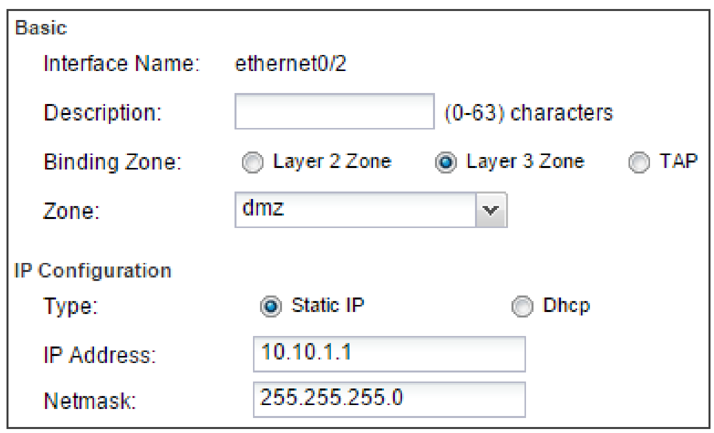
Select **Network > Interface**, double click ethernet0/1.



- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0

2. Configuring the interface connected to Server

Select **Network > Interface**, double click ethernet0/2.

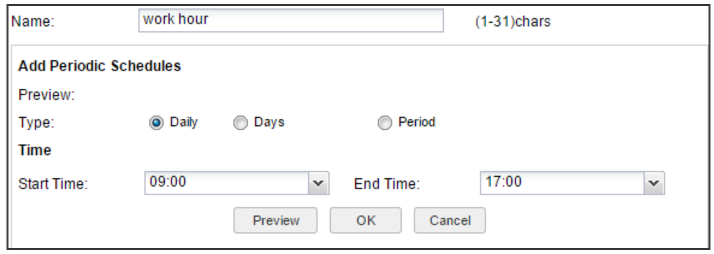


- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0

Step 2: Configuring Schedule

Select **Object > Schedule**, and click **New**.

In the prompt, click **Add**.



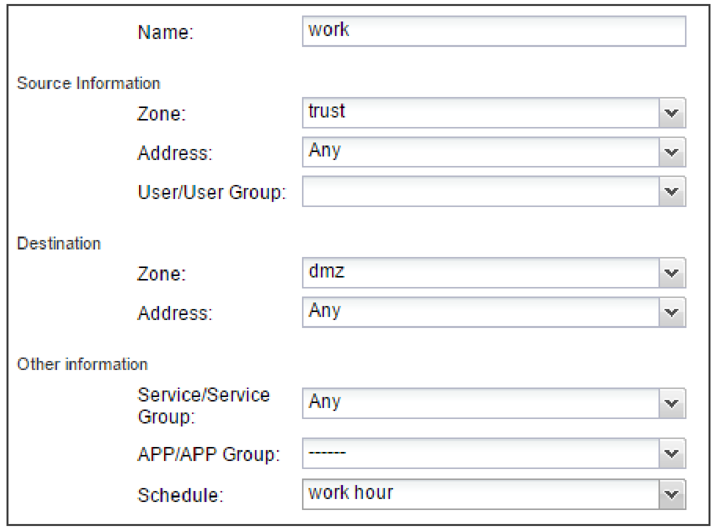
- Name: work hour
- Type: Daily
- Start Time: 09:00
- End Time: 17:00

Click **OK** to add it.

Step 3: Configuring Policies

1. Configuring a policy to allow internal users access to server during work hour

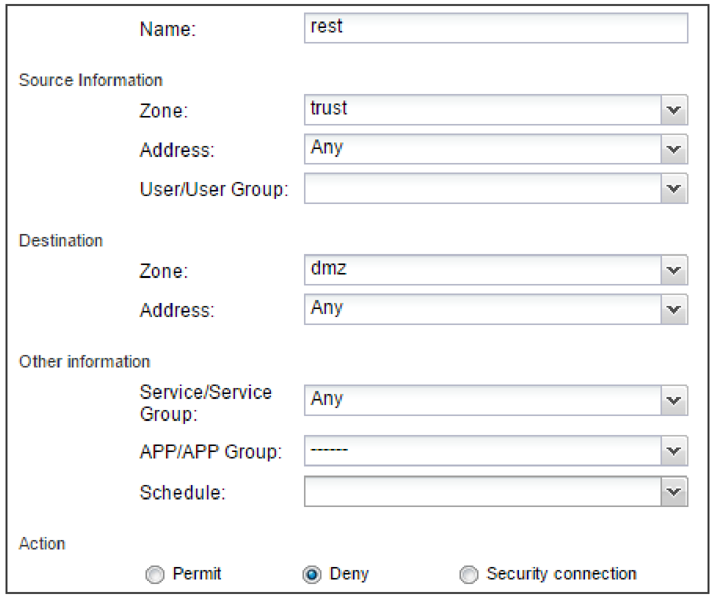
Select **Policy > Security Policy**, and click **Add**.



- Name: work
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other Information
  - Schedule: work hour
  - Action: Permit

Step 3: Configuring Policies

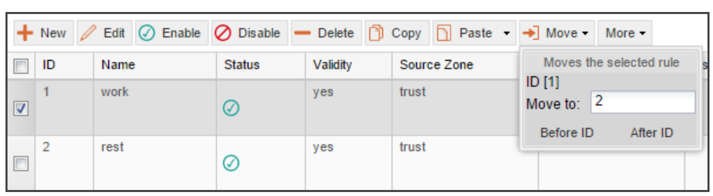
2. Configuring a policy that internal users cannot visit server



Select **Policy > Security Policy**, and click **Add**.

- Name: rest
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other Information
  - Schedule: work hour
  - Action: Deny

3. Adjusting priority of policies



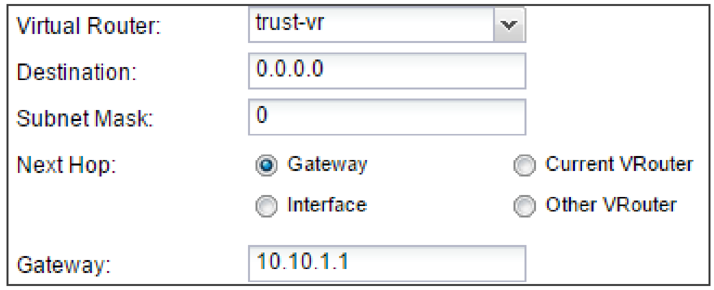
Select **Policy > Security Policy**, and select the "work" policy. Select "work" policy, and click **Move**, and enter "rest" policy's ID, then click **Before ID**.

Note: The priority of a policy is only determined by its position in the list.

Step 4: Configuring a default route

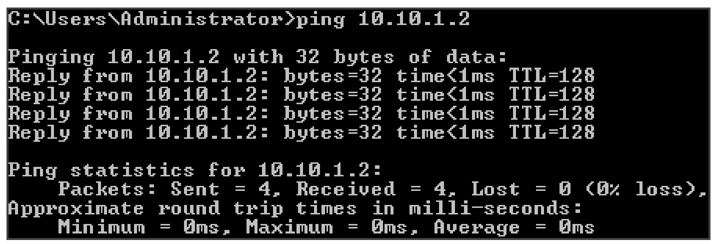
Select **Network > Routing > Destination Route**, and select **New**.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: Gateway
- Gateway: 10.10.1.1

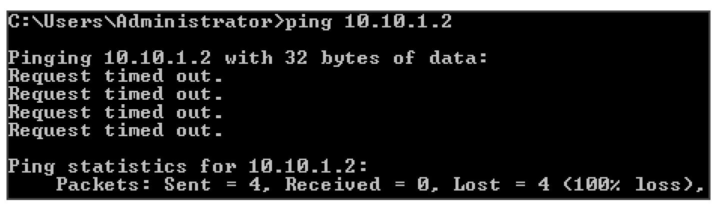


Step 5: Results

After configuration, the internal PC can ping the server address successfully during 9:00 to 17:00.



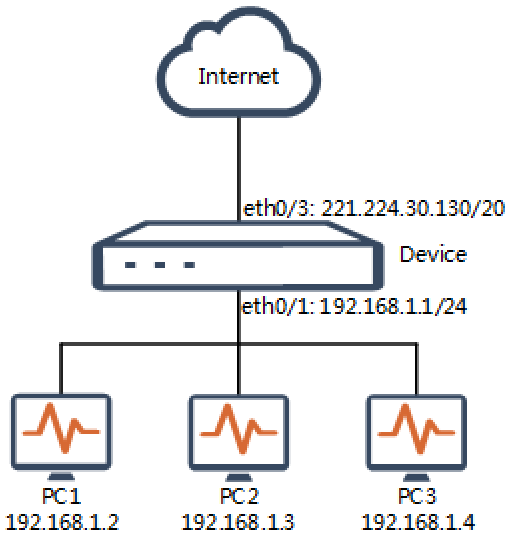
When internal PC pings the server during offwork time, it fails.



Allowing Private Network to Access Internet Using SNAT

SNAT rule is used to allow users in private network to access Internet. An SNAT rule will translate the internal IP addresses to a public IP address, so that internal users can have access to public network via the public interface.

As shown in the topology, via SNAT, internal PCs use the eth0/3 (221.224.30.130/20) to visit Internet.



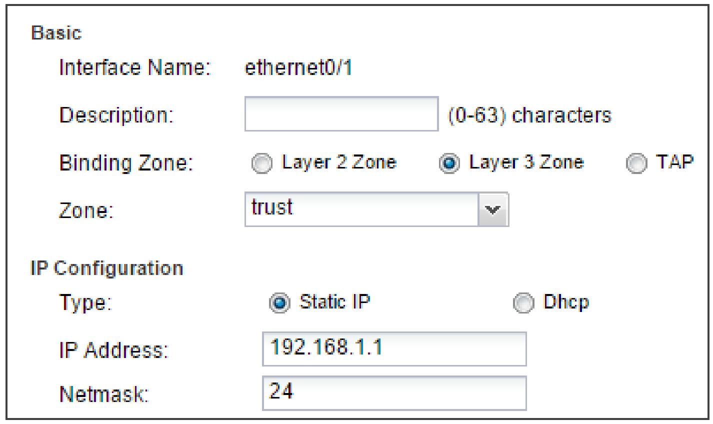
Configuration Steps

Step 1: Configuring Interface

1. Configuring the interface connected to private network

Select **Network** > **Interface**, and double click ethernet0/1.

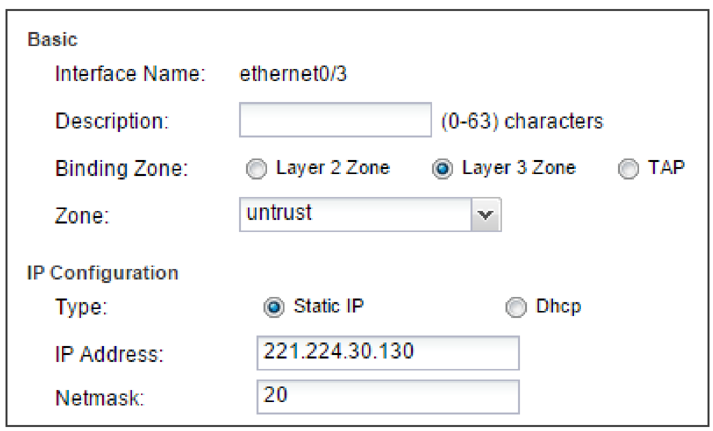
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 24



2. Configuring the interface connected to Internet

Select **Network** > **Interface**, and double click ethernet0/3.

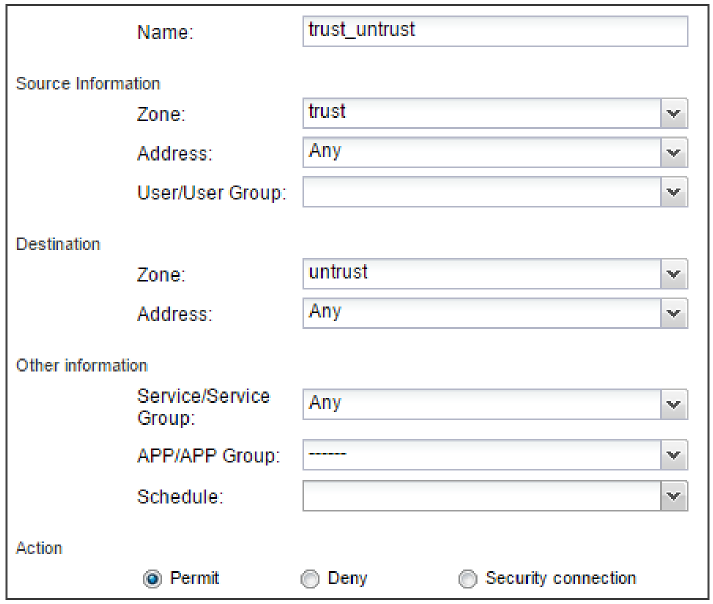
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 221.224.30.130
- Netmask: 20



Step 2: Configuring security policy

Configuring a security policy to allow private network to Internet

Select **Policy > Security Policy**, and click **Add**.

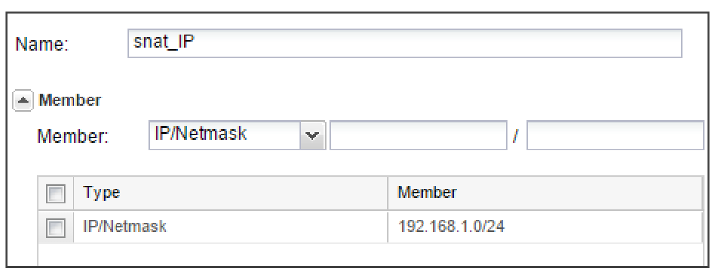


- Name: trust_untrust
- Source Information
  - Zone: trust
  - Address: Any
- Destination
  - Zone: untrust
  - Address: Any
- Other Information
  - Action: Permit

Step 3: Configuring Address book

Configuring an address range for private network users

Select **Object > Address Entry**, and click **New**.

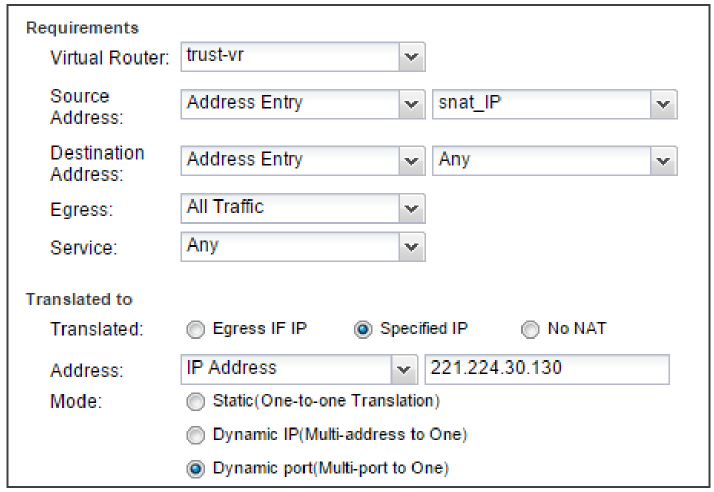


- Name: snat_IP
- Member: add "192.168.1.0/24"

Step 4: Configuring SNAT rule

Select **Policy > NAT > SNAT**, and click **New**.

- Requirement:
  - Source Address: Address Entry, snat_IP (Note: enter the server's internal IP address.)
- Translated to:
  - Specified IP: "IP Address", "221.224.30.130"
    （Note: enter public IP address here)
  - Mode: Dynamic Port (multi-port to one)

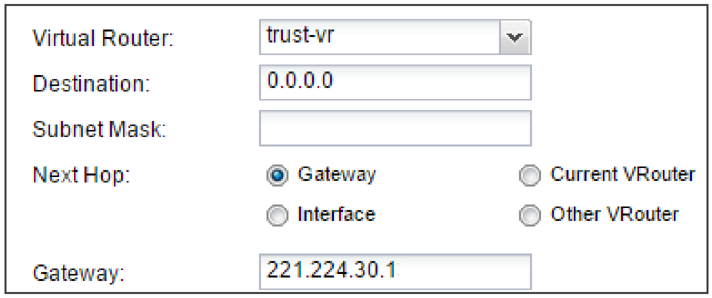


(Optional) Under Advanced tab, select NAT log check box to enable NAT logging (for checking results).

Step 5: Configuring default route

Select **Network > Routing > Destination Route**, and click **New**.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: Gateway
- Gateway: 221.224.30.1



Step 6: Results

After configuration, PCs in private network can ping 221.224.30.131 successfully.

```
C:\Users\Administrator>ping 221.224.30.131

Pinging 221.224.30.131 with 32 bytes of data:
Reply from 221.224.30.131: bytes=32 time=182ms TTL=127
Reply from 221.224.30.131: bytes=32 time=1ms TTL=127
Reply from 221.224.30.131: bytes=32 time=1ms TTL=127
Reply from 221.224.30.131: bytes=32 time=1ms TTL=127

Ping statistics for 221.224.30.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 182ms, Average = 46ms
```

Step 6: Check if DNAT rule works

Make sure NAT logging is enabled in monitor module (Select **Monitor > Log > Log Monitor**, under NAT tab, select **Enable**.)

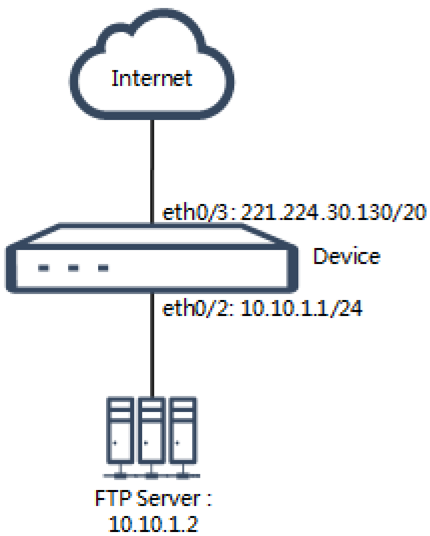
Go to **Monitor > Log > NAT**, you will be able to see the destination IP 192.168.1.2 has been translated to internal IP 221.224.30.130.

Time	NAT type	ID	Source IP	AAA: user @ host	Source port	Destination IP	Destination port	Translated IP	Translated port	Protocol
2015-02-12 13:34:40	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1048	ICMP
2015-02-12 13:34:39	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1047	ICMP
2015-02-12 13:34:38	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1046	ICMP
2015-02-12 13:34:38	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1045	ICMP

Allowing Internet to Visit a Private Server Using DNAT

Destination network address translation (DNAT) is normally used to allow Internet users visit an internal server by providing Internet IP address for internal server.

As shown in the topology, the FTP server hides its internal IP address using DNAT rule. DNAT rule will give the server an Internet IP address for FTP users to access. In this way, the server can be accessed from Internet.



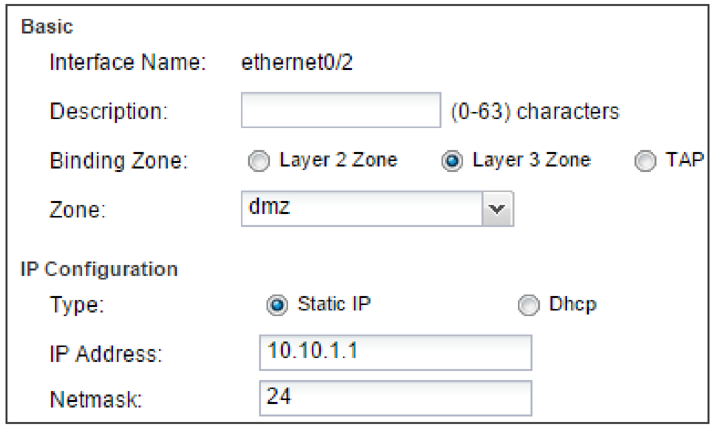
Configuration Steps

Step 1: Configuring interfaces

1. Configuring the interface connected to the server

Select **Network > Interface**, and double click ethernet0/2.

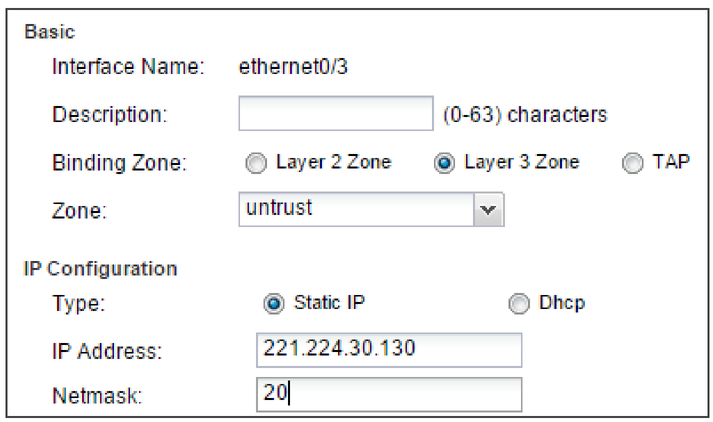
- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 24



2. Configuring the interface connected to Internet

Select Network > Interface, and click ethernet0/3.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 221.224.30.130
- Netmask: 20

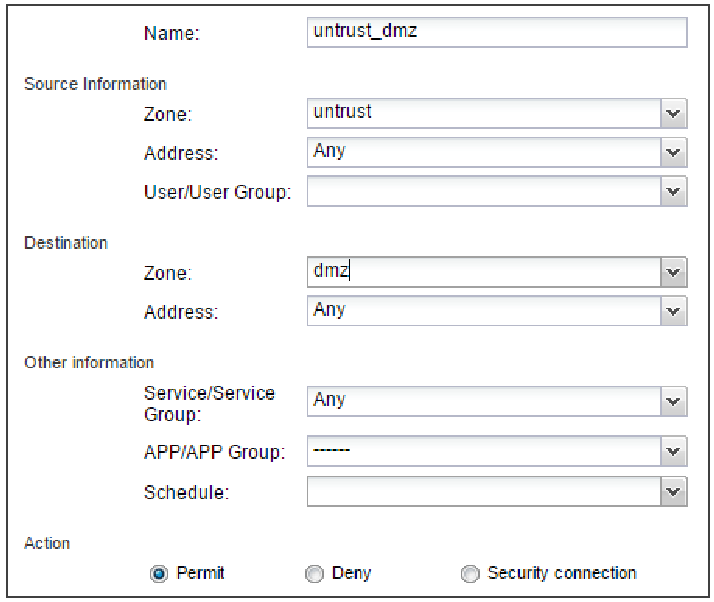


Step 2: Configuring security policies

Configuring a policy allowing Internet to visit internal network

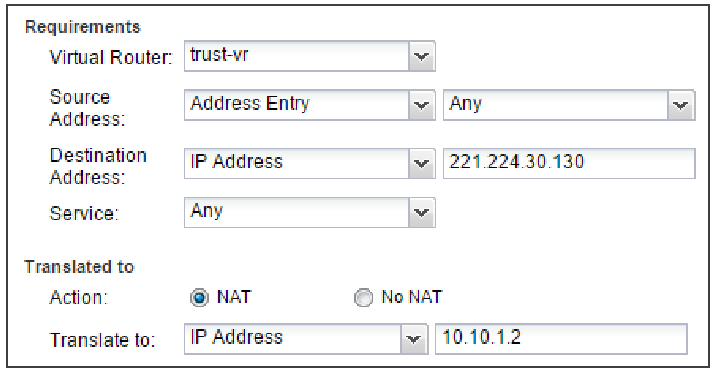
Select Policy > Security Policy, and click Add.

- Name: untrust_dmz
- Source Information
  - Zone: untrust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other Information
  - Action: Permit



Step 3: Configuring DNAT rule

Select **Policy > NAT > DNAT**, and click **New > Advanced Configuration**.

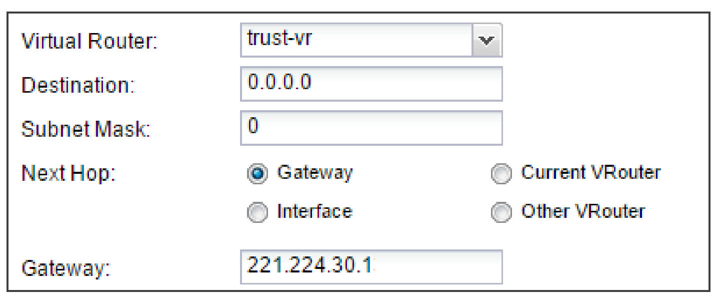


- Requirement:
  - Destination Address: IP Address, 221.224.30.130 (Note: enter public IP address here.)
- Translated to:
  - Translated to: "IP Address", "10.10.1.2"
    （Note: enter the server's internal IP address)

(Optional) Under Advanced tab, select NAT log check box to enable NAT logging (for checking results.)

Step 4: Configuring default route

Select **Network > Routing > Destination Route**, and click **New**.



- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: Gateway
- Gateway: 221.224.30.1

Step 5: Results

After configuration, use a PC in Internet to ping the server's public address 221.224.30.130.

```
C:\Users\Administrator>ping 221.224.30.130

Pinging 221.224.30.130 with 32 bytes of data:
Reply from 221.224.30.130: bytes=32 time<1ms TTL=128
Reply from 221.224.30.130: bytes=32 time<1ms TTL=128
Reply from 221.224.30.130: bytes=32 time<1ms TTL=128
Reply from 221.224.30.130: bytes=32 time<1ms TTL=128

Ping statistics for 221.224.30.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 6: Check if DNAT rule works

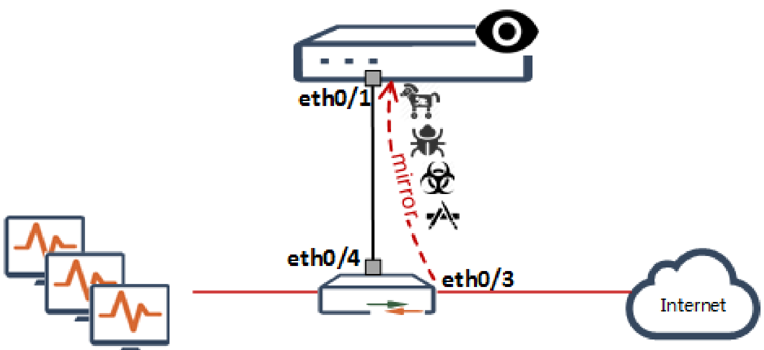
Make sure NAT logging is enabled in monitor module (Select **Monitor > Log > Log Monitor**, under NAT tab, select **Enable**.)

Go to **Monitor > Log > NAT**, you will be able to see the destination IP 221.224.30.130 has been translated to internal IP 10.10.1.2.

Time	NAT type	ID	Source IP	AAA: user @ host	Source port	Destination IP	Destination port	Translated IP	Translated port	Protocol
2015-02-12 14:28:00	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:59	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:58	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:57	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:56	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP

Deploying Tap Mode to Monitor Network Traffic

Inline mode places a device directly in the network path, while in tap mode, the device only connects to a mirrored interface of core network. Tap device monitors or sniffs the packet information mirrored from core network gateway. Tap products tend to be resilient and transparent so as to minimize or eliminate the effect they can have on production traffic. If you just want a sensor to monitor, analyze and log network traffic, not data forwarding, it is best to choose tap mode.



In this example, a Hillstone device (T-Series Intelligent Next Generation Firewall recommended) is a network tap. Its tap interface eth0/1 directly connects to mirror interface of inline network gateway. Hillstone T-Series threat detection features to analyze mirrored data packets in search for network threats.

We present 4 threat detecting functions in this example. All the functions require respective licenses installed before they take effect.

- **Intrusion Prevention System (IPS)**: Requires Threat Prevention (TP) or IPS license installed.
- **Application Identification**: Requires APP DB license installed. This license is issued with platform license for free. No need to purchase APP DB license individually.
- **Advanced Threat Detection (ATD)**: Requires StoneShield license installed.
- **Abnormal Behavior Detection (ABD)**: Requires StoneShield license installed.

Preparation

As shown in the topology above, you need use a RJ-45 cable to connect the mirror port eth0/4 and the tap interface eth0/1.

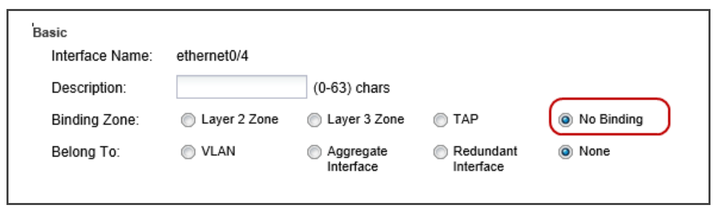
Configure port mirroring on gateway of core network. We take Hillstone gateway as example.

Configuring port mirroring

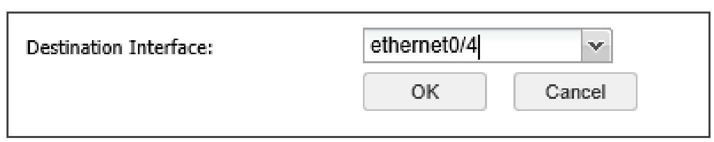
1. Select **Network > Interface**, and double-click **ethernet0/3**.

2. In the pop-up, click the **Properties** tab, under Mirror part, select the checkbox to enable traffic mirroring.

3. Return to interface list, make sure that the mirror port ethernet0/4 is not bound to any zone.



4. Select **Network > Port Mirroring**, select **ethernet0/4** from drop-down menu, and click **OK**.



Configuring Tap Mode and Threat Detection

Configure all the following settings on tap device.

Step 1: Creating a tap mode

1. Select **Network > Zone**, click **New**.

Step 1: Creating a tap mode

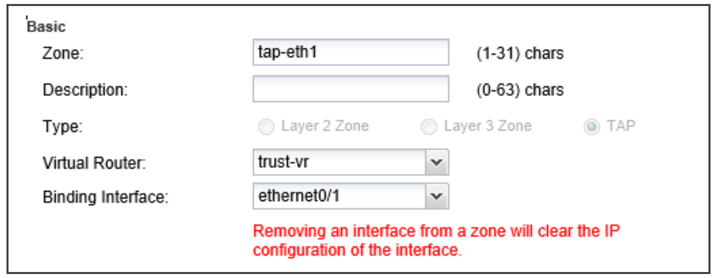
2. In the Zone Configuration dialog, configure the following:

   Zone: tap-eth1

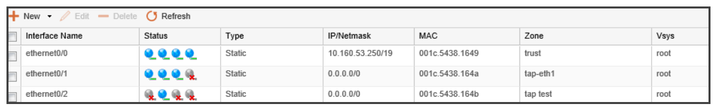
   Type: TAP

   Virtual Router: trust-vr

   Binding Interface: ethernet0/1



3. Return to **Network > Interface**, in the interface list, check that eth0/1 is in the "tap-eth1" zone.

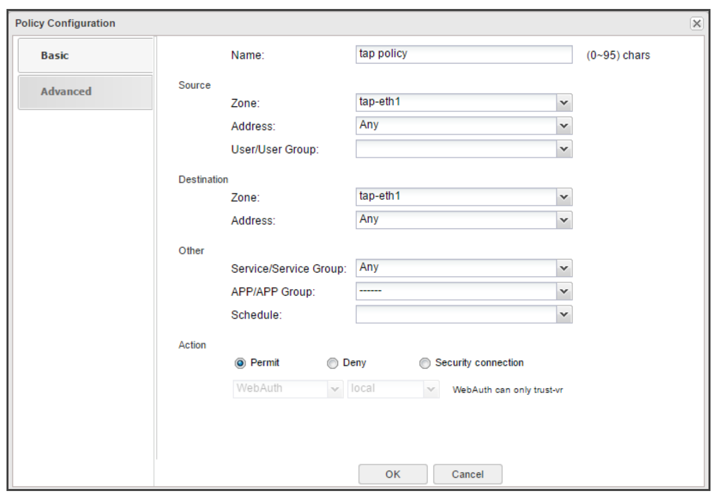


Step 2: Creating a Policy

Creating a "permit" policy on the tap device so that it can establish sessions within itself.

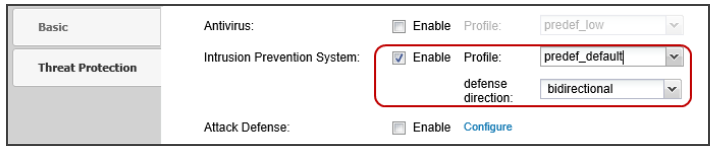
1. Select **Policy > Security Policy**, click **New**.

2. In the **Policy Configuration** dialog, make a "permit" rule from and to the same tap zone.



Step 3: Enabling IPS and viewing IPS attacks

Enabling IPS:



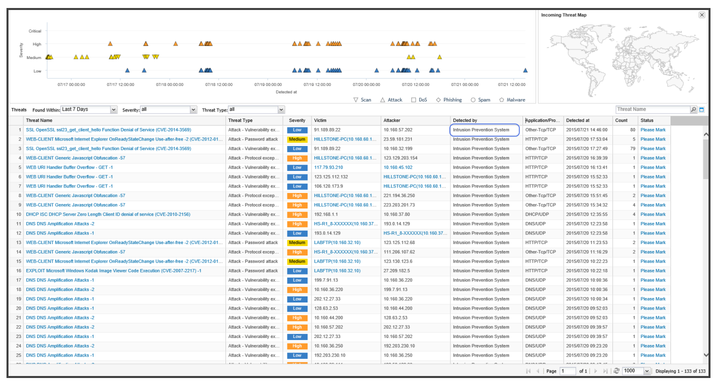
1. Select **Network > Zone**, double-click **tap-eth1**.

2. Under the **Threat Prevention** tab, select **Enable** check-box on the right of **Intrusion Prevention System**.

   Profile: predef_default

   Defense Direction: bidirectional

Checking detection results:



1. Select **iCenter > Threat**.

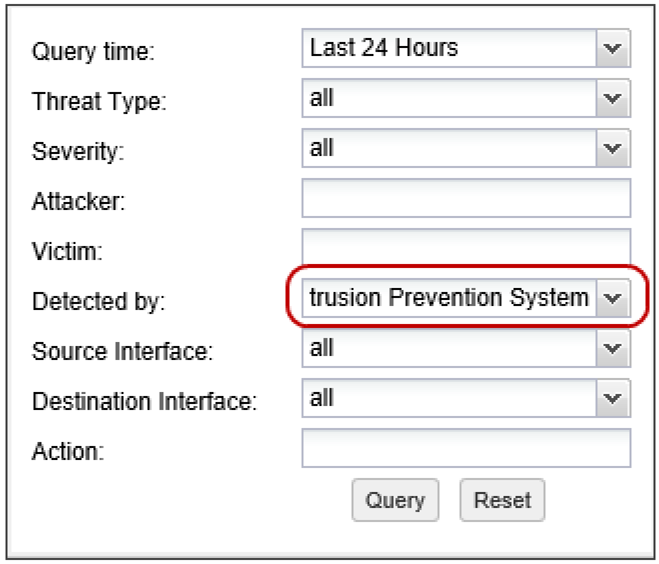
2. In the list, , items marked as "Intrusion Prevention System" under the **Detected by** column are IPS attacks detected by tap device.

Step 3: Enabling IPS and viewing IPS attacks

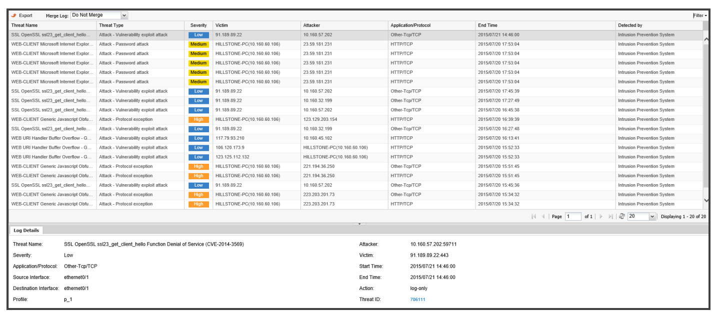
Viewing IPS logs:

1. Select **Monitor > Log > Threat**, click **Filter** on the top right corner.

- **Detected by:** Intrusion Prevention System



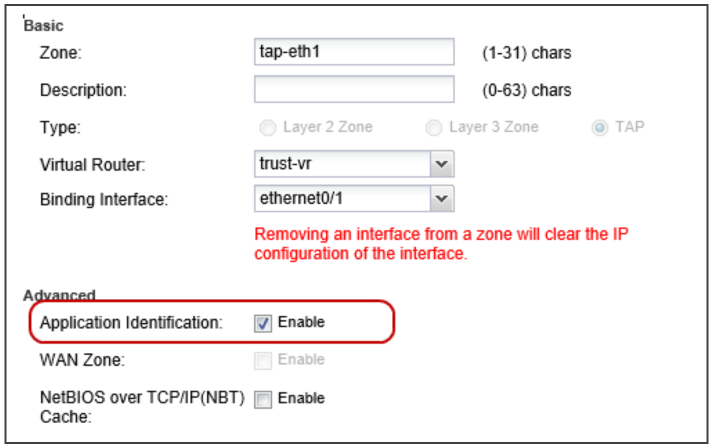
2. Click **Query**, and the page will show IPS logs.



Step 4: Enabling Application Identification and viewing APP usage statistics

Enabling APP Identification:

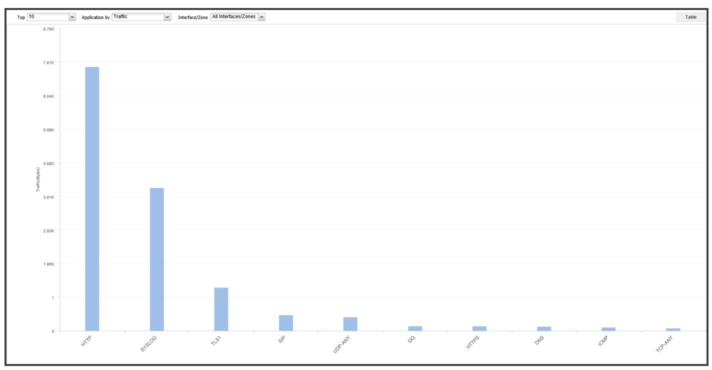
1. Select **Network > Zone**, double-click the **tap-eth1** zone.
2. Under the **Basic** tab, select the **Enable** check-box after Application Identification.



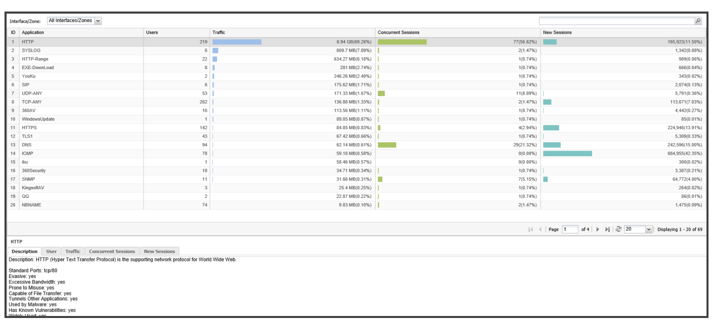
Viewing App monitor results:

Select **Monitor > Application**.

- **Summary**: Application usage statistics by user, traffic, new session or concurrent session.

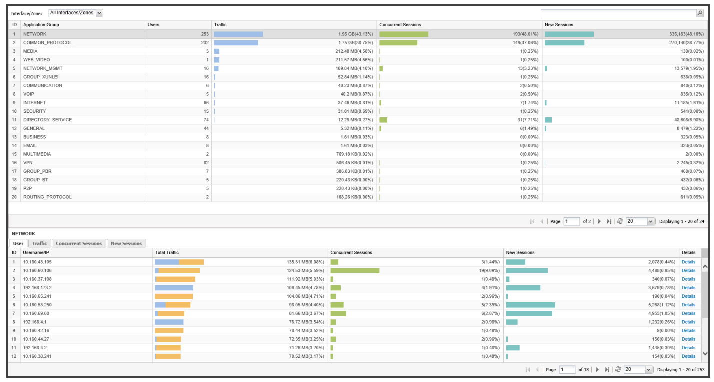


- **Application Details**: Details of every application.



Step 4: Enabling Application Identification and viewing APP usage statistics

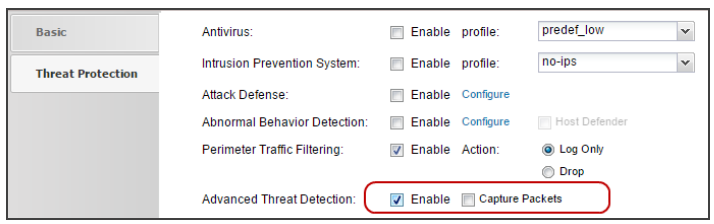
- **Group Details**: Application group usage details.



Step 5: Enabling Advanced Threat Detection (ATD) and viewing ATD attacks

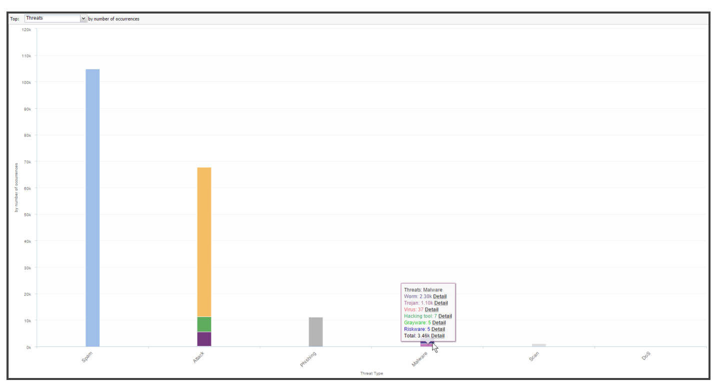
Enabling ATD:

1. Select **Network > Zone**, double-click the **tap-eth1** zone.
2. Under the **Threat Prevention** tab, select the **Enable** check-box after **Advance Threat Detection**.



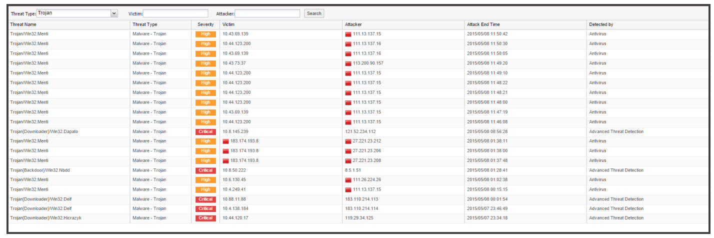
Viewing ATD monitor result:

1. Select **Monitor > Threat > Summary**, hover your cursor over **Malware** bar to show a balloon of malware attacks.



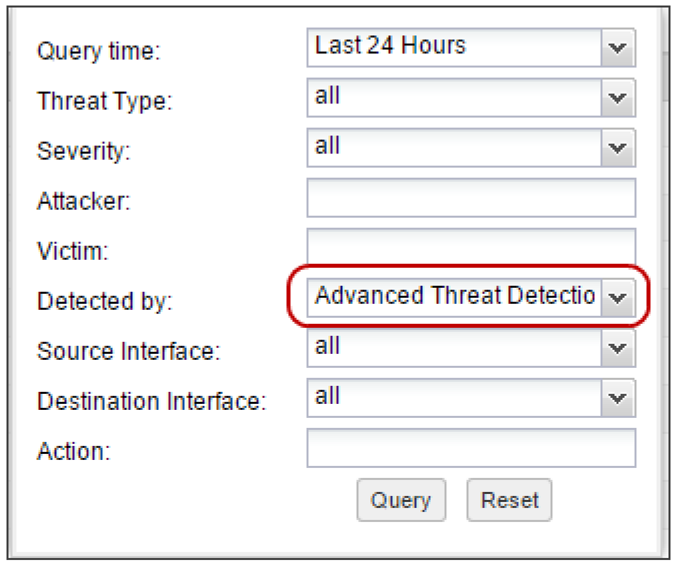
Step 5: Enabling Advanced Threat Detection (ATD) and viewing ATD attacks

2. Click **Details** after **Trojan** in the balloon, you can see details of this attack.



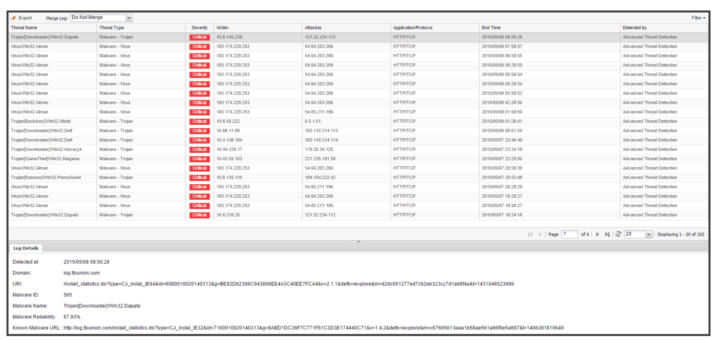
Viewing ATD logs

1. Select **Monitor > Log > Threat**, and click **Filter** on the top right corner.



- **Detected by:** Advanced Threat Detection

2. Click **Query**, the page will show ATD logs.

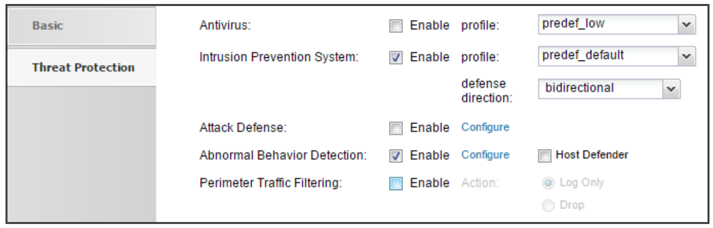


To know more about ATD, you may refer to another case in this cookbook "Finding Malware Attacks via Advanced Threat Detection" on Page 281.

Step 6: Enabling Abnormal Behavior Detection and viewing abnormal behaviors

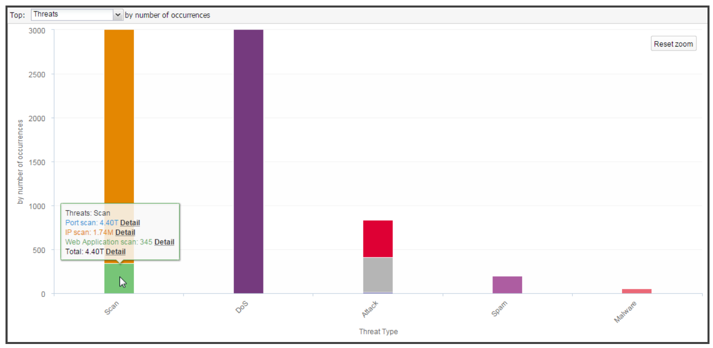
Enabling ABD:

1. Select **Network > Zone**, double-click the **tap-eth1** zone.
2. Under the **Threat Prevention** tab, select the **Enable** check-box after **Abnormal Behavior Detection**.



Viewing monitor results:

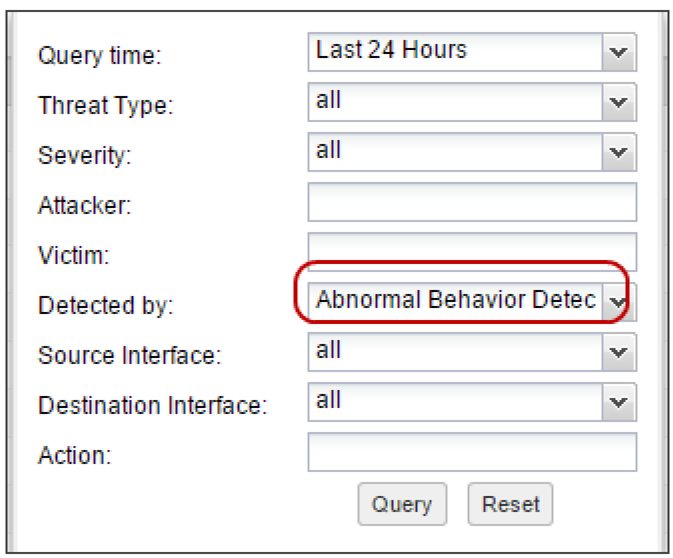
1. Select **Monitor > Threat > Summary**.
2. Hover you cursor over **Scan** or **DoS** bar, a balloon will show up to indicate number of **Scan** and **DoS** attacks.



Viewing ABD logs

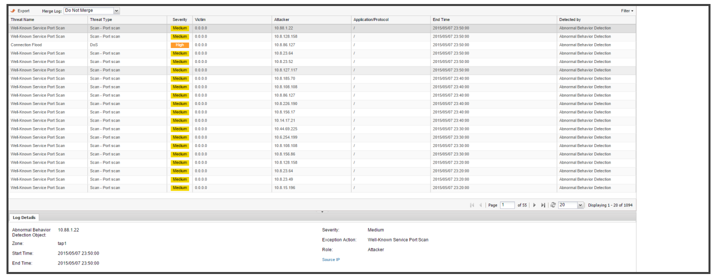
1. Select **Monitor > Log > Threat**, and click **Filter** on the top right corner.

- **Detected by:** Abnormal Behavior Detection



Step 6: Enabling Abnormal Behavior Detection and viewing abnormal behaviors

2. Click Query, ABD logs will show.



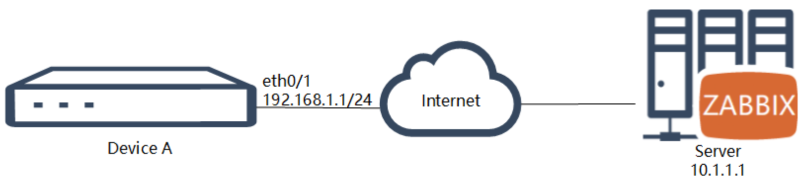
Threat Name	Threat Type	Severity	Victim	Attacker	Application/Protocol	End Time	Detected by
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.88.1.22	/	2015/05/07 23:50:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.128.158	/	2015/05/07 23:50:00	Abnormal Behavior Detection
Connection Flood	DoS	High	0.0.0.0	10.8.86.127	/	2015/05/07 23:50:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.23.64	/	2015/05/07 23:50:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.23.52	/	2015/05/07 23:50:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.127.117	/	2015/05/07 23:50:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.185.70	/	2015/05/07 23:40:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.108.108	/	2015/05/07 23:40:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.86.127	/	2015/05/07 23:40:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.226.190	/	2015/05/07 23:40:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.156.17	/	2015/05/07 23:40:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.14.17.21	/	2015/05/07 23:40:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.44.69.225	/	2015/05/07 23:30:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.6.254.199	/	2015/05/07 23:30:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.108.108	/	2015/05/07 23:30:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.156.86	/	2015/05/07 23:30:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.128.158	/	2015/05/07 23:20:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.23.64	/	2015/05/07 23:20:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.23.49	/	2015/05/07 23:20:00	Abnormal Behavior Detection
Well-Known Service Port Scan	Scan - Port scan	Medium	0.0.0.0	10.8.15.196	/	2015/05/07 23:20:00	Abnormal Behavior Detection

To know more about ABD, you may refer to another case in cookbook "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 272.

Configuring the Device to Communicate with Zabbix Using SNMP

This example introduces how to configure the device to communicate with Zabbix using SNMP. Zabbix can monitor various network parameters of the device to ensure the safe operation of the device.

The following shows a network environment. The device connects to Zabbix using SNMPv2 to manage the device.

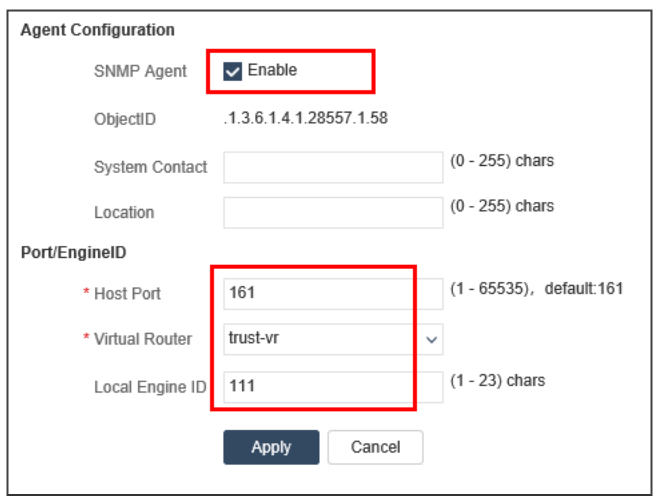


StoneOS

Step1: Configuring SNMP Agent

Select **System > SNMP > SNMP Agent**.

- SNMP Agent: Click **Enable**
- Host Port: 161
- Virtual Router: trust-vr
- Local Engine ID: 111

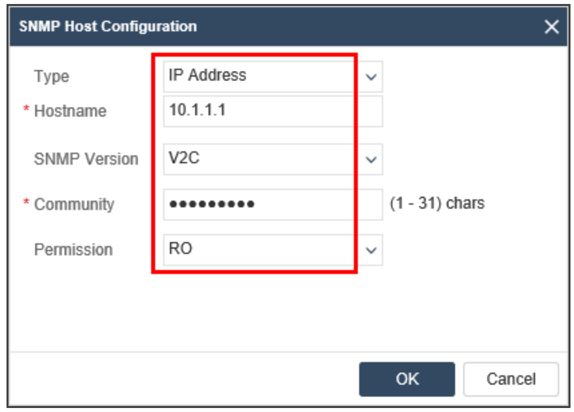


Step2: Configuring SNMP Host

Select **System > SNMP > SNMP Host**.

Click **New**.

- Type: IP Address
- Hostname: 10.1.1.1
- SNMP Version: V2C
- Community: hillstone
- Permission: RO

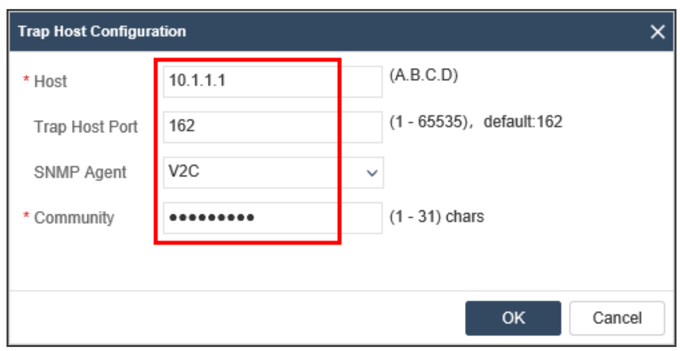


Step3: Configuring Trap Host

Select **System > SNMP > Trap Host**.

Click **New**.

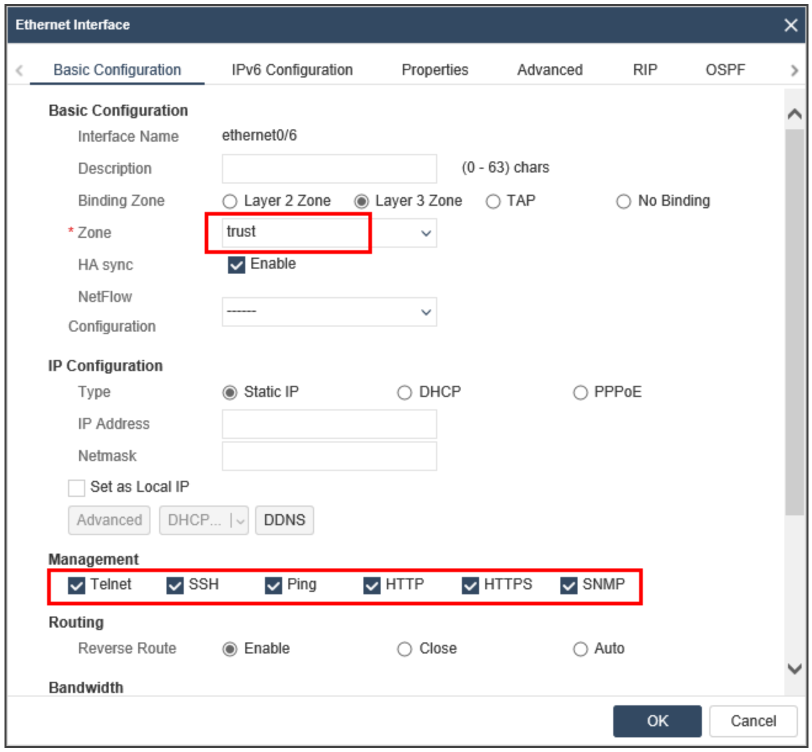
- Host:　10.1.1.1
- Trap Host Port: 162
- SNMP Agent: V2C
- Community: hillstone



Step4: Enabling the SNMP Mode of the Interface

Select **Network > Interface** and double click ethernet0/6.

- Zone: trust
- Management: Click **SNMP**



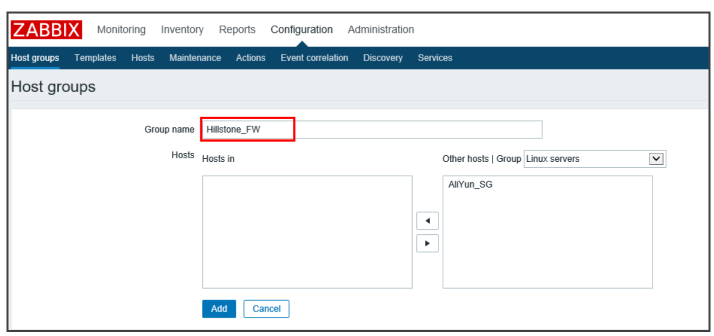
Zabbix:

Step1: Configuring Host Group

Select **Configuration > Host groups**.

Click **Create host group**.

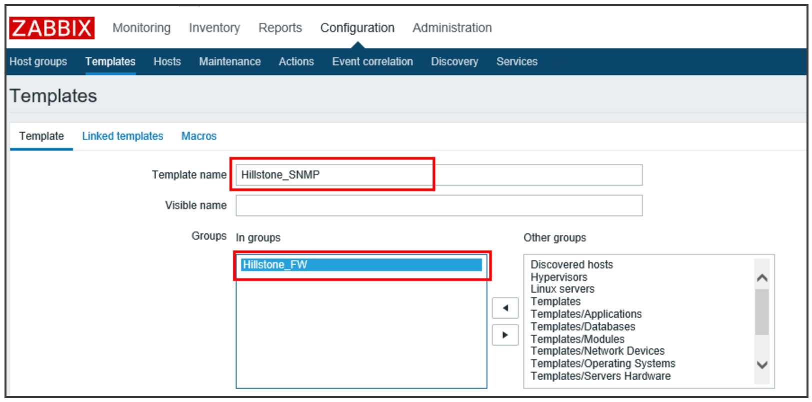
- Group name: Hillstone_FW



Step2: Configuring Templates

Select **Configuration** > **Templates** . Click **Create template**.

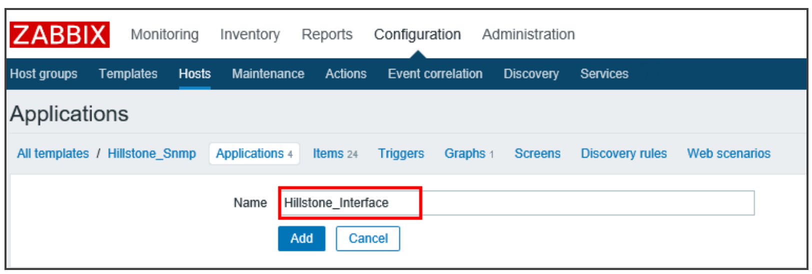
- Template name: Hillstone_SNMP
- Click ◀ icon to add **Hillstone_FW** to **In groups** list.



Step3: Configuring Application

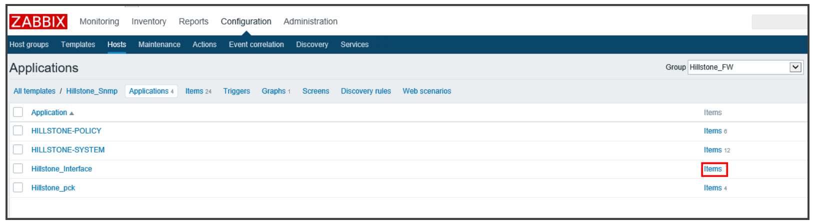
Select **Configuration** >**Template** > **Applications**. Click **Create application**.

- Name: Hillstone_Interface

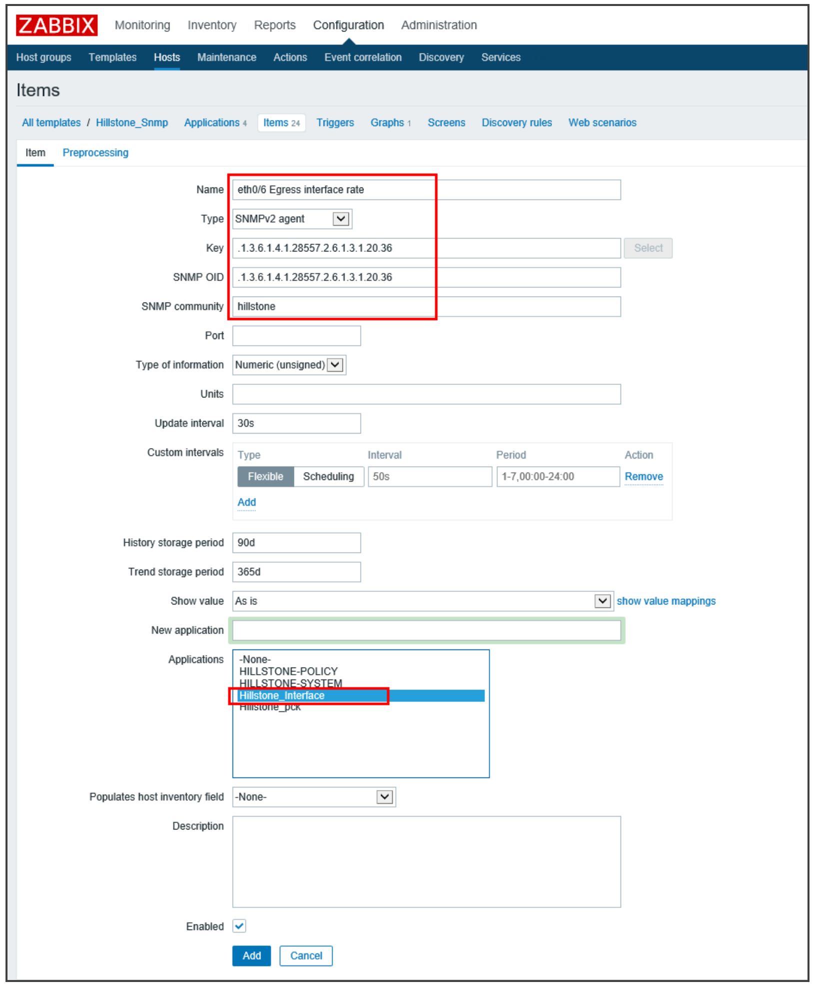


Step4: Configuring Item

Select **Configuration > Templates > Applications**. Click **Items** of **Hillstone_Interface** and click **Create item**.



- Name: eth0/6 Egress interface rate
- Type: SNMPv2 agent
- SNMP OID: .1.3.6.1.4.1.28557.2.6.1.3.1.20.-36
- SNMP community: hillstone
- Applications: Select **Hillstone_Interface**

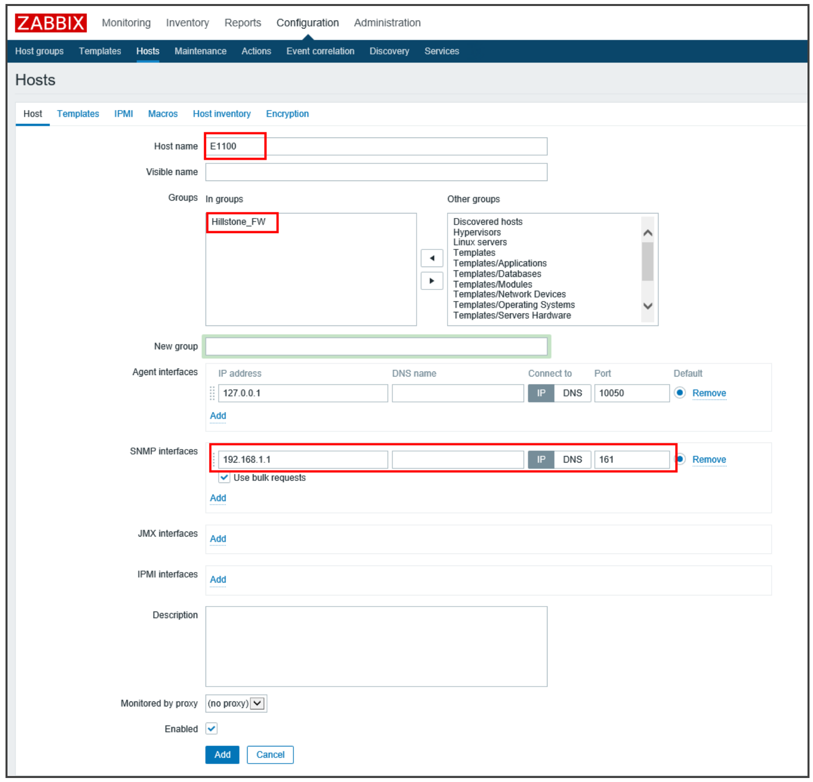


Note: You need to add the index of the specified interface after OID. To view the index of the interface, use the command `show ip route interface`.

Step5: Configuring Host

Select **Configurations > Hosts**. Click **Create host**.

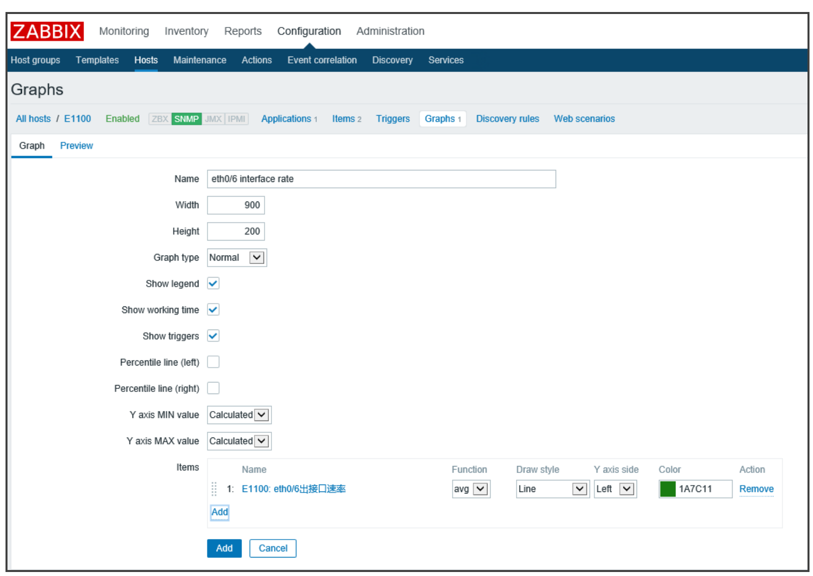
- Host name： E1100
- Click ◄ icon to add **Hillstone_FW** to **In groups** list.
- In **SNMP interfaces** area, click **Add** and type the ip address of StoneOS 192.168.1.1, Port 161.



Step6: Configuring Graph

Select **Configuration > Hosts**. Click **E1100 > Graphs** and click **Create graph**.

- Name: eth0/6 interface rate
- Click **Add** in the **Items** area. Select **eth0/6 Egress interface rate**.

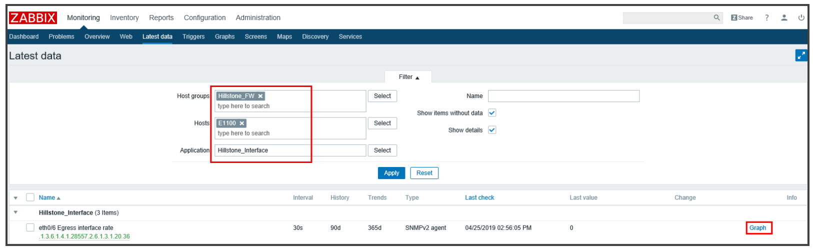


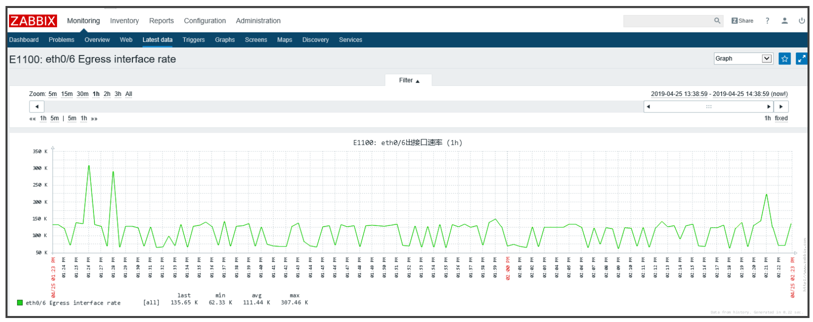
Step7: Results

After configuration, select **Monitoring >Latest data** to view the monitoring data.

- Host groups: Select **Hillstone_FW**
- Hosts: Select **E1100**
- Application: Select **Hillstone_Interface**

Click **Graph** to view the monitoring graph.



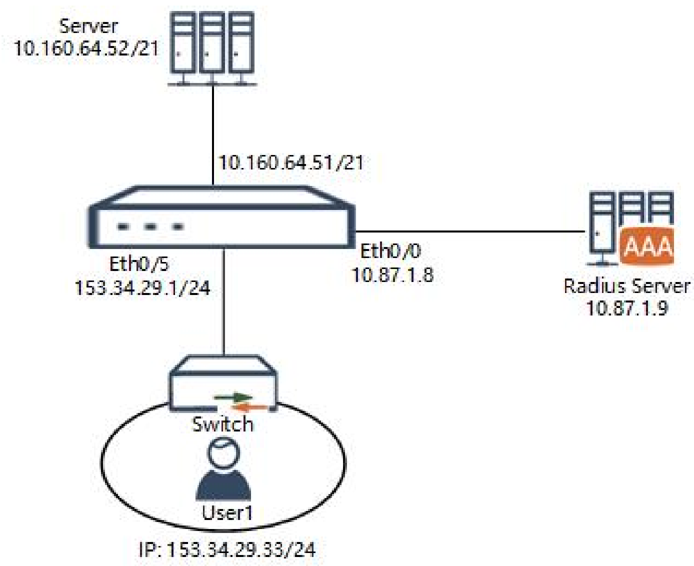


Dynamically Manage Access Authority Via Radius Dynamic Authorization

This example introduces how to dynamically manage access authority via radius dynamic authorization.

Scenario

As shown in the topology, one enterprise can configure Radius server authentication and enable authorization policy to dynamically manage the access authority of visitors. When the visitor logins the SSLVPN, the radius server issues authorization policy to the firewall allowing the visitor to visit the network segment 10.160.64.0/21. When the visitor successfully logins, the administrator can use CoA messages to modify the issued authorization policy, adding new network segment 10.160.32.0/21 that the visitor is allowed to visit. When the visitor logs out, the firewall will automatically delete the responding authorization policy.

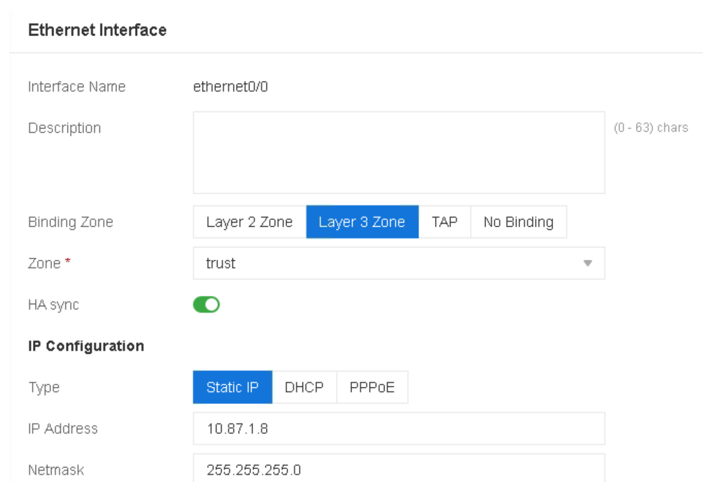


Configuration Steps

Step 1: Configure the Interface to Link Radius Server.

Select **Network>Interface**, and double click **ethernet0/0**.

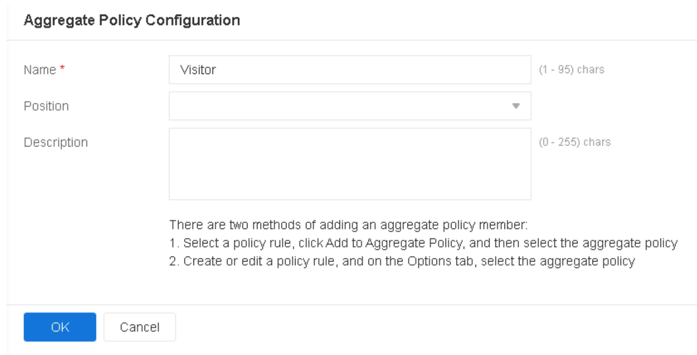
- Binding zone: Layer 3 zone
- Zone: trust
- Type: Static IP
- IP Address: 10.87.1.8
- Netmask: 255.255.255.0



Step 2: Create New Aggregate Policy.

Select **Policy>Security Policy>Policy**, and click **New>Aggregate Policy**.

- Name: Visitor



Step 3: Configure Radius Server, and Enable Authorization Policy and Accounting.

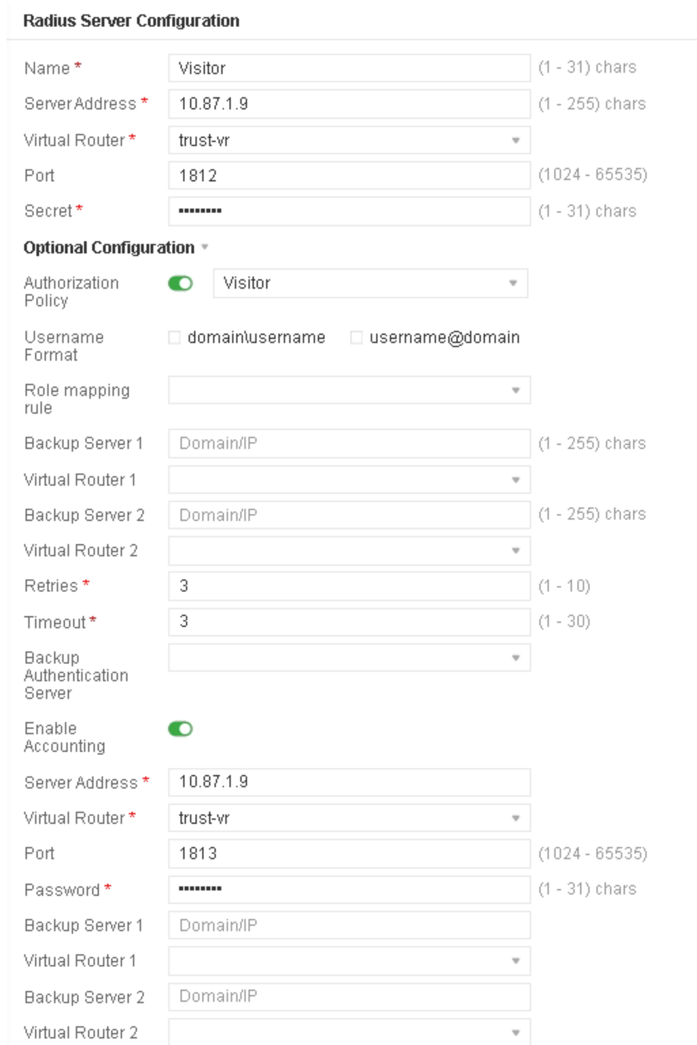
1. Select **Object>AAA Server**, and click **New>Radius Server**.

- Name: Visitor
- Server Address: 10.87.1.9
- Virtual Router: trust-vr
- Port: 1812
- Secret: 12345678

2. Click the **Enable** button of Authorization, and select **Visitor** from the drop-down menu.

3. Click the **Enable** button of Accounting.

- Server Address: 10.87.1.9
- Virtual Router: trust-vr
- Port: 1813
- Password: 12345678



Step 3: Configure Radius Server, and Enable Authorization Policy and Accounting.

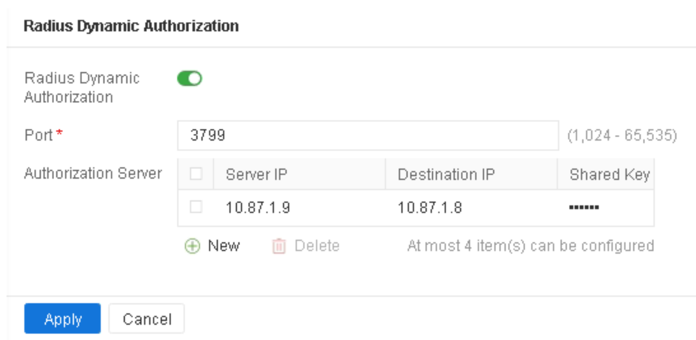
4. Create a new user account.

Client needs to created a new user account on Radius server.

- Username: user1
- Password: 123456
- Authorized network segment: 10.160.64.0/21

Step 4: Enable Radius Dynamic Authorization.

Click Object>Radius Dynamic Authorization, and click the Enable button of Radius Dynamic Authorization.



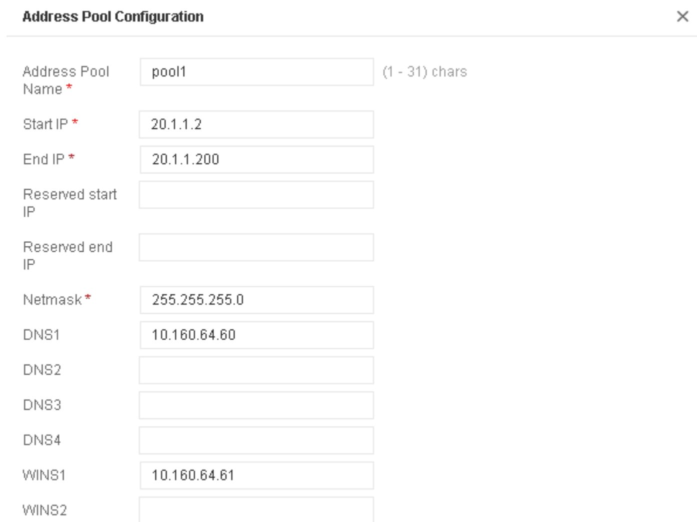
- Port: 3799
- Server IP: 10.87.1.9
- Destination IP: 10.87.1.8
- Shared Key: 12345678

Step 5: Configure SSLVPN on StoneOS.

1. Configure SSLVPN address pool.

Select **Network>SSL VPN**, click **Configuration>Address Pool**, and click **New**.

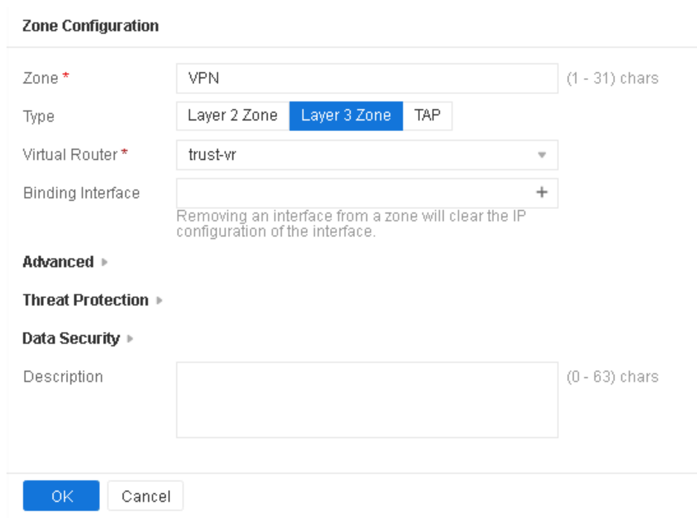
- Address Pool: pool1
- Start IP: 20.1.1.2
- End IP: 20.1.1.200
- Netmast: 255.255.255.0
- DNS1: 10.160.64.60
- WINS1: 10.160.64.61



2. Create new zone.

Select **Network>Zone**, and click **New**.

- Zone: VPN
- Type: Layer 3 Zone
- Virtual Router: trust-vr

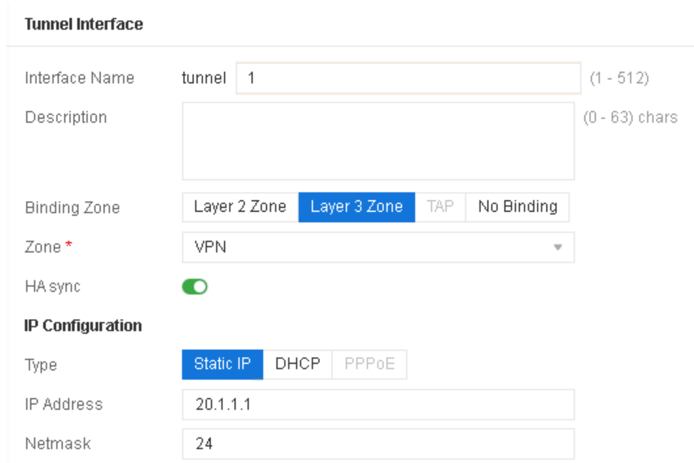


Step 5: Configure SSLVPN on StoneOS.

3. Create new tunnel interface.

Select **Network>Interface**, and click **New>Tunnel Interface**.

- Interface Name: tunnel 1
- Binding Zone: Layer 3 Zone
- Zone: VPN
- Type: Static IP
- IP Address: 20.1.1.1
- Netmask: 24



Step 5: Configure SSLVPN on StoneOS.

4. Configure SSLVPN.

Select **Network>SSL VPN**, and click **New**.

In the Name/Access User tab, configure as below.

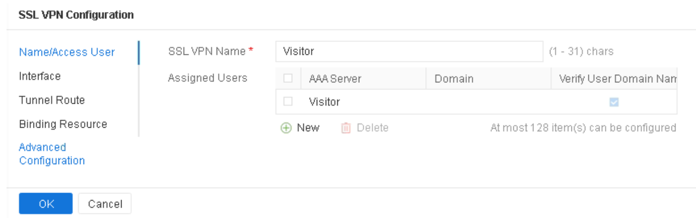
- SSL VPN Name: Visitor
- AAA Server: Visitor

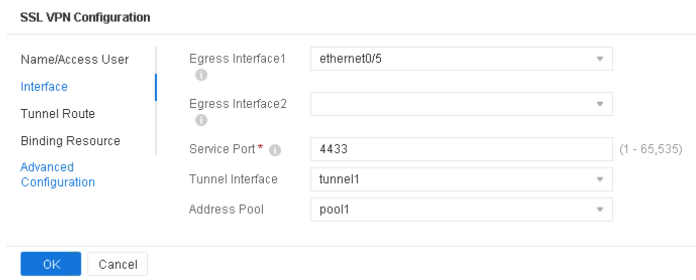
In the Interface tab, configure as below.

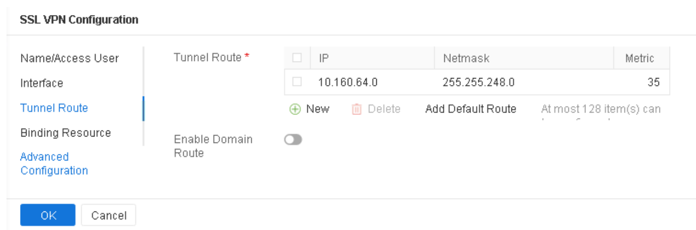
- Egress Interface 1： ethernet0/5
- Service Port： 443
- Tunnel Interface： tunnel1
- Address Pool： pool1

In the Tunnel Route tab, configure as below.

- IP： 10.160.64.0
- Netmask： 255.255.248.0



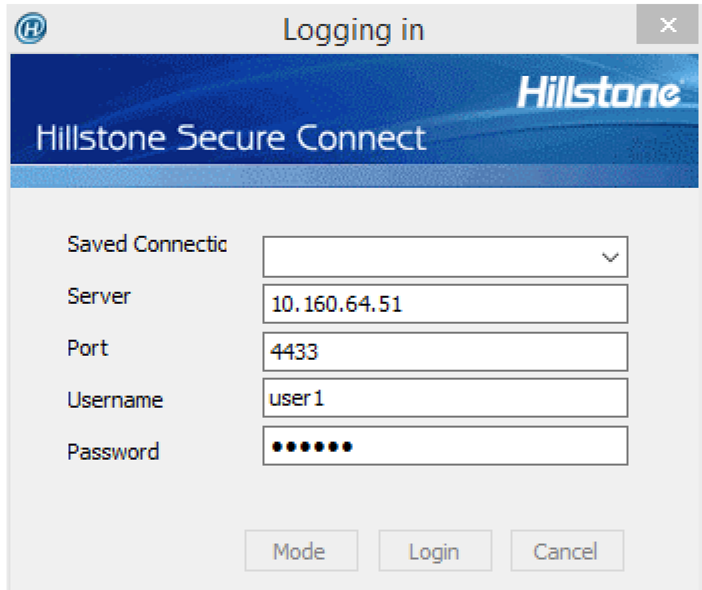




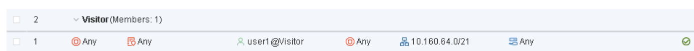
Step 6: Results.

1. User1 can access 10.160.64.52.

   - Server: 10.160.64.51
   - Port: 4433
   - Username: user1
   - Password: 123456



2. Corresponding policy is created on Firewall.

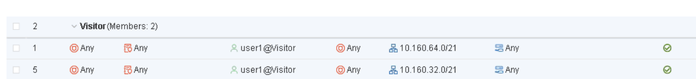


Step 7: Use CoA message to modify the access authority of the authorized user.

1. Use CoA message in CLI commands to modify the network segment that the authorized user has access to (If the radius server that the client uses is customized, the client can operate directly on radius server rather than use CLI commands).

- Create a new txt file named coa-auth of which the content is as below:
  User-Name： user1
  Framed-IP-Address=20.1.1.3
  NAS-IP-Address=10.87.1.8
  Acct-Seesion-Id= “1”
  Hillstone-User-Data-Filter= “rule 1 permit dst 10.160.64.0/21”
  Hillstone-User-Data-Filter= “rule2 permit dst 10.160.32.0/21”
  Calling-Station-Id="00-1c-54-ff-08-05"
- Use the blow CLI command to send the instruction (take freeradius for example):
  root@hillstone-HVM-domU:/etc/-freeradius# radclient 10.87.1.8:3799 coa 12345678 -f coa-auth.txt -x

2. Policies are updated on Firewall.



2	Visitor (Members: 2)					
1	Any	Any	user1@Visitor	Any	10.160.64.0/21	Any
5	Any	Any	user1@Visitor	Any	10.160.32.0/21	Any

Step 8: User1 logs out of SSLVPN.

User1 logs out of SSLVPN, and the corresponding policies are deleted from Firewall.

DNS Proxy

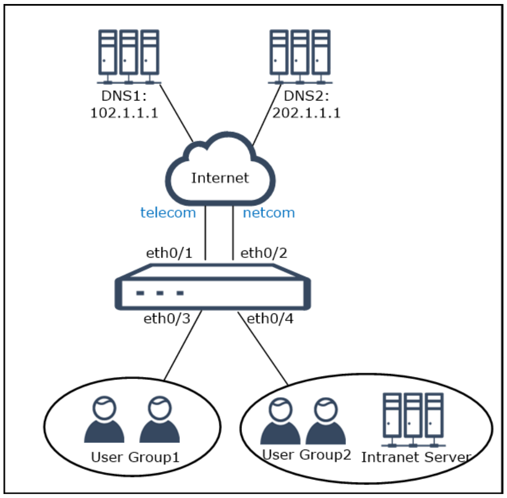
This example shows how to configure the DNS proxy function. By configuring flexible DNS proxy rules, users from different segments are assigned to different DNS servers for domain name resolution.

Scenario

A secondary ISP rents the bandwidth of telecom, netcom and other ISP to different users for Internet access. The telecom and netcom ISP have their own DNS servers. So the secondary ISP want to assign users of different network segments to the DNS servers of corresponding ISP for domain name resolution through DNS proxy devices.

This example simulates the export scenario of the above secondary ISP through the following configuration. Use eth0/1 (IP:101.0.0.1) of the device to connect to the telecom special line to access the Internet, and use eth0/2 (IP: 201.1.1.1) to connect to the netcom special line to access the Internet. In the public network, the DNS server of telecom is DNS1:102.1.1.1, and that of netcom is DNS2:202.1.1.1. Also, eth0/3, eth0/4 connect to the Intranet user groups. The administrator now has the following requirements:

1. The DNS request of user group 1 (network segment: 192.168.10.1 / 28) is uniformly proxy to dns1 for domain name resolution;
2. The DNS request of user group 2 (network segment: 172.168.10.1 / 24) is uniformly proxy to dns2 for domain name resolution;
3. The DNS request of intranet server (172.168.10.88) is not restricted and bypassed directly.



Preparation

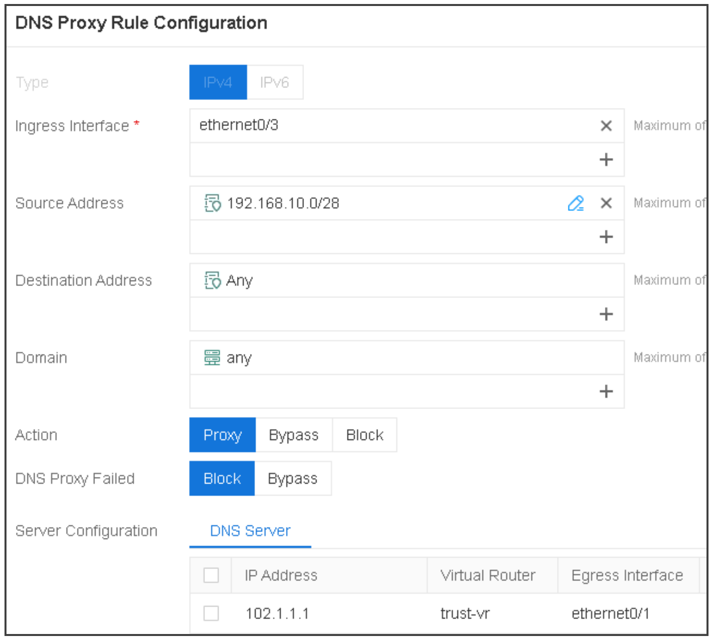
The basic interface and route configuration have been completed, and users can access the Internet normally.

Configuration Steps

Step 1： Configure a DNS proxy rules to proxy DNS requests of user group 1 to DNS1 for domain name resolution;

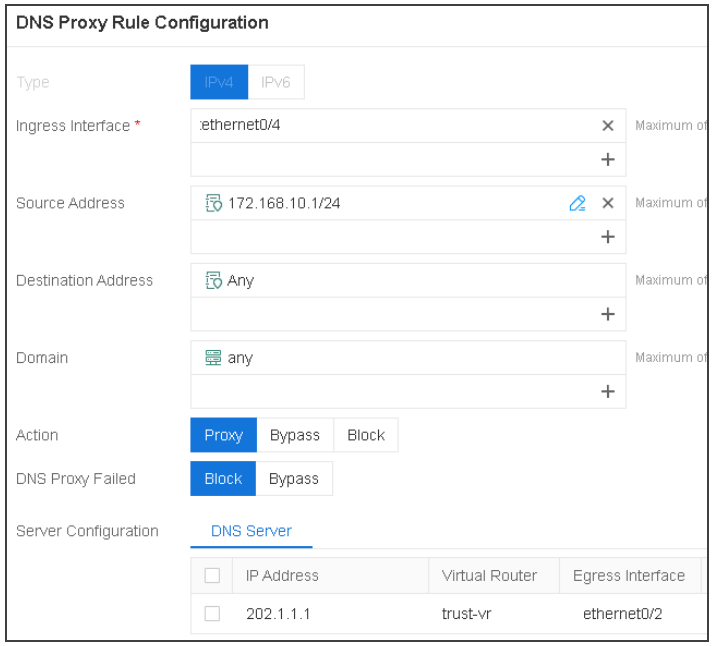
Login WebUI and select **Network > DNS >DNS Proxy**, and click **New**.

- Ingress Interface: ethernet0/3;
- Source Address: Configure a new address book 192.168.10.1/28
- Destination Address: Any
- Domain: any
- Action: Proxy
- DNS Proxy Failed: Block
- DNS Server：
  - IP Address: 102.1.1.1
  - Virtual Router: trust-vr
  - Egress Interface： etherent0/1



Step 2: Configure another DNS proxy rule to uniformly proxy DNS requests of user group 2 to DNS2 for domain name resolution.

Continue to configure another rule. Select **Network > DNS >DNS Proxy**, and click **New**.

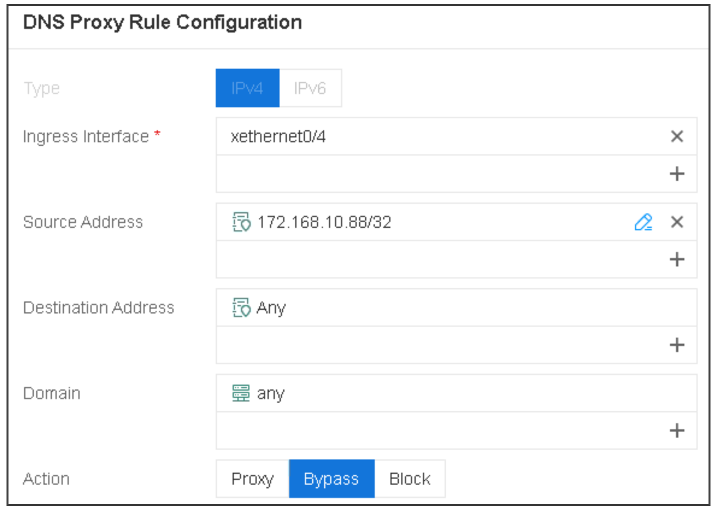


- Ingress Interface: ethernet0/4;
- Source Address: Configure a new address book 172.168.10.1/24
- Destination Address: Any
- Domain: any
- Action: Proxy
- DNS Proxy Failed: Block
- DNS Server：
  - IP Address: 202.1.1.1
  - Virtual Router: trust-vr
  - Egress Interface： etherent0/2

Step 3: Configure one more DNS proxy rule to release DNS requests from the Intranet server (172.168.10.88) directly.

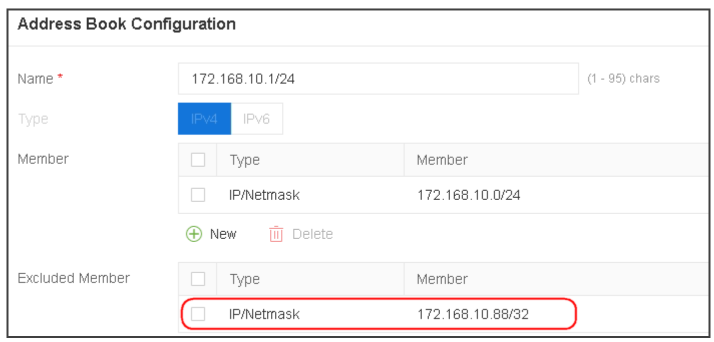
Continue to configure one more rule. Select **Network > DNS >DNS Proxy**, and click **New**.

- Ingress Interface: ethernet0/4;
- Source Address: Configure a new address book 172.168.10.88/32
- Destination Address: Any
- Domain: any
- Action: Bypass



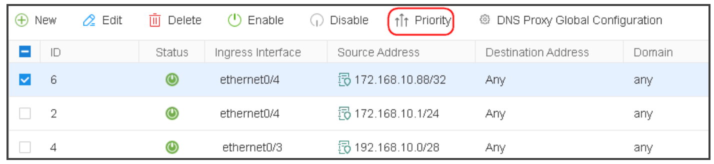
(Optional) In addition to creating a new address rule, the following methods can also be used to bypass the DNS requests from intranet servers. Select **Object** > **Address Book**,and select the "172.168.10.1/24" item, and click **Edit** to add the IP address of intranet server to the **Exclude Member**.

- Exclude Member: 172.168.10.88



Step 4: Adjust the priority of DNS proxy rules.

After the above steps, you will get three DNS proxy rules. Because the DNS proxy rules match from top to bottom, so the DNS rules for releasing the Intranet server should be placed on top of the other two. When configuring, select the corresponding rule item and click **Priority**to adjust.



	ID	Status	Ingress Interface	Source Address	Destination Address	Domain
☑	6		ethernet0/4	172.168.10.88/32	Any	any
☐	2		ethernet0/4	172.168.10.1/24	Any	any
☐	4		ethernet0/3	192.168.10.0/28	Any	any

Step 5： Results

After configuration, capture packets on eth0 / 1 and eth0 / 2 interfaces. The results are as follows:

- The users of 192.168.10.1/28 network segment in user group 1 can still access the Internet normally, and their DNS requests will be sent to the DNS1 server of Telecom for domain name resolution through the device.
- The uesrs of 172.168.10.1/24 network segment in user group 2 can still access the Internet normally, and DNS requests will be sent to the DNS2 server of Netcom for domain name resolution.
- The DNS request of the internal server 172.168.10.88 will not be proxy through the device, but will be resolved according to the DNS server set by itself.

Q&A

- Q： What is the order and manner of matching multiple DNS proxy rules?

  A： The device will query for DNS proxy rules by turns from up to down. In each rule, only if all matching conditions are met can the matching be successful.

- Q： When multiple DNS servers are configured in a DNS proxy rule, what is the priority of preferred and bound out interface properties?

  A： When you configure multiple DNS servers, the DNS server with preferred property will be selected for domain name resolution. If no preferred server is specified, the system will query whether there are DNS servers that have specified the egress interface.

- Q： Can DNS proxy for specific domain names?

  A： Yes, you can configure a specific domain name in the option "**Domain Name**", and then configure the proxy action and the corresponding DNS server when creating a new rule.

Routing

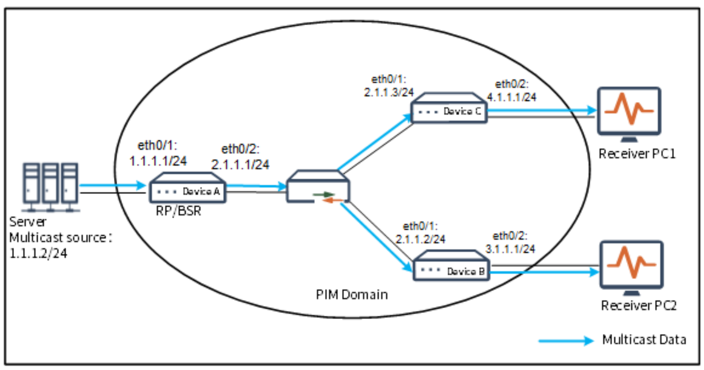
This chapter introduces different routing configuration use cases.

This chapter contains the following recipes:

Realizing Multicast Forwarding Through PIM-SM Multicast Protocol

This example introduces how to configure the basic functions of PIM-SM to realize multicast forwarding so that users can receive data from any multicast source.

In the topology below, the multicast source sends data to the multicast group, and the multicast address is 225.0.0.1. The receivers PC1 and PC2 send IGMPv2 Report to join the multicast group, and the PIM domain adopts the PIM-SM mode. Assume that Device A is the candidate RP and candidate BSR, the interface loopback1 is the interface for electing the RP, and the interface eth0/1 is the multicast data inbound interface. By configuring the PIM-SM function on each device in the PIM domain, multicast data can be forwarded to the recipient PC in a normal multicast manner.



Configuration Steps

Step 1: Configure the IP address and unicast routing protocol of each device interface (OSPF is used in this example).

```
Device A：
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 1.1.1.1
hostname(config-router)# network 1.1.1.0/24 area 0
hostname(config-router)# network 2.1.1.0/24 area 0
```

Device B:

hostname(config)# **interface ethernet0/1**

hostname(config-if-eth0/1)# **zone trust**

hostname(config-if-eth0/1)# **ip address 2.1.1.2/24**

hostname(config-if-eth0/1)# **exit**

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/1)# **zone trust**

hostname(config-if-eth0/1)# **ip address 3.1.1.2/24**

hostname(config-if-eth0/1)# **exit**

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **router ospf**

hostname(config-router)# **router-id 2.2.2.2**

hostname(config-router)# **network 2.1.1.0/24 area 0**

hostname(config-router)# **network 3.1.1.0/24 area 0**

```
Device C:
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.3/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 4.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 3.3.3.3
hostname(config-router)# network 2.1.1.0/24 area 0
hostname(config-router)# network 4.1.1.0/24 area 0
```

Step 2: Enable a multicast route.

```
Device A:
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

```
Device B:

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip multicast-routing

hostname(config-vrouter)# exit

hostname(config)#
```

```
Device C:

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip multicast-routing

hostname(config-vrouter)# exit

hostname(config)#
```

Step 3: Enable and configure PIM-SM.

```
Device A:

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter))# router pim

hostname(config-vrouter)# pim-sm enable

hostname(config-vrouter))# exit

hostname(config)#interface ethernet0/1

hostname(config-if-eth0/1)# ip pim sparse-mode

hostname(config-if-eth0/1)# exit

hostname(config)#interface ethernet0/2

hostname(config-if-eth0/2)# ip pim sparse-mode
```

Device B:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Device C:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Step 4: Configure RP and Candidate BSR.

Device A：

hostname(config)# **interface loopback1**

hostname(config-if-loo1))# **zone trust**

hostname(config-if-loo1)# **ip address 2.2.2.2/24**

hostname(config-if-loo1)# **ip pim sparse-mode**

hostname(config-if-loo1))# **exit**

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **rp-candidate loopback1**

hostname(config-vrouter)# **bsr-candidate loopback1**

hostname(config-vrouter))# **exit**

hostname(config)#

Step 5: Verify result.

Device A :

hostname(config)# **show ip mroute**

U:interface up D:interface down

V:valid multicast entry I:invalid multicast entry Y:sync multicast entry

===-

================================

source: 1.1.1.2 group : 225.0.0.1 vrouter: trust-vr

status: V update time: -

ingress interface: ethernet0/1(U)

egress interface : ethernet0/2(U)

===-

================================

hostname(config)# **show ip pim rp**

PIM Rendezvous Point for Virtual Router <trust-vr>

===-

================================

Group: 225.0.0.1, RP:2.2.2.2, v2, via bootstrap, priority 0 holdtime 35.

===-

================================

hostname(config)# **show ip pim bsr-router**

PIM Bootstrap Router for Virtual Router <trust-vr>

===-

================================

PIMv2 Bootstrap information

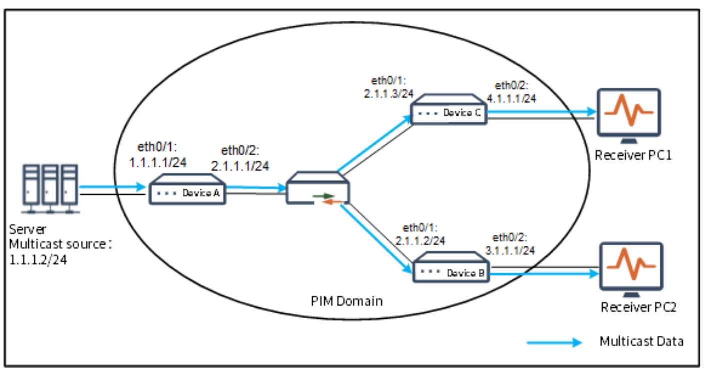
BSR address: 2.2.2.2

```
BSR Priority: 0

=====================================================-

================================
```

Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol

This example introduces how to configure the basic functions of PIM-SSM to realize multicast forwarding so that users can receive data from any multicast source.

In the topology below, the multicast source sends data to the multicast group, and the multicast address is 232.0.0.1. Receivers PC1 and PC2 send IGMPv3 Report to join the multicast group. The PIM domain adopts the PIM-SSM mode. The relationship between the host and the devices in the PIM domain is maintained through IGMPv3, so that the members of the multicast group can quickly join, directly at the multicast source SPT (Shortest Path Tree) is established with the recipient PC. Assume that the interface eth0/1 of Device A is used as the inbound interface for multicast data. By configuring the PIM-SSM function on each device in the PIM domain, multicast data can be multicast forwarded to the recipient PC normally.



Configuration Steps

Step 1: Configure the IP address and unicast routing protocol of each device interface (OSPF is used in this example).

```
Device A:
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 1.1.1.1
hostname(config-router)# network 1.1.1.0/24 area 0
hostname(config-router)# network 2.1.1.0/24 area 0
```

```
Device B:
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 3.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 2.2.2.2
hostname(config-router)# network 2.1.1.0/24 area 0
hostname(config-router)# network 3.1.1.0/24 area 0
```

```
Device C:
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.3/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 4.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 3.3.3.3
hostname(config-router)# network 2.1.1.0/24 area 0
hostname(config-router)# network 4.1.1.0/24 area 0
```

Step 2: Enable a multicast route.

```
Device A:
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

Device B:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip multicast-routing**

hostname(config-vrouter)# **exit**

hostname(config)#

Device C:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip multicast-routing**

hostname(config-vrouter)# **exit**

hostname(config)#

Step 3: Configure PIM-SSM.

Device A:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter)# **pim-ssm default**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Device B:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter)# **pim-ssm default**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Device C:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter)# **pim-ssm default**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Step 4: Verify result.

Device A:

hostname(config)# **show ip mroute**

```
U:interface up D:interface down
V:valid multicast entry I:invalid multicast entry Y:sync multicast entry
=================================================-
===============================
source: 1.1.1.2 group : 232.0.0.1 vrouter: trust-vr
status: V update time: -
ingress interface: ethernet0/1(U)
egress interface : ethernet0/2(U)
=================================================-
===============================
```

Authentication

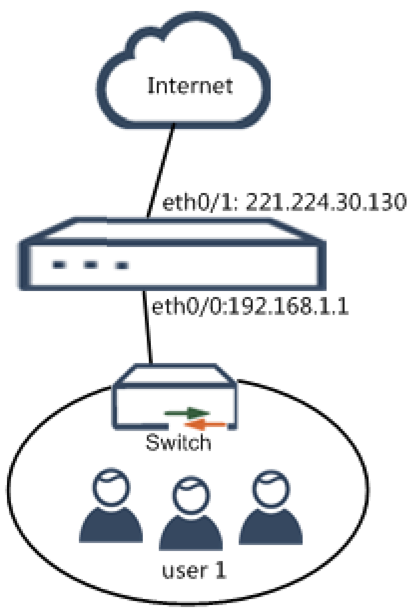
Authentication is a method of verifying visitor's identity. When a visitor is confirmed as a valid user, he is allowed to use a certain network. The visitor can be a PC, a mobile phone or a tablet.

This chapter contains the following recipe:

Allowing the Internet Access via User Authentication

This example shows how to use Web authentication (WebAuth). An AAA server is required in this example to confirm the identity of a user.

The topology describes the scenarios of the case. In this scenario, only user 1 passes the authentication, and then accesses the Internet; while other users fail to pass the authentication, and they are not allowed to access the Internet.

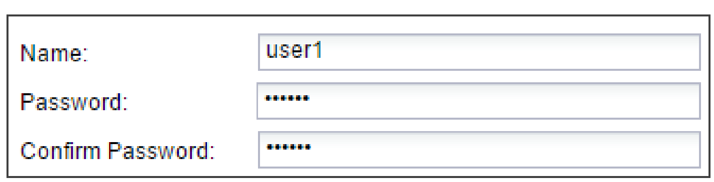


Configuration Steps

Step 1: Configuring the user and address book

Select **Object > User > Local User**.

Under **Local Server**, click **New > User**.

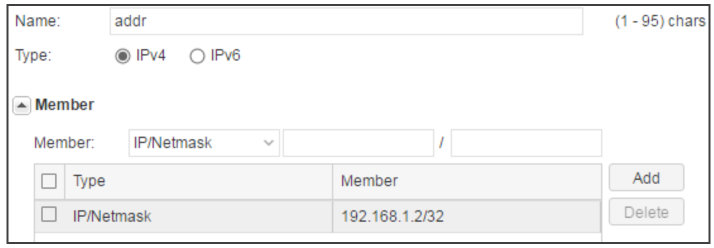


- Name: user1
- Password: 123456
- Confirm Password: 123456

Step 1: Configuring the user and address book

Select **Object > Address Book > New**.

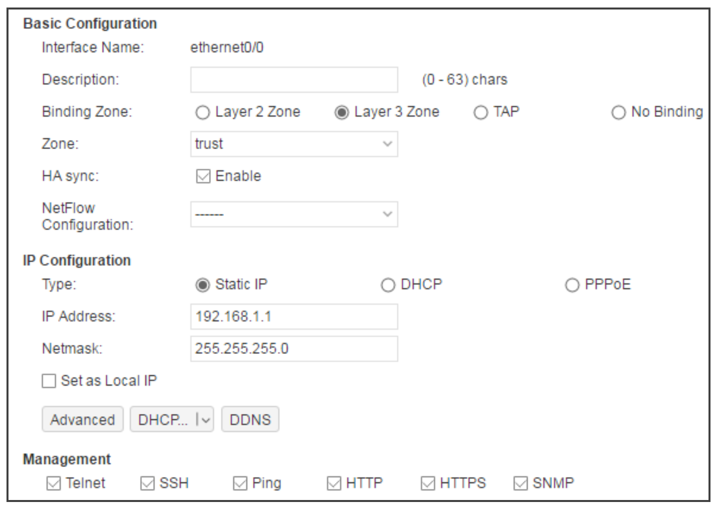
- Name: addr
- Member: Select **IP/Netmask**, enter **192.168.1.2**, **32**, and click **Add**



Step 2: Configuring the interface and zone

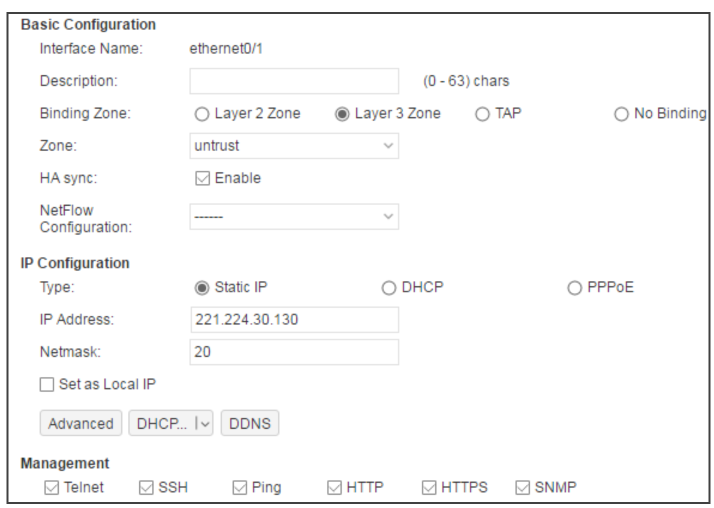
Select **Network > Interface**, and double click **ethernet0/0**.

- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 24



Select **Network > Interface**, and double click **ethernet0/1**.

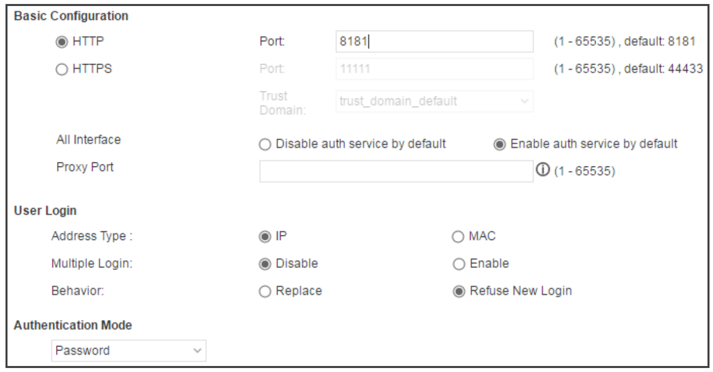
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 221.224.30.130
- Netmask: 20



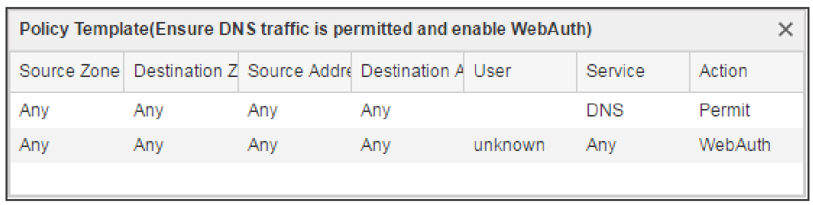
Step 3: Configuring Web Authentication

Select **Network > WebAuth > WebAuth**, and select the **Enable** check box

- Basic Configuration:
  - HTTP Port: 8181
- Authentication Mode: Password



After the above configurations, continue to create policy rules in **Security Policy** to make WebAuth effective. Click **Policy Template** for reference.

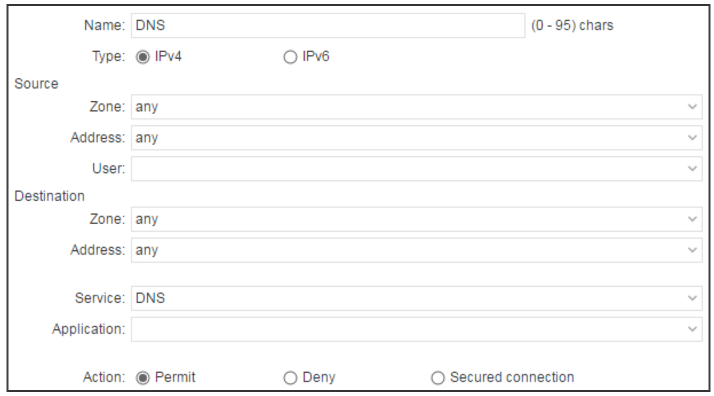


Policy Template(Ensure DNS traffic is permitted and enable WebAuth)

Source Zone	Destination Z	Source Addre	Destination A	User	Service	Action
Any	Any	Any	Any		DNS	Permit
Any	Any	Any	Any	unknown	Any	WebAuth

Step 4: Configuring Security Policy

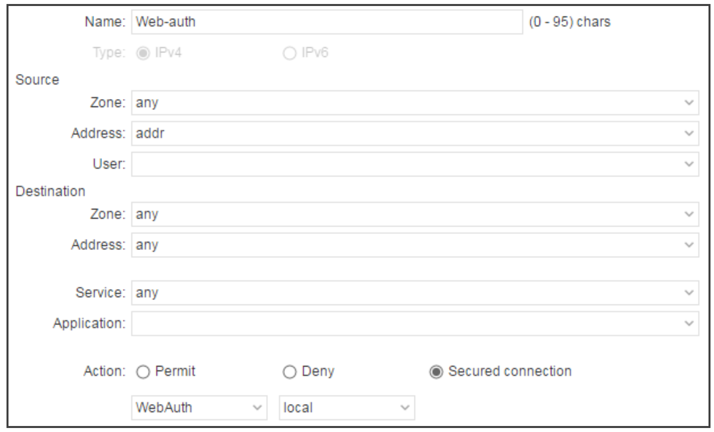
Click the "Security Policy" quick link on the bottom of the Web authentication page or select **Policy > Security Policy**, and click **New**.



- Name: DNS
- Source
  - Zone: Any
  - Address: Any
- Destination
  - Zone: Any
  - Address: Any
  - Service: DNS
  - Action: Permit

Step 4: Configuring Security Policy

Click **New**, and create the "Web-auth" -policy.



- Name: Web-auth
- Source
  - Zone: Any
  - Address: addr
- Destination
  - Zone: Any
  - Address: Any
  - Action: Secured connection
  - WebAuth: local

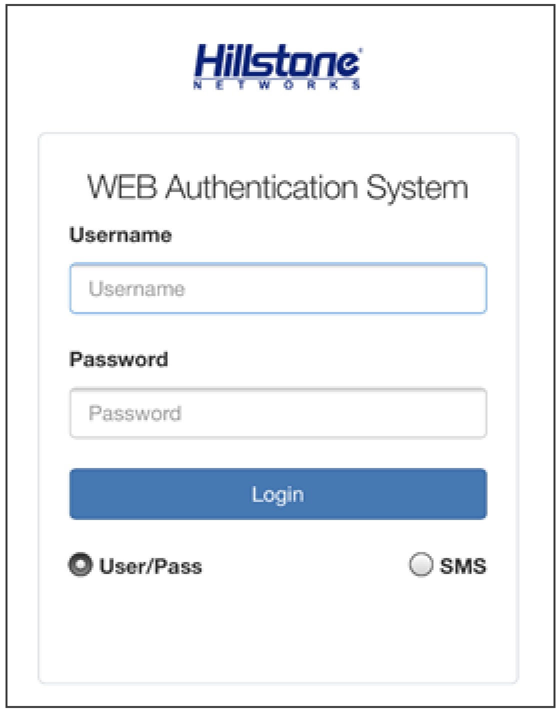
Step 4: Configuring Security Policy

Click **New**, and create the "user" policy. Specify the source user who is allowed to access the Internet.

- Name: user
- Source
  - Zone: Any
  - Address: Any
  - User: user1
- Destination
  - Zone: Any
  - Address: Any
  - Action: Permit

Step 5: Triggering WebAuth through HTTP requests

After the above configurations, when there are HTTP requests sent from the interface 192.168.1.2/32, user1 will be prompted to authenticate by entering the username/password (user1/123456) before accessing the Internet.



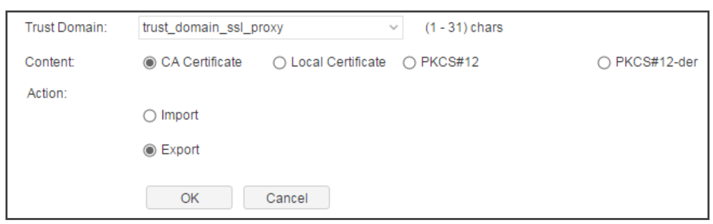
Step 6: Triggering WebAuth through HTTPS requests

Export the certificate from the device.

Select **System > PKI > Trust Domain Certificate**.

- Trust Domain: trust_domain_ssl_proxy
- Content: CA Certificate
- Action: Export

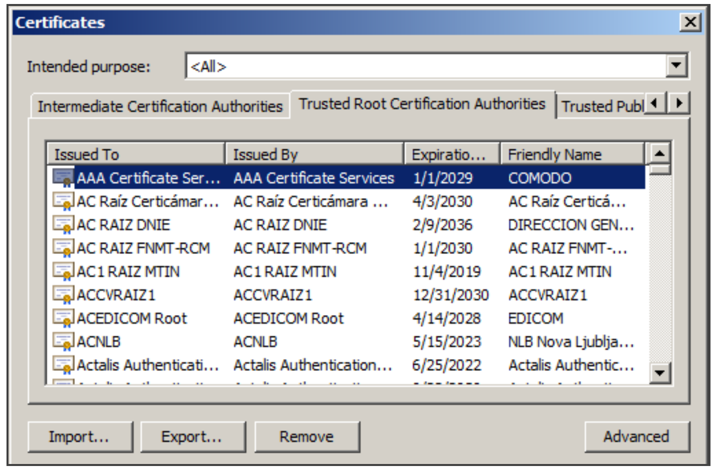
Click **OK** to export the certificate.



Step 6: Triggering WebAuth through HTTPS requests

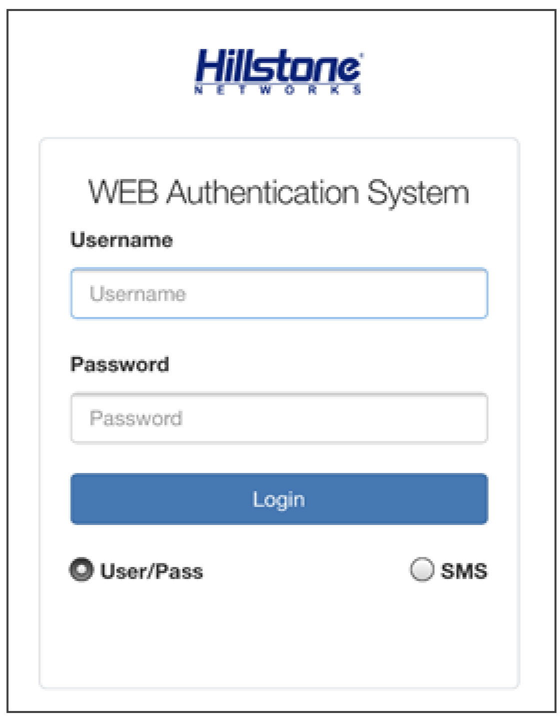
Import the certificate to client's Web browser.

1. In the Chrome Web browser, select **Settings > Show advanced settings**.
2. In the HTTPS/SSL section, select **Manage certificates**.
3. In the **Trusted Root Certification Authorities** tab, select **Import**.
4. Follow the wizard to import the certificate.



After the above configurations are finished, when there are HTTPS requests sent from the interface 192.168.1.2/32, user1 will be prompted to authenticate by entering the username/password (user1/123456) before accessing the Internet.

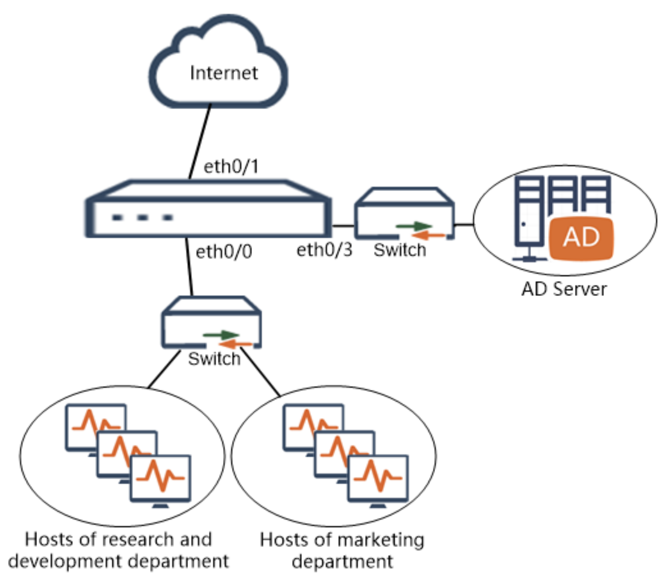
Note: Triggering WebAuth through HTTPS requests depends on the feature of SSL proxy . If the device does not support the SSL proxy. Triggering WebAuth through HTTPS requests will not work and you can then trigger WebAuth through HTTP requests.



Using AD Polling for SSO

This example introduces how the domain users access the Internet directly without Web authentication, after logging in the AD domain via configuring AD Polling.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Only the staffs in R&D department join in the AD domain (scep.pki.com), while the staffs in marketing department are excluded. The security device enables Web authentication. All the staffs of the enterprise are allowed to access the Internet only after they pass the authentication. After the AD Polling being configured, there will be login logs when staff in R&D department login though the AD server (Log in the PC which is added into the AD domain through domain user name and password). The device can check the logs through AD Polling, as well as obtain authentication users information on the AD server. With this information, staff of R&D department can access the Internet directly without Web authentication.



Preparation

Before configuring the AD Polling function, prepare the following first:

- The AD server has been set up according to the user network environment.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should open the RPC service and remote management. To enable the RPC service, you need to enter the **Control Panel > Administrative Tools > Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **`netsh firewall set service RemoteAdmin`**
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security> Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- The security device should be configured with related policy to protect the AD server, which may result in the port used by WMI service (port 135 and random port) being restricted by policy. Therefore, it’s necessary to configure another policy (the source IP is the IP address of ethernet0/3) allows all interface traffic to pass through.
- The rule has been configured on the security device that all the staff of the enterprise should pass the Web authentication before they access the Internet. For the detailed configuration method, please see "Allowing the Internet Access via User Authentication" on Page 81.

Configuration Steps

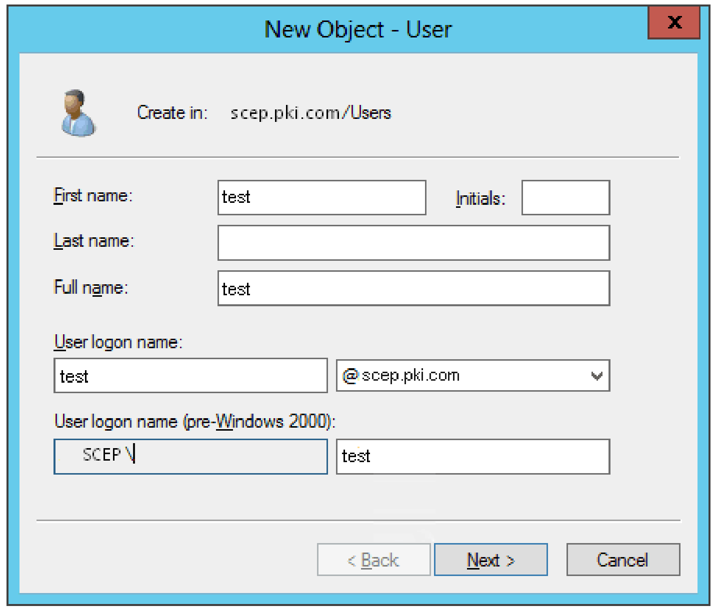
Step 1: Creating a new domain user on the AD server and configuring the user as the Domain Admins group.

Access the PC with AD server, select **Start > Administrative Tools > Active Directory Users and Computers**, and enter the Active Directory Users and Computers page.

Step 1: Creating a new domain user on the AD server and configuring the user as the Domain Admins group.

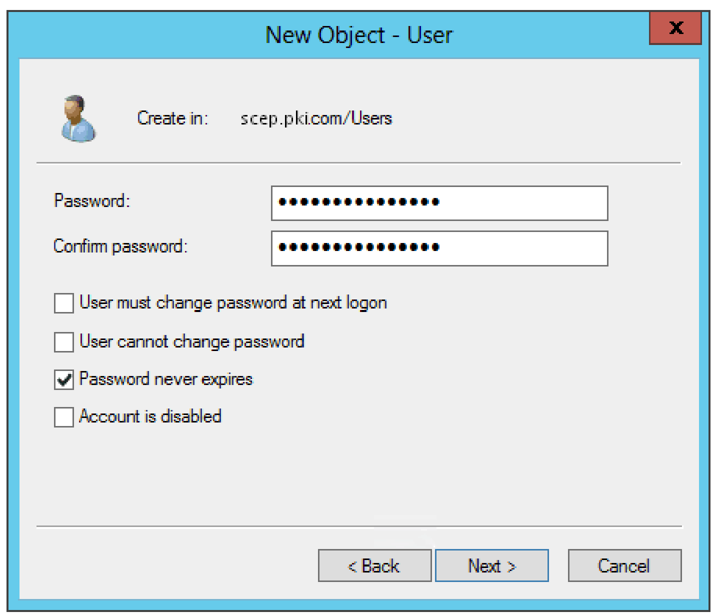
Right-click **Users** and select **New Object > User**. Click **Next.**

- First name: test
- User logon name: test@scep.pki.com



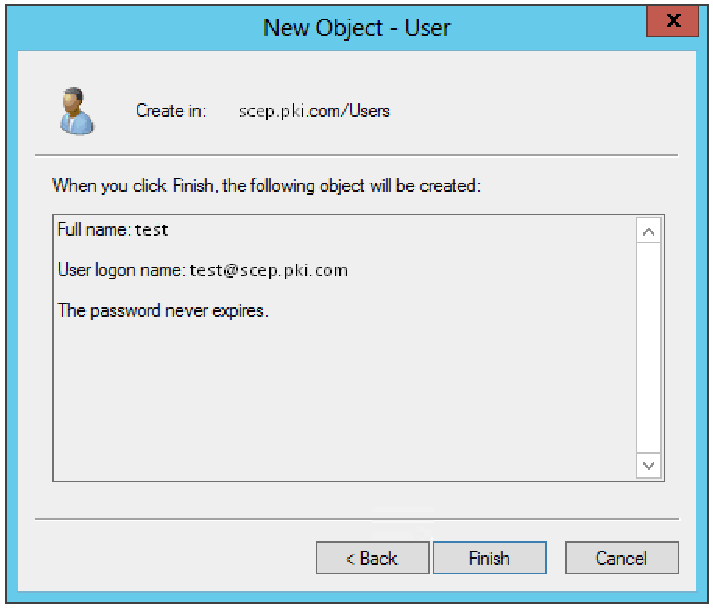
Configure a password on the **New Object- User** page, and click **Next.**

- Password: Hillstone123456
- Confirm password: Hillstone123456
- Password never expires: Select the check box



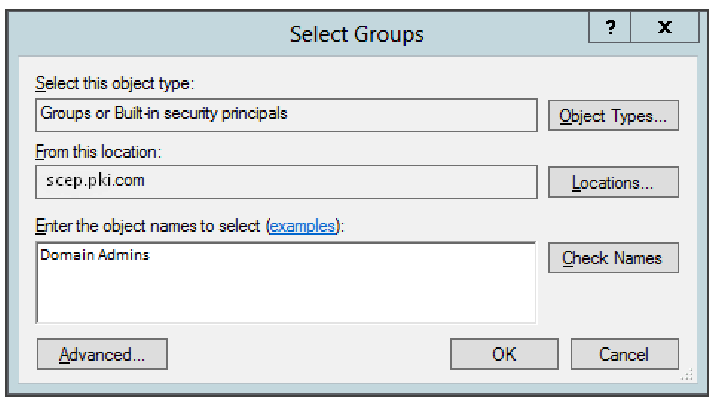
Step 1: Creating a new domain user on the AD server and configuring the user as the Domain Admins group.

Click **Finish** to finish the creating of domain user **test**.



In the user list, right-click **test**, and select **Add to group**. Click **OK**.

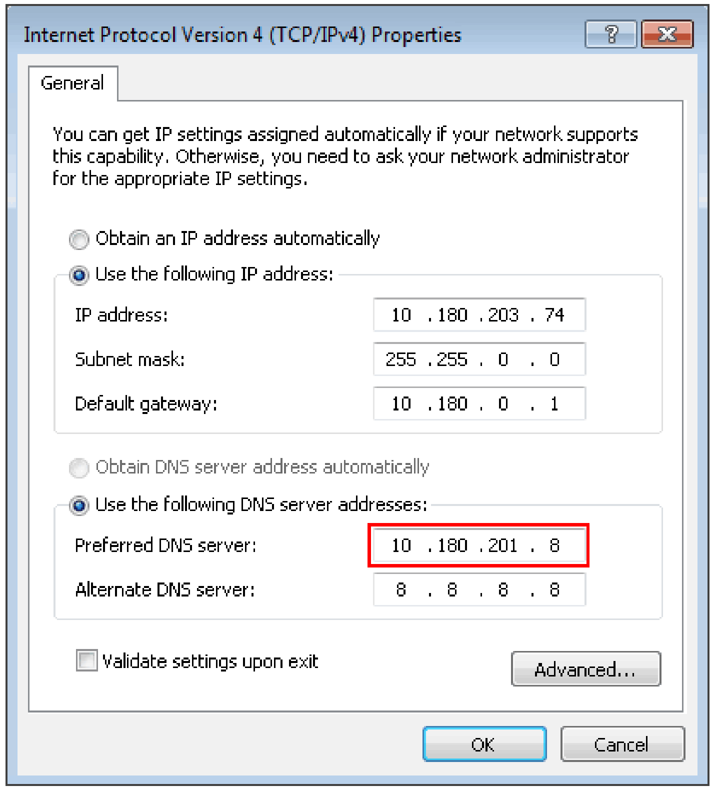
- Enter the object names to select: Domain Admins



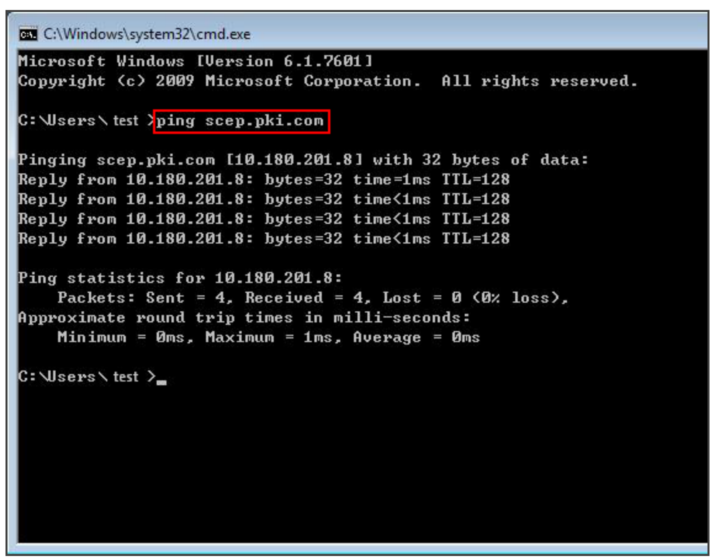
Step 2: Adding PCs of R&D staff into the AD domain (taking one PC as example).

Select **Control Panel > Network and Internet > Network and Sharing Center** to check the attribute of network connection. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, enter the Internet Protocol Version 4 (TCP/IPv4) Properties page and change the IP address of Preferred DNS server to the IP address of AD domain controller.

- Preferred DNS server: 10.180.201.8
- Alternate DNS server: 8.8.8.8



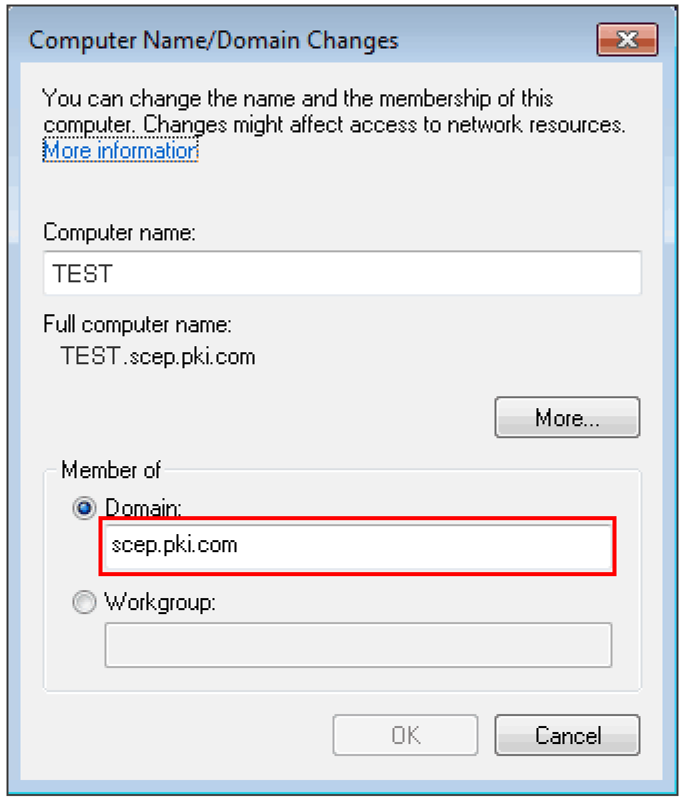
Search **cmd** in the Start menu and double-click to open the command prompt(cmd) application window, so as to make sure that the PC can be connected to the AD domain controller(scep.pki.com).



Step 2: Adding PCs of R&D staff into the AD domain (taking one PC as example).

Select **Control Panel** > **System and Security** > **System** > **Computer name, domain, and workgroup settings** > **Change settings**, and add the PC into the AD domain (scep.pki.com). Click **OK**.

- Domain: scep.pki.com



Step 2: Adding PCs of R&D staff into the AD domain (taking one PC as example).

In the **Windows security** dialog box, enter Domain name\User name and Password. The user name should be the one in the Domain Admins group.

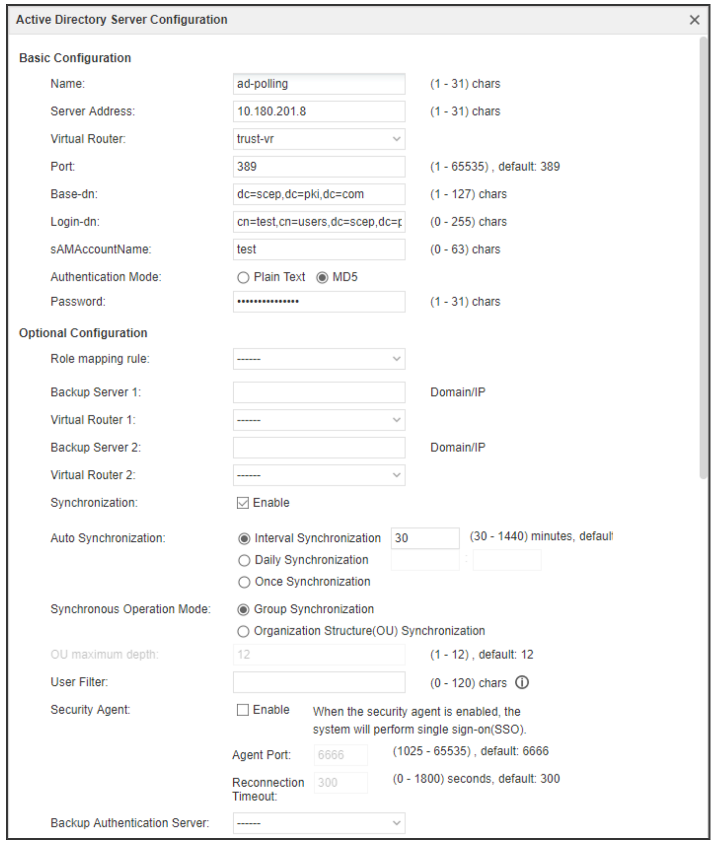
- Domain name\User name: scep\test
- Password: Hillstone123456

After the PC being added in the AD domain (scep.pki.com) successfully, restart the computer to make it take effect.

Step 3: Configuring AD server parameters in StoneOS.

Select **Object > AAA server**, and select **Active Directory Server** from the newly created drop-down list.

- Server Name: ad-polling
- Server Address: 10.180.201.8
- Base-dn: dc=scep,dc=pki,dc=com
- Login-dn: cn=test,cn=users,dc=scep,dc=pki,dc=com
- sAMAccountName: test
- Authentication Mode: MD5
- Password: Hillstone123456

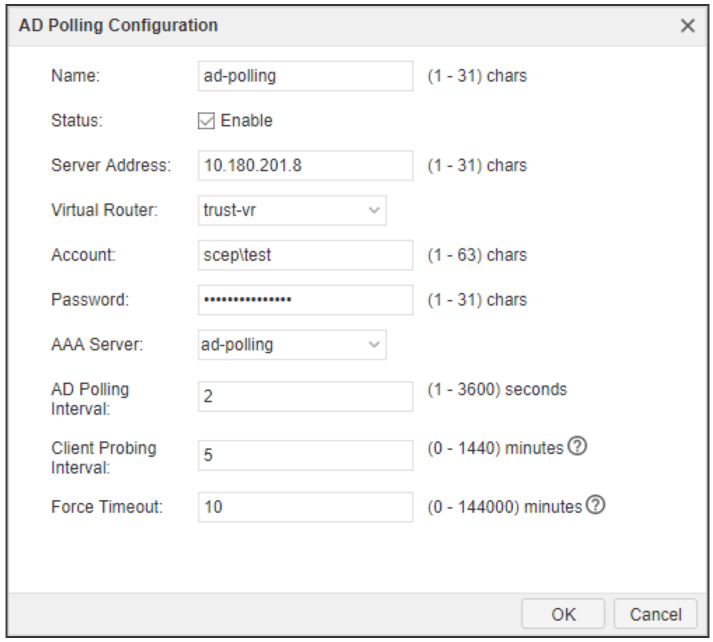


Click **OK** and the AD server is created successfully.

Step 4: Configuring AD Polling in StoneOS

Select **Object > SSO Client > AD Polling**, click **Create** and enter AD Polling Configuration page.

- Name: ad-polling
- Status: click **Enable**
- Host: 10.180.201.8
- Virtual Router: trust-vr
- Account: scep\test
- Password: Hillstone123456
- AAA Server: select the AD server **ad-polling** created in step 3
- AD Polling Interval: 2 seconds
- Client Probing Interval: 5 minutes
- Force Timeout: 10 minutes



Click **OK** to finish AD Polling configuration.

Step 5: Verifying result

After all the above configurations being finished, staff of R&D department (such as the user **test** added in AD domain in this example) can access the Internet without passing Web authentication. However, the staff of marketing department still needs to pass Web authentication before visiting the Internet.

If user needs to check the mapping information between user and IP on the device via AD Polling, you're suggested to log in the StoneOS commands operation system and enter the command **show user-mapping user-sso ad-polling** or **show auth-user**.

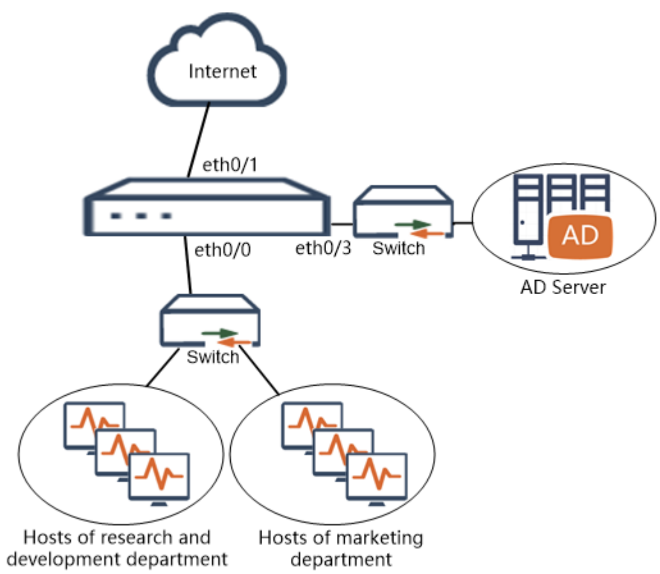
```
SG-6000# show user-mapping user-sso ad-polling ad-polling
Total entries count: 1.
=========================================================
IP/MAC            VRouter     User              life
---------------------------------------------------------
10.180.203.74     trust-vr    test              265
=========================================================
SG-6000# show auth-user
Total count: 2
Server: authentication server
Ref: reference session count
==========================================================================================
IP/MAC           Interface/VR  Username     Server     Role/Group  Ref   Live(s)  ID
------------------------------------------------------------------------------------------
3.3.3.3          trust-vr       est         local                  0       -      1
10.180.203.74    trust-vr      test         ad-poll~               0     290      23
==========================================================================================
```

As shown in the figure, in the authentication user list obtained via AD Polling, the corresponding IP of the user **test** is **10.180.203.74**.

Allowing Internet Access via AD Polling

This example introduces how to configure AD polling to allow users to access the Internet.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. All the staff in R&D department and marketing department join in the AD domain (scep.pki.com). After the AD Polling being configured, there will be login logs when staffs login though the AD server (Log in the PC which is added into the AD domain through domain user name and password). System can check the logs through AD Polling, as well as obtain authentication users information (user name and IP) on the AD server. With the user-based security policy, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.



Preparation

Before configuring the AD Polling function, prepare the following first:

- The AD server has been set up according to the user network environment.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should open the RPC service and remote management. To enable the RPC service, you need to enter the **Control Panel >**

Administrative Tools > Services and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command `netsh firewall set service RemoteAdmin`

- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security > Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- The security device should be configured with related policy to protect the AD server, which may result in the port used by WMI service (port 135 and random port) being restricted by policy. Therefore, it’s necessary to configure another policy (the source IP is the IP address of ethernet0/3) allows all interface traffic to pass through.
- The rule has been configured on the security device that all the staff of the enterprise should pass the Web authentication before they access the Internet. For the detailed configuration method, please see "Allowing the Internet Access via User Authentication" on Page 81.

Configuration Steps

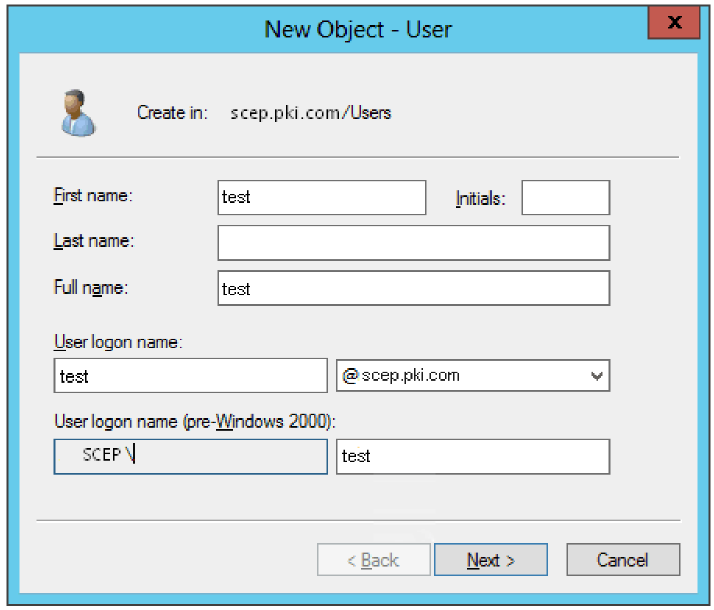
Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Access the PC with AD server, select **Start > Administrative Tools > Active Directory Users and Computers**, and enter the Active Directory Users and Computers page.

Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

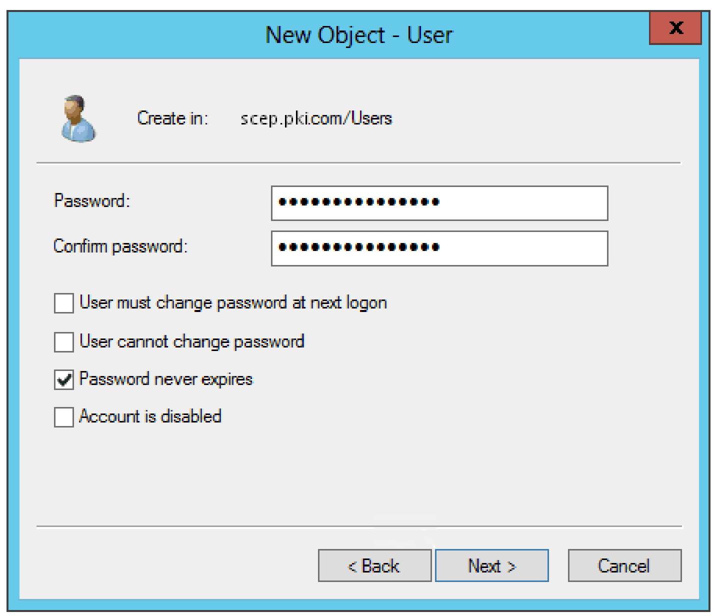
Right-click **Users** and select **New Object > User**. Click **Next**.

- First name: test
- User logon name: test@scep.pki.com



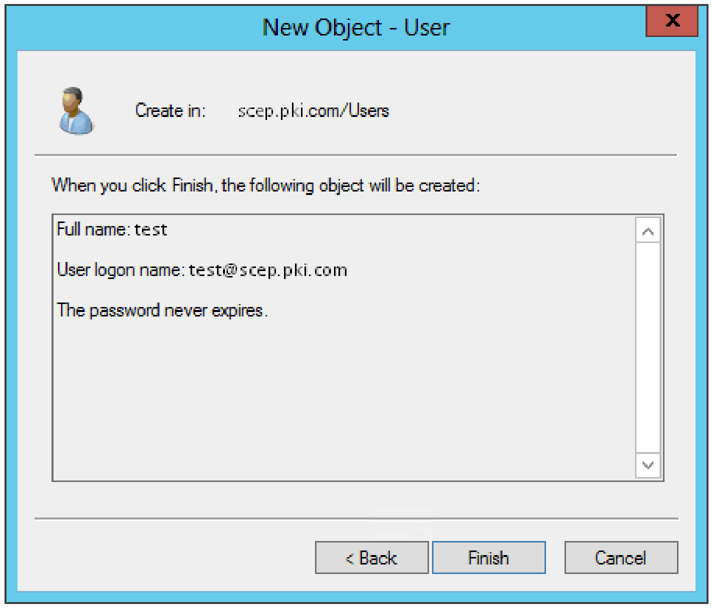
Configure a password on the **New Object- User** page, and click **Next**.

- Password: Hillstone123456
- Confirm password: Hillstone123456
- Password never expires: Select the check box



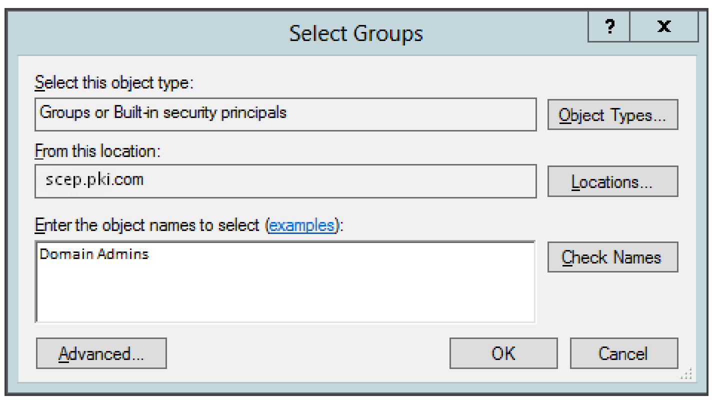
Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Click **Finish** to finish the creating of domain user **test**.



In the user list, right-click **test** and select **Add to group**. Click **OK**.

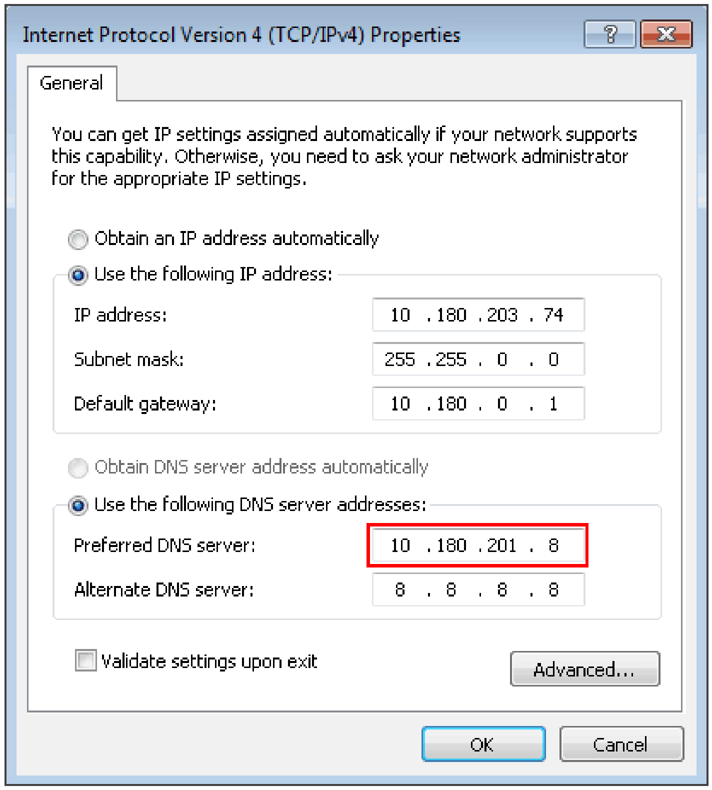
- Enter the object names to select: Domain Admins



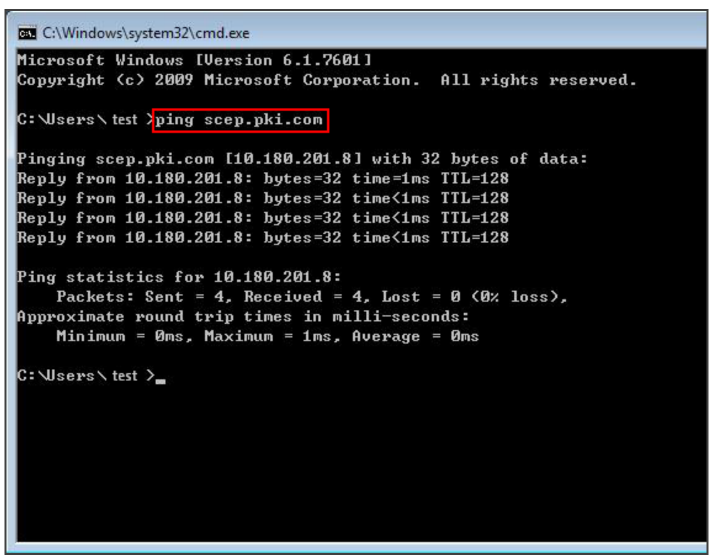
Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > Network and Internet > Network and Sharing Center** to check the attribute of network connection. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, enter the Internet Protocol Version 4 (TCP/IPv4) Properties page and change the IP address of Preferred DNS server to the IP address of AD domain controller.

- Preferred DNS server: 10.180.201.8
- Alternate DNS server: 8.8.8.8



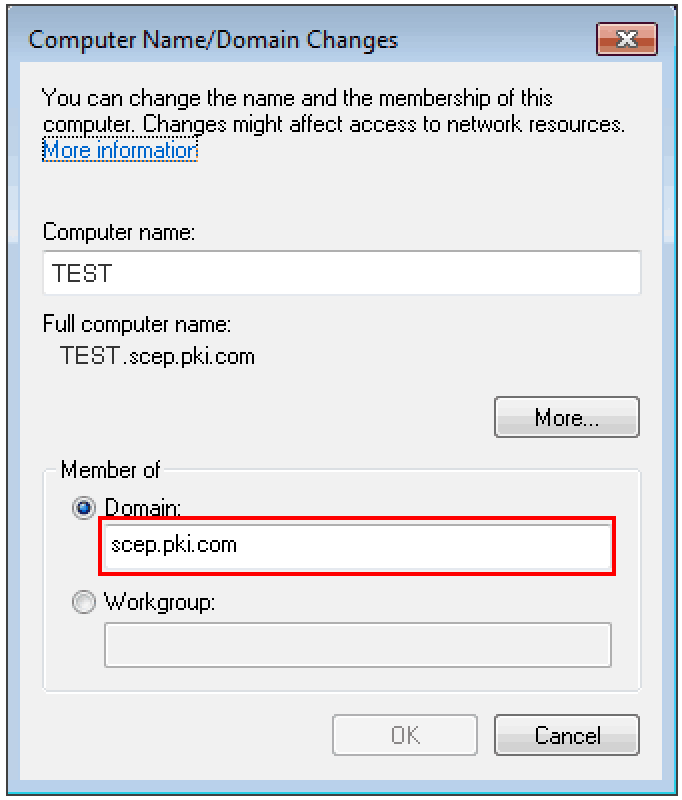
Search **cmd** in the Start menu and double-click to open the command prompt(cmd) application window, so as to make sure that the PC can be connected to the AD domain controller(scep.pki.com).



Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > System and Security > System > Computer name, domain, and workgroup settings > Change settings**, and add the PC into the AD domain (scep.pki.com). Click **OK**.

- Domain: scep.pki.com



Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

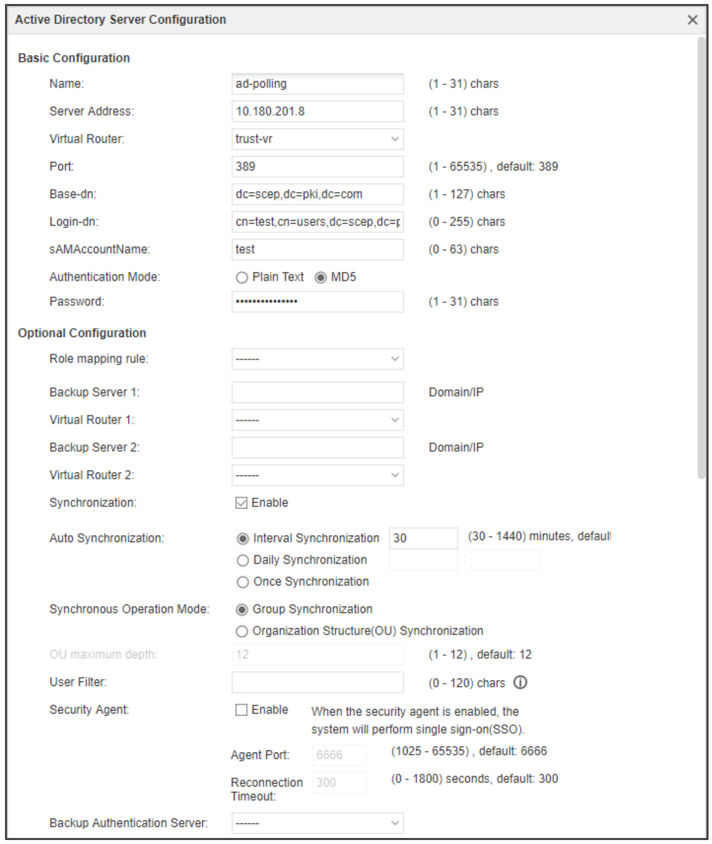
In the **Windows security** dialog box, enter Domain name\User name and Password. The user name should be the one in the Domain Admins group.

- Domain name\User name: scep\test
- Password: Hillstone123456

After the PC being added in the AD domain (scep.pki.com) successfully, restart the computer to make it take effect.

Step 3: Configure AD server parameters in StoneOS.

Select **Object > AAA server**, and select **Active Directory Server** from the newly created drop-down list.

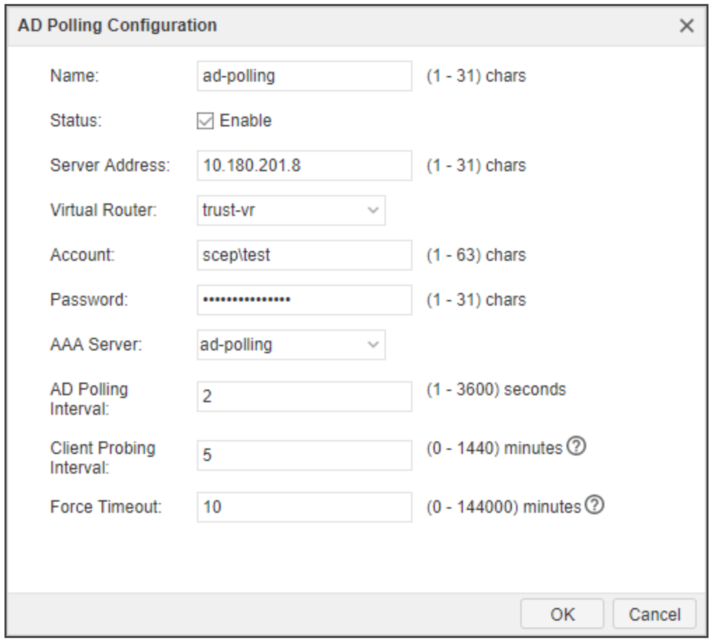


- Server Name: ad-polling
- Server Address: 10.180.201.8
- Base-dn: dc=scep,dc=pki,dc=com
- Login-dn: cn=test,cn=users,dc=scep,dc=pki,dc=com
- sAMAccountName: test
- Authentication Mode: MD5
- Password: Hillstone123456

Click **OK** and the AD server is created successfully.

Step 4: Configure AD Polling in StoneOS

Select **Object > SSO Client > AD Polling**, click **Create** and enter AD Polling Configuration page.



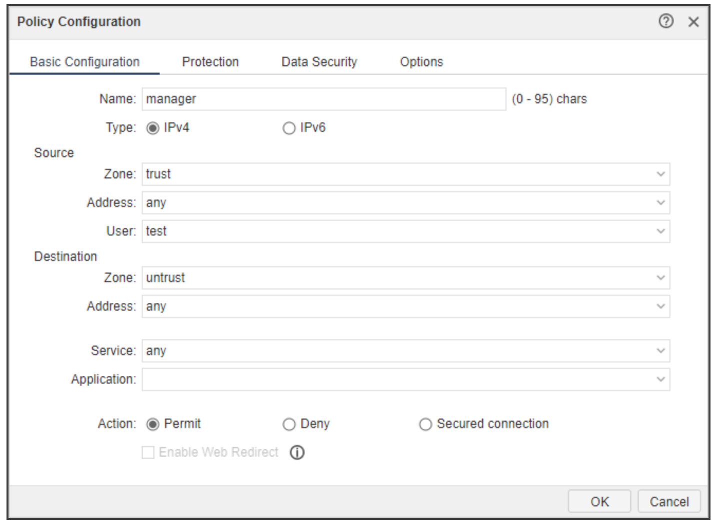
- Name: ad-polling
- Status: click **Enable**
- Host: 10.180.201.8
- Virtual Router: trust-vr
- Account: scep\test
- Password: Hillstone123456
- AAA Server: select the AD server **ad-polling** created in step 3
- AD Polling Interval: 2 seconds
- Client Probing Interval: 5 minutes
- Force Timeout: 10 minutes

Click **OK** to finish AD Polling configuration.

Step 5: Configure policies

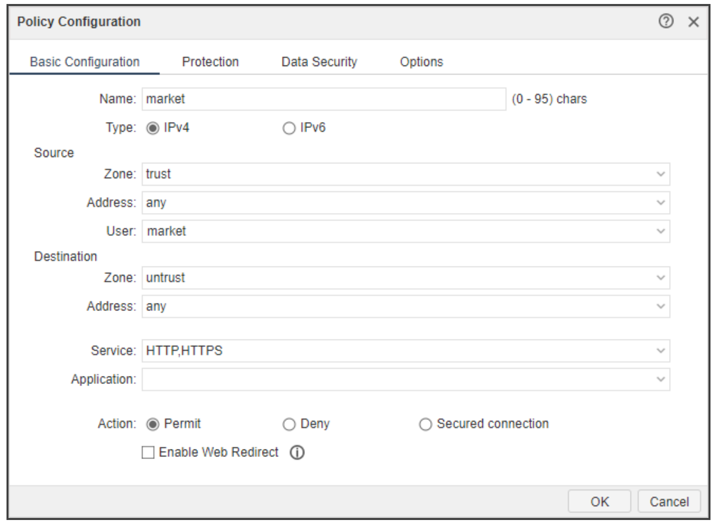
Configuring a policy to allow the manager of R&D department to access the Internet

Select **Policy > Security Policy**, and click **New**.



- Name: manager
- Source
    - Zone: trust
    - Address: any
    - User: Select the user name "test" of R&D manager
- Destination
    - Zone: untrust
    - Address: any
- Other Information
    - Action: Permit

Step 5: Configure policies



Configuring a policy to allow the staff of the marketing department to access the Web service based on HTTP or HTTPS

Select **Policy > Security Policy**, and click **New**.

- Name: market
- Source
  - Zone: trust
  - Address: any
  - User: Select the user group "market" of the marketing department
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Service: HTTP, HTTPS
  - Action: Permit

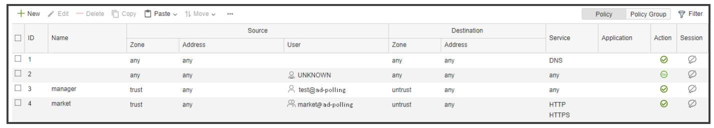
Step 5: Configure policies

Adjusting the priority of policies

1. Select **Policy > Security Policy** to enter the Security Policy page.

2. Select the check box of "manager" and "market" policies, and click **Move**.

3. Type the ID (2) of the second WebAuth policy into the **ToID** text, and click **After ID**.



New Edit Delete Copy Paste Move ... Policy Policy Group Filter

ID	Name	Source			Destination		Service	Application	Action	Session
		Zone	Address	User	Zone	Address				
1		any	any		any	any	DNS			
2		any	any	UNKNOWN	any	any	any			
3	manager	trust	any	test@ad-polling	untrust	any	any			
4	market	trust	any	market@ad-polling	untrust	any	HTTP HTTPS			

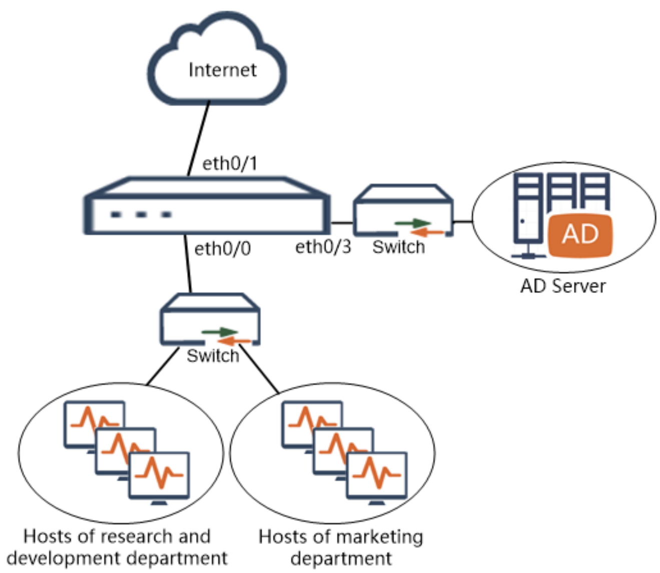
Step 6: Verify result

After all the above configurations, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.

Allowing Internet Access via AD Agent

This example introduces how to configure AD agent to allow users to access the Internet.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. All the staff in the R&D department and marketing department join in the AD domain (scep.pki.com). After the AD Agent being configured, there will be login information when staffs login though the AD server (Log in the PC which is added into the AD domain through domain user name and password). The AD Security Agent will send the authentication users information (user name and IP) to system. With the user-based security policy, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.



Preparation

Before configuring the AD Agent function, prepare the following first:

- The AD server has been set up according to the user network environment.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should open the RPC service and remote management. To enable the RPC service, you need to enter the **Control Panel >**

Administrative Tools > Services and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command `netsh firewall set service RemoteAdmin`

- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security > Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- The security device should be configured with related policy to protect the AD server, which may result in the port used by WMI service (port 135 and random port) being restricted by policy. Therefore, it's necessary to configure another policy (the source IP is the IP address of ethernet0/3) allows all interface traffic to pass through.
- The rule has been configured on the security device that all the staff of the enterprise should pass the Web authentication before they access the Internet. For the detailed configuration method, please see "Allowing the Internet Access via User Authentication" on Page 81.

Configuration Steps

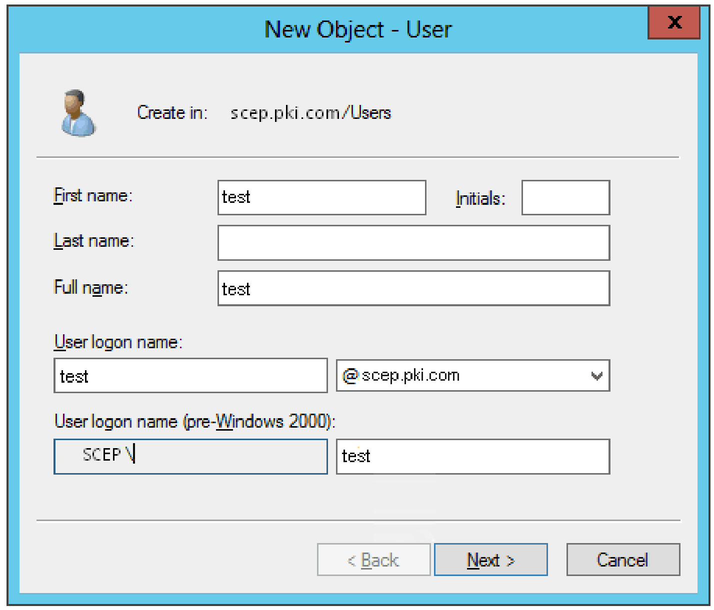
Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Access the PC with AD server, select **Start > Administrative Tools > Active Directory Users and Computers**, and enter the Active Directory Users and Computers page.

Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

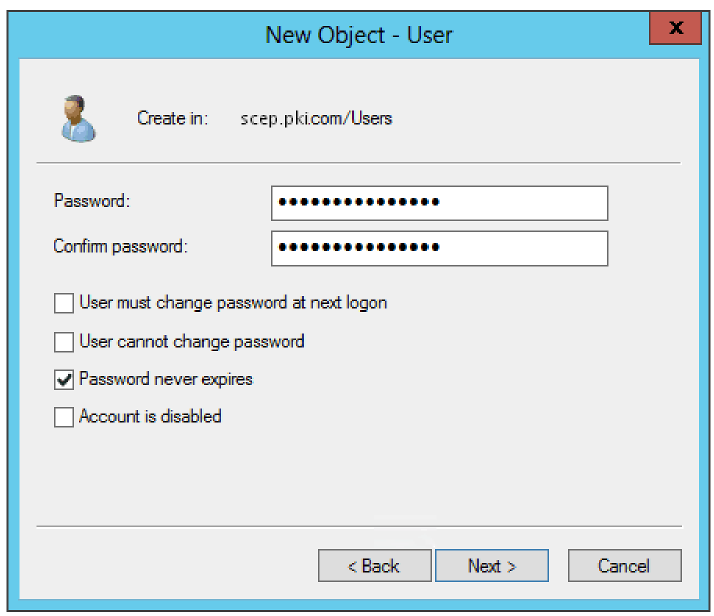
Right-click **Users** and select **New Object > User**. Click **Next**.

- First name: test
- User logon name: test@scep.pki.com



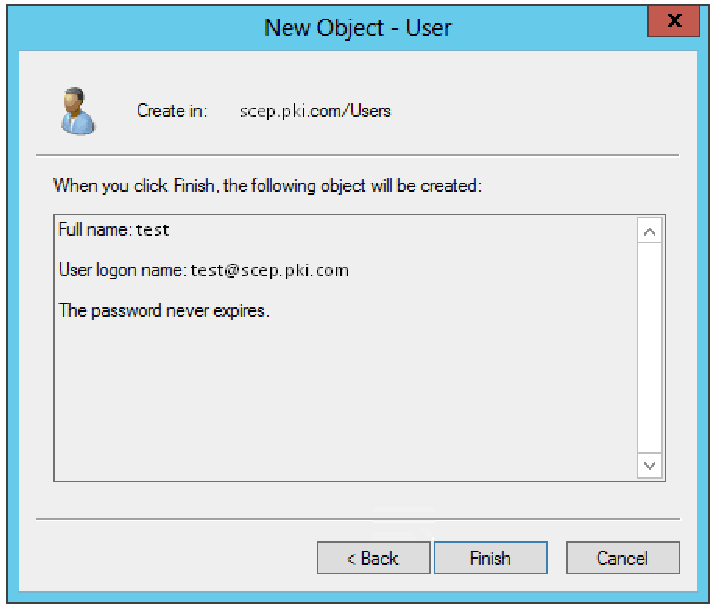
Configure a password on the **New Object- User** page, and click **Next**.

- Password: Hillstone123456
- Confirm password: Hillstone123456
- Password never expires: Select the check box



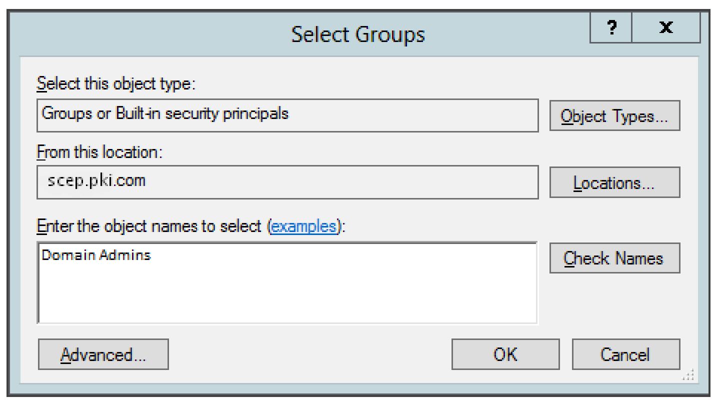
Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Click **Finish** to finish the creating of domain user **test**.



In the user list, right-click **test** and select **Add to group**. Click **OK**.

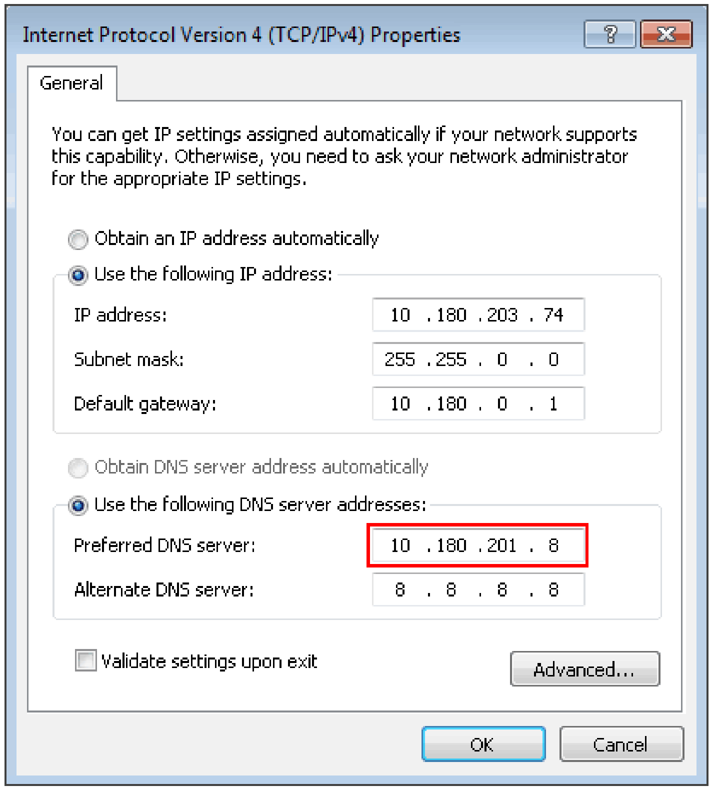
- Enter the object names to select: Domain Admins



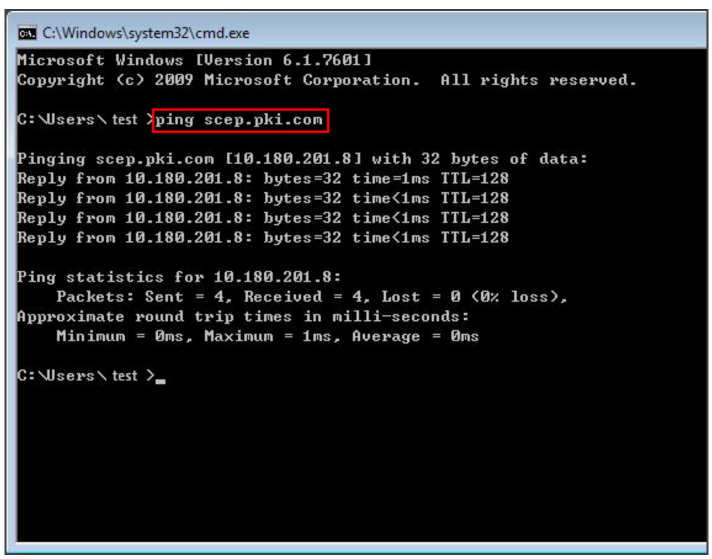
Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > Network and Internet > Network and Sharing Center** to check the attribute of network connection. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, enter the Internet Protocol Version 4 (TCP/IPv4) Properties page and change the IP address of Preferred DNS server to the IP address of AD domain controller.

- Preferred DNS server: 10.180.201.8
- Alternate DNS server: 8.8.8.8



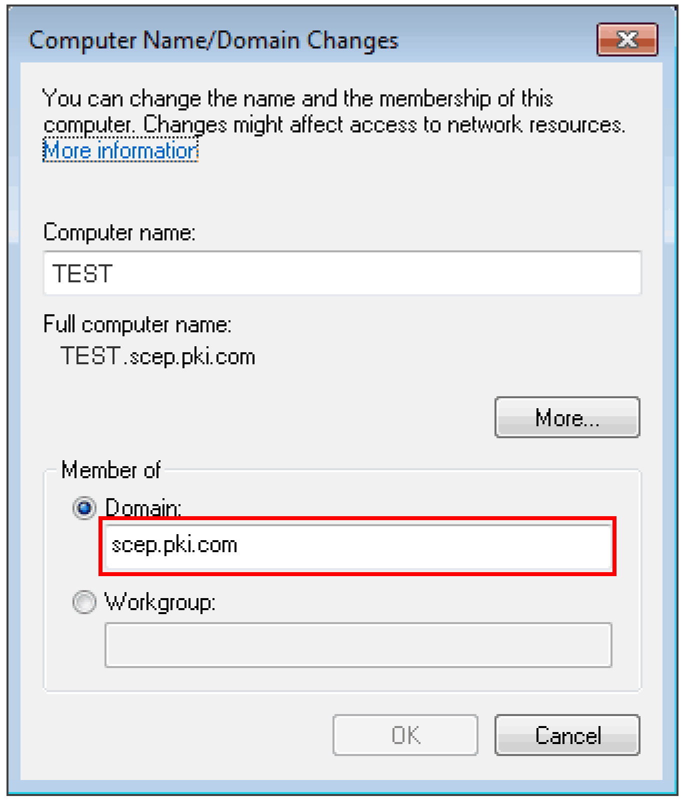
Search **cmd** in the Start menu and double-click to open the command prompt(cmd) application window, so as to make sure that the PC can be connected to the AD domain controller(scep.pki.com).



Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > System and Security > System > Computer name, domain, and workgroup settings > Change settings**, and add the PC into the AD domain (scep.pki.com). Click **OK**.

- Domain: scep.pki.com



In the **Windows security** dialog box, enter Domain name\User name and Password. The user name should be the one in the Domain Admins group.

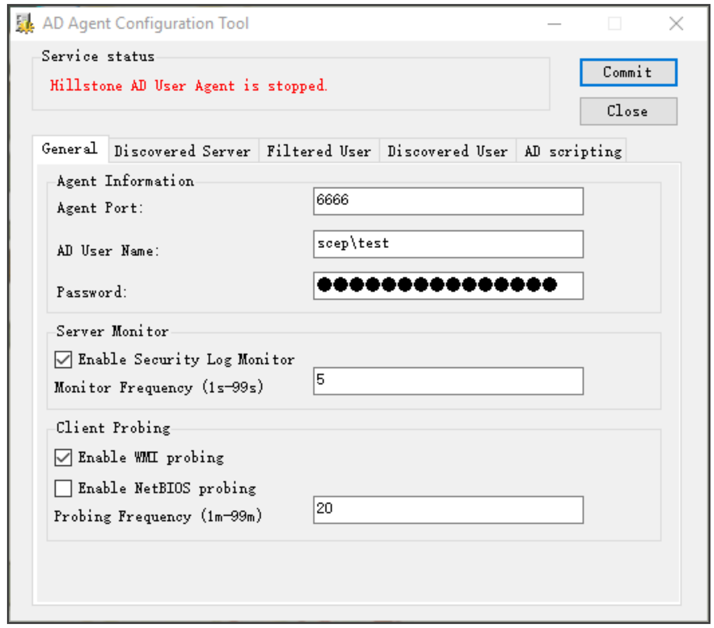
- Domain name\User name: scep\test
- Password: Hillstone123456

Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

After the PC being added in the AD domain (scep.pki.com) successfully, restart the computer to make it take effect.

Step 3: Install and configure AD Security Agent in AD server.

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-adagent to download an AD Security Agent installation program, and copy it to the AD server.
2. Double-click `ADAgentSetup.exe` to open it and follow the installation wizard to install it.
3. Double-click the `AD Agent Configuration Tool` shortcut, and the **AD Agent Configuration Tool** dialog pops up.
4. Click the **General** tab.
    - Agent Port: 6666
    - AD User Name: scep\test
    - Password: Hillstone123456
    - Server Monitor: Select the **Enable Security Log Monitor** check box, and configure the Monitor Frequency as 5 seconds
    - Client Probing: Select the **Enable WMI probing** check box, and configure the Probing Frequency as 20 minutes

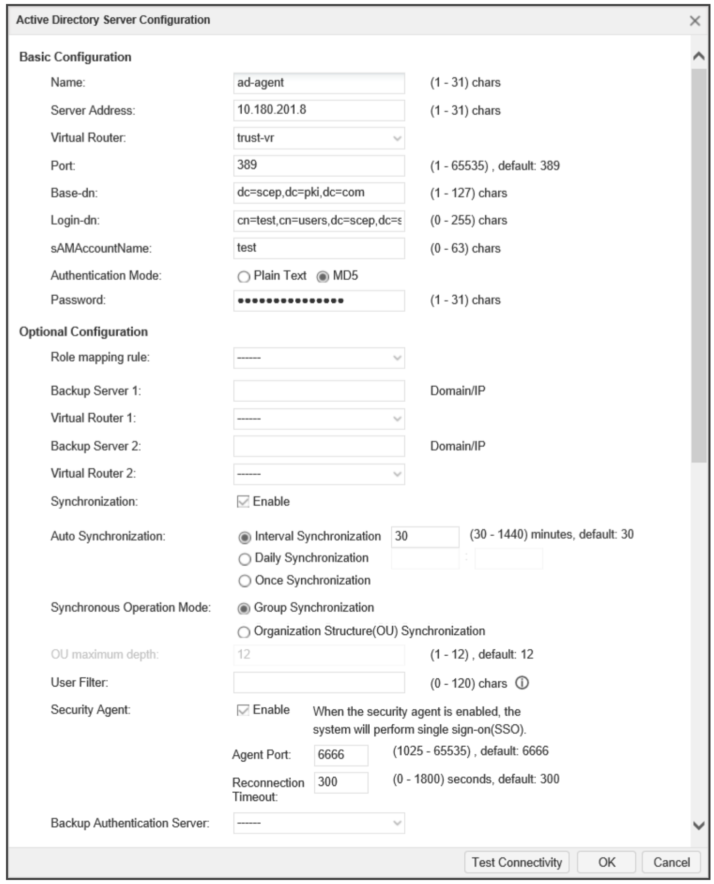


Click **Commit** to commit the above configurations and start the AD Agent service.

Step 4: Configure AD server parameters in StoneOS.

Select **Object > AAA server**, and select **Active Directory Server** from the newly created drop-down list.

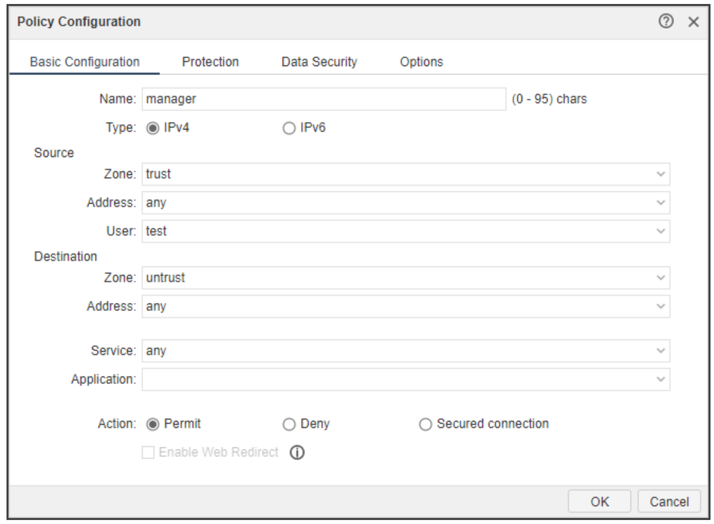
- Server Name: ad-polling
- Server Address: 10.180.201.8
- Base-dn: dc=scep,dc=pki,dc=com
- Login-dn: cn=test,cn=users,dc=scep,dc=pki,dc=com
- sAMAccountName: test
- Authentication Mode: MD5
- Password: Hillstone123456
- Security Agent: Select the check box, and configure the Agent Port as 6666



Click **OK** to finish AD server configuration.

Step 5: Configure policies

Configuring a policy to allow the manager of R&D department to access the Internet



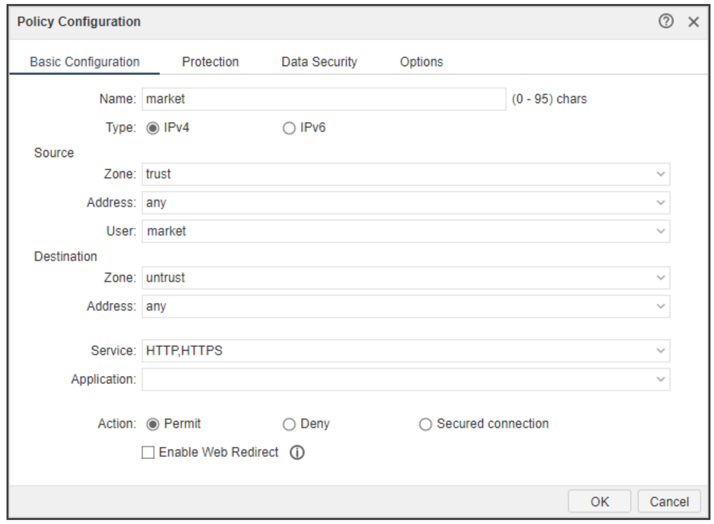
Select **Policy > Security Policy**, and click **New**.

- Name: manager
- Source
  - Zone: trust
  - Address: any
  - User: Select the user name "test" of R&D manager
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Action: Permit

Step 5: Configure policies

Configuring a policy to allow the staff of the marketing department to access the Web service based on HTTP or HTTPS

Select **Policy > Security Policy**, and click **New**.

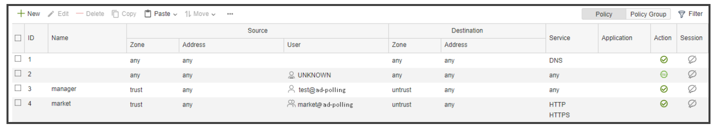


- Name: market
- Source
  - Zone: trust
  - Address: any
  - User: Select the user group "market" of the marketing department
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Service: HTTP, HTTPS
  - Action: Permit

Step 5: Configure policies

Adjusting the priority of policies

1. Select **Policy > Security Policy** to enter the Security Policy page.
2. Select the check box of "manager" and "market" policies, and click **Move**.
3. Type the ID (2) of the second WebAuth policy into the **ToID** text, and click **After ID**.



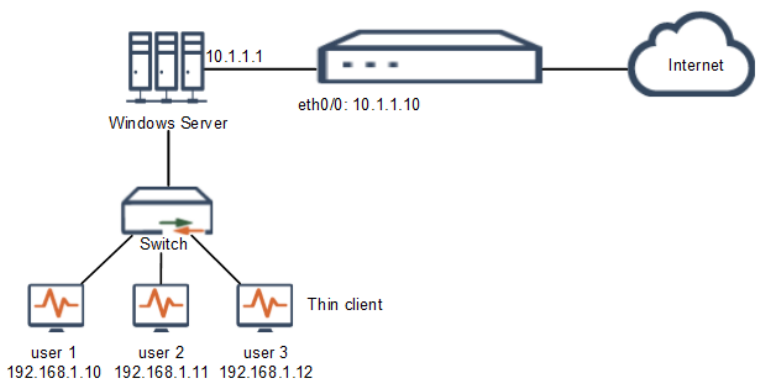
Step 6: Verify result

After all the above configurations being finished, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.

Allowing Internet Access via TS Agent

This example introduces how to configure TS Agent to allow users to access the Internet.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Internal users connect to a Windows server through thin clients. After the TS Agent is configured, when users log in the Windows server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of traffic IPs, port ranges and users. With the user-based security policy, only user 1 can access the Internet, while user 2 cannot access the Internet, and user 3 can access the Web service based on HTTP or HTTPS.



Preparation

Before configuring the TS Agent function, prepare the following first:

- The Windows server has been set up according to the user network environment. Windows Server 2008 R2, Windows Server 2016, and Windows Server 2019 are currently supported. Windows Server 2008 R2 Service Pack 1 and KB3033929 must be installed if Windows Server 2008 R2 is used.
- The SNAT rule has been configured on the security device, and all the internal users can access the Internet. For the detailed configuration method, please see "Allowing Private Network to Access Internet Using SNAT" on Page 20.

Configuration Steps

Step 1: Installing and configuring Hillstone Terminal Service Agent in Windows server.

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-tsagent to download a Hillstone Terminal Service Agent installation program, and copy it to the Windows server.

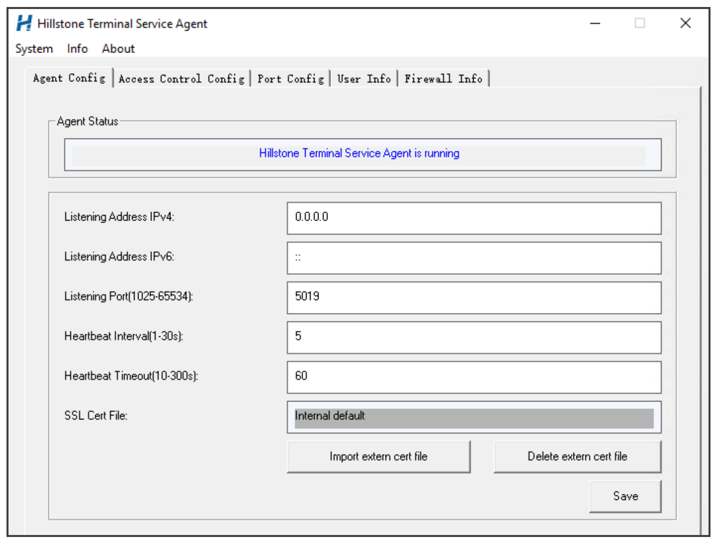
2. Double-click `HSTSAgent.exe` to open it and follow the installation wizard to install it.

3. Double-click the `Hillstone Terminal Service Agent` shortcut, and the **Hillstone Terminal Service Agent** dialog pops up.

4. Click the **Agent config** tab.

- Listening Address IPv4: 0.0.0.0
- Listening Port (1025-65534): 5019
- Heartbeat Interval (1-30s): 5
- Heartbeat Timeout (10-300s): 60

Click **Save** to save the configurations.

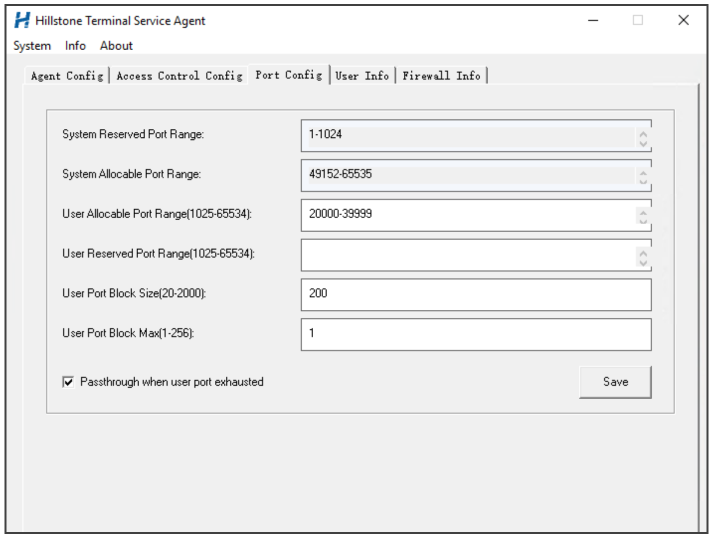


Step 1: Installing and configuring Hillstone Terminal Service Agent in Windows server.

5. Click the **Port config** tab.

- User Allocable Port Range (1025-65534): 20000-39999
- User Port Block Size (20-2000): 200
- User Port Block Max (1-256): 1
- Passthrough when user port exhausted: Select the check box

Click **Save** to save the configurations.

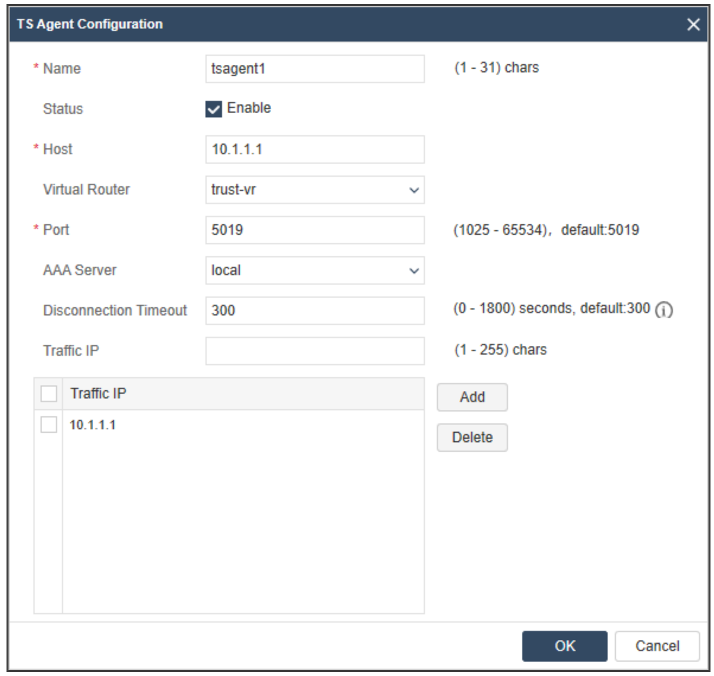


Step 2: Configuring TS Agent parameters in StoneOS via WebUI and CLI.

WebUI

Step 2: Configuring TS Agent parameters in StoneOS via WebUI and CLI.

Select **Object > SSO Client > TS Agent**, and click **New** .



- Name: tsagent1
- Status: Select the **Enable** check box
- HOST: 10.1.1.1
- Virtual Router: trust-vr
- Port: 5019
- AAA Server: local
- Disconnection Timeout: 300
- Traffic IP: Enter 10.1.1.1, and click **Add**

Click **OK** to save the configurations.

CLI

```
host-name(config)# user-sso client ts-agent tsagent1
host-name(config-ts-agent)# host 10.1.1.1
host-name(config-ts-agent)# aaa-server local
host-name(config-ts-agent)# traffic-ip 10.1.1.1
host-name(config-ts-agent)# enable
host-name(config-ts-agent)# exit
```

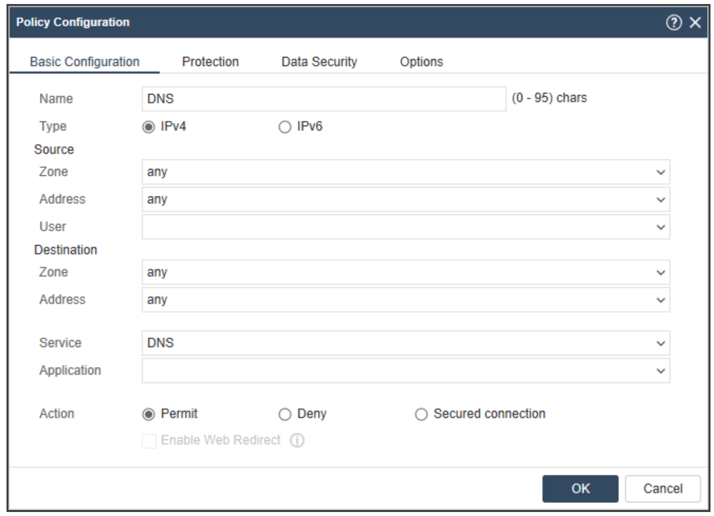
Step 3: Configuring policies in StoneOS via WebUI and CLI.

WebUI

Configuring a policy to allow all DNS traffic to get through.

Because DNS traffic is system traffic of the Windows Server, not the traffic of one specific user, configure a policy to allow all DNS traffic to get through first.

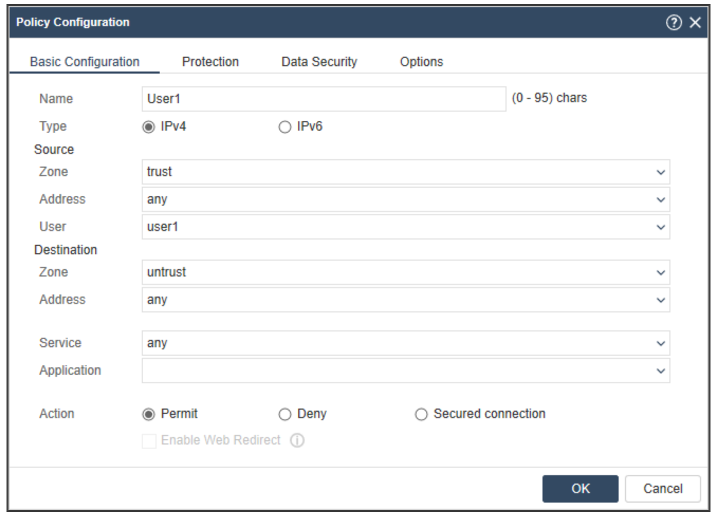
Select **Policy > Security Policy**, and click **New**.



- Name: DNS
- Source
  - Zone: any
  - Address: any
- Destination
  - Zone: any
  - Address: any
  - Service: DNS
  - Action: Permit

Step 3: Configuring policies in StoneOS via WebUI and CLI.

Configuring a policy to allow user 1 to access the Internet.



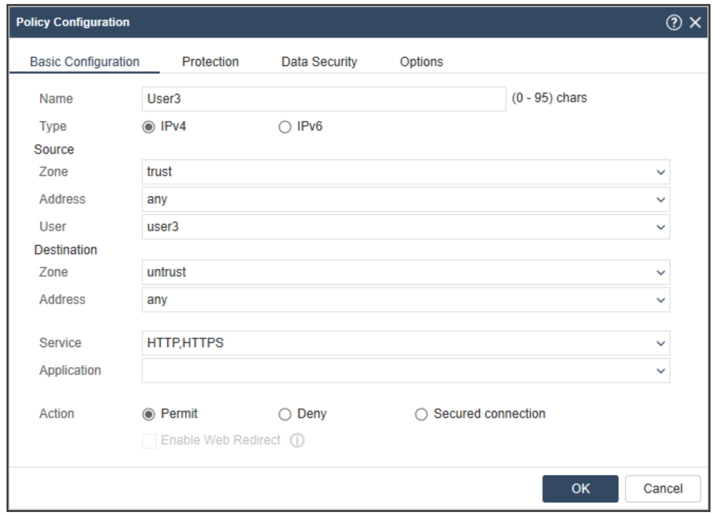
Select **Policy > Security Policy**, and click **New**.

- Name: User1
- Source
  - Zone: trust
  - Address: any
  - User: user1
- Destination
  - Zone: untrust
  - Address: any
  - Action: Permit

Step 3: Configuring policies in StoneOS via WebUI and CLI.

Configuring a policy to allow user 3 to access the Web service based on HTTP or HTTPS

Select **Policy > Security Policy**, and click **New**.



- Name: User3
- Source
  - Zone: trust
  - Address: any
  - User: user3
- Destination
  - Zone: untrust
  - Address: any
  - Service: HTTP, HTTPS
  - Action: Permit

CLI

```
host-name(config)# rule name DNS from any to any service DNS per-
mit
Rule id 2 is created.
host-name(config)# rule name User1 user local user1 from any to
any from-zone trust to-zone untrust permit
Rule id 3 is created.
host-name(config)# rule name User3 user local user3 from any to
any from-zone trust to-zone untrust service HTTP permit
Rule id 4 is created.
host-name(config)# rule id 4
host-name(config-policy-rule)# service HTTPS
host-name(config-policy-rule)# exit
```

Step 4: Verifying result

After all the above configurations are finished, only user 1 can access the Internet, while user 2 cannot access the Internet, and user 3 can access the Web service based on HTTP or HTTPS.

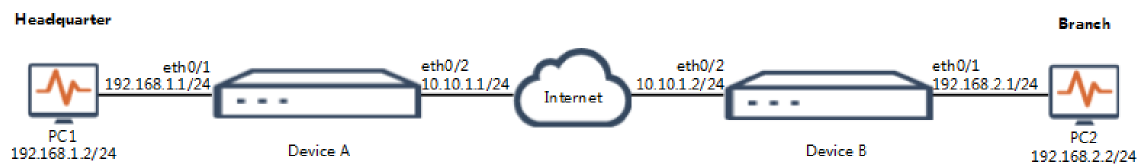
VPN

This chapter introduces virtual private network deployment.

This chapter contains the following recipes:

Connection between Two Private Networks Using IPSec VPN (IKEv1)

This example tells how to create IPSec VPN (IKEv1)tunnels to encrypt and protect the communication between two private networks . Usually, IPSec VPN tunnel is to connect the Device A in a branch office and the Device B in the headquarters.



* **Note:** This topology uses laboratory environment. In this recipe, 10.10.1.0/24 represents public network.

Configuration Steps

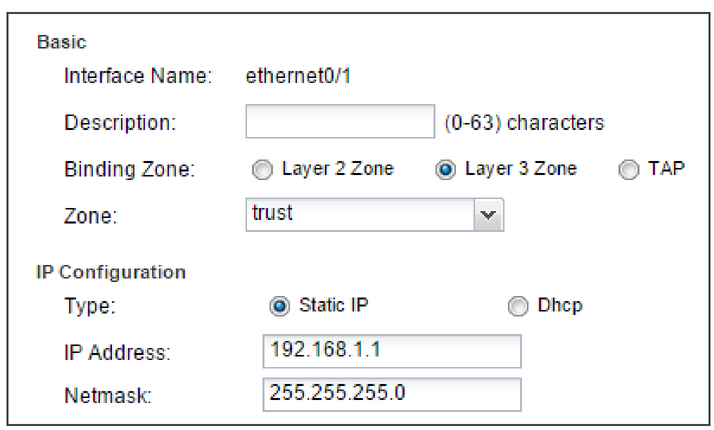
Device A

Step 1: Configuring interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.

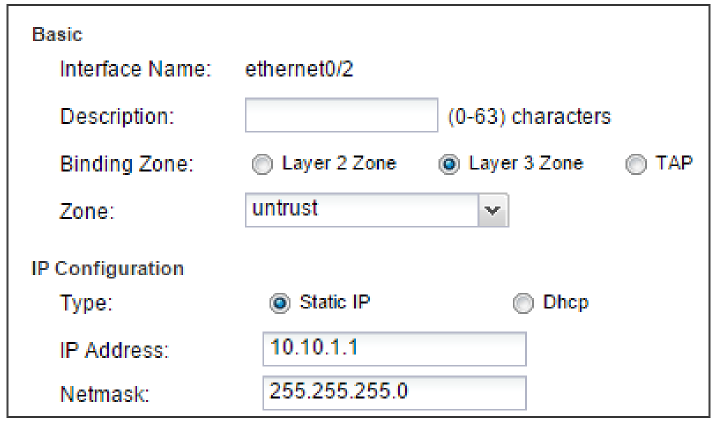
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0



Step 1: Configuring interface

2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/2.



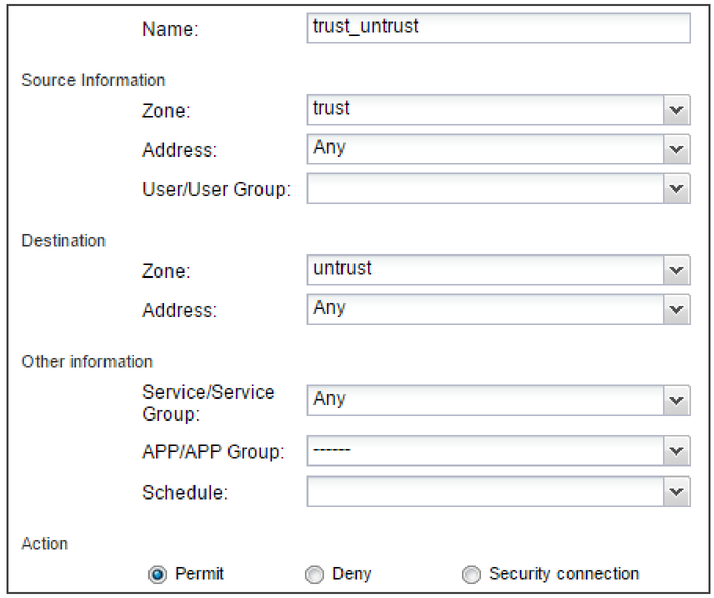
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0

Step 2: Configuring security policies

1. Creating a policy to allow private network to visit Internet

Select **Policy > Security Policy**, and click **New**.

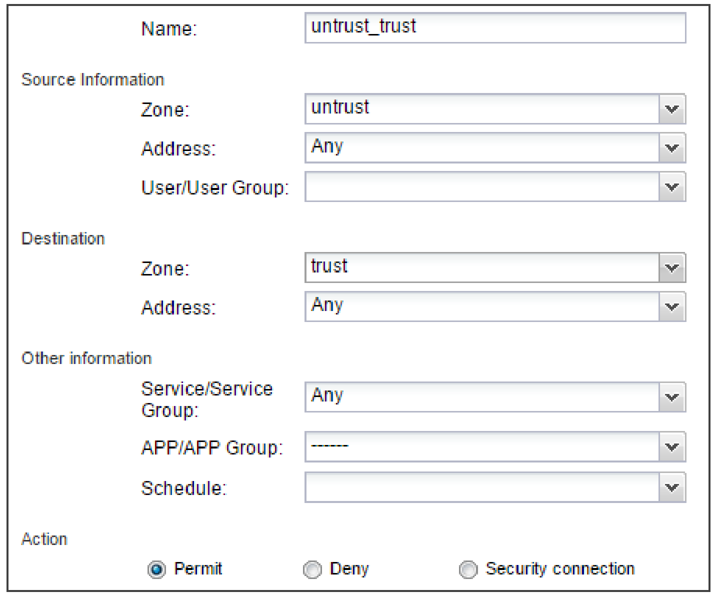
- Name: trust_untrust
- Source Information
    - Zone: trust
    - Address: Any
- Destination
    - Zone: untrust
    - Address: Any
- Other Information
    - Action: Permit



Step 2: Configuring security policies

2. Creating a security policy to allow Internet visit private network

Select **Policy > Security Policy**, and click **New**.

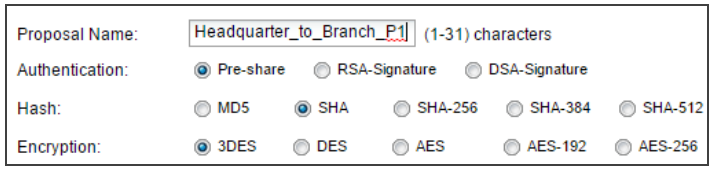


- Name: untrust_trust
- Source Information
  - Zone: untrust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other Information
  - Action: Permit

Step 3: Configuring IPSec VPN

1. Configuring P1 proposal for IKE SA

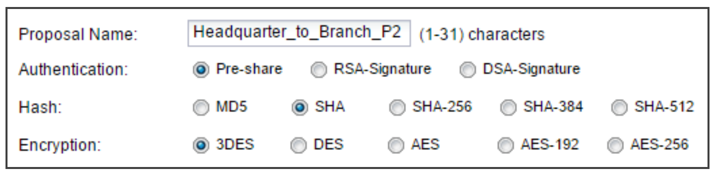
Select **Network > VPN > IPSec VPN**, under the P1 Proposal tab, click **New**.



- Proposal Name: Headquarter_to_ Branch_P1
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES

2. Configuring P2 proposal for IPSec SA

Select **Network > VPN > IPSec VPN**, under the P2 Proposal tab, click **New**.



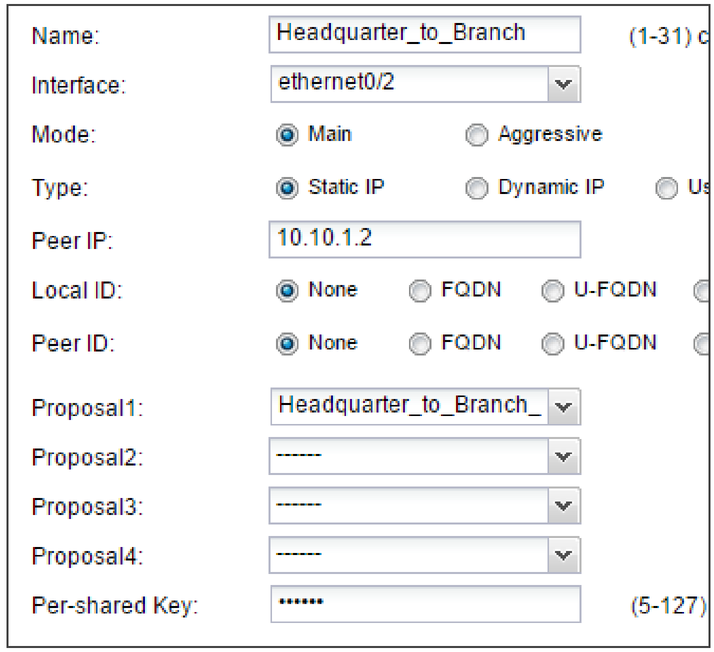
- Proposal Name: Headquarter_to_ Branch_P2
- Authentication: ESP
- Hash: SHA
- Encryption: 3DES

Step 3: Configuring IPSec VPN

3. Configuring VPN peer

Select **Network > VPN > IPSec VPN**, under the VPN Peer List tab, click **New**.

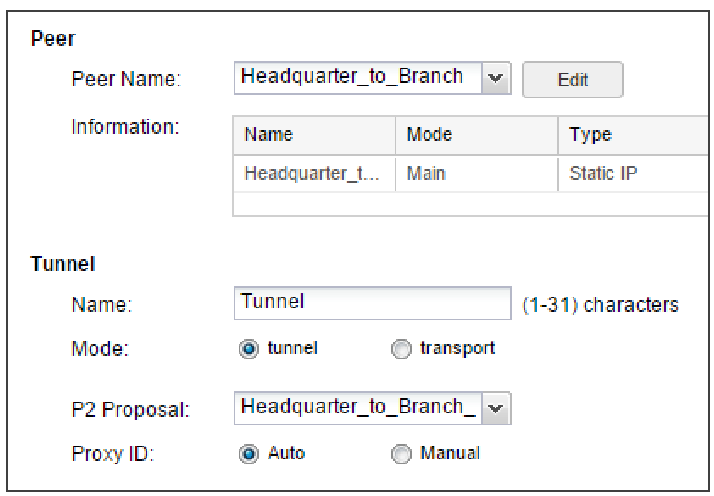
- Name: Headquarter_to_Branch
- Interface: ethernet0/2
- Mode: Main
- Type: Static IP
- Peer IP: 10.10.1.2
- Proposal 1: Headquarter_to_Branch_P1
- Pre-share Key: 123456



4. Configuring IKE VPN

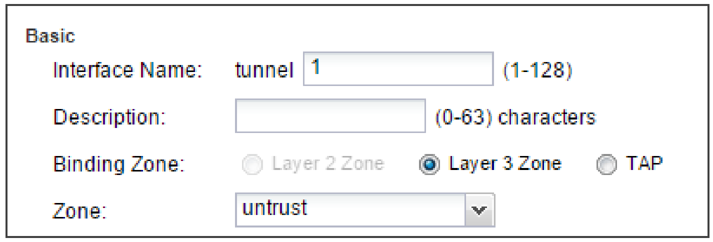
Select **Network > VPN > IPSec VPN**, under the IKE VPN List tab, click **New**.

- Peer Name: Headquarter_to_Branch
- Tunnel Name: Tunnel
- Mode: tunnel
- P2 Proposal: Headquarter_to_Branch_P2

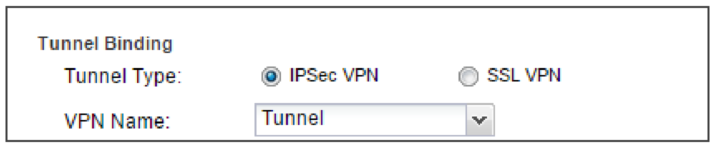


Step 4: Creating tunnel interface

Select **Network > Interface**, and click **New > Tunnel Interface**.

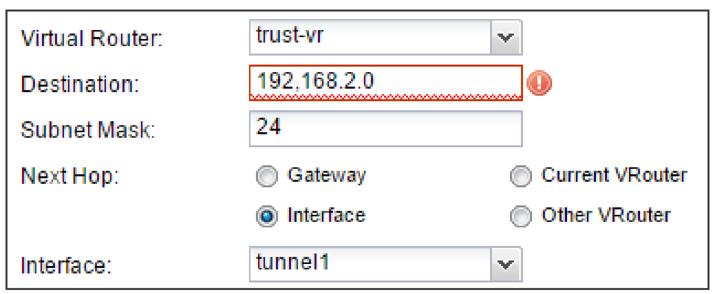


- Basic
  - Name: 1
  - Zone: untrust
- Tunnel Binding
  - Tunnel Type: IPSec VPN
  - VPN Name: Tunnel



Step 5: Configuring route

Select **Network > Routing > Destination Routing**, and click **New**.



- Destination: 192.168.2.0
- Subnet Mask: 24
- Next Hop: Interface
- Interface: tunnel1

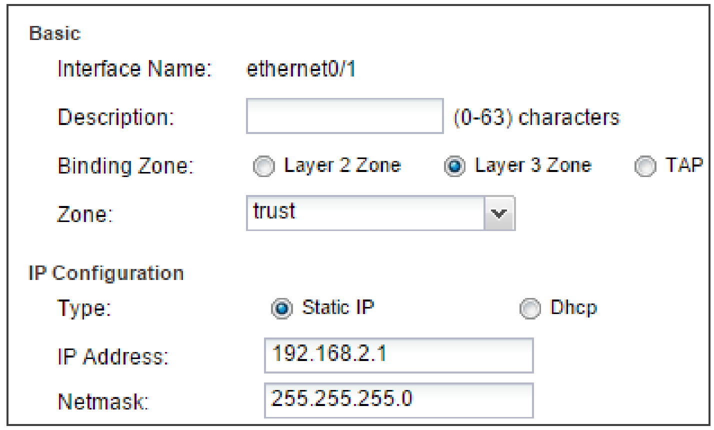
Device B

Step 1: Configuring interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.

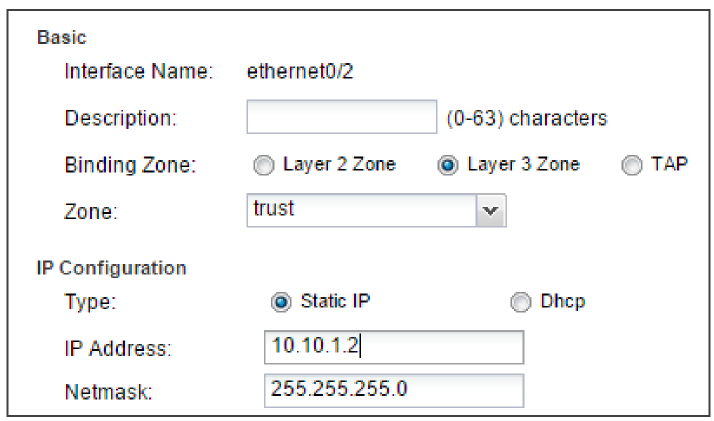
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.2.1
- Netmask: 255.255.255.0



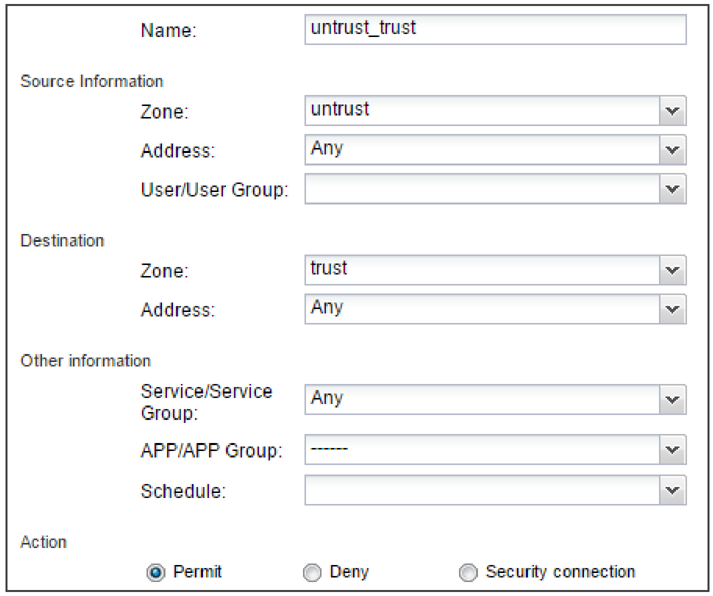
2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/2.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.2
- Netmask: 255.255.255.0



Step 2: Configuring security policies



1. Creating a policy to allow private network to visit Internet

Select **Policy > Security Policy**, and click **New**.

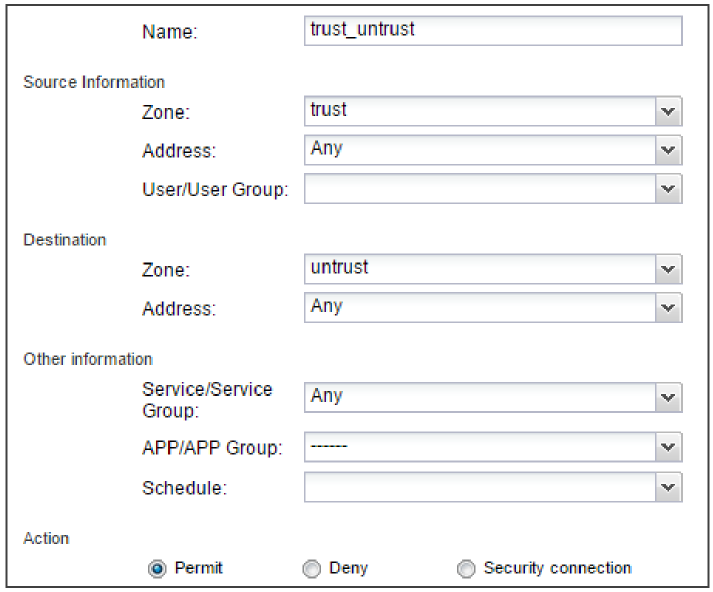
- Name: trust_untrust
- Source Information
  - Zone: trust
  - Address: Any
- Destination
  - Zone: untrust
  - Address: Any
- Other Information
  - Action: Permit

Step 2: Configuring security policies

2. Creating a security policy to allow Internet visit private network

Select **Policy > Security Policy**, and click **New**.

- Name: untrust_trust
- Source Information
  - Zone: untrust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other Information
  - Action: Permit

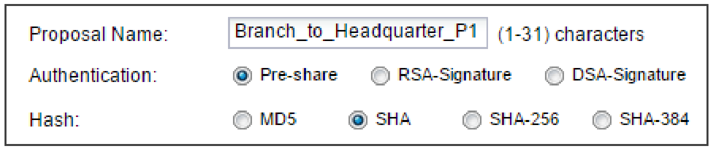


Step 3: Configuring IPSec VPN

1. Configuring P1 proposal for IKE SA

Select **Network > VPN > IPSec VPN**, under the P1 Proposal tab, click **New**.

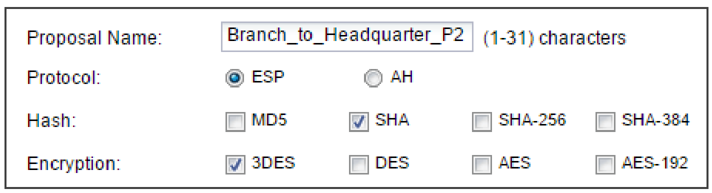
- Proposal Name: Branch_to_ Headquarter_P1
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES



2. Configuring P2 proposal for IPSec SA

Select **Network > VPN > IPSec VPN**, under the P2 Proposal tab, click **New**.

- Proposal Name: Branch_to_ Headquarter_P2
- Authentication: ESP
- Hash: SHA
- Encryption: 3DES

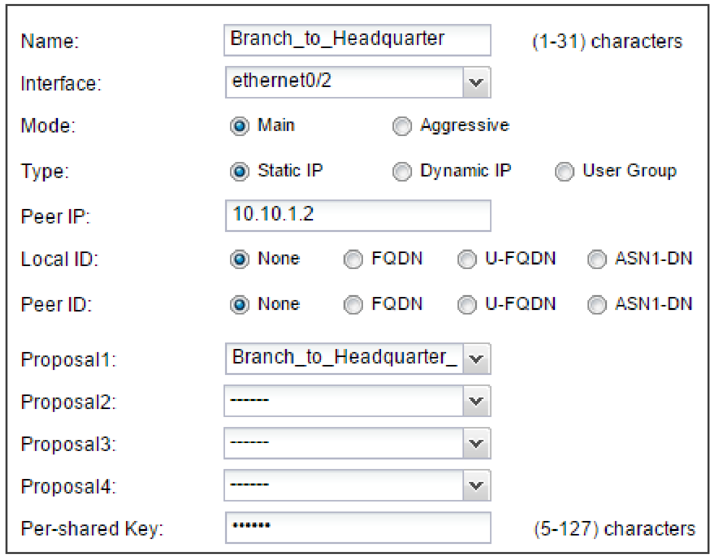


Step 3: Configuring IPSec VPN

3. Configuring VPN peer

Select **Network > VPN > IPSec VPN**, under the VPN Peer List tab, click **New**.

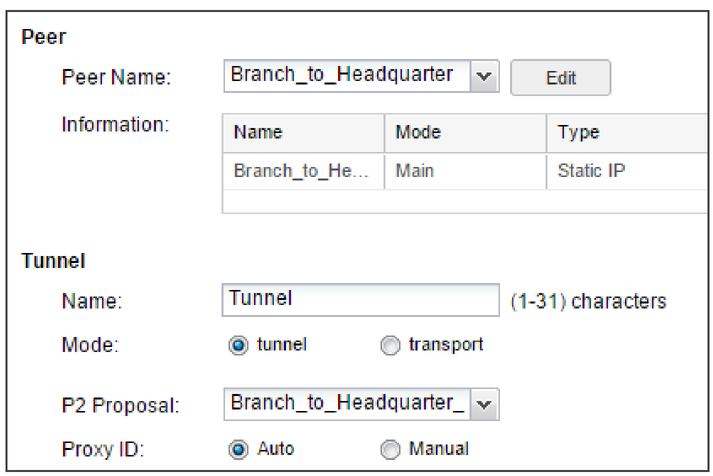
- Name: Branch_to_Headquarter
- Interface: ethernet0/2
- Mode: Main
- Type: Static IP
- Peer IP: 10.10.1.2
- Proposal 1:Branch_to_Headquarter_P1
- Pre-share Key: 123456



4. Configuring IKE VPN

Select **Network > VPN > IPSec VPN**, under the IKE VPN List tab, click **New**.

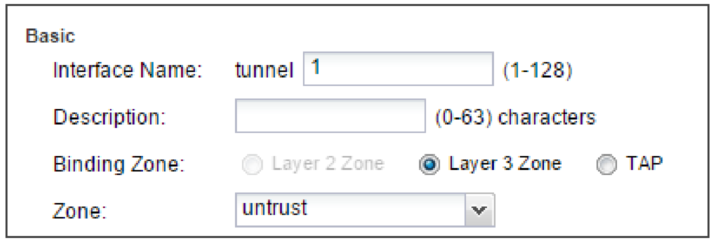
- Peer Name: Branch_to_Headquarter
- Tunnel Name: Tunnel
- Mode: tunnel
- P2 Proposal: Branch_to_Headquarter_P2

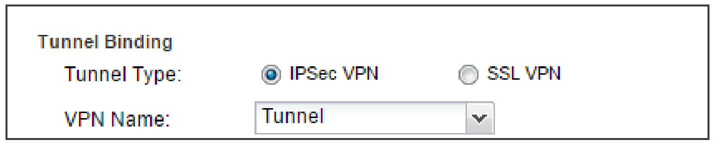


Step 4: Creating tunnel interface

Select **Network > Interface**, and click **New > Tunnel Interface**.

- Basic
  - Name: 1
  - Zone: untrust
- Tunnel Binding
  - Tunnel Type: IPSec VPN
  - VPN Name: Tunnel

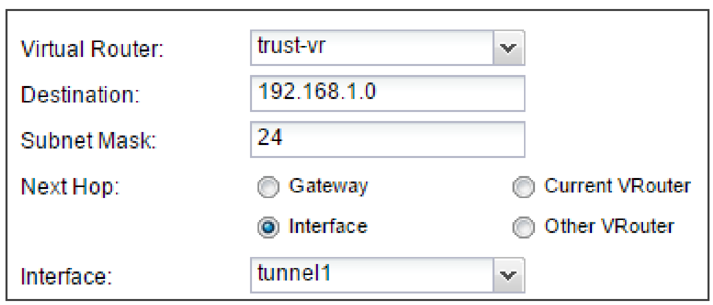




Step 5: Configuring route

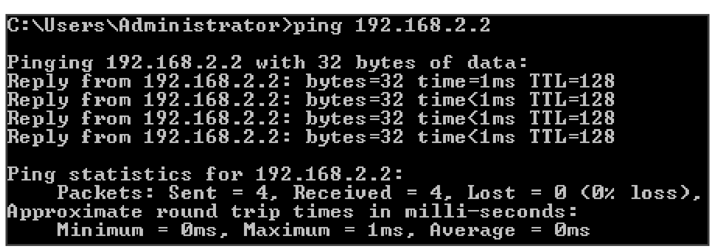
Select **Network > Routing > Destination Routing**, and click **New**.

- Destination: 192.168.1.0
- Subnet Mask: 24
- Next Hop: Interface
- Interface: tunnel1



Step 6: Results

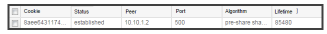
Use PC1 in the headquarters to ping PC2 in the branch. It works.



```
C:\Users\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 7: Check if IPSec VPN tunnel has been established

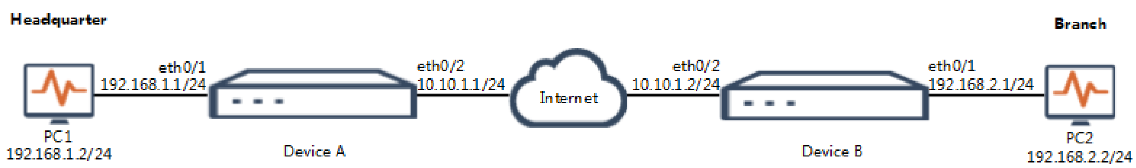
Go to **Network > VPN > IPSec VPN**, and click **IPSec VPN Monitor** on the top right corner, under the <ISAKMP SA> tab and under the IPSec SA tab, you will see the status of the tunnel.



Cookie	Status	Peer	Port	Algorithm	Lifetime
8aee6431174...	established	10.10.1.2	500	pre-share sha...	85480

Connection between Two Private Networks Using IPSec VPN (IKEv2)

This example tells how to create IPSec VPN (IKEv2) tunnels to encrypt and protect the communication between two private networks . Usually, IPSec VPN tunnel is to connect the Device A in a branch office and the Device B in the headquarters.



* **Note:** This topology uses laboratory environment. In this recipe, 10.10.1.0/24 represents public network.

Configuration Steps

Device A

Step 1: Configuring interface

```
1.Configuring the interface connected to private network.
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
2.Configuring the interface connected to Internet.
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 10.10.1.1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configuring security policies

```
hostname(config)# rule from 192.168.1.0/24 to 192.168.2.0/24 ser-
vice any permit
hostname(config)# rule from 192.168.2.0/24 to 192.168.1.0/24 ser-
vice any permit
```

Step 3: Configuring IPSec VPN

```
1.Configuring P1 proposal for IKEv2 SA.

hostname(config)# ikev2 proposal Headquarters_to_Branch_P1

hostname(config-ikev2-proposal)# hash sha

hostname(config-ikev2-proposal)# encryption 3des

hostname(config-ikev2-proposal)# group 2

hostname(config-ikev2-proposal)# exit

2.Configuring P2 proposal for IPSec IKEv2 SA.

hostname(config)# ikev2 ipsec-proposal Headquarters_to_Branch_P2

hostname(config-ikev2-ipsec-proposal)#protocol esp

hostname(config-ikev2-ipsec-proposal)#hash sha

hostname(config-ikev2-ipsec-proposal)#encryption 3des

hostname(config-ikev2-ipsec-proposal)#exit

3. Configuring IKEv2 peer.

hostname(config)# ikev2 peer peer2

hostname(config-ikev2-peer)# interface ethernet0/2

hostname(config-ikev2-peer)# match-peer 10.10.1.2

hostname(config-ikev2-peer)# local-id fqdn Headquarters

hostname(config-ikev2-peer)# ikev2-proposal Headquarters_to_
Branch_P1

4.Creating IKEv2 Profile.

hostname(config-ikev2-peer)# ikev2-profile 1

hostname(config-ikev2-profile)# remote id fqdn Branch1

hostname(config-ikev2-profile)# remote key 123456

hostname(config-ikev2-profile)# traffic-selector src subnet
```

```
192.168.1.0/24
hostname(config-ikev2-profile)# traffic-selector dst subnet
192.168.2.0/24
hostname(config-ikev2-profile)# exit
hostname(config-ikev2-peer)# exit
hostname(config)#
5.Viewing the P1 and P2 proposal information of IPsec VPN IKEv2.
hostname# show ikev2 proposal Headquarters_to_Branch_P1
Name: Headquarters_to_Branch_P1
Encryption: 3des
PRF: sha
Hash: sha
Group: 2
Lifetime: 86400
hostname# show ikev2 proposal Headquarters_to_Branch_P2
Name: Headquarters_to_Branch_P2
Protocol: esp
Encryption: 3des
Hash: sha
Group: 0
Lifetime: 28800
Lifesize: 0
```

Step 4: Creating IPsec VPN IKEv2 tunnel

```
hostname(config)# tunnel ipsec test-ikev2 ikev2
hostname(config-ikev2-tunnel)# ikev2-peer peer2
hostname(config-ikev2-tunnel)# ipsec-proposal Headquarters_to_
Branch_P2
hostname(config-ikev2-tunnel)# exit
hostname(config)#
```

Step 5 : Binding the tunnel interface to the IPsec VPN IKEv2 tunnel

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# tunnel ikev2 test-ikev2
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 6: Configuring route

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.2.0/24 tunnel1
hostname(config-vrouter)# exit
```

Device B

Step 1: Configuring interface.

```
1.Configuring the interface connected to private network.
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1/24
hostname(config-if-eth0/1)# exit
2.Configuring the interface connected to Internet.
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 10.10.1.2/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configuring security policies

```
hostname(config)# rule from 192.168.1.0/24 to 192.168.2.0/24 ser-
vice any permit
hostname(config)# rule from 192.168.2.0/24 to 192.168.1.0/24 ser-
vice any permit
```

Step 3: Configuring IPSec VPN (IKEv2).

```
1.Configuring P1 proposal for IKE SA .
hostname(config)# ikev2 proposal Branch_to_Headquarters_P1
hostname(config-ikev2-proposal)# hash sha
hostname(config-ikev2-proposal)# encryption 3des
hostname(config-ikev2-proposal)# group 2
hostname(config-ikev2-proposal)# exit
2.Configuring P2 proposal for IPSec (IKEv2) SA.
hostname(config)# ikev2 ipsec-proposal Branch_to_Headquarters_P2
hostname(config-ikev2-ipsec-proposal)#protocol esp
hostname(config-ikev2-ipsec-proposal)#hash sha
hostname(config-ikev2-ipsec-proposal)#encryption 3des
hostname(config-ikev2-ipsec-proposal)#exit
3. Configuring IKEv2 peer.
hostname(config)# ikev2 peer peer1
hostname(config-ikev2-peer)# interface ethernet0/2
hostname(config-ikev2-peer)# match-peer 10.10.1.1
hostname(config-ikev2-peer)# local-id fqdn Branch1
hostname(config-ikev2-peer)# ikev2-proposal Branch_to_Headquar-
ters_P1
4.Creating IKEv2 Profile.
hostname(config-ikev2-peer)# ikev2-profile 1
hostname(config-ikev2-profile)# remote id fqdn Headquarters
hostname(config-ikev2-profile)# remote key 123456
hostname(config-ikev2-profile)# traffic-selector src subnet
```

```
192.168.2.0/24
hostname(config-ikev2-profile)# traffic-selector dst subnet
192.168.1.0/24
hostname(config-ikev2-profile)# exit
hostname(config-ikev2-peer)# exit
hostname(config)#
5.Viewing the P1 and P2 proposal information of IPsec VPN IKEv2.
hostname# show ikev2 proposal Branch_to_Headquarters_P1
Name: Branch_to_Headquarters_P1
Encryption: 3des
PRF: sha
Hash: sha
Group: 2
Lifetime: 86400
hostname# show ikev2 proposal Branch_to_Headquarters_P2
Name: Branch_to_Headquarters_P2
Protocol: esp
Encryption: 3des
Hash: sha
Group: 0
Lifetime: 28800
Lifesize: 0
```

Step 4: Creating IPsec VPN IKEv2 tunnel .

```
hostname(config)# tunnel ipsec test-ikev2 ikev2
hostname(config-ikev2-tunnel)# ikev2-peer peer1
hostname(config-ikev2-tunnel)# ipsec-proposal Branch_to_Headquar-
ters_P2
hostname(config-ikev2-tunnel)# auto-connect
hostname(config-ikev2-tunnel)# exit
```

Step 5 : Binding the tunnel interface to the IPsec VPN IKEv2 tunnel.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# tunnel ikev2 test-ikev2
hostname(config-if-tun1)# exit
```

Step 6: Configuring route

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

Step 7: Results

Use PC1 in the headquarters to ping PC2 in the branch. It works.

```
C:\Users\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 8: Check if IPSec VPN tunnel has been established

1.With the command **show ikev2 ike-sa**, you can see that the first phase of IPsec VPN has been successfully established.

```
hostname# show ikev2 ike-sa
Total: 1
L-time - Lifetime
=================================================================-
================
Cookies Gateway Port Algorithm L-time Prof-id
-----------------------------------------------------------------
----------------
aba8467000~ 10.10.1.2 500 psk/sha/sha/3des 84972 1
=================================================================-
================
```

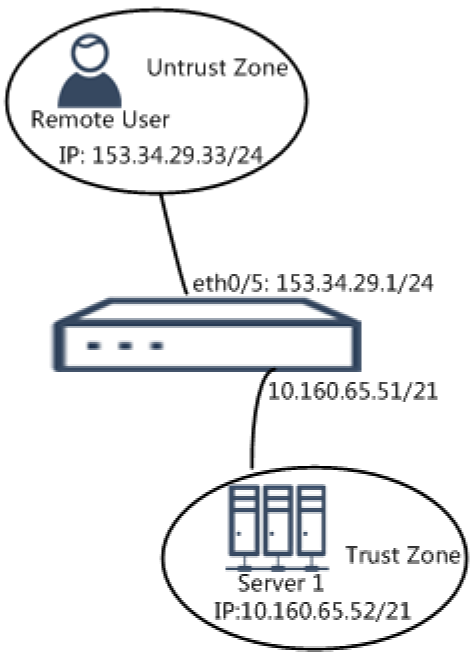
2.With the command **show ikev2 ipsec-sa**, you can see that the second phase of IPsec VPN has been successfully established.

```
hostname# show ikev2 ipsec-sa
Total: 1
S - Status, I - Inactive, A - Active;
================================================================-
================
Id VPN Peer IP Port Algorithms SPI Life(s) S
----------------------------------------------------------------
----------------
1 test-ikev2 >10.10.1.2 500 ESP:3des/sha 2c21b5d6 27355 A
1 test-ikev2 <10.10.1.2 500 ESP:3des/sha 292b6e44 27355 A
================================================================-
================
```

Allowing Remote Users to Access a Private Network Using SSL VPN

This example shows how to use SSL VPN to provide remote users with access to corporate internal network.

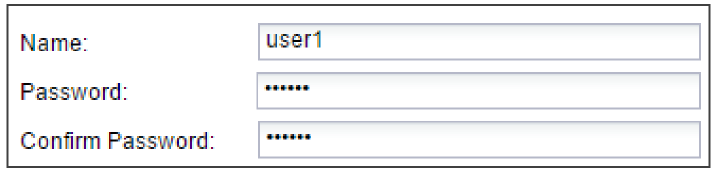
The topology describes a remote user trying to visit the internal server within a corporate. Using SSL VPN tunnel, the connection between remote users and private server is encrypted and safe.



Configuration Steps

Step 1: Creating local user

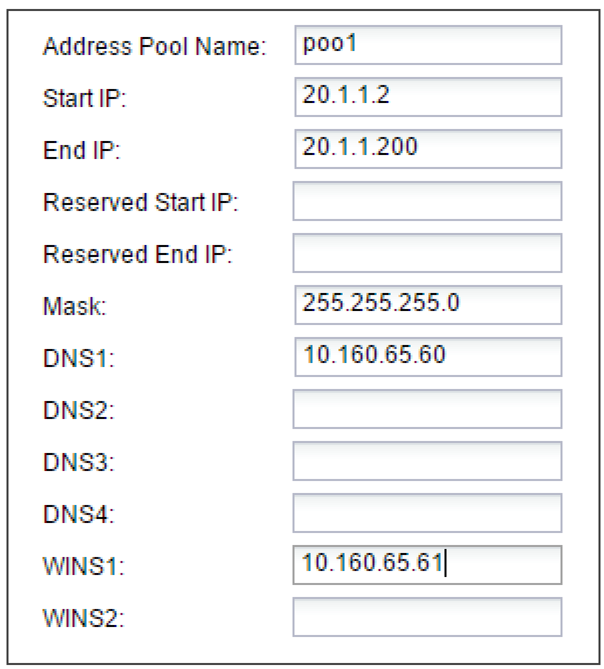
Select **Object > User**. In the Local User tab, under Local Server, click **New > User**.



- Name: user1
- Password: 123456
- Confirm Password: 123456

Step 2: Configuring SCVPN address pool

Select **Network > VPN > SSL VPN**, and click **Address Pool**. In the prompt, click **New**.

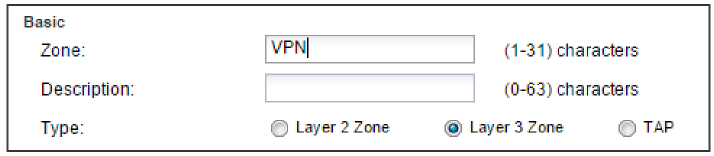


- Address Pool Name: pool1
- Start IP: 20.1.1.2
- End IP: 20.1.1.200
- Mask: 255.255.255.0
- DNS1: 10.160.65.60
- WINS1: 10.160.65.61

Step 3: Creating tunnel interface

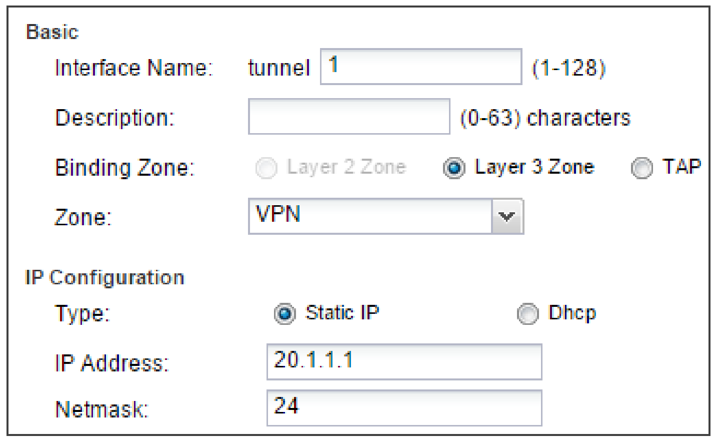
Select **Network > Zone**, and click **New**.

- Zone: VPN
- Type: Layer 3 Zone



Select **Network > Interface**, and click **New > Tunnel Interface**.

- Interface Name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: VPN
- Type: Static IP
- IP Address: 20.1.1.1
- Netmask: 24



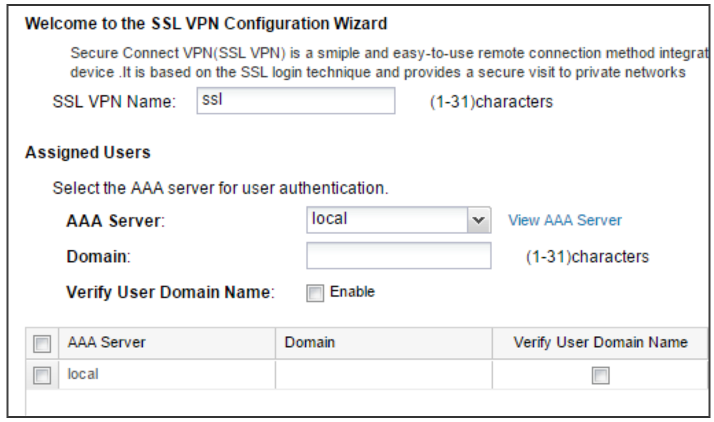
Note: Tunnel interface must be of the same network segment of SSL VPN address pool.

Step 4: Configuring SCVPN

Select **Network > VPN > SSL VPN**, and click **New**.

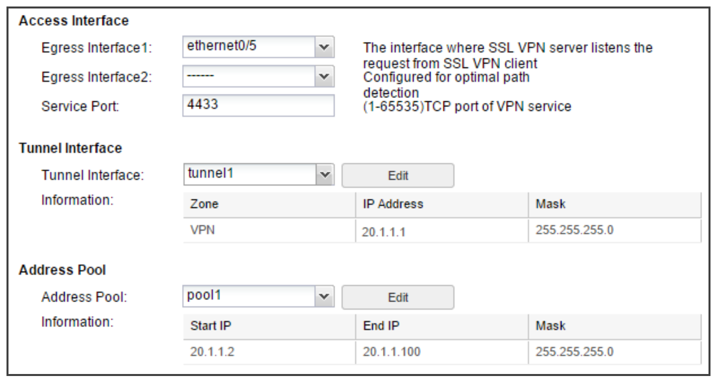
In the Name/Access User tab:

- SSL VPN Name: ssl1
- AAA Server: select **local**, and click **Add**



In the Interface tab:

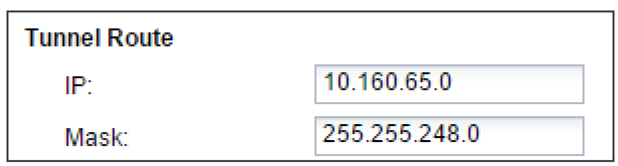
- Egress Interface 1: ethernet0/5
- Service port: 4433
- Tunnel Interface: tunnel1
- Address Pool: pool1



In the Tunnel Route tab:

- IP: 10.160.65.0
- Netmask: 255.255.248.0

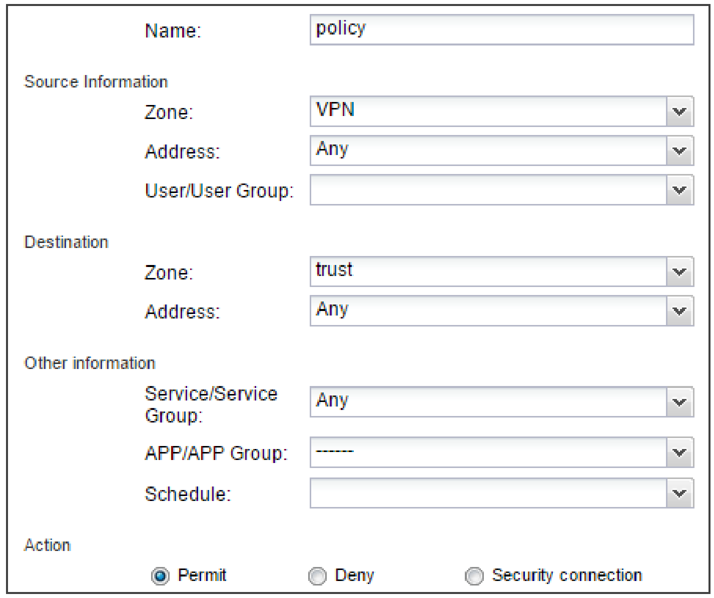
Tunnel route must be of the same network segment of internal server ("Server1")



Step 5: Creating policy from VPN to any

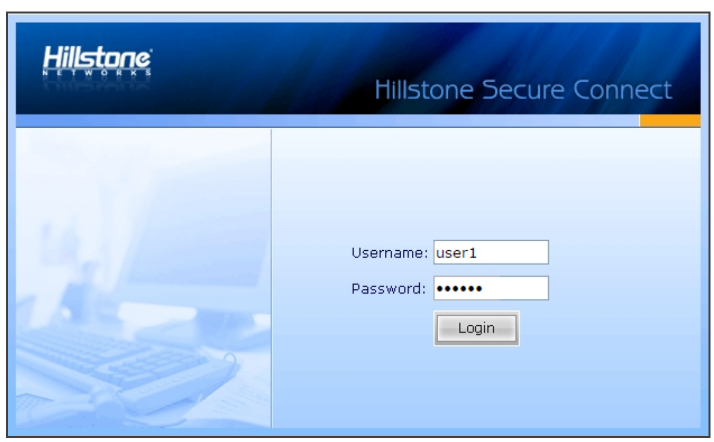
Select **Policy > Security Policy**, and click **New**.

- Name: policy
- Source Information
  - Zone: VPN
  - Address: Any
- Destination Information
  - Zone: trust
  - Address: Any
- Other Information
  - Service/Service Group: Any
- Action: Permit



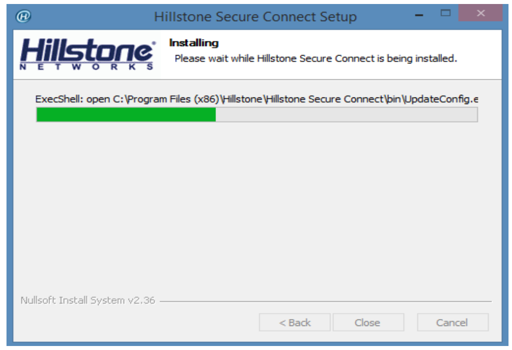
Step 6: Results

After configuration, the remote user enters address "https://153.34.29.1:4433" in a browser. The browser will show login page. Enter username and password ("user1" and "123456").



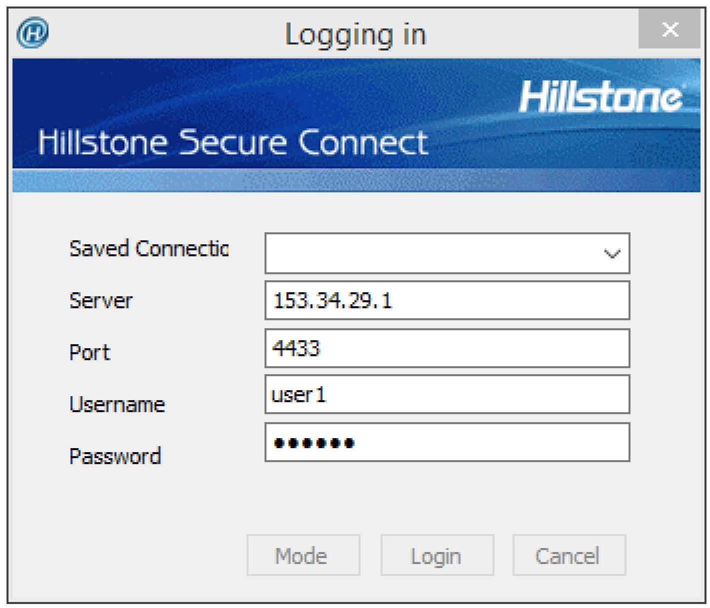
Step 6: Results

The browser will prompt to hint you to download the VPN client. Follow the steps to download and install the scvpn client.



The remote user click open the Hillstone Secure Connect client, and enter information below:

- Server: 153.34.29.1
- Port: 4433
- Username: user1
- Password: 123456



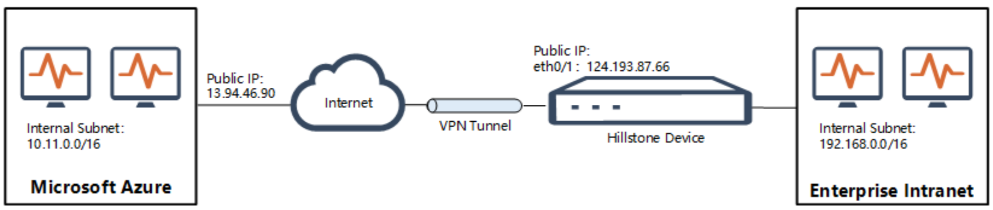
When the icon in the taskbar becomes green, the client is connected. Then, the remote user access the internal server via SSL VPN.

Connecting to Microsoft Azure Using Site-to-Site VPN

Today, more and more customers are using public cloud service providers such as Microsoft Azure to deploy their server or services, to get high performance, reliable services that are easy to deploy and get to market fastest.

This example shows how to configure site-to-site VPN to establish a VPN tunnel (IPSec VPN tunnel) between Microsoft Azure and Hillstone device.

The topology is shown as below, the Hillstone device is the gateway for the enterprise. It requires an IPsec VPN tunnel between the company and Microsoft Azure through the Hillstone device. The authentication algorithm uses SHA and the encryption algorithm uses 3DES, thus the local service can be connected with hosted cloud services.



* **Note:** This topology uses laboratory environment. In this recipe, 124.193.87.66 represents Hillstone device public IP, 192.168.0.0/16 represents the internal subnet of enterprise, 13.94.46.90 represents public IP of Microsoft Azure, 10.11.0.0/16 the internal subnet of Microsoft Azure.

The configuration process as follows:

Configure Microsoft Azure:

1. Create a virtual network
2. Create the gateway subnet
3. Create the VPN gateway
4. Create the local network gateway
5. Create the VPN connection

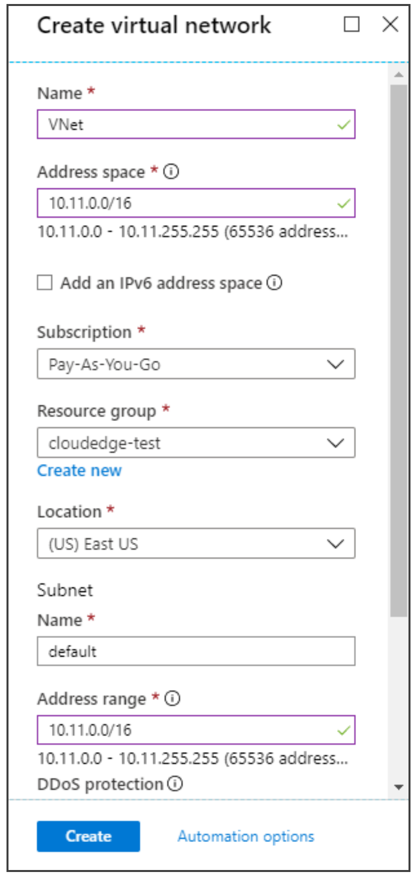
Configure Hillstone device:

1. Configuring IPSec VPN
2. Creating IPsec VPN IKEv2 tunnel
3. Binding the tunnel interface to the IPsec VPN IKEv2 tunnel
4. Configuring route

Configure Microsoft Azure

In Microsoft Azure, configure the following settings:

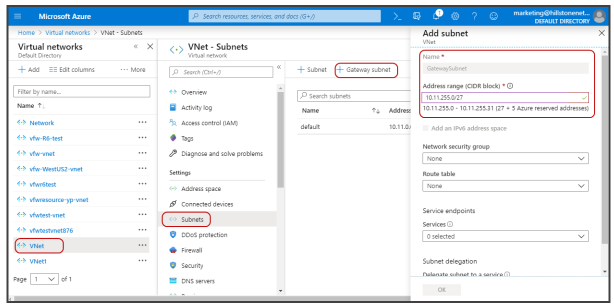
Step 1 : Create a virtual network



1. Access the Microsoft Azure website via the browser and sign in with your Azure account.
2. Click **Virtual networks** in the "Azure service" section of the Home page to open the virtual network page.
3. Click **+Add**.
4. In the **Create virtual network** page, configure the following information (take the environment in the topology as an example):
   - Name: VNet
   - Address space: 10.11.0.0/16
   - Subscription: select the existing subscription to use: “Pay-As-You-Go”
   - Resource group: cloudedge-test
   - Location: East US
   - Subnet name: default
   - Subnet address range: 10.11.0.0/16
5. Click **Create** to create the virtual network.

Step 1 : Create a virtual network

Step 2: Create the gateway subnet



1. In the list of virtual network page, select the created virtual network "VNet" in the list and click its name.

2. In the **Settings** section on the left side of the virtual network detail page, select **Subnet**.

3. In "VNet-Subnets" page. click **+Gateway subnet**.

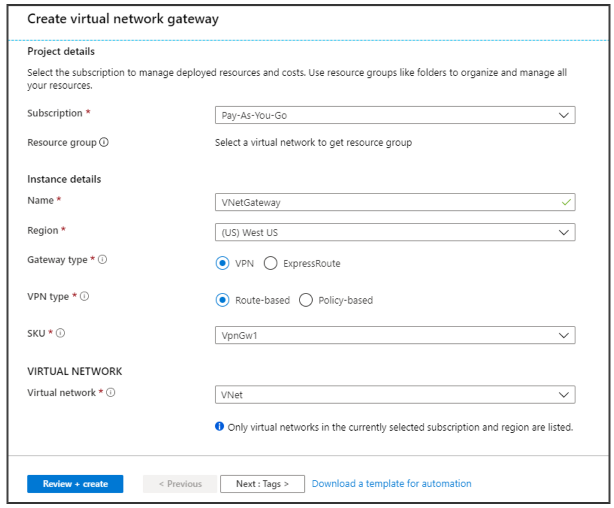
4. In **Add subnet** page, configure the following information (take the environment in the topology as an example):

    - Name: The default value "Gate-waySubnet"

    - o Address range (CIDR block): 10.11.255.0/27

5. Click **OK** to create the gateway sub-net.

Step 3: Create a VPN geteway



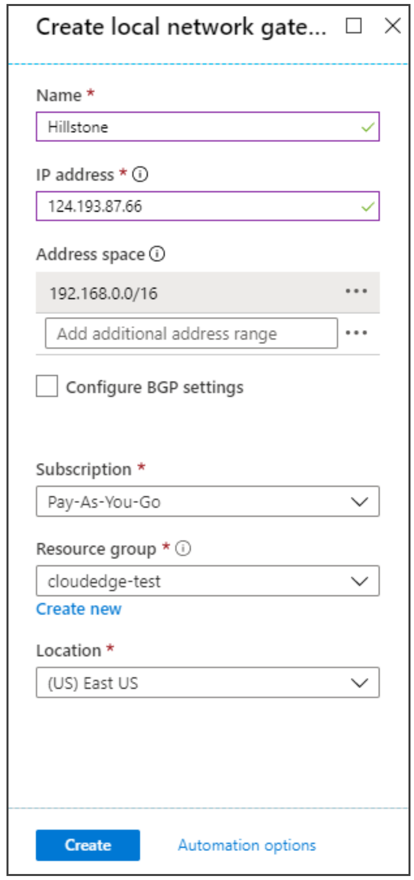
1. Click **Create a resource** in the "Azure service" section of the Home page.
2. In **Search the Marketplace field**, search **Virtual Network Gateway**.
3. Click **Create**.
4. In **Create virtual network gateway** page, configure the following information (take the environment in the topology as an example):
   - Name: VNetGateway
   - Region: West US (choose the one where your virtual network is located)
   - Gateway type: VPN
   - VPN type: Route-based
   - SKU: VpnGw1 (About SKU, refer to https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsku)
   - Virtual network: VNet (choose the one to which you want to add the gateway)

Step 3: Create a VPN geteway

- Public IP address: Create new (only dynamic Public IP address allocation is supported currently; input the public address name)
- Public IP address name: PublicIP

5. Click **Review +create** and wait for the virtual network gateway deployment. After the virtual network gateway created, the public IP address will be assigned

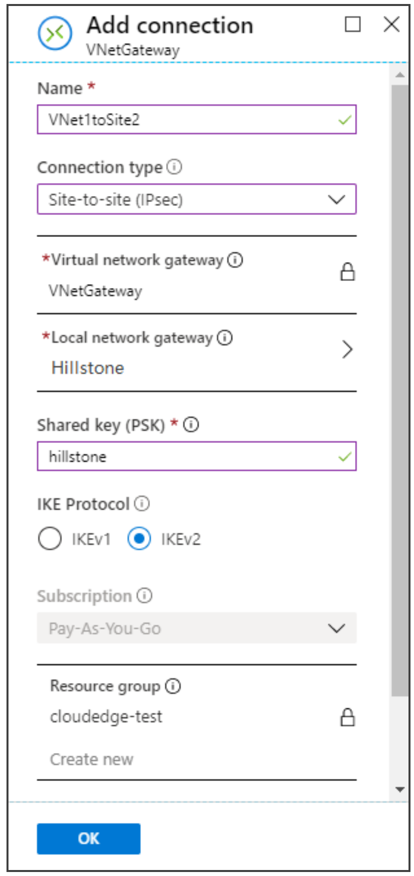
Step 4: Create the local network gateway



1. Click **Create a resource** in the "Azure service" section of the Home page.
2. In **Search the Marketplace field**, search **Local Network Gateway**
3. Click **Create**.
4. In **Create local network gateway** page, configure the following information (take the environment in the topology as an example):
   - Name: Hillstone
   - IP address: 124.193.87.66
   - Address space: 192.168.0.0/16
   - Subscription: select the existing subscription to use: "Pay-As-You-Go"
   - Resource group: cloudedge-test
   - Location: East US
5. Click **Create** to create the local network gateway.

Step 5: Create the VPN connection (This step is performed after completing the "Configure Hillstone Device")

1. Click the created virtual network gateway **VNetGateway** in the **Recent resources** list on the home page.
2. In the **Settings** section on the left side of the virtual network gateway detail page, select **Connections**
3. Click **Add**.
4. In **Add connection** page, configure the following information (take the environment in the topology as an example):
   - Name: VNet1toSite2
   - Connection type: Site-to-site (IPSec)
   - Virtual network gateway: VNetGateway
   - Loacl network gateway: Hill-stone
   - Shared key (PSK): hillstone (Consistent with "Configure Hillstone Device")
   - Resource group: cloudedge-test



Step 5: Create the VPN connection (This step is performed after completing the "Configure Hillstone Device")

5. Click **OK** to create the connection.

Note:

- About VPN devices and IPsec/IKE parameters for Site-to-Site VPN Gateway connections, refer to the Microsoft Azure documentation: https://docs.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-about-vpn-devices.
- About "Create a Site-to-Site connection in the Azure portal", refer to the Microsoft Azure documentation: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal.

Configure Hillstone Device

Step 1: Configuring IPSec VPN

```
1.Configuring P1 proposal for IKEv2 SA.
hostname(config)# ikev2 proposal Azure_to_Hillstone_P1
hostname(config-ikev2-proposal)# hash sha
hostname(config-ikev2-proposal)# encryption 3des
hostname(config-ikev2-proposal)# group 2
hostname(config-ikev2-proposal)# lifetime 10800
hostname(config-ikev2-proposal)# exit
2.Configuring P2 proposal for IPSec IKEv2 SA.
hostname(config)# ikev2 ipsec-proposal Azure_to_Hillstone_P2
hostname(config-ikev2-ipsec-proposal)#hash sha
hostname(config-ikev2-ipsec-proposal)#encryption aes
hostname(config-ikev2-ipsec-proposal)#lifetime 3600
hostname(config-ikev2-ipsec-proposal)#exit
3. Configuring IKEv2 peer.
hostname(config)# ikev2 peer peer1
hostname(config-ikev2-peer)# interface ethernet0/1
hostname(config-ikev2-peer)# match-peer 13.94.46.90
hostname(config-ikev2-peer)# ikev2-proposal Azure_to_Hillstone_
P1
hostname(config-ikev2-peer)# local-id ip 124.193.87.66
4.Creating IKEv2 Profile.
hostname(config-ikev2-peer)# ikev2-profile esp-peer1
hostname(config-ikev2-profile)# remote id ip 13.94.46.90
hostname(config-ikev2-profile)# remote key hillstone
```

```
hostname(config-ikev2-profile)# traffic-selector src subnet
192.168.0.0/16
hostname(config-ikev2-profile)# traffic-selector dst subnet
10.11.0.0/16
hostname(config-ikev2-profile)# exit
hostname(config-ikev2-peer)# exit
hostname(config)#
```

Step 2: Creating IPsec VPN IKEv2 tunnel

```
hostname(config)# tunnel ipsec Azure ikev2
hostname(config-ikev2-tunnel)# ikev2-peer peer1
hostname(config-ikev2-tunnel)# ipsec-proposal Azure_to_Hill-
stone_P2
hostname(config-ikev2-tunnel)# auto-connect
hostname(config-ikev2-tunnel)# exit
hostname(config)#
```

Step 3 : Binding the tunnel interface to the IPsec VPN IKEv2 tunnel

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# tunnel ikev2 Azure
hostname(config-if-tun1)# exit
hostname(config)#
```

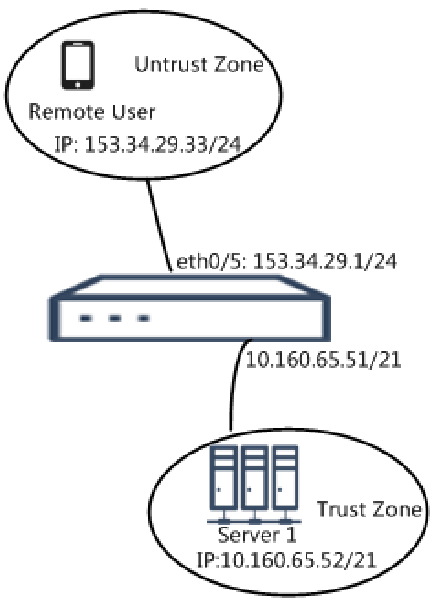
Step 4: Configuring route

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 10.11.0.0/16 tunnel1

hostname(config-vrouter)# exit
```

Using an iOS/Android Device to Remotely Access Intranet Services

This example introduces how to use an iOS/Android device to remotely access the resources in the private network.

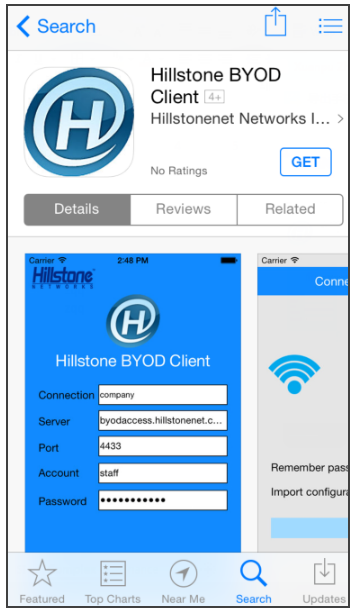
In the topology below, a remote user located in the Internet uses an iOS/Android device to access the intranet server **Server1**. The authentication method requires username and password, and the connection is based on SSL VPN. Please first see step 1 to 5 in "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 157 to create a SSL VPN instance.



Using an iOS Device to Remotely Access Intranet Services

Step 1: Downloading and installing Hillstone BYOD Client

In APP Store, search Hillstone BYOD Client, click **Get** to download and install this application.



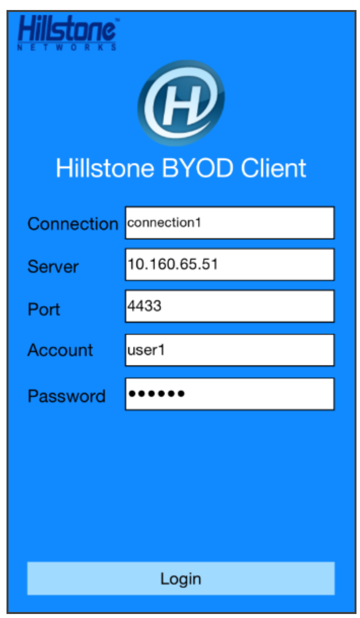
Step 2: Connecting to the device

Click the HBC icon in the iOS desktop.

In the login page:

- Connection: connection1
- Server: 153.34.29.1
- Port: 4433
- Account: user1
- Password: 123456

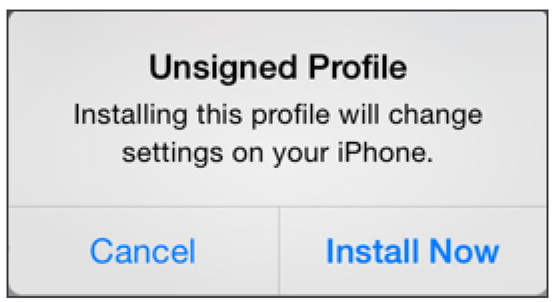
Click **Login**. The client starts to connect to the server.



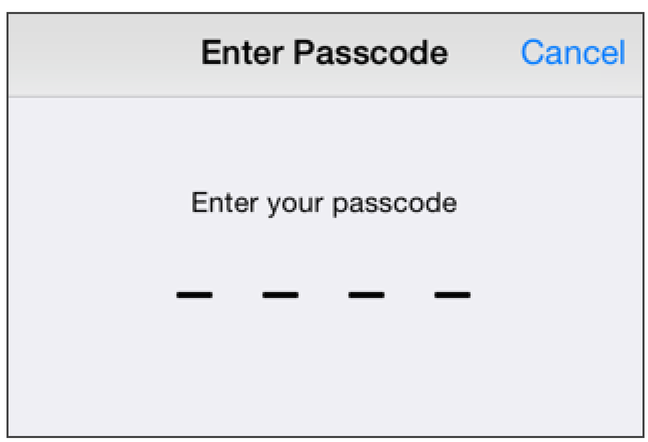
Step 3: Installing the VPN configuration profile

In the Install Profile dialog, click **Install** to install the VPN configuration profile.

In the Unsigned Profile dialog, click **Install Now** to start the installing.



Enter your passcode.



Step 3: Installing the VPN configuration profile

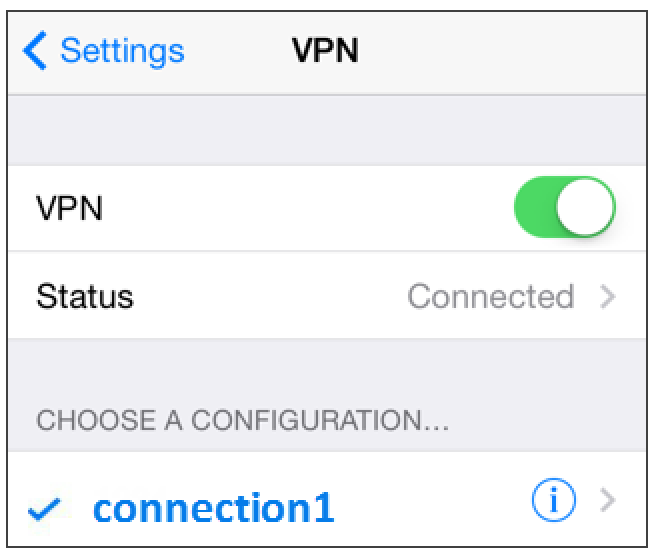
Click **Done**.

Step 4: Creating a VPN connection

In iOS, select **Settings** > **VPN**.

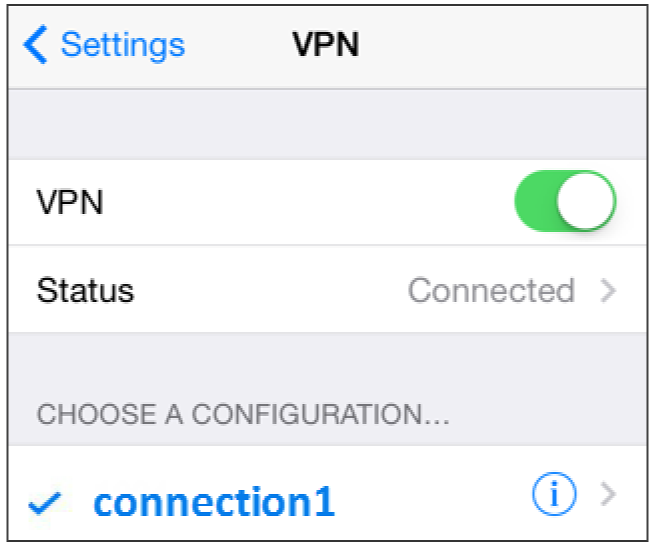
In the **CHOOSE A CONFIGURATION** list, select **connection1**.

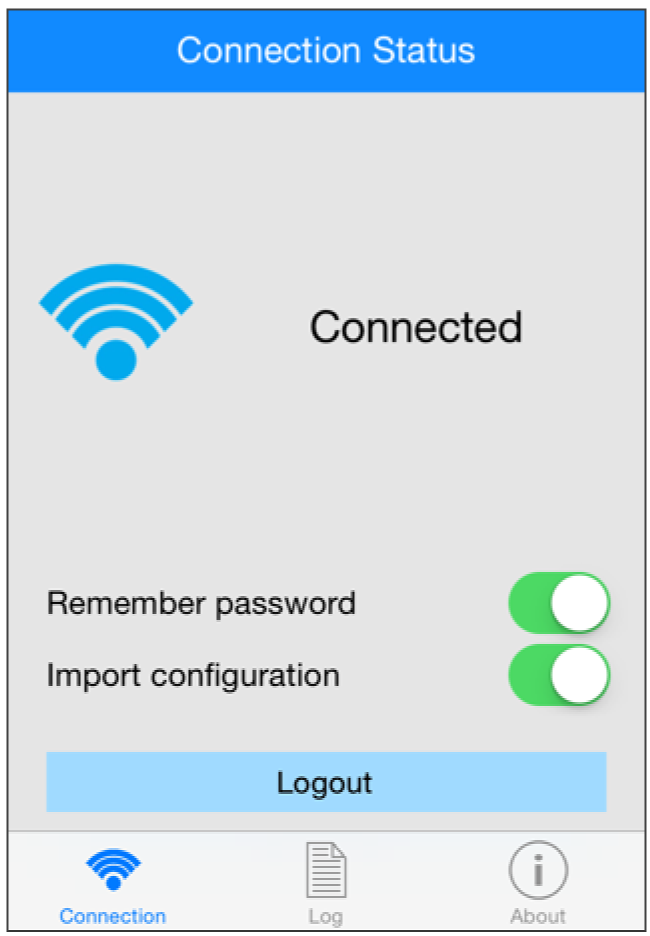
Turn on the VPN switch. iOS connects to the VPN.



Step 5: Verifying the connection status.

When the VPN status is **Connected** and the Connection tab of the client displays **Connected**, the client successfully establishes VPN connection to the device.





Step 6: Accessing intranet services

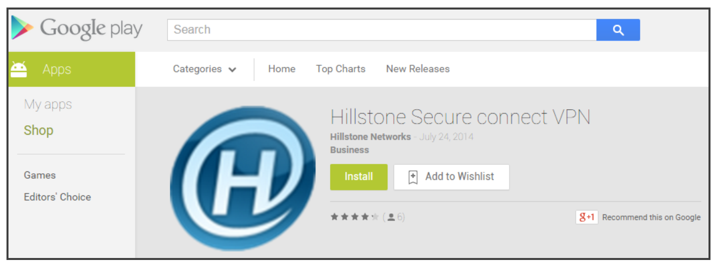
Use the iOS device to visit Server1.

Using an Android Device to Remotely Access Intranet Services

Step 1: Downloading and installing Hillstone Secure Connect

Visit Google Play to download and install Hillstone Secure Connect VPN.

https://play.google.com/store/apps/details?id=com.hillstone.vpn

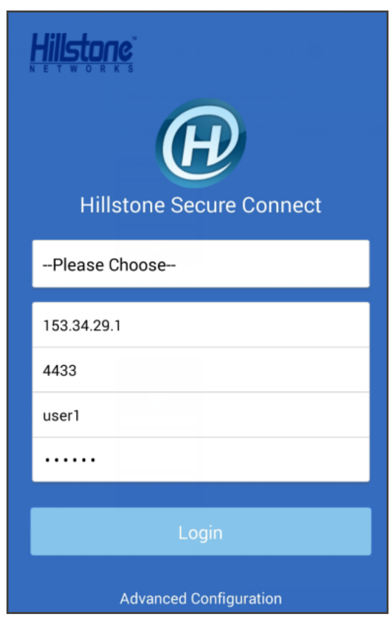


Step 4: Creating a VPN connection

In Android, click the Hillstone Secure Connection icon:

- Server: 153.34.29.1
- Port: 4433
- Account: user1
- Password: 123456

Click **Login**.



Step 4: Creating a VPN connection

After the VPN connection is established successfully, the key icon will appear at the notification area of your Android system.

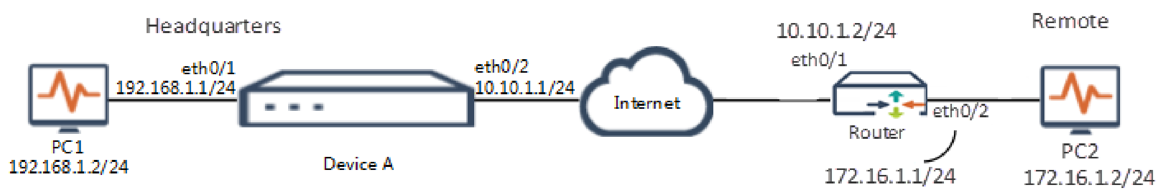
Step 6: Accessing intranet services

Use the Android device to visit Server1.

Allowing Remote Users (PC) to Access a Private Network Using L2TP over IPSec VPN

This example shows how to use L2TP over IPSec VPN to provide remote users with access to corporate internal network.

The topology is shown as below. A remote user, located at home or a hotel, accesses the Internet through a router with NAT enabled. This remote user uses L2TP over IPSec VPN to visit the server (PC1) in the corporate internal network. And this server is protected by the device A.



*Due to lab environment, use 10.10.1.0./24 to represent the public network segment.

The configuration process consists of five parts:

- Configure basic settings
- Configure IPSec VPN
- Configure L2TP VPN
- Set up a VPN connection in Windows/ Mac
- Adjust whether to use IPSec for L2TP VPN

Configuring Basic Settings

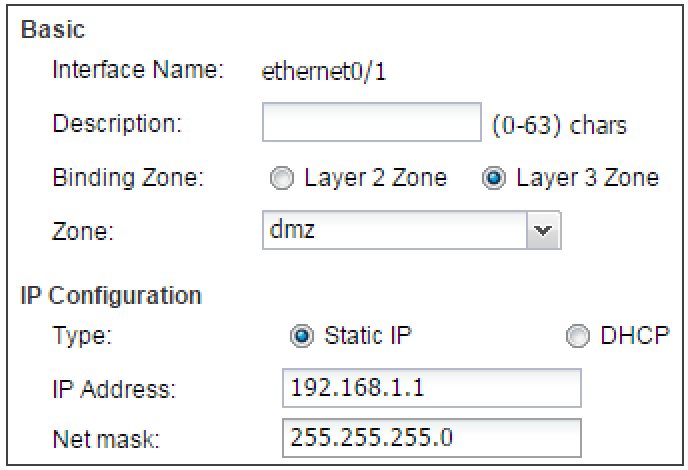
In device A, configure the following settings:

Step 1: Configuring an interface

Configuring the interface connected to the intranet

Select **Network > Interface**, and double-click ethernet0/1.

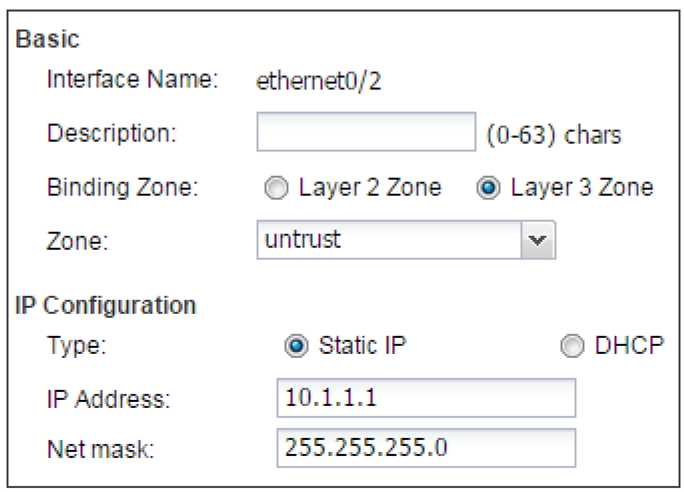
- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/2.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

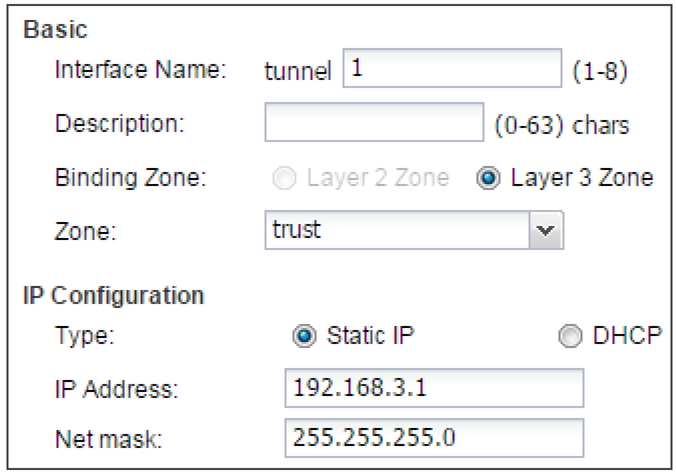


Step 1: Configuring an interface

Configuring the tunnel interface.

Select **Network** > **Interface** > **New** > **Tunnel Interface**.

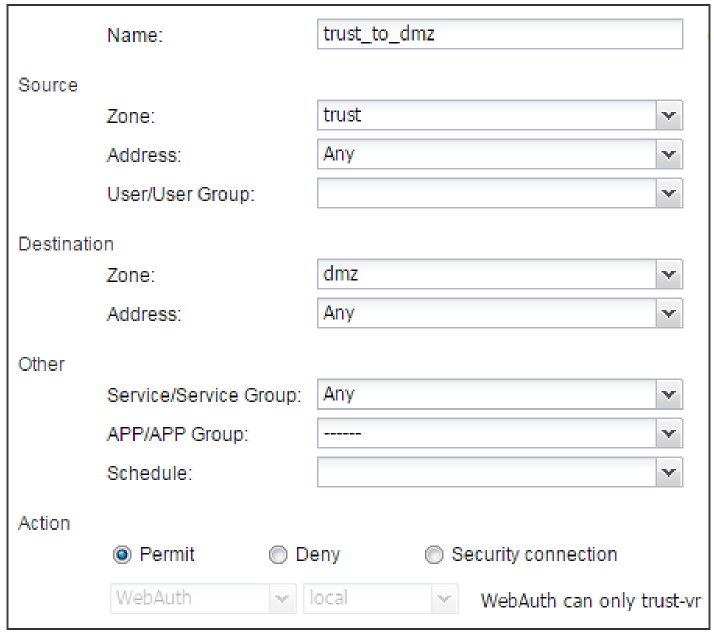
- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 192.168.3.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Step 2: Configuring a security policy

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the DMZ zone where the internal server locates.

Select **Policy > Security Policy > New**.



- Name: trust_to_dmz
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

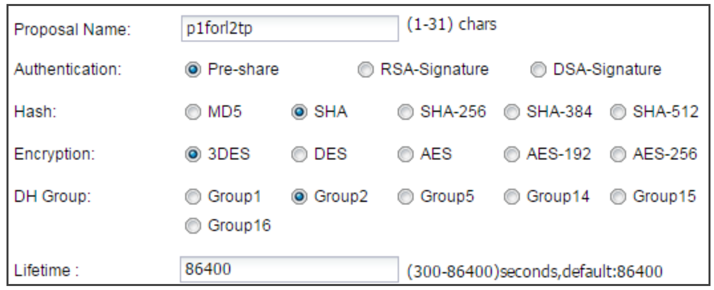
Configuring IPSec VPN

In device A, configure the following settings:

Step 1: Creating a P1 proposal and a P2 proposal

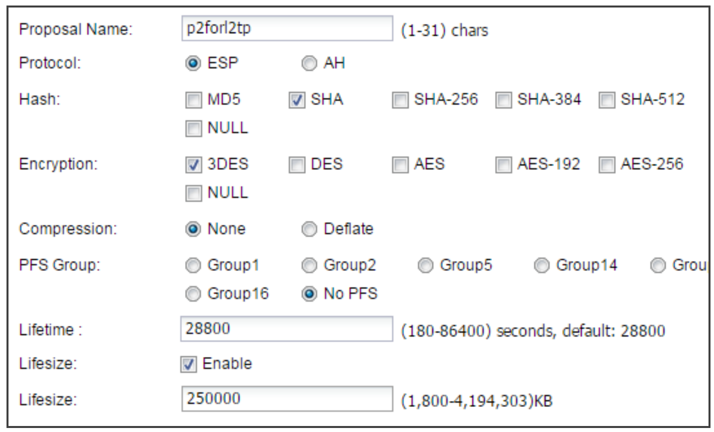
Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.

- Proposal Name: p1forl2tp
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400



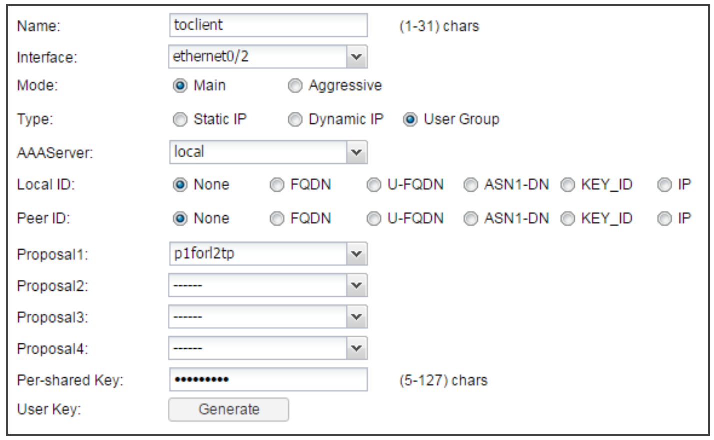
In the P2 Proposal tab, click **New**.

- Proposal Name: p2forl2tp
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800
- Lifesize: Enable
  - Lifesize: 250000



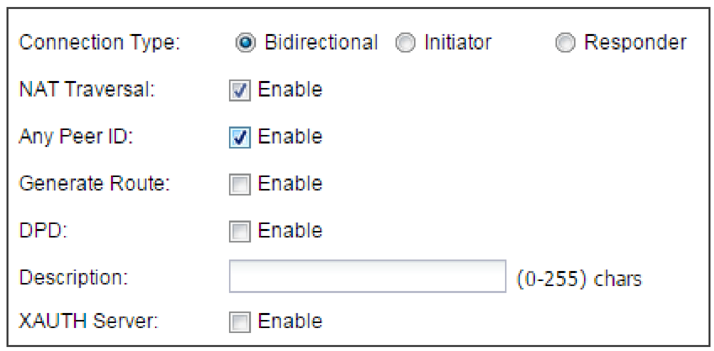
Step 2: Configuring a VPN peer

Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.



In the Basic tab, configure the following settings:

- Name: toclient
- Interface: ethernet0/2
- Mode: Main
- Type: User Group
- AAA Server: local
- Proposal1: p1forl2tp
- Pre-shared Key: hillstone



In the Advanced tab, configure the following settings:

- NAT Traversal: Enable
- Any Peer ID: Enable
- Keep the default of other parameters

Step 3: Configuring IKE VPN

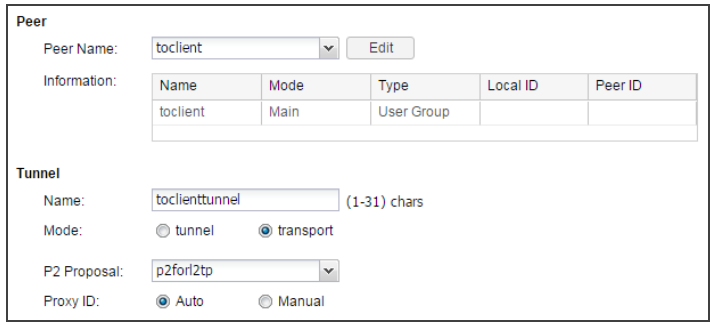
Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

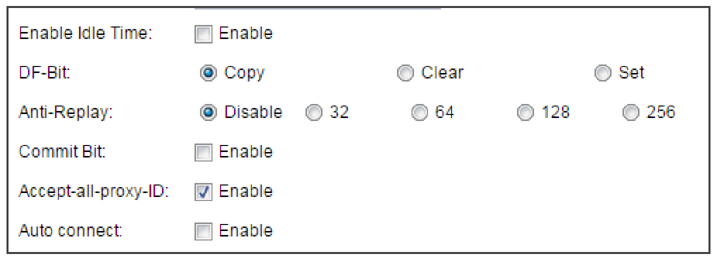
In the Basic tab, configure the following settings:

- Peer
  - Peer Name: toclient
- Tunnel
  - Name: toclienttunnel
  - Mode: transport
  - P2 proposal: p2forl2tp

In the Advanced tab, configure the following settings:

- Accept-all-proxy-ID: Enable
- Keep the default of other parameters





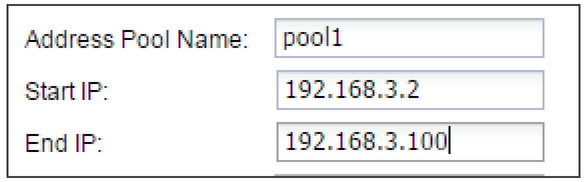
Configuring L2TP VPN

In device A, configure the following settings:

Step 1: Creating a L2TP pool

Select **Network > VPN > L2TP VPN > Address Pool**.

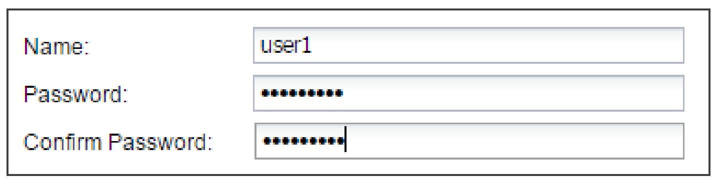
In the Address Pool dialog, click **New**.



- Address Pool Name: pool1
- Start IP: 192.168.3.2
- End IP: 192.168.3.100

Step 2: Adding a user in the 'local' AAA server

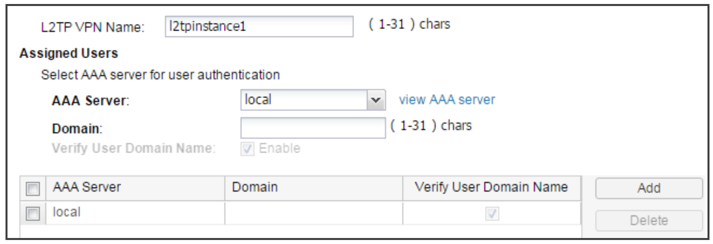
Select **Object > User > Local User > New > User**.



- Name: user1
- Password: hillstone
- Confirm Password: hillstone

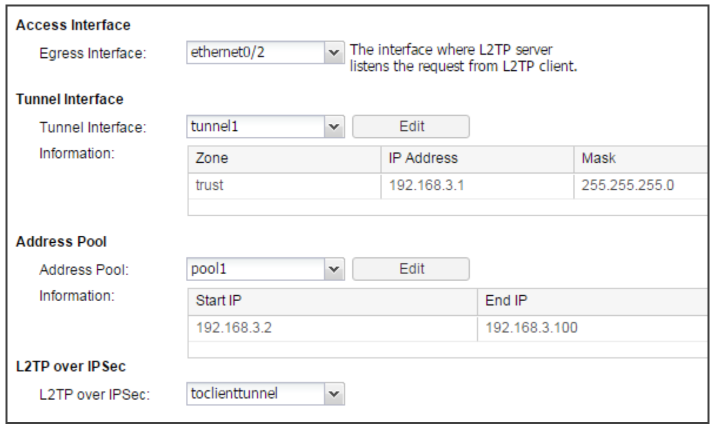
Step 3: Configuring a L2TP VPN instance

Select **Network > VPN > L2TP VPN > New**.



In the Name/Access User tab, configure the following settings:

- L2TP VPN Name: l2tpinstance1
- AAA Server: local
- Click **Add**



In the Interface/Address Pool/IPSec Tunnel tab, configure the following settings:

- Egress Interface: ethernet0/2
- Tunnel Interface: tunnel1
- Address Pool: pool1
- L2TP over IPSec: toclienttunnel

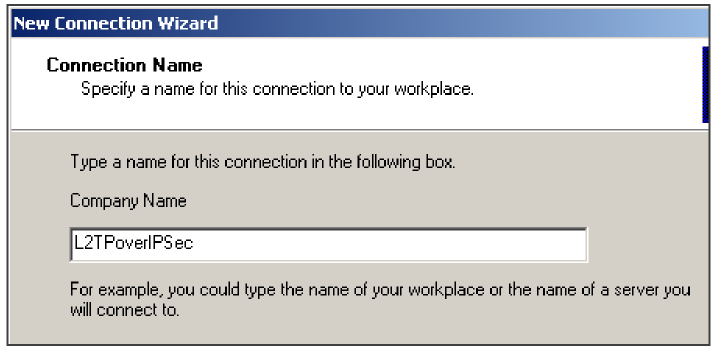
Setting up a VPN Connection

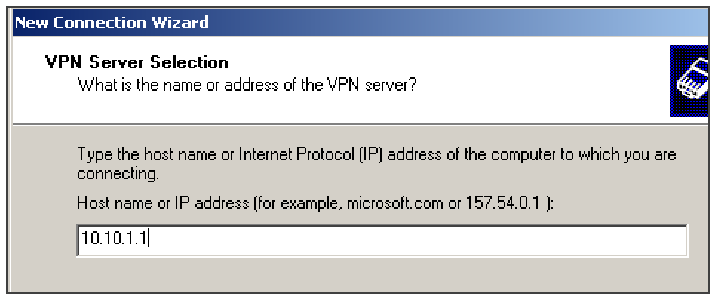
The steps of setting up a VPN connection differ in different PC operating systems. Take Windows 7, Windows XP/2003 and Mac OS for example.

Steps of setting up a VPN connection in Windows XP/2003

Set up a connection:

1. In Control Panel , double-click **Network Connections**.
2. From the Network Tasks pane, Click **Create a new connection**. The New Connection Wizard dialog appears
3. In the pop-up dialog, click **Next**.
4. Select **Connect to the network at my workplace**. Then click **Next**.
5. Select **Virtual Private Network connection**. Then click **Next**.
6. Enter a name for this connection in the **Company Name** text box: **L2TPoverIPSec**. Then click **Next**.
7. Enter the IP address of the VPN server: 10.10.1.1. Then click **Next**.
8. Click **Finish**.

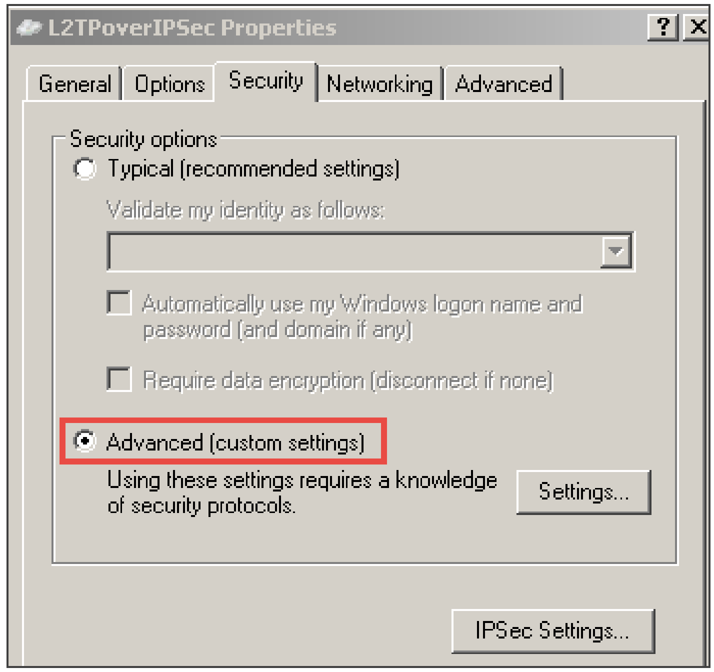


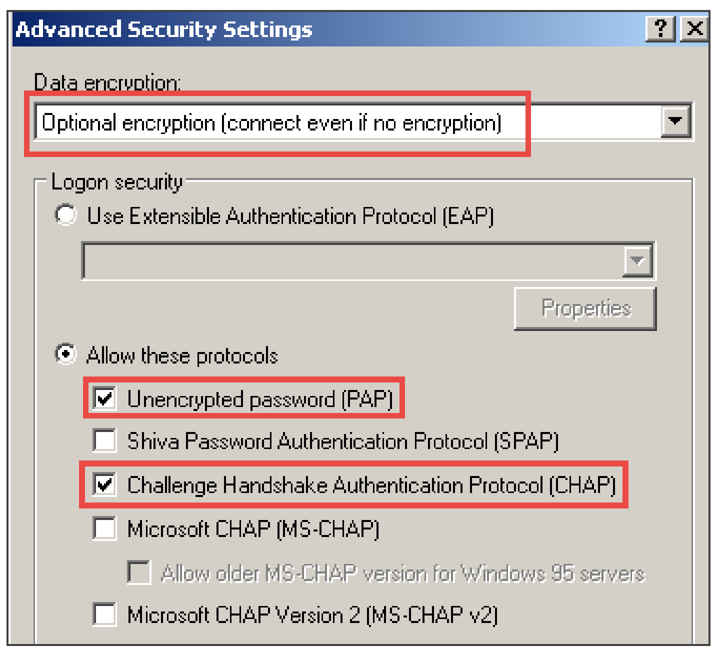


Steps of setting up a VPN connection in Windows XP/2003

Configure the Security properties of this connection:

1. After you have completed the new connection wizard, the Connect L2TPoverIPSec dialog appears.
2. Click **Properties**. The L2TPover-IPSec Properties dialog appears.
3. Select the **Security** tab.
4. Select **Advanced (custom settings)**. Then click **Settings**. The Advanced Security Settings dialog appears.
5. In the **Data encryption** drop-down menu, select **Optional encryption (connect even if no encrypting)**.
6. In the Logon security section, select **Allow these protocols**.
7. Continue to select **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**.
8. Click **OK** to close the **Advanced Security Settings** dialog and return to the L2TPoverIPSec Properties dialog.



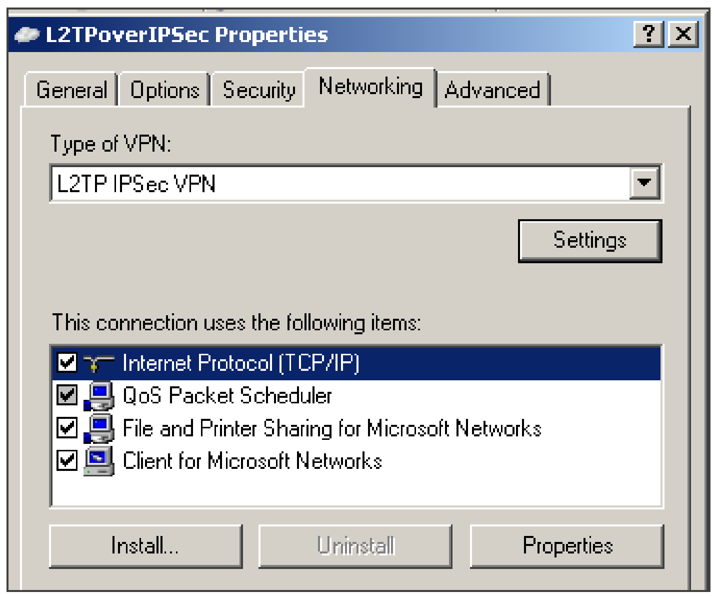


Steps of setting up a VPN connection in Windows XP/2003

9. Click **IPSec Settings**.
10. Select **Use pre-shared key for authentication** and enter the pre-shared key **hillstone**.
11. Click **OK** to close the IPSec Settings dialog.

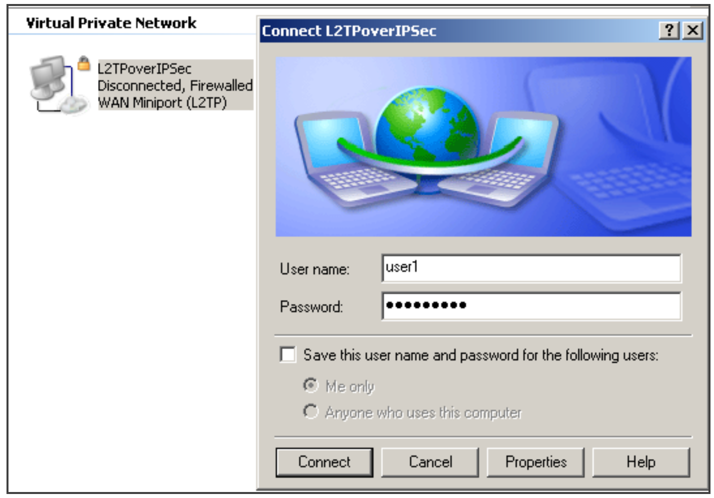
Configure the Networking properties of this connection:

1. In the L2TPoverIPSec Properties dialog, select the **Networking** tab.
2. In the Type of VPN drop-down menu, select **L2TP IPSec VPN**.
3. Ensure that you have select the **Internet Protocol (TCP/IP)** check box.
4. Click **OK** to save the configurations.



Steps of setting up a VPN connection in Windows XP/2003

Connect to the L2TPoverIPSec VPN:

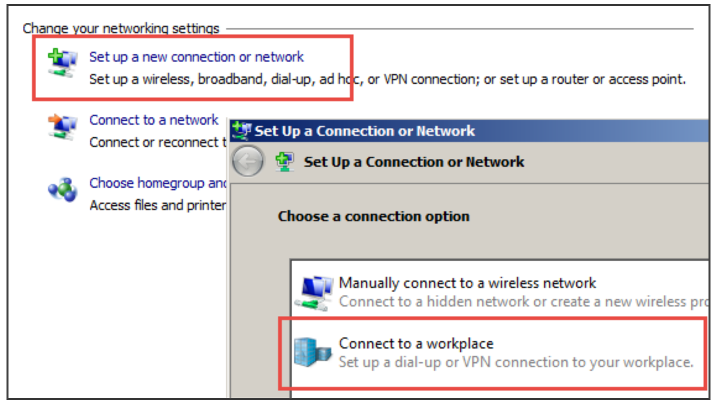


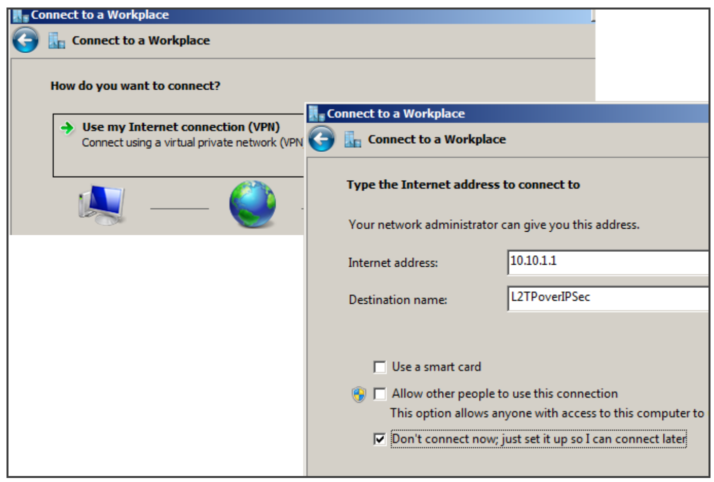
1. Find the **L2TPoverIPSec** connection and double-click it.
2. Enter the user name: user1
3. Enter the password: hillstone
4. Click **Connect**.
5. After the connection is successful, you can visit the internal server 192.168.1.2

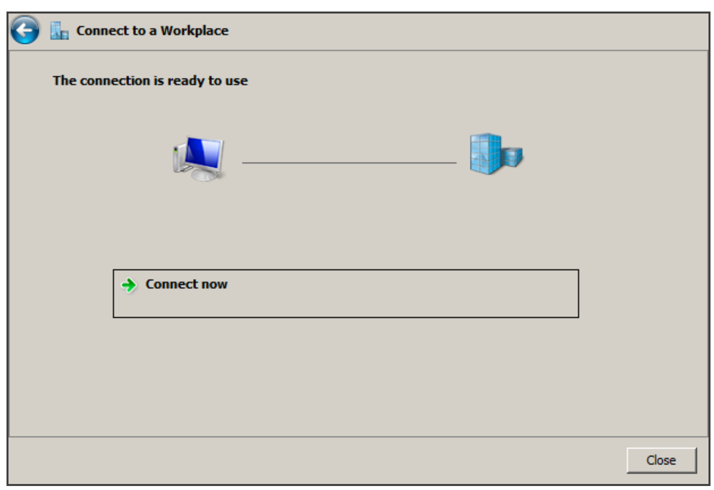
Steps of setting up a VPN connection in Windows 7

Set up a connection:

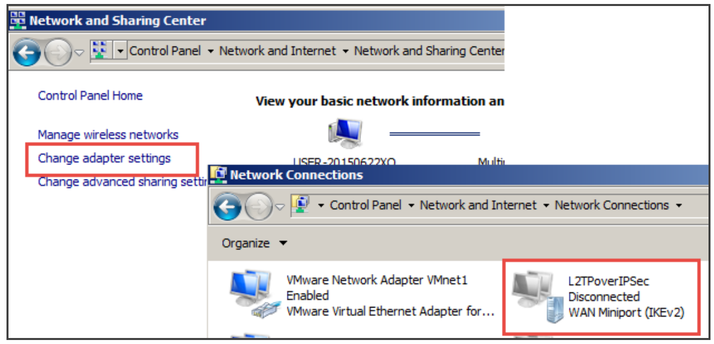
1. Select **Control Panel > Network and Internet > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the pop-up dialog, select **Connect to a workplace**. Then click **Next**.
4. Select **Use my Internet connection (VPN)**.
5. Enter the IP address of the VPN server: 10.10.1.1
6. Enter the destination name: L2TPoverIPSec
7. Select **Don't connect now; just set it up so I can connect later**. Then click **Next**.
8. Enter the username: user1
9. Enter the password: hillstone
10. Click **Creat**.
11. After the connection is ready to use, click **Close**.





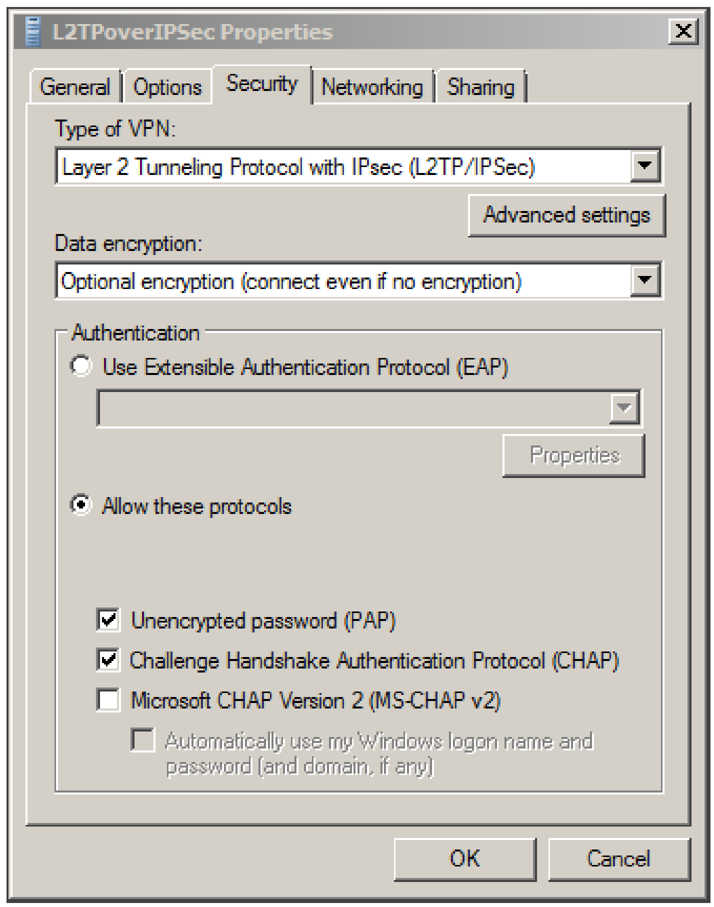


Steps of setting up a VPN connection in Windows 7



Configure the Security properties of this connection:

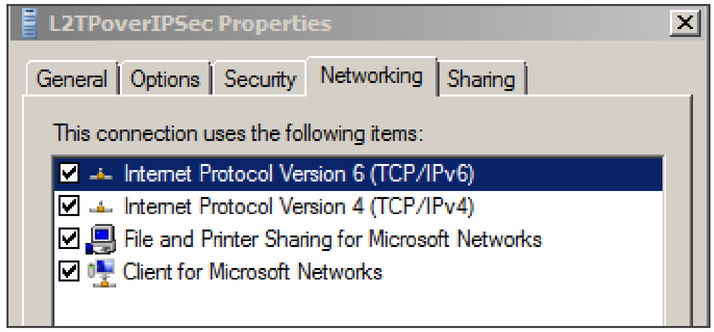
1. In the Network and Sharing Center, click **Change adapter settings**.
2. Find the **L2TPoverIPSec** connection and right-click it.
3. In the pop-up menu, select **Properties**. The L2TPoverIPSec Properties dialog appears.
4. Select the **Security** tab.
5. In the **Type of VPN** drop-down menu, select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**.
6. Click **Advanced settings**, select **Use preshared key for authentication**, then enter the key **hillstone**.
7. In the **Data encryption** drop-down menu, select **Optional encryption (connect even if no encryption)**.
8. In the **Authentication** section, select **Allow these protocols** and then select **Unencrypted password (PAP)** and **Challenge Handshank Authentication Protocol (CHAP)**.



Steps of setting up a VPN connection in Windows 7

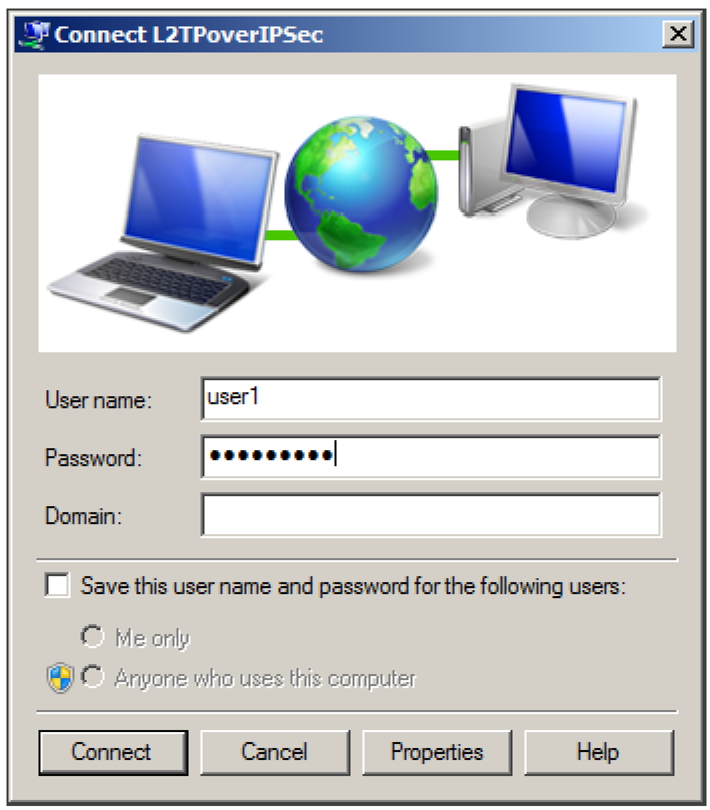
Configure the Networking properties of this connection:

1. In the L2TPoverIPSec Properties dialog, select the **Networking** tab.
2. Ensure that you have select the **Internet Protocol Version 4 (TCP/IPv4)** check box.
3. Click **OK** to save the configurations.

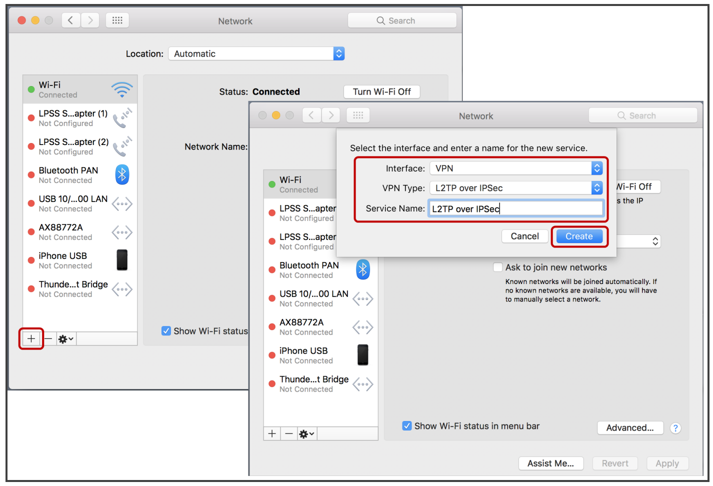


Connect to the L2TPoverIPSec VPN:

1. Find the **L2TPoverIPSec** connection and double-click it.
2. Enter the password: hjllstone
3. Click **Connect**.
4. After the connection is successful, you can visit the intranet server 192.168.1.2



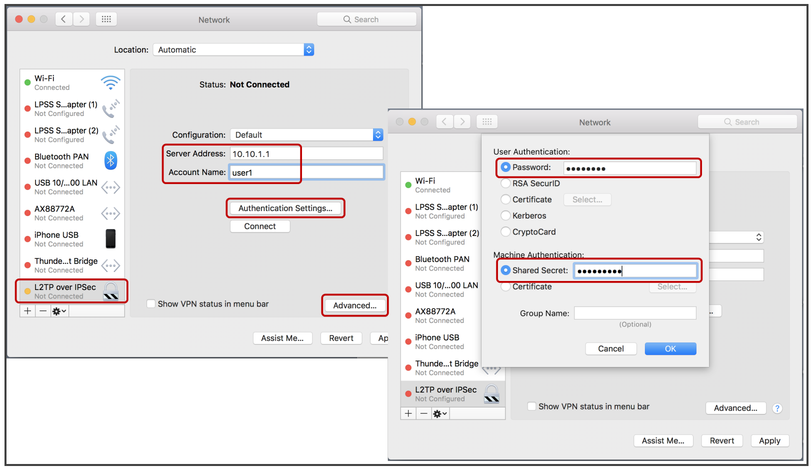
Steps of setting up a VPN connection in Mac OS



Set up a connection:

1. Select **System Preferences > Network**.
2. Click **+** to create a new network connection
3. Enter the connection configuration in the pop-up dialog.
4. Click Interface drop-down list and select VPN
5. Click **VPN Type** drop-down list and select **L2TP over IPSec**.
6. Enter the **Service Name**: L2TP over IPSec.
7. Click Create.

Steps of setting up a VPN connection in Mac OS



Configure the properties of connection:

1. Find **L2TP over IPSec** on the left web page and click it.

2. Enter the **Server Address** on the right web page: 10.10.1.1.

3. Enter the **Account Name**: user1.

4. Click **Authentication Settings** button and enter authentication password in the pop-up dialog.

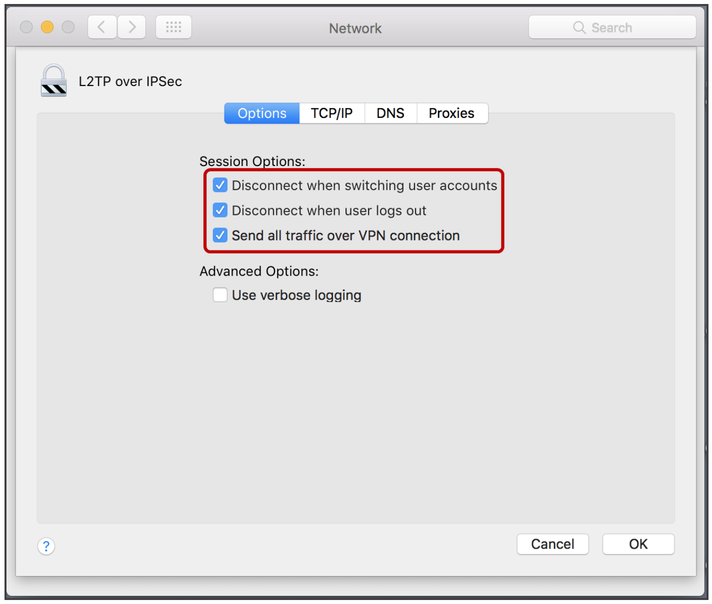
5. In the **User Authentication** section, select **Password** button and enter the corresponding password: hillstone.

6. In the **Machine Authentication** section, select **Shared Secret** button in the Machine Authentication and enter the **Shared Secret**: hillstone.

Steps of setting up a VPN connection in Mac OS

7. Click **OK** to save the configurations.

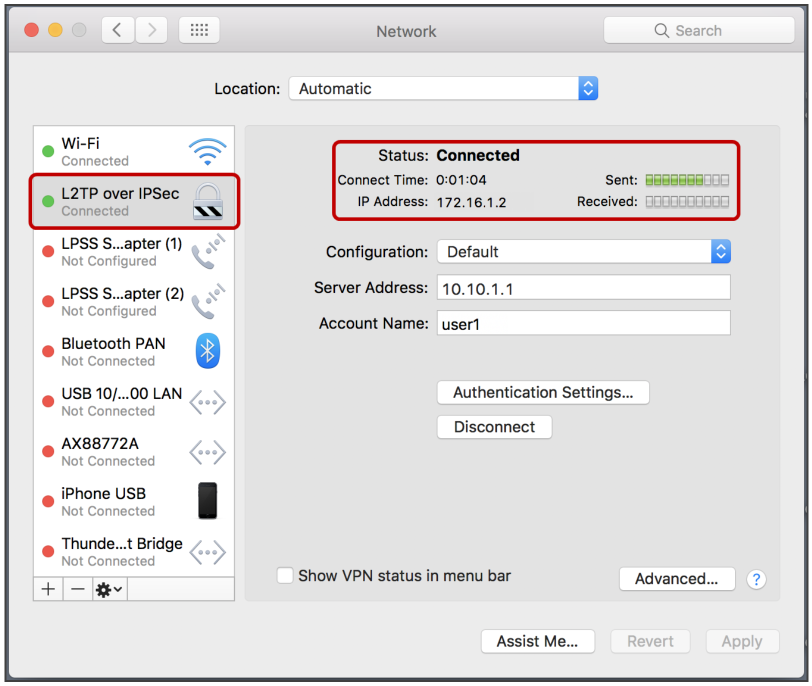
Configure the advanced properties of connection:



1. Click **Advanced** button.
2. Configure the advanced properties in the pop-up dialog.
3. Select all the check boxes in **Session Options** and make sure that the check box of **Send all traffic over VPN connection** is selected.
4. Click **OK** to save the configurations.

Steps of setting up a VPN connection in Mac OS

Connect to the L2TP over IPSec VPN:



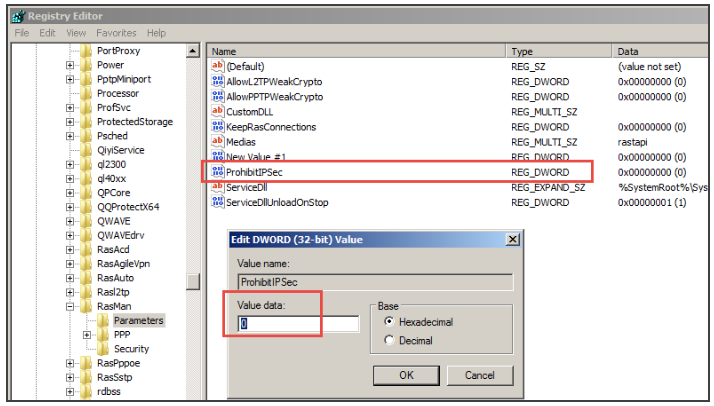
1. Find **L2TP over IPSec** on the left web page and click it.
2. Click **Connect** button on the right page.
3. The status shows **Connecting**.
4. After connecting successfully, the page shows Status: **Connected**, Connect Time and so on.
5. Click **Apply** to save the configurations.
6. After the connection is successful, you can visit the intranet server 192.168.1.2.
7. If you need to disconnect the connection, click **Disconnect** button.

Adjusting Whether to Use IPSec for L2TP VPN

By default, the L2TP VPN is required by Windows to use IPSec. For the above L2TP over IPSec VPN, you do not need to modify the system's registry.

If the system has disabled IPSec, take the following steps to make the system use L2TP over IPSec:

Enable IPSec

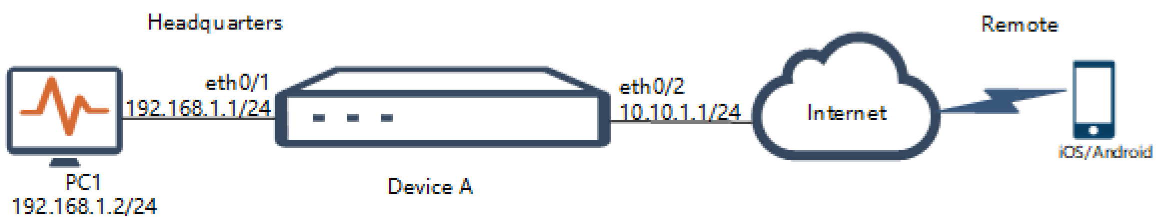


1. Select **Start > Run**.
2. In **Run**, enter **regedit**.
3. Click **OK**
4. Navigate to **HKEY_Local_Machine\System\CurentControlSet\Services\RasMan\Parameters**.
5. In the right pane, find the entry **ProhibitIPSec** whose type is **REG_DWORD**.
6. Double-click this entry and modify the value in the **Value data** text box to **0**.
   - **0** represents that the system enables IPSec.
   - **1** represents that the system disables IPSec.
7. Save the modifications and restart the system.

Allowing Remote Users (iOS/Android) to Access a Private Network Using L2TP over IPSec VPN

This example shows how to use L2TP over IPSec VPN to provide remote users (iOS/Android) with access to corporate internal network.

The topology is shown as below. A remote user, located at home or a hotel, accesses the Internet via mobile 3G/4G or Wi-Fi. This remote user (iOS/Android) uses L2TP over IPSec VPN to visit the server (PC1) in the corporate internal network. And this server is protected by the device A.



*Due to lab environment, use 10.10.1.0./24 to represent the public network segment.

The configuration process consists of five parts:

- Configure basic settings
- Configure IPSec VPN
- Configure L2TP VPN
- Set up a VPN connection in iOS/Android

Configuring Basic Settings

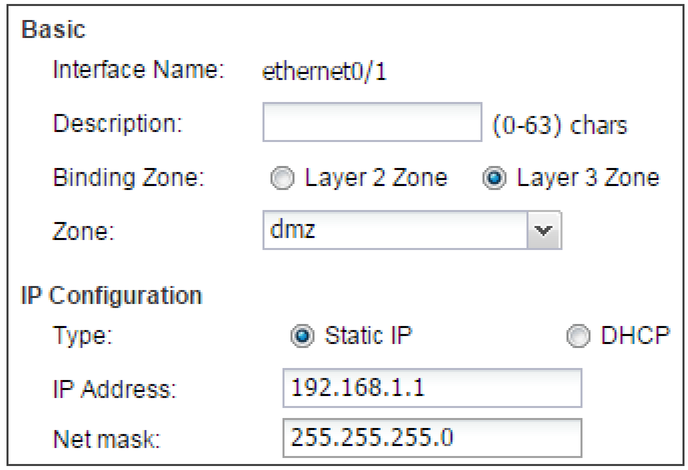
In device A, configure the following settings:

Step 1: Configuring an interface

Configuring the interface connected to the intranet

Select **Network > Interface**, and double-click ethernet0/1.

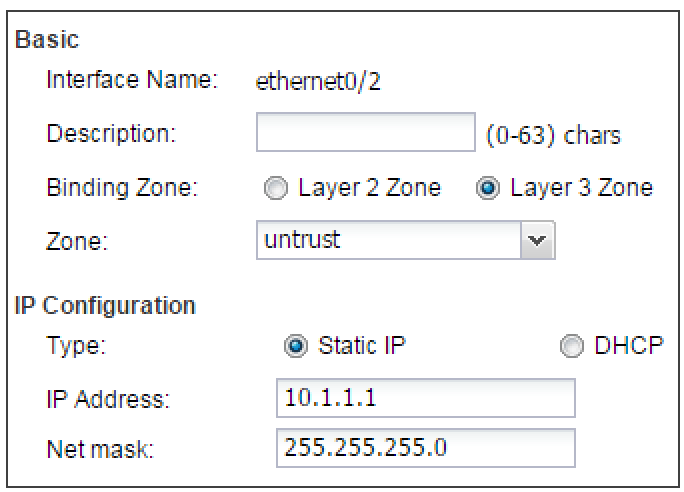
- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/2.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

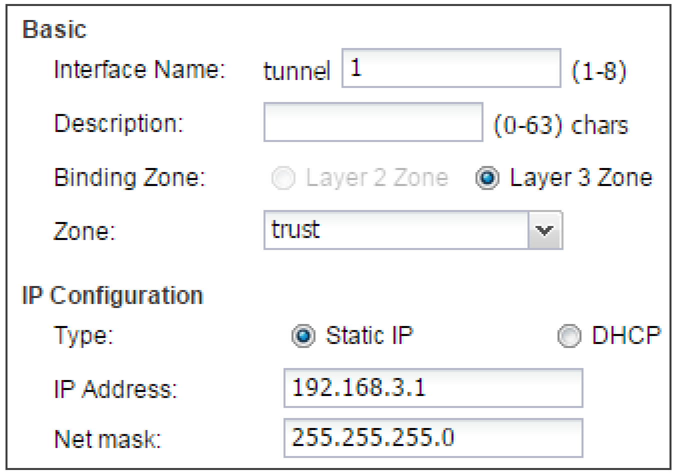


Step 1: Configuring an interface

Configuring the tunnel interface.

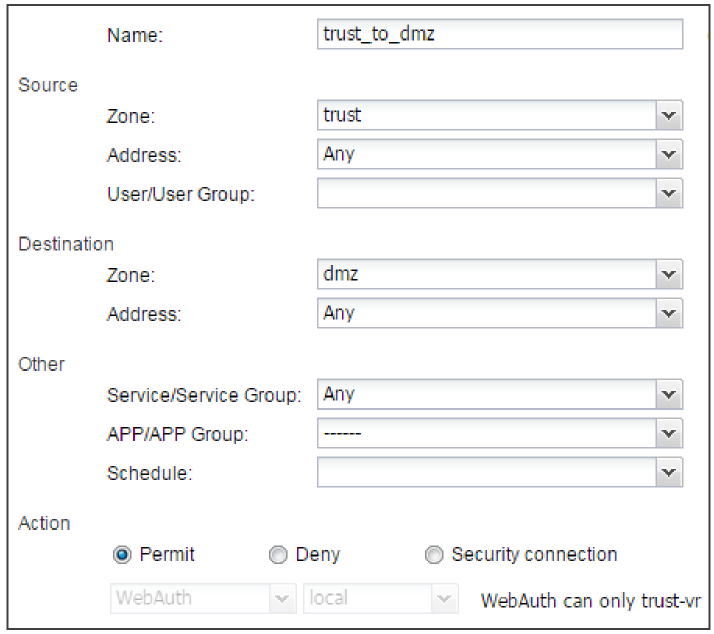
Select **Network** > **Interface** > **New** > **Tunnel Interface**.

- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 192.168.3.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Step 2: Configuring a security policy

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the DMZ zone where the internal server locates.



Select **Policy > Security Policy > New**.

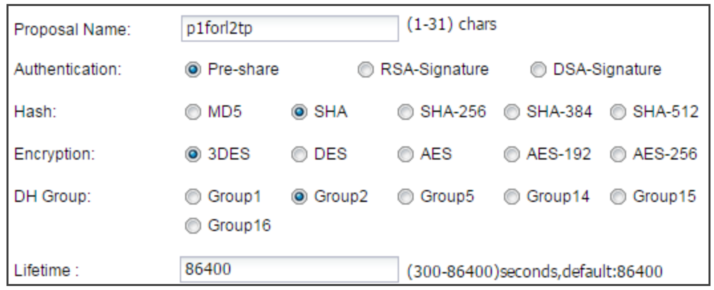
- Name: trust_to_dmz
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

Configuring IPSec VPN

In device A, configure the following settings:

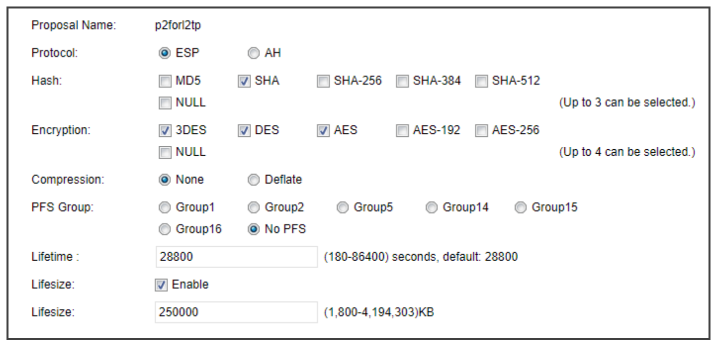
Step 1: Creating a P1 proposal and a P2 proposal

Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.



- Proposal Name: p1forl2tp
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400

In the P2 Proposal tab, click **New**.



- Proposal Name: p2forl2tp
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES, DES, AES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800
- Lifesize: Enable
  - Lifesize: 250000

Step 2: Configuring a VPN peer

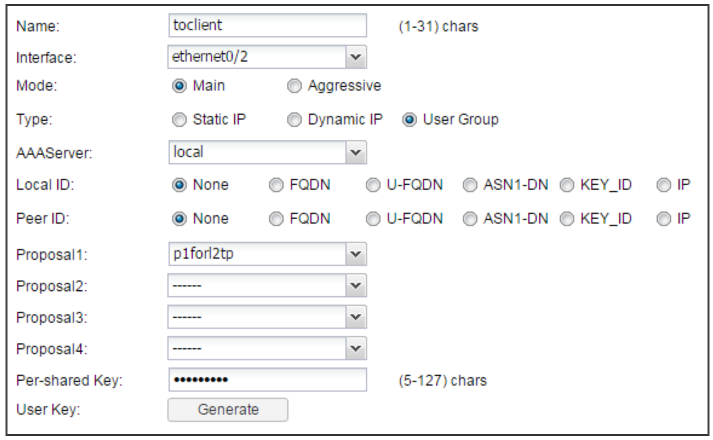
Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

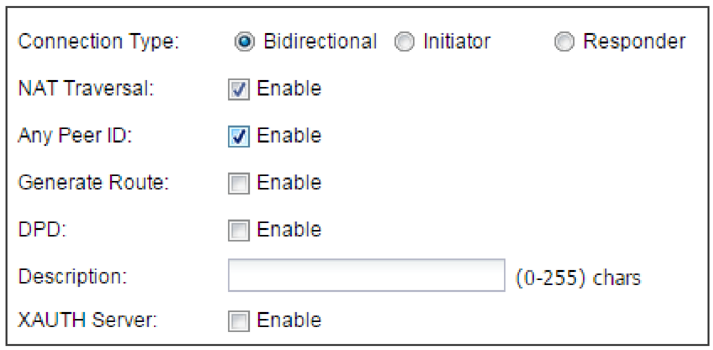
In the Basic tab, configure the following settings:

- Name: toclient
- Interface: ethernet0/2
- Mode: Main
- Type: User Group
- AAA Server: local
- Proposal1: p1forl2tp
- Pre-shared Key: hillstone

In the Advanced tab, configure the following settings:

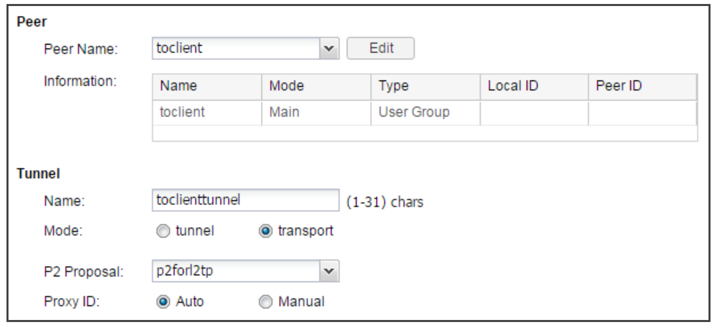
- NAT Traversal: Enable
- Any Peer ID: Enable
- Keep the default of other parameters

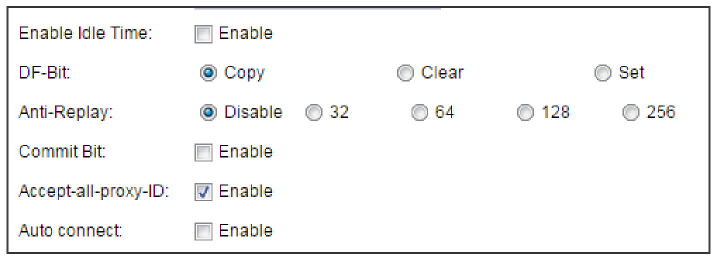




Step 3: Configuring IKE VPN

Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.





In the Basic tab, configure the following settings:

- Peer
  - Peer Name: toclient
- Tunnel
  - Name: toclienttunnel
  - Mode: transport
  - P2 proposal: p2forl2tp

In the Advanced tab, configure the following settings:

- Accept-all-proxy-ID: Enable
- Keep the default of other parameters

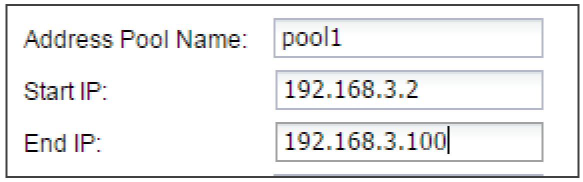
Configuring L2TP VPN

In device A, configure the following settings:

Step 1: Creating a L2TP pool

Select **Network > VPN > L2TP VPN > Address Pool**.

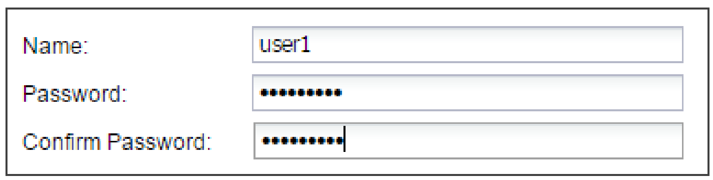
In the Address Pool dialog, click **New**.



- Address Pool Name: pool1
- Start IP: 192.168.3.2
- End IP: 192.168.3.100

Step 2: Adding a user in the 'local' AAA server

Select **Object > User > Local User > New > User**.



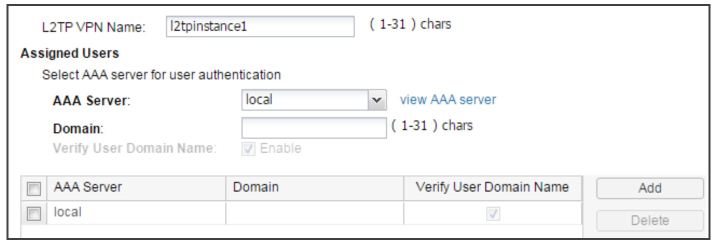
- Name: user1
- Password: hillstone
- Confirm Password: hillstone

Step 3: Configuring a L2TP VPN instance

Select **Network > VPN > L2TP VPN > New**.

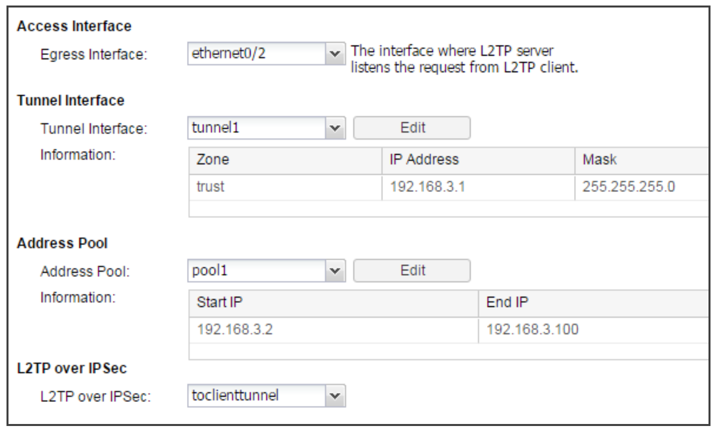
In the Name/Access User tab, configure the following settings:

- L2TP VPN Name: l2tpinstance1
- AAA Server: local
- Click **Add**



In the Interface/Address Pool/IPSec Tunnel tab, configure the following settings:

- Egress Interface: ethernet0/2
- Tunnel Interface: tunnel1
- Address Pool: pool1
- L2TP over IPSec: toclienttunnel



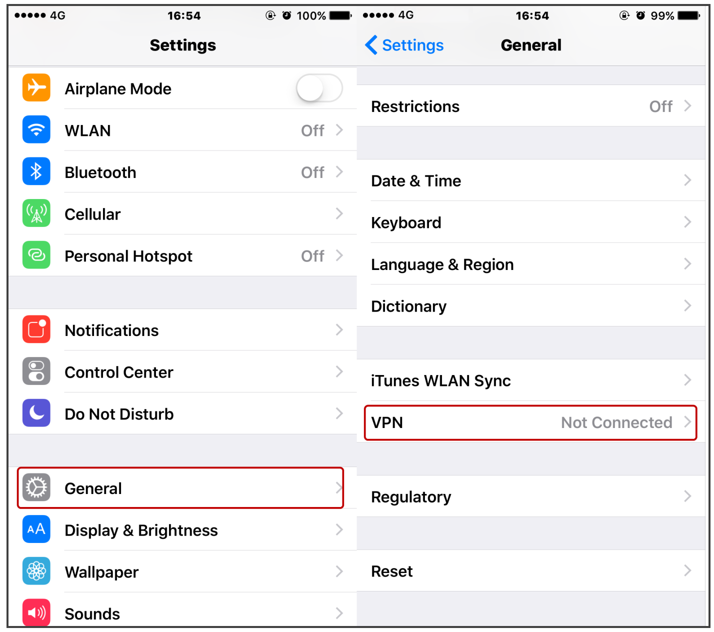
Set up a VPN connection in iOS/ Android

Take iOS 10 and Android 7 as examples.

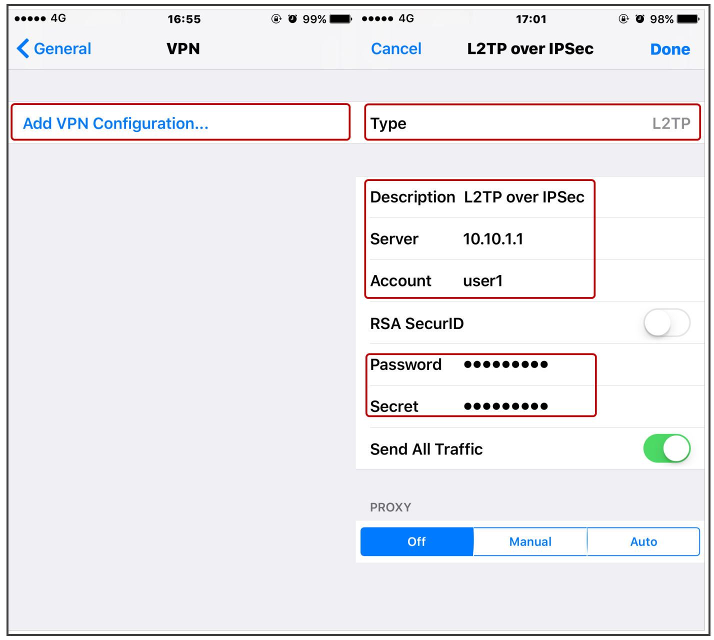
Steps of setting up a VPN connection in iOS 10. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Enter VPN configuration page:

1. Select **Settings > General** in your iPhone.
2. Swipe down and click **VPN**.
3. Click **Add VPN Configuration…**



Steps of setting up a VPN connection in iOS 10. (Before configuring your iPhone, make sure that it can access the Internet normally.)



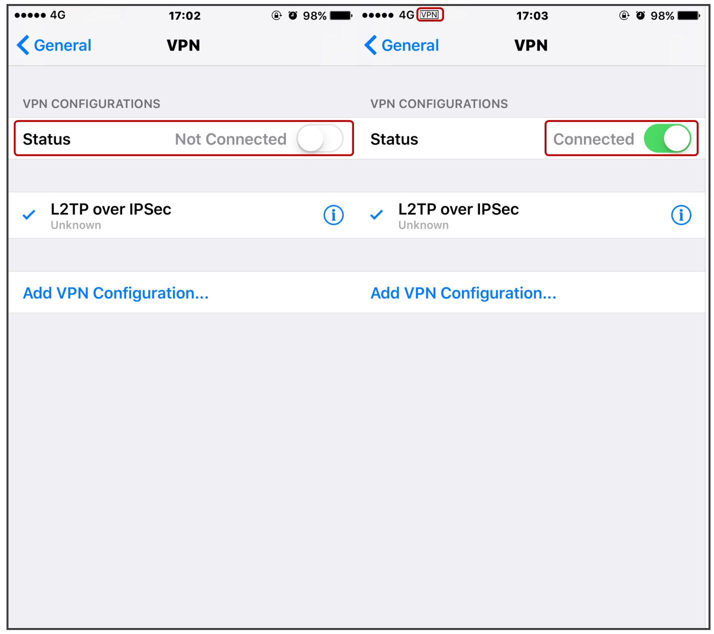
Configuring VPN properties:

1. Click **Add VPN Configuration** on VPN page.
2. Enter the following configurations on Add Configuration page.
   - Type: Click the drop-down list and select **L2TP**.
   - Description: Enter the custom name **L2TP over IPSec** to mark the L2TP connection.
   - Server: 10.10.1.1
   - Account: user1, the login account that has been added in local AAA server
   - Password: hillstone, the corresponding password of the account.
   - Secret: hillstone, the pre-shared key.
3. Click Done on the top right corner.

Steps of setting up a VPN connection in iOS 10. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Enabling VPN and connect L2TP over IPSec VPN:

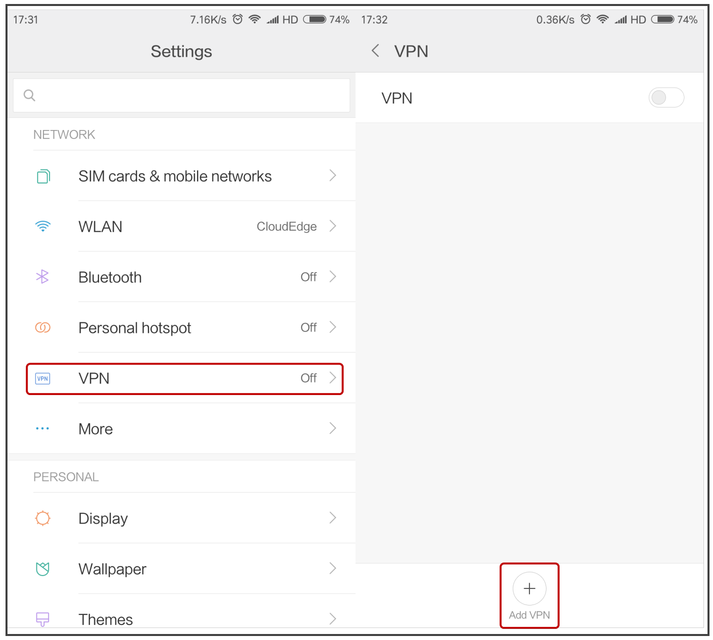
1. Select the configured VPN: **L2TP over IPSec**.
2. Swipe the **Status** button.
3. After VPN being connected successfully, the status shows **Connected** and there will appear VPN on the top of screen.
4. After VPN being connected successfully, you can access the internal server: 192.168.1.2.



Steps of setting up a VPN connection in Android. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Enter the VPN configuration page:

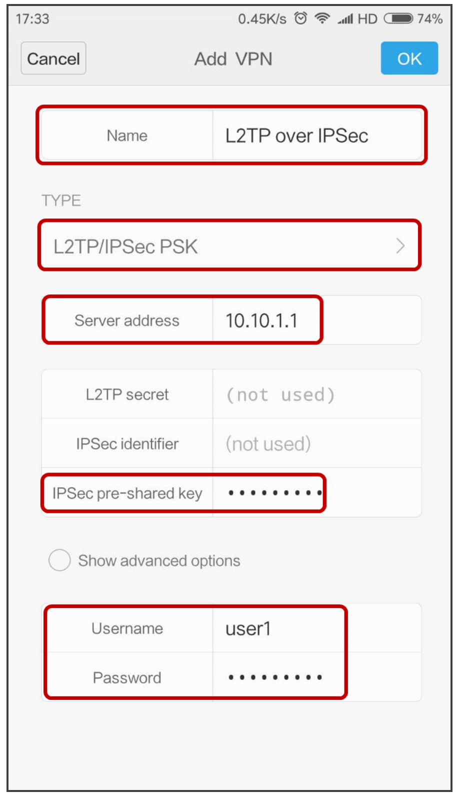
1. Select **Settings > VPN** in your Android phone.
2. Click **Add VPN** at the bottom of screen.



Steps of setting up a VPN connection in Android. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Configuring VPN properties:

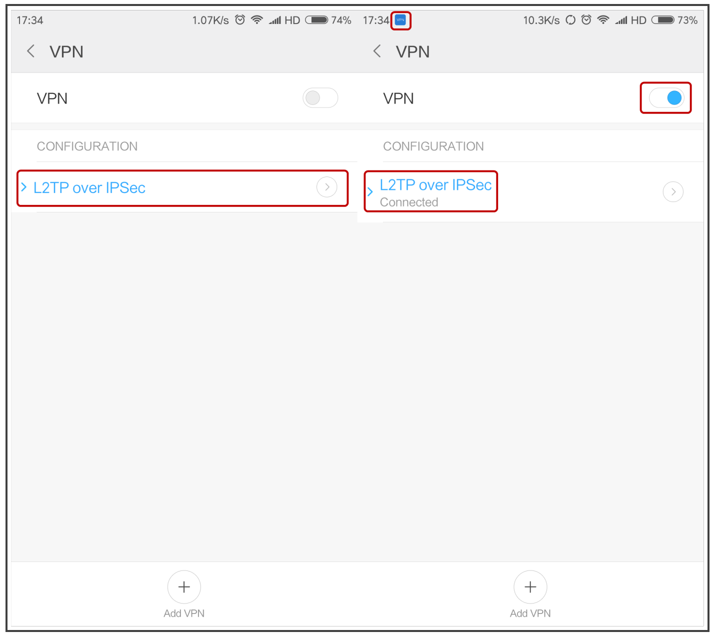
1. Enter the following configurations on Add VPN page.
   - Enter the custom name **L2TP over IPSec** to mark the L2TP connection.
   - TYPE: Click the drop-down list and select **L2TP/IPSec PSK**.
   - Server address: 10.10.1.1
   - IPSec pre-shared key: hillstone
   - Account: user1, the login account that has been added in local AAA server.
   - Password: hillstone, the corresponding password of the account.
2. Click OK on the top right corner.



Steps of setting up a VPN connection in Android. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Enabling VPN and connect L2TP over IPSec VPN:

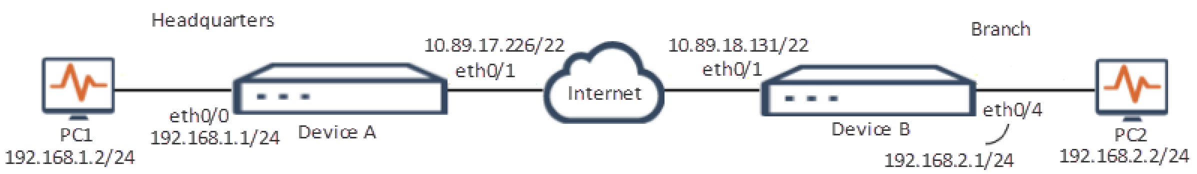
1. Select the configured VPN: **L2TP over IPSec**.
2. Swipe the **VPN** button.
3. After VPN being connected successfully, the status shows **Connected** and there will appear a VPN sign on the top screen.
4. After VPN being connected successfully, you can access the internal server: 192.168.1.2.



Connection between Two Private Networks Using GRE over IPSec VPN

This example introduces how to create GRE over IPSec VPN to protect the communication between the private network of the headquarters and the private network of the branch.

The topology is shown as below. Device A acts as the gateway of the headquarters and device B acts as the gateway of the branch. To protect the communication between two private networks, use GRE over IPSec VPN.



*Due to lab environment, use 10.89.16.0/22 to represent the public network segment.

The configuration process consists of five parts:

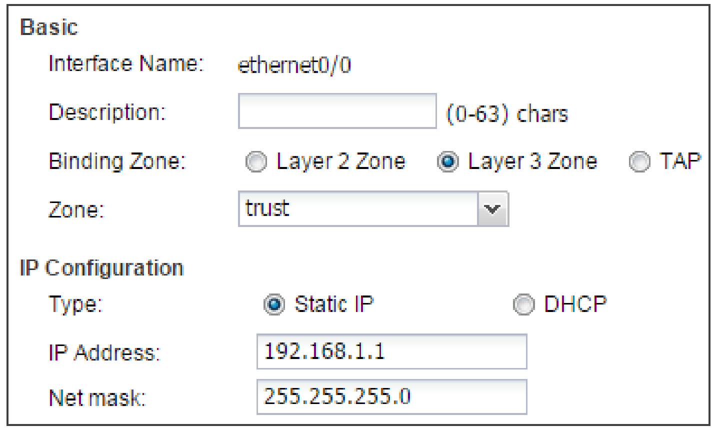
- Configure basic settings
- Configure IPSec VPN
- Configure GRE VPN
- Configure route and policies

Configuring Basic Settings

Step 1: Configuring interfaces for device A

Configuring the interface connected to the intranet

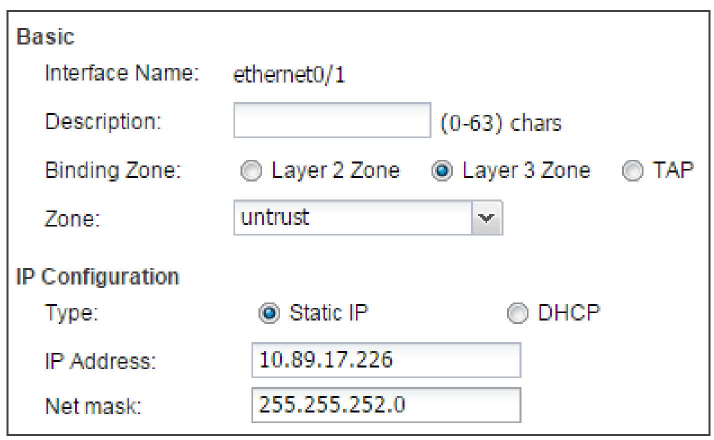
Select **Network > Interface**, and double-click ethernet0/0.



- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

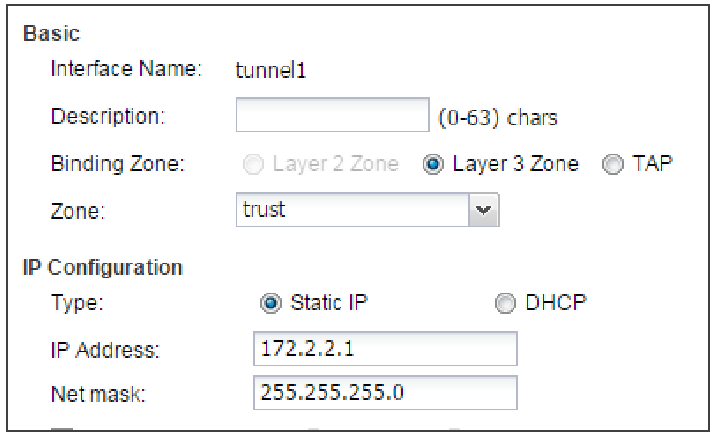
Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/1.



- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.89.17.226
- Netmask: 255.255.252.0
- Keep the default of other parameters

Step 1: Configuring interfaces for device A

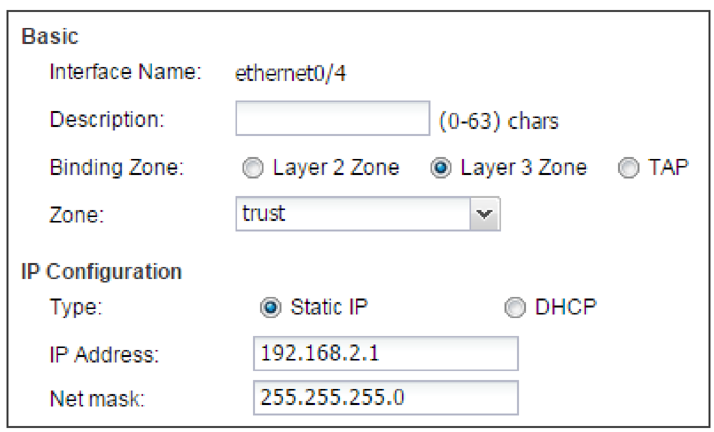


Configuring the tunnel interface.

Select **Network** > **Interface** > **New** > **Tunnel Interface**.

- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 172.2.2.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

Step 2: Configuring interfaces for device B



Configuring the interface connected to the intranet

Select **Network** > **Interface**, and double-click ethernet0/4.

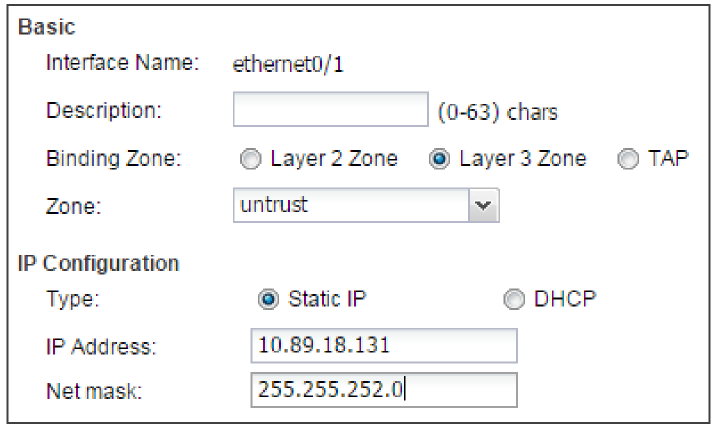
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.2.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

Step 2: Configuring interfaces for device B

Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/1.

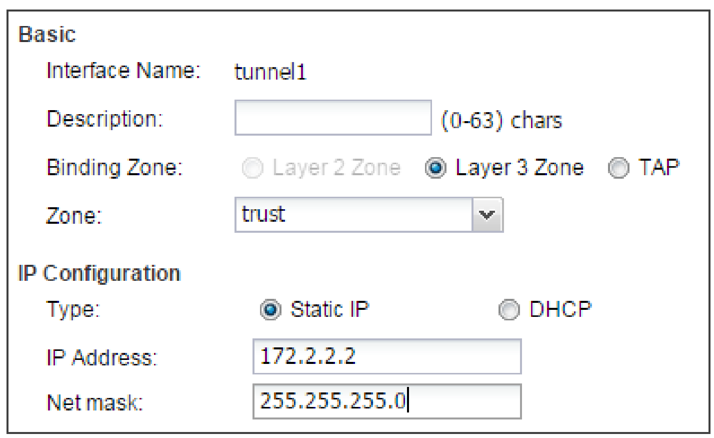
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.89.18.131
- Netmask: 255.255.252.0
- Keep the default of other parameters



Configuring the tunnel interface.

Select **Network > Interface > New > Tunnel Interface**.

- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 172.2.2.2
- Netmask: 255.255.255.0
- Keep the default of other parameters

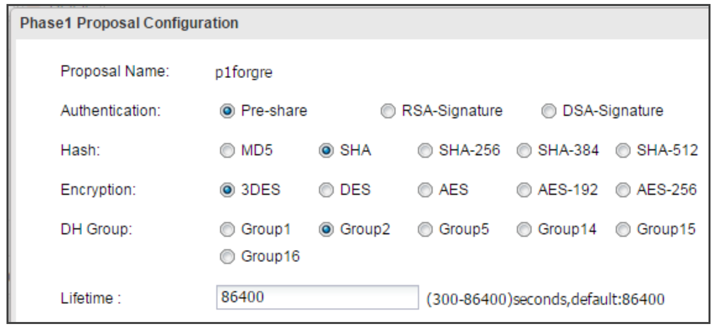


Configuring IPSec VPN

Step 1: Configuring IPSec VPN for device A

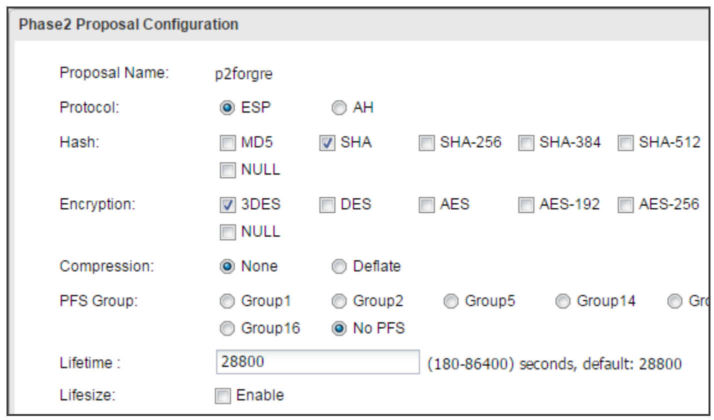
Create a P1 proposal and a P2 proposal.

Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.



- Proposal Name: p1forgre
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400

In the P2 Proposal tab, click **New**.



- Proposal Name: p2forl2tp
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800

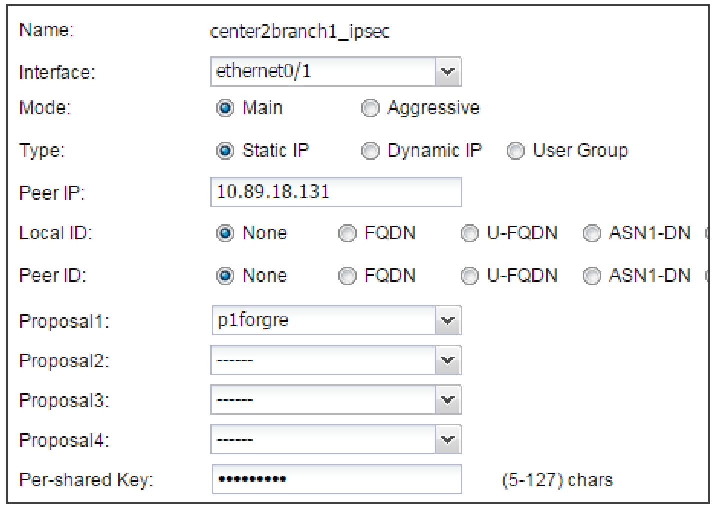
Step 1: Configuring IPSec VPN for device A

Configure a VPN peer.

Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

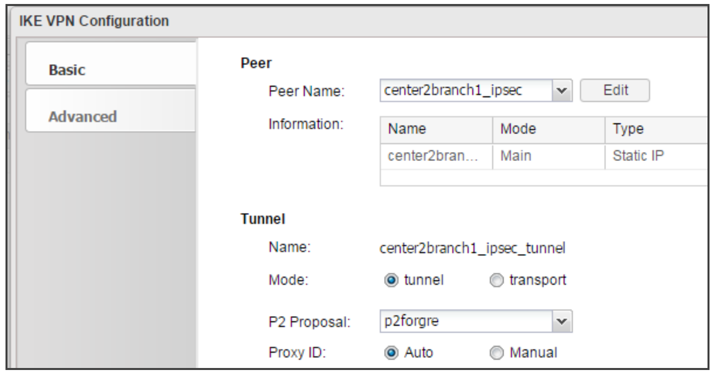
In the Basic tab, configure the following settings:

- Name: center2branch1_ipsec
- Interface: ethernet0/1
- Mode: Main
- Type: Static IP
- Peer IP: 10.89.18.131
- Proposal1: p1forgre
- Pre-shared Key: hillstone
- Keep the default of other parameters



Step 1: Configuring IPSec VPN for device A

Configure IKE VPN.



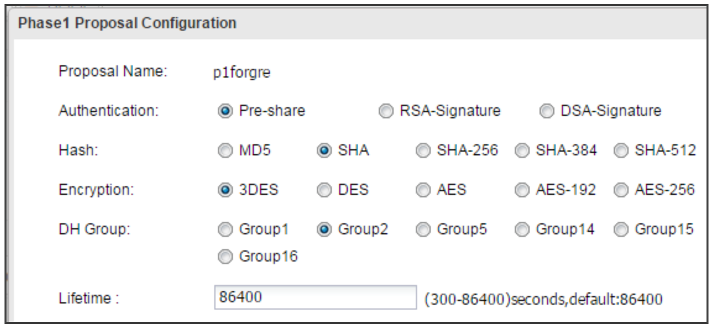
Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

In the Basic tab, configure the following settings:

- Peer
  - Peer Name: center2branch1_ ipsec
- Tunnel
  - Name: center2branch1_ipsec_tun- nel
  - Mode: tunnel
  - P2 proposal: p2forgre
- Keep the default of other parameters

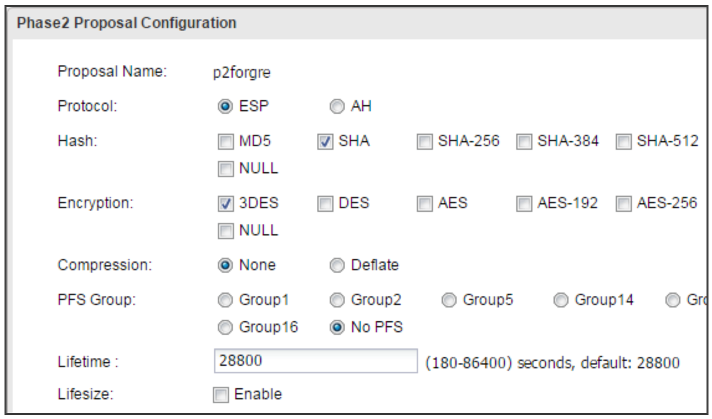
Step 2: Configuring IPSec VPN for device B

Create a P1 proposal and a P2 proposal.



Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.

- Proposal Name: p1forgre
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400



In the P2 Proposal tab, click **New**.

- Proposal Name: p2forgre
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800

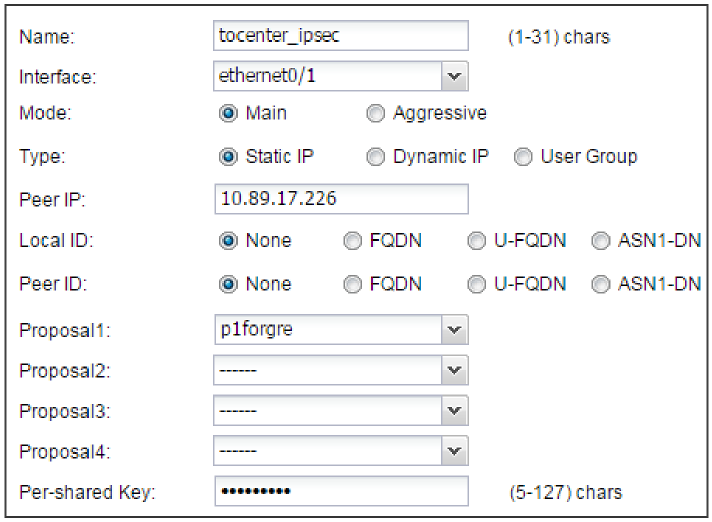
Step 2: Configuring IPSec VPN for device B

Configure a VPN peer.

Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

In the Basic tab, configure the following settings:

- Name: tocenter_ipsec
- Interface: ethernet0/1
- Mode: Main
- Type: Static IP
- Peer IP: 10.89.17.226
- Proposal1: p1forgre
- Pre-shared Key: hillstone
- Keep the default of other parameters

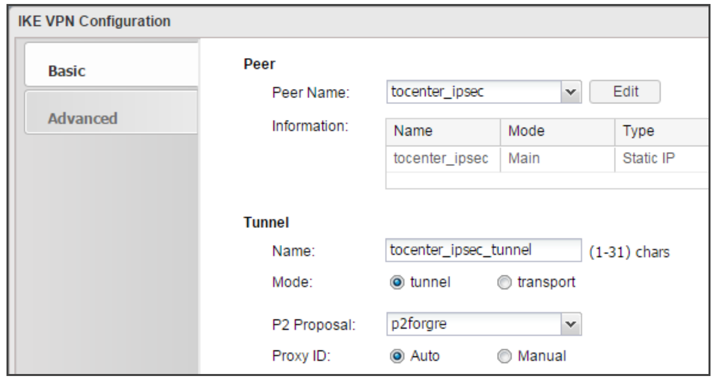


Step 2: Configuring IPSec VPN for device B

Configure IKE VPN.

Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

In the Basic tab, configure the following settings:



- Peer
  - Peer Name: tocenter_ipsec
- Tunnel
  - Name: tocenter_ipsec_tunnel
  - Mode: tunnel
  - P2 proposal: p2forgre
- Keep the default of other parameters

Configuring GRE VPN

GRE VPN configurations are not supported by WebUI. You need to use CLI to complete the following GRE VPN configurations.

Step 1: Configuring GRE VPN for device A

Create a GRE tunnel.

```
Device-A(config)# tunnel gre center2branch1
Device-A(config-tunnel-gre)# source 10.89.17.226
Device-A(config-tunnel-gre)# destination 10.89.18.131
Device-A(config-tunnel-gre)# interface eth0/1
Device-A(config-tunnel-gre)# next-tunnel ipsec center2branch1_ipsec_tunnel
```

1. In the global configuration mode, create a GRE tunnel:

   tunnel gre center2branch1

2. Specify the source IP address of the tunnel:

   source 10.89.17.226

3. Specify the destination IP address of the tunnel:

   destination 10.89.18.131

4. Specify the egress interface of the tunnel:

   interface ethernet0/1

5. Specify the IPSec VPN tunnel:

   next-tunnel ipsec center2branch1_ ipsec_tunnel

Step 1: Configuring GRE VPN for device A

Bind the GRE tunnl to the tunnel interface.

```
Device-A(config)# int tunnel1
Device-A(config-if-tun1)# tunnel gre center2branch1
```

1. Enter the interface configuration mode of tunnel1:

   int tunnel1

2. Bind the GRE tunnel:

   tunnel gre center2branch1

Step 2: Configuring GRE VPN for device B

Create a GRE tunnel.

1. In the global configuration mode, create a GRE tunnel:

   tunnel gre branch1

2. Specify the source IP address of the tunnel:

   source 10.89.18.131

3. Specify the destination IP address of the tunnel:

   destination 10.89.17.226

4. Specify the egress interface of the tunnel:

   interface ethernet0/1

5. Specify the IPSec VPN tunnel:

   next-tunnel ipsecto_center_tunnel

```
Device-B(config)# tunnel gre branch1
Device-B(config-tunnel-gre)# source 10.89.18.131
Device-B(config-tunnel-gre)# destination 10.89.17.226
Device-B(config-tunnel-gre)# interface eth0/1
Device-B(config-tunnel-gre)# next-tunnel ipsec to_center_tunnel
```

Bind the GRE tunnl to the tunnel interface.

1. Enter the interface configuration mode of tunnel1: int tunnel1

2. Bind the GRE tunnel: tunnel gre branch1

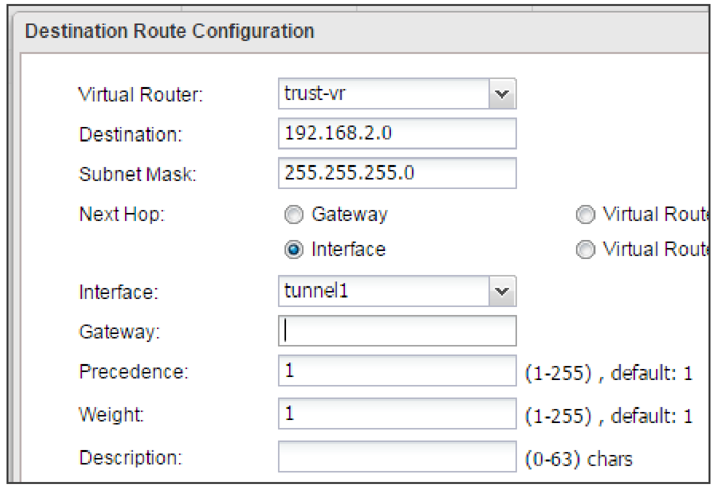
```
Device-B(config)# int tunnel1
Device-B(config-if-tun1)# tunnel gre branch1
```

Configuring Route and Policies

Step 1: Configuring route and policies for device A

Configure routes.

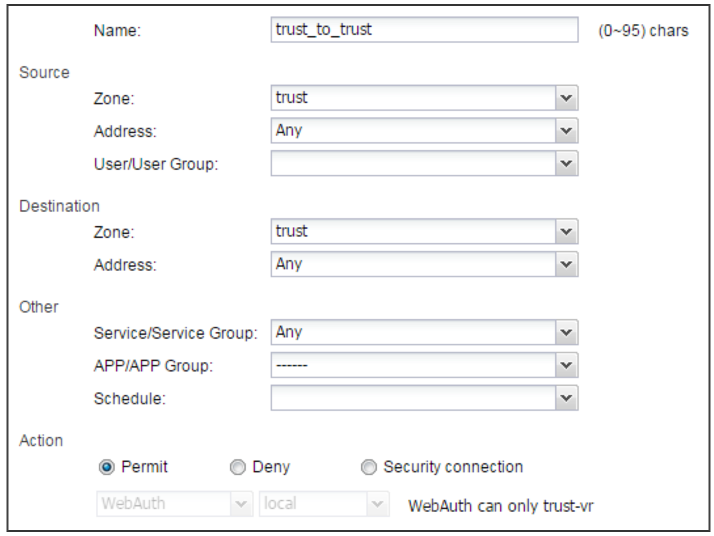
Select **Network > Routing > Destination Route**. Click **New**.



- Destination: 192.168.2.0
- Subnet Mask: 255.255.255.0
- Next Hop: Interface
- Interface: tunnel1
- Keep the default of other parameters

Step 1: Configuring route and policies for device A

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the Trust zone where the internal server locates.



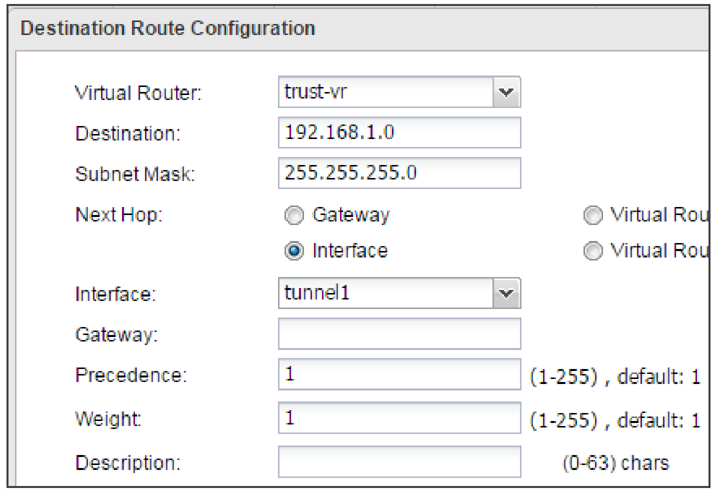
Select **Policy > Security Policy**. Click **New**.

- Name: trust_to_trust
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

Step 2: Configuring route and policies for device B

Configure routes.

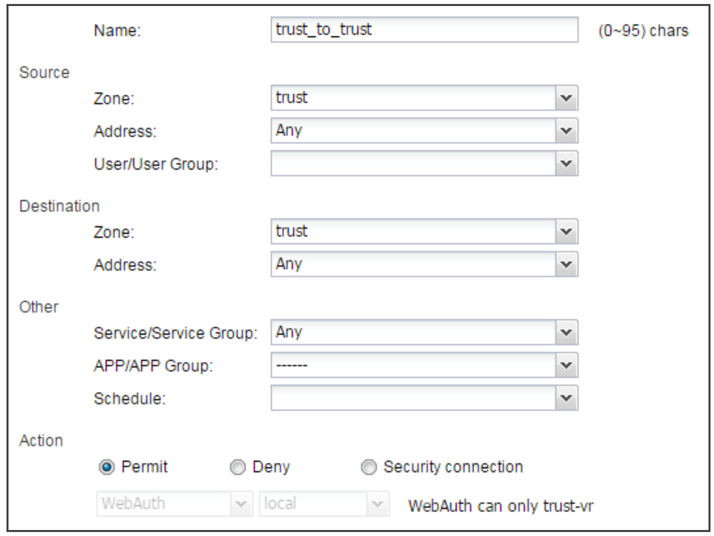
Select Network > Routing > Destination Route. Click **New**.



- Destination: 192.168.1.0
- Subnet Mask: 255.255.255.0
- Next Hop: Interface
- Interface: tunnel1
- Keep the default of other parameters

Step 2: Configuring route and policies for device B

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the Trust zone where the internal server locates.

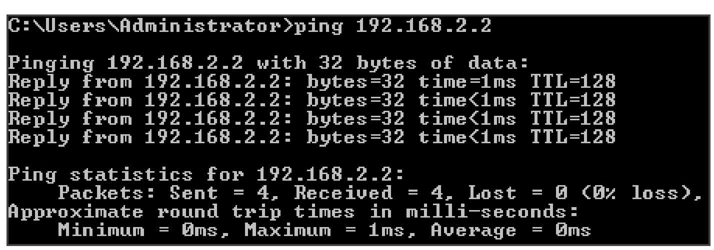


Select **Policy > Security Policy > New**.

- Name: trust_to_trust
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

Step 3: Verifying the connection between two private networks

After completing the above steps, the headquarters and branch can visit each other.

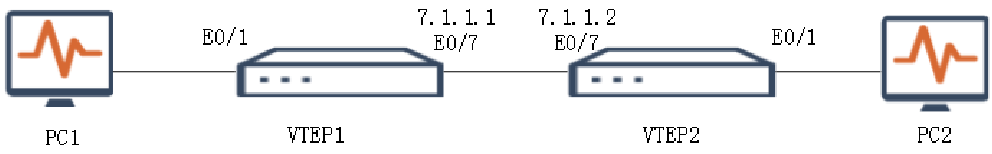


Configuring VXLAN Static Unicast Tunnel

This example introduces how to configure VXLAN static unicast tunnel. VXLAN uses MAC-in-UDP encapsulation to extend Layer 2 networks, allowing a large number of tenant accesses to virtual networks.

In the topology below, PC1 and PC2 communicate through the VXLAN tunnel (VNI100).

Note: In the same tunnel, different VNIs cannot communicate with each other.



Configuration Steps

VTEP1 Configuratio

Step 1: Configure the interface.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# ip address 10.1.2.1/24
hostname(config-if-eth0/1)# exit
```

Step2: Configure VXLAN tunnel.

```
hostname(config)# tunnel vxlan tunnel 1
hostname(config-tunnel-vxlan)# interface ethernet0/7
hostname(config-tunnel-vxlan)# destination 7.1.1.2
hostname(config-tunnel-vxlan)# vni 100
hostname(config-tunnel-vxlan)# exit
hostname(config)#
```

Step 3: Configure the tunnel interface and bind the Layer 2 security zone.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone l2-trust
hostname(config-if-tun1)#tunnel vxlan tunnel1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-addr -any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

VTEP2 Configuration

Step 1: Configure the interface.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
```

Step2: Configure VXLAN tunnel.

```
hostname(config)# tunnel vxlan tunnel 1
hostname(config-tunnel-vxlan)# interface ethernet0/7
hostname(config-tunnel-vxlan)# destination 7.1.1.1
hostname(config-tunnel-vxlan)# vni 100
hostname(config-tunnel-vxlan)# exit
hostname(config)#
```

Step 3: Configure the tunnel interface and bind the Layer 2 security zone.

```
hostname(config)#  interface tunnel1
hostname(config-if-tun1)# zone l2-trust
hostname(config-if-tun1)#tunnel vxlan tunnel1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure the policy

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-addr -any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step5: Verify result

PC1 and PC2 can communicate with each other through the VXLAN tunnel successfully.

High Availability

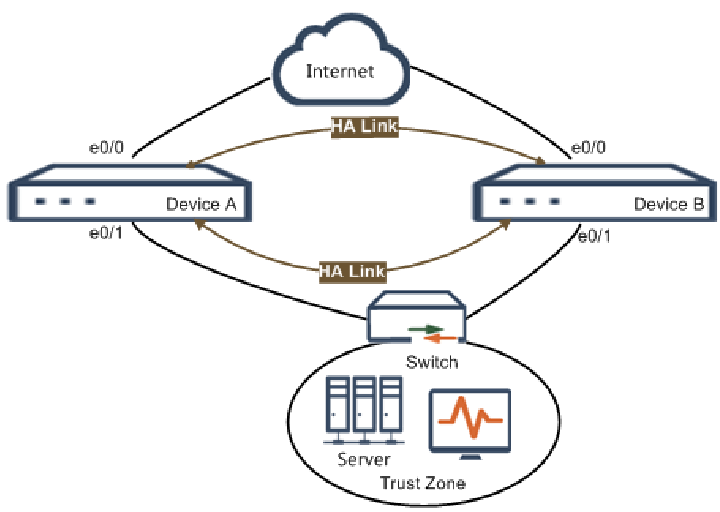
High Availability is a redundancy backup methhod. It uses two identical devices to ensure that when one fails to work, the other will immediately takes over to provide network consistency.

This chapter includes the following recipe:

Ensuring Uninterrupted Connection Using HA

This example introduces how to configure two devices working under Active-Passive mode to provide high availability for the protected network.

The topology gives a typical user scenario for HA. In the designed scenario, one (Device A)of the HA devices will be working under the active mode, while the other (Device B) is under passive mode. The active device will synchronize its data and status to the passive device. When the active one fails, the passive device will immediately switch to be active, without interrupting the network.

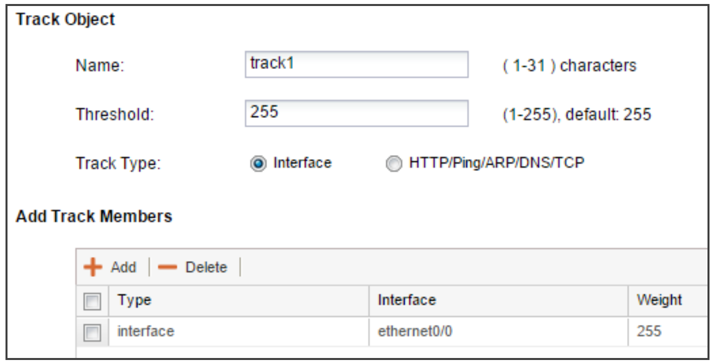


Configuration Steps

Step 1: Configuring track object of Device A. This monitors Device A's eth0. When A's interface fails to work, Device B takes over.

Select **Object > Track Object**, and click **New**.

- Name: track1
- Threshold: 255
- Track Type: Select **Interface**, and click **Add**. In the prompt, select ethernet0/0, and weight as 255.

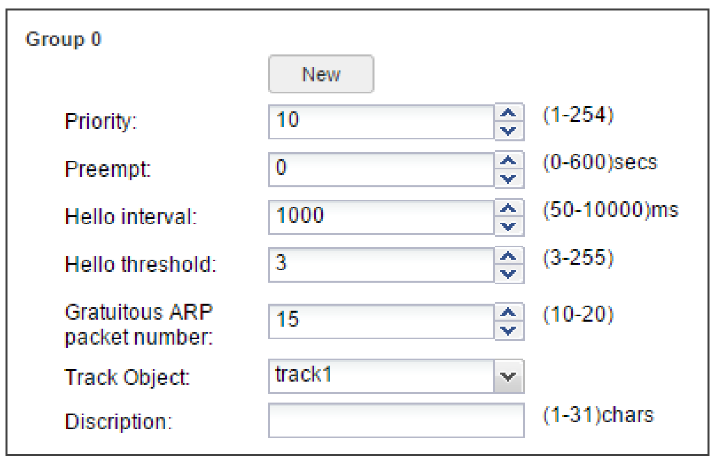


Step 2: Configuring HA

Device A

Select **System > HA**, under the Group0 part:

- Priority: 10
- Track Object: track1

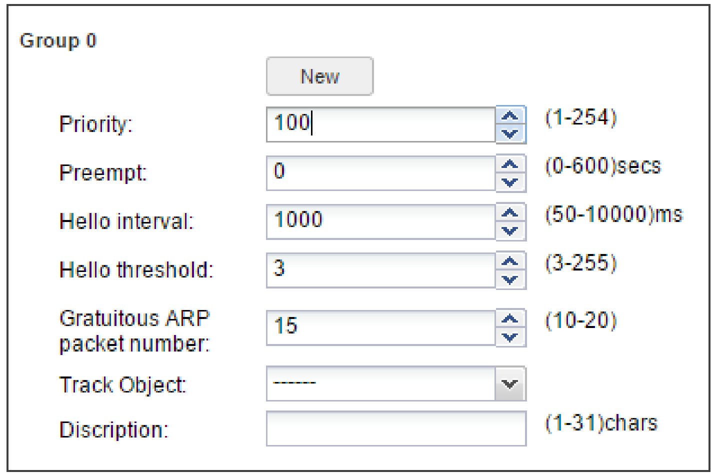


Step 2: Configuring HA

Device B

Select **System > HA**, under the Group0 part:

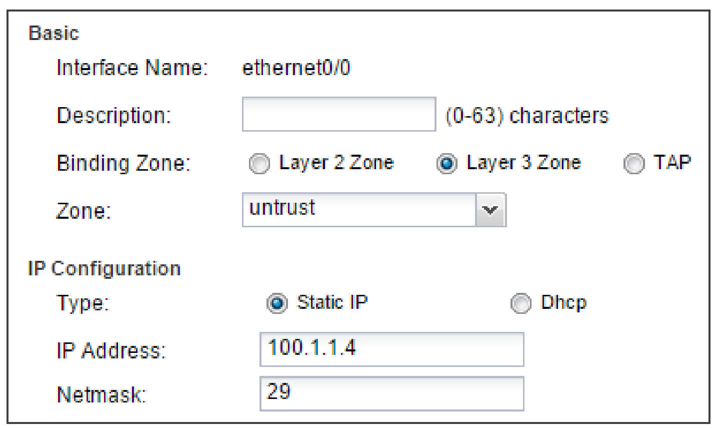
- Priority: 100



Step 3: Configuring Device A's interface and policy

Select **Network > Interface**, and double click ethernet0/0.

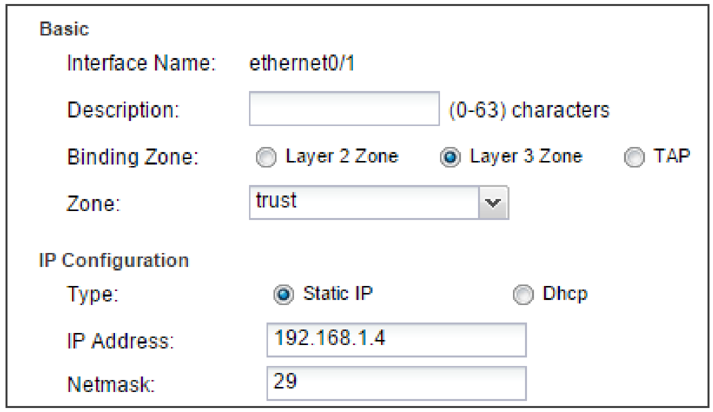
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 100.1.1.4
- Netmask: 29



Step 3: Configuring Device A's interface and policy

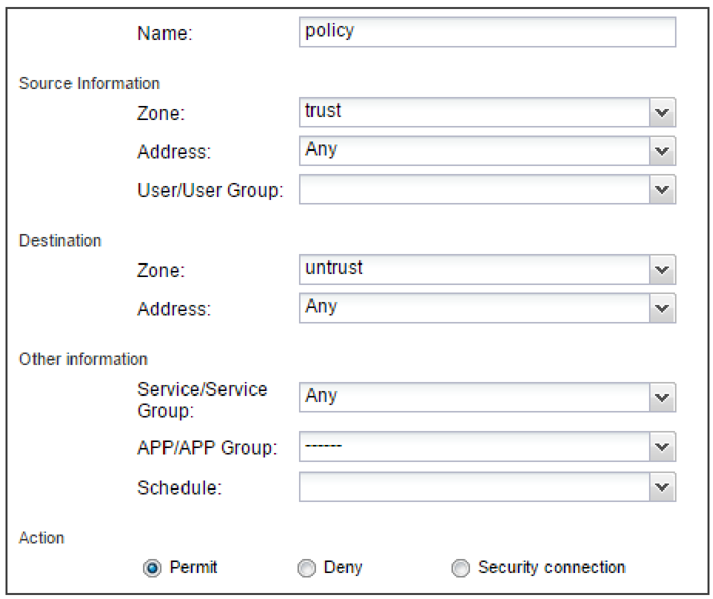
Select **Network > Interface**, and double click ethernet0/1.

- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.4
- Netmask: 29



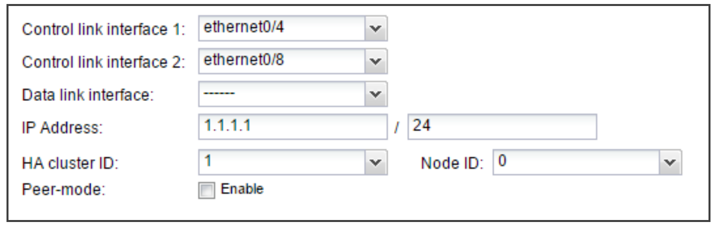
Select **Policy > Security Policy**, and click **New**.

- Name: policy
- Source Information
  - Zone: trust
  - Address: Any
- Destination Information
  - Zone: untrust
  - Address: Any
- Other Information
  - Service/Server Group: Any
- Action: Permit



Step 4: Configuring HA control link interface and enabling HA

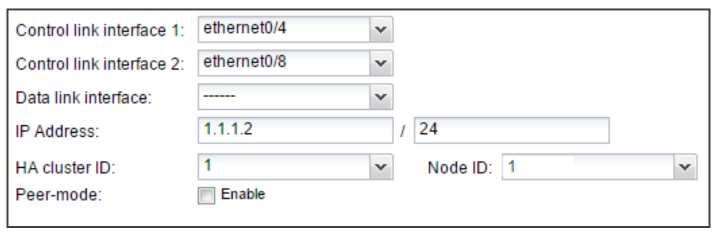
Device A



Select **System > HA**.

- Control Link Interface 1 : ethernet0/4
- Control Link Interface 2 : ethernet0/8
- IP Address: 1.1.1.1/24
- HA Cluster ID: 1

Device B



Select **System > HA**.

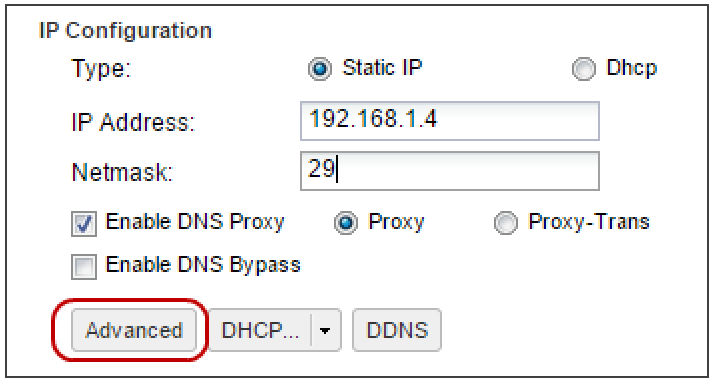
- Control Link Interface 1 : ethernet0/4
- Control Link Interface 2 : ethernet0/8
- IP Address: 1.1.1.2/24
- HA Cluster ID: 1

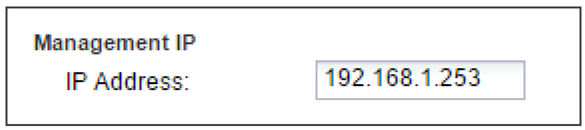
Step 5: Configuring management IP of active and passive devices after synchronization

Device A

Select **Network > Interface**, and double click ethernet0/1. Under the Basic tab, under IP Configuration, click **Advanced**.

- Management IP
  - IP Address: 192.168.1.253

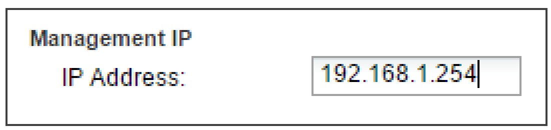




Device B

Select **Network > Interface**, and double click ethernet0/1. In the Basic tab, under IP Configuration, click **Advanced**.

- Management IP
  - IP Address: 192.168.1.254



Step 6: Results

After configuration, select **System > System Information**. Behind the "HA state" item, the device's HA status will show.

Device A

- HA Status: Master

Device B

- HA Status: Backup

Device A :

Device B :

When Device A fails to forward traffic or its eth0/0 is disconnected, Device B will turn to Active and starts forwarding without interrupting protected network.

Select **System > System Information**. The HA state item shows device's status.

Device A

- HA Status: Monitor Failed

Device B

- HA Status: Master

Device A :

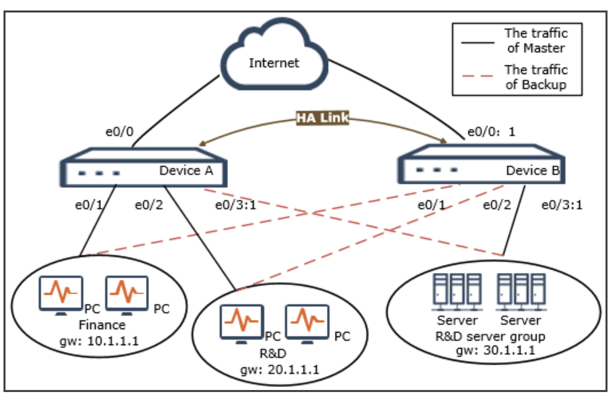
Device B :

Ensuring Uninterrupted Connection Using HA AA

This example introduces how to configure two devices working under Active-Active mode to provide high availability for the protected network.

Before configuration, confirm that the two Hillstone devices built into HA typical networking mode use exactly the same hardware platform, firmware version, and install the same license, and the two devices use the same interface to connect to the network.

As shown in the figure below, the two devices forming the HA AA mode are Device A and Device B. After the configuration is complete, both devices will enable the HA function. The system elects Device A as the master device of group 0, and Device B preempts it as the master device of group 1. Device A performs synchronization configuration with Device B. Under normal circumstances, the two devices run their own tasks independently: Device A forwards the traffic that the finance department and R&D department access the network; Device B forwards the traffic that the R&D server group accesses the network. If one of the devices fails, the other device can run its own work while taking over the work of the failed device to ensure uninterrupted work. For example: Device B fails to work, Device A will forward the network traffic of the R&D server group while forwarding the network traffic of the finance department and the R&D department.



Configuration Steps

Step 1: Configuring HA

Device A

Select **System > HA**, under the Group0 part:

- Priority: 10
- Preempt: 3
- Gratuitous ARP packet number: 15

Device A

Select **System > HA**, under the Group0 part, click **New**. Under the Group1 part:

- Priority: 200
- Preempt: 3

Device B

Select **System > HA**, under the Group0 part:

- Priority: 200
- Preempt: 3
- Gratuitous ARP packet number: 15

Step 1: Configuring HA

Device B

Select **System > HA**, under the Group0 part, click **New**. Under the Group1 part:

- Priority: 20
- Preempt： 3
- Gratuitous ARP packet number: 15

Step 2: Configuring HA control link interface and enabling HA

Device A

Select **System > HA**.

- Control Link Interface 1： ethernet0/4
- IP Address: 100.0.0.1/24
- HA Cluster ID: 1

Device B

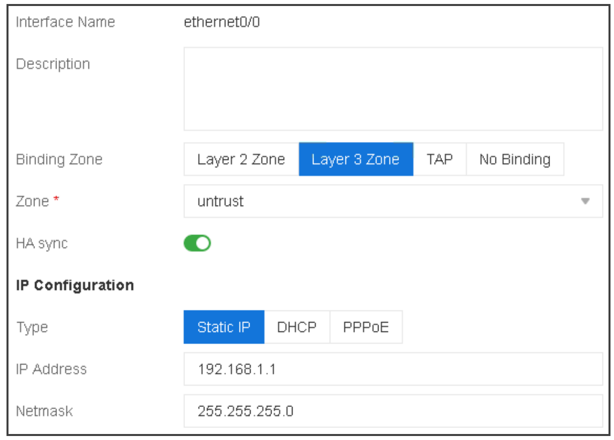
Select **System > HA**.

- Control Link Interface 1： ethernet0/4
- IP Address: 100.0.0.100/24
- HA Cluster ID: 1

Step 3: Configuring Device A's interface

Select **Network > Interface**, and double click ethernet0/0.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0

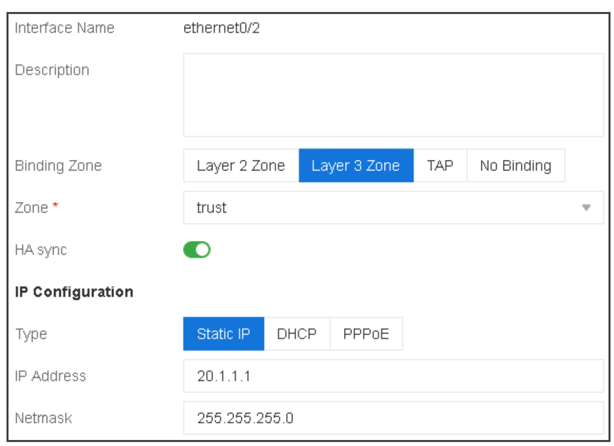


Select **Network > Interface**, and double click ethernet0/1.

- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 10.1.1.1
- Netmask: 255.255.255.0

Select **Network > Interface**, and double click ethernet0/2.

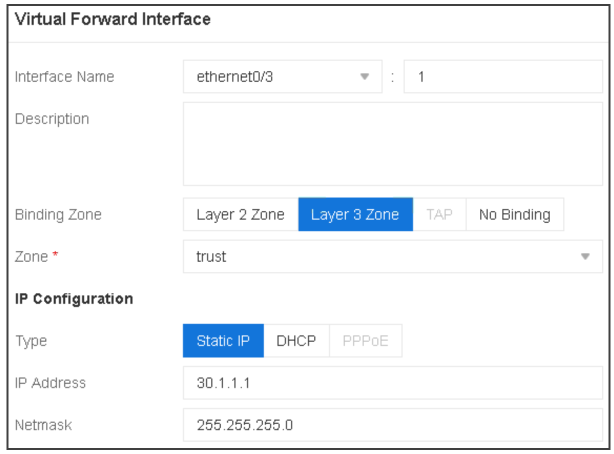
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 20.1.1.1
- Netmask: 255.255.255.0



Step 3: Configuring Device A's interface

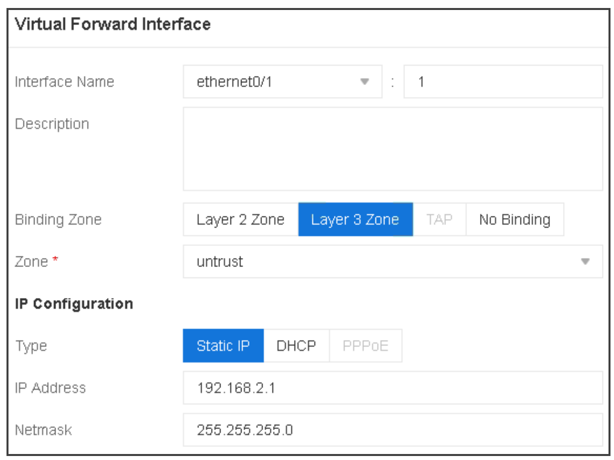
Select **Network > Interface**, click **New**.Choose **Virtual Forward Interface**.

- Interface Name: ethernet0/3:1
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 30.1.1.1
- Netmask: 255.255.255.0



Select **Network > Interface**, click **New**.Choose **Virtual Forward Interface**.

- Interface Name: ethernet0/0:1
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 192.168.2.1
- Netmask: 255.255.255.0

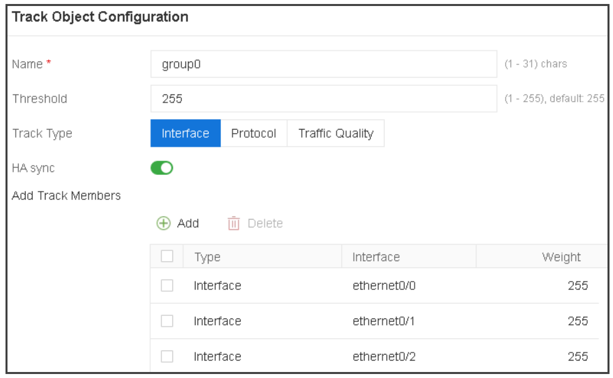


Step 4: Configuring track object of device. Use the monitoring object to monitor the status of the interfaces of Device A and B. Once one of the interfaces fails to work, it will be switched.

Device A

Select **Object > Track Object**, and click **New**.

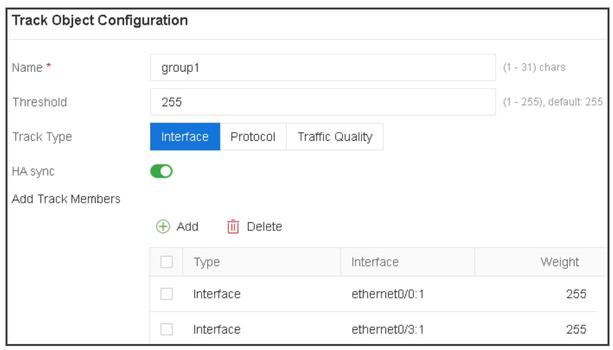
- Name: group0
- Track Type: Interface
- Add Track Members: Click **Add**. In the prompt, select ethernet0/0、 ethernet0/1、 ethernet0/2.



Device A

Select **Object > Track Object**, and click **New**.

- Name: group1
- Track Type: Interface
- Add Track Members: Click **Add**. In the prompt, select ethernet0/0:1、 ethernet0/3:1.



Step 4: Configuring track object of device. Use the monitoring object to monitor the status of the interfaces of Device A and B. Once one of the interfaces fails to work, it will be switched.

Device A

Select **System > HA**, under the Group0 part:

- Track Object: group0

Under the Group1 part:

- Track Object: group1

Group0 :

Group1 :

Device B

Select **System > HA**, under the Group0 part:

- Track Object: group0

Under the Group1 part:

- Track Object: group1

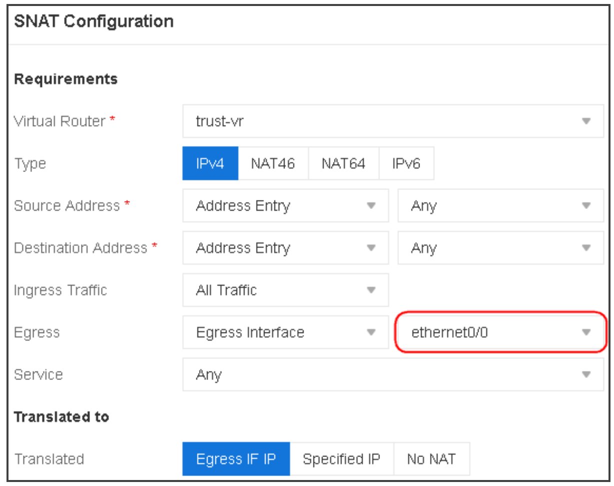
Group0 :

Group1 :

Step 5: Configuring Device A's SNAT

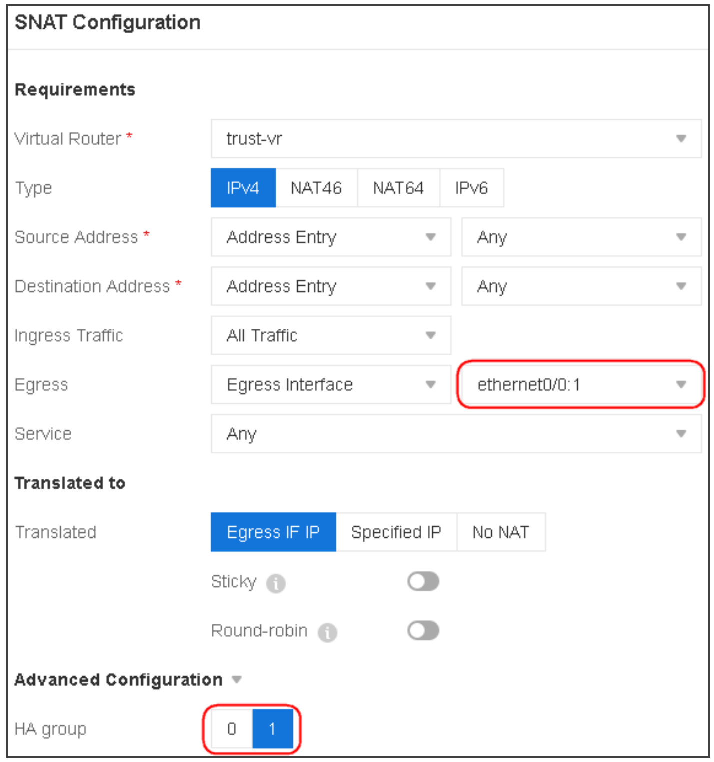
Select **Policy > NAT > SNAT**, and click **New**.

- Requirements
  - Type: IPv4
  - Source Address: Address Entry; Any
  - Destination Address: Address Entry; Any
  - Egress: Egress Interface; ethernet0/0
- Translated to
  - Egress IF IP



Step 5: Configuring Device A's SNAT

Select **Policy > NAT > SNAT**, and click New.

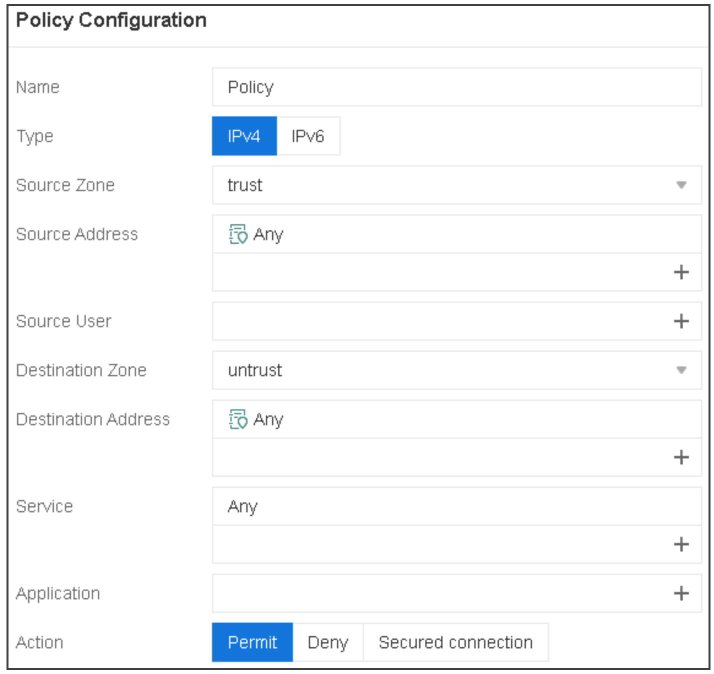


- Requirements
  - Type: IPv4
  - Source Address: Address Entry; Any
  - Destination Address: Address Entry; Any
  - Egress: Egress Interface; ethernet0/0:1
- Translated to
  - Egress IF IP
- Advanced Configuration
  - HA group: 1

Step 6: Configuring Device A's policy

Select **Policy > Security Policy > Policy**, click **New** and choose **Policy**.

- Name: policy
- Source Information
  - Zone: trust
  - Address: Any
- Destination Information
  - Zone: untrust
  - Address: Any
- Other Information
  - Service: Any
- Action: Permit



Step 7: Results

After configuration, select **System > System Information**. Behind the "HA state" item, the device's HA status will show.

Device A

- HA State:

  group0: Master group1: Backup

Device B

- HA State:

  group0: Backup group1: Master

Device A :

Device B :

When Device B fails to work, Device A will forward the network traffic of the R&D server group while forwarding the network traffic of the finance department and the R&D department.

Select **System > System Information**. The HA state item shows device's status.

Device A

- HA Status:

  group0: Master group1: Master

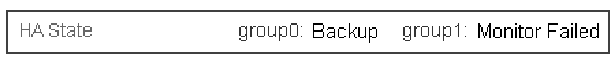
Device B

- HA Status:

  group0: Backup group1: Monitor Failed

Device A :

Device B :



Quality of Service (QoS)

QoS adopts the concept "pipe" to indicate traffic control method. A pipe is a bandwidth limit. The system divides bandwidth by creating pipe of different sizes.

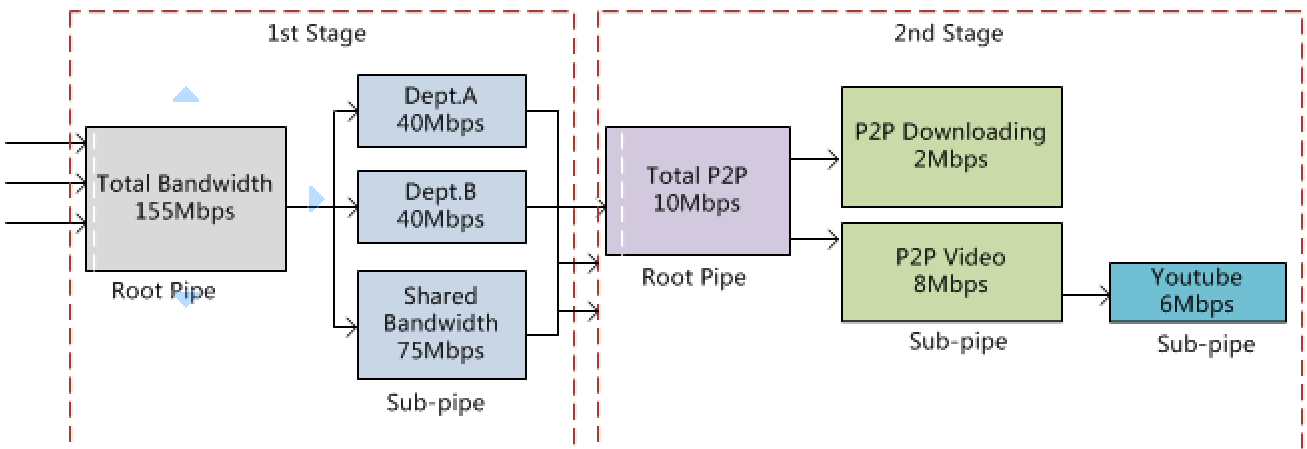
This chapter contains the following recipe:

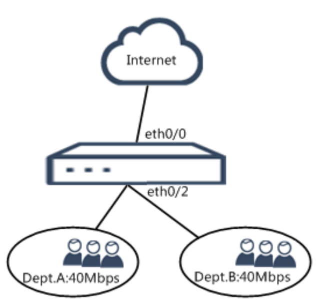
QoS Control

This examples shows how to control Internet bandwidth allocation to different users and applications. The key feature that applies in this situation is 2-Stage QoS flow control.

As shown in the topology below, a company of 155 MB Internet bandwidth has a 2-Stage QoS requirement:

- In 1st Stage QoS: Within the 155 Mbps bandwidth, 40 Mbps will be allocated to Department A, 40 Mbps to Department B, and the remaining 75 Mbps will be shared by all employees.
- In 2nd Stage QoS: The total P2P flow is limited to 10 Mbps, in which downloading is limited to 2 Mbps, streaming video is limited to 8 Mbps, and within the video bandwidth, Youku streaming is limited to 6 Mbps.



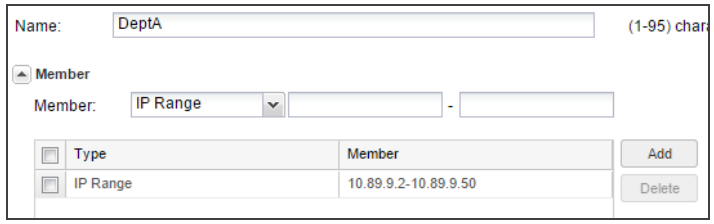


Configuration Steps

Step 1: Creating address entries for Dept. A and Dept. B

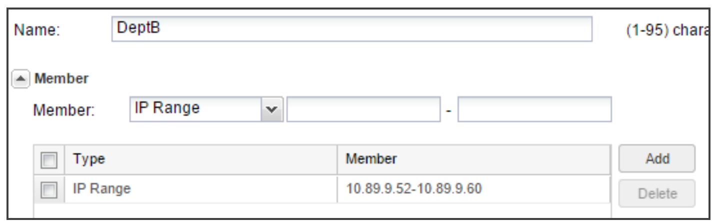
Select **Object > Address Entry**, and click **New**.

- Name: DeptA
- Member: select IP Range, and enter "10.89.9.2" and "10.89.9.50" and click **Add**.



Create another address entry:

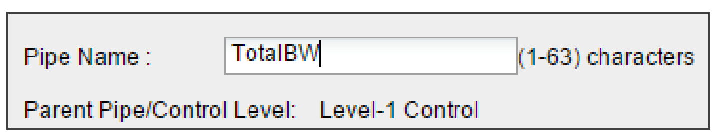
- Name: DeptB
- Member: select IP Range, and enter "10.89.9.52" and "10.89.9.60" and click **Add**.



Step 2: Create a root pipe of 155 Mbps under Level-1 Control

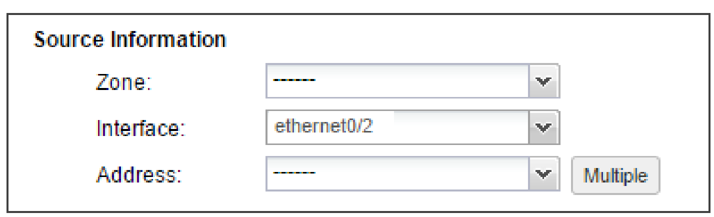
Select **Policy > QoS**, click **Level-1 Control**, and click **New > Pipe**.

- Pipe Name: TotalBW



In the same tab, click **New**.

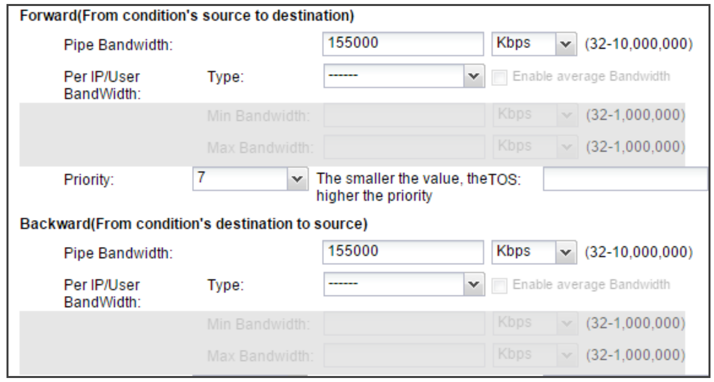
- Source Information
  - Interface: ethernet0/2



Step 2: Create a root pipe of 155 Mbps under Level-1 Control

Under the Action tab:

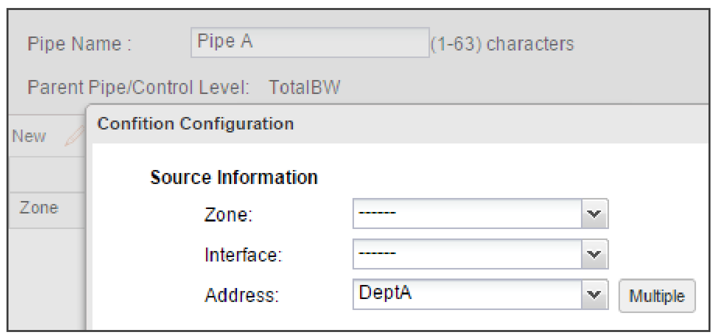
- Forward
  - Pipe Bandwidth: 155000 Kbps
- Backward
  - Pipe Bandwidth: 155000 Kbps

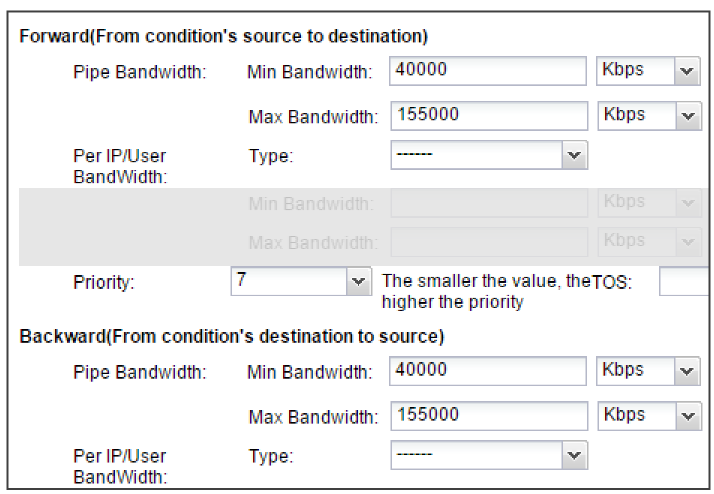


Step 3: Creating sub-pipes for two departments below root pipe

Select root pipe "TotalBW"and click **New**.

- Pipe Name: pipeA
- Click **New**, and under Source Information, select "DeptA" as Address.
- Click the Action tab:
  - Forward: Bandwidth: min: 40000 Kbps; max: 155000 Kbps
  - Backward Bandwidth: min:40000 Kbps; max: 155000 Kbps





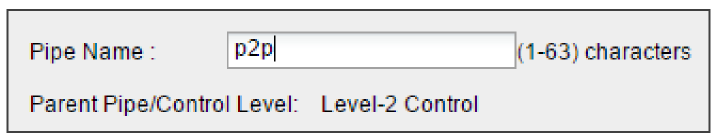
Step 3: Creating sub-pipes for two departments below root pipe

Use the same steps to create "pipe B":

- Pipe name: pipeB
- Source address: DeptB
- (Forward and Backward) min bandwidth: 40000 kbps
- (Forward and Backward) max bandwidth: 155000 kbps

Step 4: Creating root pipe "p2p" under Level-2 control to limit P2P total to 10 Mbps

Select **Policy > QoS**, select Level-2 Control and click **New > Pipe**.

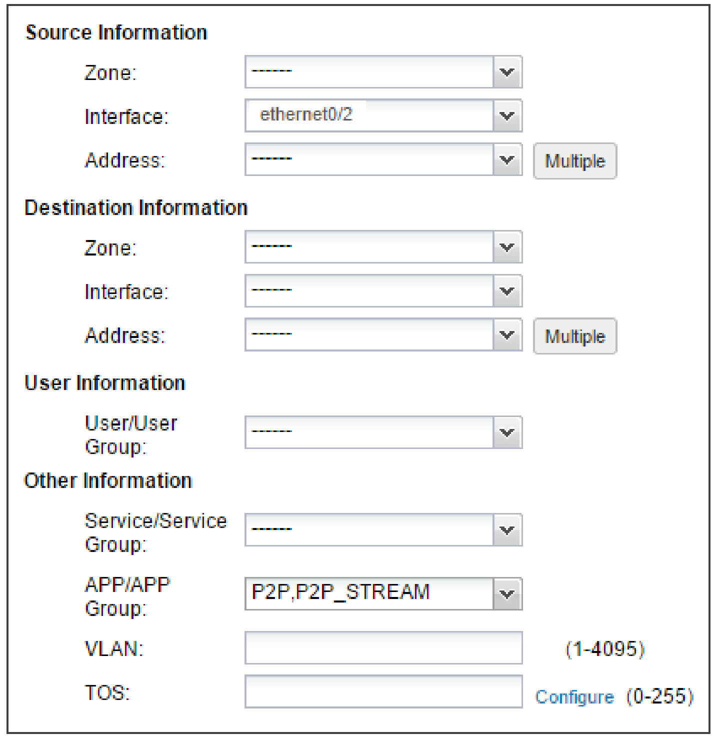


- Pipe Name: p2p

Step 4: Creating root pipe "p2p" under Level-2 control to limit P2P total to 10 Mbps

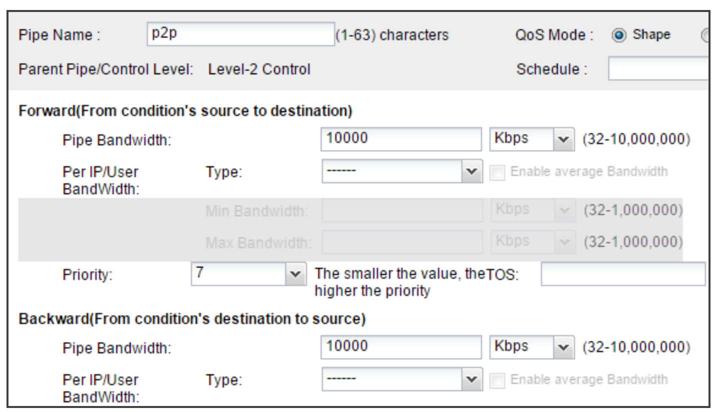
In the same tab, click **New**.

- Source Information
  - Interface: ethernet0/2
- Other
  - APP/APP Group: P2P. P2P_ Stream



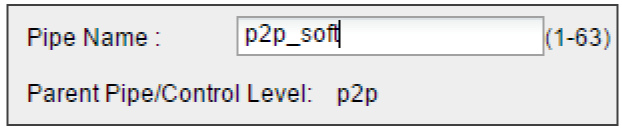
Under the Action tab:

- Forward
  - Bandwidth: 10000 kbps
- Backward:
  - Bandwidth: 10000 kbps



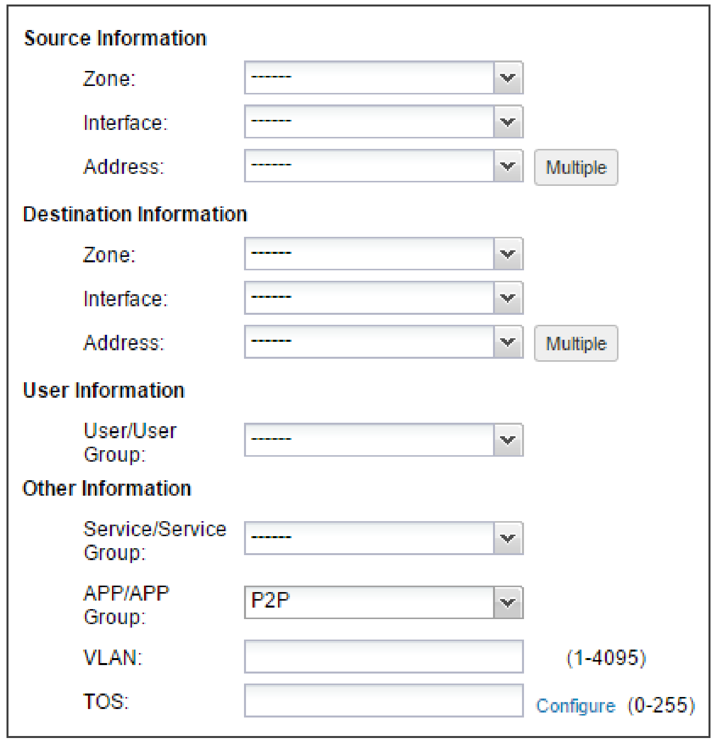
Step 5: Creating sub pipes under root pipe "p2p"

1. Creating a sub-pipe to limit p2p software



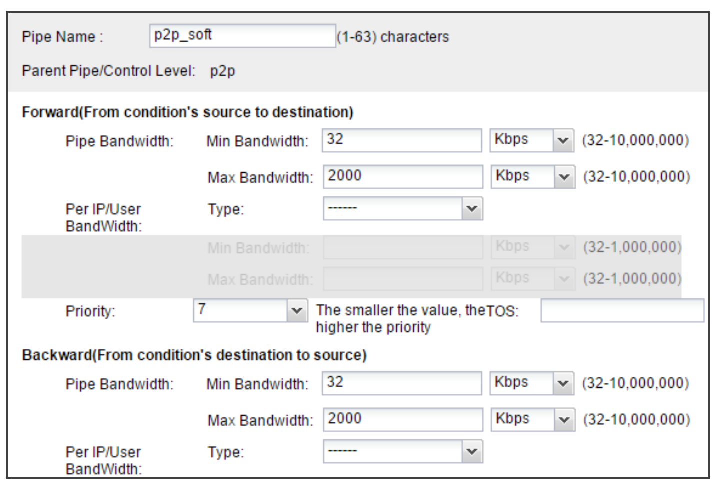
Under Level-2 Control, select root pipe "p2p", and click **New > Pipe**.

- Pipe Name: p2p_soft
- Click **New**: in the prompt, select **P2P** as APP/APP Group.
- Select the Action tab:
    - Forward bandwidth: min: 32; max 2000
    - Backward bandwidth: min: 32; max: 2000



2. Creating a sub-pipe to limit p2p video streaming

Under Level-2 Control, select root pipe "p2p", and click **New > Pipe**.



- Pipe Name: p2p_stream
- Click **New**: in the prompt, select **P2P_Stream** as APP/APP Group.
- Select the Action tab:
    - Forward bandwidth: min: 32; max 8000
    - Backward bandwidth: min: 32;

Step 5: Creating sub pipes under root pipe "p2p"

max: 8000

3. Creating a sub-pipe to limit p2p video streaming

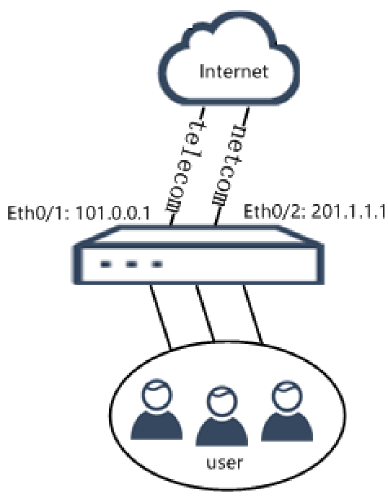
Under Level-2 Control, select sub pipe "p2p_stream", and click **New > Pipe**.

- Pipe Name: p2p_stream
- Click **New**: in the prompt, select **Youku** and **Youku_Stream** as APP/APP Group.
- Select the Action tab:
  - Forward bandwidth: min: 32; max 6000
  - Backward bandwidth: min: 32; max: 6000

Outbound Link Load Balance

This example shows how to configure outbound link load balancing. Through the configuration of efficient drainage strategy to achieve dynamic link load balancing, improve the export bandwidth utilization.

As shown in the following figure, this lab environment simulates the deployment of equipment at the second-level ISP exit scene.The second-level ISP rent Tele-com, China Netcom and other operators of the bandwidth to the user to achieve Internet access. The figure use 101.0.0.1 to connect to the Internet by Tele-com and 201.1.1.1 to connect to Netcom.

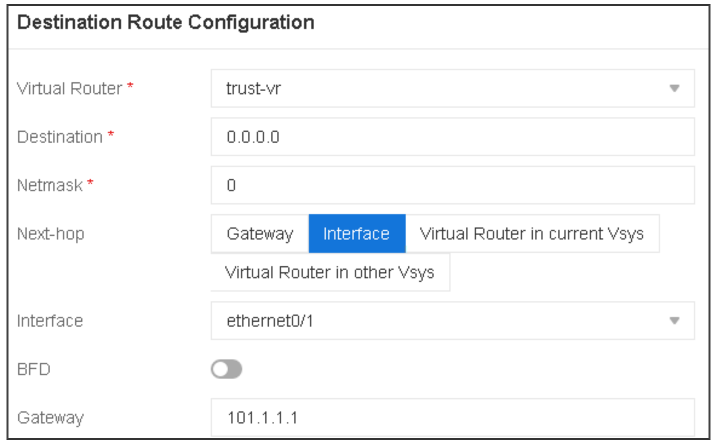


Configuration Steps

Step 1: Configure multiple equal-cost routes

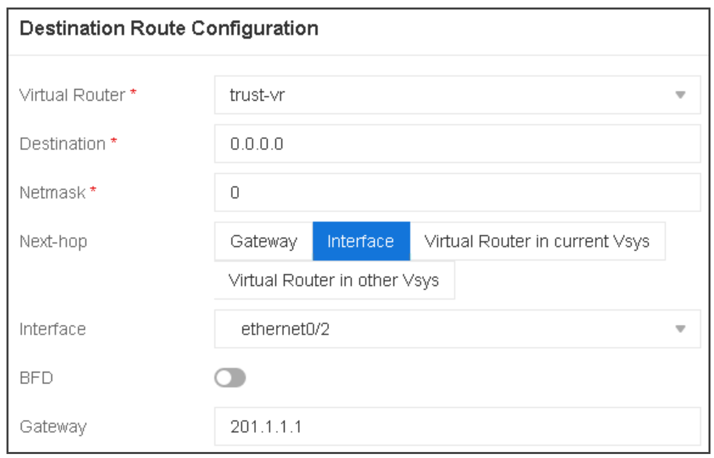
1.Select **Network > Routing >Destination Route**, and click **New**.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: interface
- Interface: ethernet0/1
- Gateway: 101.1.1.1



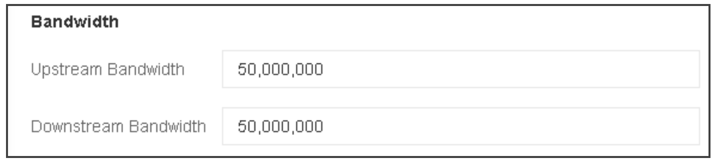
2.Select **Network > Routing >Destination Route**, and click **New**to configure another equal-cost route.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: interface
- Interface: ethernet0/2
- Gateway: 201.1.1.1



Step 2: Configure the outbound interface bandwidth

Network > Interface, select interface ethernet0 / 1, and click **Edit** to configure the bandwidth as 50M (according to the actual situation to determine the value of the configuration bandwidth).

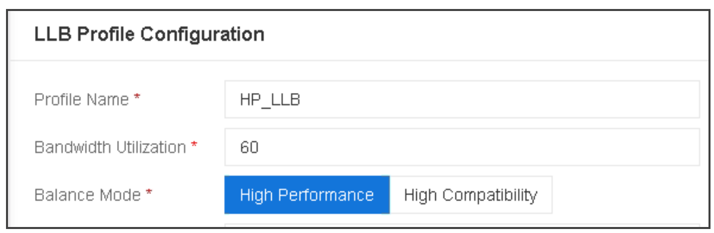


- Bandwidth
  - Up Bandwidth： 50000000bps
  - Down Bandwidth： 50000000bps

Follow the same steps to set the bandwidth of the interface ethernet0 / 2 to 50M.

Step 3: Configure the outbound load balancr profile

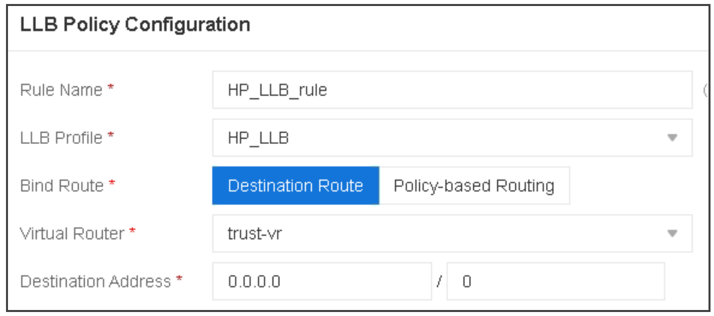
Select **Network > Outbound >Profile**, click **New**.



- Profile： HP_LLB
- Bandwidth Utillzation : 60%
- Balance Mode： High Performance

Step 4: Configure the outbound load balancr rule

Select **Network > Outbound >Rule**, click **New**.



- Rule Name： HP_LLB_rule
- LLB Profile： Select the Profile "HP_ LLB"
- Bind Route： Destination Route
- Vitual Router： trust-vr
- Destination Address： 0.0.0.0/0

Step 5: Verify that outbound load balance is in effect

After completing the above steps, use the test tool to construct traffic through ethernet0/1 and ethernet0/2, respectively, and then observe the traffic on each link.By changing the size of outgoing traffic,you can find that the traffic on two links can be adjusted equitably. The system routing mechanism is as follows:

- When the bandwidth of each link does not exceed 30M (50M*60%), the system calculates the link overhead based on the link delay, jitter and packet loss rate. The link with the lower link overhead eventually allocates more traffic, while the other link has less traffic,but the two links are basically balanced.
- When the link bandwidth exceeds 30M, the system adds the bandwidth utilization factor to the calculation, that is, the system calculates the link overhead based on the delay, jitter, packet loss rate and bandwidth utilization. The link with lower link overhead eventually allocates more traffic, while the other link has less traffic, but the two links are basically balanced.

Q&A

- Q: What factors in the network affect the link load balancing routing of the system?

  A: The delay, jitter, packet loss rate and bandwidth utilization of each link are the impact factors. System can intelligently oute and dynamically adjust the traffic load of each link by monitoring the delay, jitter, packet loss rate and bandwidth utilization of each link in real-time.

- Q: Which modes do link load balancing support?

  A: Two load balancing modes are supported, namely, high performance and high compatibility modes.

  - High Performance - In this mode, system adjusts link to keep the link balance as fast as possible
  - High Compatibility - In this mode, When the link load changes, system does not switch the link frequently, but ensures that the service is as far as possible on the previous link. This mode is suitable for services that are sensitive to link switching, such as banking services, only when the previous link is overloaded.

Threat Prevention

Threat prevention, that device can detect and block network threats occur. By configuring the threat protection function, Device can defense network attacks, and reduce losses caused by internal network.

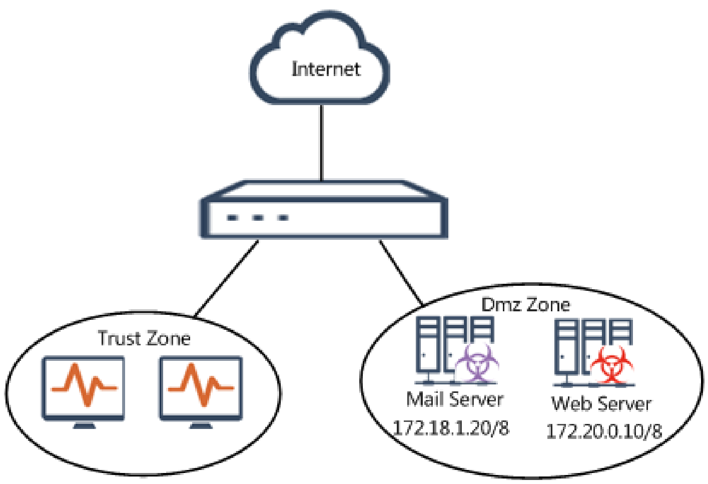
This chapter includes the following recipes:

Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection

This example introduces how to use Abnormal Behavior Detection to find attacks about servers as early as possible, and integrate with Mitigation to protect servers better.

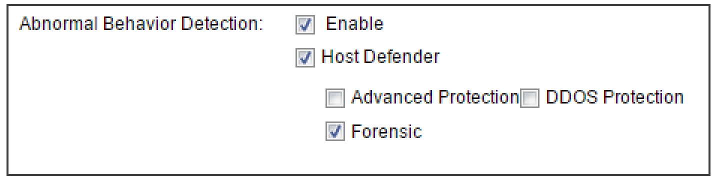
As shown in the topology, the device is deployed in the data center exit. After enable and configure the Abnormal Behavior Detection, when a Web server is infected by SYN flood frequently, a mail server is infected by port scan attacks periodically, Trojan implanted to the intranet host, Trojan fake domain name by DGA algorithm technology, and connect external network control server, the administrator can find these attacks and protect the internal hosts and servers.

* To use Abnormal Behavior Detection, apply and install the StoneShield license.



Configuration Steps

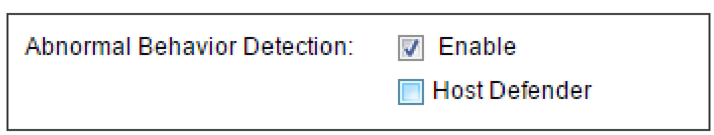
Step 1: Enabling Abnormal Behavior Detection to defend internal hosts



Select **Network > Zone**. Select '**trust**' zone, click **Edit**, and select the <Threat Protection> tab.

- Abnormal Behavior Detection: Select the **Enable** check box .
- Host Defender : Select the **Host Defender** check box. To enable the abnormal behavior detection of the HTTP factor, select the **Advanced Protection** check box. To enable the DDoS protection for the host, select the **DDoS Protection** check box. To capture and save the corresponding evidence that leads to the alarm of abnormal behavior, select **Forensic**.

Step 2: Configuring the critical asset object (Web Server and Mail Server)



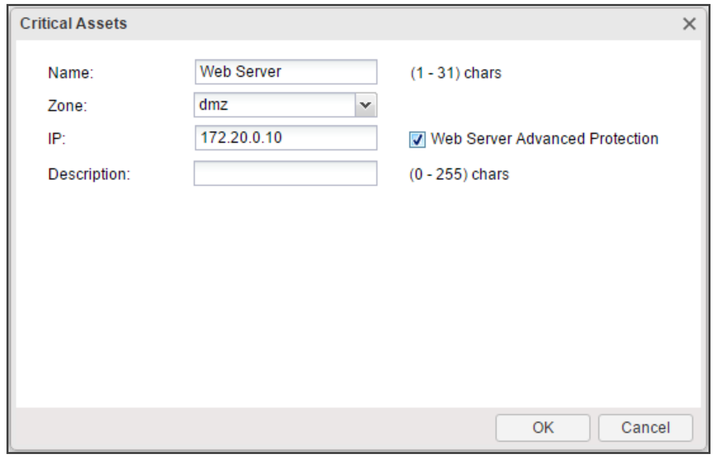
Select **Network > Zone**. Select '**dmz**' zone, click **Edit**, and select the <Threat Protection> tab.

- Abnormal Behavior Detection: Select the **Enable** check box .

Step 2: Configuring the critical asset object (Web Server and Mail Server)

1. Configuring the Abnormal Behavior Detection object (Web Server), and enabling the web server advanced protection.

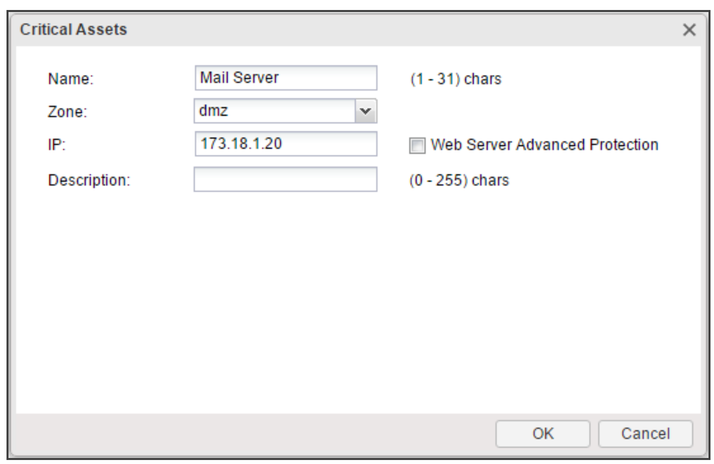
Click **Object** > **Critical Assets**, and click **New**.



- Name: Web Server
- Type: Server
- IP: 172.20.0.10
- Web Server Advanced Protection: Select the check box.

2. Configuring the Abnormal Behavior Detection object (Mail Server)

Click **Object** > **Critical Assets**, and click **New**.



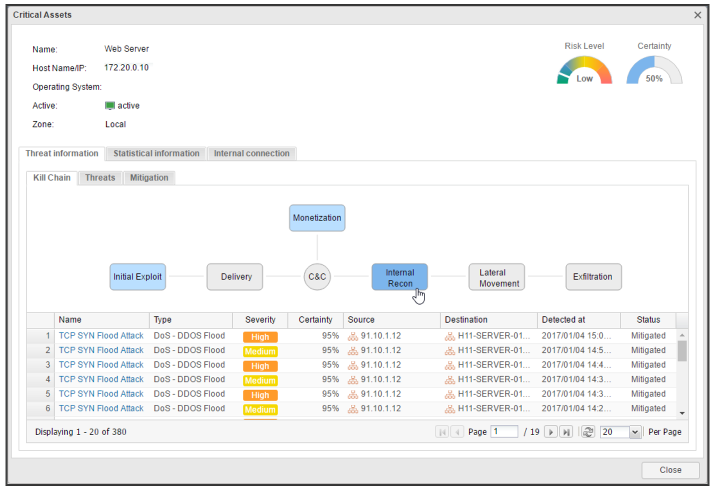
- Name: Mail Server
- Type: Server
- IP: 172.18.1.20

Step 3: Viewing the results of Abnormal Behavior Detection

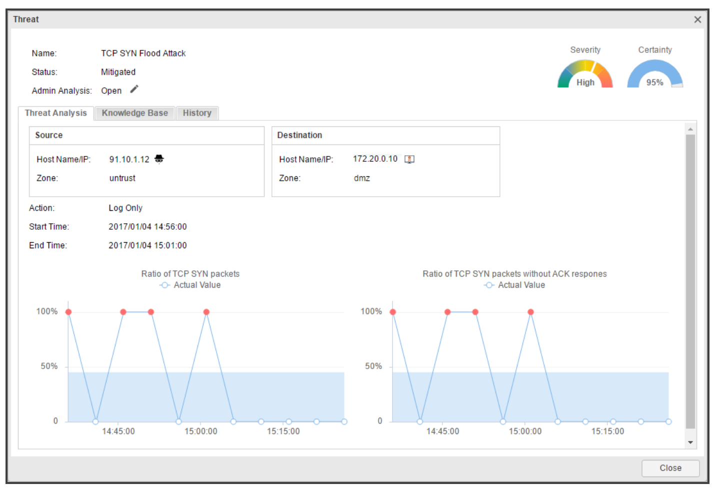
1. Viewing the results from iCenter

Results of Web Server:

- Select **iCenter>Critical Assets**, click the critical assets name **'Web Server'** link in the list, to view the information of this critical asset.

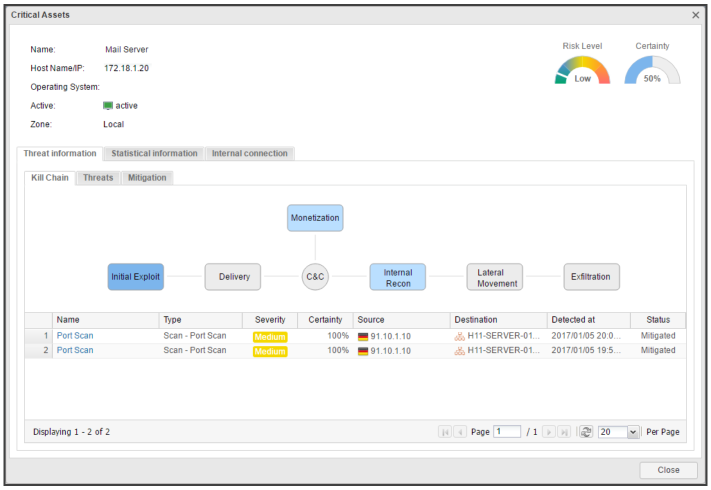


- For example, click the **Internal Recon> 'TCP SYN Flood Attack'** link in the kill chain list, to view the Abnormal Behavior Detection information and the trend chart of the actual value, predictive value of the detected object.

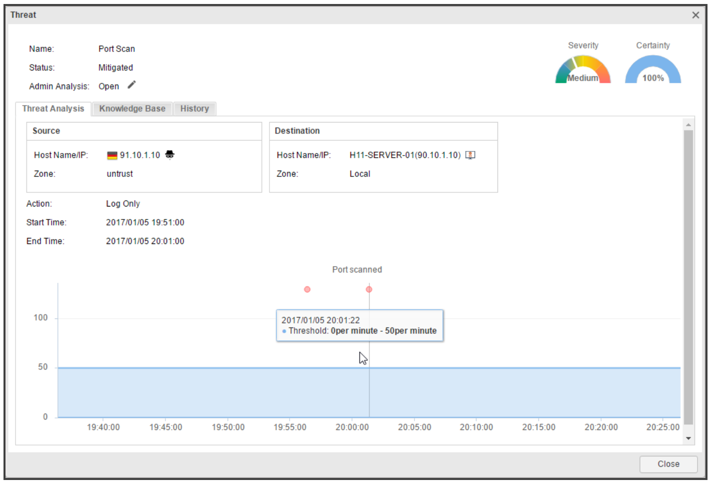


Step 3: Viewing the results of Abnormal Behavior Detection

Results of Mail Server:



- Select **iCenter>Critical Assets**, click the critical assets name **'Mail Server'** link in the list, to view the information of this critical asset.



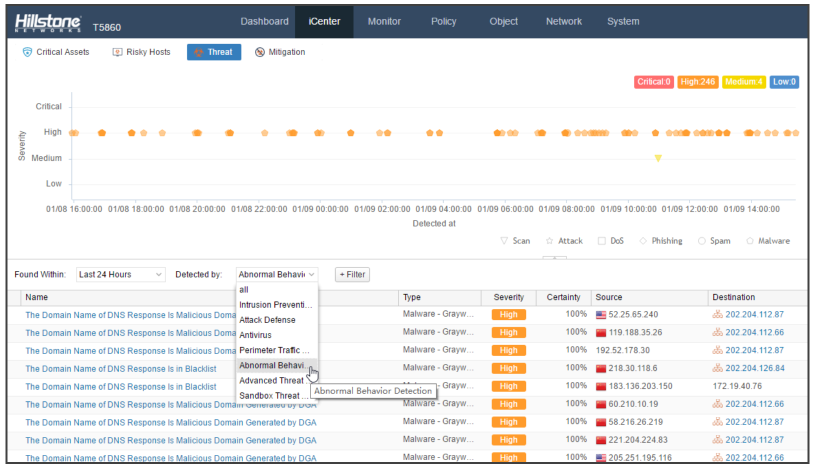
- For example, click the **Initial Exploit> 'Port Scan'** link in the kill chain list, to view the Abnormal Behavior Detection information and the trend chart of the baseline, thresholds of the detected object.

Step 3: Viewing the results of Abnormal Behavior Detection

Results of Internal Host:

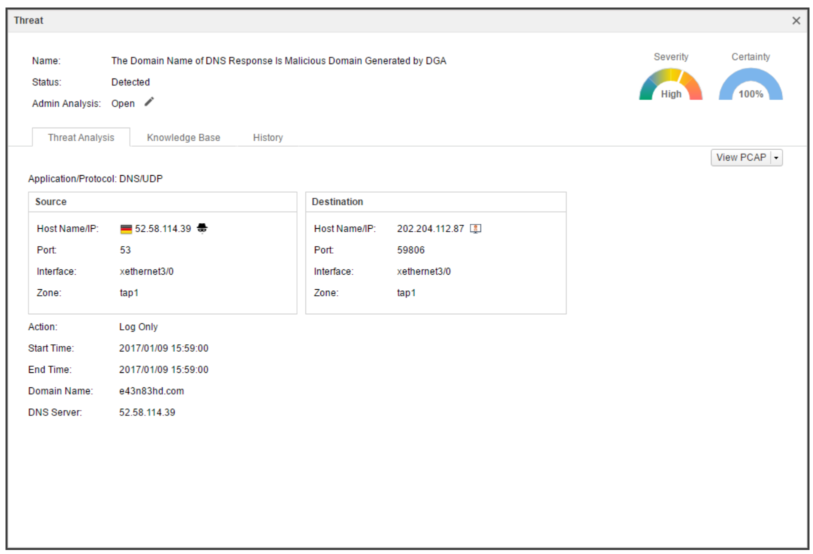
1. Click **iCenter > Threat**, and click Filter to add conditions.

   - Detected by : Abnormal Behavior Detection



2. For example, click the **The Domain Name of DNS Response Is Malicious Domain Generated by DGA** link in the list, to view the malware and abnormal behavior attack details detected according the DNS mapping.

In **Threat Analysis** tab, you can view the information of host that send DGA fake domain name attack.

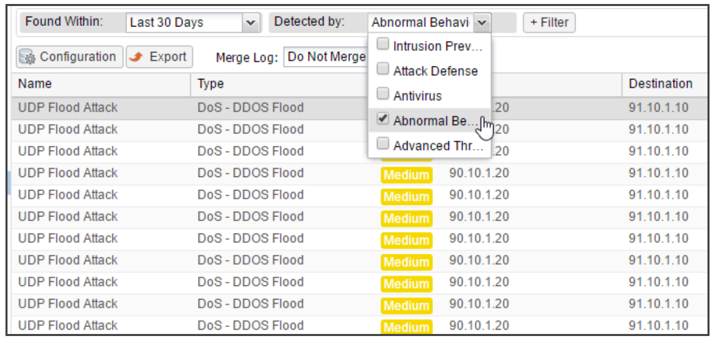


Step 3: Viewing the results of Abnormal Behavior Detection

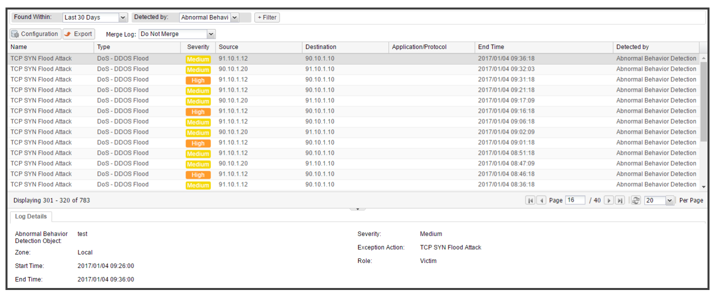
2. Viewing the results from threat log

1. Select **Monitor>Log>Threat**, click Filter to add conditions to show logs that march your filter.

- Detected By: Abnormal Behavior Detection

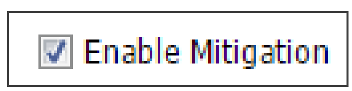


2. The log of Abnormal Behavior Detection will be displayed.



Step 4: Integrating with Mitigation, and configuring the mitigation rules for attacks.

Select **iCenter> Mitigation> Mitigation Rule**, and select the **Enable Auto Mitigation** check box.

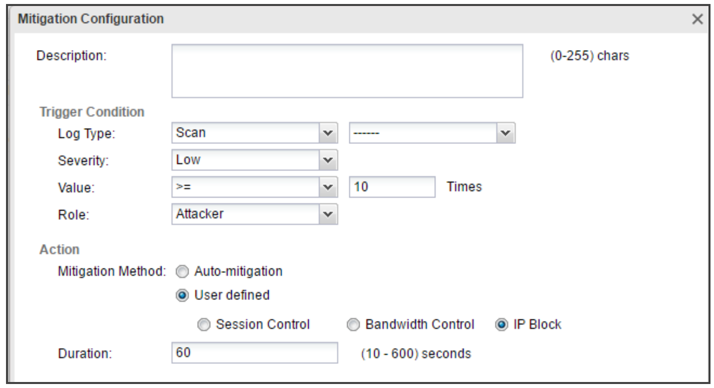


Step 4: Integrating with Mitigation, and configuring the mitigation rules for attacks.

Configuring mitigation rules for Port Scan

In **Mitigation Rule**page, click **New**

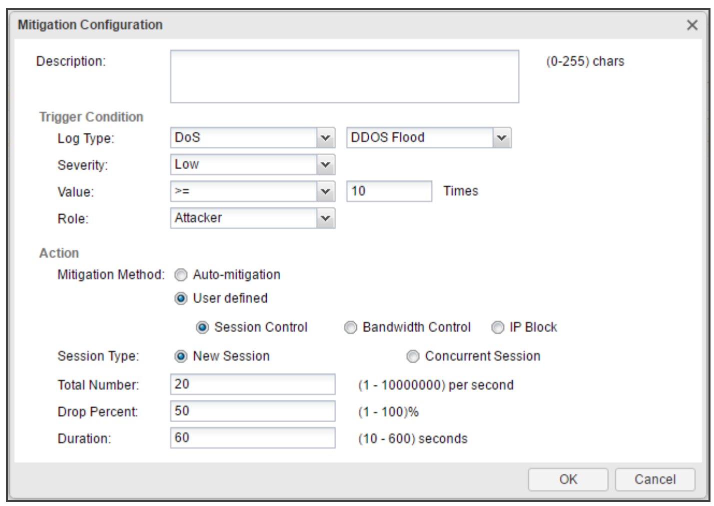
- Log Type: Scan
- Severity: Low
- Value: >= 10 Time
- Action Type: User defined > IP Block
- Duration: 60



Configuring mitigation rules for TCP SYN Flood Attack

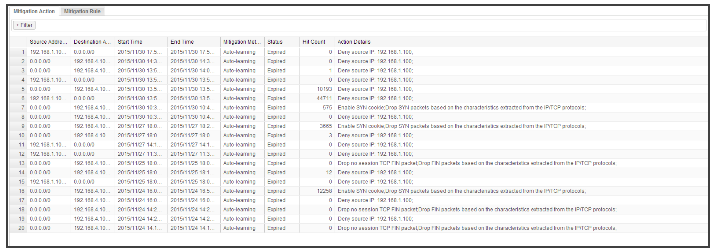
In **Mitigation Rule**page, click **New**

- Log Type: DoS> DDoS Flood
- Severity: Low
- Value: >= 10 Time
- Role: Attacker
- Action Type: User defined >Session Control
- Session Type: New Session
- Total Number: 20
- Drop Percent: 50
- Duration: 60



Step 5: Viewing the results of mitigation rules

Click **iCenter > Mitigation>Mitigation Action** to view the mitigation action results details of mitigation rules


Mitigation Action Mitigation Rule

+ Filter

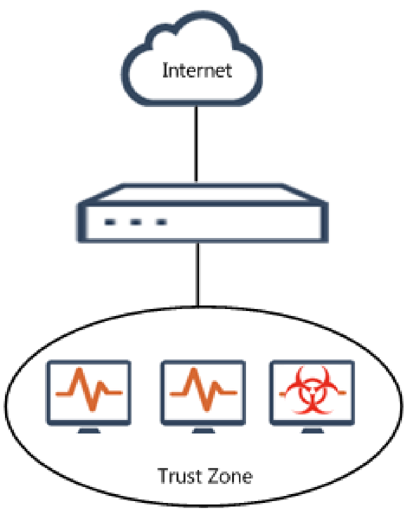
	Source Addre...	Destination A...	Start Time	End Time	Mitigation Met...	Status	Hit Count	Action Details
1	192.168.1.10...	0.0.0.0/0	2015/11/30 17:5...	2015/11/30 17:5...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
2	0.0.0.0/0	192.168.4.10...	2015/11/30 14:3...	2015/11/30 14:3...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
3	0.0.0.0/0	192.168.4.10...	2015/11/30 13:5...	2015/11/30 14:0...	Auto-learning	Expired	1	Deny source IP: 192.168.1.100;
4	192.168.1.10...	0.0.0.0/0	2015/11/30 13:5...	2015/11/30 13:5...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
5	0.0.0.0/0	192.168.4.10...	2015/11/30 13:5...	2015/11/30 13:5...	Auto-learning	Expired	10193	Deny source IP: 192.168.1.100;
6	192.168.1.10...	0.0.0.0/0	2015/11/30 13:5...	2015/11/30 13:5...	Auto-learning	Expired	44711	Deny source IP: 192.168.1.100;
7	0.0.0.0/0	192.168.4.10...	2015/11/30 10:3...	2015/11/30 10:4...	Auto-learning	Expired	575	Enable SYN cookie;Drop SYN packets based on the characteristics extracted from the IP/TCP protocols;
8	0.0.0.0/0	192.168.4.10...	2015/11/30 10:3...	2015/11/30 10:4...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
9	0.0.0.0/0	192.168.4.10...	2015/11/27 18:0...	2015/11/27 18:2...	Auto-learning	Expired	3665	Enable SYN cookie;Drop SYN packets based on the characteristics extracted from the IP/TCP protocols;
10	0.0.0.0/0	192.168.4.10...	2015/11/27 18:0...	2015/11/27 18:0...	Auto-learning	Expired	3	Deny source IP: 192.168.1.100;
11	192.168.1.10...	0.0.0.0/0	2015/11/27 14:1...	2015/11/27 14:1...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
12	192.168.1.10...	0.0.0.0/0	2015/11/27 11:3...	2015/11/27 11:3...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
13	0.0.0.0/0	192.168.4.10...	2015/11/25 18:0...	2015/11/25 18:0...	Auto-learning	Expired	0	Drop no session TCP FIN packet;Drop FIN packets based on the characteristics extracted from the IP/TCP protocols;
14	0.0.0.0/0	192.168.4.10...	2015/11/25 18:0...	2015/11/25 18:1...	Auto-learning	Expired	12	Deny source IP: 192.168.1.100;
15	192.168.1.10...	0.0.0.0/0	2015/11/25 18:0...	2015/11/25 18:0...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
16	0.0.0.0/0	192.168.4.10...	2015/11/24 16:0...	2015/11/24 16:5...	Auto-learning	Expired	12258	Enable SYN cookie;Drop SYN packets based on the characteristics extracted from the IP/TCP protocols;
17	0.0.0.0/0	192.168.4.10...	2015/11/24 16:0...	2015/11/24 16:0...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
18	0.0.0.0/0	192.168.4.10...	2015/11/24 14:2...	2015/11/24 14:2...	Auto-learning	Expired	0	Drop no session TCP FIN packet;Drop FIN packets based on the characteristics extracted from the IP/TCP protocols;
19	0.0.0.0/0	192.168.4.10...	2015/11/24 14:2...	2015/11/24 14:2...	Auto-learning	Expired	0	Deny source IP: 192.168.1.100;
20	0.0.0.0/0	192.168.4.10...	2015/11/24 14:1...	2015/11/24 14:1...	Auto-learning	Expired	0	Drop no session TCP FIN packet;Drop FIN packets based on the characteristics extracted from the IP/TCP protocols;

Finding Malware Attacks via Advanced Threat Detection

This example shows how to use the Advanced Threat Detection to detect the malicious behavior and recognise the APT attacks, thus find malware earlier and stop the spread of its in internal network .

As shown in the topology, the device is deployed in the data center exit. After enable and configure the Advanced Threat Detection, when a internal host is infected by Trojan attacks, the administrator can find and solve this attack.

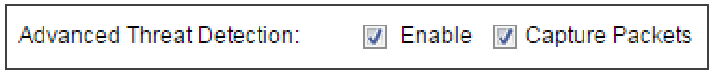
* To use Advanced Threat Detection, apply and install the StoneShield license.



Configuration Steps

Step 1: Enabling Advanced Threat Detection and capture packets to defend internal hosts

Select **Network > Zone**. Select "**trust**" zone, click **Edit**, and select the <Threat Protection> tab.

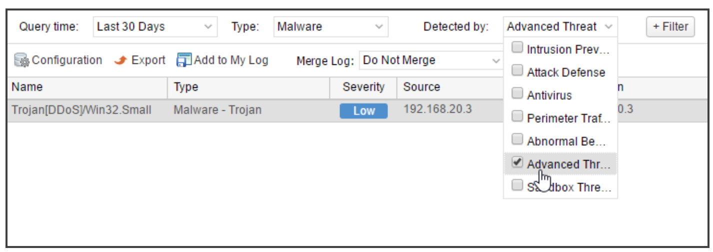


- Advanced Threat Detection: Select the **Enable** check box .
- Capture Packets: Select the check box , the system will save the evidence messages, and support to download it.

Step 2: Viewing the results of detection

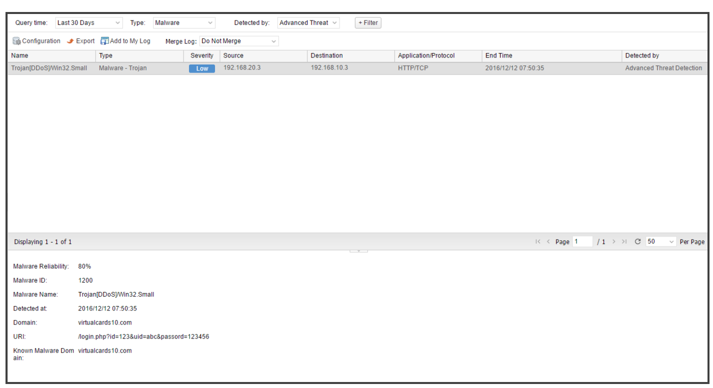
Viewing the results from threat log

1. Select **Monitor>Log>Threat**, click **+Filter**to add the conditions.



- Type: Malware
- Detected By: Advanced Threat Detection

2. Tthe logs of Trojan attacks will be displayed.



Step 2: Viewing the results of detection

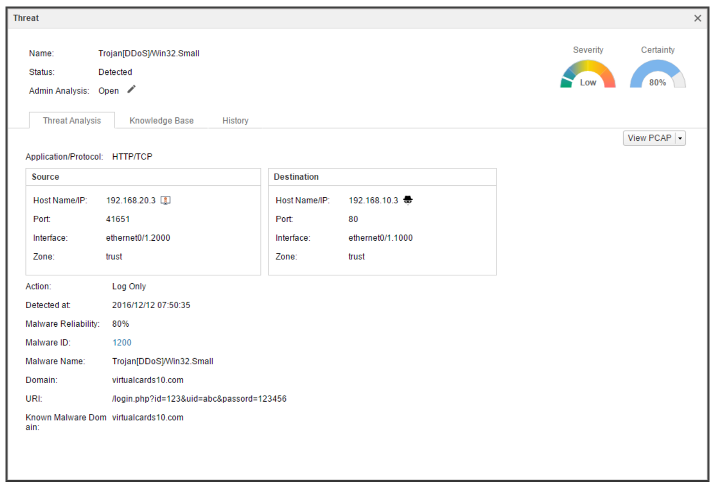
Viewing the results from iCenter

1. Select **iCenter>Threat**, set up filters as follows:

- Type: Malware
- Detected By: Advanced Threat Detection

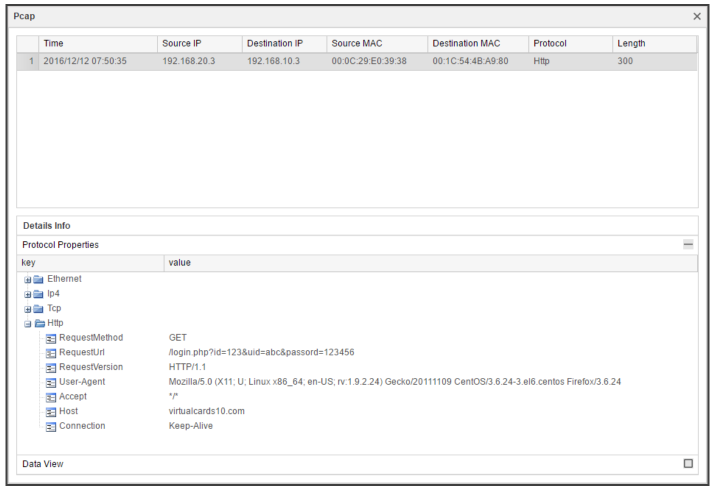
Viewing the detected time, severity, threat map .etc

2. Click the threat name link in the list, to view advanced threat detection information, malware reliability information etc.

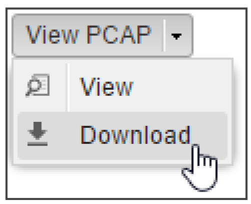


Step 2: Viewing the results of detection

3. Click **View PCAP** drop-down list and select **View**, to view the detail of packets.

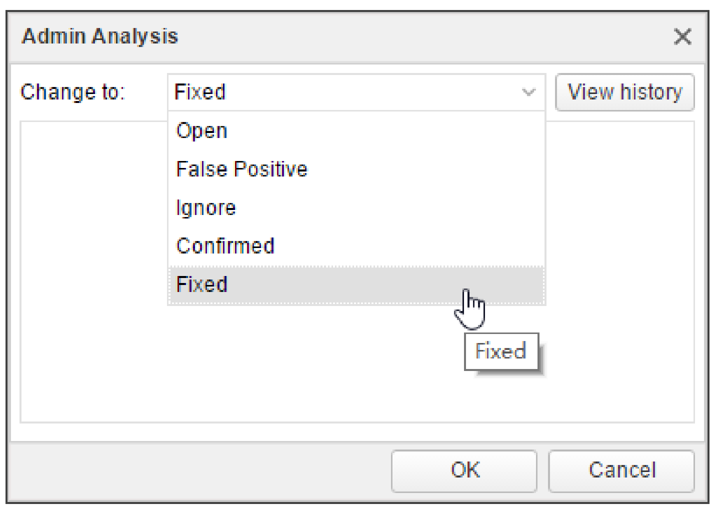


4. Click **View PCAP** drop-down list and select **Download**, the data packets will be downloaded to local.



Step 3: Mark the threat status

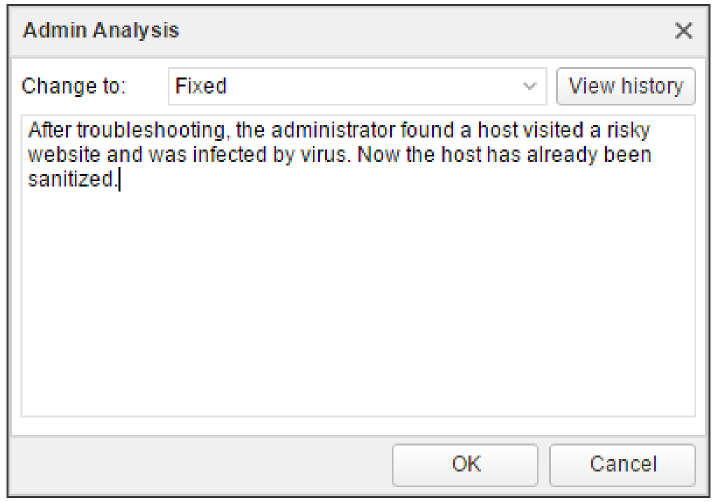
In Detail dialog, click , and select the status of threat in the **Admin Analysis** dialog.



Step 3: Mark the threat status

Resolved

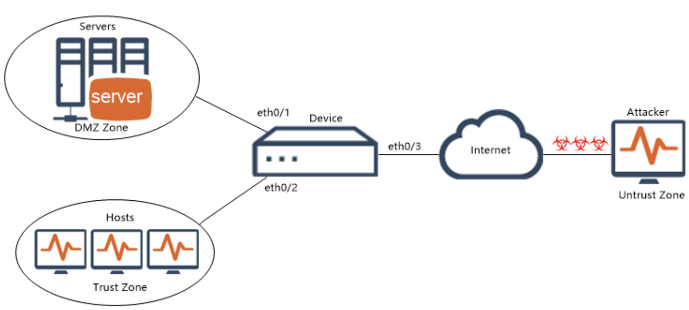
When the threat entry status is Fixed , it will not participate in the 'Network Risk Index' score.



Protecting Intranet to Defend Attacks via Intrusion Prevention System

This example introduces how to use Intrusion Prevention System to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration.

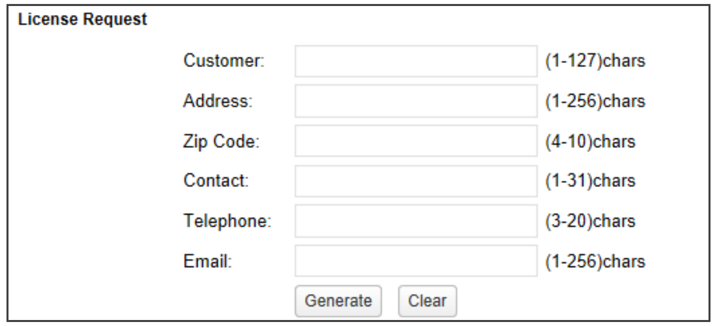
As shown in the following topology, the device is deployed in the Intranet exit. After enabling and configuring the Intrusion Prevention System, the device will protect Intranet against internet attacks.



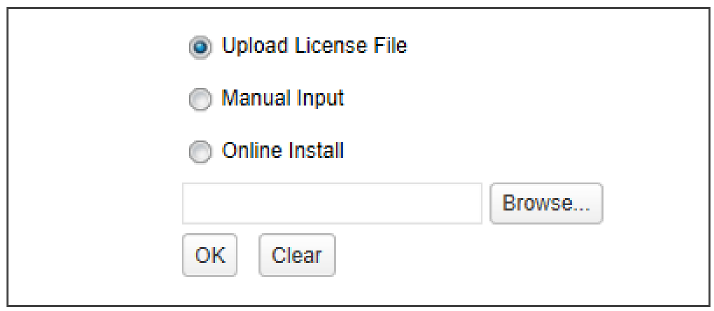
Configuration Steps

Step 1: Installing the Intrusion Prevention System license

1. Select **System> License**. Under **License Request**, input all user information. Then send the code to your sales contact. The sales person will get the license and send it back to you.



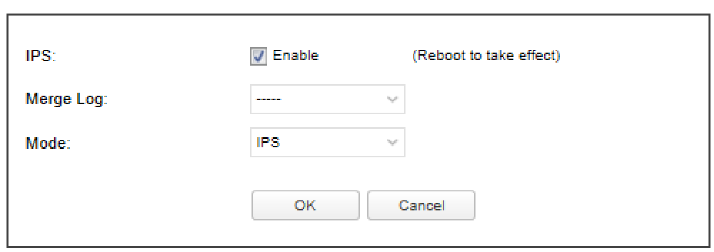
2. Select **Upload License File**, Click **Browse** to select the Intrusion Prevention System license file, and then click **OK** to upload it.



3. Select **System > Device Management>Option**, and click **Reboot**. When it starts again, the installed license will take effect.

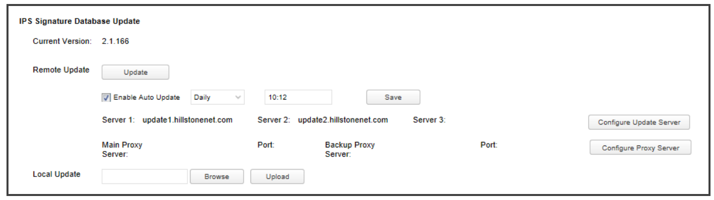
Step 2: Enabling Intrusion Prevention System and updating Signature Database

1. Select **Object>Intrusion Prevention System>Configuration** to view the Intrusion Prevention System function status. If disabled, click **Enable** and reboot.



Step 2: Enabling Intrusion Prevention System and updating Signature Database

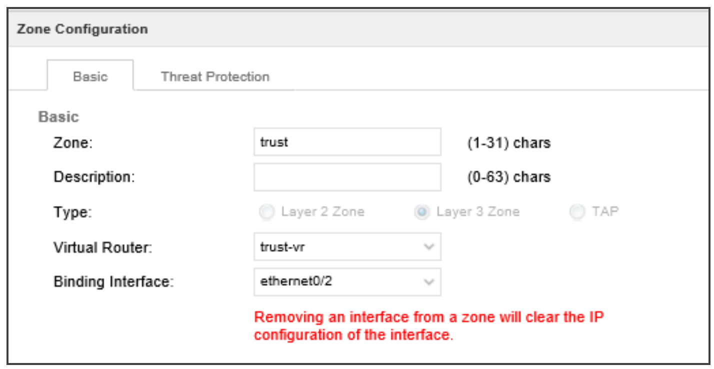
2. Select **System>Upgrade Management>Signature Database Update**. Under **IPS Signature Database Update**, click **Update** to update IPS Signature Database to assure its integrity and accuracy.



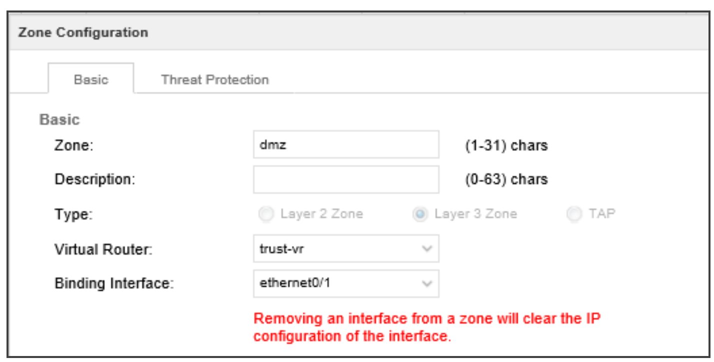
Step 3: Binding internal and external interfaces to the specified zones

1. Binding internal interface ethernet0/2 to **trust**. Select **Network>Zone**, select **trust** and click **Edit** to jump to the Zone Configuration dialog.

- Binding Interface: ethernet0/2

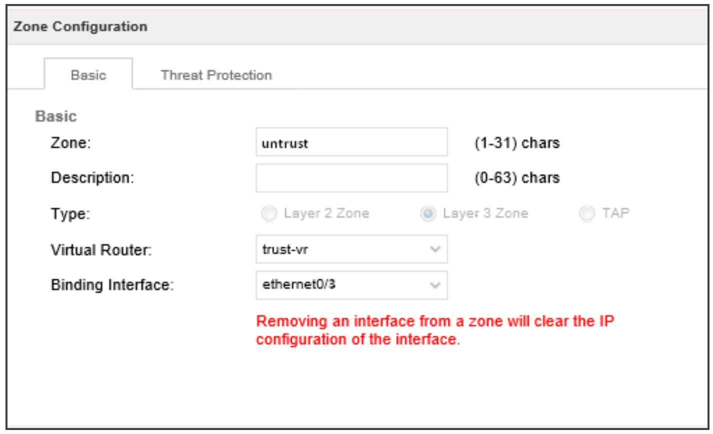


2. Binding internal interface ethernet0/1 to **dmz**, which can be configured as above.



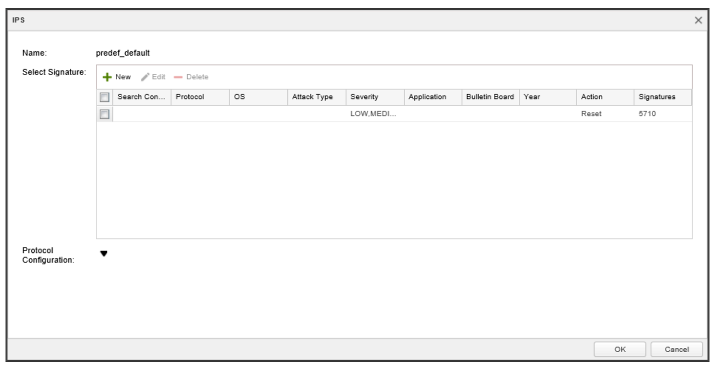
Step 3: Binding internal and external interfaces to the specified zones

3. Binding external interface ethernet0/3 to **untrust** , which can be configured as above.



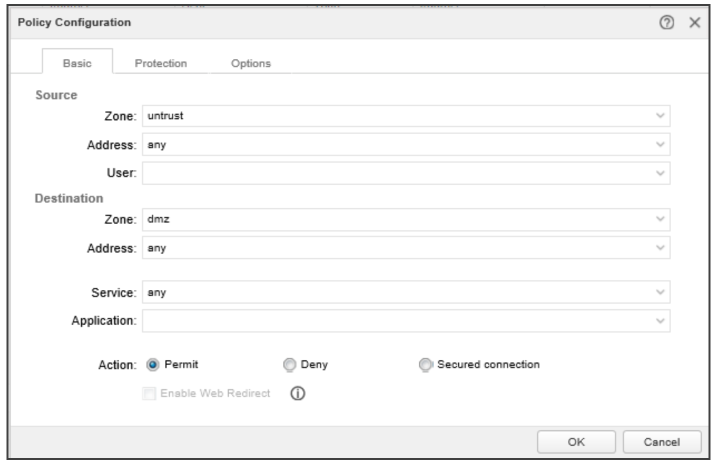
Step 4: Creating Intrusion Prevention System rules

Users can use the default rule or create a new rule. Select **Object>Intrusion Prevention System>Profile**, click **New** to jump to the IPS dialog. This example uses the predef_default rule, which includes all the IPS signatures and the default action is reset.



Step 5: Creating Security Policies.

Security policy: untrust to dmz



By default, the devices will deny all traffic between security zones. This case permits internet and internal hosts to access internal servers. Take the following steps to configure the security policies:

1.Select **Policy> Security Policy**, click **new** to jump to the Policy Configuration Dialog. In the Basic tab:

Source:

- Zone： untrust
- Address： any

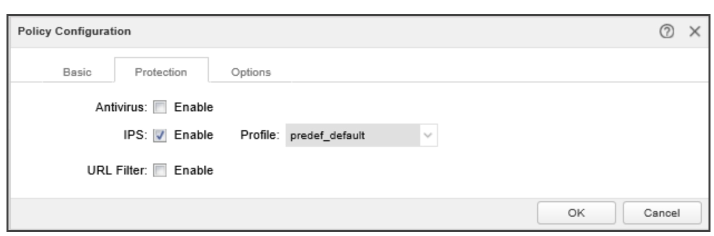
Destination:

- Zone： dmz
- Address： any

Others:

- Service： any
- Action： Permit

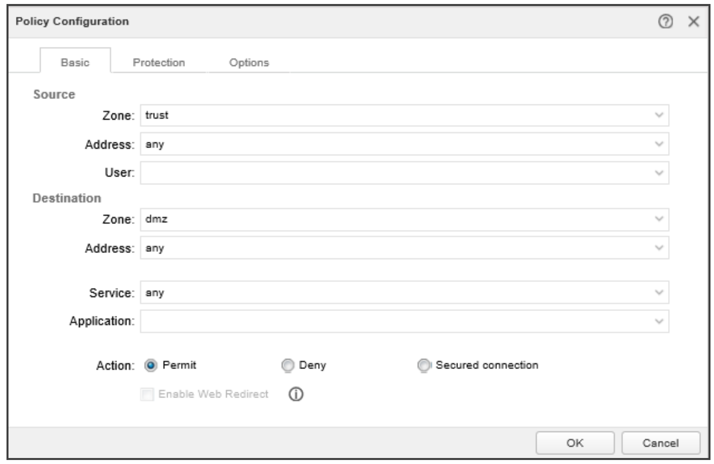
2.In the Protection Tab:



- IPS： Click the **Enable** check box .
- Profile： Select **predef_default** from the drop-down list

Step 5: Creating Security Policies.

Security policy: trust to dmz



1.Select **Policy> Security Policy**, click **new** to jump to the Policy Configuration Dialog. In the Basic tab:

Source:

- Zone： trust
- Address： any

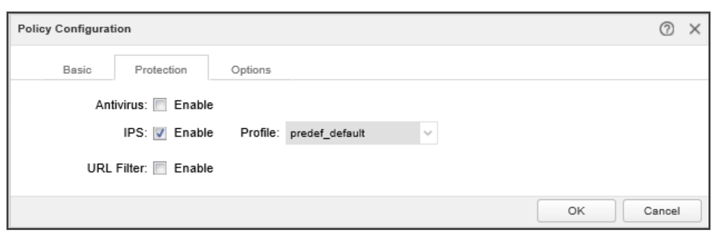
Destination:

- Zone： dmz
- Address： any

Others:

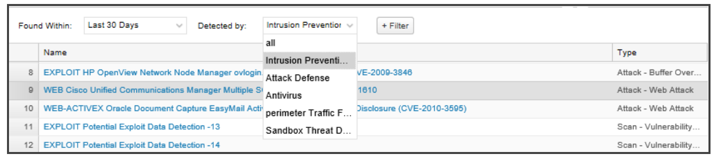
- Service： any
- Action： Permit

2.In the Protection Tab:



- IPS： Select the **Enable** check box .
- Profile： predef_default

Step 6: Viewing the results



After configuring the above steps, the device can protect Intranet against the known attacks. For example: the attacker creates SQL injections to attack the HTTP Server, and visits the URL of ' http://192.168.4.79/ccmcip/xml

dir-

ect-

oryl-

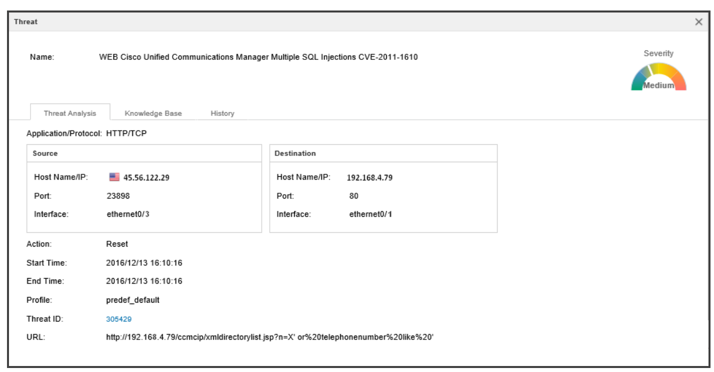
ist.jsp?n=X'or%20telephonenumber%20like%20''.

The device will display the attack information and block the attack.

Viewing the results from iCenter

1. Select **iCenter>Threat**, click + Filter to add the conditions.

    - Detected by: Intrusion Prevention System



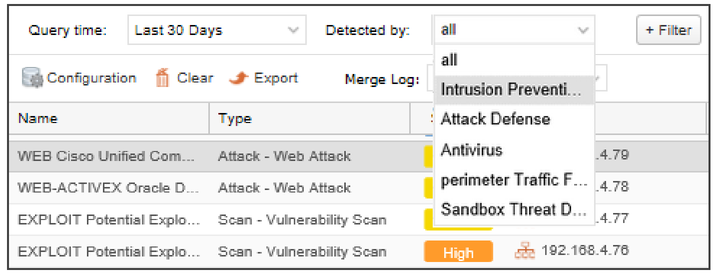
2. The log of Intrusion Prevention System will be displayed. Click the threat name to view the detailed information.

Step 6: Viewing the results

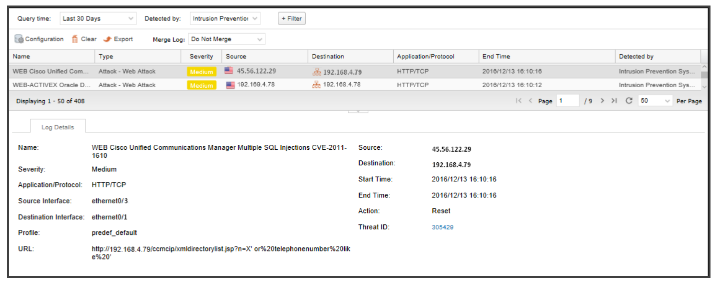
Viewing the results from Threat log

1. Select **Monitor>Log>Threat**, click + Filter to add the conditions.

- Detected by: Intrusion Prevention System



2. The log of Intrusion Prevention System will be displayed. Click the threat name to view the detailed information.



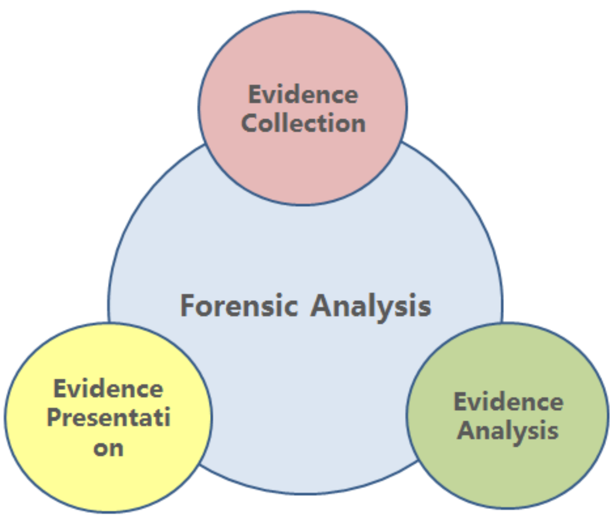
Forensic Analysis

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

This example shows how to in-depth view the threat of the whole network and analyze the threat evidence.

Forensic Analysis provides evidence chain of network threats to collect, multi-perspective analysis and the depth of integration.

- Evidence Collection: Through the configuration of Forensic Analysis function (packet capture), detect the attack generated at the same time evidence collection.
- Evidence Analysis: Analyze the collected evidence.
- Evidence Presentation: Display the threat details, logs, evidence pacp via iCenter, to achieve the threat of visualization.

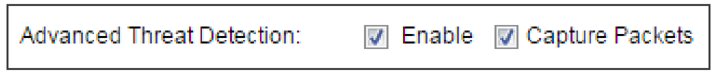


Configuration Steps

At present, the system only supports the Forensic Analysis function of three threat detection engines (Advanced Threat Detection, Intrusion Prevention System, Anti Virus)

Advanced Threat Detection

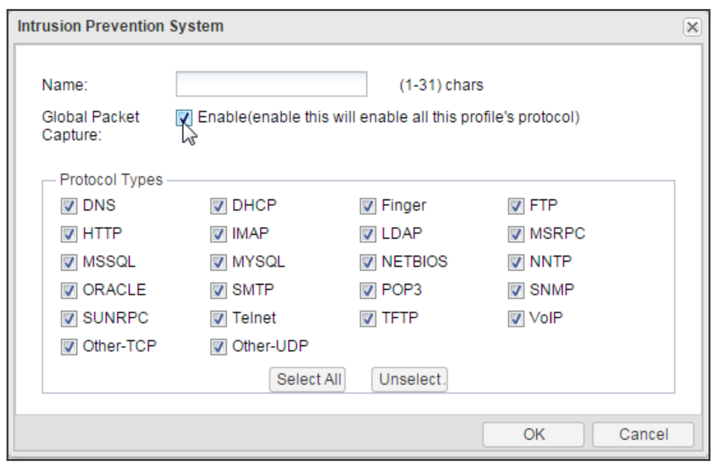
Enable the packet capture for Advanced Threat Detection, the system will capture packets when generating logs.



Select **Network > Zone**, Select "**trust**" zone, click **Edit**, and select the <Threat Protection>tab . Select the Capture Packets check box.

Intrusion Prevention System

1. Enable the packet capture for IPS rules, it will enable all this profile's protocols.

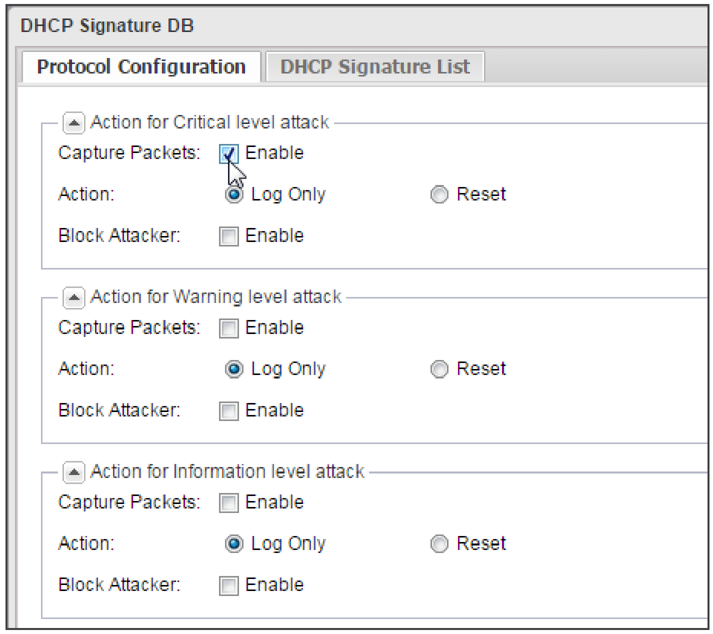


Select **Object>Intrusion Prevention System**, click **New**, and select the **Enable** check box to enable capture packets.

Intrusion Prevention System

2. According to your requirements, configure the capture packets for a specific protocol.

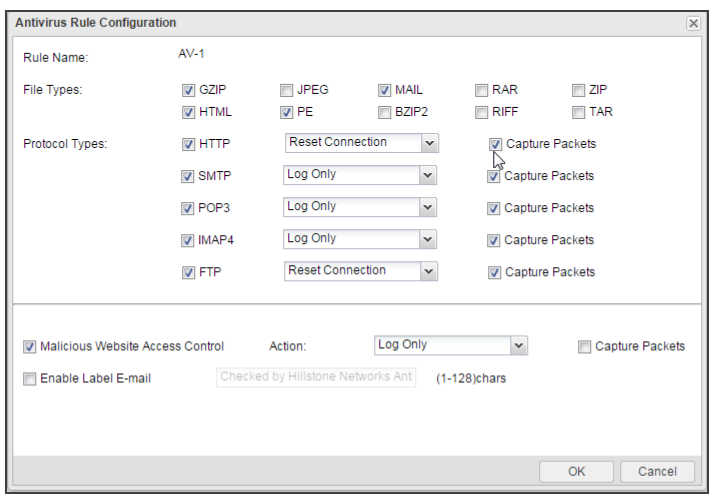
Select **Object>Intrusion Prevention System**, in the IPS rules list, click protocol type, for example ' DHCP', select the **Enable** check box to enable the capture packet for different attack levels.



Anti Virus

Enable the packet capture for Anti Virus rules.

Select **Object > Antivirus**, click **New**, Select the Enable check box before Capture Packet to enable the capture function.

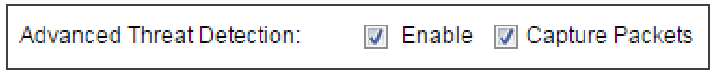


Forensic Analysis Configuration Example

As follows, taking advanced threat detection (ATD) as an example to demonstrate the process of Forensic Analysis

Step 1: Threat Detection

Enabling Advanced Threat Detection and capture packets



Select **Network > Zone**. Select "**trust**" zone, click **Edit**, and select the <Threat Protection> tab.

- Advanced Threat Detection: Select the **Enable** check box .
- Capture Packets: Select the check box , the system will save the evidence messages, and support to download it.

Step 2: Evidence Collection

When ATD attacks occurred, the system will generate a relevant threat log and capture evidence, sent to the system database.

According to the source IP, Advanced threat detection engine capture relational pacp at the same time, it is the HTTP traffic data (including TCP interaction) in 5 minutes or 64K size package, and used to assist in the analysis.

Step 3: Evidence Analysis

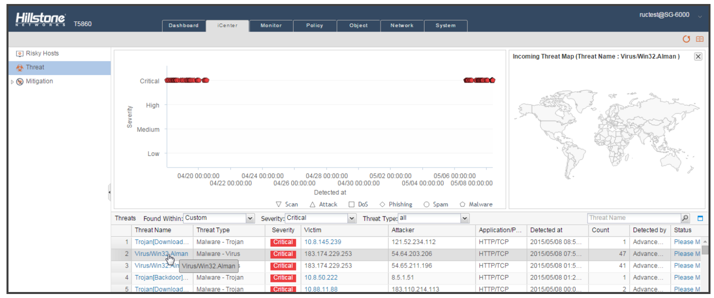
1. Analyze and get the threat detail information .

2. Collect the analysis of evidence.

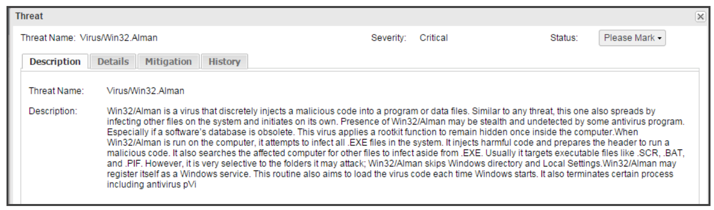
Step 4: Evidence Presentation

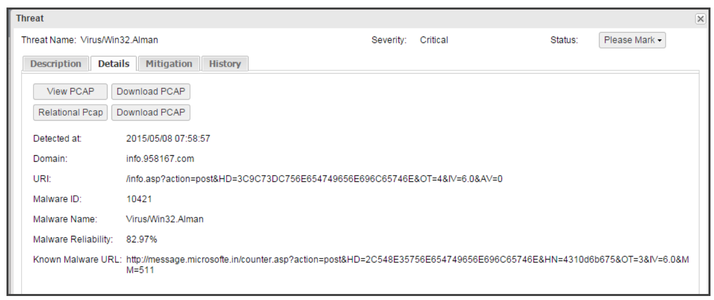
1. **Display the threat information, including the threat name, type, severity, victim host, attack host, etc.**

Click "iCenter", and select Threat tab.



Click the threat name link in the list, to view the threat details.

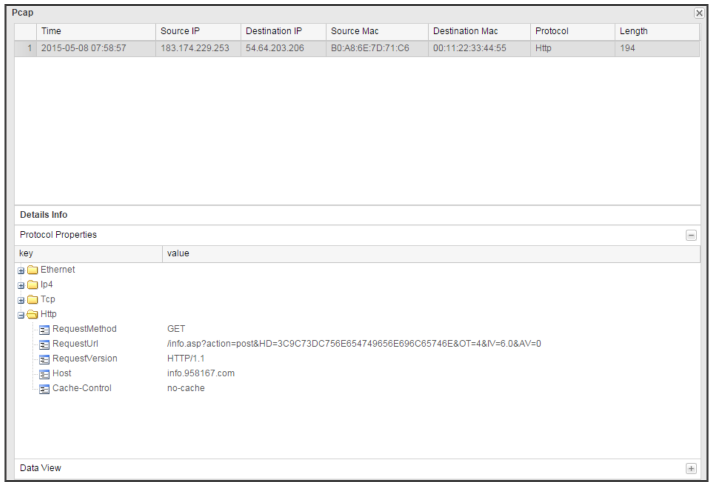


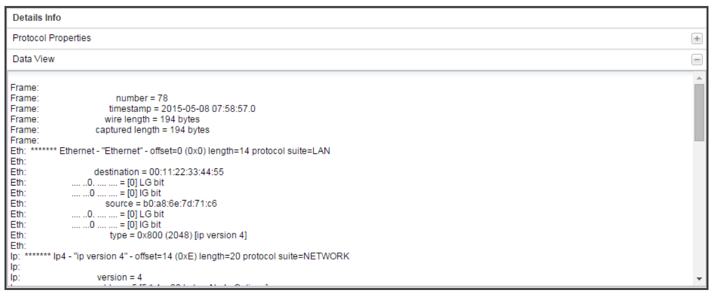


Step 4: Evidence Presentation

2. **Viewing the evidence details.**

Select the select the <Details>tab, and click **View PACP**.

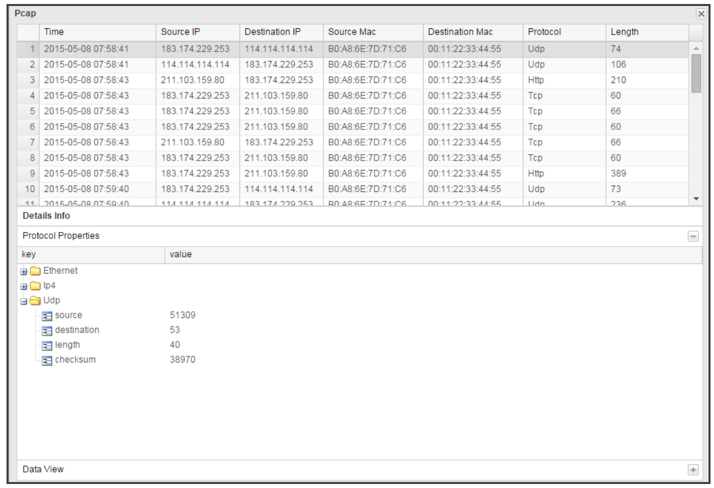


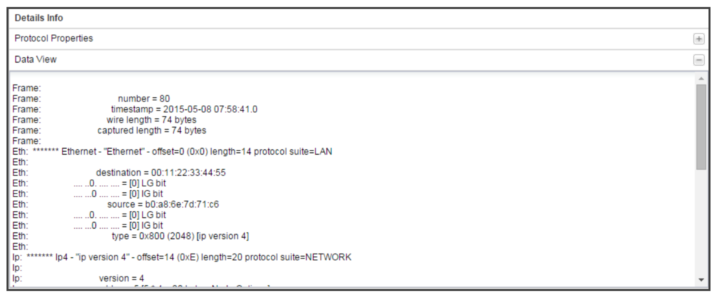


Step 4: Evidence Presentation

3. **Viewing the relational pacp details.**

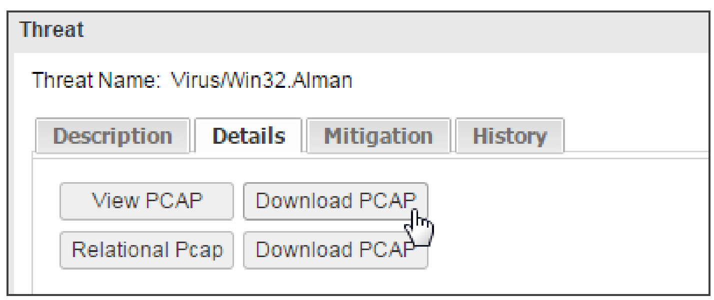
Select the select the <Details>tab, and click **Relational Pacp**.





4. **Downloading evidence.**

Select the select the <Details>tab, and click **Download Pacp**, the evidence will be downloaded to local.



Data Security

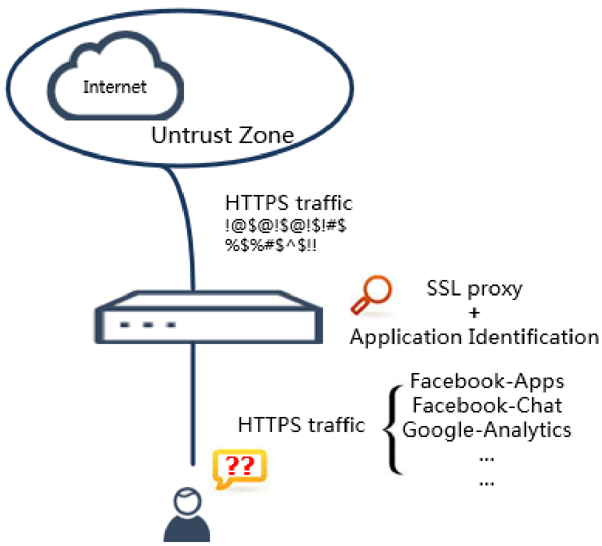
The data security allows you to flexibly configure control rules to comprehensively control and audit (by behavior logs) on user network behavior.

This chapter contains the following recipe:

Decrypting HTTPS Traffic and Identifying the Encrypted Application

This example introduces how to decrypt HTTPS traffic and identify the encrypted application, which meets the requirements of fine-grained application management.

As shown in the below scenario, an internal user accesses a HTTPS website and the traffic is encrypted by SSL protocol. With the SSL proxy and application identification functions enabled, the device can decrypt the HTTPS traffic and identify the encrypted application.



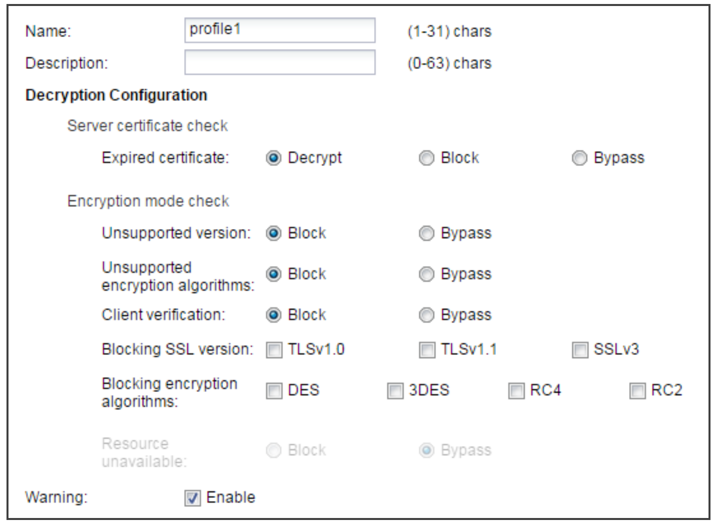
Configuration Steps

Step 1: Configuring a SSL proxy profile

Select **Policy > SSL Proxy**, and click **New**.

In the Basic tab:

- Name: profile1
- Expired certificate: Decrypt
- Unsupported version: Block
- Unsupported encryption algorithms: Block
- Client verification: Block
- Warning: Enable



Step 2: Specifying a SSL profile in the security policy

Configure a security policy that allows internal users to access Internet, and specify a SSL proxy profile in the Advanced tab:

- SSL Proxy: Select the **Enable** checkbox and select **profile1** from the drop-down list.

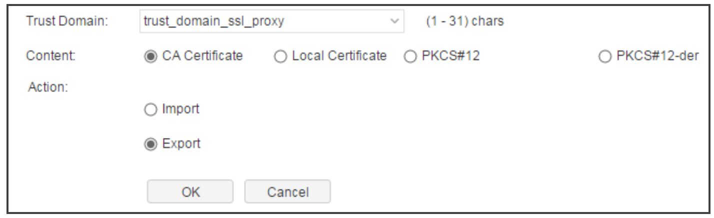
Step 3: Importing the device certificate to client's Web browser

Export the certificate from the device.

Click **System > PKI**. In the Management tab:

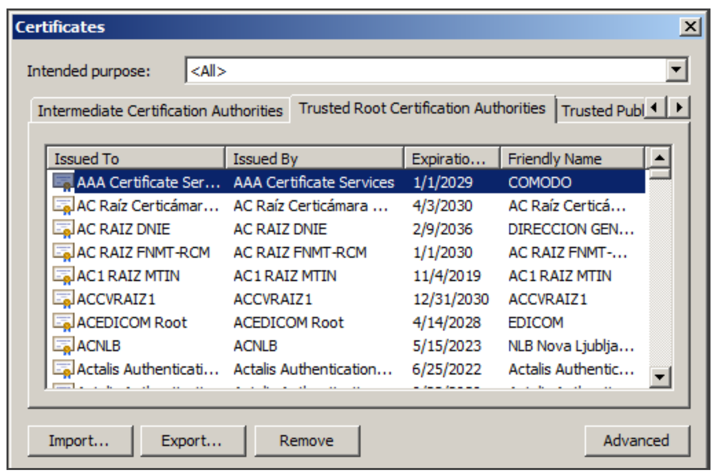
- Trust Domain: trust_domain_ssl_proxy
- Content: CA Certificate
- Action: Export

Click **OK** to export the certificate.



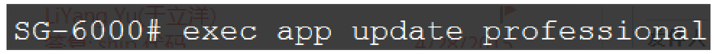
Import the certificate to client's Web browser.

1. In the Chrome Web browser, select **Settings > Show advanced settings**.
2. In the HTTPS/SSL section, select **Manage certificates**.
3. In the Trusted Root Certification Authorities tab, select **Import**.
4. Follow the wizard to import the certificate.



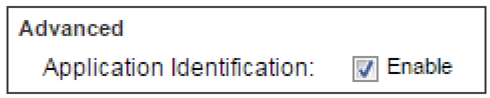
Step 4: Upgrading to the professional application signature database and enabling the application identification function

In CLI, execute the upgrade command to upgrade to the professional application signature database



Select **Network > Zone**, and double-click the **untrust** zone. In the Basic tab:

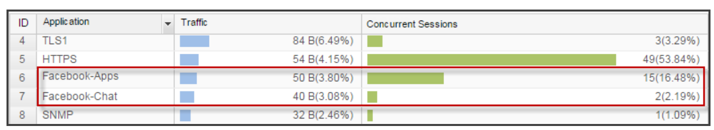
- Application Identification: Select **Enable**.



Step 6: Viewing application monitor

Select **Monitor > Application > Application Details**.

When an internal user accesses a HTTPS website, the SSL proxy function decrypts the HTTPS traffic and the application identification function identify the encrypted application.



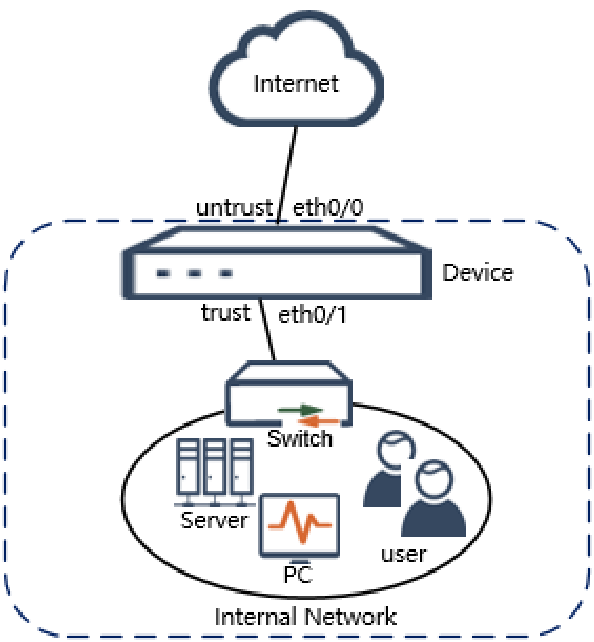
ID	Application	Traffic	Concurrent Sessions
4	TLS1	84 B(6.49%)	3(3.29%)
5	HTTPS	54 B(4.15%)	49(53.84%)
6	Facebook-Apps	50 B(3.80%)	15(16.48%)
7	Facebook-Chat	40 B(3.08%)	2(2.19%)
8	SNMP	32 B(2.46%)	1(1.09%)

URL Filtering for HTTPS Traffic without the CA Certificate

This example shows how to achieve the URL filtering for HTTPS traffic without installing the CA certificate.

As shown in the following topology, Hillstone device works as the gateway of an enterprise. The ethernet0/0 connects the Internet and belongs to the untrust zone. The ethernet0/1 connects to the Intranet and belongs to the trust zone.

With the configured URL filtering rule, staff of the enterprise (the network segment: 10.100.0.0/16) are prohibited from accessing shopping websites and the entertainment websites https:// www.bcd.com during working hours (09:00 to 18:00, Monday to Friday). The access and search attempts will be logged.



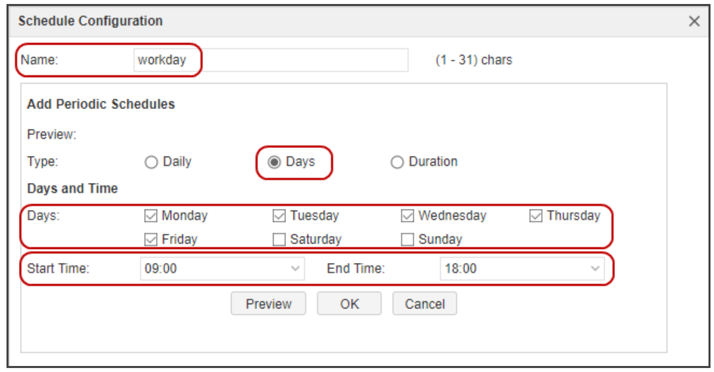
Preparation

Before configuring the URL filtering function, prepare the following first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps

Step 1: Configure a schedule

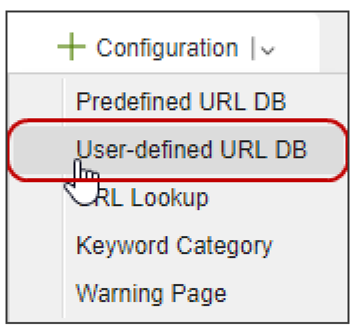


Select **Object > Schedule**, and click **New**.

In the **Schedule Configuration** dialog:

- Name: workday
- Days: Click **Add** to add a periodic schedule.
- Type: Days.
- Days: Monday, Tuesday, Wednesday, Thursday, Friday
- Start Time: 09:00
- End Time: 18:00

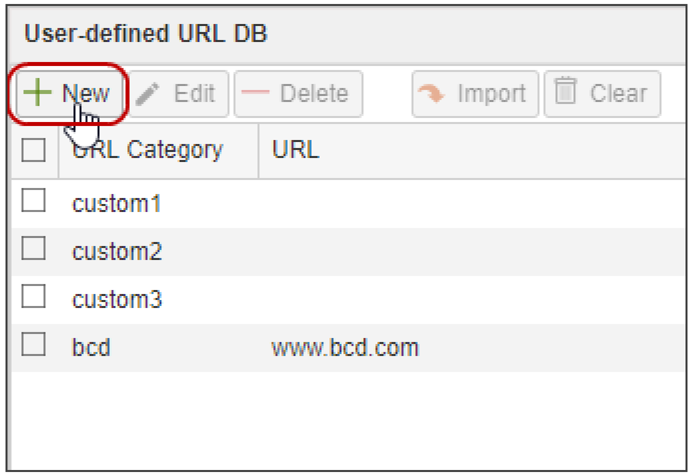
Step 2: Configure the user-defined URL category named bcd that contains https://www.bcd.com



Select **Object > URL Filtering**, and select **Configuration > User-defined URL DB** at the top-right corner.

Step 2: Configure the user-defined URL category named bcd that contains https://www.bcd.com

In the **User-defined URL DB** dialog, click **New**.



In the **URL Category** dialog:

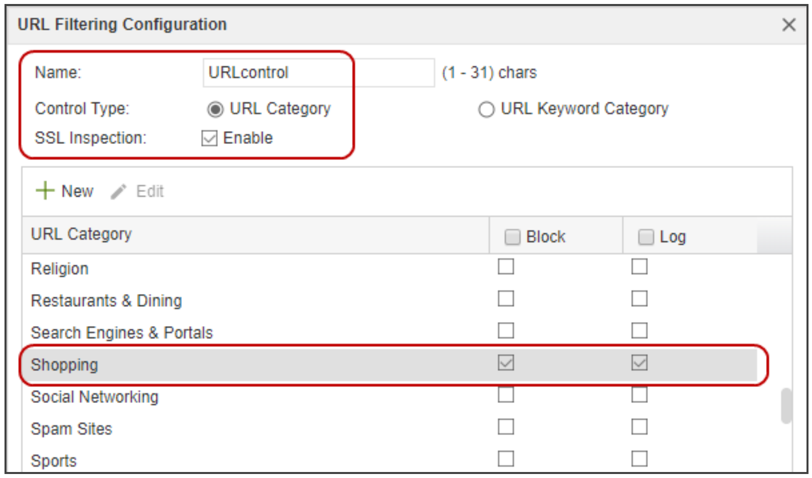
- Category: bcd
- URL http(s)://: www.bcd.com
- Click **Add** to add the "https://www.bcd.com" and its category to the table.

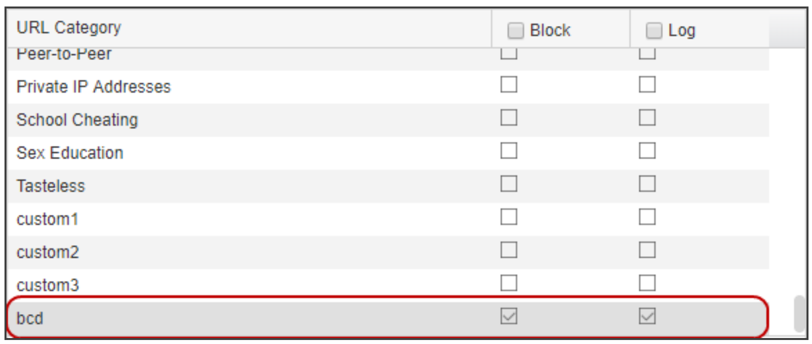
Step 3: Configure the URL filtering rule named URLcontrol, and enable the SSL Inspection

Select **Object > URL Filtering**, and click **New**.

In the **URL Filtering Rule Configuration** dialog:

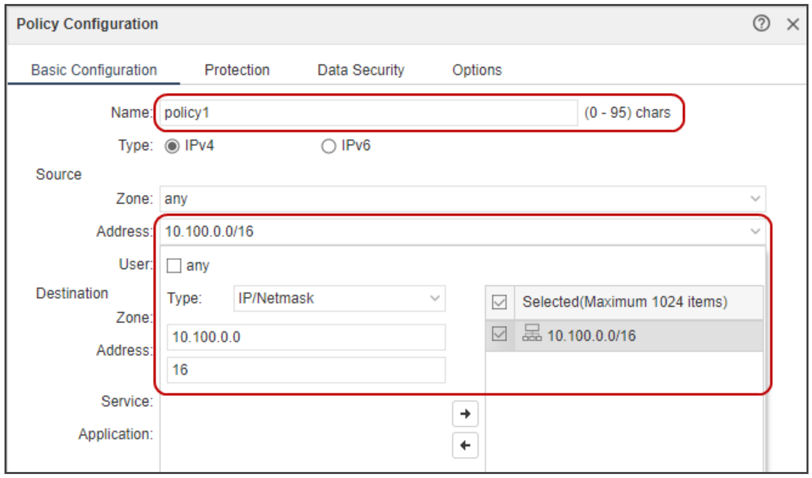
- Name: URLcontrol
- Control Type: URL Category
- SSL Inspection: Select the **Enable** check box to enable SSL negotiation packets inspection.
- Select the predefined URL category **Shopping**, and then select the **Block** check box and **Log** check box.
- Select the user-defined URL category **bcd**, and then select the **Block** check box and **Log** check box.





Step 4: Bind the URL filtering rule to a policy rule

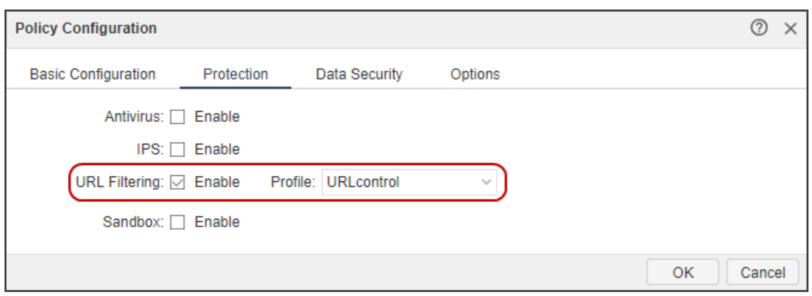
Select **Policy > Security Policy**, and click **New**.



In the **Basic Configuration** tab of the **Policy Configuration** dialog:

- Name: policy1
- Source Address: Select the address type **IP/Netmask** , type 10.100.0.0 and 16 into the **IP**and **Netmask** text box respectively, and click **->** to add the address to the right pane.

In the **Protection** tab of the **Policy Configuration** dialog:

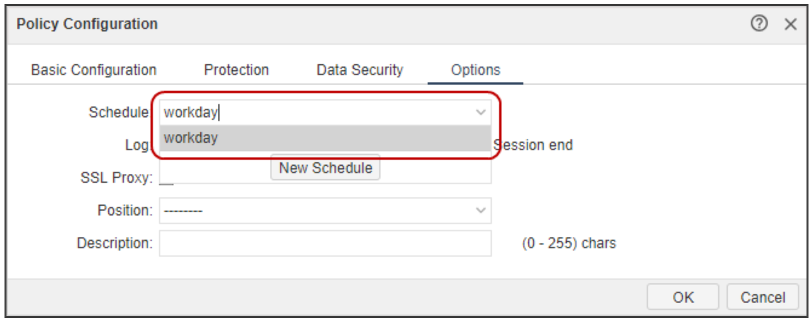


- URL Filtering: Select the **Enable** check box.
- Profile: Select the created URL filtering rule "URL-control" from the drop-down list.

Step 4: Bind the URL filtering rule to a policy rule

In the **Options** tab of the **Policy Configuration** dialog:

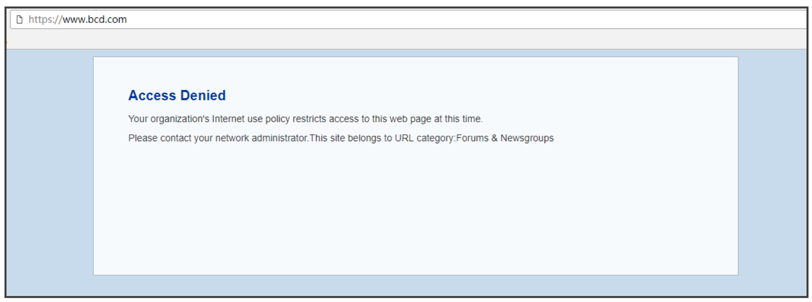
- Schedule: Select the schedule "workday" from the **Schedule** drop-down list.



Step 5: Result

After the configuration, adjust the configured rule to the highest priority rule for traffic matching.

When the rule takes effect, during the working hours, company staff cannot access shopping websites and the entertainment websites "https:// www.bcd.com". The system will log the access and search attempts.



IPv6

StoneOS is dual-stack firmware that supports both IPv4 and IPv6. It also supports tunneling technique (the latest version supports manual IPv6 tunnel) for IPv6 communication.

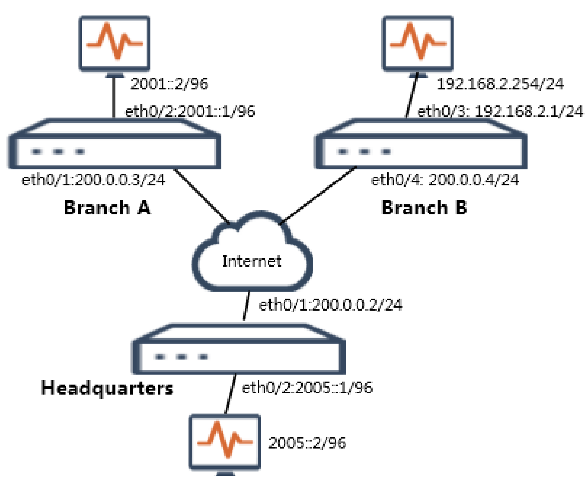
This chapter includes the following recipe:

Connecting IPv6 and IPv4 Networks

One enterprise has a headquarters, branch A and branch B. The headquarters and two branches all can access the Internet. The headquarters and branch A are deployed with IPv6 network for intranet and IPv4 network for internet, while the branch B is deployed with IPv4-only networks for both intranet and internet. For the business needs, it’ s necessary to connect IPv6 and IPv4 networks to achieve the following goals:

- The IPv6 network of headquarters can connect with the IPv4 Internet and be accessed by the Internet users.
- The networks of headquarters can connect with the IPv6 network of branch A via 6in4 tunnel.
- The networks of headquarters can connect with the IPv4 network of branch B.

The headquarters, branch A and branch B is deployed with a Hillstone device separately and the topology is as follows:



There are three parts of configurations:

- Configuring networks of headquarters
- Configuring networks of branch A
- Configuring networks of branch B

Configuring Networks of Headquarters

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 200.0.0.2 255.255.255.0
hostname(config-if-eth0/1)# manage http
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# dns-proxy
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2005::1/96
hostname(config-if-eth0/2)# manage ping
hostname(config-if-eth0/2)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 branchA
hostname(config-if-tun1)# exit
```

Step 2: Configure the route and NAT rules, including headquarters accessing the Internet, headquarters communicating with branch B, and public IP accessing IPv6 server of headquarters.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from 2005::/96 to 2003::/96 service any eif ethernet0/1 trans-to eif-ip mode dynamicport
hostname(config-vrouter)# snatrule id 2 from 2005::2/96 to 2004::2 service any eif ethernet0/1 trans-to eif-ip mode dynamicport
hostname(config-vrouter)# snatrule id 3 from any to 200.0.0.2 service any eif ethernet0/2 trans-to 2005::1 mode dynamicport
hostname(config-vrouter)# dnatrule id 1 from 2005::/96 to 2003::/96 service any v4-mapped
hostname(config-vrouter)# dnatrule id 2 from 2005::2/96 to 2004::2 service any trans-to 200.0.0.4
hostname(config-vrouter)# dnatrule id 3 from any to 200.0.0.2 service any trans-to 2005::2
hostname(config-vrouter)# ip route 0.0.0.0/0 200.0.0.1
hostname(config-vrouter)# ipv6 route 2001::/96 tunnel1
hostname(config-vrouter)# exit
```

Step 3: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 2
Rule id 2 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2004::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 3
Rule id 3 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2003::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

```
hostname(config)# policy-global
hostname(config-policy)# rule id 4
Rule id 4 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2001::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 5
Rule id 5 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2001::/96
hostname(config-policy-rule)# dst-ip 2005::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 6
Rule id 6 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip ipv6-any
hostname(config-policy-rule)# dst-ip ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

Step 4: Configure an IPv6 tunnel.

```
hostname(config)# tunnel ip6in4 branchA manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 200.0.0.3
hostname(config-ip6in4-manual)# exit
hostname(config)# ip name-server 8.8.8.8 vrouter trust-vr
hostname(config)# ip dns-proxy domain any name-server 8.8.8.8 vrouter trust-vr
hostname(config)# ipv6 dns64-proxy id 1 prefix 2003::/96 source 2005::/96 trans-mapped-ip any
```

Note: The `ipv6 dns64-proxy` command is not supported for some versions.

Configuring Networks of Branch A

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 200.0.0.3 255.255.255.0
hostname(config-if-eth0/1)# manage ping
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2001::1/96
hostname(config-if-eth0/2)# manage ping
hostname(config-if-eth0/2)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 headquarters
hostname(config-if-tun1)# exit
```

Step 2: Configure the route and NAT rules.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 200.0.0.1
hostname(config-vrouter)# ipv6 route 2005::/96 tunnel1
hostname(config-vrouter)# exit
```

Step 3: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 31
Rule id 31 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 32
Rule id 32 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2001::/96
hostname(config-policy-rule)# dst-ip 2005::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 33
Rule id 33 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2001::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

```
hostname(config)# policy-global
hostname(config-policy)# rule id 34
Rule id 34 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip ipv6-any
hostname(config-policy-rule)# dst-ip ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

Step 4: Configure an IPv6 tunnel.

```
hostname(config)# tunnel ip6in4 headquarters manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 200.0.0.2
hostname(config-ip6in4-manual)# exit
```

Configuring Networks of Branch B

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1 255.255.255.0
hostname(config-if-eth0/1)# manage ping
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 200.0.0.4 255.255.255.0
hostname(config-if-eth0/4)# manage ping
hostname(config-if-eth0/4)# exit
```

Step 2: Configure the route and NAT rules.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from any to any service any eif ethernet0/4
trans-to eif-ip mode dynamicport
hostname(config-vrouter)# dnatrule id 1 from 200.0.0.2 to 200.0.0.4 service any trans-
to 192.168.2.254
hostname(config-vrouter)# ip route 0.0.0.0/0 200.0.0.1
hostname(config-vrouter)# exit
```

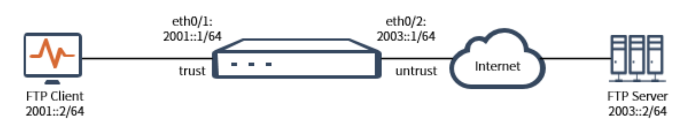
Step 3: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 35
Rule id 35 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

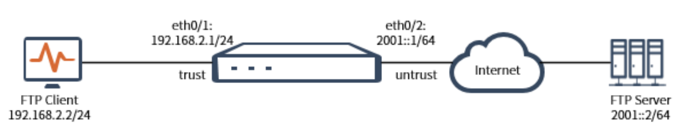
Realizing FTP Service in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG

This example introduces how to configure ALG to realize the FTP service in IPv6-only or IPv4/IPv6 hybrid networks, including the following three scenarios:

- **Scenario 1: IPv6-only network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Both internal and external network IP addresses are deployed with IPv6 addresses. With the ALG function configured, the internal FTP client can access the FTP server in the extranet.



- **Scenario 2: IPv4 network to IPv6 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv4 addresses and the external network is deployed with IPv6 addresses. With the ALG function configured, the internal FTP client can access the FTP server in the extranet.



- **Scenario 3: IPv6 network to IPv4 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv6 addresses and the external network is deployed with IPv4 addresses. With the ALG function configured, the internal FTP client can access the FTP server in the extranet.

Before You Start

Before starting the configuration, you need to ensure that the configuration of the FTP server and the FTP client has been completed. This example only describes the relevant configuration on the device.

Configuration Steps of Scenario 1

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ip address 2002::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2003::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service ftp permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Enable the ALG function of FTP.

```
hostname(config)# alg ftp
```

Note: The ALG function of FTP is enabled by default.

Step 4: Verify result.

```
Download session in FTP active mode:

session: id 44, proto 6, flag 0, flag1 20000, flag2 0, flag3 0, created 39340, life 1787,
policy 1,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64348->[2001::2]:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2003::2]:64348

session: id 2, proto 6, flag 8000000, flag1 20000, flag2 0, flag3 0, created 39408, life
1800, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(31(ethernet0/1)/208810): [2001::2]:20->[2003::2]:64363

flow1(32(ethernet0/2)/40208810): [2003::2]:64363->[2001::2]:20


Download session in FTP passive mode:

session: id 61, proto 6, flag 10000, flag1 20000, flag2 0, flag3 0, created 39683, life 1775,
policy 1,app 4(FTP) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64362->[2001::2]:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2003::2]:64362

session: id 22, proto 6, flag 8000000, flag1 20000, flag2 0, flag3 0, created 39684, life
1776, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40208810): [2003::2]:64398->[2001::2]:56008

flow1(31(ethernet0/1)/208810): [2001::2]:56008->[2003::2]:64398
```

Configuration Steps of Scenario 2

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2001::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from any to any service ftp permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from any to 192.168.2.10 service any trans-to 2001::10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from any to 192.168.2.10 service any trans-to ip 2001::2
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of FTP.

```
hostname(config)# alg ftp
```

Note: The ALG function of FTP is enabled by default.

Step 5: Verify result.

```
Download session in FTP active mode:

session: id 64, proto 6, flag e, flag1 20007, flag2 0, flag3 0, created 133143, life 1797,
policy 2,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40300b10): 192.168.2.2:58259->192.168.2.10:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2001::10]:1025

session: id 14, proto 6, flag 8000016, flag1 2000b, flag2 0, flag3 0, created 133147, life
297, policy 2,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(31(ethernet0/1)/208810): [2001::2]:20->[2001::10]:58261

flow1(32(ethernet0/2)/40200810): 192.168.2.2:58261->192.168.2.10:20


Download session in FTP passive mode:

session: id 20, proto 6, flag e, flag1 20007, flag2 0, flag3 0, created 133393, life 1797,
policy 2,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40300b10): 192.168.2.2:58272->192.168.2.10:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2001::10]:1030

session: id 2, proto 6, flag 800000e, flag1 20007, flag2 0, flag3 0, created 133397, life
1797, policy 2,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40200810): 192.168.2.2:58273->192.168.2.10:61665

flow1(31(ethernet0/1)/208810): [2001::2]:61665->[2001::10]:61665
```

Configuration Steps of Scenario 3

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2003::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 192.168.1.1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service ftp permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat

hostname(config-nat)# snatrule id 1 from ipv6-any to 2003::10 service any trans-to 192.168.1.10 mode dynamicport

rule ID=1

hostname(config-nat)# dnatrule id 1 from ipv6-any to 2003::10 service any trans-to ip 192.168.1.2

rule ID=1

hostname(config-nat)# exit
```

Step 4: Enable the ALG function of FTP.

```
hostname(config)# alg ftp

Note: The ALG function of FTP is enabled by default.
```

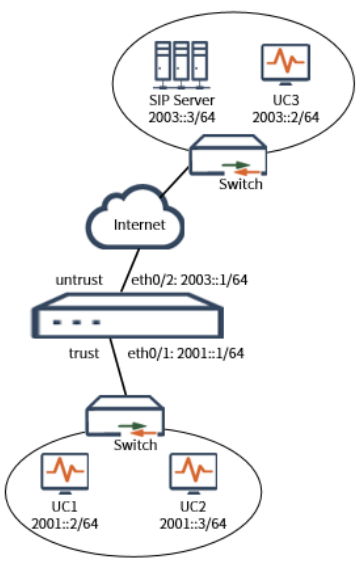
Step 5: Verify result.

```
Download session in FTP active mode:

session: id 6, proto 6, flag e, flag1 2000b, flag2 0, flag3 0, created 40792, life 1799, policy 1,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64537->[2003::10]:21

flow1(31(ethernet0/1)/300b10): 192.168.1.2:21->192.168.1.10:1034

session: id 5, proto 6, flag 8000016, flag1 20007, flag2 0, flag3 0, created 40798, life 1799, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(31(ethernet0/1)/200810): 192.168.1.2:20->192.168.1.10:64538

flow1(32(ethernet0/2)/40208810): [2003::2]:64538->[2003::10]:20


Download session in FTP passive mode:

session: id 21, proto 6, flag e, flag1 2000b, flag2 0, flag3 0, created 40093, life 1799, policy 1,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64435->[2003::10]:21

flow1(31(ethernet0/1)/300b10): 192.168.1.2:21->192.168.1.10:1026

session: id 14, proto 6, flag 800000e, flag1 2000b, flag2 0, flag3 0, created 40099, life 300, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40208810): [2003::2]:64436->[2003::10]:56075

flow1(31(ethernet0/1)/200810): 192.168.1.2:56075->192.168.1.10:56075
```

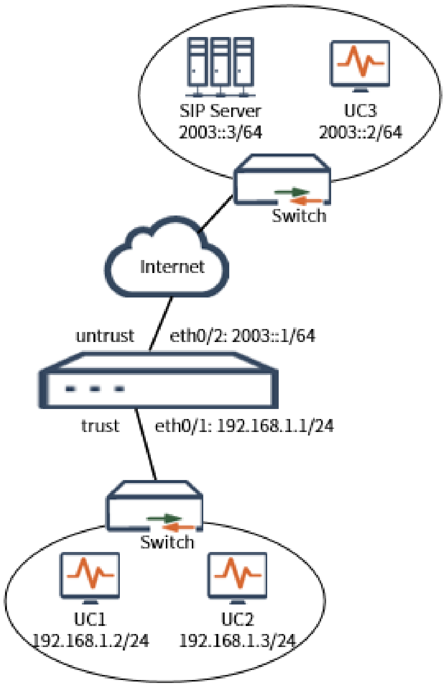
Realizing SIP Communication in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG

This example introduces how to configure ALG to realize the SIP communication in IPv6-only or IPv4/IPv6 hybrid networks, including the following three scenarios:

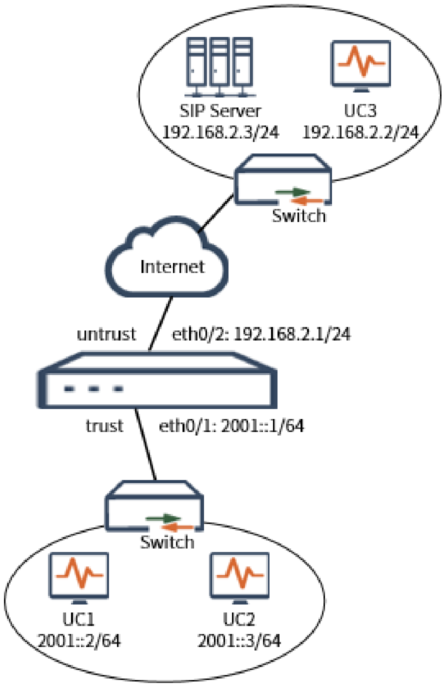
- **Scenario 1: IPv6-only network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Both internal and external network IP addresses are deployed with IPv6 addresses. With the ALG function configured, the internal SIP UC1 and the external SIP UC3 can successfully establish communication with each other.



- **Scenario 2: IPv4 network to IPv6 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv4 addresses and the external network is deployed with IPv6 addresses. With the ALG function configured, the internal SIP UC1 and the external SIP UC3 can successfully establish communication with each other.



- **Scenario 3: IPv6 network to IPv4 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv6 addresses and the external network is deployed with IPv4 addresses. With the ALG function configured, the internal SIP UC1 and the external SIP UC3 can successfully establish communication with each other.



Before You Start

Before starting the configuration, you need to ensure that the configuration of the SIP Server and the SIP user agent (SIP UC) has been completed. This example only describes the relevant configuration on the device.

Configuration Steps of Scenario 1

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2001::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2003::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service sip permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Enable the ALG function of SIP.

```
hostname(config)# alg sip
```

Note: The ALG function of SIP is enabled by default.

Step 4: Verify result.

View the information of media pinhole. Total pinhole count is 5, including 1 register pinhole and 4 media pinhole.

```
hostname# show pinhole
Total pinhole count in D-Plane: 5
[Pinhole0]========================================
Seq 10
App SIP MEDIA (id:875)
Flag: Enabled,
[Ingress info]--------------------------------------------------
Zone trust (id:2)
Flow0 (ifid 0) :::any -> 2003::2:5001
[Egress info]---------------------------------------------------
Zone untrust (id:3)
Flow1 (ifid 0) 2003::2:5001 -> :::any
[Life info]-----------------------------------------------------
After_hit 600
Before_hit 120
Timer 217
[Other info]----------------------------------------------------
Auth_user_id 0
```

Configuration Steps of Scenario 2

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2003::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from any to any service sip permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from any to 192.168.1.10 service any trans-to
2003::10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from any to 192.168.1.10 service any trans-to ip
2003::3
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of SIP.

```
hostname(config)# alg sip
```

Note: The ALG function of SIP is enabled by default.

Step 5: Verify result.

View the information of media pinhole. Total pinhole count is 5, including 1 register pinhole and 4 media pinhole.

hostname# show pinhole

Total pinhole count in D-Plane: 5

[Pinhole 1]===-=============

Seq 15

App SIP MEDIA (id:875)

Flag: Enabled,

[Ingress info]--

Zone untrust (id:3)

Flow0 (ifid 0) :::any -> 2003::10:1025

[Egress info]---

Zone trust (id:2)

Flow1 (ifid 31) 192.168.1.2:5002 -> 192.168.1.10:any

[Life info]---

After_hit 600

Before_hit 120

Timer 38

[Other info]--

Auth_user_id 0

Configuration Steps of Scenario 3

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2002::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 192.168.2.1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service sip permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from ipv6-any to 2001::10 service any trans-to
192.168.2.10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from ipv6-any to 2001::10 service any trans-to ip
192.168.2.3
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of SIP.

```
hostname(config)# alg sip
```

Note: The ALG function of SIP is enabled by default.

Step 5: Verify result.

View the information of media pinhole. Total pinhole count is 5, including 1 register pinhole and 4 media pinhole.

SG-6000# show pinhole

Total pinhole count in D-Plane: 5

[Pin-

hole1]-

===-

====

Seq 36

App SIP MEDIA (id:875)

Flag: Enabled,

[Ingress info]--

Zone trust (id:2)

Flow0 (ifid 0) 0.0.0.0:any -> 192.168.2.10:5002

[Egress info]---

Zone trust (id:2)

Flow1 (ifid 31) 2001::2:5002 -> 2001::10:any

[Life info]---

After_hit 600

Before_hit 120

Timer 107

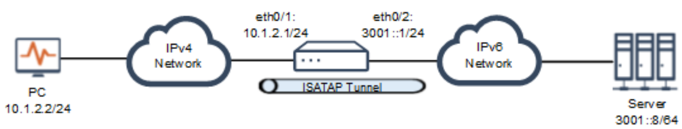
[Other info]--

Auth_user_id 0

Realizing Dual-stack Host in IPv4 Network Accessing IPv6 Network Via ISATAP Tunnel

This example introduces how to configure ISATAP tunnel to realize dual stack host access to IPv6 network in IPv4 network.

In the topology below, PC supports dual protocol stacks. Hillstone device is connected to the corresponding IPv6 network and IPv4 network. It is required to configure the ISATAP tunnel so that the dual-stack host PC in the IPv4 network can access the server in the intranet IPv6 network.



Configuration Steps

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.1.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 3001::1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configure ISATAP tunnel and bind a interface

```
hostname(config)# tunnel ip6in4 tunnel isatap
hostname(config-ip6in4-isatap)# interface ethernet0/1
hostname(config-ip6in4-isatap)# exit
hostname(config)#
```

Configure the tunnel interface and bind the tunnel interface to the ISATAP tunnel.

```
hostname(config)#  interface tunnel1
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# ipv6 address 2001::/64 eui-64
hostname(config-if-tun1)# ipv6 address fe80::5efe:10.1.2.1 link-local
hostname(config-if-tun1)# tunnel ip6in4 tunnel
hostname(config-if-tun1)# no ipv6 nd ra suppress
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5 : Configure routing for PC, take win7 PC as an example

```
C:\>netsh interface ipv6 isatap set router 10.1.2.1
C:\>netsh interface ipv6 isatap set router 10.1.2.1 enabled
```

Step 6: Verify result.

> The dual-stack host (10.1.2.2) can access the IPv6 Server (3001::8) through FTP successfully.

Change Log

Cookbook V1

Release Date: January, 2015

Added the following cases:

1. " Using Security Policy to Allow Access to Another Zone" on Page 14 (Security Policy)
2. "Allowing Internet to Visit a Private Server Using DNAT" on Page 25 (DNAT)
3. "Allowing Private Network to Access Internet Using SNAT" on Page 20 (SNAT)
4. "Allowing the Internet Access via User Authentication" on Page 81 (User Authentication, WebAuth)
5. "Connection between Two Private Networks Using IPSec VPN (IKEv1)" on Page 132 (IPSec VPN)
6. "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 157 (SSL VPN, SCVPN)
7. " Ensuring Uninterrupted Connection Using HA" on Page 240 (High Availability, HA)
8. " QoS Control" on Page 259 (Quality of Service, QoS, Traffic Management)

Cookbook V2

Release Date: April, 2015

Added the following cases:

1. "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 272 (Abnormal Behavior Detection, ABD)
2. "Finding Malware Attacks via Advanced Threat Detection" on Page 281 (Advanced Threat Detection, ATD)

Cookbook V3

Release Date: July, 2015

Add the following cases:

1. "Decrypting HTTPS Traffic and Identifying the Encrypted Application" on Page 301 (SSL Proxy, Decryption, Encrytion)
2. "Using an iOS/Android Device to Remotely Access Intranet Services" on Page 175 (iOS, Android, Mobile, iPad, remote device, SSL VPN)
3. "Forensic Analysis " on Page 293
4. "Deploying Tap Mode to Monitor Network Traffic " on Page 30(Tap Mode)

Cookbook V4

Release Date: September, 2015

Add the following cases:

1. "Upgrading Firmware to Higher Version" on Page 5 (Upgrade)
2. "Allowing Remote Users (PC) to Access a Private Network Using L2TP over IPSec VPN" on Page 182 (L2TP VPN)
3. "Connection between Two Private Networks Using GRE over IPSec VPN" on Page 218 (GRE, IPSec VPN)

Cookbook V5

Release Date : January, 2017

Add the following cases:

1. "Protecting Intranet to Defend Attacks via Intrusion Prevention System" on Page 285(IPS)
2. "Outbound Link Load Balance" on Page 266(LLB)

Optimize the following cases:

1. "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 272(ABD)
2. "Finding Malware Attacks via Advanced Threat Detection" on Page 281(ATD)

Cookbook V6

Release Date : October, 2017

Add the following cases:

1. "Allowing Remote Users (iOS/Android) to Access a Private Network Using L2TP over IPSec VPN" on Page 203 (L2TP VPN)

Cookbook V7

Release Date : August, 2018

Add the following cases:

1. " Using AD Polling for SSO" on Page 89 (Authentication)
2. " Allowing Internet Access via AD Polling" on Page 99(Authentication)
3. " Allowing Internet Access via AD Agent" on Page 111(Authentication)
4. "Connecting IPv6 and IPv4 Networks" on Page 312
5. "URL Filtering for HTTPS Traffic without the CA Certificate" on Page 305

Cookbook V8

Release Date : June, 2019

Add the following cases:

1. "Connection between Two Private Networks Using IPSec VPN (IKEv2)" on Page 146 (IPSec VPN)
2. "Upgrading Firmware to Higher Version in HA mode" on Page 10 (Upgrade)
3. "Configuring the Device to Communicate with Zabbix Using SNMP" on Page 40 (SNMP)

Cookbook V8.1

Release Date : November, 2019

Add the following cases:

1. "Connecting to Microsoft Azure Using Site-to-Site VPN" on Page 163 (IPSec VPN)

Cookbook V9

Release Date : October, 2020

Add the following cases:

1. " DNS Proxy" on Page 56 (DNS Proxy)
2. "Dynamically Manage Access Authority Via Radius Dynamic Authorization" on Page 46 （Authorization）
3. "Realizing Multicast Forwarding Through PIM-SM Multicast Protocol" on Page 64 （Routing, PIM）
4. "Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol" on Page 73 （Routing, PIM）
5. "Ensuring Uninterrupted Connection Using HA AA" on Page 247 （HA）
6. " Allowing Internet Access via TS Agent" on Page 123 （Authentication）
7. " Configuring VXLAN Static Unicast Tunnel" on Page 235 （VPN）
8. "Realizing FTP Service in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG" on Page 323 （IPv6）
9. "Realizing SIP Communication in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG" on Page 332 （IPv6）
10. "Realizing Dual-stack Host in IPv4 Network Accessing IPv6 Network Via ISATAP Tunnel" on Page 343 （IPv6）

This book is updated on requirement, not periodically.

The current version you are using is based on StoneOS 5.5R8.