SANGFOR WOC

(Version 9.0-9.1)

User Manual

December 2015

Table of Contents

Declaration

SINFOR, SANGFOR and the Sangfor logo are the trademarks or registered trademarks of Sangfor Inc. All other trademarks used or mentioned herein belong to their respective owners.

This manual shall only be used as usage guide, and no statement, information, or suggestion in it shall be considered as implied or express warranty of any kind, unless otherwise stated. This manual is subject to change without notice. To obtain the latest version of this manual, please contact the Customer Service of Sangfor.

Preface

About This Manual

This WAN Optimization Controller (WOC) User Manual includes the following chapters:

Chapter	Describe…
Chapter 1 Knowing Your Sangfor Device	The product appearance, features and performance parameters of Sangfor WOC, wiring and cautions before installation
Chapter 2 Initial Login to Admin Console	The configuration steps required when administrator accesses the Web administrator console of Sangfor WOC for the first time
Chapter 3 Deployment and Configuration	How to deploy the physical Sangfor WOC and configure system and network related settings through the administrator console
Chapter 4 Sangfor VPN	How to configure Sangfor VPN to establish inbound/outbound secure VPN connection to a remote Sangfor WOC
Chapter 5 WAN Optimization	How to configure WAN optimization module to accelerate data transmitted across the WAN
Chapter 6 Bandwidth Management	How to configure bandwidth management module to ensure or restrict bandwidth usage of specific application, user or IP address.
Chapter 7 Firewall	How to configure firewall related settings
Chapter 8 High Availability	How to configure the high availability (HA) feature, which makes the system redundant and run more stable
Chapter 9 IPSec VPN	How to set up IPSec VPN connection between Sangfor WOC and third-party VPN device
Chapter 10 Maintenance	How to license the Sangfor WOC, maintain and debug the system, etc.
Appendix A: Internal Report Center	How to enter and use the internal WOC Report Center
Appendix B: PACC & Mobile VPN Client	The installation and usage of the Portable Acceleration (PACC) client and Mobile VPN client
Appendix C: Sangfor Firmware Updater	How to use Sangfor Firmware Updater 6.0 to update the Sangfor device

Document Conventions

Graphic Interface Conventions

This user manual uses the following typographical conventions for special terms and instructions:

Convention	Meaning	Example
boldface	Page title, parameter, menu/submenu, button, key press, link, other highlighted keyword or item	Page/tab name example: Navigate to System > Users to enter the User page. Parameter example: IPAddress: Specifies the IP address that you want to reserve for certain computer Menus/submenus example: Log in to the Web administrator console and go to System > Network > Deployment. Button example: Click the Save button to save the settings. Key press example: Press Enter key to enter the administrator console. Link example: Once the certificate signing request is generated, click the Download link to download the request. Highlighted keyword/item example: The user name and password are Admin by default.
italics	Directory, URL	Website: http://www.sangfor.com
>	Multilevel menu and submenu	Log in to the Web administrator console and go to System > Network > Deployment.
“ ”	Prompt, quotation	Click on “This site might require the following ActiveX control: ‘WebUI Control’ from ‘Sangfor Technologies Co., Ltd’. Click here to install…”.

Symbol Conventions

This manual also adopts the following symbols to indicate the parts which need special attention to be paid during the operation:

Convention	Meaning	Description
⚠	Caution	Indicates actions that could cause setting error, loss of data or damage to the device
⚡	Warning	Indicates actions that could cause injury to human body
💡	Note	Indicates helpful suggestion or supplementary information

CLI Conventions

Command syntax on Command Line Interface (CLI) applies the following conventions:

Content in brackets ( ]) is optional

Content in {} is necessary

If there is more than one option, use vertical bar (|) to separate each option, for example,

ip wccp 60 redirect { in | out }

CLI command appears in bold, for example:

configure terminal

Variables appear in italic, for example:

interface e0/1

Technical Support

For technical support, please contact us through the following:

Website: http://www.sangfor.com

MSN, Email: tech.support@sangfor.com

Skype: sangfor.tech.support

Tel: + 60 3 2282 1206

Acknowledgements

Thanks for using our product and user manual. If you have any suggestion about the product or user manual, please provide feedback to us through phone call or email. Your suggestion will be much appreciated.

Chapter 1 Knowing Your Sangfor Device

This chapter introduces the Sangfor WAN Optimization Controller (WOC) and the way of connecting Sangfor WOC. After proper hardware deployment and installation, you can configure and debug the system.

Operating Environment

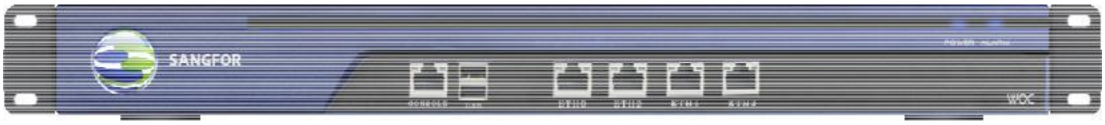
Voltage input: 110V/230V (AC, alternating current)
Temperature: 0-45 ℃
Humidity: 5%-90%

To ensure endurance and stability of the Sangfor WOC, please ensure the following:

The power supply is well grounded
Dustproof measures are taken
Working environment is well ventilated
Indoor temperature is kept stable

This product conforms to the requirements on environment protection. The placement, usage and discard of the product should comply with the relevant national laws and regulations of the country where it is applied.

Product Appearance



Front Panel of SANGFOR WOC 2050

Above is the front panel of SANGFOR WOC 2050. The interfaces from left to right are described in the following table:

Interface	Description
CONSOLE	Network interface used for high availability (HA) feature or used by device supplier to debug system.
USB	Standard USB port, connecting to peripheral device

ETH0	LAN interface, connecting to the LAN network segment; orange LED on the left side indicates link status, while green LED on the right side indicates data flow.
ETH1	DMZ interface, connecting to the DMZ network segment; orange LED on the left side indicates link status, while green LED on right side indicates data flow.
ETH2	WAN1 interface, connecting to the first Internet line; orange LED on the left side indicates link status, while green LED on the right side indicates data flow.
ETH3	WAN2 interface, connecting to the second Internet line; orange LED on the left side indicates link status, while green LED on the right side indicates data flow.
POWER	Power LED
ALARM	Alarm LED

The picture above is just for reference. The actual product you purchased and received may vary.

Connecting Sangfor Device

After deploying the Sangfor WAN Optimization Controller (WOC) in your network (for details, please refer to the Device Deployment section in Chapter 3), follow the instructions below to connect the Sangfor WOC.

1. Plug the power cable into the power interface on the rear panel of the device. Attach and turn on power supply, and then watch the LEDs on the front panel of the Sangfor WOC.

   When the device starts up, ALARM LED will turn on and keep on for 1 to 2 minutes, then turn off; POWER LED (in green) will turn on; connection status LEDs (in orange) next to WAN and LAN interface will also turn on.

   After successful bootup, POWER LED (in green), connection status LEDs (in orange) WAN and LAN interface will stay on. If data are being transferred through a port, the data flow LED (in green, beside connection status LED) will blink.

   If ALARM LED stays on always, please switch off the power supply and reboot the device. If ALARM LED still keeps on after reboot, contact SANGFOR Customer Service.

If the corresponding LED indicates normal working status, turn off and unplug the power supply, and perform the following steps.

2. Use RJ-45 straight-through Ethernet cable to connect the LAN interface to the internal network.
3. Use RJ-45 Ethernet crossover cable to connect the WAN1 interface to the external network, (i.e., router, optical fiber transceiver or ADSL Modem for external network).
4. If you want the Sangfor WOC to provide secure protection for DMZ (Demilitarized Zone), use RJ-45 Ethernet cable to connect DMZ interface to the DMZ network from which Web server, SNMP Server are providing services to external networks.

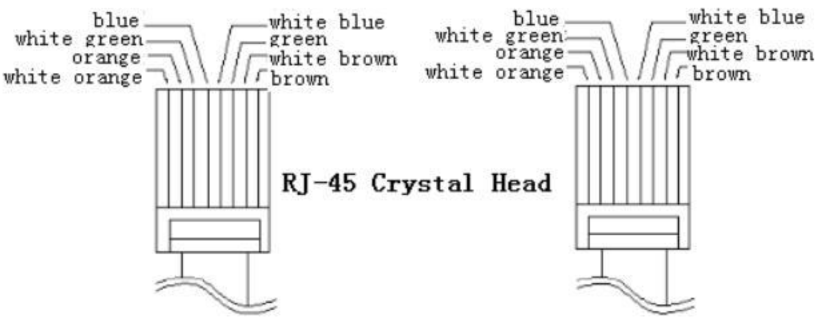
Use crossover cable to connect WAN interface to the router for external network.

Use straight-through cable to connect LAN interface to switch in the internal network.

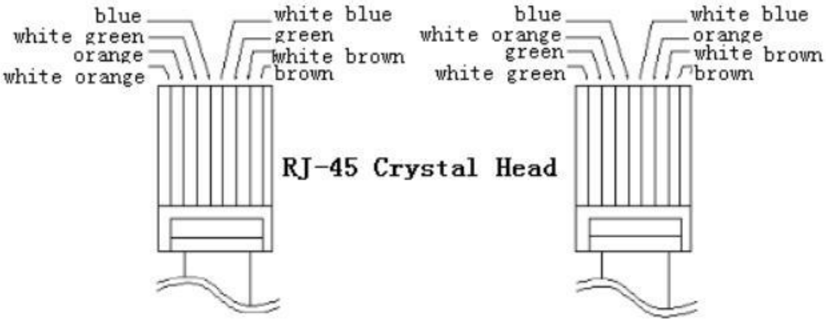
For direct access to administrator Web console, use crossover cable to connect LAN interface to the computer.

In case session cannot be established but the corresponding LED indicates normal working status, please check whether the right type of cables are being used. The differences between straight-through cable and crossover cable are shown in the figures on the following page.

1. Wire Sequence of Straight-through Cable



2. Wire Sequence of Crossover Cable



Chapter 2 Initial Login to Admin Console

Sangfor WAN Optimization Controller (WOC) provides Web-based administration. The initial URL for Web administrator console access is http://10.254.254.254.

Before logging in to administrator console of WOC, please ensure the following:

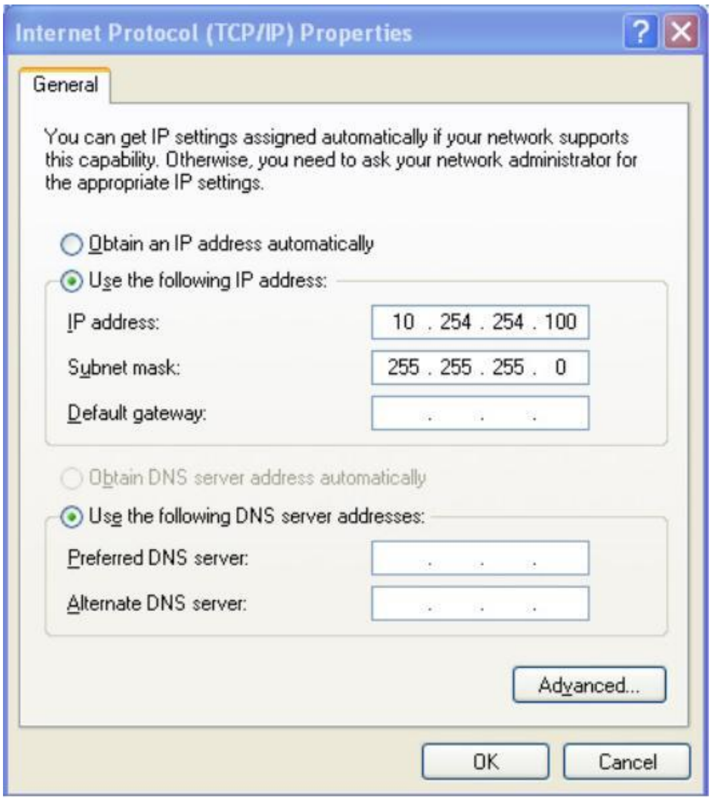
Deploy a computer in the subnet where the Sangfor WOC resides.

Connect the PC's network interface card (NIC) and LAN interface of Sangfor WOC to a same layer-2 switch, or connect the PC's NIC to LAN interface directly with a network cable.

Ensure IE browser is installed on the PC. Non-IE browsers Opera, Firefox, Safari and Chrome are not supported.

Logging in to Admin Console

1. Turn on the PC and the Sangfor WOC. Add an IP address on the PC, an IP address that resides in the network segment 10.254.254.X (for instance, 10.254.254.100) with subnet mask 255.255.255.0, as shown below:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 254 . 254 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

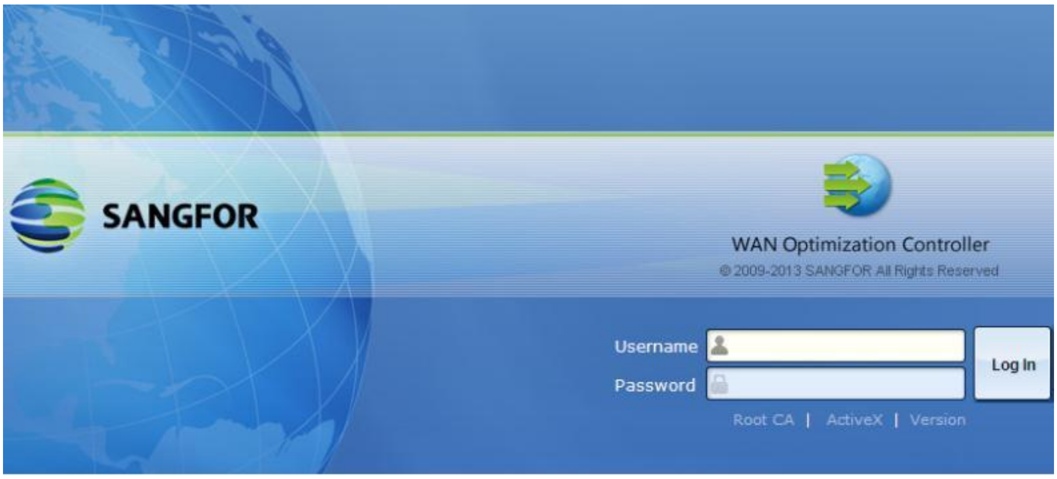
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

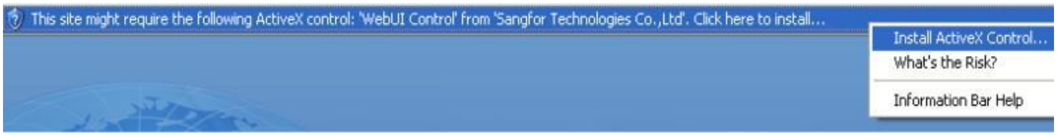
Preferred DNS server: . . .

Alternate DNS server: . . .

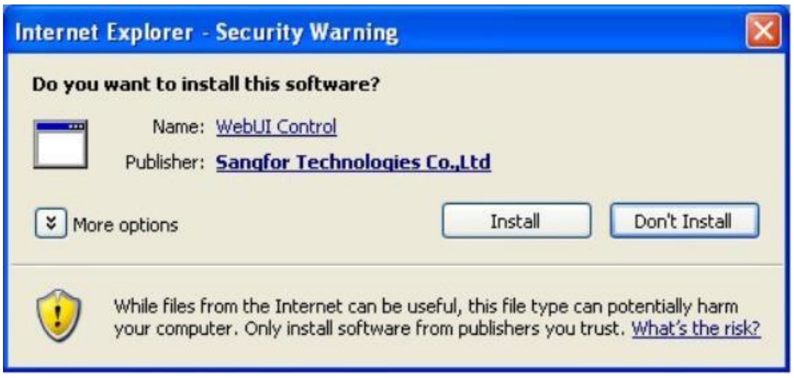
2. Open the IE browser and enter the URL address (http://10.254.254.254) into the address bar. Press Enter key to visit the login page to Web administrator console, as shown below:


SANGFOR
WAN Optimization Controller
© 2009-2013 SANGFOR All Rights Reserved
Username
Password
Log In
Root CA | ActiveX | Version

3. Before login, you may install the required ActiveX control, as shown below:


This site might require the following ActiveX control: 'WebUI Control' from 'Sangfor Technologies Co.,Ltd'. Click here to install...

Click on "This site might require the following ActiveX control: 'WebUI Control' from 'Sangfor Technologies Co., Ltd'. Click here to install..." and then click on "Install ActiveX Control..." to install the control, as shown below:


Internet Explorer - Security Warning

Do you want to install this software?

Name: WebUI Control

Publisher: Sangfor Technologies Co.,Ltd

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

If no pop-up appears, click the link ActiveX on the login page to download the required ActiveX controls.

4. Enter the administrator username and password and click the Log In button. The default administrator username is admin (case-insensitive) and password is Admin (case-sensitive).

5. To download root CA certificate, click on the link Root CA.

6. For version information of the software e, click on Version below the textboxes.

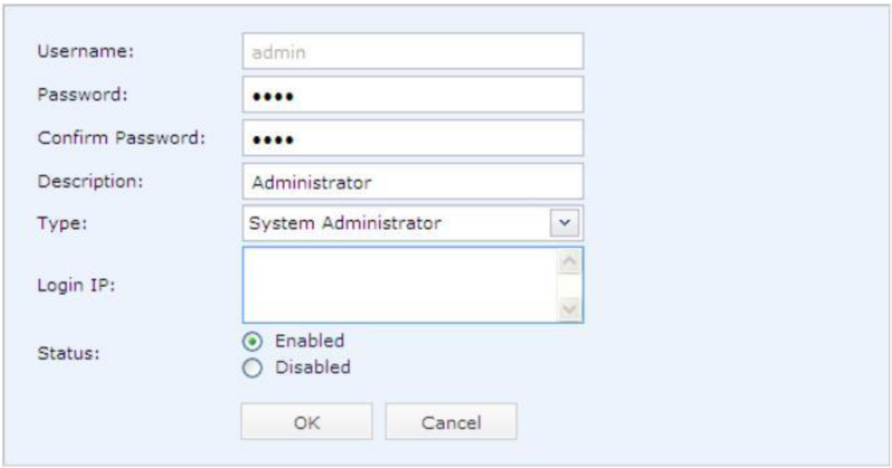
Modifying Administrator Password

We strongly recommend you to change the administrator password on initial login, so as to prevent others from logging in to the administrator Web console and using default admin credentials to make unauthorized changes on the administrator account and initial configurations.

To modify default administrator password, perform the following steps:

1. Navigate to System > Users to enter the Users page. The default administrator account is admin, super administrator of the system.

2. Click the account name admin to edit information of the administrator account:



Username: admin

Password: ••••

Confirm Password: ••••

Description: Administrator

Type: System Administrator

Login IP:

Status: ● Enabled ○ Disabled

3. Enter and confirm the new password and click the OK button.

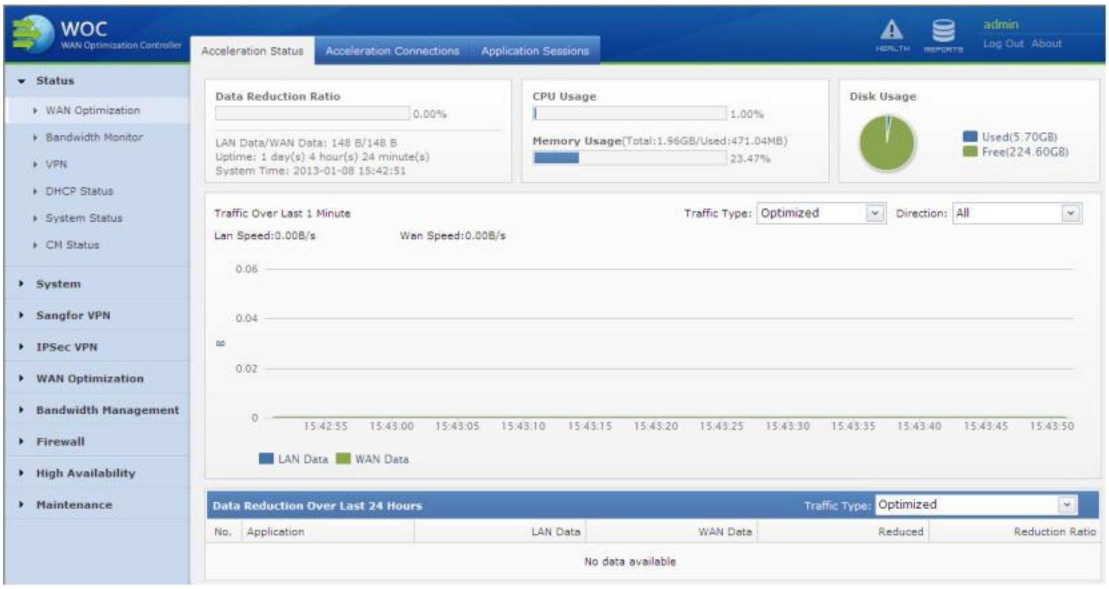
Password of the account admin should not be shared with anyone.

If the Sangfor WOC is to be maintained by several administrators, create multiple administrator accounts for segregation of duty.

Chapter 3 Deployment and Configuration

After logging in to the administrator console, you will see the left tree of configurable modules, including System, Sangfor VPN, IPSec VPN, WAN Optimization, Bandwidth Management, Firewall, High Availability and Maintenance.

What needs to be noted is that some modules may be invisible to you if the corresponding licenses are not purchased.



Data Reduction Ratio 0.00%

LAN Data/WAN Data: 148 B/148 B
Uptime: 1 day(s) 4 hour(s) 24 minute(s)
System Time: 2013-01-08 15:42:51

CPU Usage 1.00%

Memory Usage(Total:1.96GB/Used:471.04MB) 23.47%

Disk Usage
🟦 Used(5.70GB)
🟩 Free(224.60GB)

Traffic Over Last 1 Minute

Traffic Type: Optimized

Direction: All

Lan Speed:0.00B/s

Wan Speed:0.00B/s

Data Reduction Over Last 24 Hours

Traffic Type: Optimized

No.	Application	LAN Data	WAN Data	Reduced	Reduction Ratio
No data available					

⚠

During configuration, if there is an OK, Save or Save and Apply button on a page, click it after modifying or configuring the parameters to save or apply the settings on that page. This will not be illustrated again in the subsequent parts in this user manual.

Device Deployment

The first thing you need to consider before deploying the physical Sangfor WAN Optimiztion Controller (WOC) in your network is what deployment mode you should use, in that system and network setting are subject to the deployment mode you choose. Take CDP and WCCP for example. The two pages are available only in Acceleration Only service mode and Single arm deployment mode.

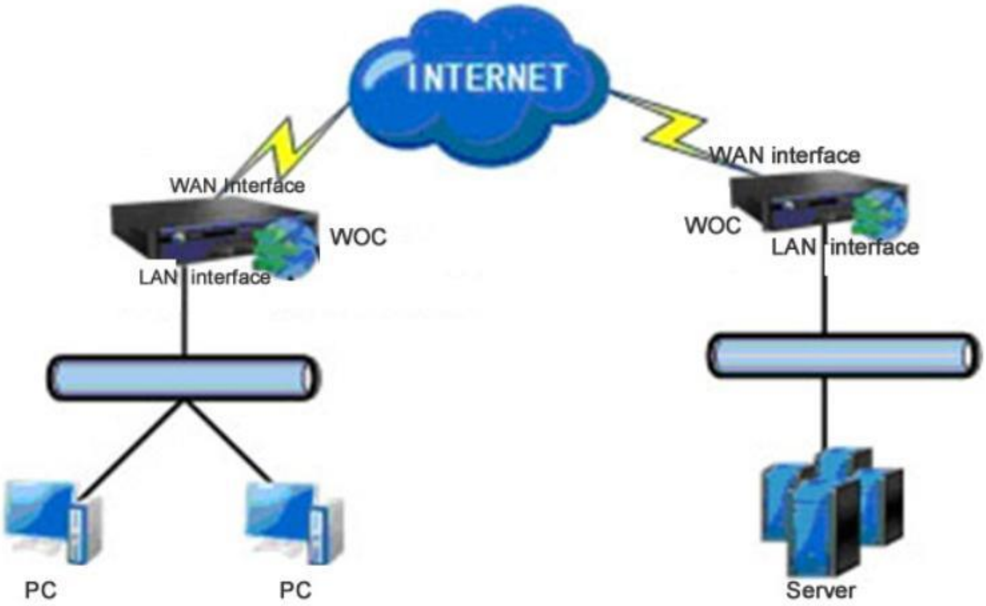
Sangfor WOC supports Gateway Mode (or in-line mode in another term), Bridge Mode, Double Bridge mode, Single Arm mode and Double Arm mode with Acceleration Only functionality, as well as Gateway mode and Single Arm mode with VPN and Acceleation functionalities.

The followings sections describe what each mode is like and how to perform the essential configuration.

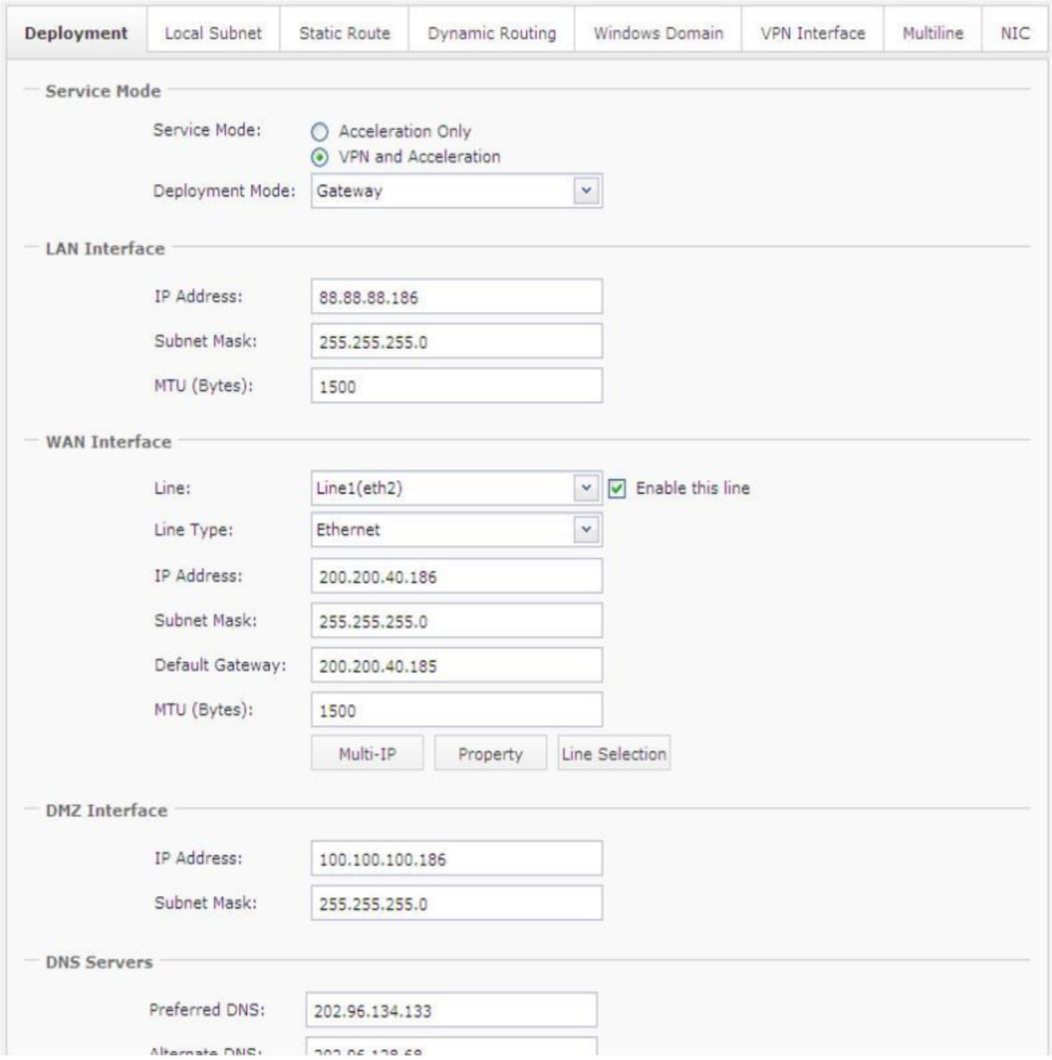
Deploying WOC in Gateway Mode

Posit your Sangfor WOC on your network. Connect it to the other network (for details, please refer to the section

1. Connecting Sangfor Device in Chapter 1). The network topology with WOCs deployed in Gateway mode is as shown in the figure below:



2. Log in to the Web administrator console and go to System > Network > Deployment. Select service mode Acceleration Only or VPN and Acceleration, and deployment mode Gateway mode, as shown in the figure below:



Service Mode

Service Mode: ○ Acceleration Only ● VPN and Acceleration

Deployment Mode: Gateway

LAN Interface

IP Address: 88.88.88.186

Subnet Mask: 255.255.255.0

MTU (Bytes): 1500

WAN Interface

Line: Line1(eth2) ☑ Enable this line

Line Type: Ethernet

IP Address: 200.200.40.186

Subnet Mask: 255.255.255.0

Default Gateway: 200.200.40.185

MTU (Bytes): 1500

DMZ Interface

IP Address: 100.100.100.186

Subnet Mask: 255.255.255.0

DNS Servers

Preferred DNS: 202.96.134.133

Alternate DNS: 202.96.128.68

3. Configure the fields on the above page. The following are the contents included on the Deployment page with Gateway mode selected:

Service Mode: Service mode falls into Acceleration Only and VPN and Acceleration.

Acceleration Only: If this option is selected, only acceleration feature is enabled, which means the Sangfor VPN feature does not work. Under this service mode, you can deploy the WAN Optimization Controller (WOC) in Gateway mode, Bridge mode, Double Bridge mode, Single Arm mode and Double Arm mode.

VPN and Acceleration: If this option is selected, both Sangfor VPN and acceleration features are enabled. This service mode is suitable for the environment that the local and peer WAN Optimization Controllers are deployed in public networks and need to establish VPN connection in between. The Sangfor VPN module can help to build VPN tunnel on which acceleration connection is established between the two terminals.

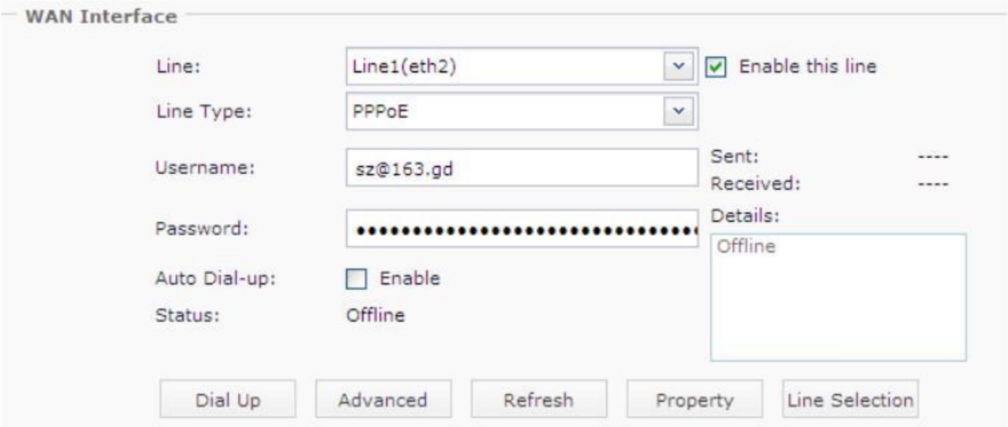
LAN Interface: Configures the IP address of the internal interface, LAN interface, which is protected by the firewall. This IP address must be identical as that of the physical LAN interface on the Sangfor WOC.

WAN Interface: This is the external (public) interface of the Sangfor WOC, corresponding to an WAN link.

Line: Select a line and the configured IP address, network mask and gateway are applied to that internet line.

Line Type: Defines how the specified WAN link connects to the Internet and how the public IP address is assigned. Options are Ethernet, PPPoE and DHCP. Prarameters of each type vary. You can select Ethernet and configure the IP address, netmask and default gateway by hand, or select PPPoE to have it dial up or auto-dialup to the the Internet, or simply select DHCP to use DHCP to automatically assign a public IP address to the WAN interface.

Dial Up: Before new PPPoE settings take effect, all the services will restart. After restart, you can go to this page again and click the Dial Up button to connect the Sangfor WOC to the Internet. If Auto Dial-up is enabled, the WOC will automatically dial up again once it disconnects from the Internet.



WAN Interface

Line: Line1(eth2) ☑ Enable this line

Line Type: PPPoE

Username: sz@163.gd

Password: ••••••••••••••••••••••••••••••••

Auto Dial-up: □ Enable

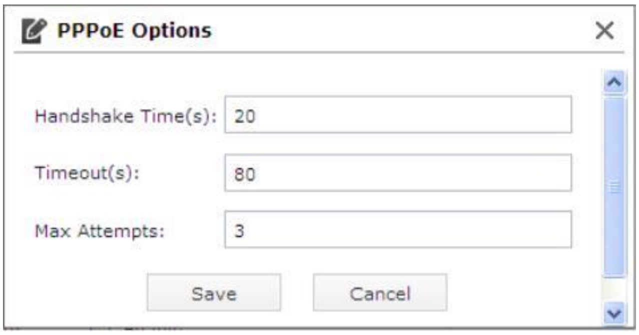
Status: Offline

Sent: ----

Received: ----

Details: Offline

Advanced: Click this button to configure the advanced options of PPPoE, handshake times, timeout and maximum attempts, which are 20, 80 and 3 by default.



PPPoE Options

Handshake Time(s): 20

Timeout(s): 80

Max Attempts: 3

Multi-IP: If WAN interface uses static IP address, you can bind multiple IP addresses to it by clicking this button and add the IP address/netmask entry.

⚠

The IP address binding to WAN interface cannot be the same as the WAN interface IP you configured previously, yet should be in the same network segment as that WAN interface; otherwise, the binding IP address will not work properly.

None of the binding IP addresses should be used by VPN settings.

MTU: It is Minimum Transmission Unit in short. Default is the Ethernet standard value 1500 bytes. In some network environment, if the MTU of certain network device is lower than 1500, the related data packets might be discarded; in that case, you can manually modify this MTU value and keep it relevant with other network devices.

DMZ Interface: Configures the IP address and netmask of the internal interface, DMZ inteface. DMZ is a network segment on a local area network. Some servers are located in DMZ, such as web server, mail server, FTP server and external DNS server and so on, providing services for the external networks. The firewall allows the services from this network segment to be delivered over WAN and protects them from attacks at the same time.

IP addresses of LAN interface, WAN interface and DMZ interface must be coherent with the actual IP addresses of the physical interfaces.

If the physical DMZ interface is not connecting to the DMZ, keep the default settings unchanged.

DNS Servers: Indicates the Domain Name Server provided by the local Internet Service Provider (ISP) to solve domain names. Preferred DNS is required while Alternate DNS is optional.

4. Configure Sangfor VPN (for details, please refer to Chapter 4 Sangfor VPN).
5. Go to WAN Optimization to complete WAN optimization settings (for details, please refer to the section Chapter 5 WAN Optimization).
6. If your network is divided into several network segments and deployed with a layer 3 switch, go to System > Network > Local Subnet to add route for each network segment (except the network segment in which the LAN interface resides) on the WOC to ensure normal communication between this WOC and the hosts on other network segments.

Deploying WOC in Single Arm Mode

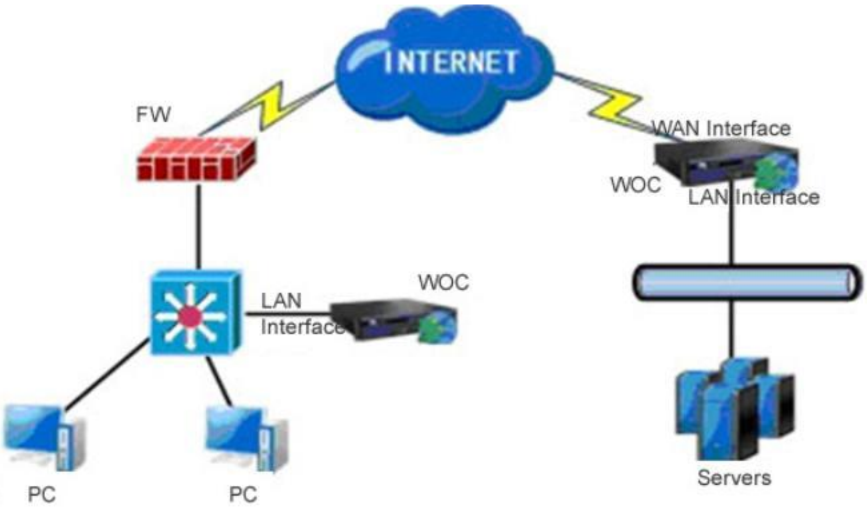
Sangfor WOC can be deployed in Single Arm mode in two situations, Internet environment and leased line environment, which are slightly different in network topology and configuration.

The following are the steps of how to deploy WOC in Internet environment:

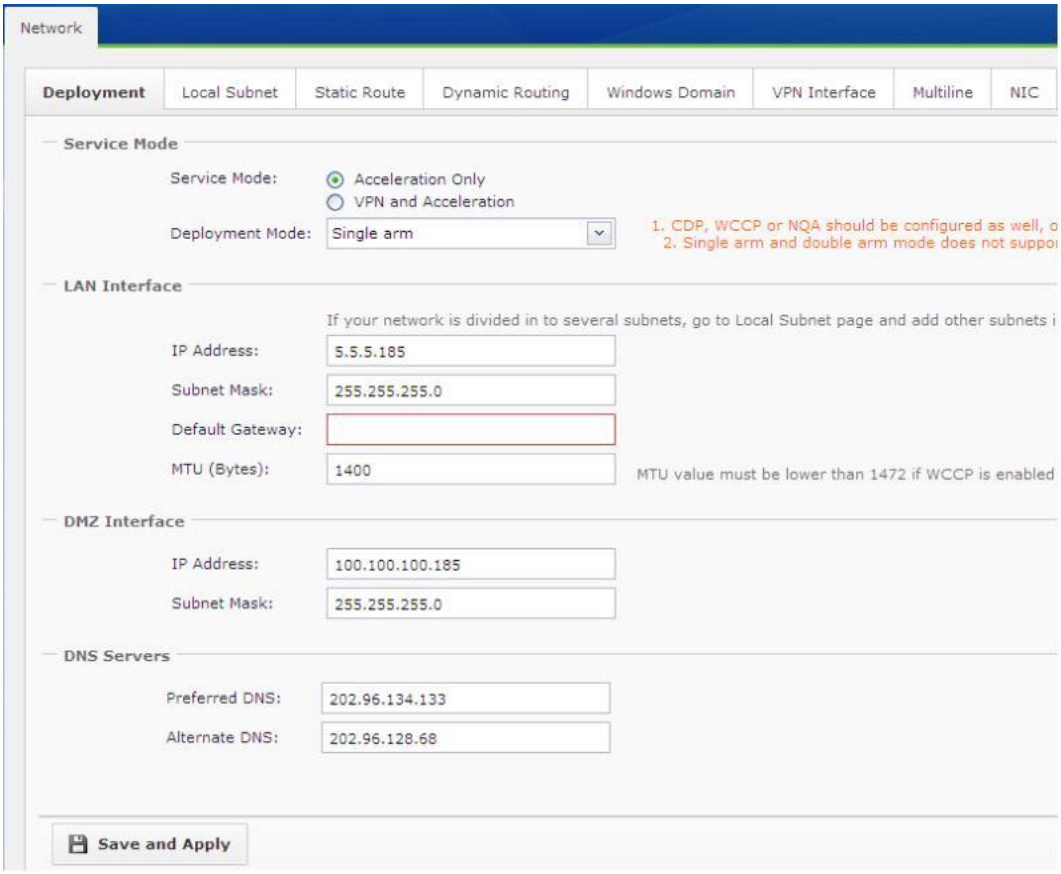
Posit your Sangfor WOC in your network. Connect it to the other network devices (for details, please refer to the section

1. Connecting Sangfor Device in Chapter 1).

   The network topology with WOCs deployed in Single Arm mode is as shown below:



2. Log in to the Web administrator console and go to System > Network > Deployment. Select service mode Acceleration Only or VPN and Acceleration, and deployment mode Single arm.



Service Mode

Service Mode: ● Acceleration Only ○ VPN and Acceleration

Deployment Mode: Single arm

1. CDP, WCCP or NQA should be configured as well, o
2. Single arm and double arm mode does not suppo

LAN Interface

If your network is divided in to several subnets, go to Local Subnet page and add other subnets i

IP Address: 5.5.5.185

Subnet Mask: 255.255.255.0

Default Gateway:

MTU (Bytes): 1400

MTU value must be lower than 1472 if WCCP is enabled

DMZ Interface

IP Address: 100.100.100.185

Subnet Mask: 255.255.255.0

DNS Servers

Preferred DNS: 202.96.134.133

Alternate DNS: 202.96.128.68

3. Configure the fields on the above page. The following are the contents included on the Deployment page with Acceleration Only and Single Arm selected:

    Service Mode: Service mode falls into Acceleration Only and VPN and Acceleration.

    Acceleration Only: If this option is selected, only acceleration feature is enabled, which means the VPN feature does not work. Under this service mode, you can deploy the WOC in Gateway mode, Bridge mode, Double Bridge mode, Single Arm mode and Double Arm mode.

    VPN and Acceleration: If this option is selected, both VPN and acceleration features are enabled. This service mode is suitable for the environment that the local and peer WAN optimization controllers are deployed in public networks and need to establish VPN connection in between. The Sangfor VPN module can help to build VPN tunnel on which acceleration connection is established between the two terminals.

    LAN Interface: Configures the IP address of the internal interface, LAN interface, which is protected by the firewall. This IP address must be identical as that of the physical interface on the Sangfor WOC.

    Arm Interface: Select a internet line that this interface is corresponding to, and configure the IP address, subnet mask and default gateway. This section is missing if the service mode is Acceleration Only.

    DMZ Interface: Configures the IP address and netmask of the internal interface, DMZ inteface. DMZ is a network segment in an enterprise network. Some servers are located in DMZ, such as web server, mail server, FTP server and external DNS server and so on, providing services for the external networks. The firewall allows the services from this network segment to be delivered over WAN and protects them from attacks at the same time.

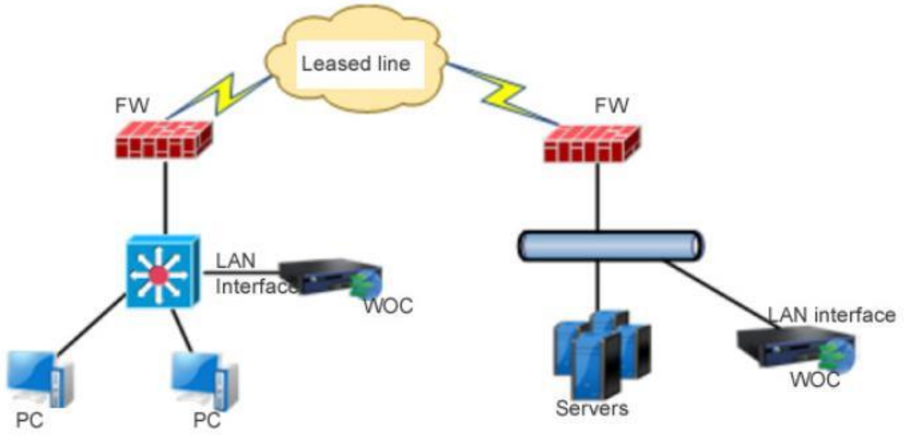
    DNS Servers: Indicates the Domain Name Server provided by the local Internet Service Provider (ISP) to solve domain names. Preferred DNS is required while Alternate DNS is optional.

4. Configure Sangfor VPN (for details, please refer to Chapter 4 Sangfor VPN).
5. Configure WAN Optimization module (for details, please refer to Chapter 5 WAN Optimization).
6. Configure the gateway IP address on the internal computers to have the gateway of internal computers direct to the LAN interface of the WOC, or enable the policy-based routing or WCCP function on the frontend switch or router.

The following are the steps of how to deploy WOC in leased line environment:

Posit your Sangfor WOC in your network. Connect it to the other network devices (for details, please refer to the section

1. Connecting Sangfor Device in Chapter 1). The network topology is as shown below:



2. Log in to the Web administrator console and go to System > Network > Deployment. Select service mode Acceleration Only or VPN and Acceleration, and deployment mode Single arm. The Deployment page is the same as that when WOC is deployed in Internet environment. Please refer the Step 3 in the above section.

3. Configure WAN Optimization module (for details, please refer to Chapter 5 WAN Optimization).

4. Configure the gateway IP address on the internal computers to have the gateway of internal computers direct to the LAN interface of the WOC, or enable the policy-based routing or WCCP function on the frontend switch or router.

⚠

If your network is divided into several subnets, go to System > Network > Local Subnet and Sangfor VPN > Advanced > VPN Local Subnet to add the all the subnets into the local subnet list except the one in which the LAN interface of the WOC resides.

For Single-arm WOC deployed in leased line environment, routing loop may appear and disable data transfer between the devices at both ends. You may ensure the following to avoid routing loop:

a. In Layer 2 environment, have the gateway of the internal PCs direct to the Sangfor WOC;

b. In Layer 2 environment, add a route for each PC that directs to the peer terminal, the local WOC as the gateway of the route;

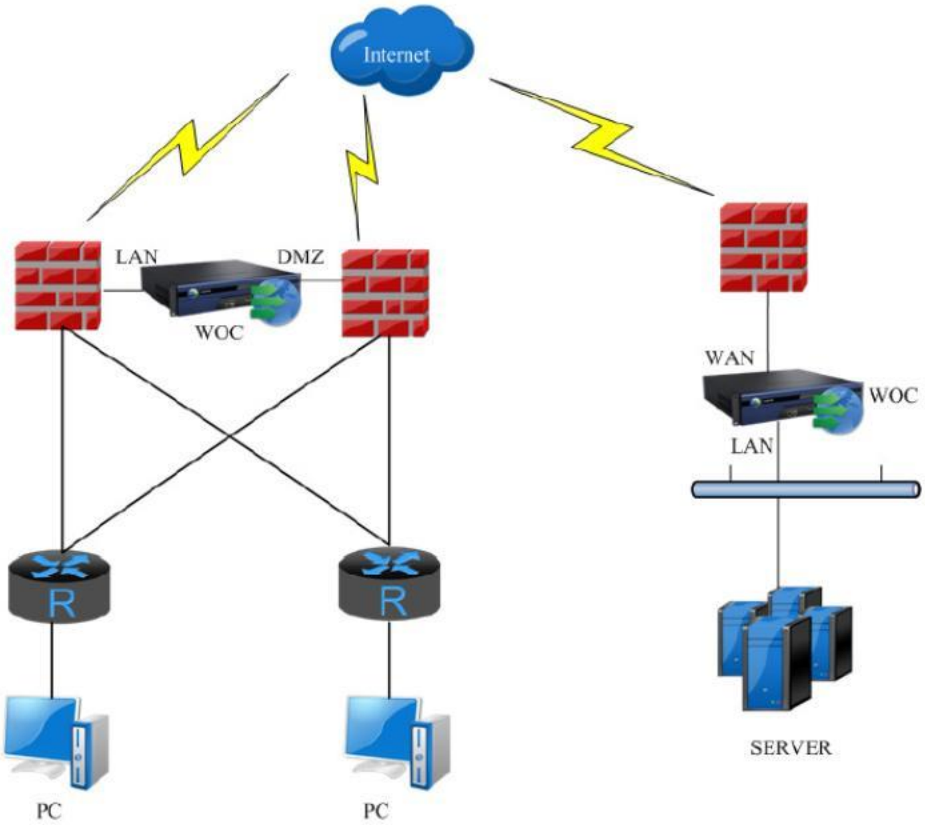
c. Enable policy-based routing and CDP on the frontend device;

d. Enable WCCP function on the frontend device.

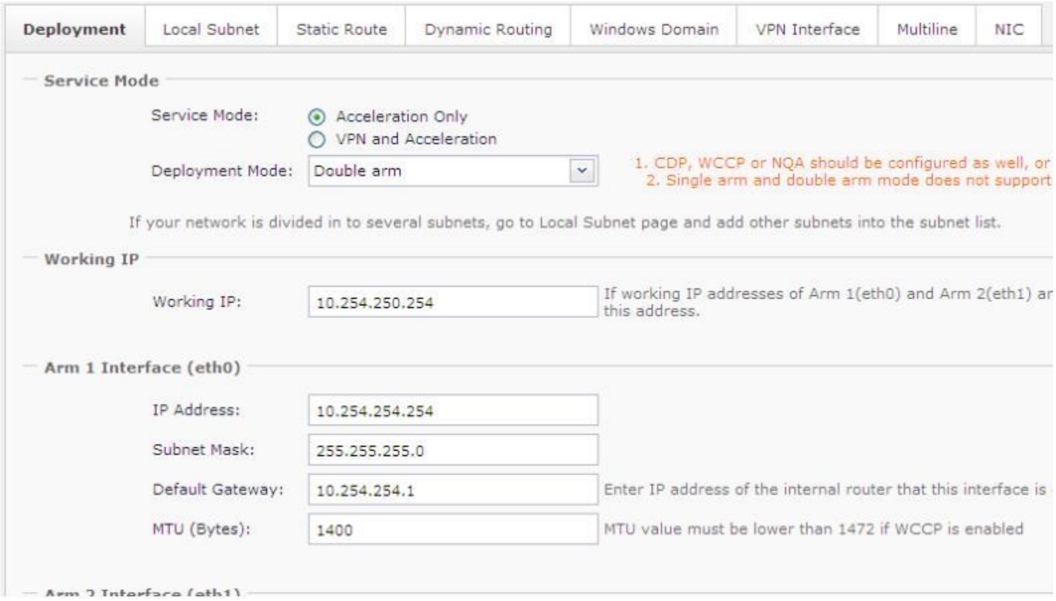
Deploying WOC in Double Arm Mode

Posit your Sangfor WOC in your network. Connect it to the other network devices (for details, please refer to the section

1. Connecting Sangfor Device in Chapter 1).



2. Log in to the Web administrator console and go to System > Network > Deployment. Select service mode Acceleration Only, and deployment mode Double arm.



Service Mode

Service Mode: ● Acceleration Only ○ VPN and Acceleration

Deployment Mode: Double arm

1. CDP, WCCP or NQA should be configured as well, or
2. Single arm and double arm mode does not support

If your network is divided in to several subnets, go to Local Subnet page and add other subnets into the subnet list.

Working IP

Working IP: 10.254.250.254 If working IP addresses of Arm 1(eth0) and Arm 2(eth1) ar this address.

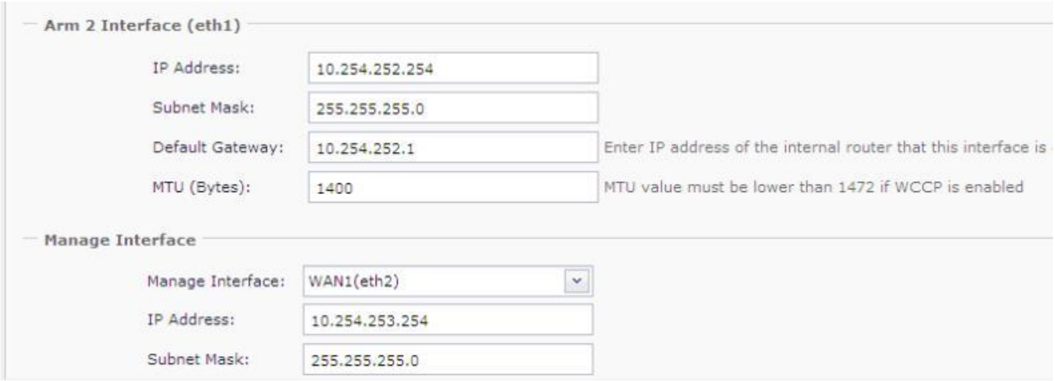
Arm 1 Interface (eth0)

IP Address: 10.254.254.254

Subnet Mask: 255.255.255.0

Default Gateway: 10.254.254.1 Enter IP address of the internal router that this interface is

MTU (Bytes): 1400 MTU value must be lower than 1472 if WCCP is enabled



Arm 2 Interface (eth1)

IP Address: 10.254.252.254

Subnet Mask: 255.255.255.0

Default Gateway: 10.254.252.1 Enter IP address of the internal router that this interface is

MTU (Bytes): 1400 MTU value must be lower than 1472 if WCCP is enabled

Manage Interface

Manage Interface: WAN1(eth2)

IP Address: 10.254.253.254

Subnet Mask: 255.255.255.0

3. Configure the fields on the above page. The following are the contents included on the Deployment page with Acceleration Only and Double arm mode selected:

   Service Mode: Service mode falls into Acceleration Only and VPN and Acceleration. However, Double arm mode is available only in Acceleration Only service mode, which indicates acceleration feature is enabled and VPN feature does not work.

   Working IP: Configures virtual IP address of the double arms. It should be able to communicate with the peer WOC. The local WOC uses this IP address to establish acceleration connections with other remote WAN Optimization Controllers.

   Arm Interface: Configures the IP address, subnet mask and default gateway of the two arm interfaces respectively. The IP addresses of Arm 1/Arm 2 and the working IP could (or not) be on a same network segment, but they should be able to communicate with the internal network.

   Manage Interface: Select a interface as the Manage interface of the WOC.

   DNS Servers: Indicates the Domain Name Server provided by the local Internet Service Provider (ISP) to solve domain names. Preferred DNS is required while Alternate DNS is optional.

4. Configure WAN Optimization module (for details, please refer to Chapter 5 WAN Optimization).

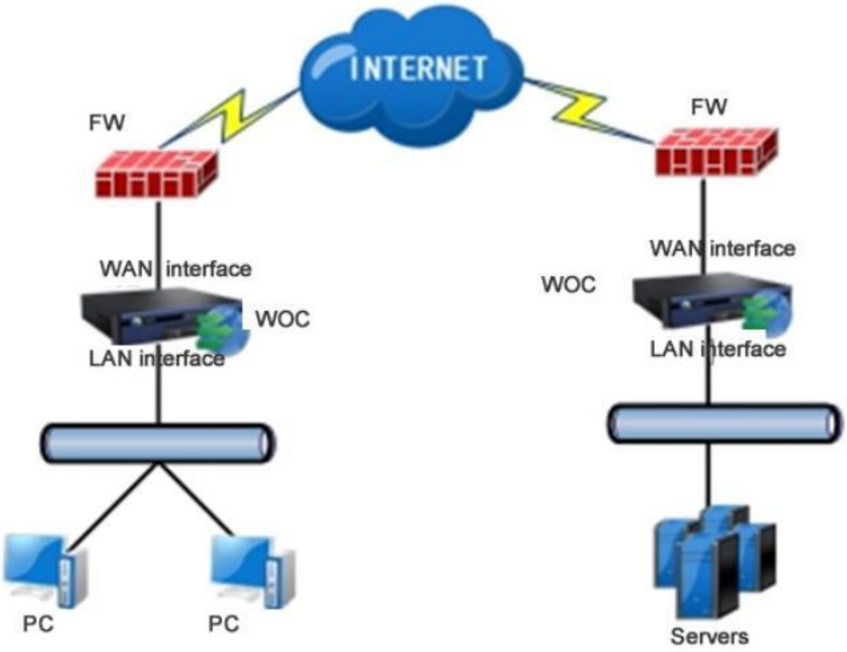
⚠

If the peer WOC initiates acceleration connection to the local WOC that is deployed in Double single arm mode, you need to enable pre-connection on the peer WOC.

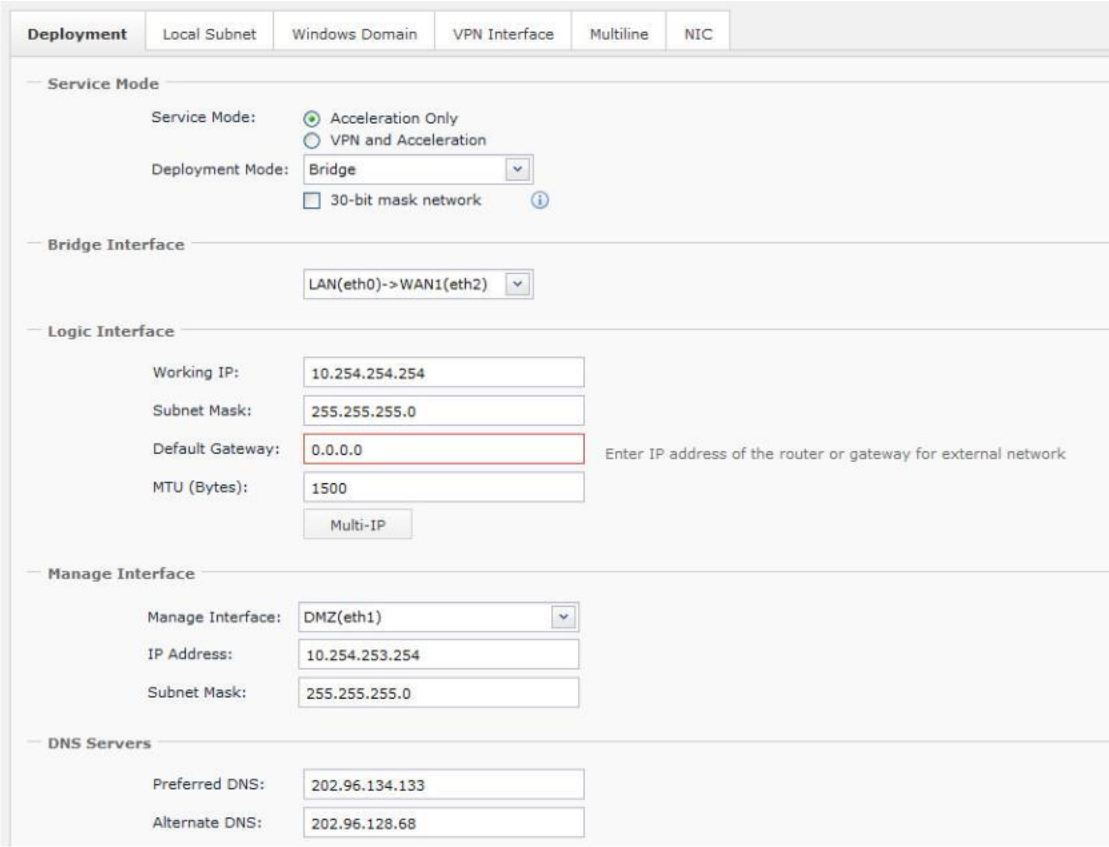
Deploying WOC in Bridge Mode

Posit the Sangfor WOC in your network. Connect it to the other network devices (for details, please refer to the section

1. Connecting Sangfor Device in Chapter 1). The network topology with WOCs deployed in Bridge mode is shown in the figure below:



2. Log in to the Web administrator console and go to System > Network > Deployment. Select service mode Acceleration Only or VPN and Acceleration and deployment mode Bridge.



Service Mode

Service Mode: ● Acceleration Only ○ VPN and Acceleration

Deployment Mode: Bridge

□ 30-bit mask network

Bridge Interface

LAN(eth0)->WAN1(eth2)

Logic Interface

Working IP: 10.254.254.254

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0 Enter IP address of the router or gateway for external network

MTU (Bytes): 1500

Manage Interface

Manage Interface: DMZ(eth1)

IP Address: 10.254.253.254

Subnet Mask: 255.255.255.0

DNS Servers

Preferred DNS: 202.96.134.133

Alternate DNS: 202.96.128.68

3. Configure the fields on the above page. The following are the contents included on the Deployment page with Acceleration Only and Bridge mode selected:

Service Mode: Service mode falls into Acceleration Only and VPN and Acceleration. However, Bridge mode is available only in Acceleration Only service mode.

Acceleration Only: Under this service mode, acceleration feature is enabled, which means the VPN feature cannot work.

VPN and Acceleration: If this option is selected, both Sangfor VPN and acceleration features are enabled. This service mode is suitable for the environment that the local and peer WAN Optimization Controllers are deployed in public networks or lease line environment and need to establish VPN connection in between. The Sangfor VPN module can help to build VPN tunnel on which acceleration connection is established between the two terminals.

30-bit mask network: This option is for when the router and core switch in 30-bit subnet and no more available IP address. After enable this option you can insert another segment IP in bridge interface. (Make sure this IP is able to reach by route) After that make sure to configure a manage interface to manage WANO and join domain for Exchange optimization. If Domain controller is different range with the manage IP, you may configure a static route.

Bridge Interface: Select an interface pair to form a bridge between the external network and internal network. Options are LAN(eth0)->WAN1(eth2) and DMZ(eth1)->WAN2(eth3).

Logic Interface: Configures the IP address, subnet mask and default gateway of the logic interface, Br0.

Manage Interface: Configures the IP address of the Manage interface of the WOC. You can select any interface as the Manage interface except the interface pair used for bridging.

DNS Servers: Indicates the Domain Name Server provided by the local Internet Service Provider (ISP) to solve domain names. Preferred DNS is required while Alternate DNS is optional.

⚠

Under Bridge mode, LAN interface (eth0) and WAN (eth2/3) interface cannot be mixed up; otherwise, no acceleration effect will be achieved.

The IP address of the logic interface must be on the same subnet segment as the firewall device/ router for external network and the core switch for internal network.

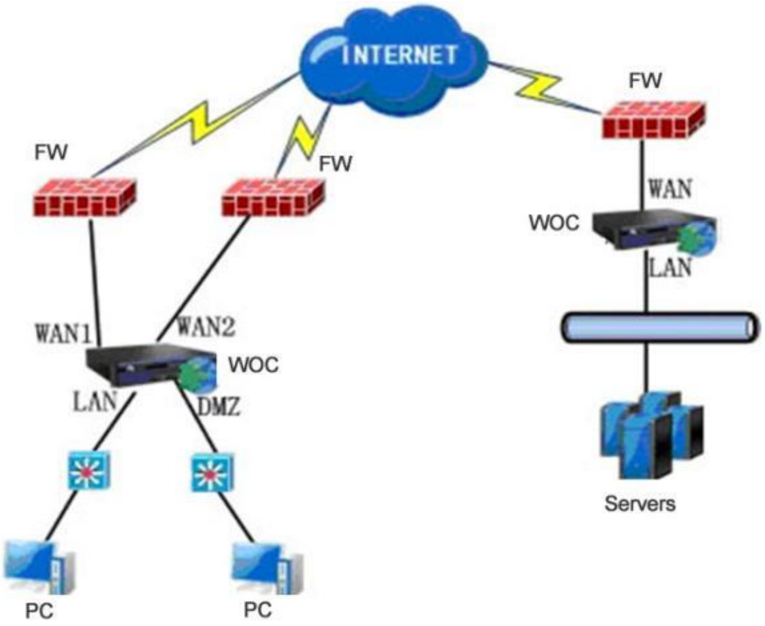
The Manage interface can only be used for managing the Sangfor WOC, not supporting other uses such as connecting to the Internet.

To configure Bridge mode, you need to ensure that the two WAN Optimization Controllers are able to communicate with each other through the VPN tunnel established by a VPN device or through a leased line.

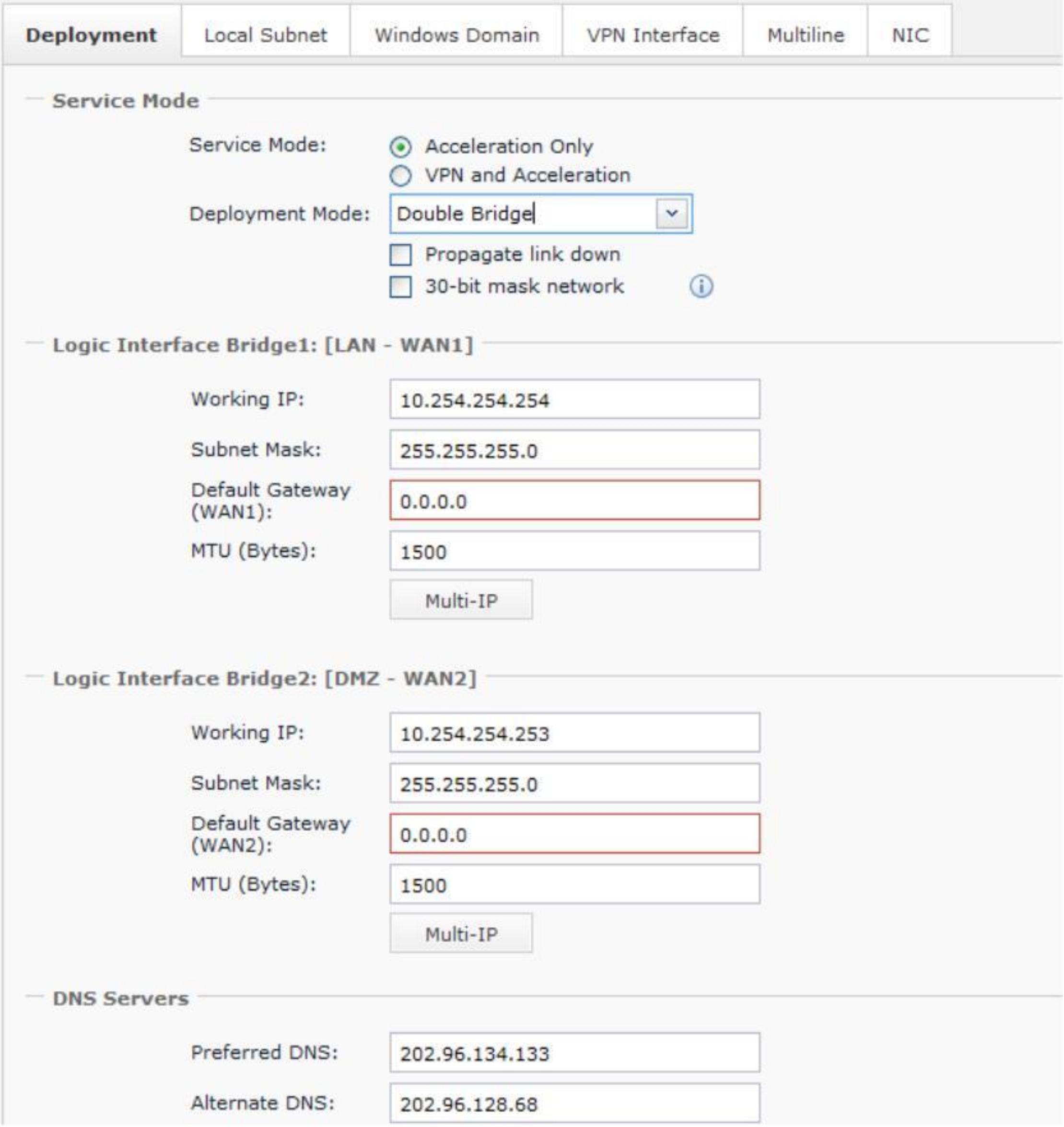
Deploying WOC in Double Bridge Mode

Posit your Sangfor WOC in your network. Connect it to the other network devices (for details, please refer to the section

1. Connecting Sangfor Device in Chapter 1). The network topology with WOCs deployed in Double Bridge mode is as shown in the figure below:



2. Log in to the Web administrator console and go to System > Network > Deployment. Select service mode Acceleration Only and deployment mode Double bridge. The Deployment page is as shown in the figure below:



Service Mode

Service Mode: ● Acceleration Only ○ VPN and Acceleration

Deployment Mode: Double Bridge

□ Propagate link down

□ 30-bit mask network

Logic Interface Bridge1: [LAN - WAN1]

Working IP: 10.254.254.254

Subnet Mask: 255.255.255.0

Default Gateway (WAN1): 0.0.0.0

MTU (Bytes): 1500

Multi-IP

Logic Interface Bridge2: [DMZ - WAN2]

Working IP: 10.254.254.253

Subnet Mask: 255.255.255.0

Default Gateway (WAN2): 0.0.0.0

MTU (Bytes): 1500

Multi-IP

DNS Servers

Preferred DNS: 202.96.134.133

Alternate DNS: 202.96.128.68

3. Configure the fields on the above page. The following are the contents included on the Deployment page with Double Bridge mode selected:

    Service Mode: Service mode falls into Acceleration Only and VPN and Acceleration. However, Double Bridge mode is available only in Acceleration Only service mode, which indicates acceleration feature is enabled and VPN feature does not work.

    30-bit mask network: This option is for when the router and core switch in 30-bit subnet and no more available IP address. After enable this option you can insert another segment IP in bridge interface. (Make sure this IP is able to reach by route) After that make sure to configure a manage interface to manage WANO and join domain for Exchange optimization. If Domain controller is different range with the manage IP, you may configure a policy route.

    Propagate link down: Select this option if the WOC is deployed in redundant network environment (such as VRRP). Once the system detects that any interface of the bridge pair falls out, it will automatically disconnect the other interface of the bridge pair, to ensure smooth data transmission and switch between the clustered WAN optimization controllers.

Logic Interface: Configures the working IP address, subnet mask, default gateway and MTU of the two bridge pairs respectively.

⚠

If IP addresses of the two logic interfaces Br0 and Br1 are on a same network segment, the Working IP should be on the same network segment. If IP addresses of the two logic interfaces Br0 and Br1 are NOT on a same network segment, the Working IP should not be on the same network segment as either of them, and you need to ensure that the peer Sangfor WOC can connect to this working IP address.

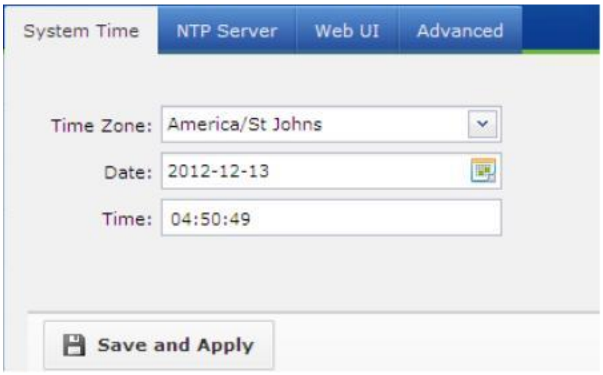
If there is a layer 3 switch on the local area network, Default Gateway(LAN/DMZ) must be filled in; otherwise, leave the two fields empty.

System Settings

System settings include System Time, NTP Server, Web UI and Advanced settings.

System Time

1. Navigate to System > System to enter the System Time page, as shown below:



Time Zone: America/St Johns

Date: 2012-12-13

Time: 04:50:49

2. Configure the following:

   Time Zone: Specifies the time zone of the country or region where your Sangfor device is resides.

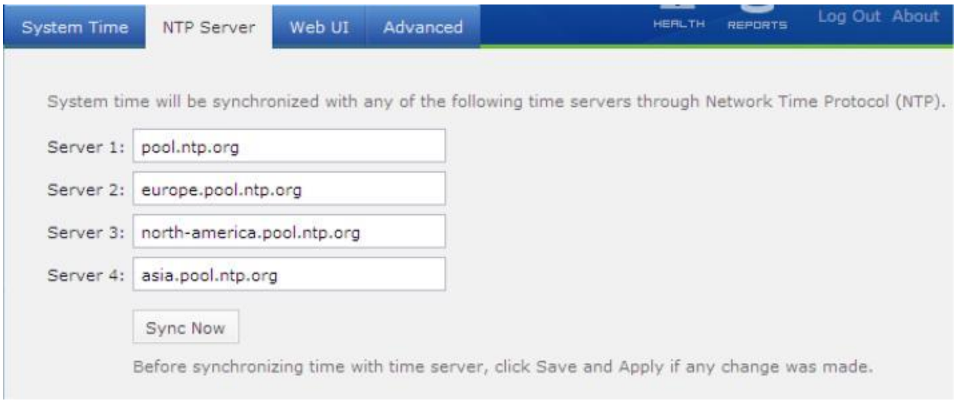
   Date: Specifies the date. To select date, click the icon.

   Time: Specifies the time. Enter the time into this field and set it as the current time of this Sangfor WOC. Date format should be hh: mm: ss.

3. Click the Save and Apply button to save the settings. This operation leads to service restart.

NTP Servers

NTP server is the server with which system time on the Sangfor WOC can synchronize.



System time will be synchronized with any of the following time servers through Network Time Protocol (NTP).

Server 1: pool.ntp.org

Server 2: europe.pool.ntp.org

Server 3: north-america.pool.ntp.org

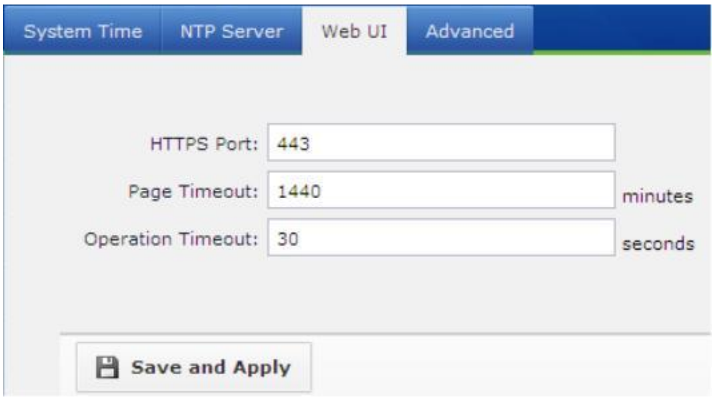
Server 4: asia.pool.ntp.org

Before synchronizing time with time server, click Save and Apply if any change was made.

Enter the addresses of the Network Time Protocol (NTP) servers, and then click the Sync Now button to synchronize time with the server right now.

Web UI Settings

Web UI settings include Web service port of the administrator console and the inactivity timeout.



HTTPS Port: 443

Page Timeout: 1440 minutes

Operation Timeout: 30 seconds

The following are the contents included on the Web UI tab:

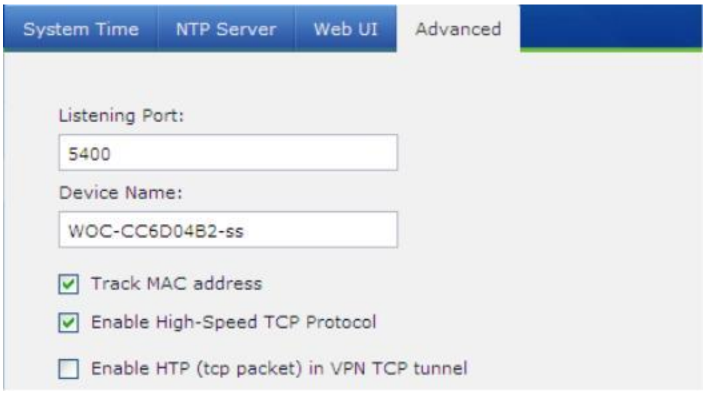
HTTPS Login Port: Configures the HTTPS port used for logging in to the Web administrator console. If HTTPS port is modified, you need to log in through the new port.

Page Timeout: If no operation is performed on the administrator console for so long a period of time, the console user will be logged out. In unit of minute.

Operation Timeout: If a page fails to open after loading so long a period of time, it will get timed out.

Advanced System Settings

Advanced system settings includes listening port for acceleration service, device name and others.



Listening Port: 5400

Device Name: WOC-CC6D04B2-ss

☑ Track MAC address

☑ Enable High-Speed TCP Protocol

□ Enable HTP (tcp packet) in VPN TCP tunnel

The following are the contents included on the Advanced tab:

Listening Port: Configures the listening port of acceleration service. It is TCP and UDP 5400 port by default. WOC at both ends must be able to access its peer listening port normally; otherwise, acceleration connection cannot be established between the two WOCs.

Device Name: Configures the name of the WOC, which distinguishes it from the peer or the WOC at other sites. You can view device name and version information by clicking on About at the upper-right of the page.

Track MAC address: Select this option so that the MAC address could be tracked in Single bridge mode, even there is a layer-3 switch is involved. In that case, you need not to add packet-return route.

Track MAC address feature takes effect only in Single bridge mode.

Enable High-Speed TCP Protocol: Select this option to enable High-Speed TCP Protocol (HTP). HTP is a variable TCP protocol that is enhanced by SANGFOR.

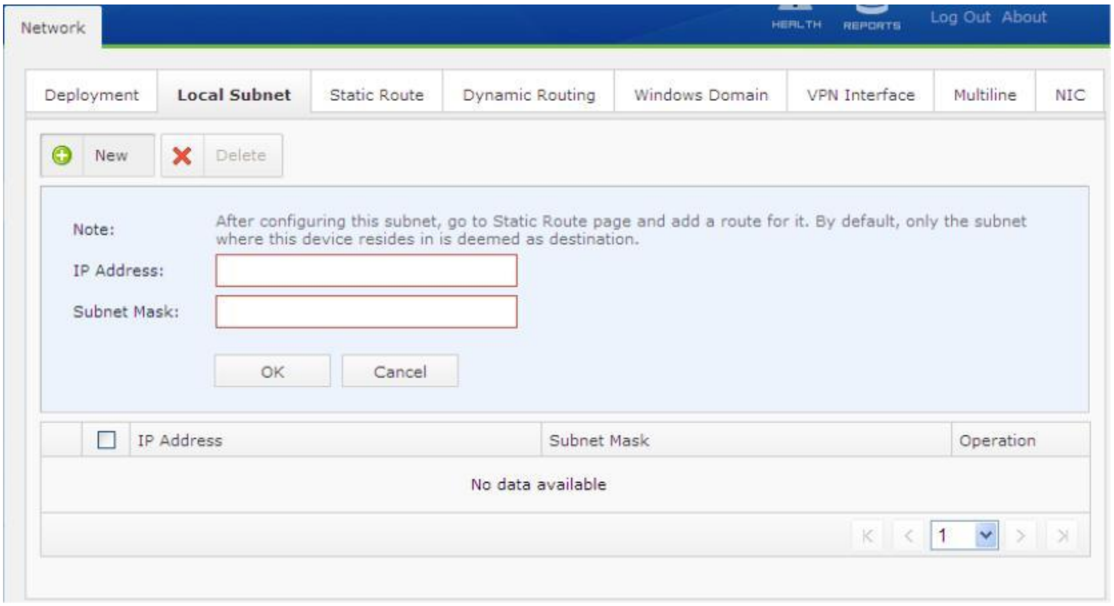
Enable HTP (tcp packet) in VPN TCP tunnel: Select this option to enable use of HTP in VPN TCP tunnel.

Network Settings

In addition to deployment settings, you may need to complete the other network related configuration after configuring the Deployment page, such as local subnet, static route, dynamic route, Windows Domain, VPN interface, VLAN, multi-line, CDP and WCCP settings.

Local Subnet

The so-called local subnet is any network segment thought on the LAN where the WAN Optimization Controller (WOC) is deployed, yet excluding the network segment in which the LAN interface of the WOC resides. Connecting VPN users can access the machines in those subnets even those machines and the Sangfor WOC are on different subnets physically.



Note: After configuring this subnet, go to Static Route page and add a route for it. By default, only the subnet where this device resides in is deemed as destination.

IP Address:

Subnet Mask:

□	IP Address	Subnet Mask	Operation
	No data available		

Creating Local Subnet

Suppose the enterprise network is divided into two subnets, 192.168.10.0/24 and 192.168.20.0/24, and the Sangfor WOC is deployed in Single Arm mode, LAN interface IP and subnet mask is 192.168.10.0/24.

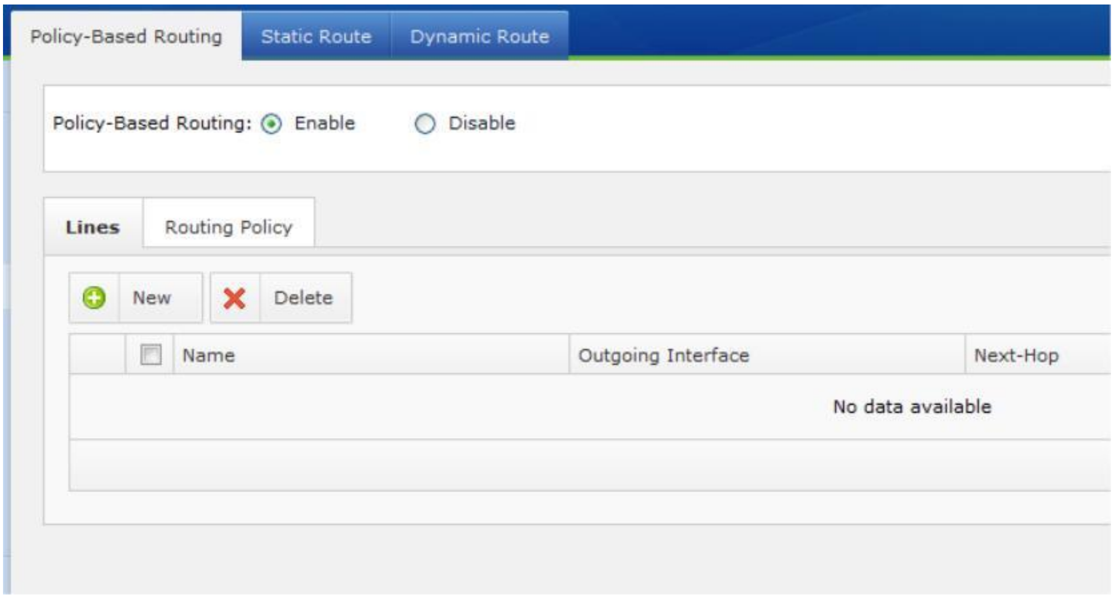
Perform the following steps to add the other subnet into the local subnet list.

1. Go to System > Network > Local Subnet page and click New.
2. Enter the 192.168.20.0 into the IP Address field and 255.255.255.0 into the Subnet Mask field.
3. Click the OK button to save the settings.

Policy-Based Routing

Policy route can base on the policy (application type, source IP, destination IP, etc.) to achieve the purpose multiple lines routing, load balancing and backup lines.

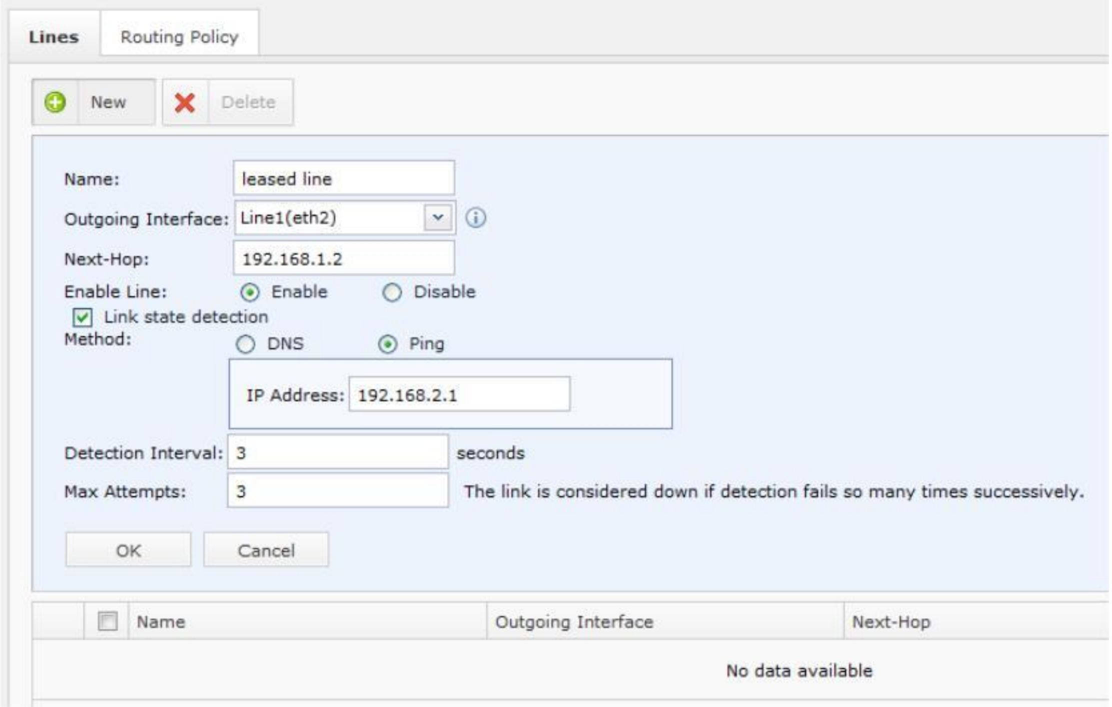
The Policy-Based Routing page is as shown below:



Policy-Based Routing: ● Enable ○ Disable

□	Name	Outgoing Interface	Next-Hop
		No data available	

Lines : Define transfer line



Name: leased line

Outgoing Interface: Line1(eth2)

Next-Hop: 192.168.1.2

Enable Line: ● Enable ○ Disable

☑ Link state detection

Method: ○ DNS ● Ping

IP Address: 192.168.2.1

Detection Interval: 3 seconds

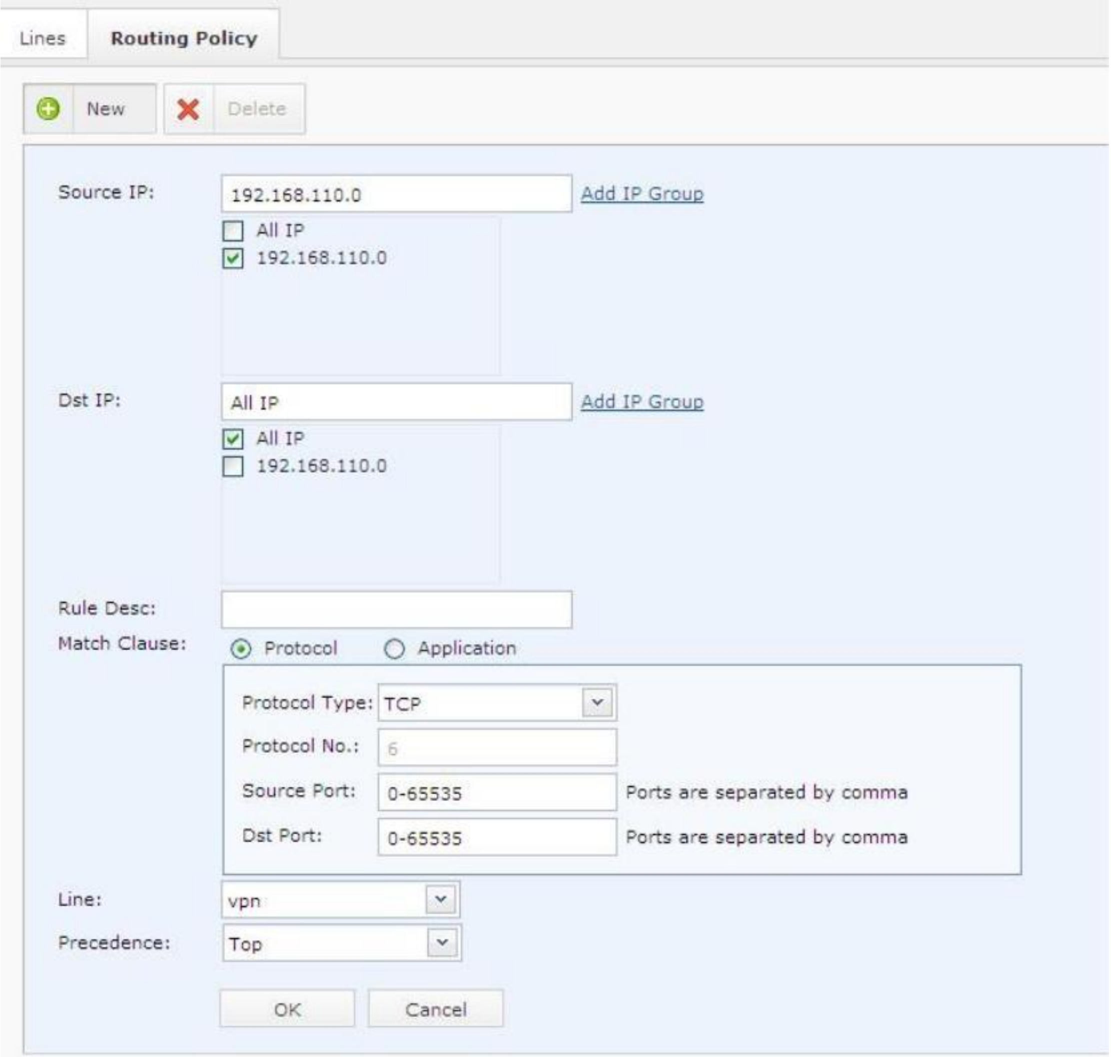
Max Attempts: 3 The link is considered down if detection fails so many times successively.

□	Name	Outgoing Interface	Next-Hop
		No data available	

Name	Description

name	Name of these line
Outgoing Interface	Select corresponding physical network interface, vpn interface, pppoe interface.
Next-Hop	Next-Hop IP address, available on bridge mode only
Link state detection	Detect link status. DNS detection method suitable for dial-up lines and not able Ping link. Ping detection method suitable for leased line or vpn line.
Detection Interval	Interval of detection packet.
Max Attempts	Maximum attempts on detection packet.

Routing Policy



Source IP: 192.168.110.0
□ All IP
☑ 192.168.110.0

Dst IP: All IP
☑ All IP
□ 192.168.110.0

Rule Desc:

Match Clause: ● Protocol ○ Application

Protocol Type: TCP
Protocol No.: 6
Source Port: 0-65535 Ports are separated by comma
Dst Port: 0-65535 Ports are separated by comma

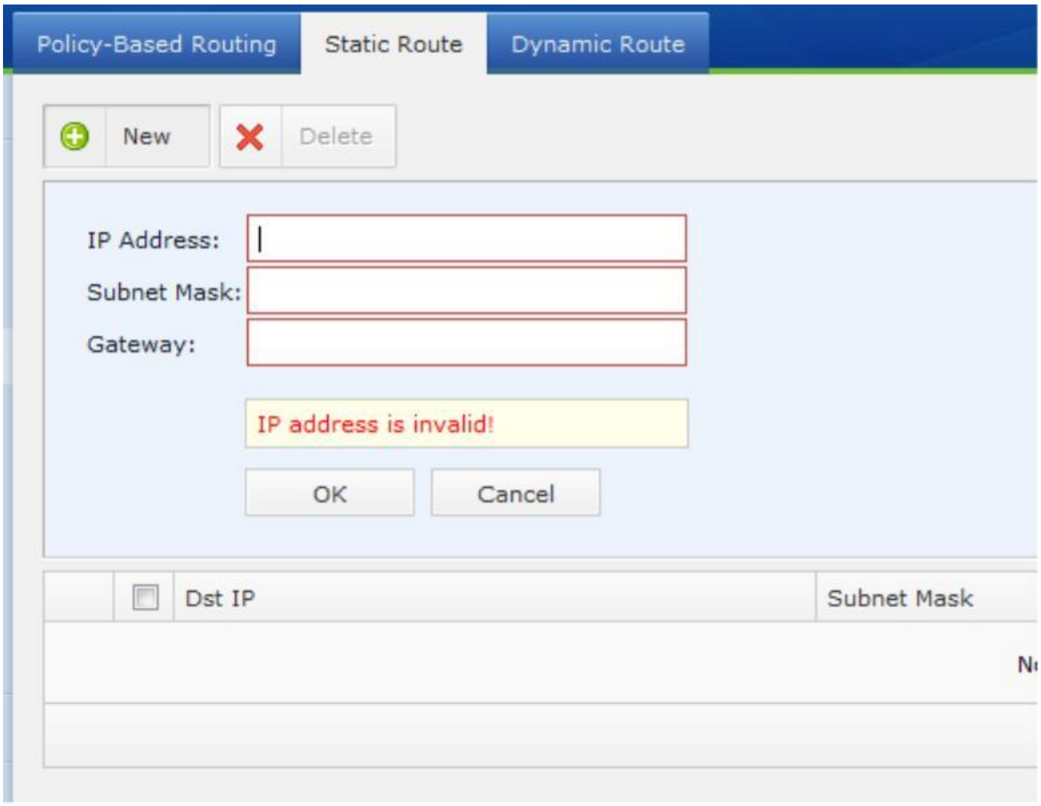
Line: vpn
Precedence: Top

Name	Description
Source IP	Source IP group, define in Objects->IP Group.
Dst IP	Destination IP group, define in Objects->IP Grou.
Rule Desc	Rule Description
Match Clause Line	Matching policy, can match with protocol or application. Select route to which line
Precedence	Priority

Static Route

Static route is intended to route the data packets (both VPN relevant and irrelevant) that need to be forwarded by the WAN Optimization Controller (WOC) and the data packets from or to the WAN WOC itself.

The Static Route page is as shown below:



IP address is invalid!

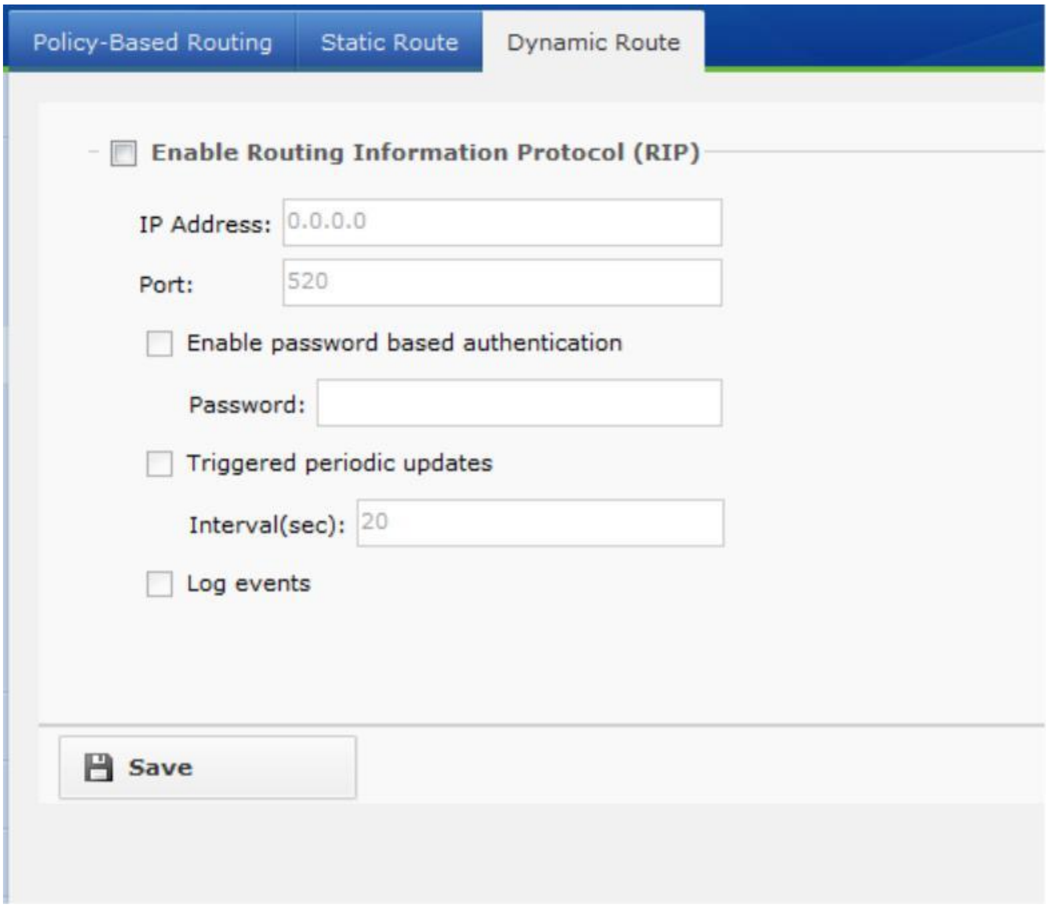
Creating Static Route

Perform the following steps to add a static route entry:

1. Go to System > Routing > Static Route page and click New.
2. Configure Destination IP, Subnet Mask and Gateway.
3. Click the OK button to save the settings.

Dynamic Routing

Dynamic RIP settings on Dynamic Route page will enable the Sangfor WAN Optimization Controller (WOC) to notify other routing devices of the routing information by using RIPv2 protocol, and therefore, to ensure that the RIP routing information on the routing devices in the internal network can be dynamically updated.



☐ Enable Routing Information Protocol (RIP)

IP Address: 0.0.0.0

Port: 520

☐ Enable password based authentication

Password:

☐ Triggered periodic updates

Interval(sec): 20

☐ Log events

The following are the contents included on the Dynamic Routing page:

Enable Routing Information Protocol (RIP): Select this option to enable dynamic routing. The WOC will inform the routing device in the internal network of the network information of the peer VPN network if it has established VPN connection with a remote network.

Enable password based authentication: Configures the password needed for exchanging RIPv2 protocol information. You can configure it according to your specific case.

IP Address, Port: Configures the IP address and port of the routing device to which the WOC sends routing updates initiatively.

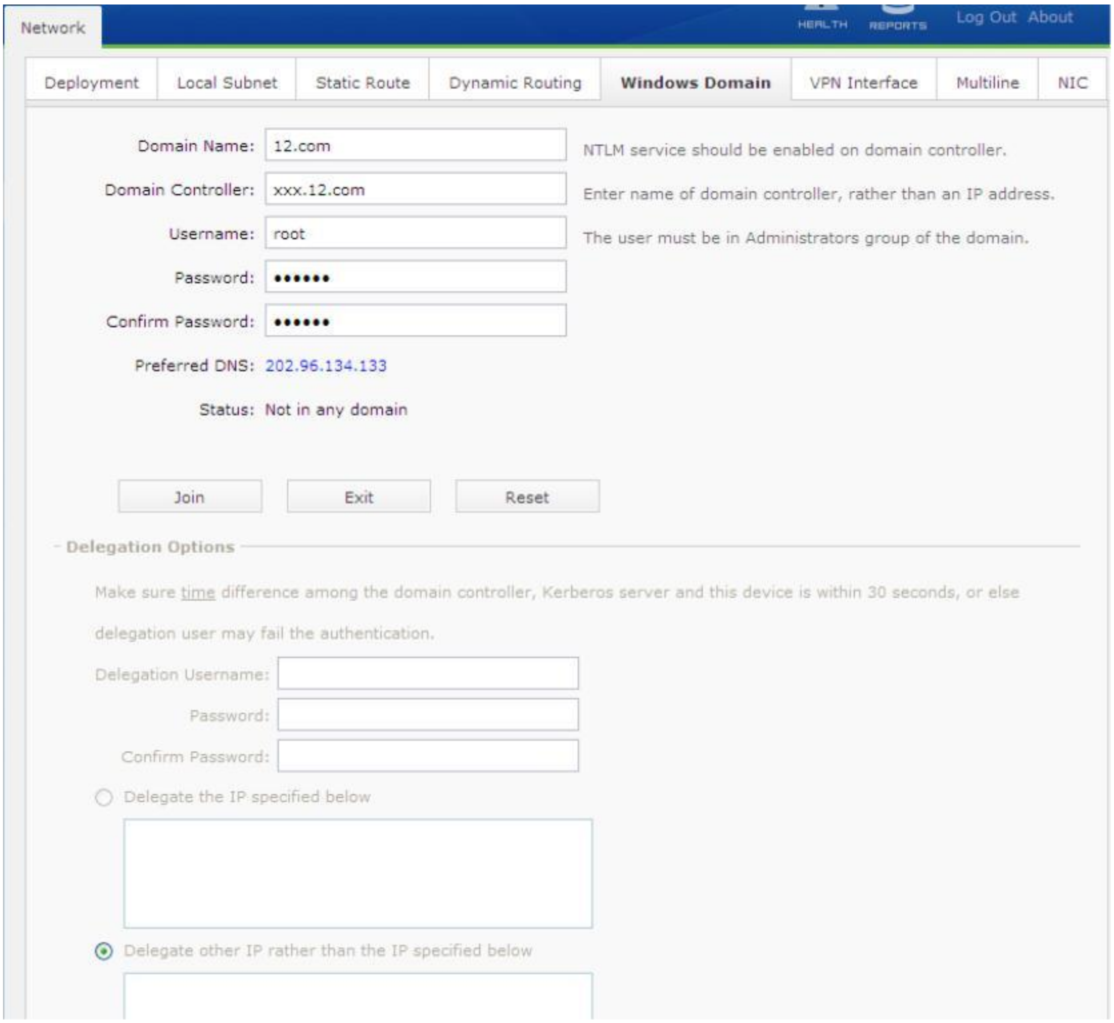
Trigger periodic updates: Select this option and the WOC will trigger an update when the routing information changes; in that case, the Interval(sec) will get invalid.

Log events: Select this option and the WOC will log the RIP routing update information.

The routing device itself does not accept dynamic update by RIP protocol. If the WOC needs to communicate with other routing devices in the internal network that have enabled RIP, you should add static route on the WOC directing to that device.

Windows Domain

You can add the Sangfor WAN Optimization Controller (WOC) into the windows domain of enterprise network, so that some corporate applications (such as Exchange, CIFS) can also be optimized.



Domain Name: 12.com NTLM service should be enabled on domain controller.

Domain Controller: xxx.12.com Enter name of domain controller, rather than an IP address.

Username: root The user must be in Administrators group of the domain.

Password: ••••••

Confirm Password: ••••••

Preferred DNS: 202.96.134.133

Status: Not in any domain

Delegation Options

Make sure time difference among the domain controller, Kerberos server and this device is within 30 seconds, or else delegation user may fail the authentication.

Delegation Username:

Password:

Confirm Password:

○ Delegate the IP specified below

● Delegate other IP rather than the IP specified below

The following are the contents included on the Windows Domain page:

Domain Name: Configures the domain name of Windows Domain.

Domain Controller: Configures the domain controller of the Windows Domain.

Username: Configures the admin account used for logging into the Windows Domain.

Password: Configures the password of the admin for logging into the Windows Domain.

Confirm Password: Enter the password again to confirm the password.

Preferred DNS: Displays the DNS server address configured on the Deployment page. This DNS server address must be the same as that in the domain.

Status: Displays the status whether it has joined any Windows Domain.

Join: Click this button to have the WOC join the specified Windows Domain.

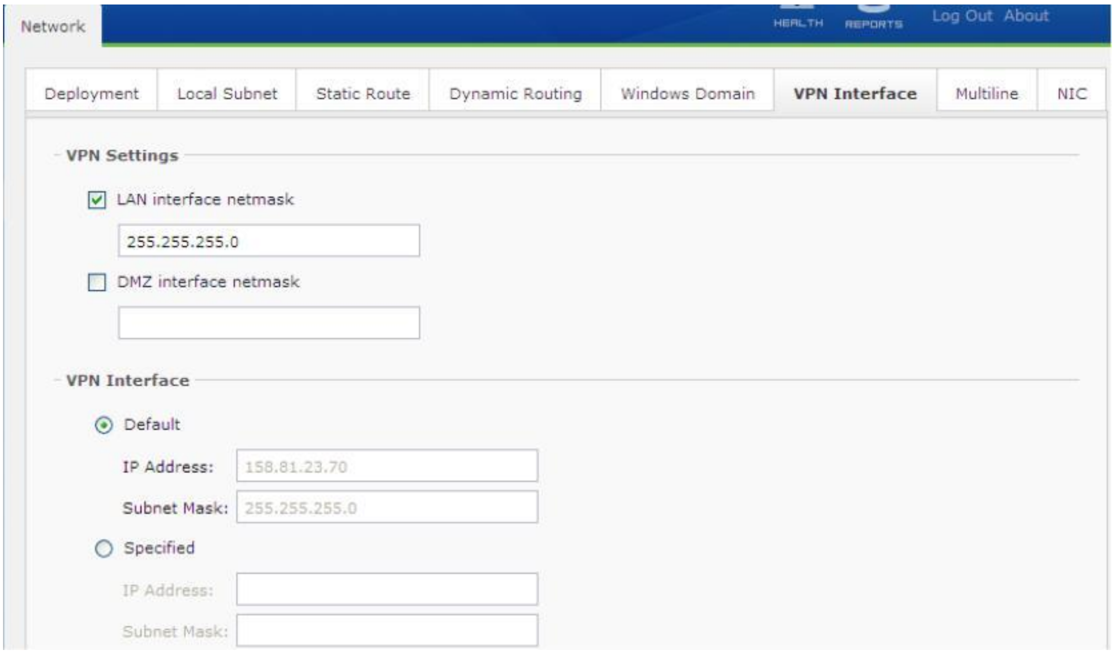
Exit: Click this button to have the WOC exit from the Windows Domain.

Reset: Click this button to reset the settings on this page.

Only the server-end Sangfor WOC needs to join Windows Domain.

VPN Interface

The VPN Interface page allows you to set the IP address of the virtual adapter for VPN service. Go to System > Network > VPN Interface to enter the VPN Interface page, as shown below:



VPN Settings

☑ LAN interface netmask

255.255.255.0

□ DMZ interface netmask

VPN Interface

● Default

IP Address: 158.81.23.70

Subnet Mask: 255.255.255.0

○ Specified

IP Address:

Subnet Mask:

The following are the contents included on the VPN Interface page:

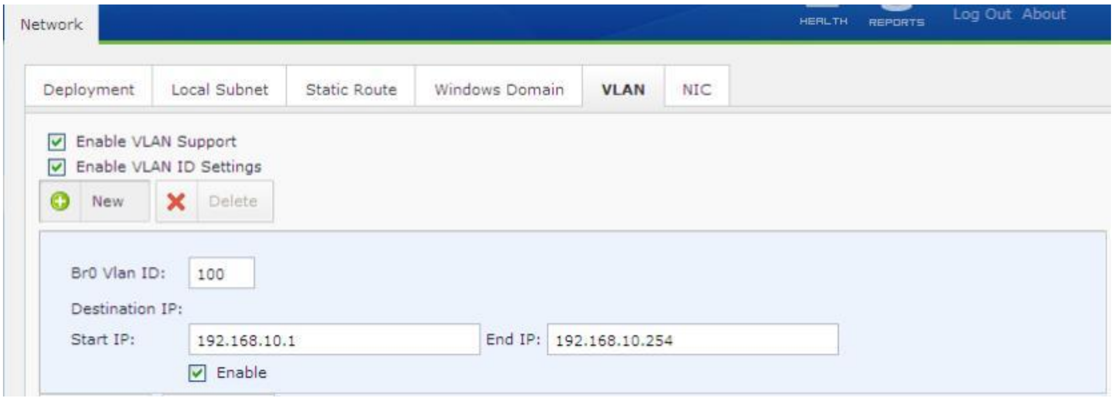
VPN Settings: If either LAN interface netmask and DMZ interface netmask is selected and configured, the local WOC will only inform the peer VPN device of its subnet mask (of LAN or DMZ interface).

VPN Interface: Select the Default option if you want to use the default IP address and subnet mask; or select Specified and specify an idle IP address if the default IP address conflicts with any working machine.

VPN interface is a virtual port; in reality, no such physical port exists.

VLAN Setting

VLAN tab is visible only when the Sangfor WAN Optimization Controller (WOC) is deployed in Bridge mode.



☑ Enable VLAN Support
☑ Enable VLAN ID Settings

Br0 Vlan ID: 100
Destination IP:
Start IP: 192.168.10.1 End IP: 192.168.10.254
☑ Enable

The following are the contents included on the VLAN page:

Enable VLAN support: Select this option, and the peer Sangfor WOC can restore the original VLAN ID of the data packet that has been processed by the local WOC previously, and thus ensures the peer device to distinguish the data packet (which VLAN it belongs to).

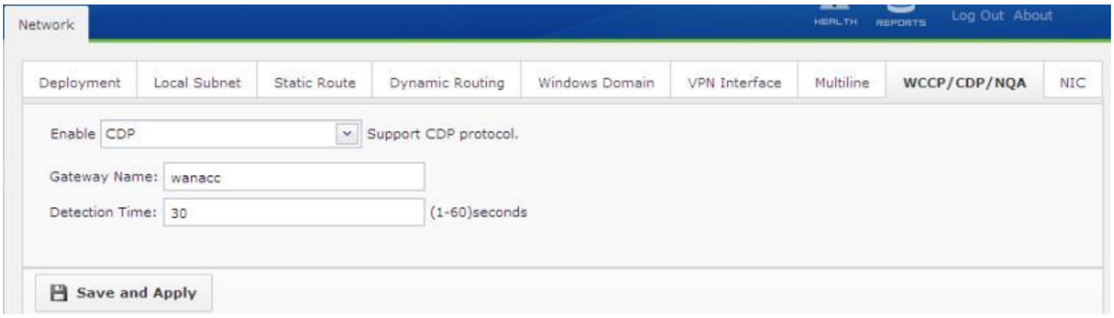
When the LAN interface of the local WOC receives a request data packet from the peer device, the local device removes the VLAN ID of the packet and sends the processed packet (accelerated) back to the peer device through its WAN interface. After that, the peer device receives the returned packet and also handles the packet, and then forwards the processed data to its local area network, at the same time, the peer device restores the original VLAN ID of the data packet according to the records made by the local device.

Enable VLAN ID Settings: Select this option to apply the VLAN ID settings. It requires the option Enable VLAN Support be selected.

New: Click this button to add a new VLAN ID entry. Enter the VLAN ID and Destination IP (single IP address or IP range), so that the data packet destined to this IP address labeled with the ID after being handled by the WOC.

CDP Settings

C0DP setting is only available when service mode is Accelerator Only and deployment mode is Single arm, as shown below:



Enable CDP Support CDP protocol.

Gateway Name: wanacc

Detection Time: 30 (1-60)seconds

Enter the gateway name and detection time.

The purpose of checking the Support CDP Protocol option is to enable the single-arm WAN Optimization Controller (WOC) (VPN function is not supported) to associate with the CDP-supported frontend device, so as to implement policy-based routing. As the front-end device will be unable to detect the existence of the WAN Optimization Controller (WOC) with CDP when the single-arm WAN Optimization Controller (WOC) is in failure, the frontend device itself will invalidate the policy-based routing and restore the previous data flow direction, so as to avoid impact caused by the failure of the WAN Optimization Controller (WOC).

At present, the only supplier supporting CDP is CISCO.

WCCP Settings

WCCP (Web Cache Communication Protocol) is a communication protocol specifying communication between a router and Cache Engine. The Cache Engine is a specific device (such as the SANGFOR WAN Optimization Controller) for data cache; while the router is in association with the Cache Engine redirecting TCP data flow to the Cache Engine, achieving the purpose of improving data transfer efficiency and shortening TCP process time.

WCCP uses UDP 2048 port to perform data communication, with two versions, WCCP V1 and WCCP V2. Currently, SANGFOR WOC only supports WCCP V2. To enable the WCCP function, the switch or router must support WCCP protocol; otherwise, the WCCP function is disabled.

The following table lists the CISCO device models and hardware versions that support WCCP.

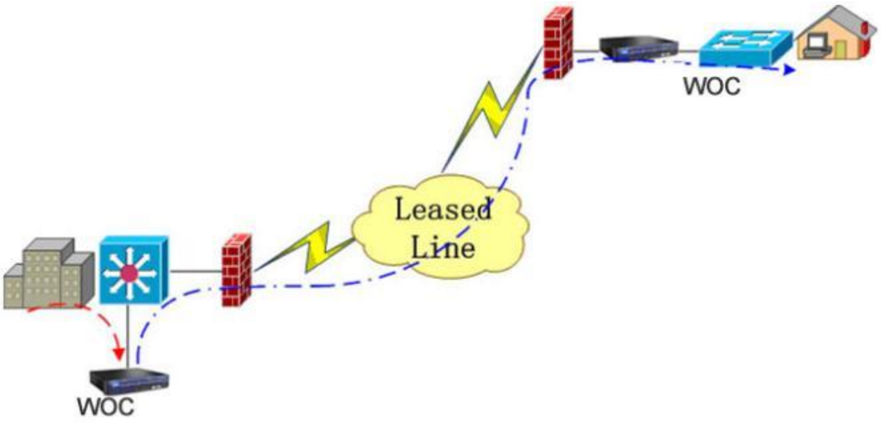
For devices of other venders, please contact your hardware device supplier.

CISCO HARDWARE	CISCO IOS
ISR and 7200 Routers	12.1(14), 12.2(26), 12.3(13), 12.4(10), 12.1(3)T, 12.2(14)T,12.3(14)T5, 12.4(9)T1
Catalyst 6500 with Sup720 or Sup32	12.2(18)SXF12
Catalyst 6500 with Sup2	12.1(27)E, 12.2(18)SXF10
Catalyst 4500	12.2(31)SG
Catalyst 3750	12.2(37)SE

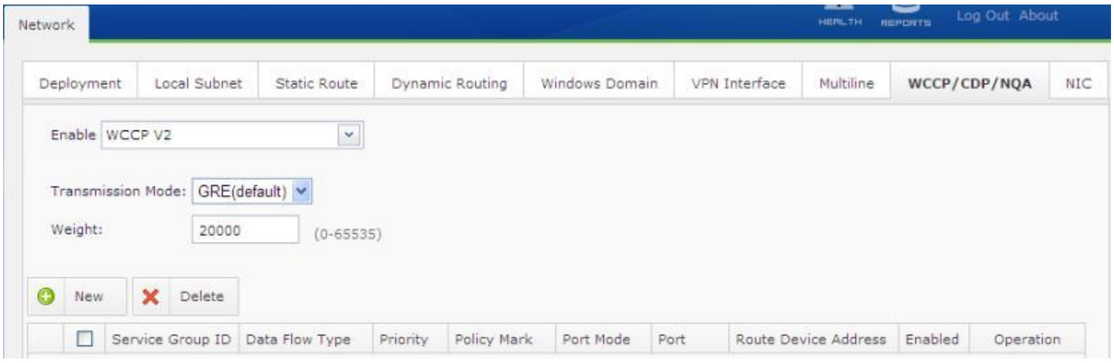
* The information in the above table is only for reference. They are subject to change without notice. Please refer to the CISCO official website.

Enabling WCCP (Web Cache Communication Protocol) can help to restore the network structure in case of network fault. Network structure could be kept unchanged when the routing table on the core switch is modified because of the single arm deployment, ensuring the robustness of the network.

The typical network topology of WCCP deployment is as shown below.



WCCP settings is only available when service mode is Accelerator Only and deployment mode is Single arm. Go to System > Network > WCCP page and the WCCP page is seen, as shown in the figure below:



Enable WCCP V2

Transmission Mode: GRE(default)

Weight: 20000 (0-65535)

□	Service Group ID	Data Flow Type	Priority	Policy Mark	Port Mode	Port	Route Device Address	Enabled	Operation

The following are the contents contained on the WCCP page:

Enable WCCP v2: Click it to enable WCCP.

Transmission Mode: Transmission mode specifies the data encapsulation method when the Sangfor WOC and the router are communicating. Options are GRE and Layer 2.

GRE can work in layer-3 network, while Layer 2 can only communicate in layer 2 environment. Selection of transmission mode is subject to the actual topology, and the transmission method of the switch or router supported.

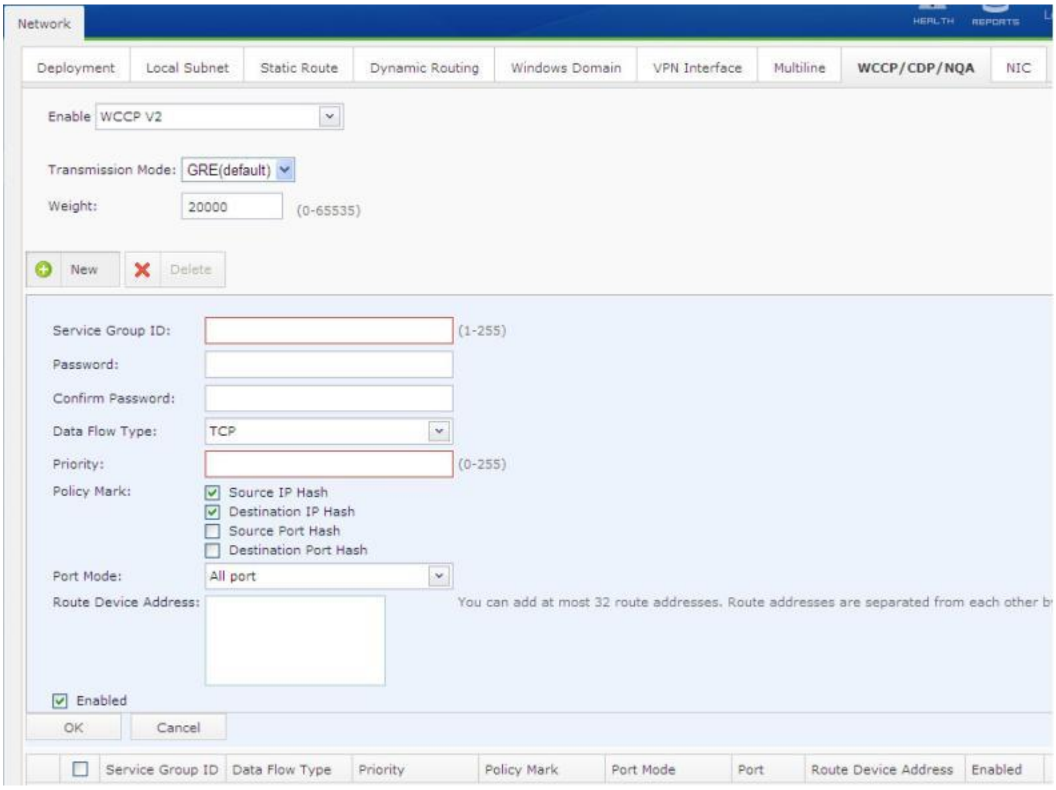
The following table contains the transmission modes supported by CISCO devices respectively. For devices of other venders, please contact your hardware device supplier:

CISCO HARDWARE	Redirection and Return Method
ISR and 7200 Routers	GRE
Catalyst 6500 with Sup720 or Sup32	GRE or L2
Catalyst 6500 with Sup2	GRE or L2
Catalyst 4500	L2
Catalyst 3750	L2

* The information in the above table is only for reference. They are subject to change without notice. Please refer to the CISCO official website.

Weight: When there are several local Sangfor WOCs deployed in your network, this parameter helps to allocate weight for these devices with TCP traffic, according to certain ratio. For example, if the weight of device A is 100 and the weight of device B is 200, device A is responsible for about 33.3% [100/(100+200)] percent of the total traffic while device B is responsible for about 66.6%[200/(100+200)] percent of the total traffic. When there is only one Sangfor WOC, you can set the weight to any value.

New: Click this button to add a new router or switch IP address to enable WCCP protocol; you can also add more than one IP addresses.



Enable: WCCP V2

Transmission Mode: GRE(default)

Weight: 20000 (0-65535)

Service Group ID: (1-255)

Password:

Confirm Password:

Data Flow Type: TCP

Priority: (0-255)

Policy Mark: ☑ Source IP Hash ☑ Destination IP Hash ☐ Source Port Hash ☐ Destination Port Hash

Port Mode: All port

Route Device Address: You can add at most 32 route addresses. Route addresses are separated from each other b

☑ Enabled

☐	Service Group ID	Data Flow Type	Priority	Policy Mark	Port Mode	Port	Route Device Address	Enabled

Service Group ID: Configures WCCP service group to which the Sangfor WOC and router/switch belongs. This service group IP must be the same as that configured on the router/switch; otherwise, the WCCP protocol cannot be used.

Password, Confirm Password: Configures the password for WCCP interaction. If the password is incorrect, relevant information of WCCP protocol will not be interacted properly. DO keep the password the same as that set on the router/switch.

Data Flow Type: TCP and ICMI options are available. It defines the types of data that the router/switch redirects to the Sangfor WOC. If no type of data traffic is selected, system will redirect the types of data according to the routing table of the router/switch. TCP data is recommended for general cases, while ICMP is mainly used for checking the validity of WCCP function with ping/tracert command.

Priority: Priority is required if there are several different service groups. In case that the different service groups have the same redirection policy, select the service group policy with higher priority to redirect the data. If there is only one service group, the priority can be set to any value.

Policy Mark: Enable Hash policy when there are several Sangfor WOCs, assigning data redirection by different policies. With this approach, it can avoid the situation that multiple connections originated from a same IP address to a same server are redirected to a different WOC. Hash policies can be created by defining and combining the Source IP, Destination IP, Source port, or Destination port. If there is only one Sangfor WOC, you can ignore this option.

Port Mode: All port mode and Application mode are available. WCCP can define the ports to redirect data. Select All port mode and all the data at TCP 1-65535 will be redirected to the WOC; select Application port mode, and only the data at the allocated 8 TCP ports are to be redirected. In this mode, ports are separated from each other by comma (,).

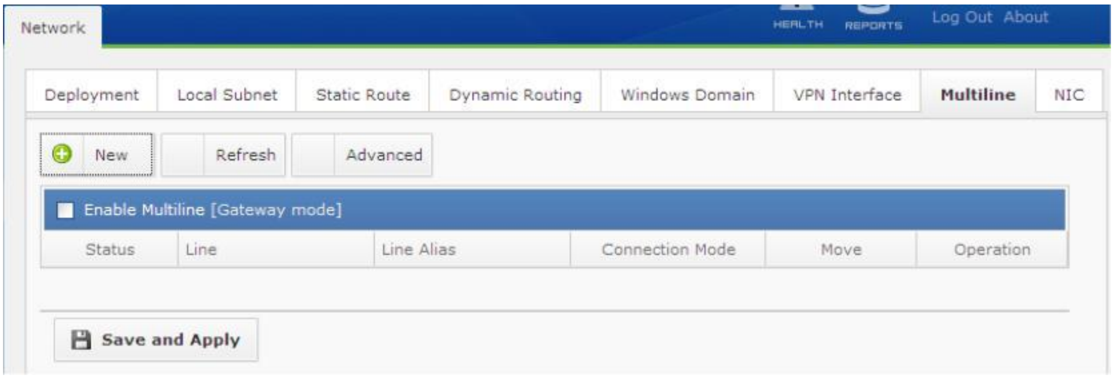
Route Device Address: Indicates the IP address of router/switch interacting with WCCP. This route device address should be the same as the route device address configured in System > Network > Deployment.

Select the check box next to Enabled, and then click the OK button to save the settings.

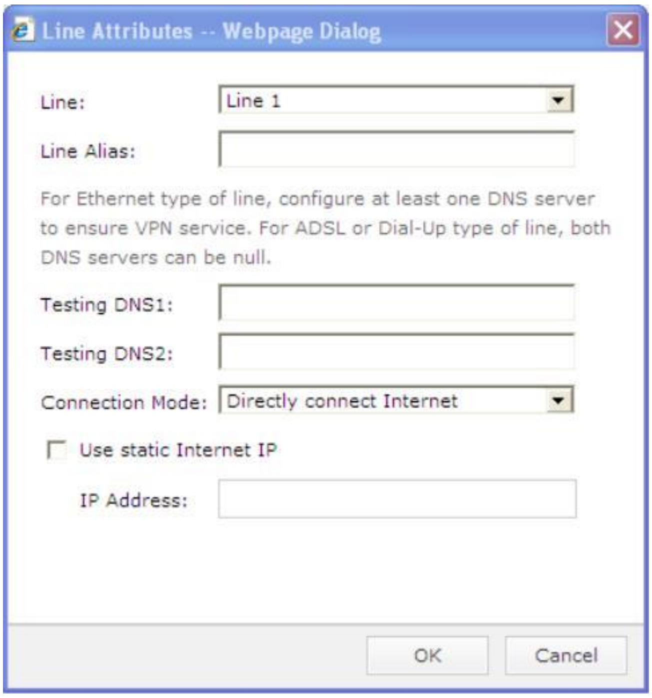
What should be noted is that, WCCP and CDP will not be available at the same time.

Configuring Multiline

If Sangfor WAN Optimization Controller (WOC) is deployed in Gateway mode and connects to multiple WAN links, or the WOC is deployed in Single-arm mode with multiline function being enabled, you need to add the lines on the Multiline page and configure the line selection policy, as shown in the figure below:



1. Select the Enable Multiline option.
2. Click New to enter the Line Attributes dialog and configure the Internet line, as shown below:



Line: Line 1

Line Alias:

For Ethernet type of line, configure at least one DNS server to ensure VPN service. For ADSL or Dial-Up type of line, both DNS servers can be null.

Testing DNS1:

Testing DNS2:

Connection Mode: Directly connect Internet

□ Use static Internet IP

IP Address:

3. Configure attributes of the Internet line. The following are the attributes:

   Line: Select a line and configure the connection mode of the line.

   Line Alias: Enter a name for this Internet line.

   Testing DNS1, Testing DNS2: Configures the preferred and alternate DNS servers respectively. They are required and should be public IP addresses if line type is Ethernet.

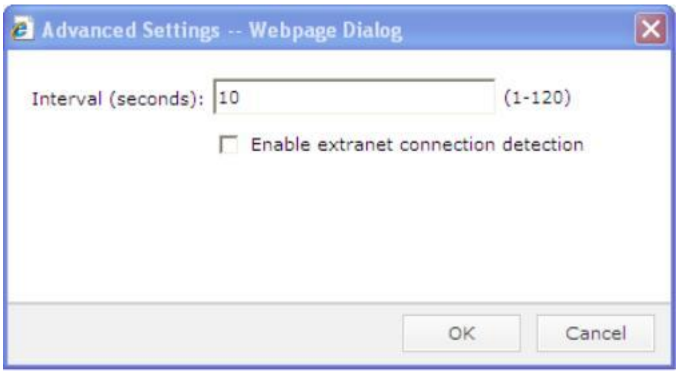
Otherwise, leave them empty.

Connection Mode: Specify whether the line is directly connected to the Internet.

Use static Internet IP: Enter the IP address according to your case. If it is using dynamic IP address, unselect this option.

IP Address: If Use static Internet IP is selected, this field is required. Enter the IP address you want to assign to the WAN interface corresponding to this Internet line.

4. Click the Advanced button to configure the advanced settings, as shown below:



Advanced Settings -- Webpage Dialog

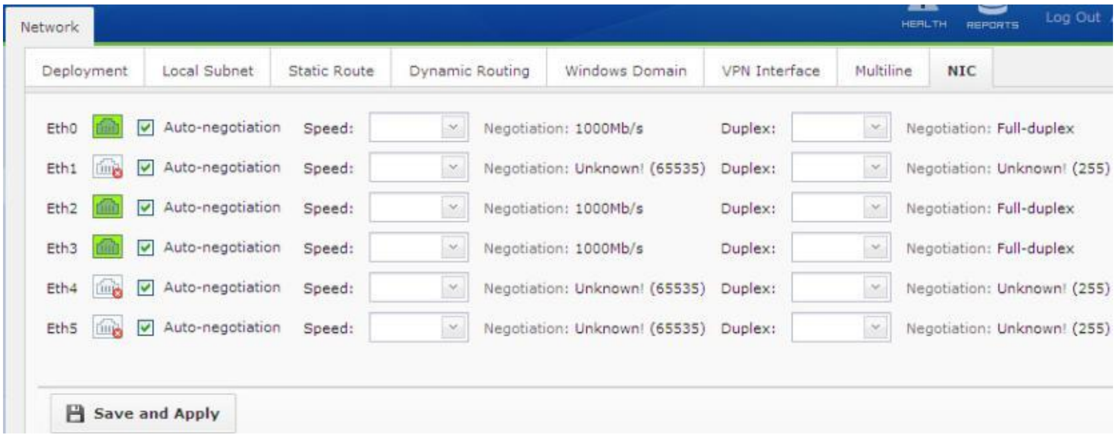
Interval (seconds): 10 (1-120)

□ Enable extranet connection detection

Enabled extranet connection detection: Select this option and enter the Interval in seconds if the network is connected to multiple Internet lines and you want line status to be detected regularly. Not recommended if the Internet lines are activated and in good status.

Network Interface Card (NIC)

For each network interface card on the Sangfor WAN Optimization Controller (WOC), transfer rate and mode are configurable, as shown in the figure below:



Eth0	☑ Auto-negotiation	Speed:		Negotiation: 1000Mb/s	Duplex:		Negotiation: Full-duplex
Eth1	☑ Auto-negotiation	Speed:		Negotiation: Unknown! (65535)	Duplex:		Negotiation: Unknown! (255)
Eth2	☑ Auto-negotiation	Speed:		Negotiation: 1000Mb/s	Duplex:		Negotiation: Full-duplex
Eth3	☑ Auto-negotiation	Speed:		Negotiation: 1000Mb/s	Duplex:		Negotiation: Full-duplex
Eth4	☑ Auto-negotiation	Speed:		Negotiation: Unknown! (65535)	Duplex:		Negotiation: Unknown! (255)
Eth5	☑ Auto-negotiation	Speed:		Negotiation: Unknown! (65535)	Duplex:		Negotiation: Unknown! (255)

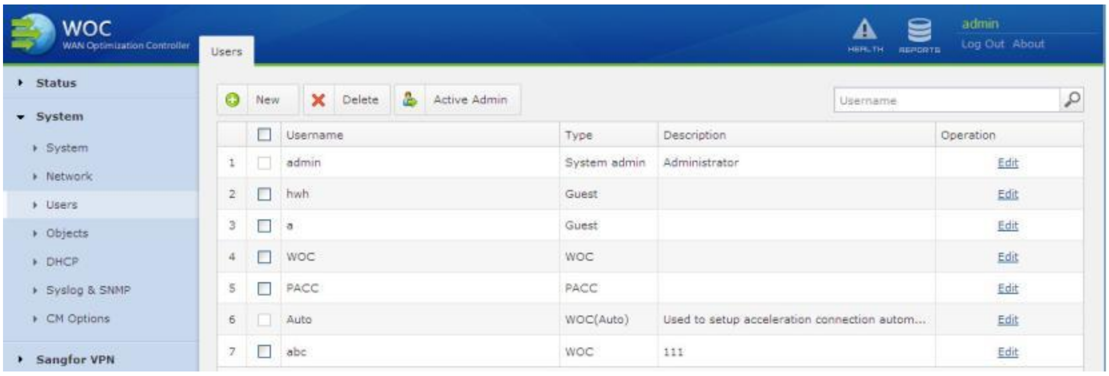
We recommend you select Auto-negotiation for general cases.

If the network interface card of WOC is incompatible with that of interface on other network devices, deselect Auto-negotiation and set the transfer rate and mode.

Users

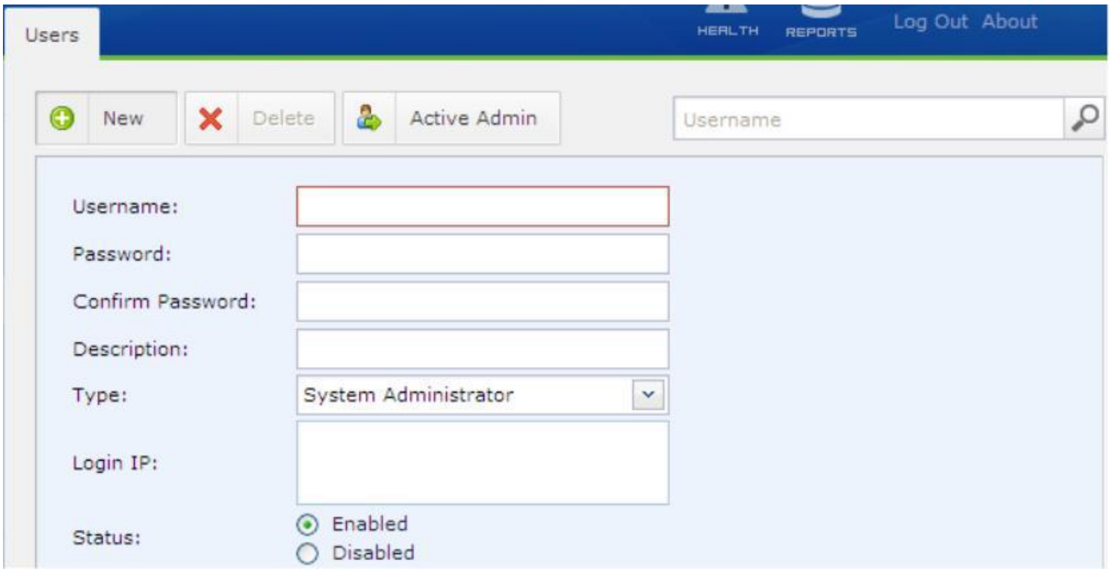
The users on Sangfor WAN Optimization Controller (WOC) indicate either the administrator accounts that are used to log in to the WOC Web administrator console or the user accounts that are used by the client-end WOC to establish acceleration connections with the local WOC.

Go to System > Users to enter the Users page, as shown in the figure below:



	□	Username	Type	Description	Operation
1	□	admin	System admin	Administrator	Edit
2	□	hwh	Guest		Edit
3	□	a	Guest		Edit
4	□	WOC	WOC		Edit
5	□	PACC	PACC		Edit
6	□	Auto	WOC(Auto)	Used to setup acceleration connection autom...	Edit
7	□	abc	WOC	111	Edit

To add a new user account, click the New button, and the attributes appear, as shown below:



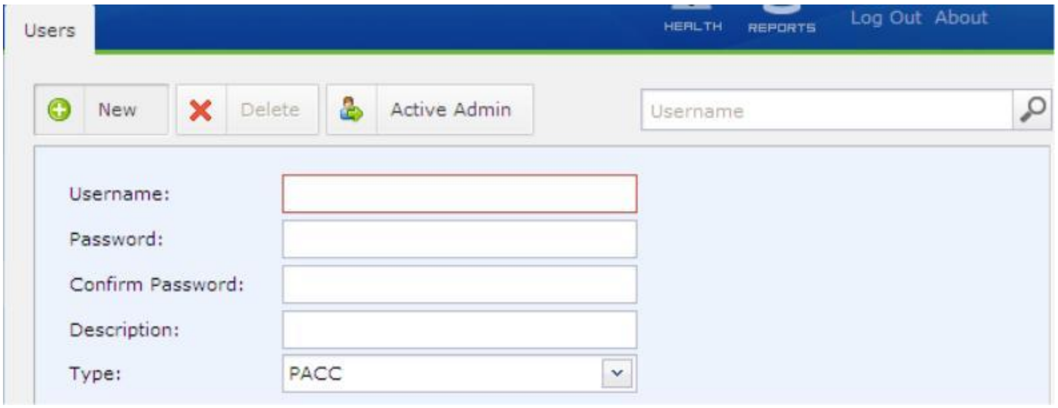
Username:	
Password:	
Confirm Password:	
Description:	
Type:	System Administrator
Login IP:	
Status:	● Enabled ○ Disabled

Username: Enter a name for this user. This field is required.

Password: Enter the password of this user account.

Type: Specifies the type of the account. Type falls into WOC, PACC, System Administrator and Guest. The former two options are client types of acceleration users that can be referenced by acceleration policy group while the latter two options are the roles of administrator account, indicating varying privileges of administrators (such as edit, view and so on).

WOC type of user account is intended to establish acceleration connection between two networks that are deployed with Sangfor WAN Optimization Controllers (hardware). PACC type of user account is intended to set up acceleration connection between Sangfor WAN Optimization Controller (hardware) and mobile user whose PC is installed Sangfor Portable Acceleration (PACC) client software. The attributes are as shown in the figure below:



Username:

Password:

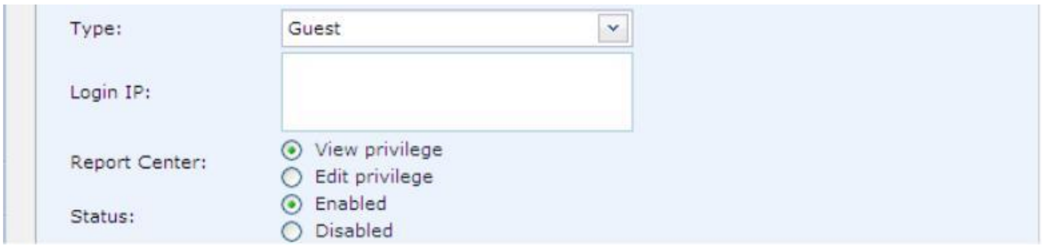
Confirm Password:

Description:

Type: PACC

There is a built-in user named Auto, which is used to discover inbound connections from the peer WOC that can be accelerated. This user cannot be deleted nor be edited.

Guest type of administrator account is the account with certain privilege of viewing or editing the settings on the WOC.



Type: Guest

Login IP:

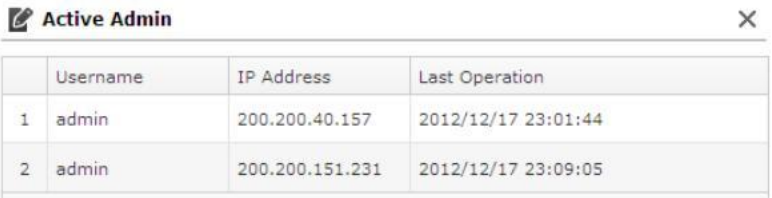
Report Center: ● View privilege ○ Edit privilege

Status: ● Enabled ○ Disabled

The system administrator with View privilege cannot change the settings on the WOC Report Center. Only the administrator with Edit privilege can do so.

The default account admin is an administrator account with Edit privilege, which cannot be deleted and nor its attributes be altered (except password).

Active Admin: Click the button to view the current active administrators that are under the realm of the logging in administrator account, , as shown below:

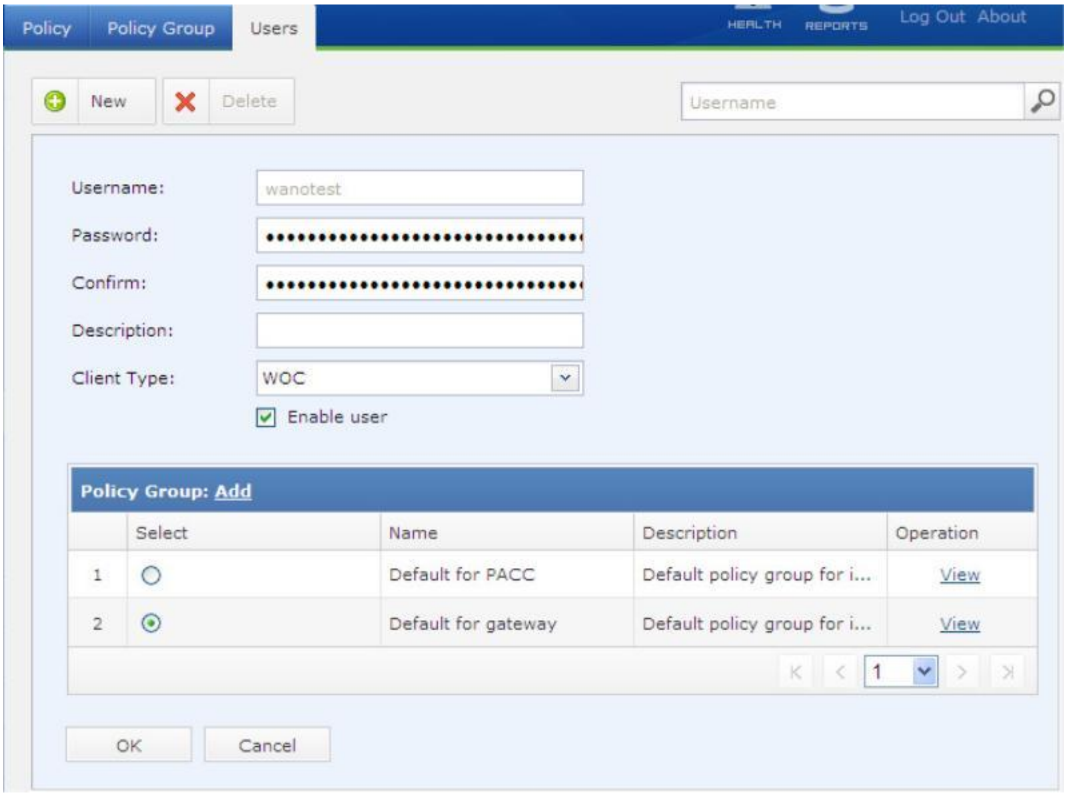


	Username	IP Address	Last Operation
1	admin	200.200.40.157	2012/12/17 23:01:44
2	admin	200.200.151.231	2012/12/17 23:09:05

Creating User

To add a user account for a branch site to establish acceleration connection with the local WOC, perform the steps below:

1. Navigate to System > Users to enter the Users page.
2. Enter the username (for example, wanotest) and password, select type WOC, and click OK to save the settings.
3. Navigate to WAN Optimization > Server > Users page, select the newly-created user account wanotest, and click Edit. Select the option Enable user and click OK.



Username: wanotest

Password: ••••••••••••••••••••••••••••••••

Confirm: ••••••••••••••••••••••••••••••••

Description:

Client Type: WOC

☑ Enable user

Policy Group: Add

	Select	Name	Description	Operation
1	○	Default for PACC	Default policy group for i...	View
2	●	Default for gateway	Default policy group for i...	View

You can also create user account in WAN Optimization > Server > Users, simply by clicking the New button and complete the above basic configuration and selecting the desired policy group (for more information, refer to the section Creating User in Chapter 5).

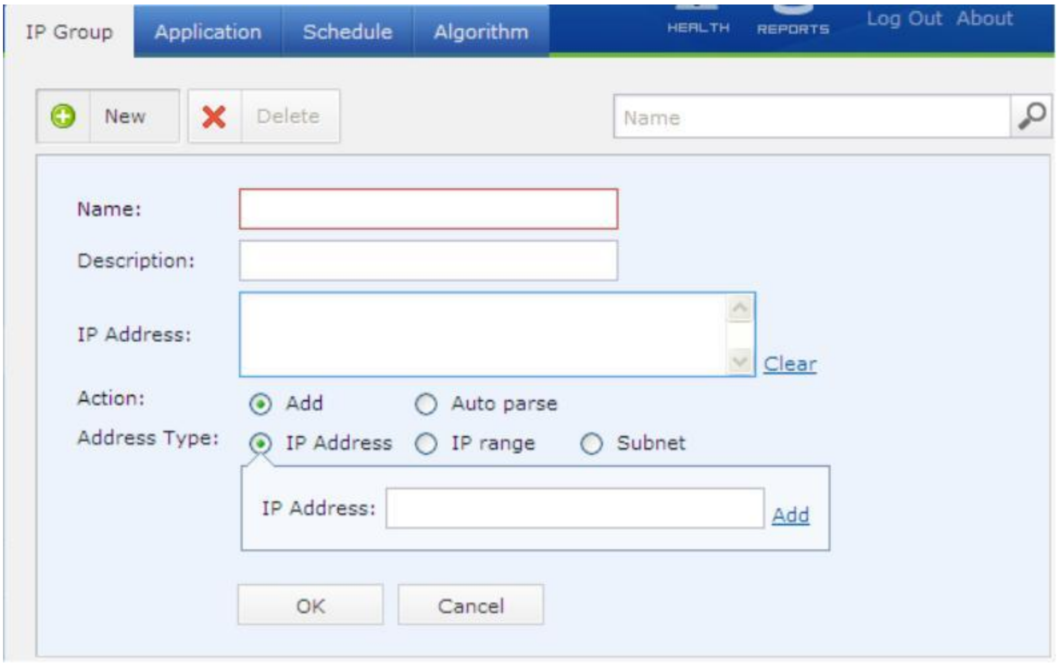
Creating IP Group

An IP group may be composed of single IP address, IP range or subnet. It is predefined object that can be referenced by acceleration policy and firewall rule.

To add a new IP group, perform the following steps:

1. Navigate to System > Objects > IP Group to enter the IP Group page.

2. Click the New button and the attributes appear, as shown in the figure below:



Name:

Description:

IP Address:

Action: ● Add ○ Auto parse

Address Type: ● IP Address ○ IP range ○ Subnet

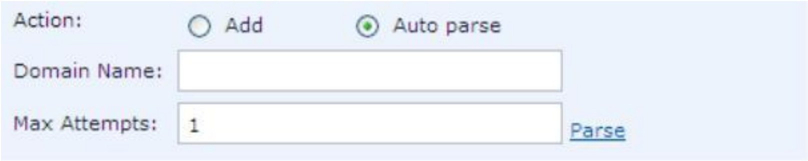
IP Address:

3. Configure attributes of the IP group. The following are the attributes:

Name: Enter a name for this IP group. This field is required.

Description: Enter brief description for this IP group.

IP Address: Enter the IP addresses to be included in this IP group. IP address can either be typed in manually or filled in automatically. Select action Add, address type IP address, IP range or Subnet, enter the address into the IP Address field and click Add. If you only know the domain name, select action Auto parse, and enter the domain name into the Domain Name field and click Parse to have the WOC parse the domain name and fill in the corresponding IP address into the IP Address field. Max Attempts indicates the maximum number of attempts that parsing operation can be executed.



Action: ○ Add ● Auto parse

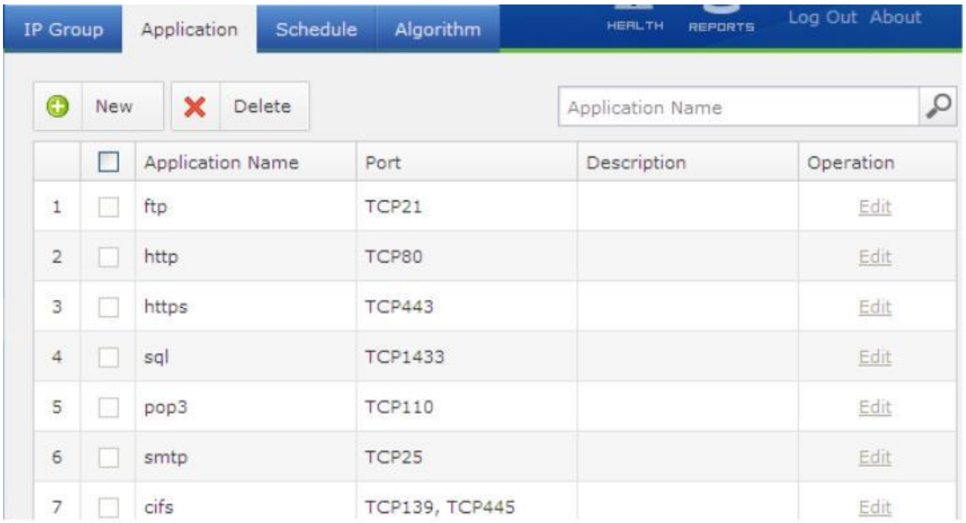
Domain Name:

Max Attempts: 1

4. Click the OK button to save the settings.

Creating Application

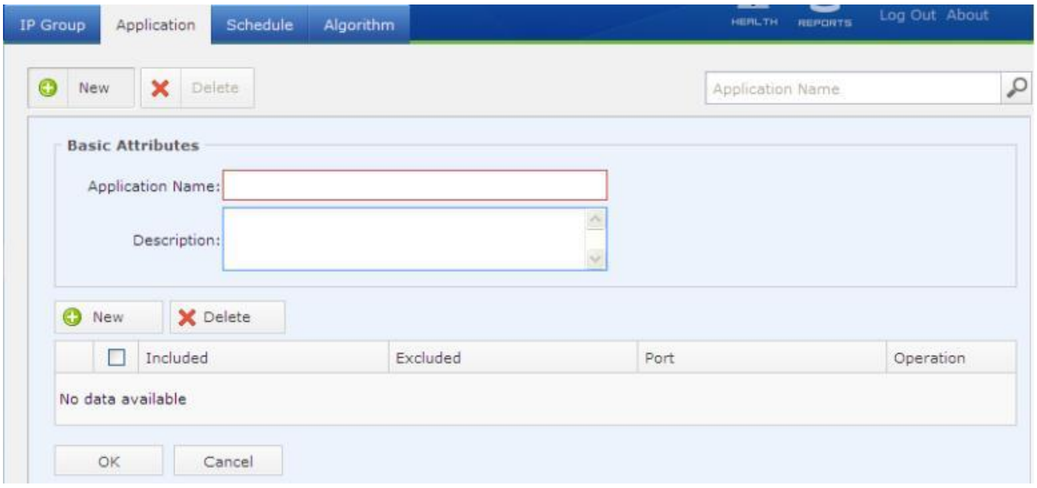
Application will be predefined and referenced by application policy and firewall rule. Some common applications are already built in the system, as shown in the figure below:



	□	Application Name	Port	Description	Operation
1	□	ftp	TCP21		Edit
2	□	http	TCP80		Edit
3	□	https	TCP443		Edit
4	□	sql	TCP1433		Edit
5	□	pop3	TCP110		Edit
6	□	smtp	TCP25		Edit
7	□	cifs	TCP139, TCP445		Edit

To add a new application, perform the steps below:

1. Navigate to System > Objects > Application to enter the Application page.
2. Click the New button and the attributes appear, as shown in the figure below:

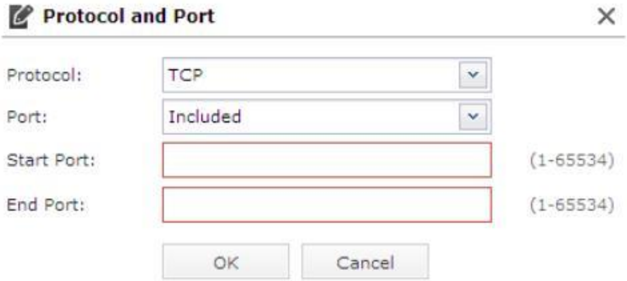


3. Configure attributes of the application. The following are the attributes:

   Name: Enter a name for this application. This field is required.

   Description: Enter brief description for this application.

   Ports: Click the New button to define the protocol and port so that packets with the specified feature will (not) be associated with acceleration policy.



Protocol: TCP

Port: Included

Start Port: (1-65534)

End Port: (1-65534)

Protocol: Select protocol applied by this application.

Port: Specifies the whether the following port range is included or excluded from this application.

Start Port: Specifies the start port of the port range.

End Port: Specifies the end port of the port range.

New: Click this button again to add another port entry.

4. Click OK to save the settings.

Scenario: Accelerating ERPApplication

To accelerate branch users’ access to ERP system at the head office, create the ERP application and associate it with an acceleration policy by performing the following steps:

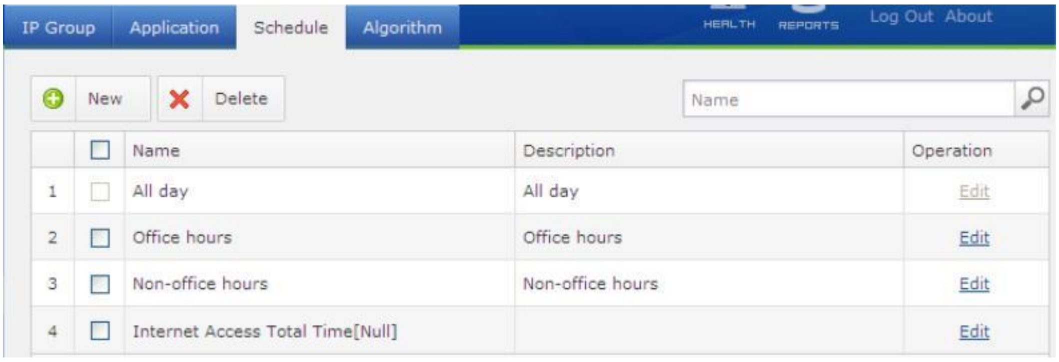
1. Navigate to System > Objects > Application, click the New button.
2. Enter application name ERP and description.
3. Click the New button above the table to specify protocol and port. In this scenario, select protocol TCP, Included port and port 8000 (start port and end port are 8000) for the ERP application.
4. Click the OK buttons.
5. Navigate to WAN Optimization > Server > Policy to create an acceleration policy and associate it with the ERP application created above by selecting ERP application.

Creating Schedule

A schedule is a combination of time segments, which can be referenced by bandwidth control policy. The date and time are based on the system time on the WAN Optimization Controller.

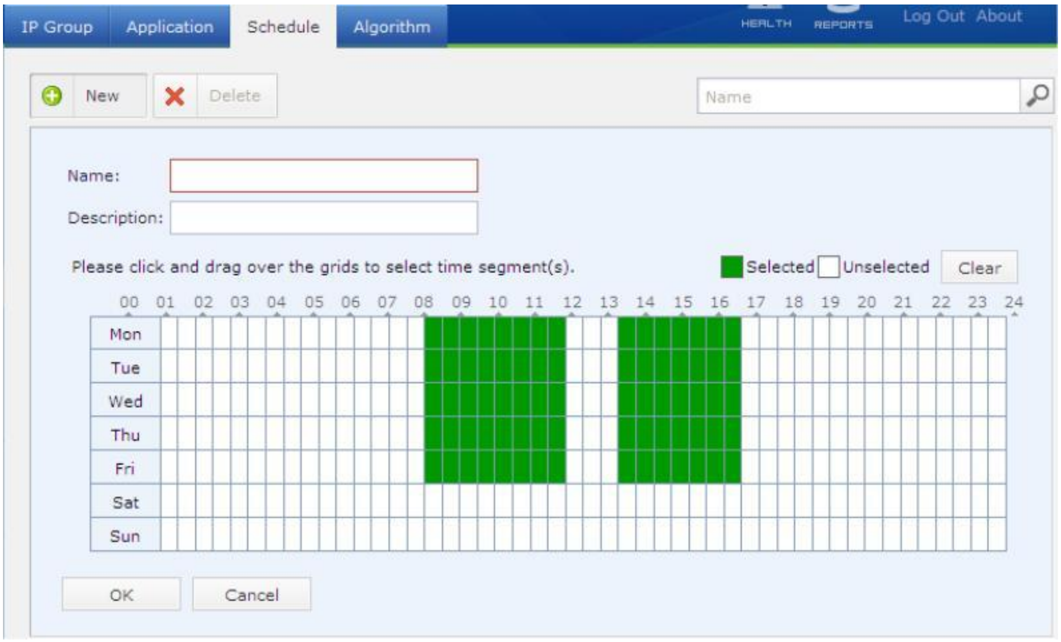
To create a schedule, perform the following steps:

1. Navigate to System > Objects > Schedule, as shown in the figure below:



	☐	Name	Description	Operation
1	☐	All day	All day	Edit
2	☐	Office hours	Office hours	Edit
3	☐	Non-office hours	Non-office hours	Edit
4	☐	Internet Access Total Time[Null]		Edit

2. Click New to add a new schedule. Enter the name into the Name field. Description is optional.
3. Click and drag over the grids to select the desired time segments.



Name:

Description:

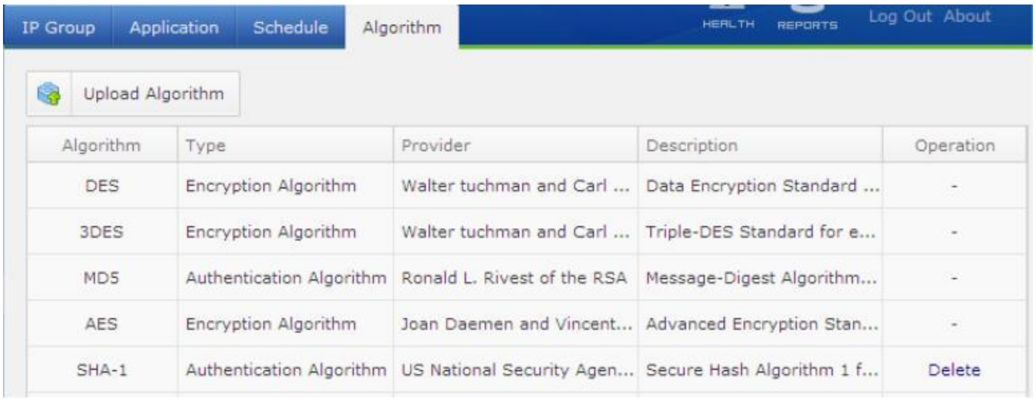
Please click and drag over the grids to select time segment(s).

4. To deselect and remove a time segment from the schedule, click on and drag over the green grids (selected time segments) to select the time segment that you want to deselect. Click Deselect.
5. Click OK to save the settings.

Viewing Algorithms

The Algorithm page displays data encryption algorithms supported by the Sangfor WAN Optimization Controller (WOC). The encryption algorithms listed here will be used to encrypt the data transferred over the VPN network constructed by Sangfor devices to ensure the security of the data transmission. You can upload other algorithms through this page.

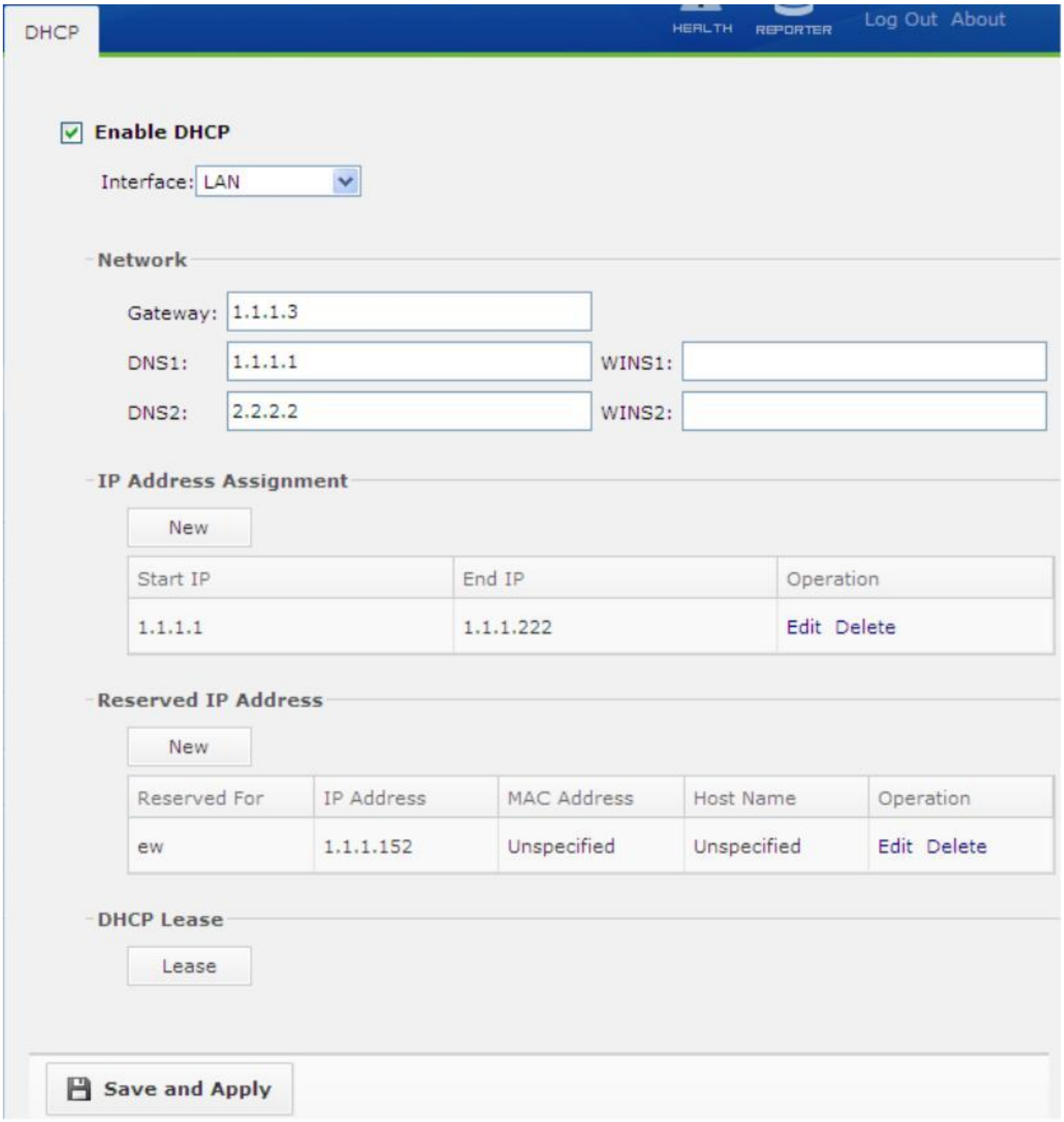
Navigate to System > Objects > Algorithm to enter the Algorithm page, as shown below:



Algorithm	Type	Provider	Description	Operation
DES	Encryption Algorithm	Walter tuchman and Carl ...	Data Encryption Standard ...	-
3DES	Encryption Algorithm	Walter tuchman and Carl ...	Triple-DES Standard for e...	-
MD5	Authentication Algorithm	Ronald L. Rivest of the RSA	Message-Digest Algorithm...	-
AES	Encryption Algorithm	Joan Daemen and Vincent...	Advanced Encryption Stan...	-
SHA-1	Authentication Algorithm	US National Security Agen...	Secure Hash Algorithm 1 f...	Delete

Configuring IP Assignment Options (DHCP)

Navigate to System > DHCP to complete the DHCP related configuration, as shown below:



☑ Enable DHCP

Interface: LAN

Network

Gateway: 1.1.1.3

DNS1: 1.1.1.1 WINS1:

DNS2: 2.2.2.2 WINS2:

IP Address Assignment

New

Start IP	End IP	Operation
1.1.1.1	1.1.1.222	Edit Delete

Reserved IP Address

New

Reserved For	IP Address	MAC Address	Host Name	Operation
ew	1.1.1.152	Unspecified	Unspecified	Edit Delete

DHCP Lease

Lease

The following are the contents included on DHCP page:

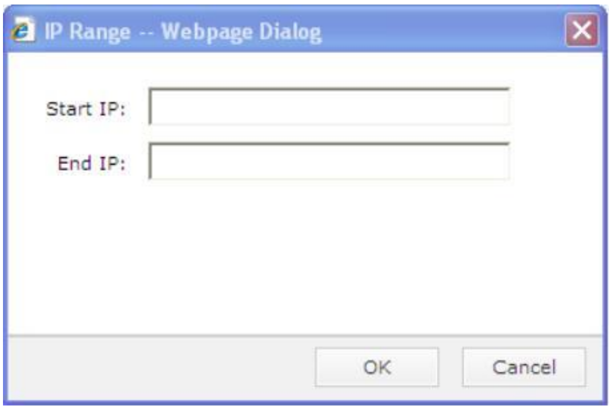
Enable DHCP: Select this option to enable the DHCP service.

Interface: Select the interface through which the IP address are assigned, LAN interface or DMZ interface.

Gateway: Enter the IP address of the interface you have selected above, LAN interface or DMZ interface.

DNS1, DNS2: Enter IP address of the preferred and alternate DNS servers provided by the local Internet Service Provider (ISP).

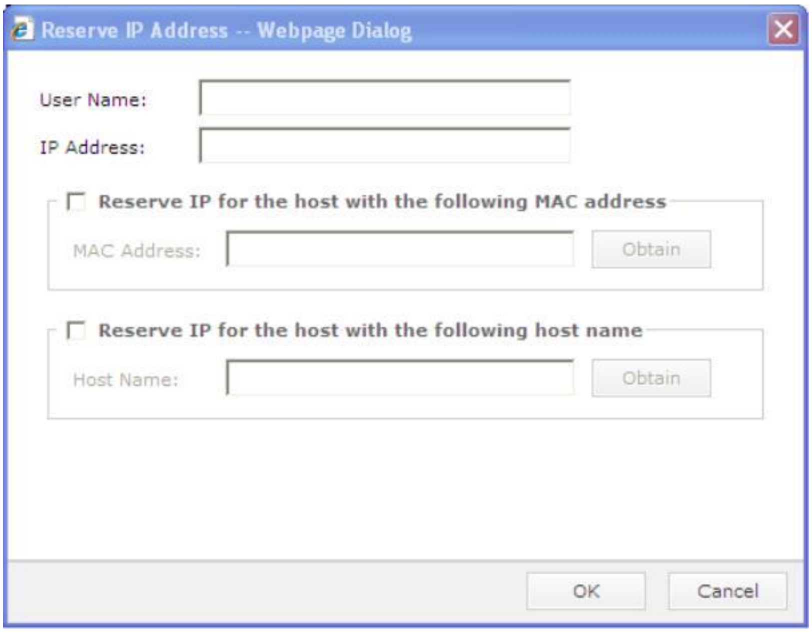
IP Address Assignment: Configure the IP address range that can be assigned through the selected interface. To add a new IP range, click New to enter the IP range page and specify the start IP and end IP, as shown in the following figure.



The IP address should not conflict with IP address occupied by any runing machine, including LAN and DMZ interface IP.

The the IP range should not contain the IP addresses ended with 0 or 255, for thery are ntwork port and broadcase IP.

Reserved IP Address: Addresses in this table are assigned to specific hosts and will not be automatically assigned to any other hosts. To reserve IP address for a host, click New to enter the Reserve IPAddress page, as shown below:


Reserve IP Address -- Webpage Dialog
User Name:
IP Address:
□ Reserve IP for the host with the following MAC address
MAC Address:
Obtain
□ Reserve IP for the host with the following host name
Host Name:
Obtain
OK
Cancel

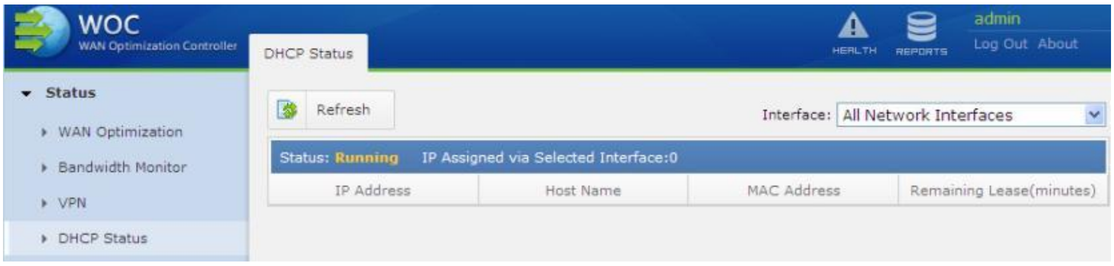
User Name: Specifies the username that you want to assign this IP address to.

IPAddress: Enter the IP address that will be assigned to the specified user or host.

Obtain: If Reserve IP for the host with the following MAC address or Reserve IP for the host with the following host name is selected, click the corresponding Obtain button to get the MAC address or host name of the host for which this IP address is reserved.

Lease: Indicates the DHCP IP address lease, the life cycle that an assigned IP address will be used by the corresponding user.

To view DHCP status, navigate to Status > DHCP Status, as shown in the figure below:



Interface: All Network Interfaces

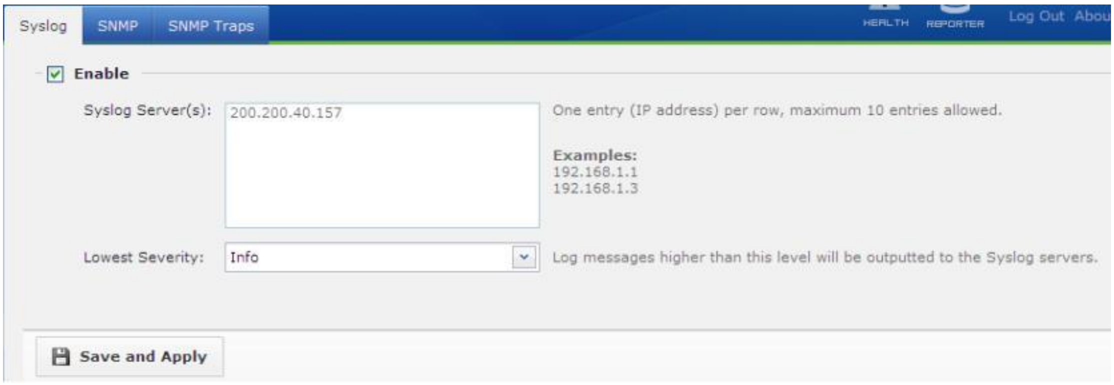
Status: Running IP Assigned via Selected Interface:0

IP Address	Host Name	MAC Address	Remaining Lease(minutes)

Configuring Syslog Server

By configuring an external Syslog server, you can export the logs generated on the Sangfor WOC to the Syslog server.

Navigate to System > Syslog & SNMP to enter the Syslog page appears, as shown below:



☑ Enable

Syslog Server(s): 200.200.40.157

One entry (IP address) per row, maximum 10 entries allowed.

Examples:
192.168.1.1
192.168.1.3

Lowest Severity: Info

Log messages higher than this level will be outputted to the Syslog servers.

The following are the contents included on the Syslog page:

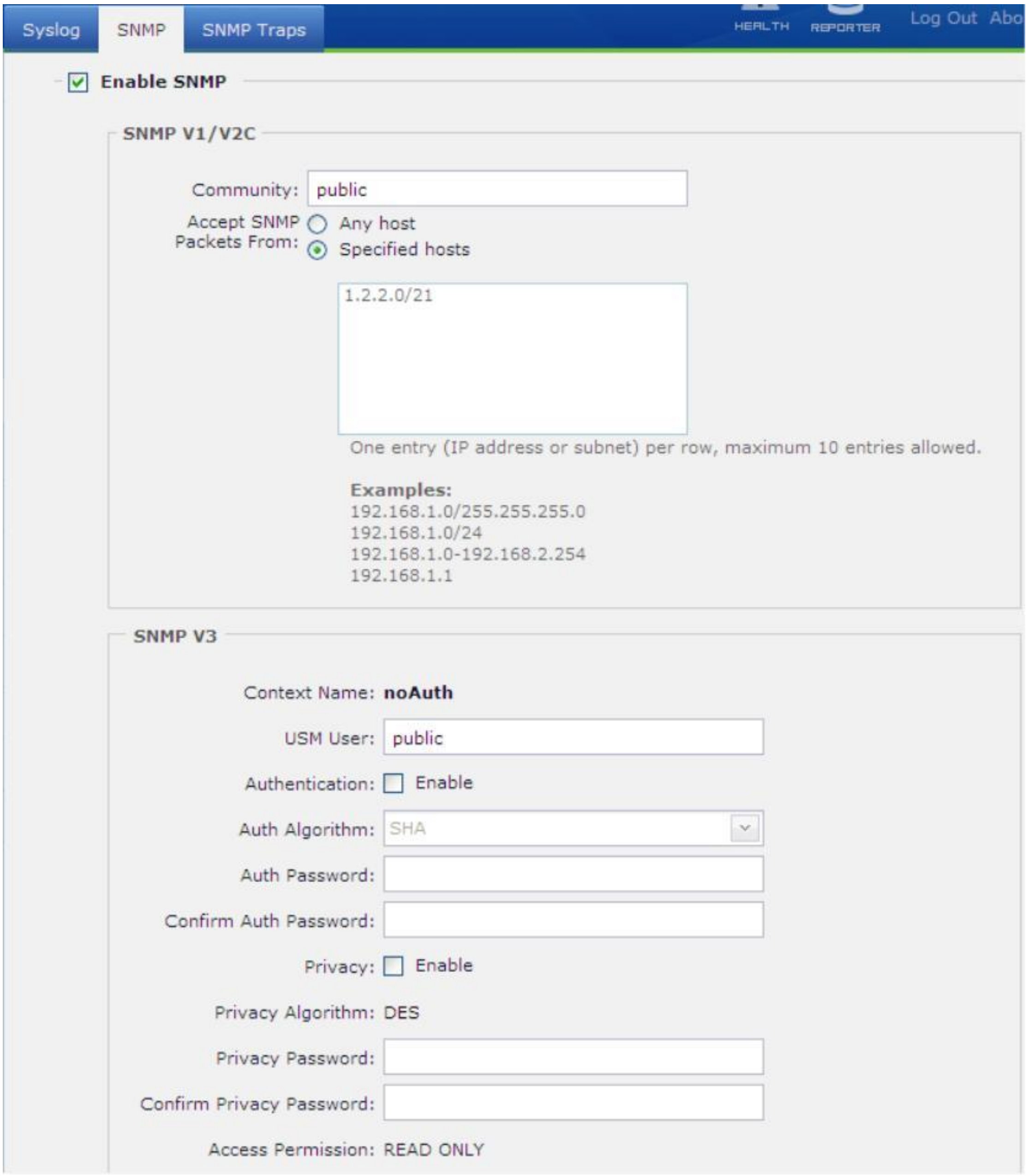
Enable: Select this option to enable the specified Syslog server.

Syslog Server(s): Enter the IP address of Syslog server. Maximum 10 server IP addresses support.

Lowest Severity: Select an option from the pull-down list and select a severity level so that log messages higher that this severity level will be exported to the specified Syslog server.

Configuring SNMP Server

Navigate to System > Syslog & SNMP > SNMP to enter the SNMP page.



☑ Enable SNMP

SNMP V1/V2C

Community: public

Accept SNMP Packets From: ○ Any host ● Specified hosts

1.2.2.0/21

One entry (IP address or subnet) per row, maximum 10 entries allowed.

Examples:
192.168.1.0/255.255.255.0
192.168.1.0/24
192.168.1.0-192.168.2.254
192.168.1.1

SNMP V3

Context Name: **noAuth**

USM User: public

Authentication: □ Enable

Auth Algorithm: SHA

Auth Password:

Confirm Auth Password:

Privacy: □ Enable

Privacy Algorithm: DES

Privacy Password:

Confirm Privacy Password:

Access Permission: READ ONLY

The following are the contents included on SNMP page:

Enable SNMP: Select this option to enable the SNMP service.

Community: Enter the community name of SNMPv1 and SNMPv2.

Accept SNMP Packets From: Specifies the hosts from which the SNMP packets will be accepted by this WOC. Options are Any host and Specified hosts.

USM User: Specifies the USM user of SNMPv3.

Authentication: Select this option to enable identity identification and configure the authentication algorithm and password. Whether the authentications related fields need to be configured is up to the SNMP settings on the SNMPv3 server.

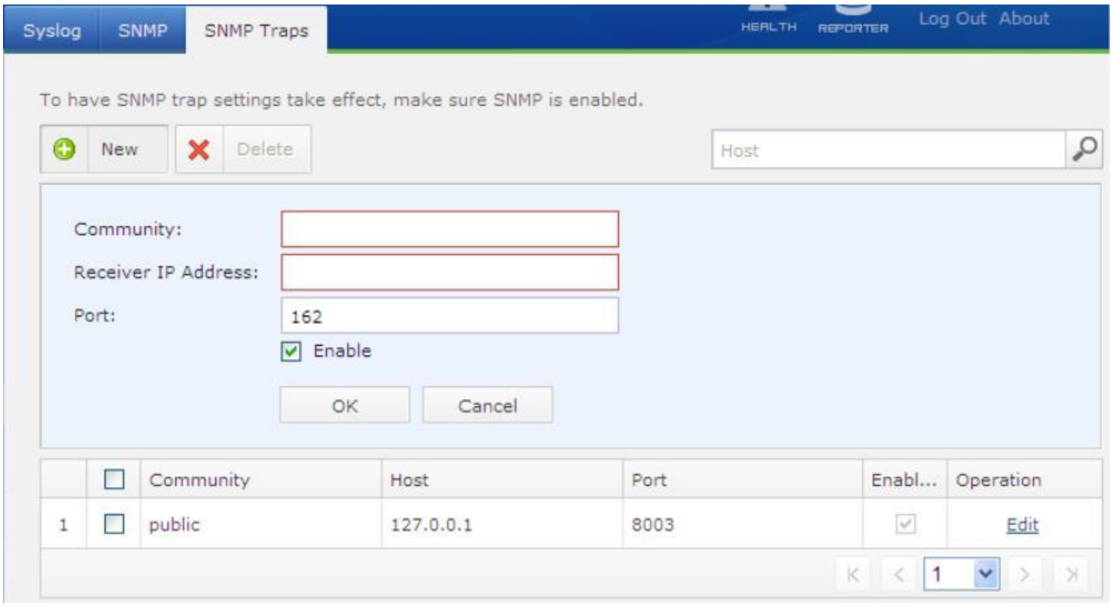
Privacy: Select his option to enable encryption settings and configure the privacy algorithm and password. Same with authentication, whether the privacy related fields need to be configured is up to the SNMP settings on the SNMPv3 server.

Download MIB: Click this button to download the Management Information Base (MIB) on the WOC. The extension of the downloaded file should be .tar. Before importing to third-party SNMP software, you need to decompress it.

Adding SNMP Traps

SNMP traps helps to report the anomaly of the WOC to the SNMP server proactively.

To add a SNMP trap, navigate to System > Syslog & SNMP > SNMP Traps, click the New button and configure the attributes of the SNMP trap, as shown below:



To have SNMP trap settings take effect, make sure SNMP is enabled.

Community:	
Receiver IP Address:	
Port:	162
	☑ Enable

OK Cancel

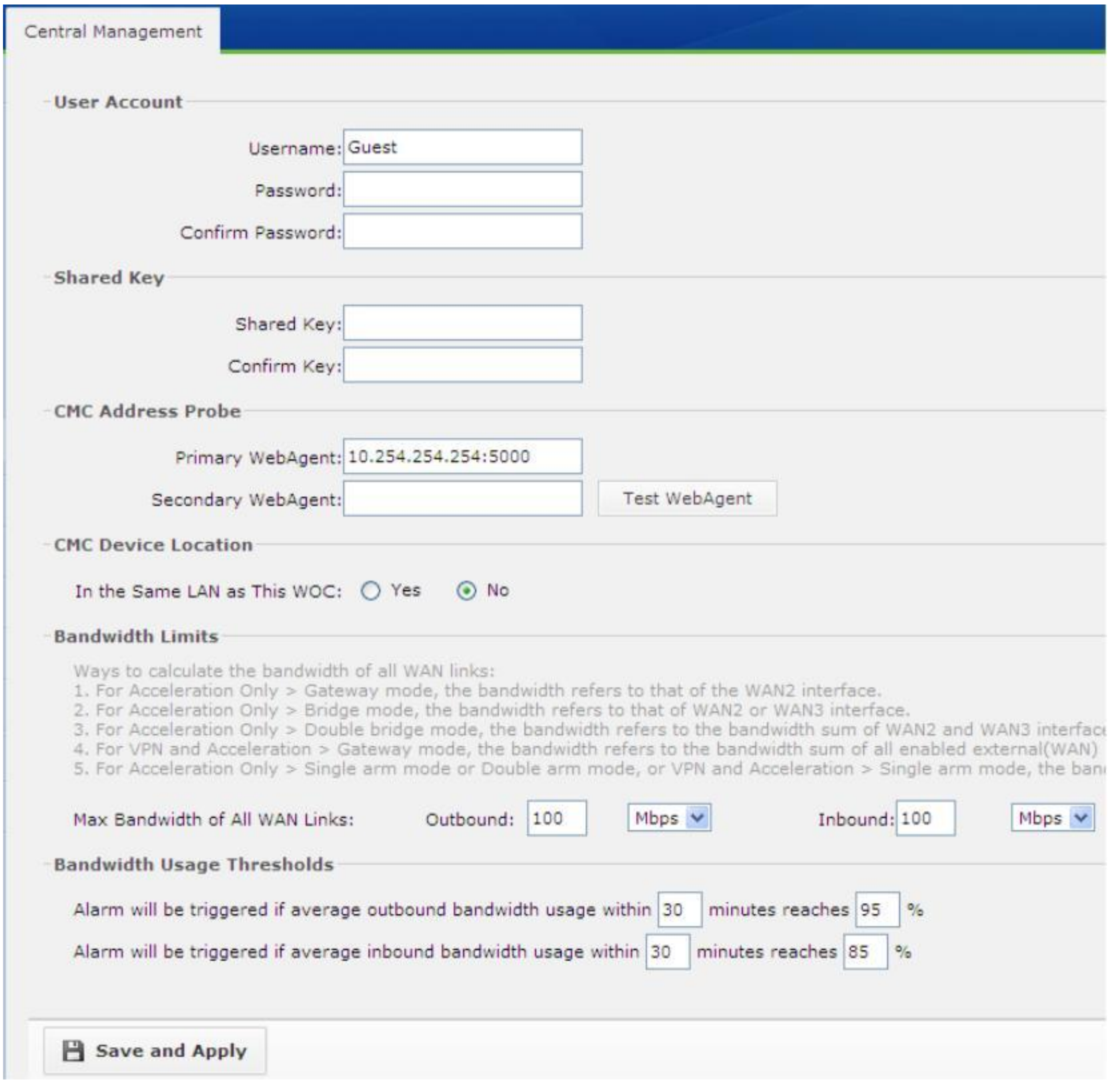
	□	Community	Host	Port	Enabl...	Operation
1	□	public	127.0.0.1	8003	✓	Edit

To have SNMP traps work, ensure SNMP is enabled on SNMP page.

Central Management

Sangfor WAN Optimization Controllers (WOC) scattered over WAN can be managed centralizedly by one Sangfor CMC (Center Management Console) device once they joined central management.

Navigate to System > CM Options to enter the Central Management page, as shown below:



Central Management

User Account

Username: Guest

Password:

Confirm Password:

Shared Key

Shared Key:

Confirm Key:

CMC Address Probe

Primary WebAgent: 10.254.254.254:5000

Secondary WebAgent:

CMC Device Location

In the Same LAN as This WOC: ○ Yes ● No

Bandwidth Limits

Ways to calculate the bandwidth of all WAN links:
1. For Acceleration Only > Gateway mode, the bandwidth refers to that of the WAN2 interface.
2. For Acceleration Only > Bridge mode, the bandwidth refers to that of WAN2 or WAN3 interface.
3. For Acceleration Only > Double bridge mode, the bandwidth refers to the bandwidth sum of WAN2 and WAN3 interfac
4. For VPN and Acceleration > Gateway mode, the bandwidth refers to the bandwidth sum of all enabled external(WAN)
5. For Acceleration Only > Single arm mode or Double arm mode, or VPN and Acceleration > Single arm mode, the ban

Max Bandwidth of All WAN Links: Outbound: 100 Mbps Inbound: 100 Mbps

Bandwidth Usage Thresholds

Alarm will be triggered if average outbound bandwidth usage within 30 minutes reaches 95 %

Alarm will be triggered if average inbound bandwidth usage within 30 minutes reaches 85 %

The following are the contents included on Central Management page:

User Account: Enter the username and password for connecting to the CMC. The name and password should be the site name and password corresponding to the site created on the CMC.

Shared Key, Confirm Key: Enter and confirm the shared key used for encrypting data transferred between the site and CMC device. The key should be the same as that configured for the corresponding site on the CMC. Ignore it if no shared key is specified.

CMC Address Probe: Enter the physical IP address or domain name (if available) of the CMC into the Primary WebAgent field (in format of IP:Port or URL). The WebAgent will be used by the site to obtain information of the network in which the CMC device resides.

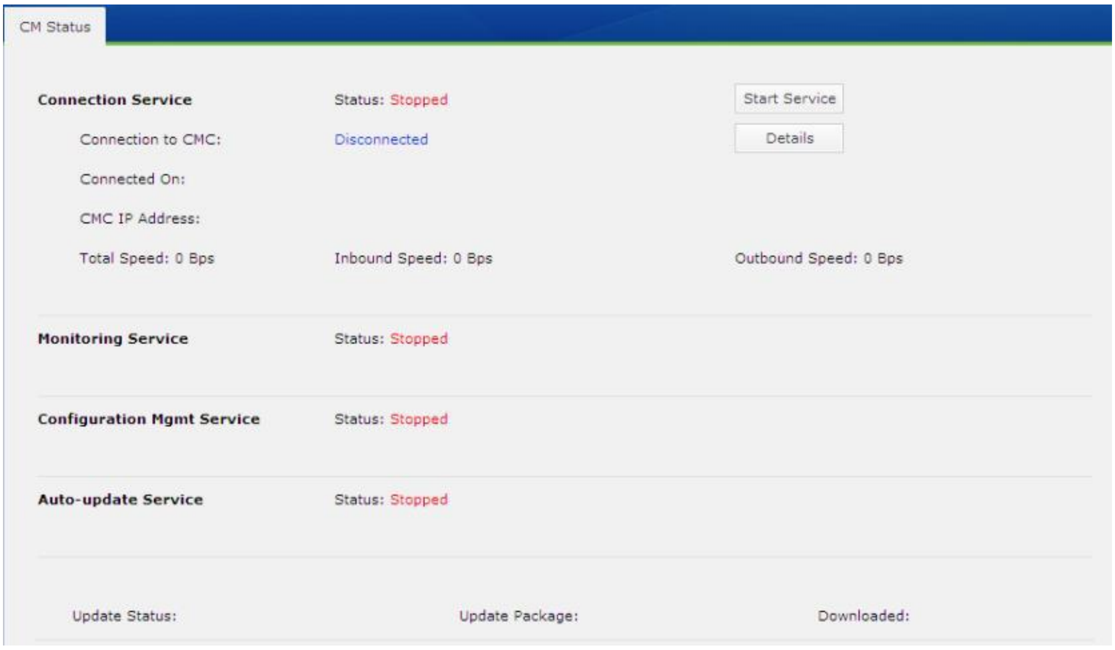
Test WebAgent: Click this button to check whether the configured WebAgent is valid.

CMC Device Location: Select Yes if the CMC device and this WOC are located in the same local area network. Otherwise, select No.

Bandwidth Limit: Specifies the maximum inbound and outbound bandwidth of the WAN links of the WOC. Once any limit is exceeded, the CMC will be informed of the event.

Bandwidth Usage Thresholds: Specifies the bandwidth usage threshold and time period during which alert will be generated if any threshold is exceeded successively.

To view central management status, navigate to Status > CM Status, as shown below:



Connection Service — Status: Stopped

Connection to CMC: Disconnected

Connected On:

CMC IP Address:

Total Speed: 0 Bps — Inbound Speed: 0 Bps — Outbound Speed: 0 Bps

Monitoring Service — Status: Stopped

Configuration Mgmt Service — Status: Stopped

Auto-update Service — Status: Stopped

Update Status: — Update Package: — Downloaded:

Chapter 4 Sangfor VPN

For the Sangfor WAN Optimization Controllers (WOCs) deployed in varying networks (head office and branch offices), VPN tunnels can be established among them to ensure secure data transmission if each network is deployed Sangfor WOC. Even mobile employee can be escorted to access the network of head office or another branch office if employee’s computer is installed the Mobile Sangfor VPN client, without worrying corporate data be intercepted or exposed.

Both sides can initiate Sangfor VPN connection. To set up an inbound VPN connection from a remote Sangfor WOC or any computer that is installed Sangfor Mobile VPN Client software, you need to complete the Server configuration on the local Sangfor WOC. Server setting includes basic parameters (such as WebAgent and listening port), creating user account for the remote WOC and configuring virtual IP pool or specifying a virtual IP address. For more information, you can refer to the following sections:

Setting Up Inbound VPN Connection on page 67
Basic Setting on page 67

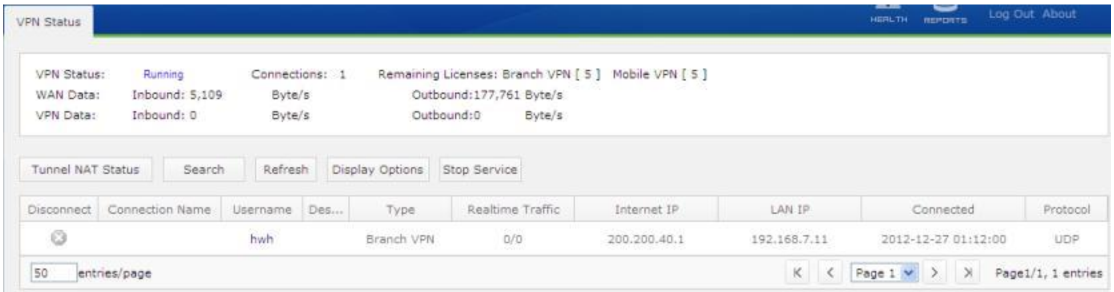
Creating VPN User on page 71

To set up an outbound VPN connection to a remote Sangfor WOC, you need to complete the Client configuration on the local Sangfor WOC. Client setting includes creating a VPN connection. For more information, you can refer to the following section:

Setting Up Outbound VPN Connection on page 82

Viewing VPN Status

Navigate to Status > VPN to enter the VPN Status page, and you will see the active VPN connections and traffic information.



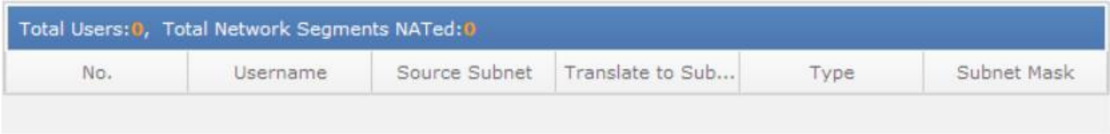
VPN Status: Running Connections: 1 Remaining Licenses: Branch VPN [5] Mobile VPN [5]
WAN Data: Inbound: 5,109 Byte/s Outbound:177,761 Byte/s
VPN Data: Inbound: 0 Byte/s Outbound:0 Byte/s

Disconnect	Connection Name	Username	Des...	Type	Realtime Traffic	Internet IP	LAN IP	Connected	Protocol
⊗		hwh		Branch VPN	0/0	200.200.40.1	192.168.7.11	2012-12-27 01:12:00	UDP

50 entries/page Page 1 Page1/1, 1 entries

To stop the VPN service, click the Stop Service button.

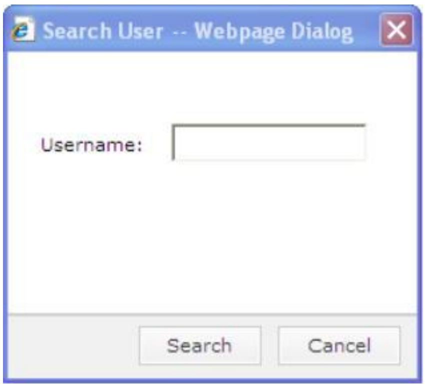
To view tunnel NAT (Network Address Translation) status, click the Tunnel NAT Status button. As shown in the following figure, the branch users involved in tunnel NAT, including username, source subnet, translated-to subnet, subnet type and network mask are seen in the table.



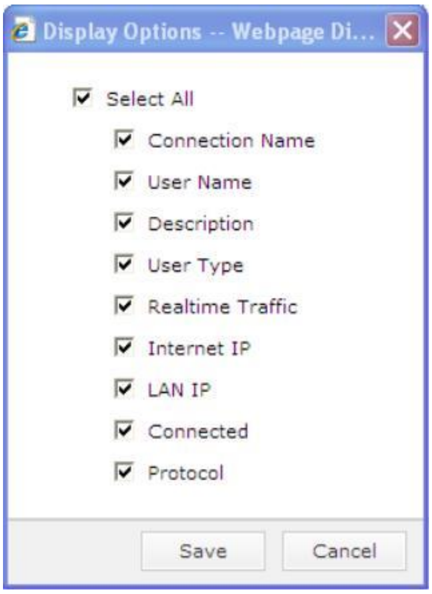
Total Users:0, Total Network Segments NATed:0

No.	Username	Source Subnet	Translate to Sub...	Type	Subnet Mask

To search for a connection related to a specific user, click the Search button to open the following dialog, enter the username and click Search.



To filter the columns, click Display Options to open the following dialog and select the desired items.



☑ Select All

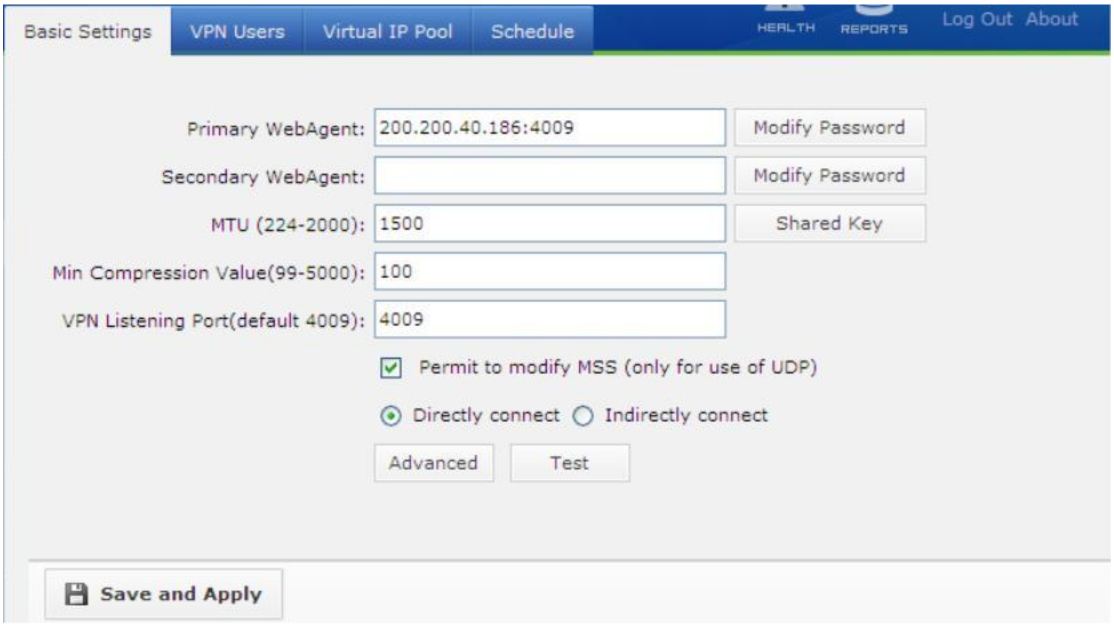
- ☑ Connection Name
- ☑ User Name
- ☑ Description
- ☑ User Type
- ☑ Realtime Traffic
- ☑ Internet IP
- ☑ LAN IP
- ☑ Connected
- ☑ Protocol

Setting Up Inbound VPN Connection

Basic Setting

The Basic Settings is fundamental for establishing inbound VPN connection, including WebAgent information, MTU value of VPN data, minimum compression value, VPN listening port, VPN connection mode, broadcast packet and performance settings.

Navigate to Sangfor VPN > Server to enter the Basic Settings page, as shown below



Primary WebAgent: 200.200.40.186:4009

Secondary WebAgent:

MTU (224-2000): 1500

Min Compression Value(99-5000): 100

VPN Listening Port(default 4009): 4009

☑ Permit to modify MSS (only for use of UDP)

● Directly connect ○ Indirectly connect

The following are the contents included on the Basic Settings page:

Primary WebAgent, Secondary WebAgent: Refers to the address of the dynamic IP addressing file on the Web server. Enter the WebAgent addresses of the local WOC here.

If the local Sangfor device uses dynamic IP (dynamic addressing), enter the WebAgent website address which typically ends with .php (please contact Sangfor to apply for WebAgent for free, or obtain WebAgent file and set up your own WebAgent Server).

If the local Sangfor device uses static IP address(es), enter IP:Port, for example, 202.96.134.133:4009. For multiple lines (up to 4 lines) deployment, enter IP1#IP2#IP3#IP4:4009, for example, 202.96.134.133#58.67.23.33:4009.

Test: Click this button to test whether the specified primary/secondary WebAgent can be connected.

MTU: Indicates Maximum Transmission Unit (MTU) of VPN data. The default value is 1500, which is recommended.

Min Compression Value: Indicates the minimum size of the VPN data packet that is to be compressed. It is 100 by default.

VPN Listing Port: Indicates the VPN listening port of the WOC. It is 4009 by default. You can change it according to the specific case.

Permit to modify MSS: Select this option (recommended) so that Maximum Segment Size (MSS) of VPN data packets could be modified when UDP transfer protocol is being used.

Directly connect, Indirectly connect: Refers to the connection mode between the WOC and Internet. If the Internet IP address can be obtained directly or the VPN port can be accessed from Internet by configuring DNAT (Destination Network Address Translation) rules, select Directly connect; otherwise, select Indirectly connect.

Modify PWD: Click this button to modify the password for WebAgent website to prevent unauthorized user from using the WebAgent to update masqueraded IP address.

Shared Key: Click this button to modify the shared key, which will encrypt the data sent to WebAgent server for updating WebAgent addresses, preventing access from unauthorized devices. If this shared key is specified on the HQ VPN device, it should be provided to all its branch VPN devices for they must use the same shared key (in Sangfor VPN > Client > VPN Connection) to establish VPN connections; otherwise, the VPN connections cannot be established.

Once the WebAgent password is set, please keep it carefully, for there is no way to get it back if it is lost. The only solution is to contact Sangfor to generate a file that does not contain the WebAgent password and use that file to replace the original one.

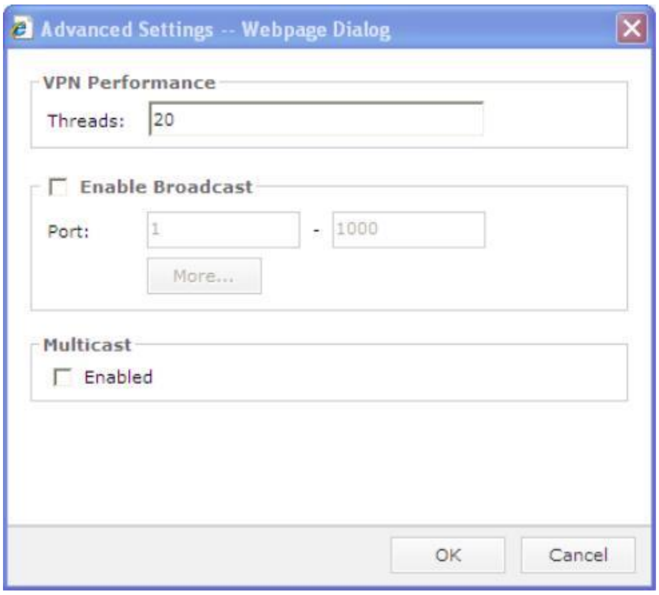
The MTU Value, Min Compression Value and Permit to modify MSS options are already configured with default values. Typically, it is recommended to keep the default settings. To change them, DO follow the instructions given by Sangfor technical engineer.

Advanced: Click this button to enter the Advanced Settings page and configure advanced parameters. The following are the contents included on Advanced Setting page:

Threads: Limit the number of VPN connections for the current Sangfor device. It supports as most as 1280 VPN connections and it is 20 by default. This parameter should be modified under the instructions given by Sangfor technical engineer.

Enable Broadcast: Specify whether to transmit the broadcast packets in VPN tunnel. If this option is enabled, specify the port range of the broadcast packet to avoid broadcast storm at both ends of VPN. Some applications, for example, My Network Places, may need broadcast support.

Multicast: Select Enabled to allow multicast packets to be transmitted on VPN tunnel. Some video applications may need multicast support.



Advanced Settings -- Webpage Dialog

VPN Performance

Threads: 20

□ Enable Broadcast

Port: 1 - 1000

Multicast

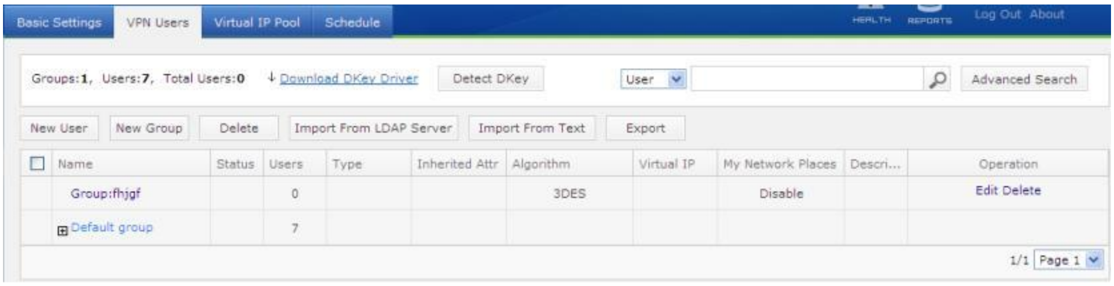
□ Enabled

Sangfor VPN Users

Sangfor VPN users are the user accounts used by remote WOC at branch VPN site or mobile user whose PC is installed Sangfor Mobile VPN Client to connect to this WAN Optimization Controller securely.

To allow remote WOC or mobile user to connect this WOC through VPN tunnel, you need to create user account which defines the username, password, encryption algorithm, user type (mobile or branch user), parent group (whether to inherit group attributes), hardware/DKey based authentication (enable or not), virtual IP address (for mobile user), account expiry time and advanced settings such as multicast, tunnel traffic control and tunnel NAT. What LAN services are accessible to connecting user can also be specified.

Navigate to Sangfor VPN > Server > VPN Users to enter the VPN Users page, as shown below



Groups:1, Users:7, Total Users:0

□	Name	Status	Users	Type	Inherited Attr	Algorithm	Virtual IP	My Network Places	Descri...	Operation
	Group:fhjgf		0			3DES		Disable		Edit Delete
	⊞ Default group		7							

1/1 Page 1

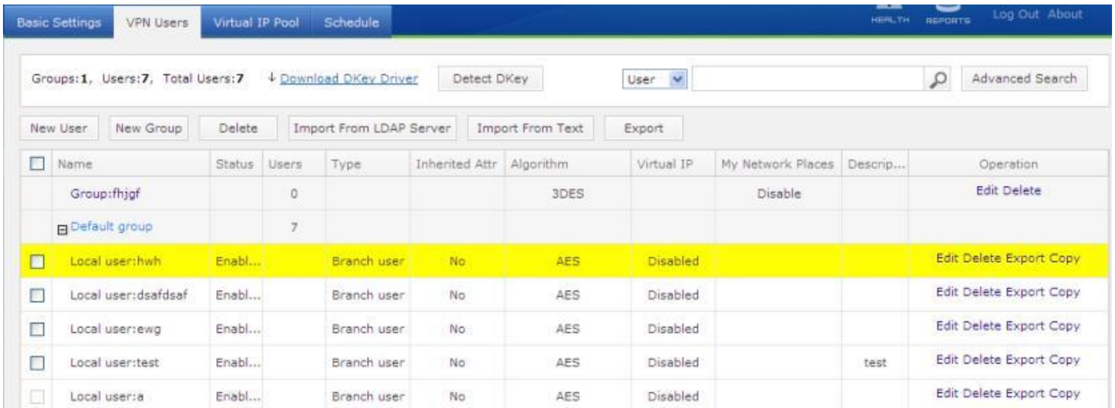
To delete one or more users, select the users, click Delete and then click Yes on the popup prompt.

If you are using USB key, click Detect DKey on the VPN Users page to check whether the USB key is inserted into the computer properly. If the USB key driver is not installed, the system will prompt you to download it. You can then click the Download DKey Driver link to download and install the USB key driver.

Before generating USB key, please install the USB key driver; otherwise, the computer cannot identify the USB key hardware. To avoid program conflict that may cause installation failure, close third-party antivirus software and firewalls before installing the USB key driver.

Searching for VPN Users

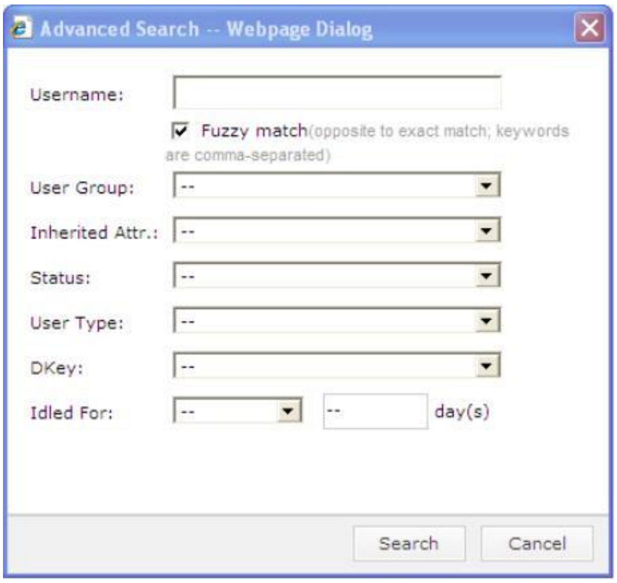
To search for a specific user or group, select user or group from the drop-down list, enter the name in the textbox next to the Search button and then click Search. The matching user/group will be highlighted in yellow, as shown below:



Groups:1, Users:7, Total Users:7

□	Name	Status	Users	Type	Inherited Attr	Algorithm	Virtual IP	My Network Places	Descrip...	Operation
	Group:fhjgf		0			3DES		Disable		Edit Delete
	⊟ Default group		7							
□	Local user:hwh	Enabl...		Branch user	No	AES	Disabled			Edit Delete Export Copy
□	Local user:dsafdsaf	Enabl...		Branch user	No	AES	Disabled			Edit Delete Export Copy
□	Local user:ewg	Enabl...		Branch user	No	AES	Disabled			Edit Delete Export Copy
□	Local user:test	Enabl...		Branch user	No	AES	Disabled		test	Edit Delete Export Copy
□	Local user:a	Enabl...		Branch user	No	AES	Disabled			Edit Delete Export Copy

To perform advanced search, click the Advanced Search button and then specify more detailed information of the user, including parent group, group attributes (inherited or not), user type (mobile/branch), USB key (enabled/disabled), and inactive time since last login, as shown in the following dialog:



Username:

☑ Fuzzy match(opposite to exact match; keywords are comma-separated)

User Group: --

Inherited Attr.: --

Status: --

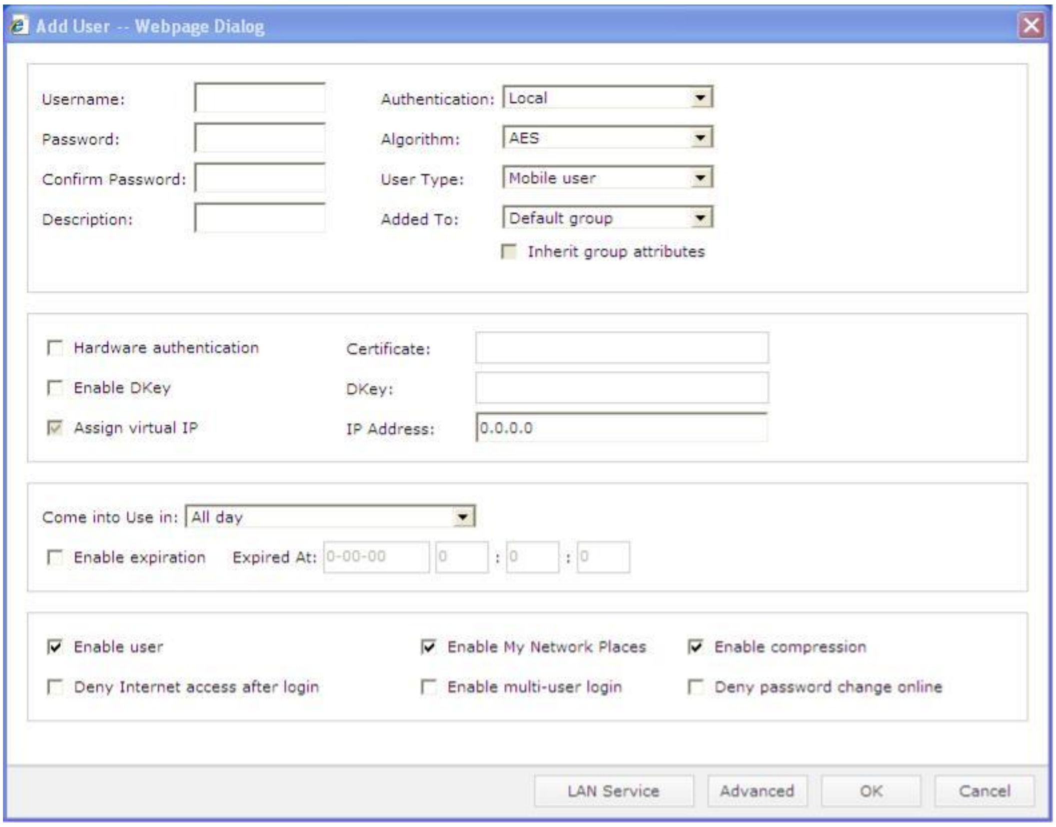
User Type: --

DKey: --

Idled For: -- -- day(s)

Creating VPN User

1. Navigate to Sangfor VPN > Server to enter the VPN Users page. Click New User to enter the Add User page, as shown below:



Username:
Password:
Confirm Password:
Description:
Authentication: Local
Algorithm: AES
User Type: Mobile user
Added To: Default group
□ Inherit group attributes

□ Hardware authentication Certificate:
□ Enable DKey DKey:
☑ Assign virtual IP IP Address: 0.0.0.0

Come into Use in: All day
□ Enable expiration Expired At: 0-00-00 0 : 0 : 0

☑ Enable user ☑ Enable My Network Places ☑ Enable compression
□ Deny Internet access after login □ Enable multi-user login □ Deny password change online

2. Specify the following basic information.

Username: Specify a name for the user.

Password, Confirm Password: Set a password for the user and then enter it again.

Description: Enter descriptive information for the user.

Authentication: Select an authentication method for the user. There are three options: Local, LDAP and RADIUS.

If LDAP/RADIUS is selected, you need to go to the LDAP Server or RADIUS Server page to configure the LDAP/RADIUS server.

Algorithm: Select an algorithm to be adopted by the user.

User Type: Specify the type of the user, Mobile user or Branch user.

Added To, Inherit group attributes: The Added To field is used to classify the user into certain group, while Inherit group attributes decides whether the user adopts the public attributes of the group.

Before classifying a user into a certain group, please add the user group. If the user inherits the attributes of a certain group, the Algorithm, Enable My Network Places, LAN Service and Advanced fields will not be editable.

Hardware authentication: Select whether to enable certificate based authentication featuring hardware ID. After selecting this option, click the Browse button to select the certificate file (*.id) corresponding to this user.

Enable DKey: Select whether to enable the USB key based authentication for mobile VPN user. After selecting this option, insert the USB key into the computer and then click the Generate button to generate the USB key.

Assign Virtual IP: Assign a virtual IP address to mobile user, which will be used as LAN IP address after the user connects to VPN. Enter an IP address (which must be in the virtual IP pool), or set it to 0.0.0.0, which indicates the system will randomly select an IP address from the virtual IP pool for the user.

This option is selected by default for mobile user and unavailable for branch user.

Come into Use in: Select a time period during which the current account is valid.

Enable expiration: Select whether to specify an expiry date for the current user account. If it is selected, specify the date and time.

Enable user: Select this option to enable the current user account.

Enable My Network Places: Select this option if the user needs to use the My Network Places service after connecting to the VPN.

Enable compression: Select whether to use algorithm to compress the data transferred between the Sangfor device and the user.

This option is an exclusive technology integrated in Sangfor VPN. It will efficiently utilize the bandwidth in low-bandwidth environment to speed up data transmission. However, it may not be applicable to all network environments.

Deny Internet access after login: Select whether to block users from accessing the Internet after they connect to the VPN.

This option applies only to mobile VPN users.

Allow multi-user login: Select whether to allow multiple users to access VPN using this account simultaneously.

Deny password change online: Select whether to allow mobile VPN users to change their login passwords after they connect to VPN. Unchecking it means changing password online is not allowed.

3. Click the LAN Service button to set the privileges of the user after the user connects to the local area network, that is, to allow/disallow the user to access certain services provided by the internal network. By default, the user can access all LAN services.

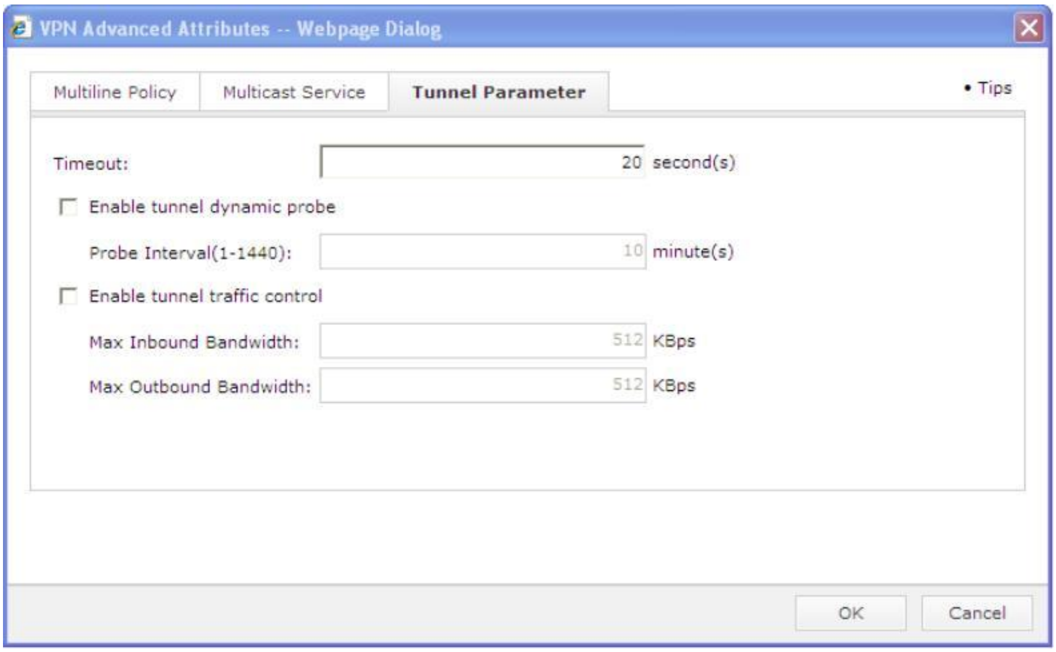
Before clicking the LAN Service button to configure LAN services accessible to the user, please go to the LAN Service page to define the services (for detailed guide, please refer to the section Configuring LAN Service in Chapter 4).

4. Click the Advanced button to configure advanced attributes for the user, including multiline policy, multicast service (whether to enable it or not), tunnel-related parameters and tunnel NAT.

   a. Configure multiline policy (for detailed guide, refer to the Creating Multiline Policy section in Chapter 4).

   b. Configure multicast service (for detailed guide, refer to the Configuring Multicast Service section in Chapter 4).

   c. Configure the tunnel parameters.



Timeout: 20 second(s)

☐ Enable tunnel dynamic probe

Probe Interval(1-1440): 10 minute(s)

☐ Enable tunnel traffic control

Max Inbound Bandwidth: 512 KBps

Max Outbound Bandwidth: 512 KBps

The following are the contents included on Tunnel Parameter tab:

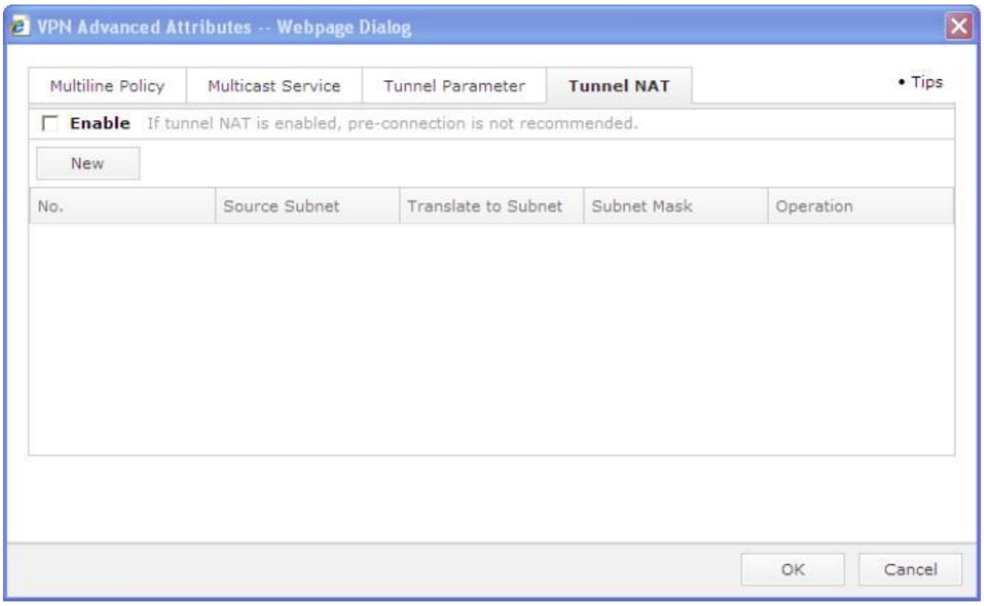
Timeout: In environments with high latency and high packet loss rate, specify the VPN tunnel timeout. This setting will prevail for each tunnel. It is 20 seconds by default. For poor network environment, enter a larger value.

Enable tunnel dynamic probe: This function will work only if the local or peer Sangfor device has deployed multiple lines. In that case, the system will regularly probe the latency and packet loss of the lines and then select the optimal line for VPN data transmission.

Enable tunnel traffic control: When multiple branches or mobile users connect to VPN, it is possible that one of the branches or mobile users preempts all the HQ bandwidth with nearly no bandwidth left for others. To avoid that situation, enable tunnel traffic control and specify a maximum inbound/outbound bandwidth allowed for each user connecting to VPN.

The values specified for maximum inbound/outbound bandwidth are approximate values instead of accurate ones. For example, if bandwidth is 100 KBps, the bandwidth of the user will be actually limited to a range between 80 and 120 KBps, fluctuating properly around 100 KBps.

Configure the tunnel NAT function (for detailed guide, please refer to Configuring Tunnel NAT in Chapter 4). This function avoids IP conflict caused by multiple branches with the same LAN subnet connecting to HQ VPN.



VPN Advanced Attributes -- Webpage Dialog

□ **Enable** If tunnel NAT is enabled, pre-connection is not recommended.

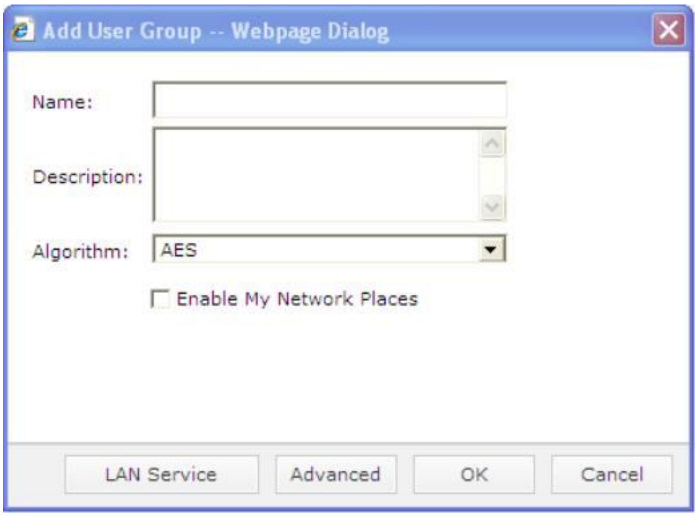
No.	Source Subnet	Translate to Subnet	Subnet Mask	Operation

- The tunnel NAT function is available only for branch users.
- Before configuring the tunnel NAT function, please go to Virtual IP Pool to add a virtual IP pool for branch users.

5. Click the OK buttons to save the settings.

Creating User Group

1. Navigate to Sangfor VPN > Server > VPN Users and click New Group to enter Add User Group page, as shown below:



Add User Group -- Webpage Dialog

Name:

Description:

Algorithm: AES

□ Enable My Network Places

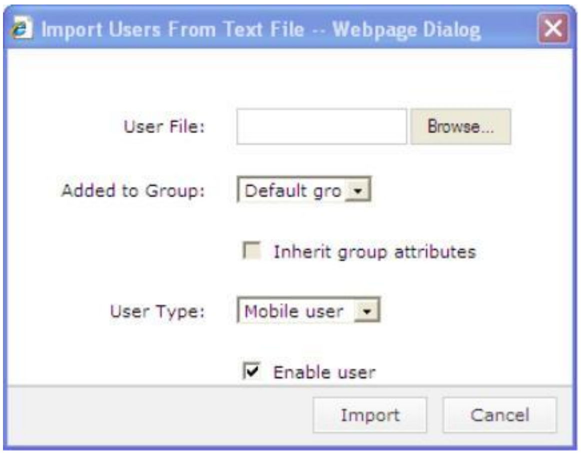
2. Specify group name, description and algorithm, and select My Network Places.
3. For the LAN Service settings and Advacned settings, please refer to the above section, Creating VPN User.

Importing Users

VPN users can be imported from a .txt or .csv file and LDAP server.

Importing Users from Text File

1. Click Import From Text to open the following dialog:



Import Users From Text File -- Webpage Dialog

User File: Browse...

Added to Group: Default gro

□ Inherit group attributes

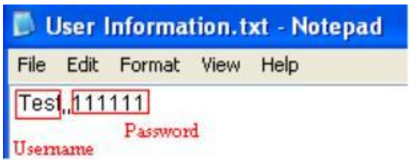
User Type: Mobile user

☑ Enable user

Import Cancel

2. Select a user group to which the users will be imported, specify whether to have the imported users inherit the attributes of the selected group by checking/unchecking the Inherit group attributes option, and specify the type for imported users (mobile user or branch user).
3. Select the file from which the users are to be imported.

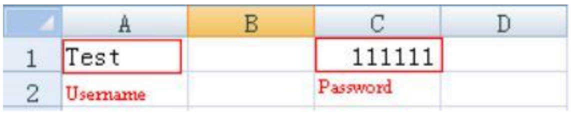
   For a .txt file, the user information should be entered in format of User Name,,Password, and no other information can be imported, as shown below:



User Information.txt - Notepad

```
Test,,111111
```

   For a .csv file, there should be an empty column between the username column and password column, as shown below:



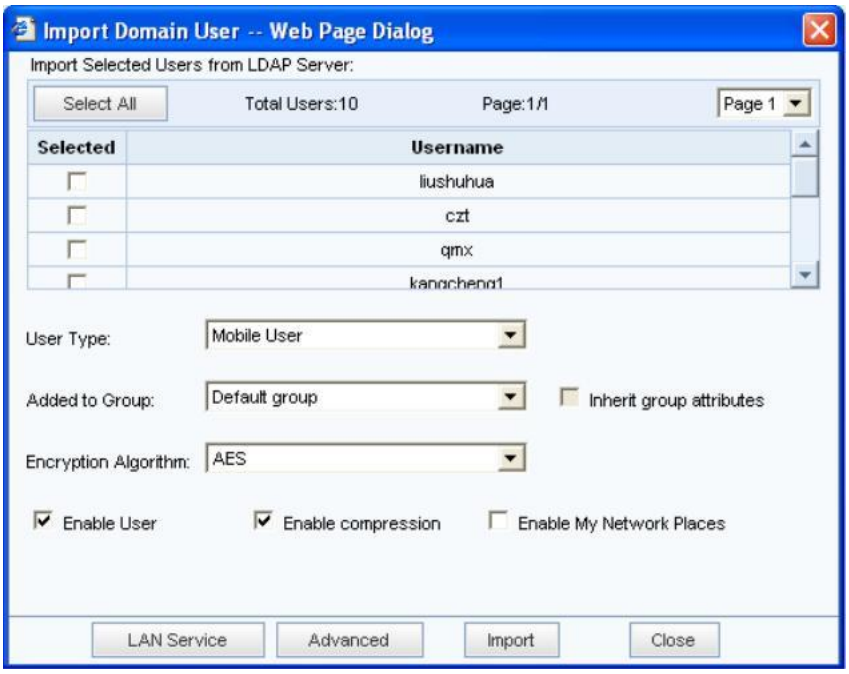
	A	B	C	D
1	Test		111111	
2	Username		Password	

4. Import the users from the file into the Sangfor WOC.

Importing Users from LDAP Server

1. Navigate to Sangfor VPN > LDAP Server to configure the LDAP server (for detailed guide, please refer to the Configuring LDAP Server section in Chapter 5).

5. Click Import Domain User on the User Management page, the system will connect to the LDAP server configured in Step 1 and read the users from it, as shown below:



Import Domain User -- Web Page Dialog

Import Selected Users from LDAP Server:

Total Users:10 Page:1/1 Page 1

Selected	Username
□	liushuhua
□	czt
□	qmx
□	kangcheng1

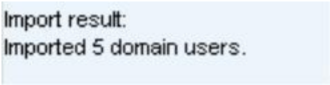
User Type: Mobile User

Added to Group: Default group □ Inherit group attributes

Encryption Algorithm: AES

☑ Enable User ☑ Enable compression □ Enable My Network Places

2. Check the users to be imported, specify other attributes and options for the users, and click the Import button. If the import succeeds, the imported users will be listed on the VPN User page, and the following prompt appears:



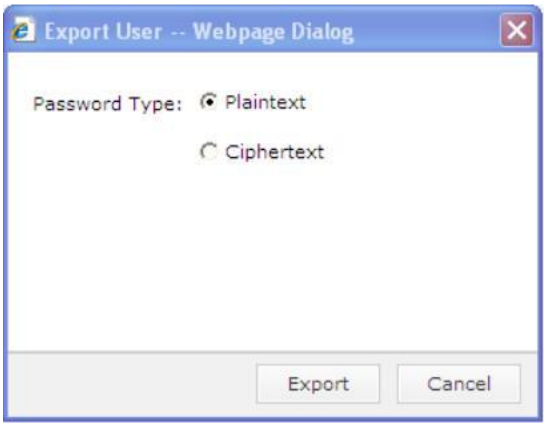
Import result:
Imported 5 domain users.

3. To view attributes of a user, select the user and click Edit to enter the Edit User page. The authentication method of the imported user is LDAP.

By default, the imported users will adopt the LDAP authentication with no password.

Exporting Users

1. Click Export and then select the type of user passwords (plaintext or ciphertext).



Password Type: ● Plaintext ○ Ciphertext

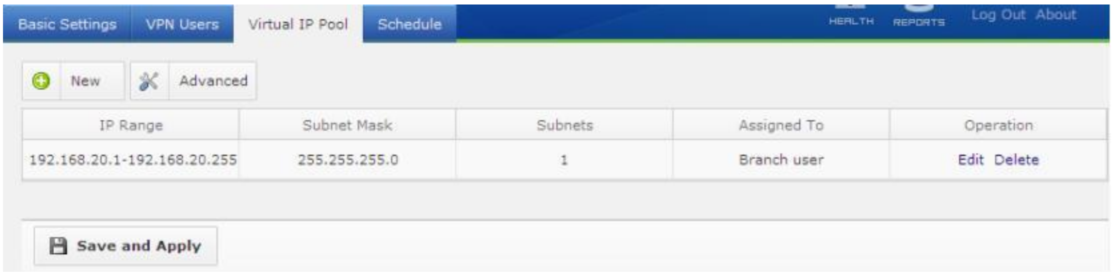
2. Click the Export button.

Virtual IP Pool

Virtual IP Pool is a pool contains idle IP addresses that will be assigned to branch VPN users when they connect to the WOC device). Virtual IP assignment helps to avoid IP conflict if two branches use the same network segment and connect to the local WOC at the same time.

When a mobile VPN user connects in, the WAN Optimization Controller (WOC) assigns a virtual IP address to the user. All the operations implemented by this mobile VPN user on the HQ VPN sites are based on that virtual IP address (source IP), completely the same as those implemented by a local user. What’s more, the mobile VPN user can also be specified with some network attributes such as DNS.

The Virtual IP Pool tab is as shown below:



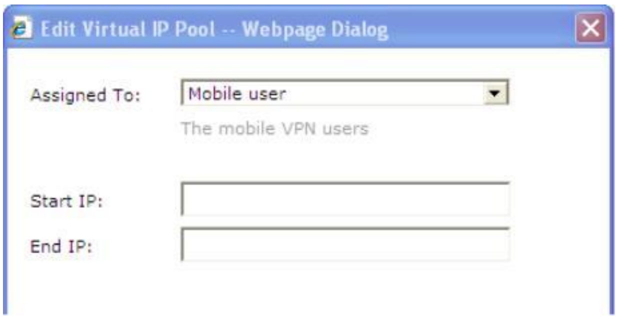
IP Range	Subnet Mask	Subnets	Assigned To	Operation
192.168.20.1-192.168.20.255	255.255.255.0	1	Branch user	Edit Delete

Creating Virtual IP Pool for Mobile VPN Users

The IP addresses in the virtual IP pool are idle IP addresses on the local area network or random IP addresses that will be assigned to connecting users. If the IP addresses are randomly specified, you should ensure that route entries of the specified IP addresses are forwarded to the Sangfor WAN Optimization Controller (WOC) by internal server, otherwise, the mobile VPN user cannot access the servers on HQ network even though the user has connected to the WOC successfully.

1. Navigate to Sangfor VPN > Server > Virtual IP Pool, and click the New button to enter the Edit Virtual IP Pool page.

2. Select the user type Mobile user, and configure the start and end IP, as shown below:



Edit Virtual IP Pool -- Webpage Dialog

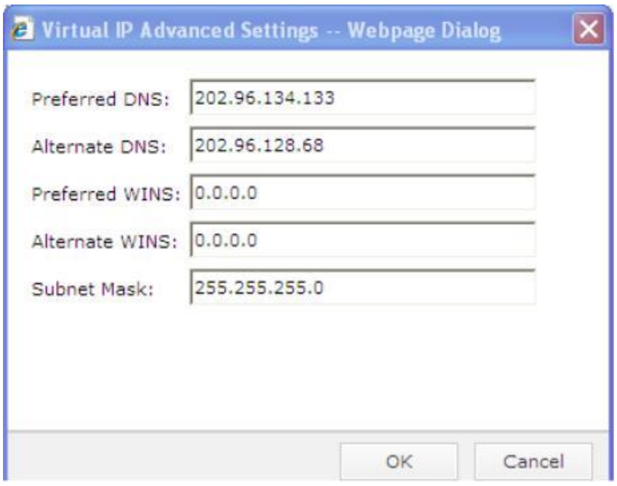
Assigned To: Mobile user

The mobile VPN users

Start IP:

End IP:

3. Click OK and then click Advanced to configure the subnet mask of the virtual IP address, DNS and WINS servers, as shown below:



Virtual IP Advanced Settings -- Webpage Dialog

Preferred DNS: 202.96.134.133

Alternate DNS: 202.96.128.68

Preferred WINS: 0.0.0.0

Alternate WINS: 0.0.0.0

Subnet Mask: 255.255.255.0

4. Go to the Sangfor VPN > Server > VPN Users tab to create a new VPN user account, selecting user type Mobile user. If the virtual IP is 0.0.0.0, the HQ WOC will automatically assign an idle virtual IP address to this mobile VPN user from the IP pool when the mobile VPN user connects in. Except using the default (0.0.0.0), we can also type in a specific IP address to assign that virtual IP address to this mobile VPN user.

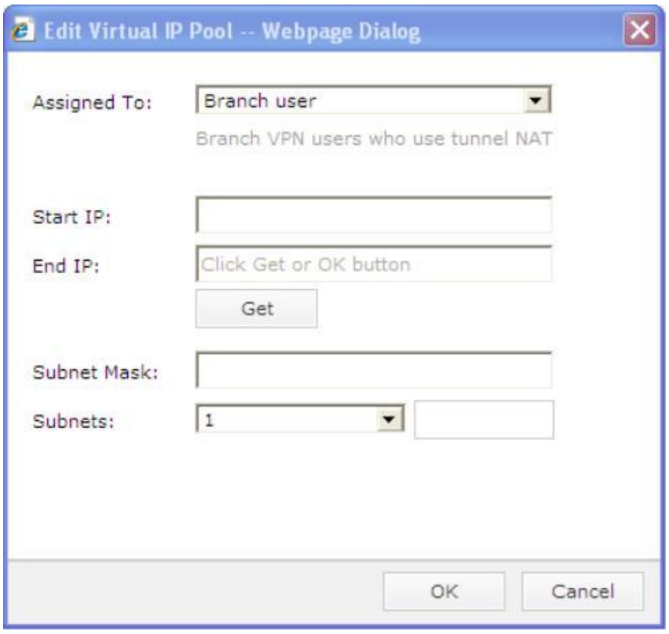
⚠

After configuring the Advanced options, the “SANGFOR VPN virtual network adapter” on the mobile VPN user’s computer must be configured to Obtain an IP address automatically and Use the following DNS server addresses, otherwise, the advanced settings will distributed to the virtual network adapter of the mobile VPN user’s PC.

Creating Virtual IP Pool for Branch VPN Users

The virtual IP addresses in the virtual IP pool will be assigned to the branch VPN users. When a branch VPN user connects in the HQ WOC, the source IP address of the branch VPN user will be replaced by one of the virtual IP addresses in the pool, which helps to avoid IP conflict when users from two branch offices use the same IP address and connect to the HQ WOC at the same time.

1. Navigate to Sangfor VPN > Server > Virtual IP Pool, and click the New button to enter the Edit Virtual IP Pool page.
2. Select the user type Branch user, and configure the start IP, subnet mask, number of subnets.
3. Click Get to have the system calculate the end IP automatically according to the other settings on the page, as shown below:



Assigned To: Branch user

Branch VPN users who use tunnel NAT

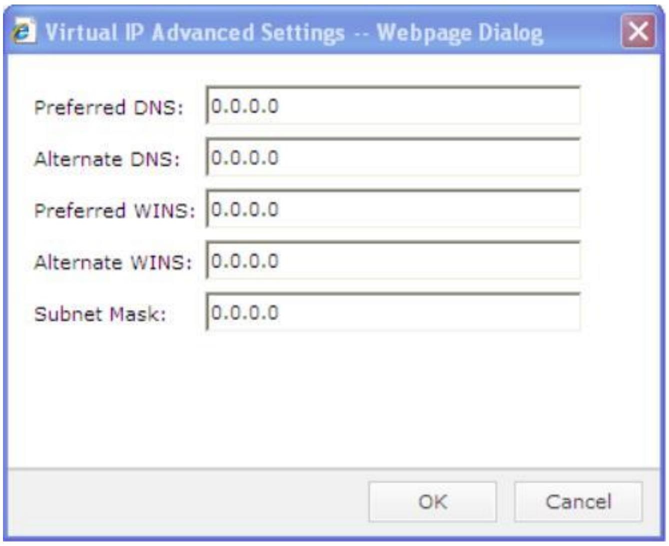
Start IP:

End IP: Click Get or OK button

Subnet Mask:

Subnets: 1

5. Click OK and then click Advanced to configure the subnet mask of the virtual IP address, DNS and WINS servers, as shown below:



Preferred DNS: 0.0.0.0

Alternate DNS: 0.0.0.0

Preferred WINS: 0.0.0.0

Alternate WINS: 0.0.0.0

Subnet Mask: 0.0.0.0

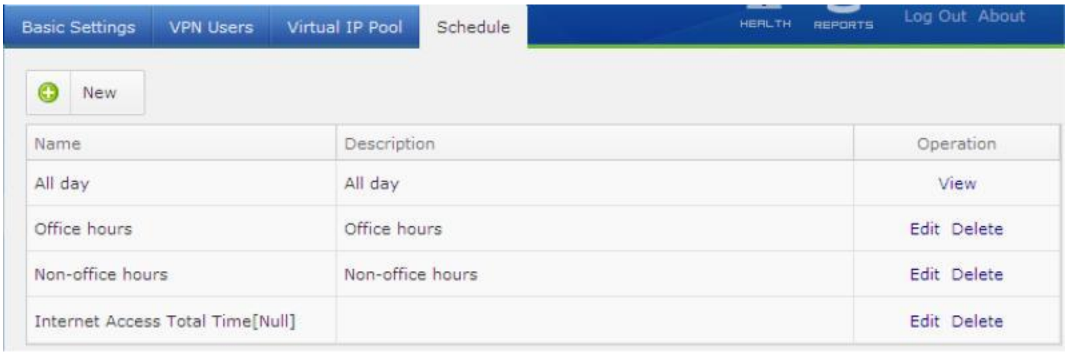
4. Go to the Sangfor VPN > Server > VPN Users tab to create a new VPN user account. Select user type Branch user, and click Advanced to enter the VPN Advanced Attributes page and select Tunnel NAT tab. Add a tunnel NAT rule for the branch user.

Creating Schedule

A schedule is a combination of time segments, which can be referenced by bandwidth control policy. The date and time are based on the system time on the WAN Optimization Controller.

To create a schedule, perform the following steps:

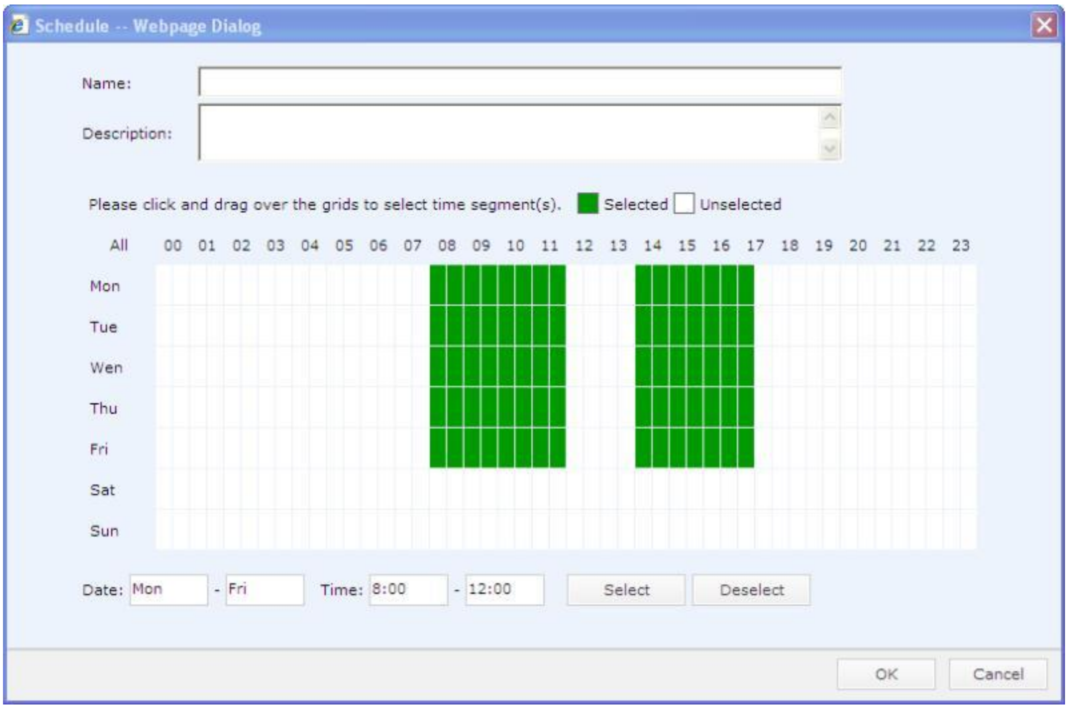
1. Navigate to Sangfor VPN > Server > Schedule, as shown in the figure below:



Name	Description	Operation
All day	All day	View
Office hours	Office hours	Edit Delete
Non-office hours	Non-office hours	Edit Delete
Internet Access Total Time[Null]		Edit Delete

2. Click New to add a new schedule. Enter the name into the Name field. Description is optional.

3. Click and drag over the grids to select the desired time segments.



Date: Mon - Fri Time: 8:00 - 12:00

4. To deselect and remove a time segment from the schedule, click on and drag over the green

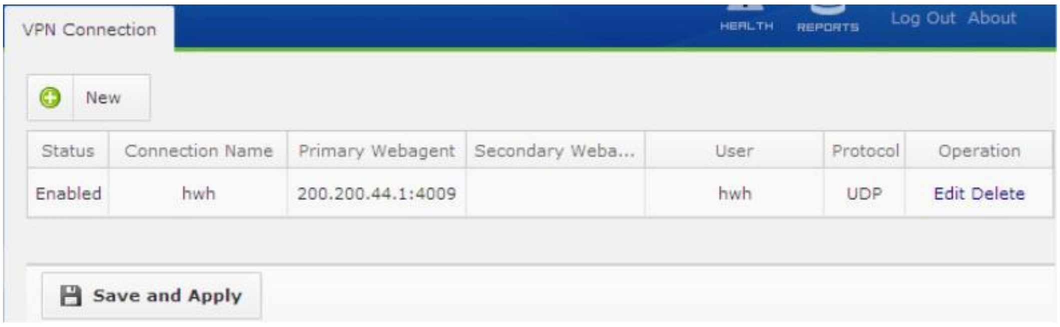
grids (selected time segments) to select the time segment that you want to deselect. Click Deselect to deselect the time segment.

5. Click OK to save the settings on this page.

Setting Up Outbound VPN Connection

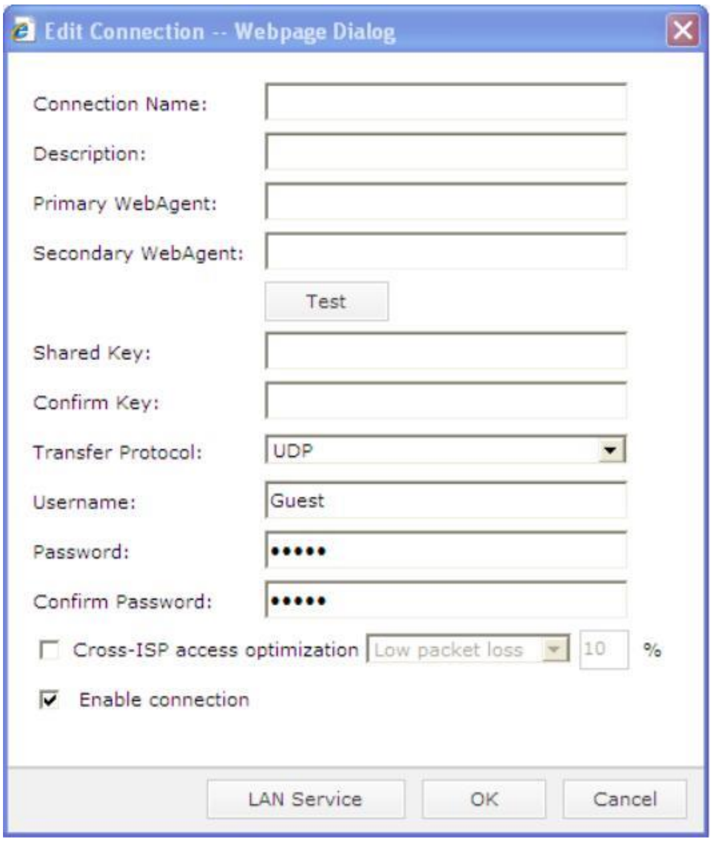
To enable VPN connection to be initiated from the local Sangfor WAN Optimization Controller (WOC) to a peer Sangfor, configure VPN Connection for that peer WOC.

1. Navigate to Sangfor VPN > Client > VPN Connection to enter VPN Connection page, as shown below:



Status	Connection Name	Primary Webagent	Secondary Weba...	User	Protocol	Operation
Enabled	hwh	200.200.44.1:4009		hwh	UDP	Edit Delete

2. Click New to open the following dialog.



Connection Name:

Description:

Primary WebAgent:

Secondary WebAgent:

Shared Key:

Confirm Key:

Transfer Protocol: UDP

Username: Guest

Password: •••••

Confirm Password: •••••

☐ Cross-ISP access optimization Low packet loss 10 %

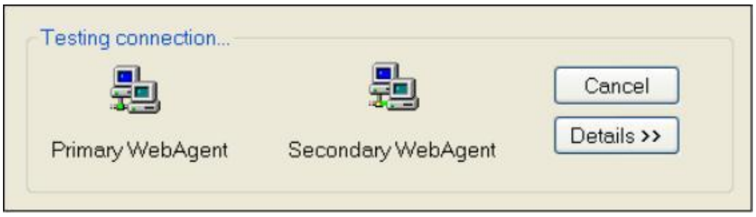
☑ Enable connection

3. Select Enable connection to activate the current connection and then specify the following

information.

Connection Name, Description: Enter a name and description for the VPN connection.

Primary WebAgent, Secondary WebAgent: Enter the WebAgent of the peer device that the local device will connect to. Then click Test to test if the WebAgent is available.



The testing request is initiated by the local computer instead of the Sangfor device. If the WebAgent is typed in format of domain name, successful testing result indicates the webpage exists; otherwise, it indicates the webpage does not exist. If the WebAgent is entered in format of static IP, successful testing result only means the format (IP:Port) of the input is correct, that is, successful testing result does not mean the device cannot connect to the WebAgent.

Shared Key, Confirm Key: Enter and confirm the shared key, which must be the same as that configured on the Sangfor VPN > Server > Basic Settings page on the peer Sangfor WOC.

Transfer Protocol: Select the protocol to be adopted for transferring VPN data. Options are TCP and UDP. It is UDP by default.

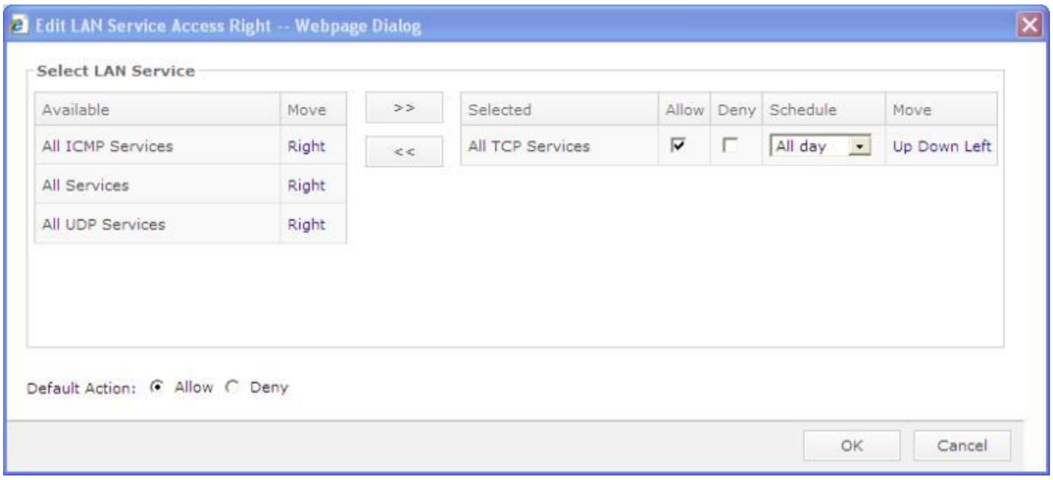
Username, Password: Enter the username/password provided by the peer VPN device for establishing the VPN connection.

Cross-ISP access optimization: This function applies to the situation where the peer and local Sangfor devices are interconnected using Internet links provided by different Internet Service Providers (ISPs) and packet loss occurs frequently. Options are Low packet loss, High packet loss and Packet loss rate is.

Before enabling cross-ISP access optimization, ensure the cross-ISP access optimization license has been activated. Once the license is activated, this function will apply to all the branch VPN users or mobile users connecting to that Sangfor device.

4. Click LAN Service to configure available services for users from peer VPN, as shown

below:



Select LAN Service

Available	Move
All ICMP Services	Right
All Services	Right
All UDP Services	Right

Selected	Allow	Deny	Schedule	Move
All TCP Services	☑	□	All day	Up Down Left

Default Action: ● Allow ○ Deny

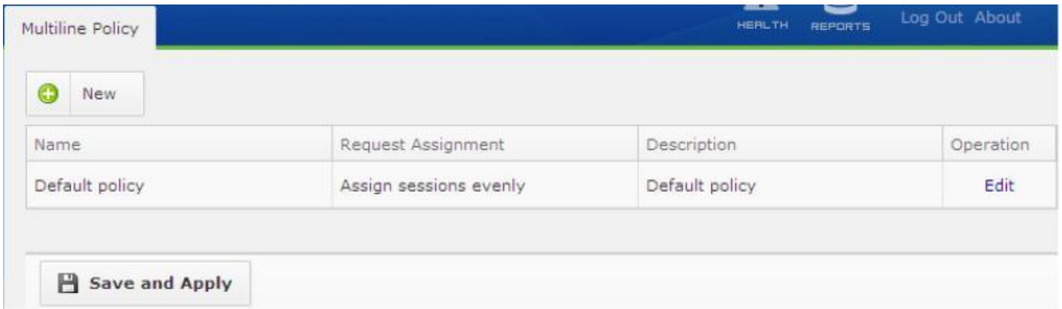
5. Click the OK buttons on the Edit LAN Service Access Right page and Edit Connection page to save the settings.

If tunnel NAT is enabled, IP address included in LAN services accessible to connecting users should be the translated-to addressees.

Creating Multiline Policy

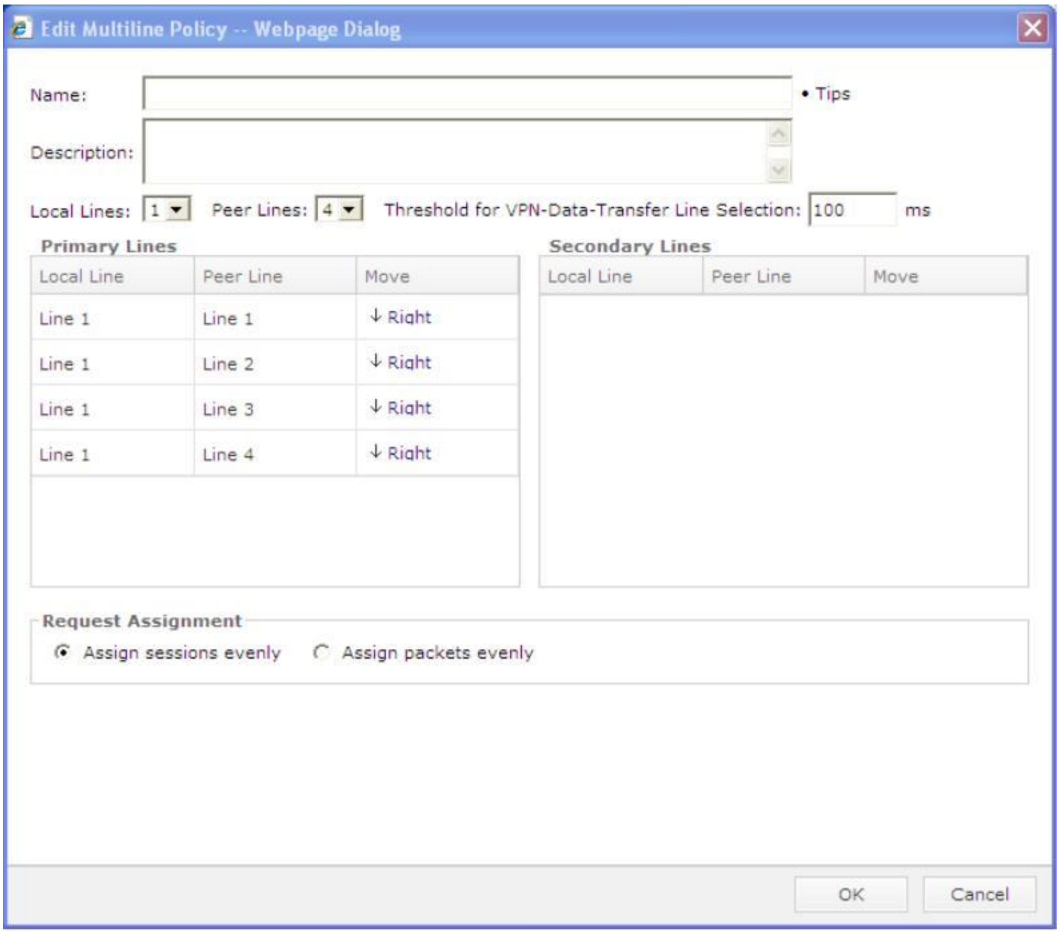
Sangfor WAN Optimization Controller (WOC) allows you to configure routing policy among multiple VPN lines. With this feature, an optimal line will be selected or multiple lines will be bound for VPN data transmission according to the connection status of the current WAN links, so that data are always transmitted through better links, greatly enhancing data transmission quality and link utilization.

1. Navigate to Sangfor VPN > Multiline Policy to enter the Multiline Policy page, as shown below:



Name	Request Assignment	Description	Operation
Default policy	Assign sessions evenly	Default policy	Edit

2. Click New to open the following dialog.



Edit Multiline Policy -- Webpage Dialog

Name: • Tips

Description:

Local Lines: 1 Peer Lines: 4 Threshold for VPN-Data-Transfer Line Selection: 100 ms

Primary Lines

Local Line	Peer Line	Move
Line 1	Line 1	↓ Right
Line 1	Line 2	↓ Right
Line 1	Line 3	↓ Right
Line 1	Line 4	↓ Right

Secondary Lines

Local Line	Peer Line	Move

Request Assignment

● Assign sessions evenly ○ Assign packets evenly

3. Specify the following information.

Name, Description: Enter a name and description for the policy.

Local Lines: Specify the number of available lines at the local VPN end.

Peer Lines: Specify the number of available lines at the peer VPN end.

Threshold for VPN-Data-Transfer Line Selection: Specify the threshold based on which VPN-data-transfer lines are selected.

If the latency difference between any two primary lines is smaller than this threshold, the system will determine that all the primary lines are VPN-data-transfer lines, and VPN data will be transferred through these lines simultaneously.

If the latency difference between a primary line and any other primary lines is larger than this threshold, the system will determine that the line of higher latency is not a VPN-Data-Transfer line and it will NOT be used for VPN data transmission.

This threshold only applies to primary lines.

Primary Lines: Specify the preferentially used lines. If all the primary lines are disconnected, the Sangfor device will switch to secondary lines for data transmission, ensuring smooth VPN connection. Once any primary line recovers, the Sangfor device will switch back to the primary line to achieve optimal data transmission.

Secondary Lines: Specify the standby lines, lines other than the primary lines. The secondary lines will not be used for VPN data transmission unless all the primary lines are unavailable.

Request Assignment: Specify how the VPN traffic is assigned when there are several VPN-data-transfer lines available for data transmission. There are two options: Assign sessions evenly and Assign packets evenly. The former indicates the traffic will be evenly assigned to lines based on sessions (that is, the traffic of a same session will be always assigned to a same line), and the latter indicates the traffic will be evenly assigned to lines based on VPN data packets.

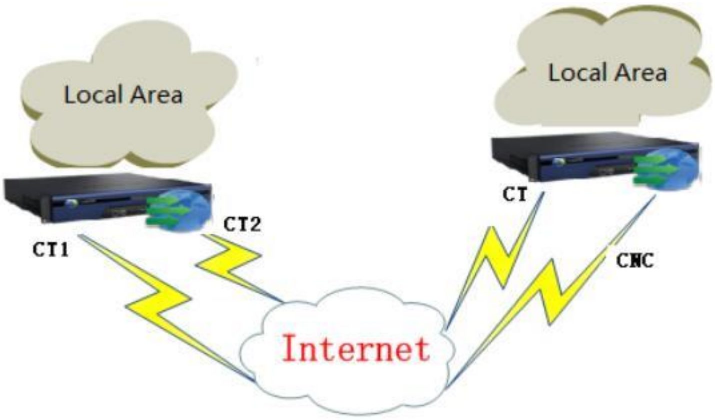
4. Click OK to save the settings.
5. Go to Sangfor VPN > Server > VPN Users > Add User/Edit User > Advanced > Multiline Policy to apply the multiline policy to a specific user.

Scenario: Creating VPN Primary Lines and Secondary Line

Sangfor WOC at HQ is connected two WAN links, CT1 and CT2. The WOC in remote branch office connects to another two WAN links, CT and CNC.

The requirement is that CT line of branch office and the two CT lines (CT1, CT2) of the HQ set up VPN connections and transmit data simultaneously, while the CNC line and the two CT lines (CT1, CT2) of the HQ VPN work as secondary lines.

The network topology is as follows:



Perform the following steps:

1. Log in to branch WOC administrator Web console and go to System > Network > Deployment > Multiline to add the two lines, CT and CNC
2. Log in to HQ WOC administrator Web console and go to System > Network > Deployment >

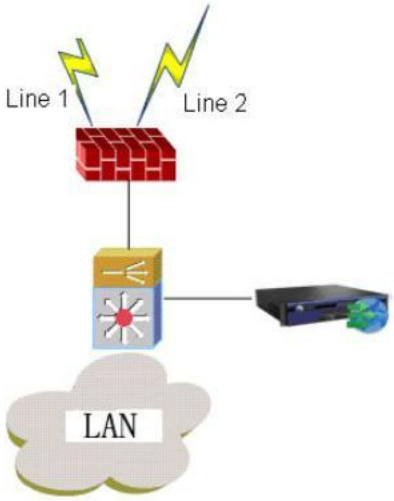
Multiline to add the two lines, CT1 and CT2.

3. On the HQ WOC administrator Web console, go to Sangfor VPN > Multiline Policy and click the New button to add a multiline policy. CT and CT1, CT and CT2 are primary lines, in combination to set up VPN connections, while CNC and CT1, CNC and CT2 are secondary lines.
4. Go to the Sangfor VPN > Server > VPN Users > Edit user and click Advanced > Multiline Policy tab. Select the multiline policy you have configured in the above step.

Scenario: Creating Multi-Line Policy for Single-Arm WOC

Enterprise network is deployed two WAN links. A Sangfor WAN Optimization Controller (WOC) is about to be deployed in the internal network, in Single Arm mode. The requirement is that external users can access the enterprise network through VPN tunnel, while the existing internet lines can be taken full use of and fulfill load-balancing function.

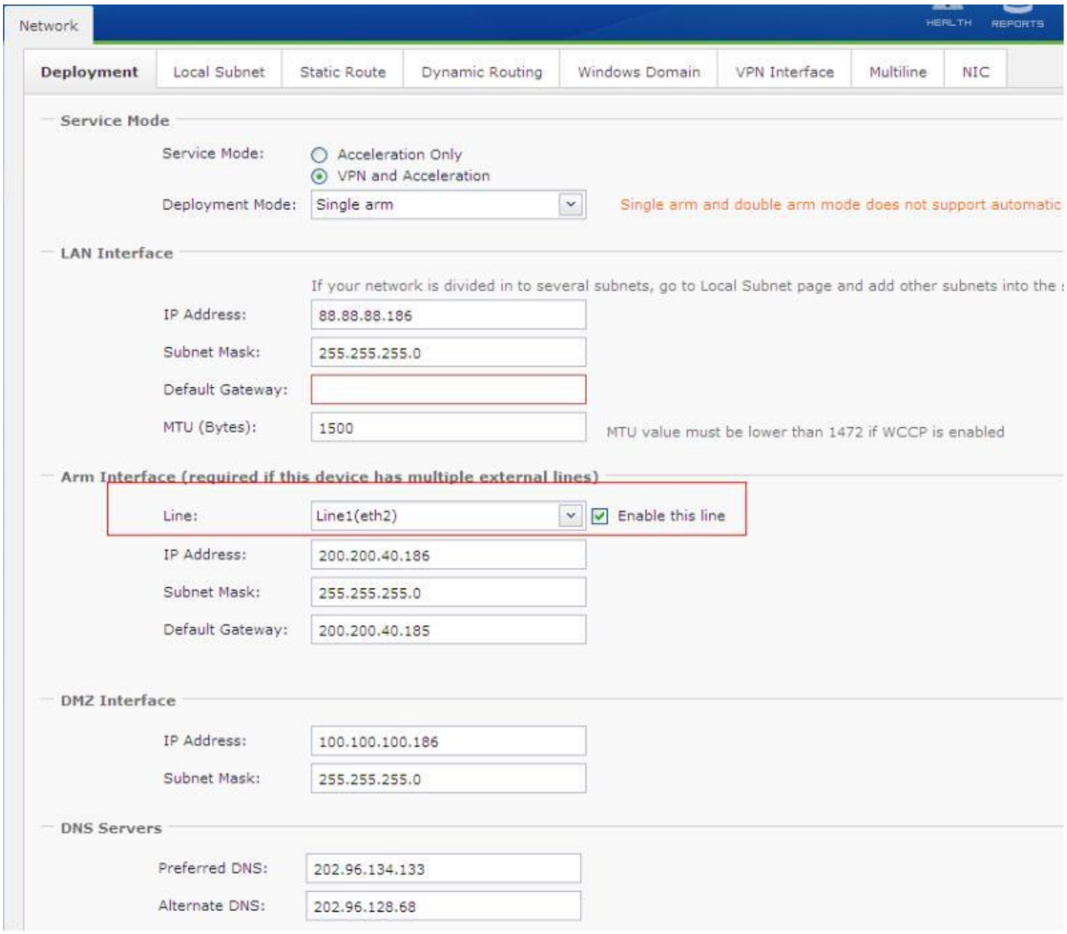
The network topology is as shown in the figure below:



To achieve the above, we need to deploy a front-end firewall or switch to do policy routing based on source IP address, enabling the Sangfor WOC to forward the packets from varying source IP addresses to different outlets of the network.

Besides, perform the following steps to complete the related configuration:

1. Configure deployment mode for the HQ WAN Optimization Controller (WOC). Go to the System > Network > Deployment tab; select service mode VPN and Acceleration and deployment mode Single Arm; configure the LAN interface IP address and two other IP addresses (please be noted that IP addresses configured for the LAN interface must be on a same network segment). The page is as shown below:



Service Mode

Service Mode: ○ Acceleration Only ● VPN and Acceleration

Deployment Mode: Single arm

Single arm and double arm mode does not support automatic

LAN Interface

If your network is divided in to several subnets, go to Local Subnet page and add other subnets into the :

IP Address: 88.88.88.186

Subnet Mask: 255.255.255.0

Default Gateway:

MTU (Bytes): 1500

MTU value must be lower than 1472 if WCCP is enabled

Arm Interface (required if this device has multiple external lines)

Line: Line1(eth2) ☑ Enable this line

IP Address: 200.200.40.186

Subnet Mask: 255.255.255.0

Default Gateway: 200.200.40.185

DMZ Interface

IP Address: 100.100.100.186

Subnet Mask: 255.255.255.0

DNS Servers

Preferred DNS: 202.96.134.133

Alternate DNS: 202.96.128.68

2. Configure multiple lines. Go the System > Network > Multiline tab and add the two Internet lines. For more details, please refer to Configuring Multiline in Chapter 3.
3. Go to the Sangfor VPN > Multiline > Multiline Policy page and configure the corresponding multiline policy
4. Go to the Sangfor VPN > Server > VPN Users tab to apply this policy to a specific user.

You need to configure the front-end firewall to map the port 4009 of the two WAN IP addresses respectively to the binding IP addresses of Arm interface.

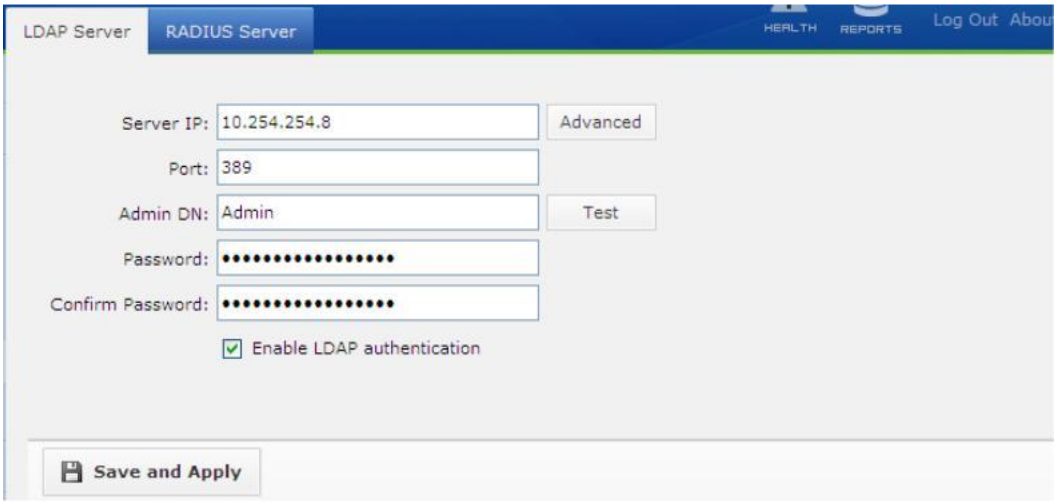
This section only shows how to configure the multiline and multiline policy for the Single-arm WOC, other VPN configurations being ignored.

Configuring LDAP Server

SANGFOR WAN Optimization Controller (WOC) supports the connecting users to be authenticated against a third party LDAP authentication server, so as to enhance the security of the VPN connection.

The VPN service provided by the Sangfor device supports third-party LDAP authentication. If third-party LDAP authentication is required, configure the LDAP server here.

1. Navigate to Sangfor VPN > External Auth Server to enter the LDAP Server page, as shown below:



Server IP: 10.254.254.8

Port: 389

Admin DN: Admin

Password: •••••••••••••••••

Confirm Password: •••••••••••••••••

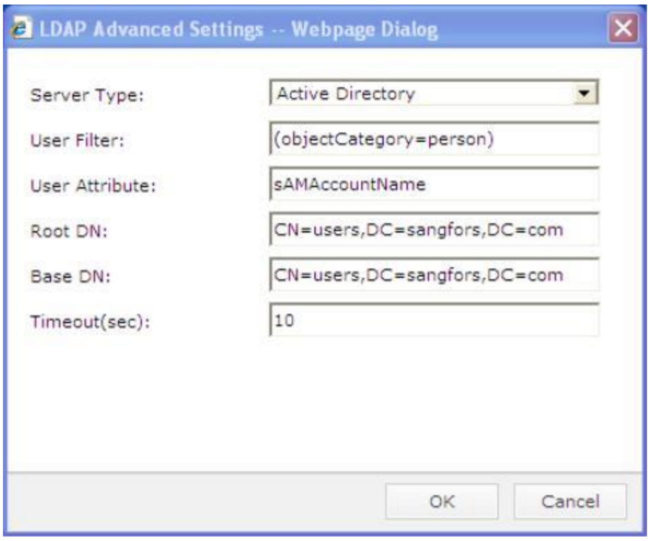
☑ Enable LDAP authentication

2. Specify the basic information of the third-party LDAP server, including server IP address, port, administrator DN and password.

Admin DN field requires the full account name of the domain administrator, for example, Administrator@support.sangfor.com.

3. Select Enable LDAP authentication to enable the third-party LDAP authentication.
4. To configure advanced parameters, click the Advanced button to specify the advanced information.

   Keep the default values for User Filter and User Attribute, and specify Root DN and Base DN according to the your case, as shown in the following figure:



LDAP Advanced Settings -- Webpage Dialog

Server Type: Active Directory

User Filter: (objectCategory=person)

User Attribute: sAMAccountName

Root DN: CN=users,DC=sangfors,DC=com

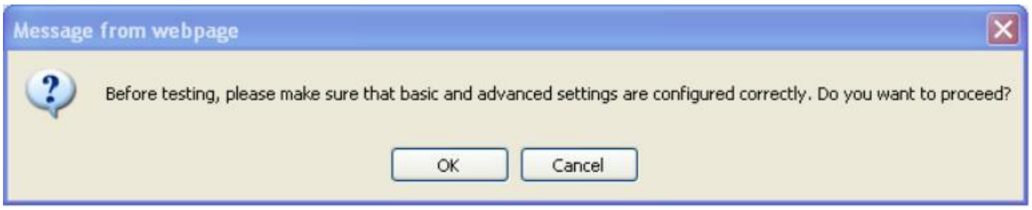
Base DN: CN=users,DC=sangfors,DC=com

Timeout(sec): 10

LDAP authentication only supports Microsoft Active Directory and Novell eDirectory, others such as OpenLDAP unsupported.

Searching and verifying user are performed according to the configured base DN when a user is being authenticated. Only when the base DN is null will the root DN come into use. Importing users is performed based on root DN.

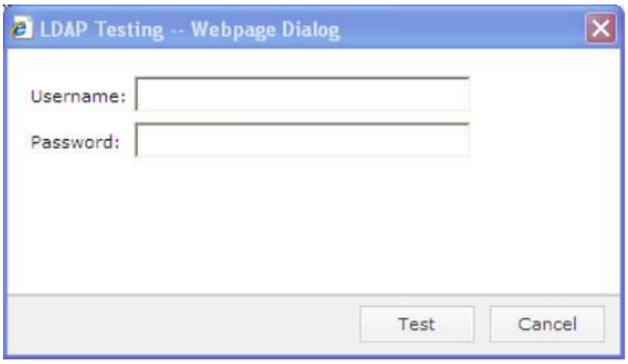
5. To test whether the LDAP server could be connected, click Test and the following prompt appears.



Message from webpage

Before testing, please make sure that basic and advanced settings are configured correctly. Do you want to proceed?

6. Click OK to proceed, and the following dialog appears.



LDAP Testing -- Webpage Dialog

Username:

Password:

7. Enter name and password of a domain user, and then click Test. If the Sangfor device can successfully connect to the LDAP server, the test result will show success.

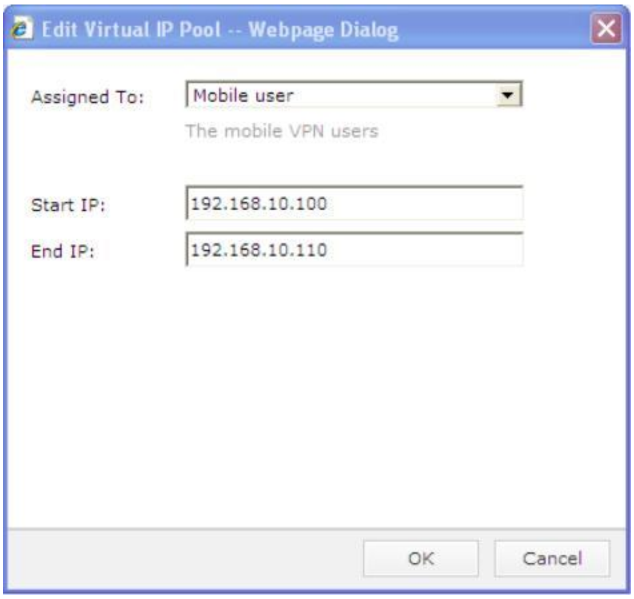
8. Click Save and Apply to save and apply the settings.

Scenario: Mobile VPN User Connects in By Using LDAP Authentication

The customer wants the mobile workers connect in the HQ VPN by using LDAP authentication, to ensure the security of its network.

Detailed configuration procedures are as follows:

1. Go to Sangfor VPN > External Auth Server > LDAP Server to configure the LDAP server.
2. Type in the full name of the domain administrator account (in this example, it is Administrator@support.sangfor.com); configure the attribute of the user (which group it belongs to; in this scenario, it is under group Users), and so type in the information “CN=Users, DC=Sangfor,DC=com” into the Root DN and Base DN fields. If the settings are tested correct, click OK to complete configuring the LDAP server option.
3. Go to the Sangfor VPN > Server > Virtual IP Pool tab to configure virtual IP pool. Click the New button to enter the Edit Virtual IP page. Select user type Mobile user, enter the virtual IP range 192.168.10.100-192.168.10.110, as shown below:



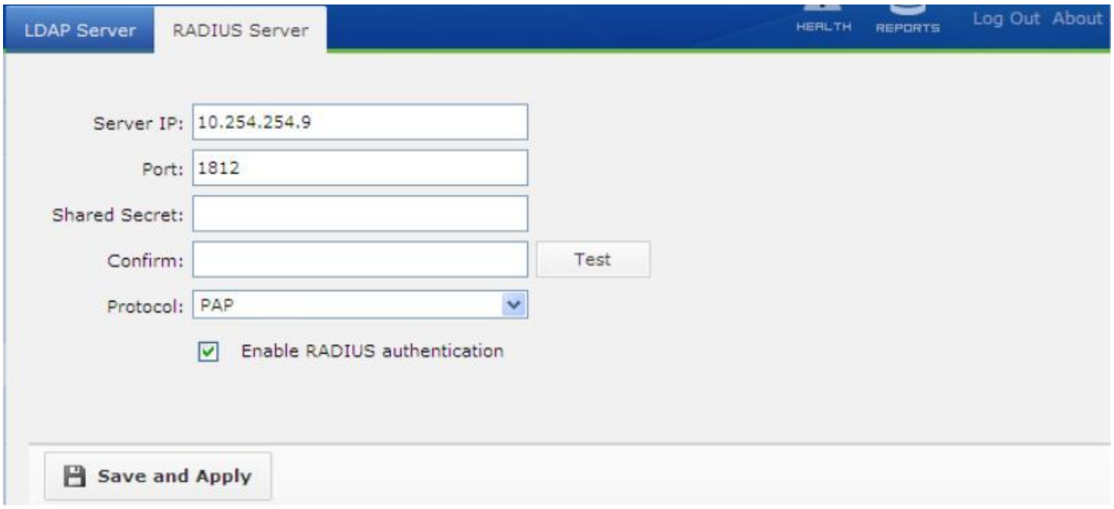
Assigned To: Mobile user
The mobile VPN users
Start IP: 192.168.10.100
End IP: 192.168.10.110

4. Go to the Sangfor VPN > Server > VPN Users tab and click Import From LDAP Server to import users from the LDAP server. The system will automatically upload the users from the configured LDAP server.
5. Select the needed domain users and select user type Mobile user, encryption algorithm, and enable the user, compression and My Network Places.
6. Finally click the Import button.

Configuring RADIUS Server

The VPN service provided by the Sangfor WAN Optimization Controller (WOC) supports third-party RADIUS authentication, Connecting users are authenticated against an external LDAP authentication server. If third-party RADIUS authentication is required, configure RADIUS server (including server IP address, port, shared key and authentication protocol), and then select Enable RADIUS authentication to enable the RADIUS authentication.

Navigate to Sangfor VPN > External Auth Server > RADIUS Server to enter RADIUS Server page, as shown below:

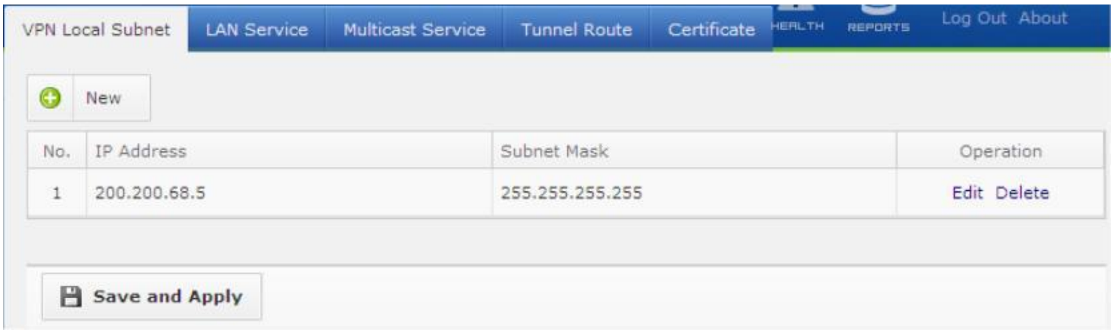


Server IP: 10.254.254.9
Port: 1812
Shared Secret:
Confirm:
Protocol: PAP
☑ Enable RADIUS authentication

Configuring VPN Local Subnet

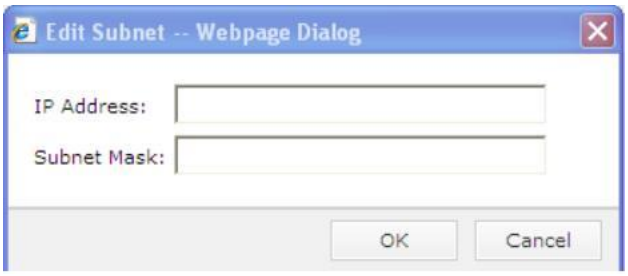
VPN local subnets are used in the situation that the local area network where the Sangfor WAN Optimization Controller (WOC) is located has multiple subnets (exclusive of the network segment where the LAN interface resides), and that the connecting-in VPN users need to access the other LAN subnets.

Navigate to Sangfor VPN > Advanced to enter the VPN Local Subnet page.



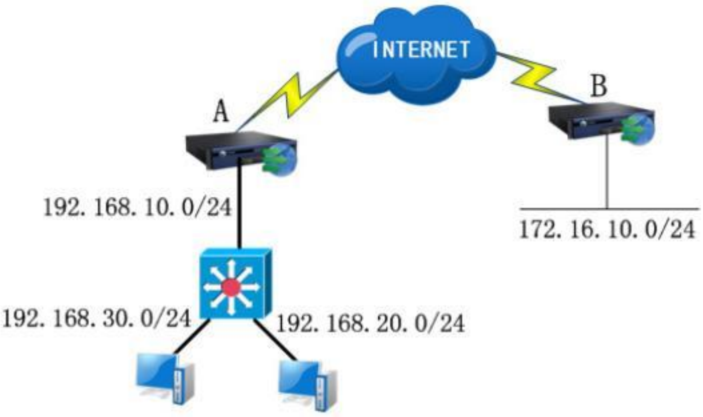
No.	IP Address	Subnet Mask	Operation
1	200.200.68.5	255.255.255.255	Edit Delete

Click the New button to enter the Edit Subnet page. Enter the subnet segment and subnet mask.



Scenario: Allowing VPN User to Access Multiple Local Subnets

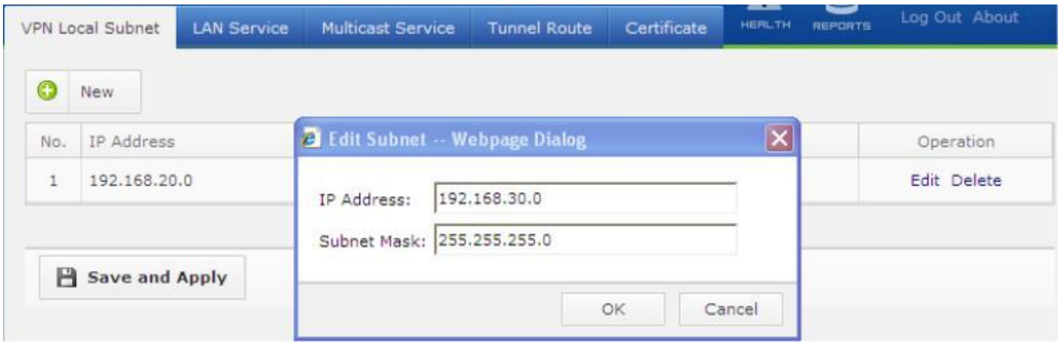
Enterprise network A has three subnets (192.168.10.X, 192.168.20.X and 192.168.30.X). Users in branch office B want to connect to Sangfor WOC device and access the three subnets. Network topology is as shown below:



To meet the needs of this customer, we have to configure VPN local subnet, by Creating the subnets (192.168.20.0/24 and 192.168.30.0/24) and the corresponding static route.

Perform the following steps:

1. Go to the Sangfor VPN > Advanced > VPN Local Subnet tab to add the subnets that branch users need to access, 192.168.20.0/24 and 192.168.30.0/24, as shown below:

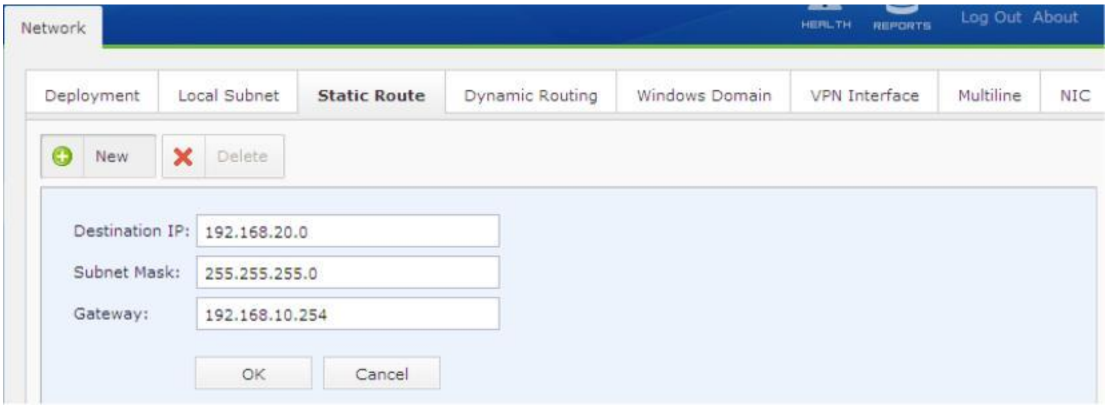


No.	IP Address	Operation
1	192.168.20.0	Edit Delete

IP Address: 192.168.30.0

Subnet Mask: 255.255.255.0

2. Go to System > Network > Static Route tab to configure static routes for the two VPN local subnets respectively, as shown below:



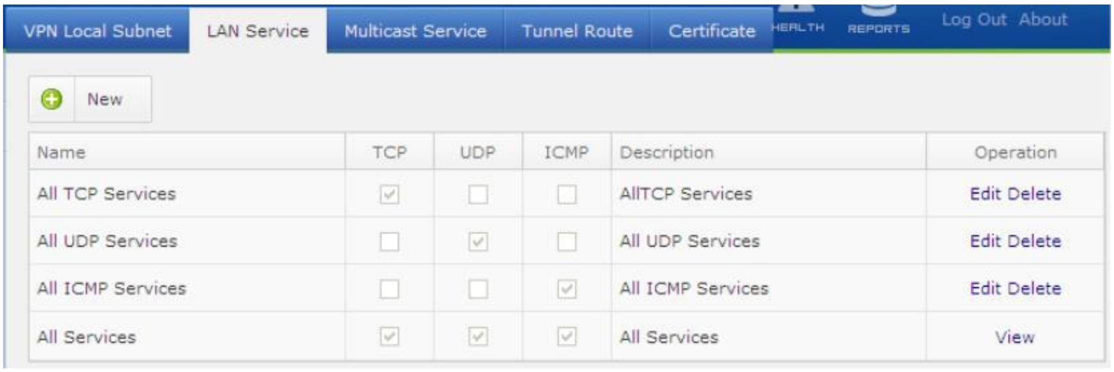
Destination IP: 192.168.20.0
Subnet Mask: 255.255.255.0
Gateway: 192.168.10.254

The branch users then are able to access the three subnets on the HQ network once they establish VPN connect in with it.

The local subnet list stands for a kind of "declaration". The subnets defined here will be taken as VPN network segments by the VPN device and the client-end software. All the data going through the VPN device or software will be encapsulated and transmitted through the VPN tunnels. Therefore, you need to configure the static route, in addition to Creating the related subnets, so as to enable the VPN users to access these subnets.

Configuring LAN Service

The LAN Service page defines the LAN services that may be available to connecting users. By specifying LAN service for users, you can control their access rights after they connect to the local VPN site. You can prevent user from accessing to a specified service provided by a specified computer. For example, allow a user to only access the OA server located at headquarters on port 80 and deny access to any other servers, or only allow one specified user in a branch site to access the SQL server located at headquarters and deny requests from any other IP addresses in the LAN of the branch. Navigate to Sangfor VPN > Advanced > LAN Service to enter the LAN Service page, as shown below:



Name	TCP	UDP	ICMP	Description	Operation
All TCP Services	☑	□	□	AllTCP Services	Edit Delete
All UDP Services	□	☑	□	All UDP Services	Edit Delete
All ICMP Services	□	□	☑	All ICMP Services	Edit Delete
All Services	☑	☑	☑	All Services	View

The LAN services defined here can be referenced in the following two ways to implement LAN service access control:

If the current Sangfor device acts as branch device, reference the LAN services when creating the VPN connection (in Sangfor VPN > Client > VPN Connection > Edit Connection > LAN Service) to specify the services can or cannot be accessed by the users from peer VPN.

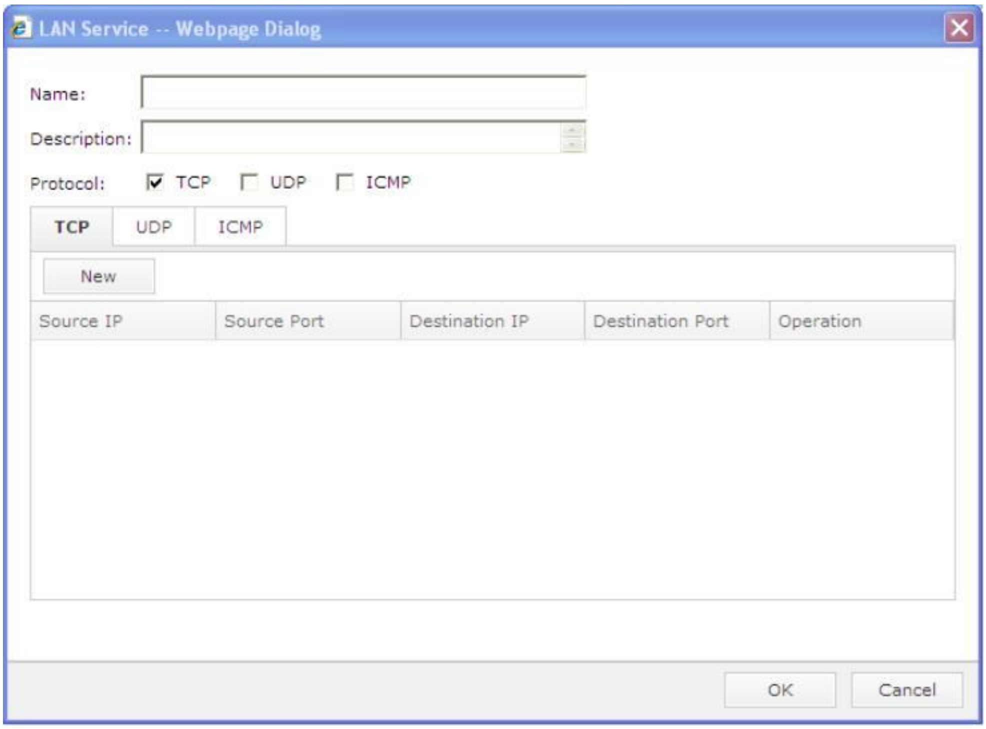
If the current Sangfor device acts as HQ device, reference the LAN services when creating the VPN user account (in Sangfor VPN > Server > VPN Users > Add User/Edit User > LAN Service) to specify the services can or cannot be accessed by the users from peer VPN.

Besides, the LAN services defined here can be referenced by outbound policy and inbound policy (for more information, please refer to Creating Inbound/Outbound Policy (Phase II) in Chapter 9).

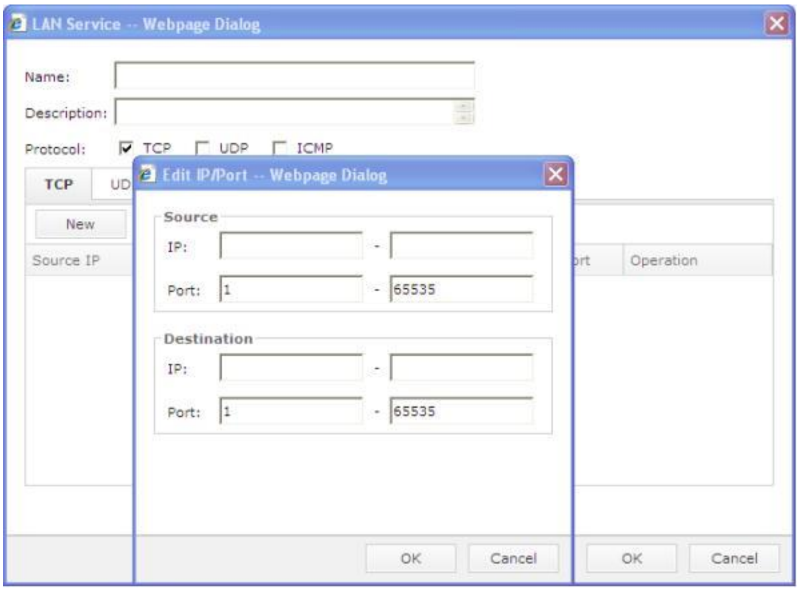
By configuring LAN services and then applying them to specific users to allow/block their accesses, you can achieve secure management in VPN tunnel. By default, the connecting VPN users can access all the LAN services.

Perform the steps below to configure a user’s access rights to the peer WOC:

1. Navigate to Sangfor VPN > Advanced > LAN Service and click the New button to create a LAN service.



2. Select TCP, UDP or ICMP tab according to your case, and click New to specify the IP source address and ports, as shown below:



LAN Service -- Webpage Dialog

Name:

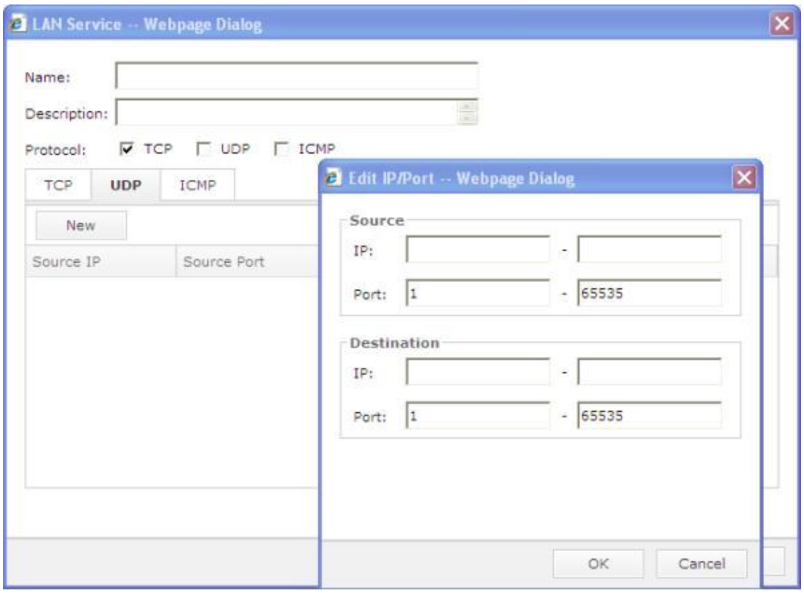
Description:

Protocol: ☑ TCP □ UDP □ ICMP

Edit IP/Port -- Webpage Dialog

Source
IP: -
Port: 1 - 65535

Destination
IP: -
Port: 1 - 65535



LAN Service -- Webpage Dialog

Name:

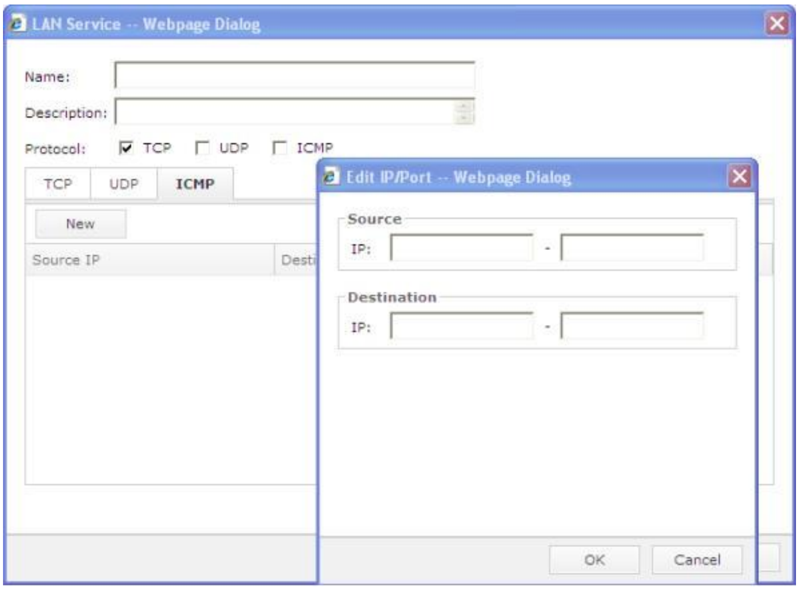
Description:

Protocol: ☑ TCP □ UDP □ ICMP

Edit IP/Port -- Webpage Dialog

Source
IP: -
Port: 1 - 65535

Destination
IP: -
Port: 1 - 65535



LAN Service -- Webpage Dialog

Name:

Description:

Protocol: ☑ TCP □ UDP □ ICMP

Edit IP/Port -- Webpage Dialog

Source
IP: -

Destination
IP: -

If tunnel NAT is applied (that is, the internal subnet of the branch is translated into a virtual subnet), the destination IP addresses here should be the translated virtual subnet instead of its original one. For LAN service configured on the peer device, the source IP addresses should be the translated virtual subnet of the branch.

After performing the above steps, you have just “defined” the LAN service. To have it work, apply it to a specific user and configure whether its access to the current LAN service is allowed/denied

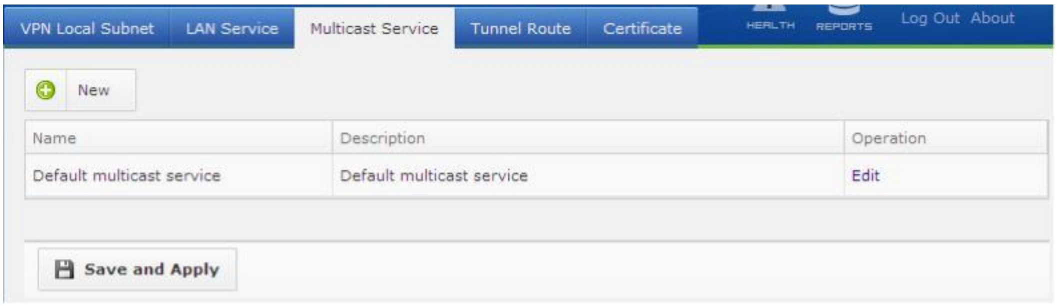
3. Navigate to Sangfor VPN > Server > VPN Users, edit or create a user account to associate the LAN service to a specific user.

Once a user is associated with a LAN service with restricted access right, user can only ping and access the specified server located on the peer network and its access to any other servers will be denied, and vise versa.

Configuring Multicast Service

To meet customers’ needs for some applications such as Voice over IP (VoIP) and video conference, Sangfor device is designed to support multicast services being transmitted among Sangfor VPN tunnels. You can define multicast services here, whose allowable IP range is 224.0.0.1-239.255.255.255 and port range is 1-65535.

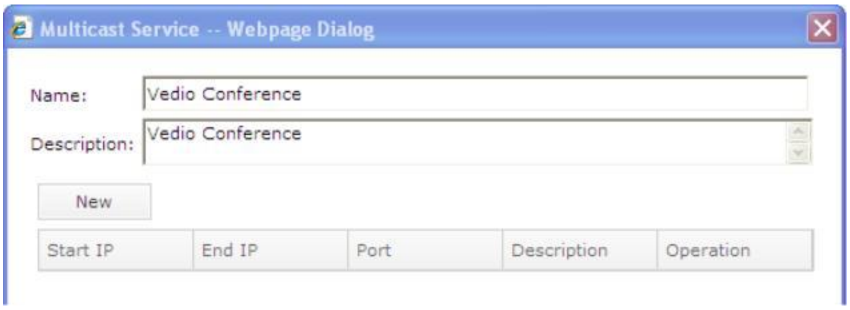
1. Navigate to Sangfor VPN > Advanced > Multicast Service to enter the Multicast Service page, as shown below:



Name	Description	Operation
Default multicast service	Default multicast service	Edit

2. Configure the multicast service.

   a. Click New to enter the Multicast Service page, and then specify the name and description according the specific case, as shown below:

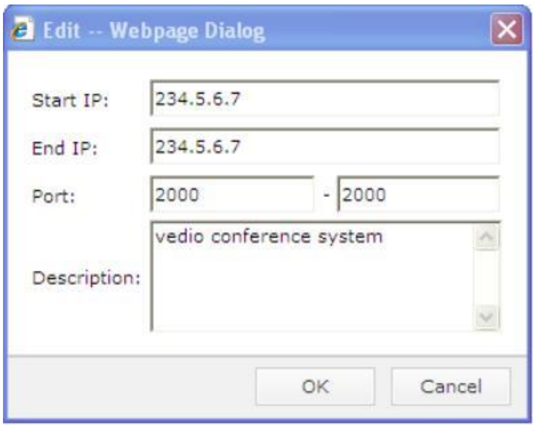


Name: Vedio Conference

Description: Vedio Conference

Start IP	End IP	Port	Description	Operation

b. Click New to configure the applicable IP address range and port range, as shown below:



Start IP: 234.5.6.7

End IP: 234.5.6.7

Port: 2000 - 2000

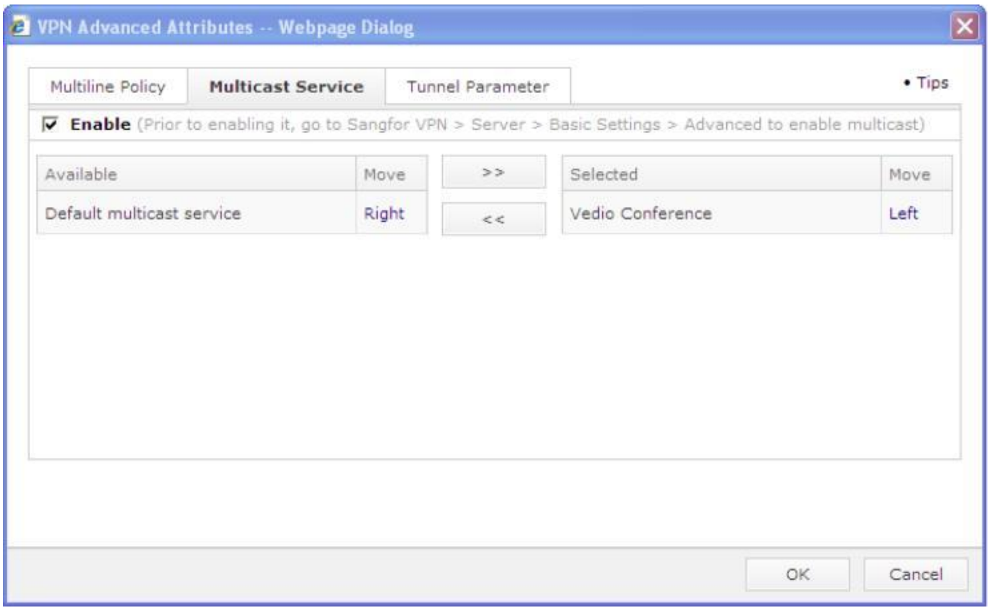
Description: vedio conference system

c. Click OK to save the settings.

3. Apply the configured multicast service to a specific user.

a. Navigate to Sangfor VPN > Server > VPN Users to enter the VPN Users page and then click New User to specify basic information for the user.

b. Click the Advanced button and then click Multicast Service tab. Select Enable and click Right to move the Video Conference service into the selected list, as shown below:



☑ **Enable** (Prior to enabling it, go to Sangfor VPN > Server > Basic Settings > Advanced to enable multicast)

Available	Move
Default multicast service	Right

Selected	Move
Vedio Conference	Left

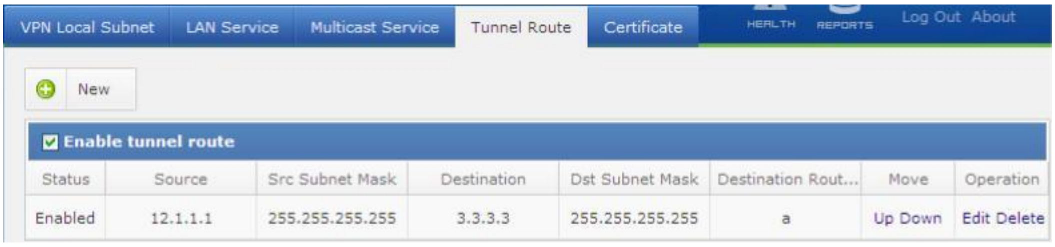
c. Click Save.

To have the multicast service work, you need to go to Sangfor VPN > Server > Basic Settings > Advanced to enable multicast.

Configuring Tunnel Route

The Sangfor WOC provides powerful routing function in VPN tunnel, by which, you can easily achieve interconnection among multiple VPN sites (software or hardware), forming a “web-like” VPN network.

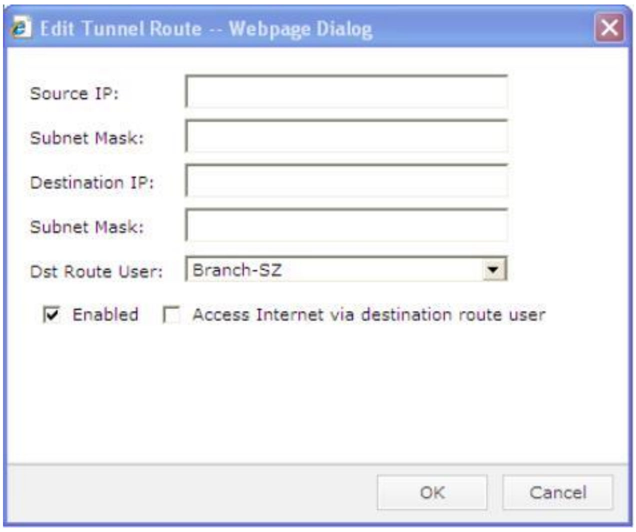
1. Navigate to Sangfor VPN > Advanced > Tunnel Route to enter the Tunnel Route page, as shown below:



☑ Enable tunnel route

Status	Source	Src Subnet Mask	Destination	Dst Subnet Mask	Destination Rout...	Move	Operation
Enabled	12.1.1.1	255.255.255.255	3.3.3.3	255.255.255.255	a	Up Down	Edit Delete

2. Click Add to open the following dialog.



Source IP:

Subnet Mask:

Destination IP:

Subnet Mask:

Dst Route User: Branch-SZ

☑ Enabled ☐ Access Internet via destination route user

3. Specify the following information.

Source IP, Subnet Mask: Enter the source subnet (IP address/netmask) of the tunnel route.

Destination IP, Subnet Mask: Enter destination subnet (IP address/netmask) of the route.

Dst Route User: This option indicates the user that has been used to establish VPN connection with the HQ VPN device. It determines to which Sangfor device the packets applicable to this tunnel route will be forwarded, that is, the next hop of this tunnel route. For example, suppose Branch A has established VPN connection with Branch B using the user account Test. If Branch A's employees want to access Branch C through Branch B, the tunnel route configured on Branch A's VPN device should use the destination route user Test.

Enabled: Select it to enable this tunnel route.

Access Internet via destination route user: If this option is selected, all the Internet traffic going through this device will be forwarded to the HQ VPN device through the VPN connection established using the destination route user and then to the Internet.

⚠

To access Internet via destination route user (that is, to enable Access Internet via dst route user), the remote Sangfor WOC must be deployed in Gateway mode, and the local WOC in Gateway or Single arm mode.

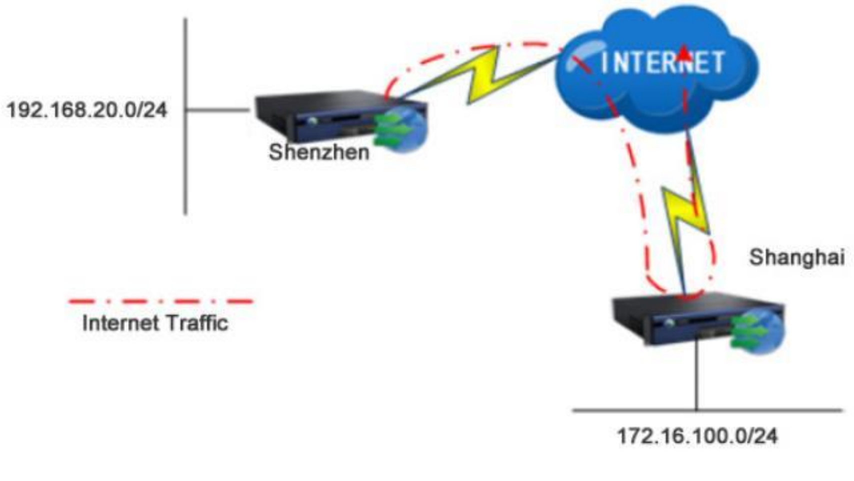
Before creating tunnel route, make sure that a user has been created in Sangfor > Server > VPN Users which can act as destination route user.

The configured tunnel routes take higher precedence to the static routes learned by system. Incorrect tunnel route will disable communication between two terminals over VPN tunnel.

4. Click Save and Apply to save the settings.

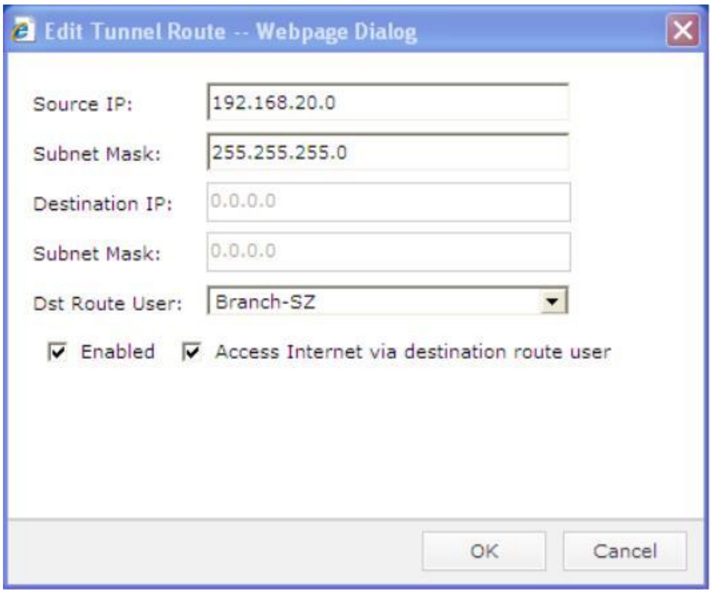
Scenario: Creating Tunnel Route to Allow VPN Access between Branch Offices

One of the features of tunnel NAT is forwarding the Internet access data from branches to server-end WOC which acts as the egress to the Internet.



As shown on the above figure, to forward the data from the branch Shenzhen (192.168.20.0/24) to the server-end WOC Shanghai (172.16.100.0/24), you need to perform the following steps on the Shenzhen WOC.

1. Log in to the administrator console of Shenzhen WOC and go to Sangfor VPN > Advanced > Tunnel Route to create a tunnel route, as shown in the figure below:

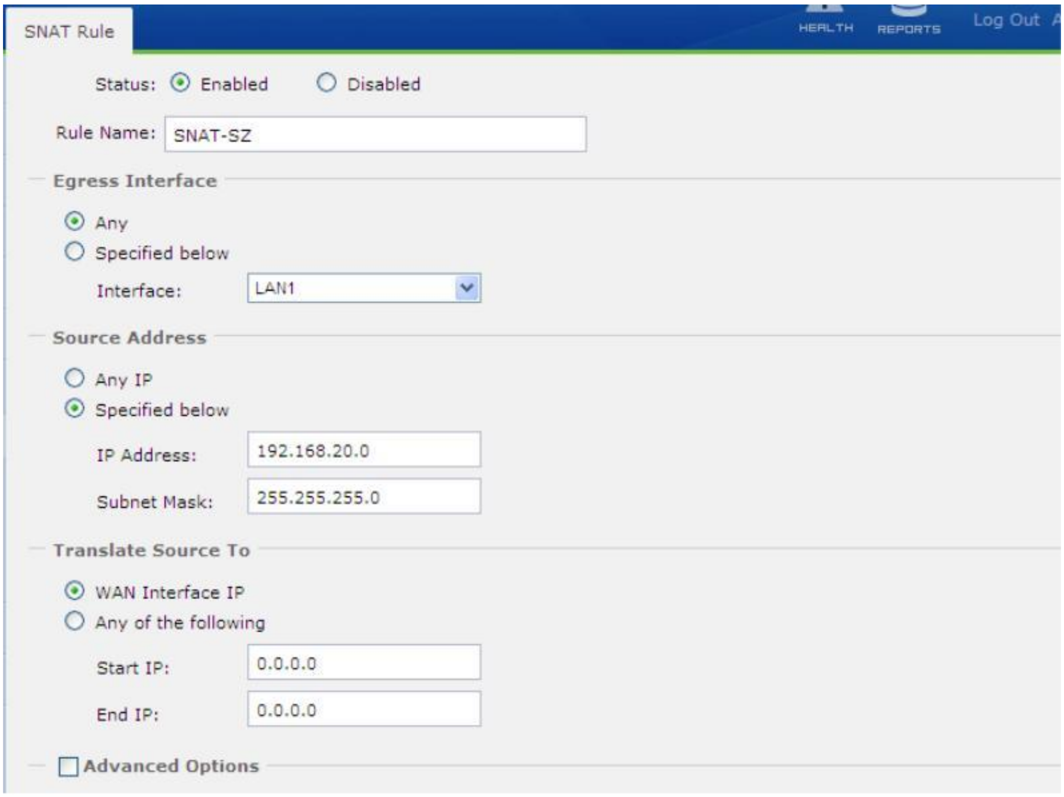


Edit Tunnel Route -- Webpage Dialog

Source IP: 192.168.20.0
Subnet Mask: 255.255.255.0
Destination IP: 0.0.0.0
Subnet Mask: 0.0.0.0
Dst Route User: Branch-SZ

☑ Enabled ☑ Access Internet via destination route user

2. Log in to administrator console of Shanghai WOC and go to Firewall > NAT > SNAT Rule to add source network address translation rule for the data packet coming from Shenzhen, as shown in the figure below:



Status: ● Enabled ○ Disabled
Rule Name: SNAT-SZ

Egress Interface
● Any
○ Specified below
Interface: LAN1

Source Address
○ Any IP
● Specified below
IP Address: 192.168.20.0
Subnet Mask: 255.255.255.0

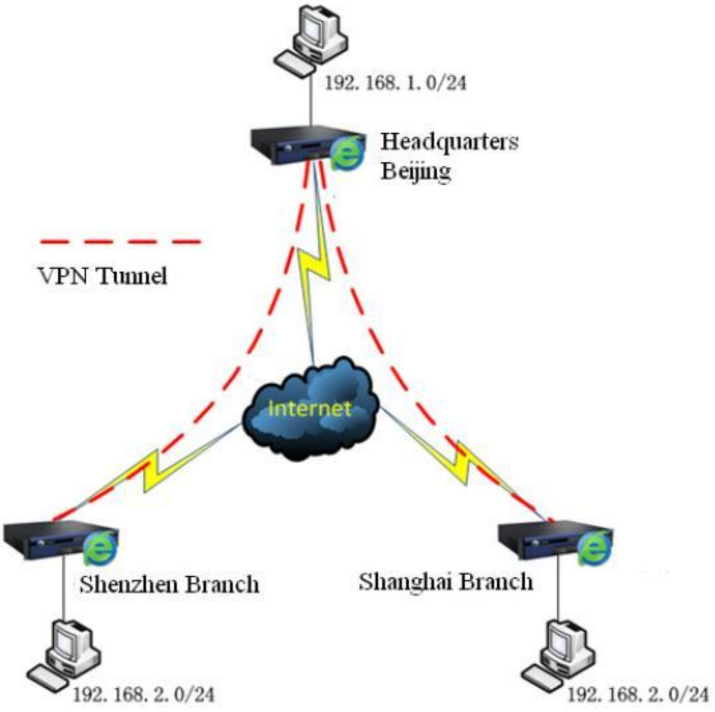
Translate Source To
● WAN Interface IP
○ Any of the following
Start IP: 0.0.0.0
End IP: 0.0.0.0

□ Advanced Options

Configuring Tunnel NAT

Tunnel NAT is NAT (network address translation) on VPN tunnel, which can prevent IP addresses of varying remote Sangfor WOCs from conflicting. It enables branch VPN users to connect in and communicate smoothly with the HQ VPN site, without modifying IP addresses.

Suppose the HQ Beijing (192.168.1.0/24) network is deployed with a Sangfor WOC, in Route mode. Hosts in Shanghai branch office (192.168.2.0/24) and Shenzhen branch office (192.168.2.0/24) want to connect to HQ Beijing through VPN tunnel. The network topology is as shown in the figure below:



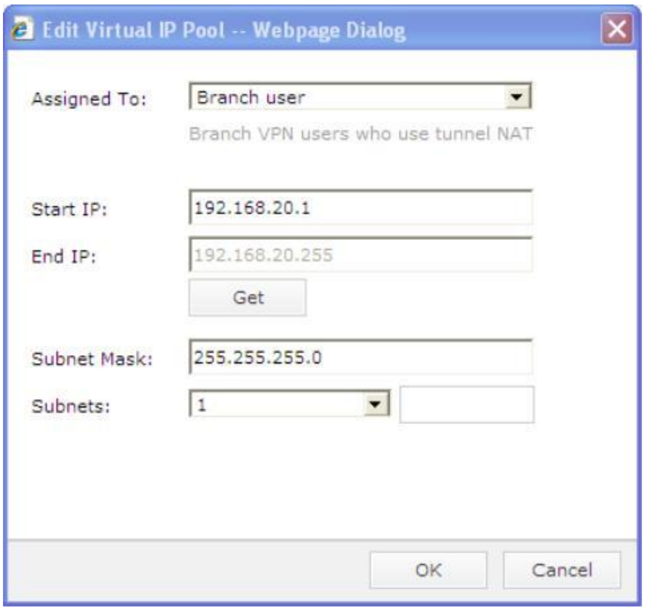
As the subnets of the two branch offices are the same, IP address conflict will occur and connection may fail if they connect to Headquarters (HQ) at the same time. To avoid that situation, ensure the following:

Define a virtual IP pool for one of the branch offices

Enable the tunnel NAT function and configure a tunnel NAT rule to translate the source address on one branch office into a different virtual IP address.

Perform the following steps to ensure the above:

1. Configure the HQ WOC and navigate to Sangfor VPN > Server > Virtual IP Pool to add a virtual IP pool for branch users, as shown below:



Edit Virtual IP Pool -- Webpage Dialog

Assigned To: Branch user

Branch VPN users who use tunnel NAT

Start IP: 192.168.20.1

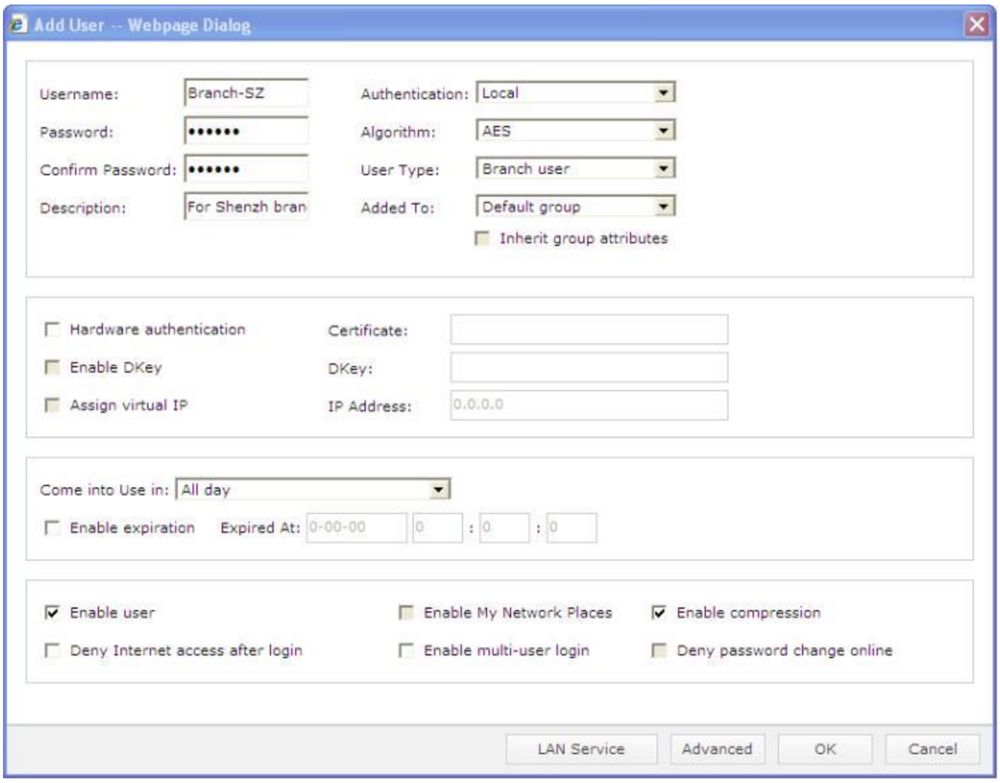
End IP: 192.168.20.255

Subnet Mask: 255.255.255.0

Subnets: 1

2. Navigate to Sangfor VPN > Server > Users to create an account for the device in Shenzhen branch office.

   a. Click New User and specify the basic user information, as shown below:



Add User -- Webpage Dialog

Username: Branch-SZ

Password: ••••••

Confirm Password: ••••••

Description: For Shenzh bran

Authentication: Local

Algorithm: AES

User Type: Branch user

Added To: Default group

□ Inherit group attributes

□ Hardware authentication

□ Enable DKey

□ Assign virtual IP

Certificate:

DKey:

IP Address: 0.0.0.0

Come into Use in: All day

□ Enable expiration

Expired At: 0-00-00 0 : 0 : 0

☑ Enable user

□ Deny Internet access after login

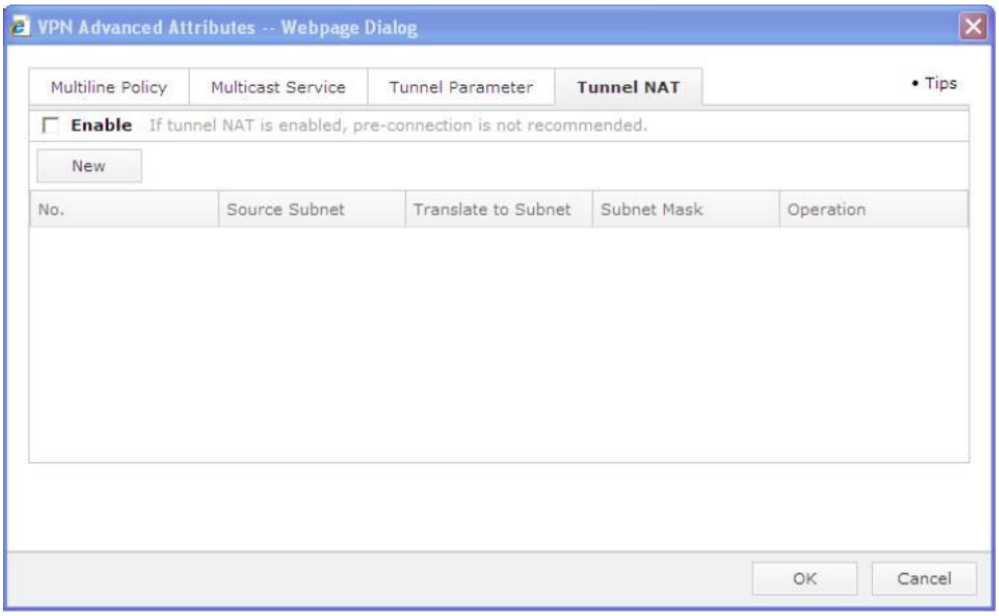
□ Enable My Network Places

□ Enable multi-user login

☑ Enable compression

□ Deny password change online

   b. Click Advanced and click Tunnel NAT tab, as shown below:



VPN Advanced Attributes -- Webpage Dialog

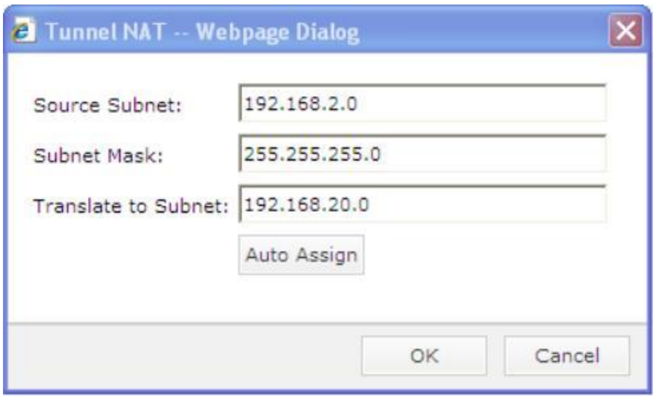
Multiline Policy | Multicast Service | Tunnel Parameter | **Tunnel NAT** | • Tips

□ **Enable** If tunnel NAT is enabled, pre-connection is not recommended.

New

No.	Source Subnet	Translate to Subnet	Subnet Mask	Operation

c. Check Enable to enable tunnel NAT and then click New. Set Source Subnet/Netmask to 192.168.2.0/255.255.255.0 (subnet on the branch office) and Translate to Subnet to 192.168.20.0 (virtual subnet to which the branch subnet will be translated, configured in step 1), as shown below:



Tunnel NAT -- Webpage Dialog

Source Subnet: 192.168.2.0

Subnet Mask: 255.255.255.0

Translate to Subnet: 192.168.20.0

Source subnet and subnet mask must be matching.

Only the network number portion of the subnet will be translated. Host number will remain unchanged.

For the Translate to Subnet field, enter the subnet or click Auto Assign to have the Sangfor WOC calculate and get a subnet from the virtual IP pool.

3. Click the OK buttons to save the settings.

The users in both Shenzhen and Shanghai branch offices then can access Headquarters Beijing through VPN connections, without changing their original IP address settings. Meanwhile, users in Beijing can access the services provided by the two branch offices, Shenzhen branch by accessing the 192.168.20.0/24 subnet and Shanghai branch by accessing the 192.168.2.0/24 subnet.

However, in the above case, the Shenzhen and Shanghai branch offices cannot access each other. To allow mutual access between the two branch offices, the following should be ensured on both Shenzhen and Shanghai WOCs:

Enable the tunnel NAT and configure a tunnel NAT rule to translate the other site's subnet into a different one (the translated-to subnets of the two sites should be different)

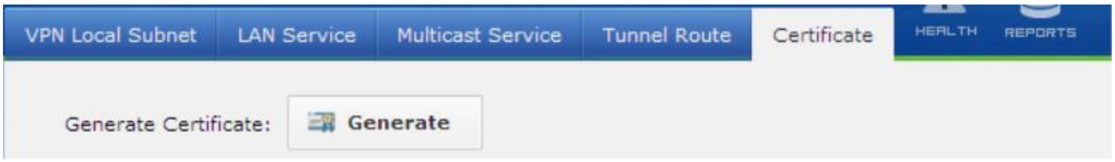
Add a tunnel route, source IP being the original subnet of the other site and destination IP being its translated virtual subnet (specified in tunnel NAT rule)

Generating Certificate

The hardware-feature-based certificate authentication is one of the patents owned by Sangfor. The SSL VPN hardware device as well as the Sangfor VPN software adopts this technology for identity authentication among different VPN nodes.

The certificate is generated based on some hardware features (such as network adapter and hard disk) of the Sangfor device or the computer that has installed the Sangfor VPN software. The uniqueness of the hardware feature makes the certificate unique and unforgeable. By authenticating the device based on the hardware feature, it ensures that only the specified device is allowed to connect to the network, avoiding potential security hazards.

Navigate to Sangfor VPN > Advance > Certificate to enter the Generate Certificate page, as shown below:

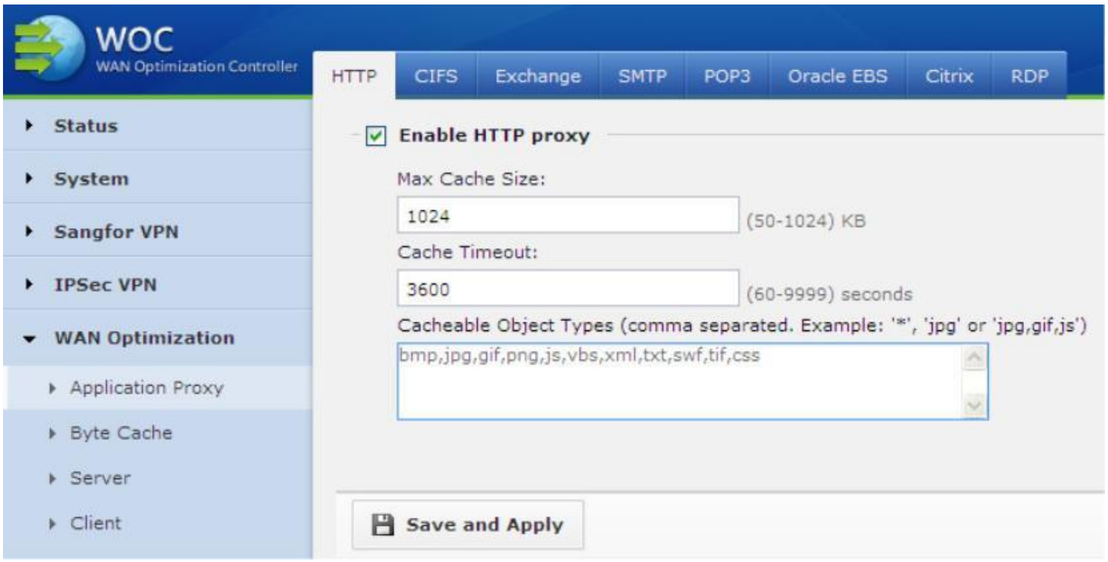


To generate a certificate for the current device, click Generate Certificate and then select a location to generate and save the certificate into the local computer, as shown below:

After the certificate is generated, send it to the administrator of the HQ VPN device, who will then select the hardware authentication and bind this certificate with the user account when creating the user account for this device.

Chapter 5 WAN Optimization

WAN Optimization is a section configuring acceleration/optimization related features, including but not limited to application proxy, Byte Cache, setting up inbound acceleration connection from remote WOC hardware or PACC (Potable Acceleration) client software and outbound acceleration connection.



☑ Enable HTTP proxy

Max Cache Size: 1024 (50-1024) KB

Cache Timeout: 3600 (60-9999) seconds

Cacheable Object Types (comma separated. Example: '*', 'jpg' or 'jpg,gif,js')

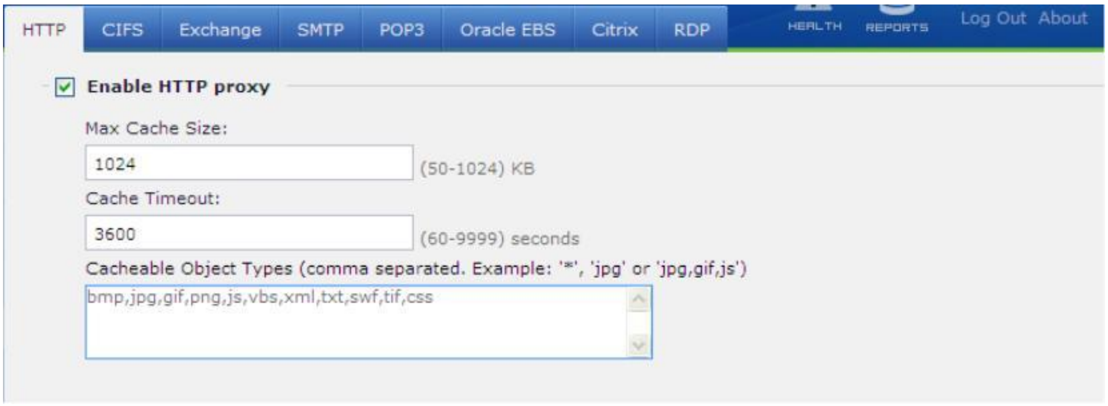
bmp,jpg,gif,png,js,vbs,xml,txt,swf,tif,css

Application Proxy

Sangfor WAN Optimization Controller (WOC) supports HTTP proxy, CIFS proxy, SMTP proxy, POP3 proxy, Exchange proxy, Oracle EBS, Citrix and RDP optimization.

HTTP Proxy

Navigate to WAN Optimization > HTTP to enable and configure HTTP proxy, as shown below:



☑ Enable HTTP proxy

Max Cache Size: 1024 (50-1024) KB

Cache Timeout: 3600 (60-9999) seconds

Cacheable Object Types (comma separated. Example: '*', 'jpg' or 'jpg,gif,js')

bmp,jpg,gif,png,js,vbs,xml,txt,swf,tif,css

The following are the contents included on the HTTP page:

Enable HTTP proxy: Select this option to enable HTTP proxy.

Max. Cache Size: Configures the upper size limit of the object type file.

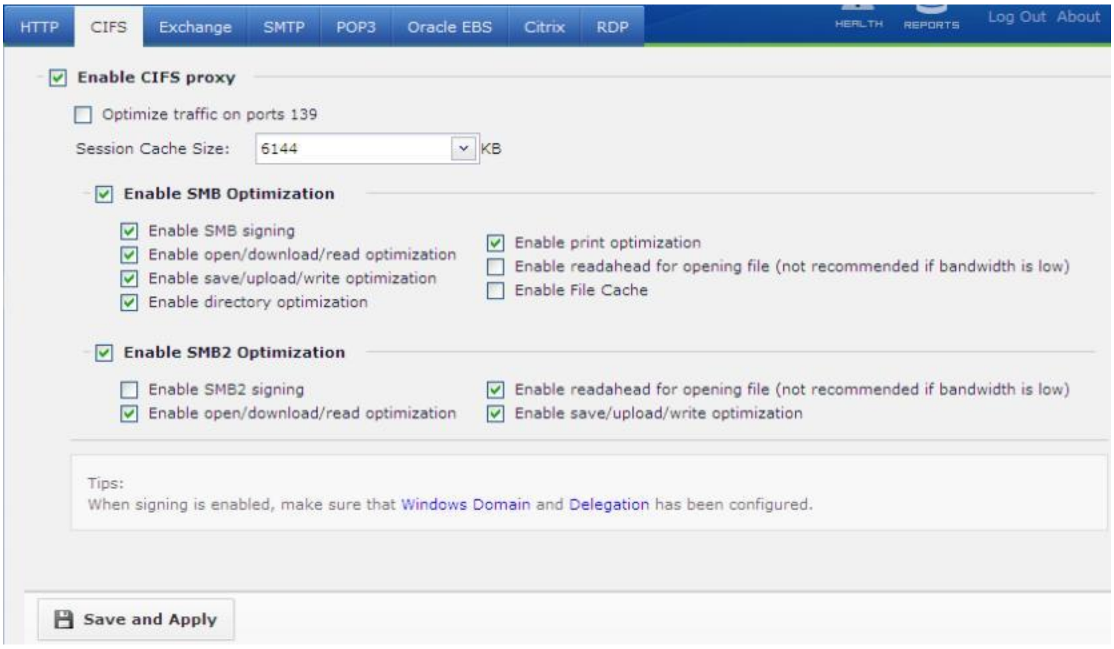
Object Timeout: Configures the timeout of caching object file.

Cacheable Object Types: Configures the HTTP object types that can be cached by the Sangfor WAN WOC. The default image file types are bmp, jpg, gif; the default script file type is js.

Save and Apply: Having completed configuring the page, click this button to save and apply the changes.

CIFS Proxy

Navigate to WAN Optimization > CIFS to enable and configure CIFS proxy, as shown below:



☑ Enable CIFS proxy

□ Optimize traffic on ports 139

Session Cache Size: 6144 KB

☑ Enable SMB Optimization

☑ Enable SMB signing
☑ Enable open/download/read optimization
☑ Enable save/upload/write optimization
☑ Enable directory optimization
☑ Enable print optimization
□ Enable readahead for opening file (not recommended if bandwidth is low)
□ Enable File Cache

☑ Enable SMB2 Optimization

□ Enable SMB2 signing
☑ Enable open/download/read optimization
☑ Enable readahead for opening file (not recommended if bandwidth is low)
☑ Enable save/upload/write optimization

Tips:
When signing is enabled, make sure that Windows Domain and Delegation has been configured.

The following are the contents included on the CIFS page:

Enable CIFS proxy: Select this option to enable CIFS proxy.

Optimize traffic on port 139: Select this option if My Network Places optimization is not working properly or effect is not good.

Enable SMB signing: Select this option to enable SMB signing.

Enable open/download/read optimization: Select this option so that file opening, download and reading from CIFS server can be optimized.

Enable save/upload/write optimization: Select this option so that file saving, writing from CIFS server can be optimized.

Enable directory optimization: Select this option to optimize access to folder.

Enable print optimization: Select this option to optimize printing.

Enable readahead for opening file (not recommended if bandwidth is low): Select this option so that the file can be read before being opened.

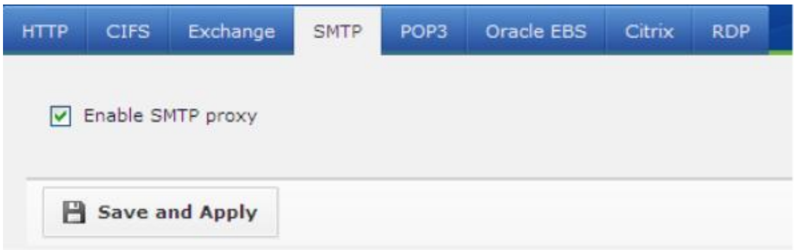
Enable File Cache: Select this option if you want the files downloaded through My Network Places be saved on the WOC for a long time. This feature will save bandwidth if the same file need to be accessed by a great deal of users, for the file is available on the local WOC. What should be noted is that the file cannot be the type that needs regular update; otherwise, subsequent users will download the outdated file. This option is unselected by default.

Session Cache Size: Configures the size of cache object in one session. The higher the value is, the better the acceleration effect would be.

Save and Apply: Having completed configuring the page, click this button to save and apply the changes.

SMTP Proxy

Navigate to WAN Optimization > SMTP to enable and configure SMTP proxy, as shown below:

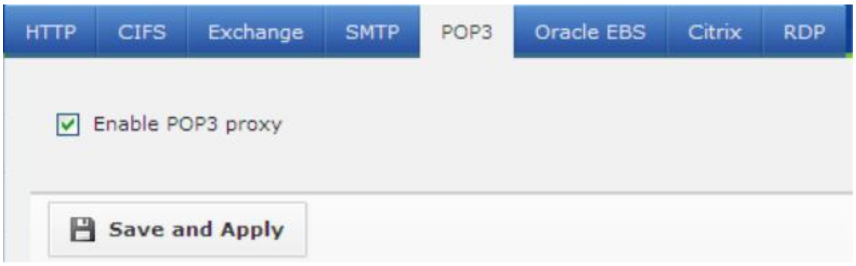


☑ Enable SMTP proxy

Select Enable SMTP proxy option to enable SMTP proxy and click Save and Apply button to save and apply the changes.

POP3 Proxy

Navigate to WAN Optimization > POP3 to enable and configure POP3 proxy, as shown below:

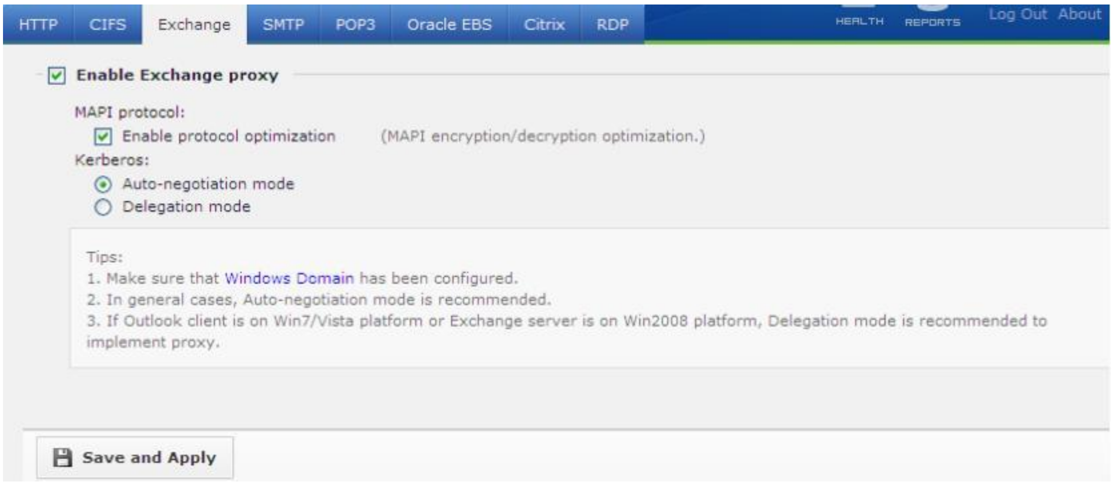


☑ Enable POP3 proxy

Select the Enable POP3 proxy option to enable the POP3 proxy and click the Save and Apply button to save and apply the changes.

Exchange Proxy

Navigate to WAN Optimization > Exchange to enable and configure the EXCHANGE proxy, as shown below:



☑ Enable Exchange proxy

MAPI protocol:

☑ Enable protocol optimization (MAPI encryption/decryption optimization.)

Kerberos:

● Auto-negotiation mode

○ Delegation mode

Tips:
1. Make sure that Windows Domain has been configured.
2. In general cases, Auto-negotiation mode is recommended.
3. If Outlook client is on Win7/Vista platform or Exchange server is on Win2008 platform, Delegation mode is recommended to implement proxy.

Save and Apply

The following are the contents included on the Exchange page:

Enable Exchange proxy: Select this option to enable the Exchange proxy.

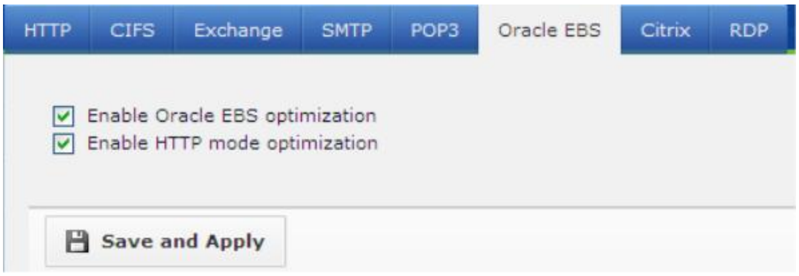
MAPI protocol: It is abbreviation of Messaging Application Programming Interface. Select Enable protocol optimization to optimize encryption and decryption of MAPI data.

Kerberos: This is an authentication method applied to communication between EXCHANGE server and client. Select Auto-negotiation mode or Delegation mode to optimize the process of authentication under the corresponding mode. Auto-negotiation mode is the default setting.

Save and Apply: Having completed configuring the page, click this button to save and apply the changes.

Oracle EBS Optimization

Navigate to WAN Optimization > Oracle EBS, as shown below:



☑ Enable Oracle EBS optimization

☑ Enable HTTP mode optimization

Save and Apply

The following are the contents included on the Oracle EBS page:

Enable Oracle EBS optimization: Select this option to enable Oracle EBS optimization.

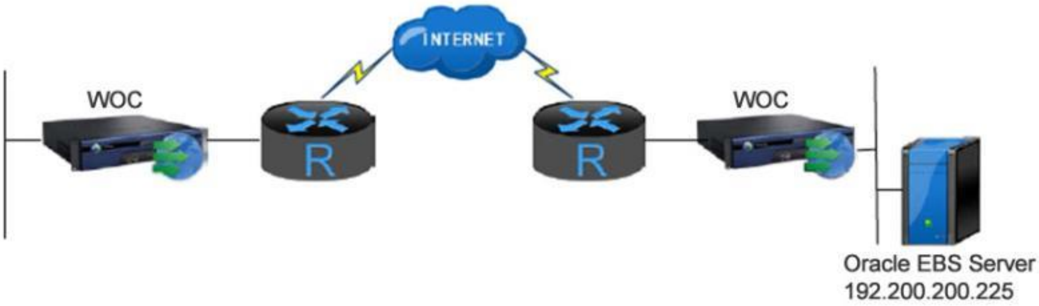
Enable HTTP mode optimization: Select this option to optimize Oracle EBS running in HTTP mode.

Oracle EBS supports connection modes such as HTTP, HTTPS, SOCKET and so on. However, Sangfor WAN Optimization Controller (WOC) only optimizes Oracle EBS running in SOCKET mode initially; if you want to optimize Oracle EBS running in HTTP mode, select Enable HTTP mode optimization; otherwise, Oracle EBS running in HTTP mode will not be optimized.

Save and Apply: Click this button to save and apply the changes.

Scenario: Accelerating HTTP/HTTPS Access to Oracle EBS

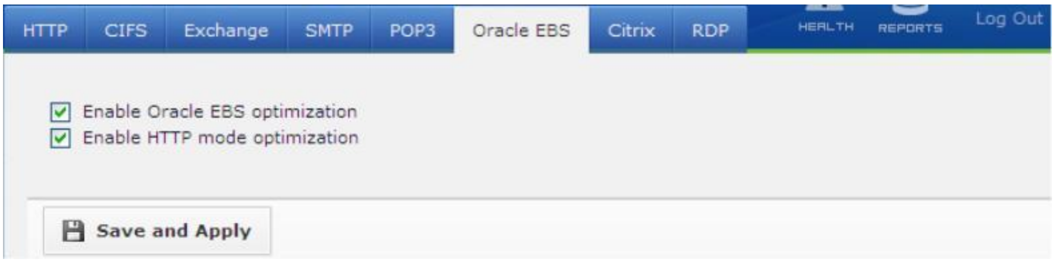
Oracle EBS server (192.200.200.225) is on the HQ network, as shown in the figure below:



To acceleration the access to the Oracle EBS server, perform the following steps on the server-end Sangfor WOC:

1. Ensure the two WOCs can access each other, and the request from client-end users goes through the server-end WOC.

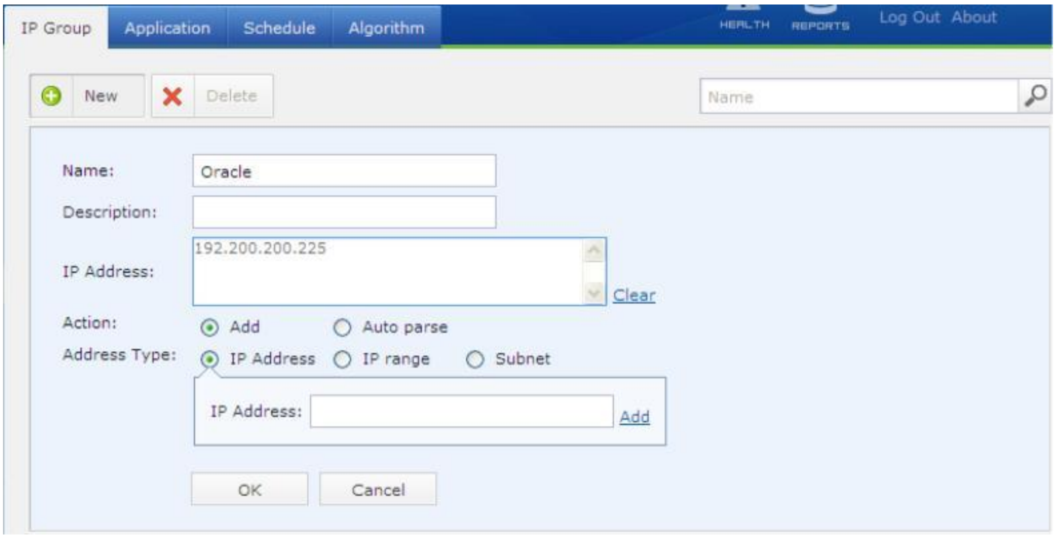
2. Go to the WAN Optimization > Application Proxy > Oracle EBS tab and select the options Enable Oracle EBS optimization and Enable HTTP mode optimization, as shown below:



☑ Enable Oracle EBS optimization
☑ Enable HTTP mode optimization

3. Go to the System > Objects > IP Group tab to add the IP address of the Oracle server, as

shown below:



Name: Oracle

Description:

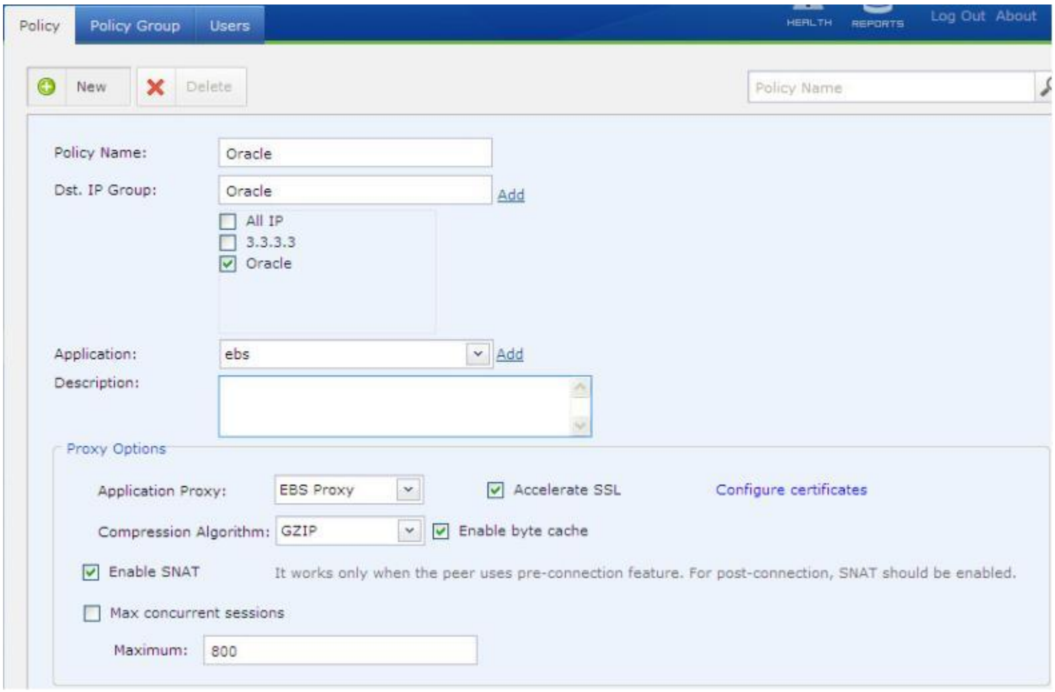
IP Address: 192.200.200.225

Action: ● Add ○ Auto parse

Address Type: ● IP Address ○ IP range ○ Subnet

IP Address:

4. Go to the WAN Optimization > Server > Policy and create an acceleration policy, as shown below:



Policy Name: Oracle

Dst. IP Group: Oracle

□ All IP
□ 3.3.3.3
☑ Oracle

Application: ebs

Description:

Application Proxy: EBS Proxy ☑ Accelerate SSL

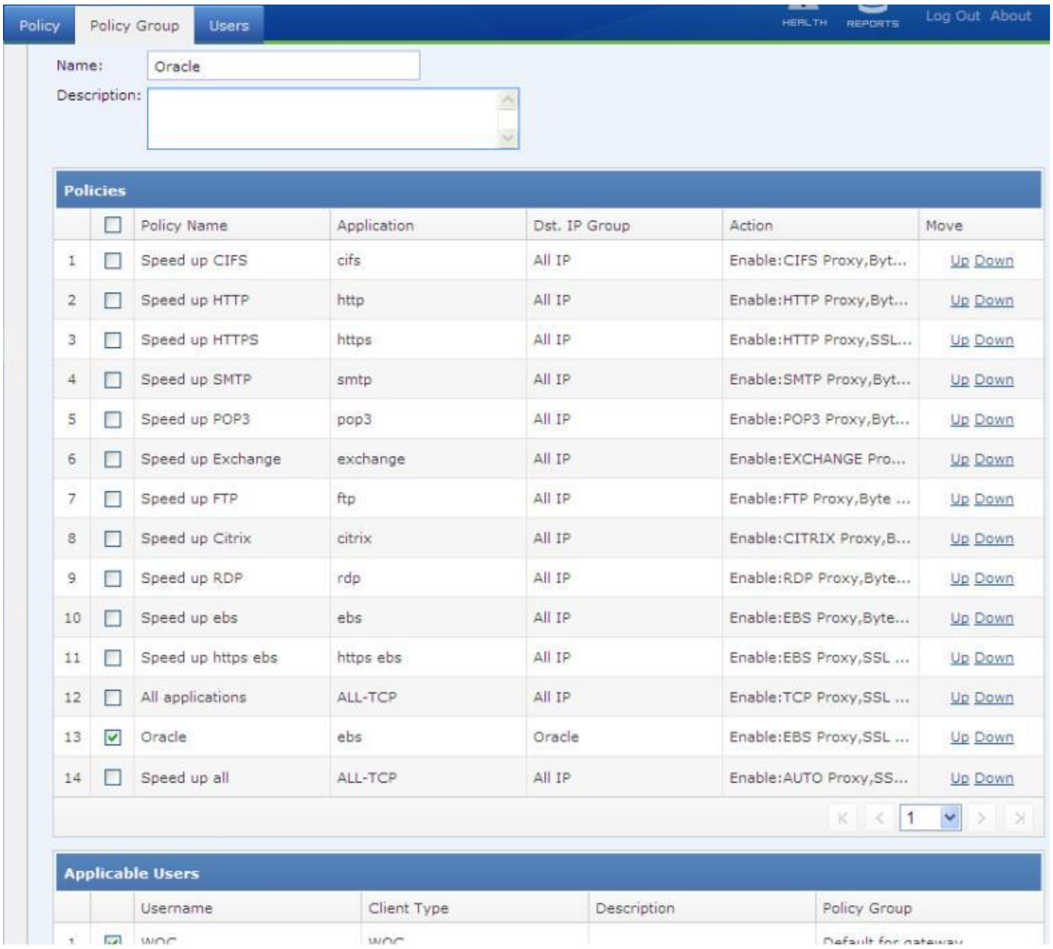
Compression Algorithm: GZIP ☑ Enable byte cache

☑ Enable SNAT It works only when the peer uses pre-connection feature. For post-connection, SNAT should be enabled.

□ Max concurrent sessions

Maximum: 800

5. Go to the WAN Optimization > Server > Policy Group and create a new acceleration policy group and associate it with the corresponding branch user, as shown below:



Name: Oracle

Description:

Policies

	□	Policy Name	Application	Dst. IP Group	Action	Move
1	□	Speed up CIFS	cifs	All IP	Enable:CIFS Proxy,Byt...	Up Down
2	□	Speed up HTTP	http	All IP	Enable:HTTP Proxy,Byt...	Up Down
3	□	Speed up HTTPS	https	All IP	Enable:HTTP Proxy,SSL...	Up Down
4	□	Speed up SMTP	smtp	All IP	Enable:SMTP Proxy,Byt...	Up Down
5	□	Speed up POP3	pop3	All IP	Enable:POP3 Proxy,Byt...	Up Down
6	□	Speed up Exchange	exchange	All IP	Enable:EXCHANGE Pro...	Up Down
7	□	Speed up FTP	ftp	All IP	Enable:FTP Proxy,Byte ...	Up Down
8	□	Speed up Citrix	citrix	All IP	Enable:CITRIX Proxy,B...	Up Down
9	□	Speed up RDP	rdp	All IP	Enable:RDP Proxy,Byte...	Up Down
10	□	Speed up ebs	ebs	All IP	Enable:EBS Proxy,Byte...	Up Down
11	□	Speed up https ebs	https ebs	All IP	Enable:EBS Proxy,SSL ...	Up Down
12	□	All applications	ALL-TCP	All IP	Enable:TCP Proxy,SSL ...	Up Down
13	☑	Oracle	ebs	Oracle	Enable:EBS Proxy,SSL ...	Up Down
14	□	Speed up all	ALL-TCP	All IP	Enable:AUTO Proxy,SS...	Up Down

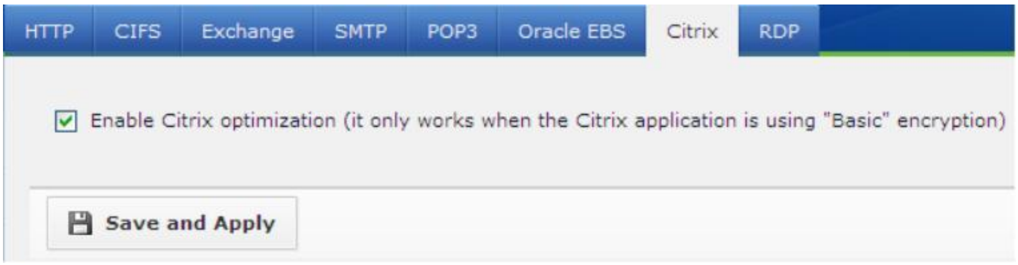
Applicable Users

		Username	Client Type	Description	Policy Group
1	☑	WOC	WOC		Default for gateway

To apply HTTPS proxy to access to Oracle EBS server, you need to create an acceleration policy that associated with https ebs and configure the corresponding server certificate.

Citrix Optimization

Navigate to WAN Optimization > Citrix to enable and configure Citrix optimization, as shown below:

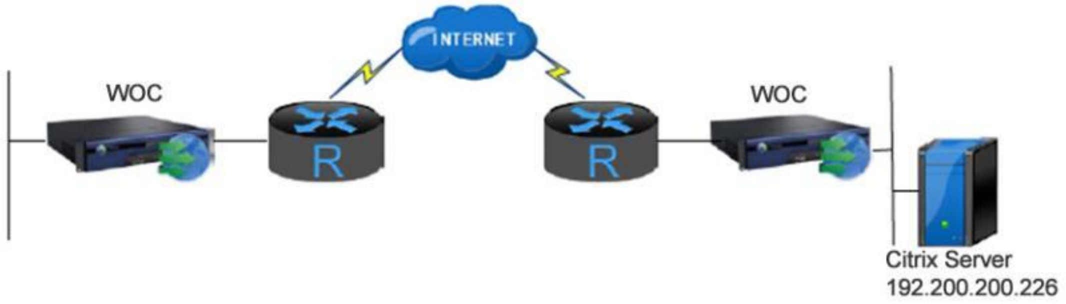


☑ Enable Citrix optimization (it only works when the Citrix application is using "Basic" encryption)

Select the Enable Citrix optimization option to enable Citrix application optimization and click the Save and Apply button to save and apply the changes.

Scenario: Accelerating Access to Citrix

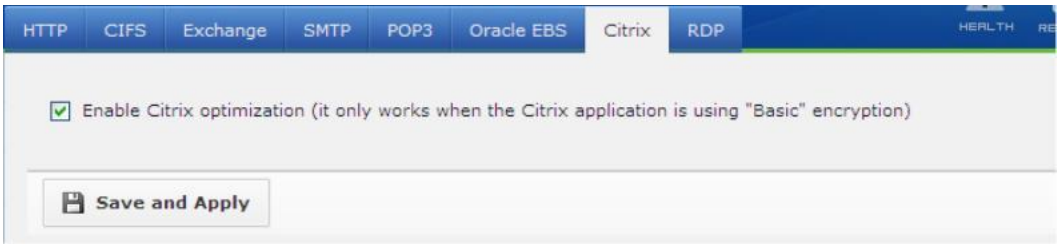
Citrix server (192.200.200.226) is on the HQ network, as shown in the figure below:



To acceleration the access to the Citrix server, perform the following steps on the server-end Sangfor WOC:

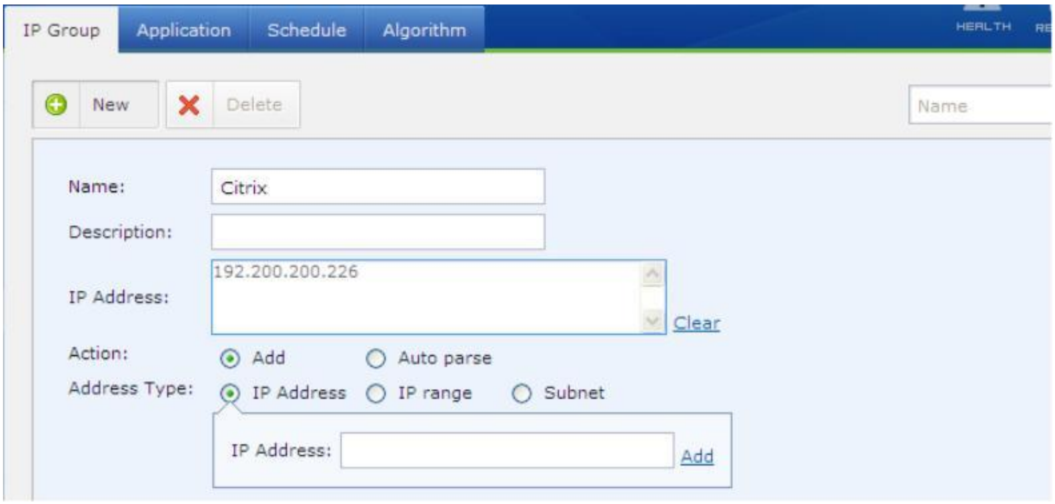
1. Ensure the two WOCs can access each other, and the request from client-end users flows through the server-end WOC.

2. Go to WAN Optimization > Application Proxy > Citrix and select the options Enable Citrix optimization, as shown below:



☑ Enable Citrix optimization (it only works when the Citrix application is using "Basic" encryption)

3. Go to System > Objects > IP Group and add the IP address of the Citrix server, as shown below:



Name: Citrix

Description:

IP Address: 192.200.200.226

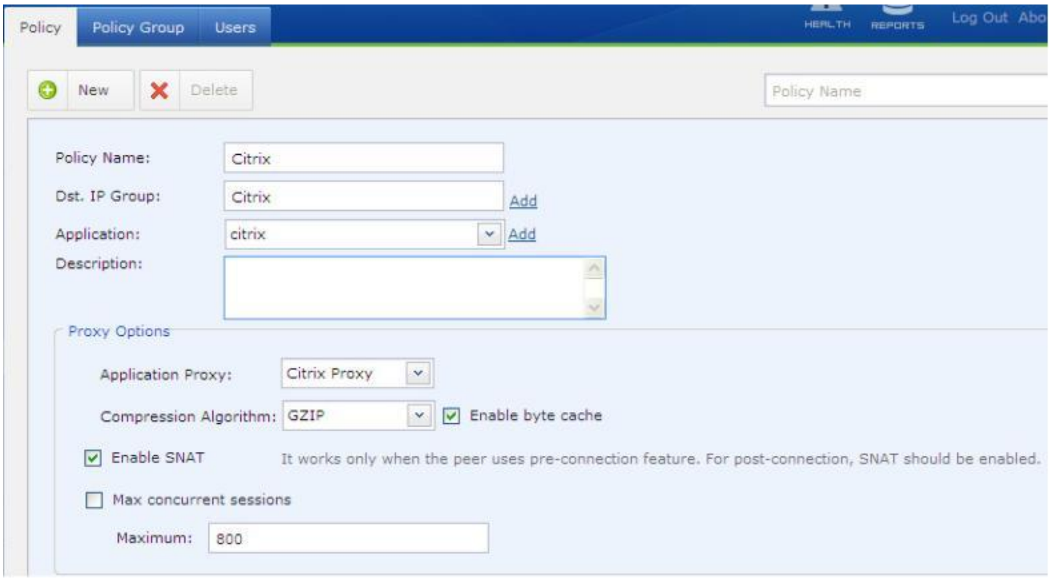
Action: ● Add ○ Auto parse

Address Type: ● IP Address ○ IP range ○ Subnet

IP Address:

4. Go to the WAN Optimization > Server > Policy and create an acceleration policy, as shown

below:



Policy Name: Citrix

Dst. IP Group: Citrix

Application: citrix

Description:

Proxy Options

Application Proxy: Citrix Proxy

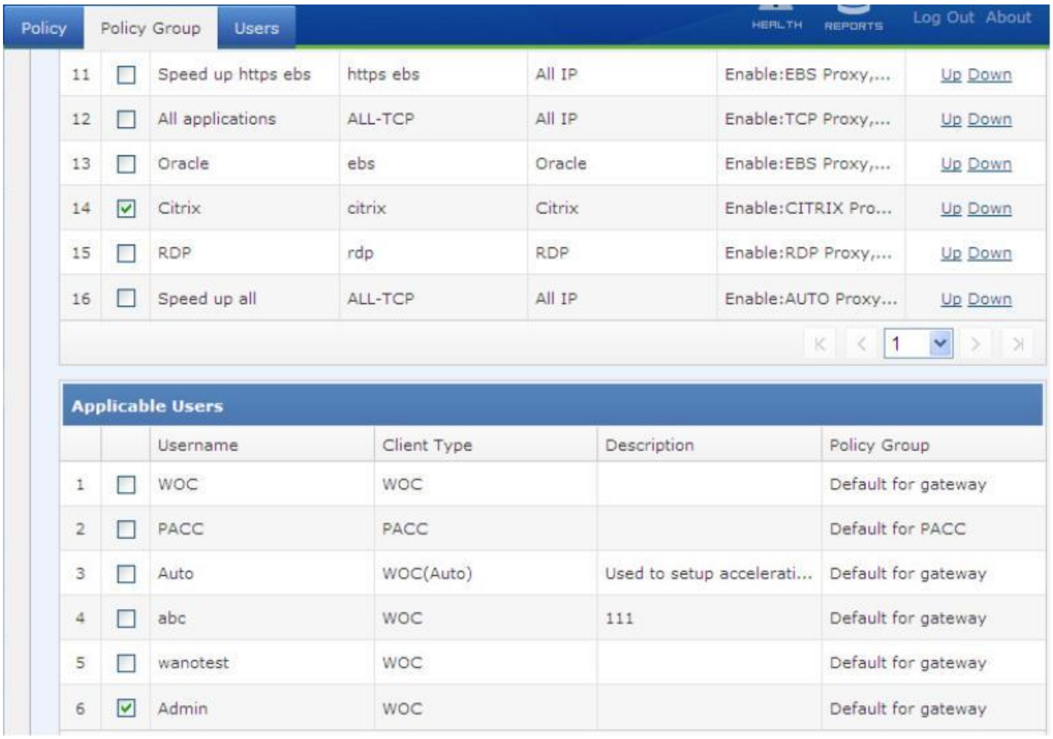
Compression Algorithm: GZIP ☑ Enable byte cache

☑ Enable SNAT It works only when the peer uses pre-connection feature. For post-connection, SNAT should be enabled.

□ Max concurrent sessions

Maximum: 800

5. Go to the WAN Optimization > Server > Policy Group and create a new acceleration policy group and associate it with the corresponding user, as shown below:



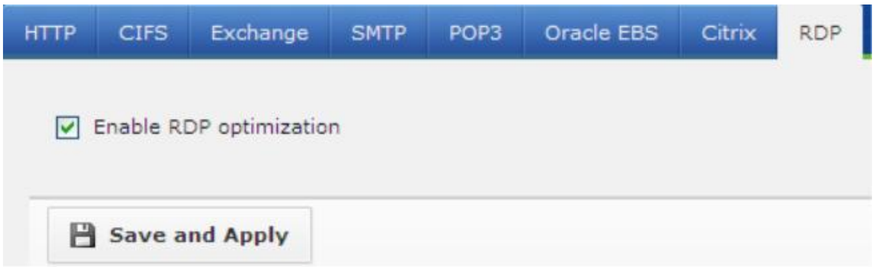
11	□	Speed up https ebs	https ebs	All IP	Enable:EBS Proxy,...	Up Down
12	□	All applications	ALL-TCP	All IP	Enable:TCP Proxy,...	Up Down
13	□	Oracle	ebs	Oracle	Enable:EBS Proxy,...	Up Down
14	☑	Citrix	citrix	Citrix	Enable:CITRIX Pro...	Up Down
15	□	RDP	rdp	RDP	Enable:RDP Proxy,...	Up Down
16	□	Speed up all	ALL-TCP	All IP	Enable:AUTO Proxy...	Up Down

Applicable Users

		Username	Client Type	Description	Policy Group
1	□	WOC	WOC		Default for gateway
2	□	PACC	PACC		Default for PACC
3	□	Auto	WOC(Auto)	Used to setup accelerati...	Default for gateway
4	□	abc	WOC	111	Default for gateway
5	□	wanotest	WOC		Default for gateway
6	☑	Admin	WOC		Default for gateway

RDP Optimization

Navigate to WAN Optimization > RDP to enable and configure RDP optimization, as shown below:

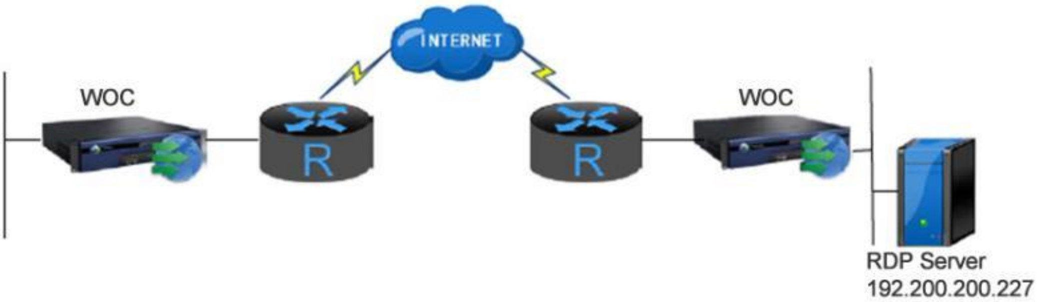


☑ Enable RDP optimization

Select the Enable RDP optimization option to enable RDP optimization and click the Save and Apply button to save and apply the changes.

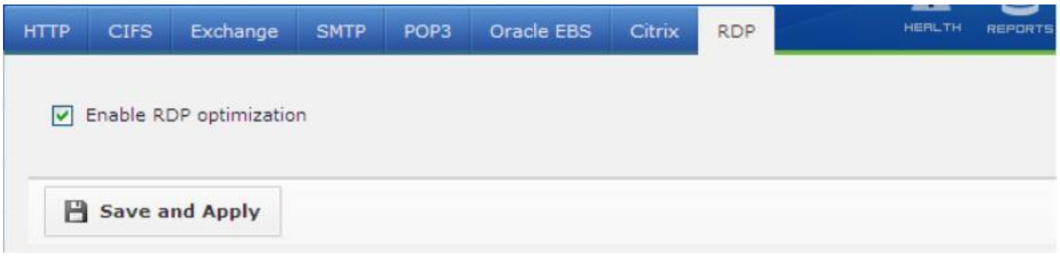
Scenario: Accelerating Access to RDP

RDP server (192.200.200.227) is in on the HQ network, as shown in the figure below:



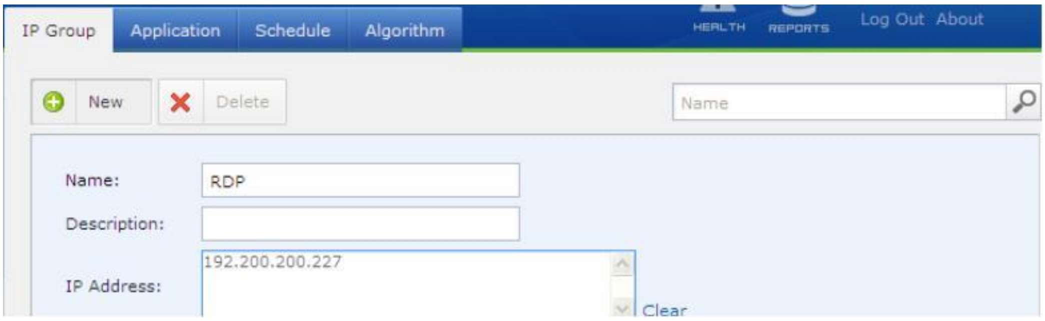
To accelerate access to the RDP server, perform the following steps on the server-end Sangfor WOC:

1. Ensure the two WOCs can access each other, and the request from client-end users goes through the server-end WOC.
2. Go to WAN Optimization > Application Proxy > RDP and select the options Enable RDP optimization, as shown below:



☑ Enable RDP optimization

3. Go to the System > Objects > IP Group tab to add the IP address of the RDP server, as shown below:

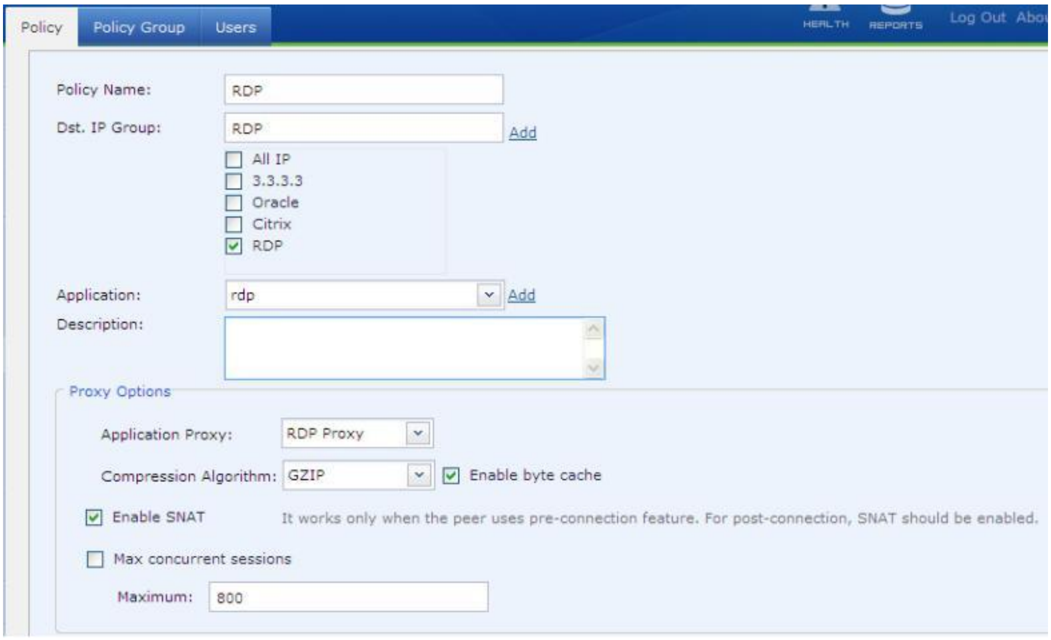


Name: RDP

Description:

IP Address: 192.200.200.227

4. Go to the WAN Optimization > Server > Policy and create an acceleration policy, as shown below:



Policy Name: RDP

Dst. IP Group: RDP

□ All IP
□ 3.3.3.3
□ Oracle
□ Citrix
☑ RDP

Application: rdp

Description:

Application Proxy: RDP Proxy

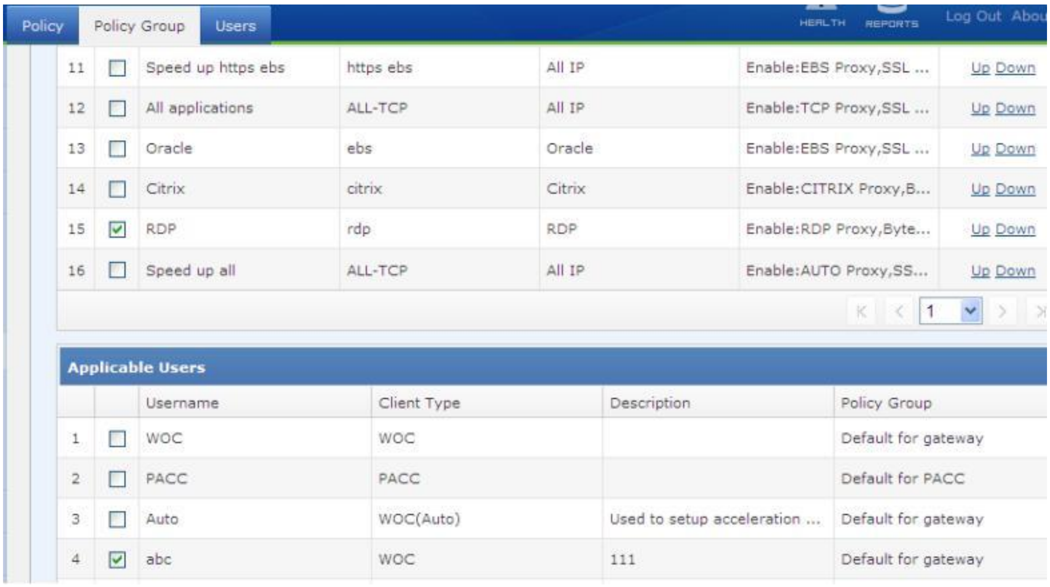
Compression Algorithm: GZIP ☑ Enable byte cache

☑ Enable SNAT It works only when the peer uses pre-connection feature. For post-connection, SNAT should be enabled.

□ Max concurrent sessions

Maximum: 800

5. Go to the WAN Optimization > Server > Policy Group and create a new acceleration policy group , as shown in the following figure:



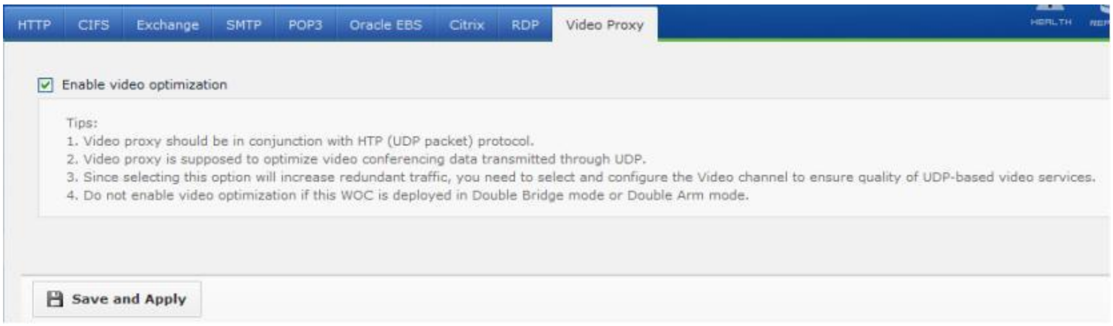
11	□	Speed up https ebs	https ebs	All IP	Enable:EBS Proxy,SSL ...	Up Down
12	□	All applications	ALL-TCP	All IP	Enable:TCP Proxy,SSL ...	Up Down
13	□	Oracle	ebs	Oracle	Enable:EBS Proxy,SSL ...	Up Down
14	□	Citrix	citrix	Citrix	Enable:CITRIX Proxy,B...	Up Down
15	☑	RDP	rdp	RDP	Enable:RDP Proxy,Byte...	Up Down
16	□	Speed up all	ALL-TCP	All IP	Enable:AUTO Proxy,SS...	Up Down

Applicable Users

		Username	Client Type	Description	Policy Group
1	□	WOC	WOC		Default for gateway
2	□	PACC	PACC		Default for PACC
3	□	Auto	WOC(Auto)	Used to setup acceleration ...	Default for gateway
4	☑	abc	WOC	111	Default for gateway

Video Optimization

Navigate to WAN Optimization > Video Proxy to enable and configure Video optimization, as shown below:



☑ Enable video optimization

Tips:
1. Video proxy should be in conjunction with HTP (UDP packet) protocol.
2. Video proxy is supposed to optimize video conferencing data transmitted through UDP.
3. Since selecting this option will increase redundant traffic, you need to select and configure the Video channel to ensure quality of UDP-based video services.
4. Do not enable video optimization if this WOC is deployed in Double Bridge mode or Double Arm mode.

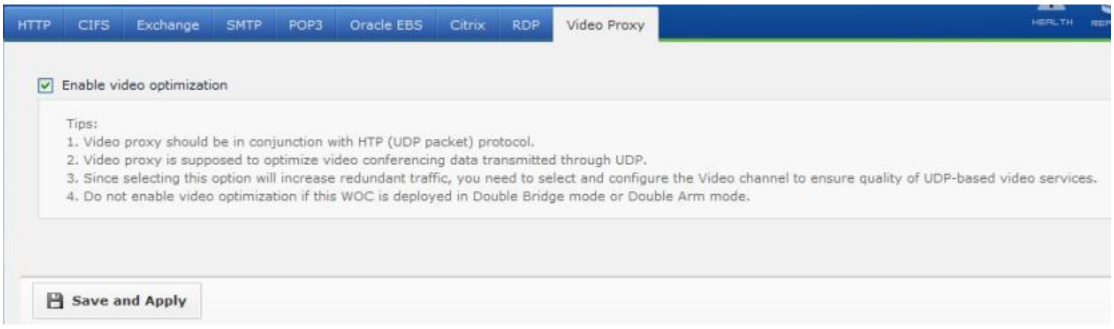
Select the Enable Video optimization option to enable video optimization and click the Save and Apply button to save and apply the changes.

Scenario: Accelerating on video Conference

To accelerate access to the Video conference for both site, perform the following steps on the server-end Sangfor WOC:

1. Ensure the two WOCs can access each other, and the request from client-end users goes through the server-end WOC.

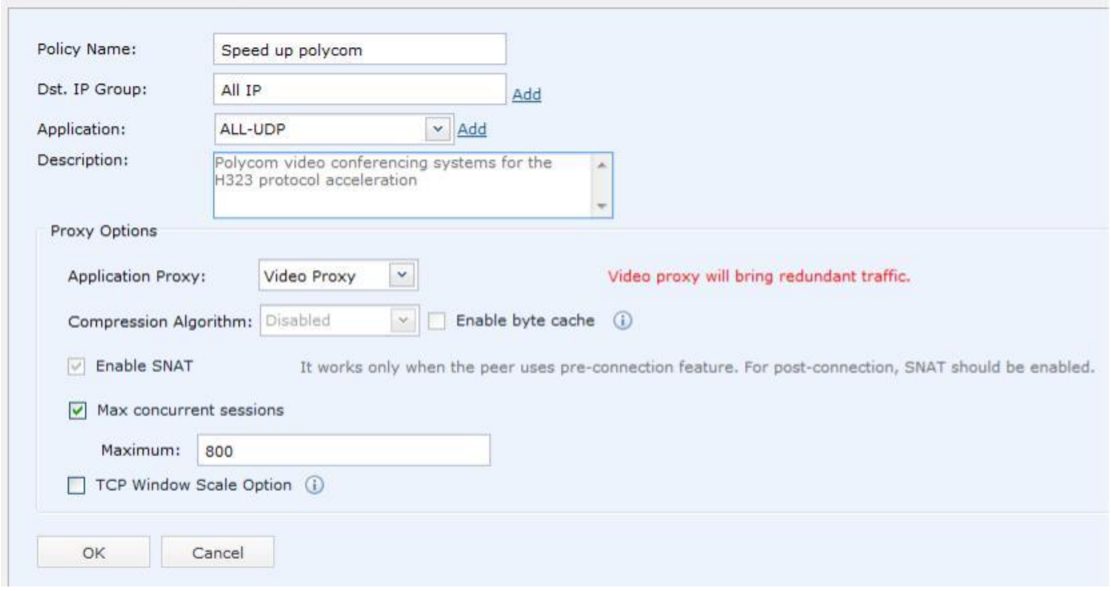
2. Go to WAN Optimization > Application Proxy > Video Proxy and select the options Enable Video optimization, as shown below:



☑ Enable video optimization

Tips:
1. Video proxy should be in conjunction with HTP (UDP packet) protocol.
2. Video proxy is supposed to optimize video conferencing data transmitted through UDP.
3. Since selecting this option will increase redundant traffic, you need to select and configure the Video channel to ensure quality of UDP-based video services.
4. Do not enable video optimization if this WOC is deployed in Double Bridge mode or Double Arm mode.

3. Go to the WAN Optimization > Server > Policy and create an acceleration policy, as shown below:



Policy Name:	Speed up polycom
Dst. IP Group:	All IP Add
Application:	ALL-UDP Add
Description:	Polycom video conferencing systems for the H323 protocol acceleration

Proxy Options

Application Proxy: Video Proxy   Video proxy will bring redundant traffic.

Compression Algorithm: Disabled   □ Enable byte cache

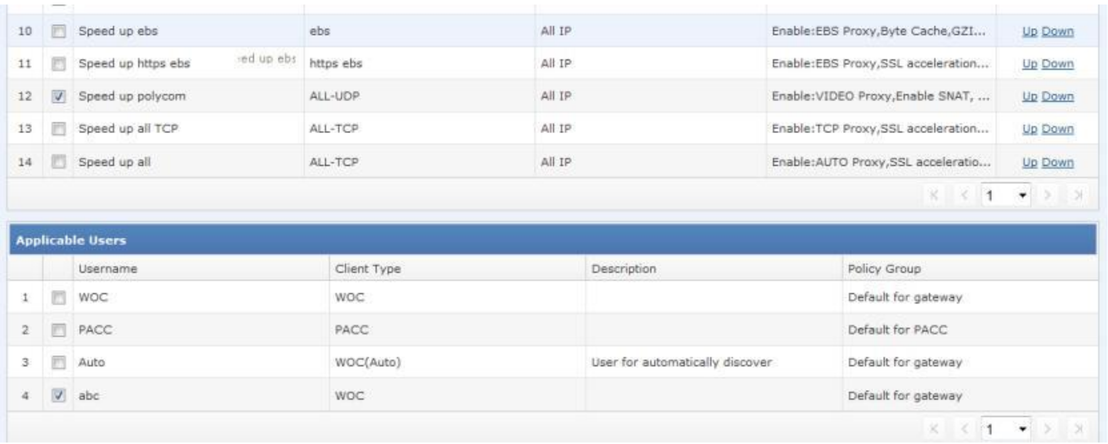
☑ Enable SNAT   It works only when the peer uses pre-connection feature. For post-connection, SNAT should be enabled.

☑ Max concurrent sessions

Maximum: 800

□ TCP Window Scale Option

4. Go to the WAN Optimization > Server > Policy Group and create a new acceleration policy group , as shown in the following figure:

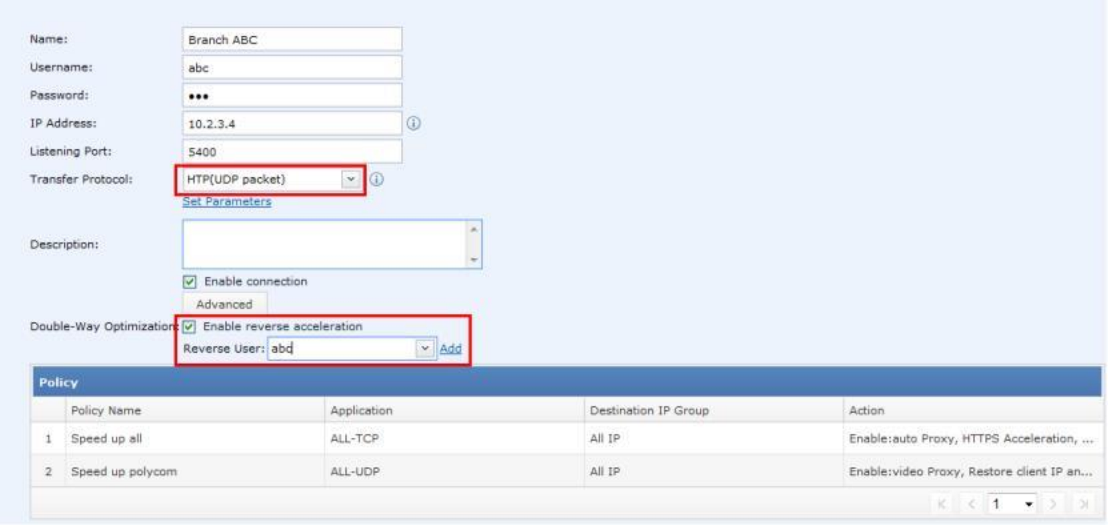


10	□	Speed up ebs	ebs	All IP	Enable:EBS Proxy,Byte Cache,GZI...	Up Down
11	□	Speed up https ebs	https ebs	All IP	Enable:EBS Proxy,SSL acceleration...	Up Down
12	☑	Speed up polycom	ALL-UDP	All IP	Enable:VIDEO Proxy,Enable SNAT, ...	Up Down
13	□	Speed up all TCP	ALL-TCP	All IP	Enable:TCP Proxy,SSL acceleration...	Up Down
14	□	Speed up all	ALL-TCP	All IP	Enable:AUTO Proxy,SSL acceleratio...	Up Down

Applicable Users

		Username	Client Type	Description	Policy Group
1	□	WOC	WOC		Default for gateway
2	□	PACC	PACC		Default for PACC
3	□	Auto	WOC(Auto)	User for automatically discover	Default for gateway
4	☑	abc	WOC		Default for gateway

5. Go to the WAN Optimization > Client > Peer WOC on Client-end WANO create a new peer WOC.



Name: Branch ABC

Username: abc

Password: •••

IP Address: 10.2.3.4

Listening Port: 5400

Transfer Protocol: HTP(UDP packet)

Description:

☑ Enable connection

Double-Way Optimization: ☑ Enable reverse acceleration

Reverse User: abd

Policy

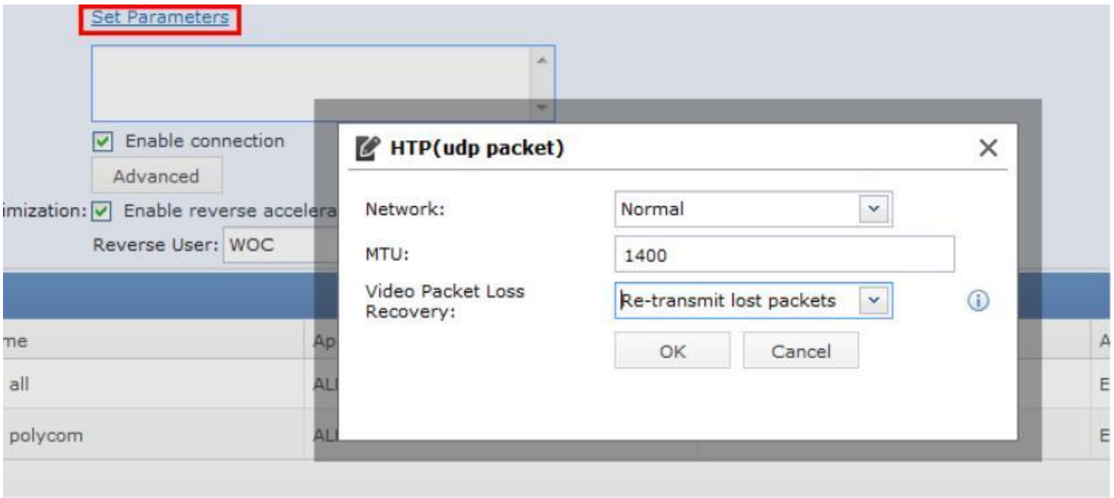
	Policy Name	Application	Destination IP Group	Action
1	Speed up all	ALL-TCP	All IP	Enable:auto Proxy, HTTPS Acceleration, ...
2	Speed up polycom	ALL-UDP	All IP	Enable:video Proxy, Restore client IP an...

*Make sure Transfer Protocol is HTP(UDP packet) and enable reverse acceleration.

6. Click on set parameter, select Video Packer Loss recovery method.

a. Re-transmit lost packets: recommended for network that packer lost rate above 1% and latency below 100ms.

b. Repair lost packet using FEC: recommended for network that packet loss rate above 1% and latency above 100ms.



☑ Enable connection

imization: ☑ Enable reverse accelera

Reverse User: WOC

HTP(udp packet)

Network: Normal

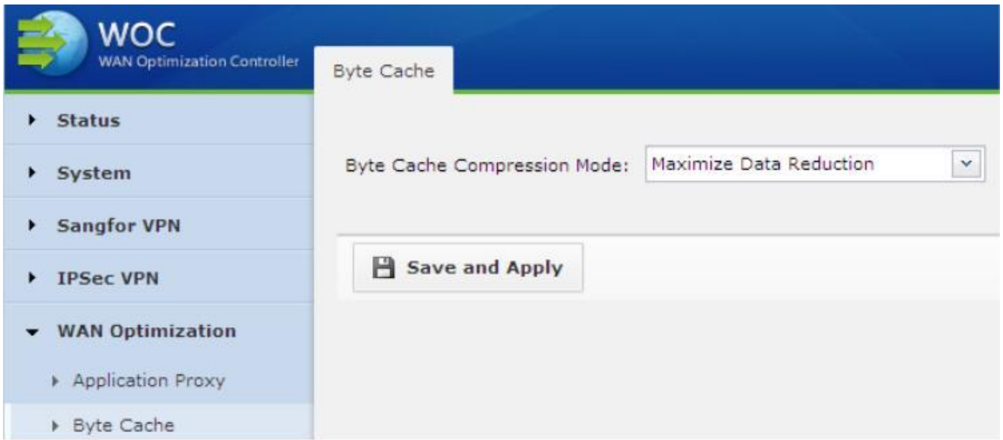
MTU: 1400

Video Packet Loss Recovery: Re-transmit lost packets

*Enable video proxy will increase additional redundant traffic which will not more than 50% of the original data.

Byte Cache

Navigate to WAN Optimization > Byte Cache to configure data compression mode, as shown below:



Byte Cache Compression Mode: Maximize Data Reduction

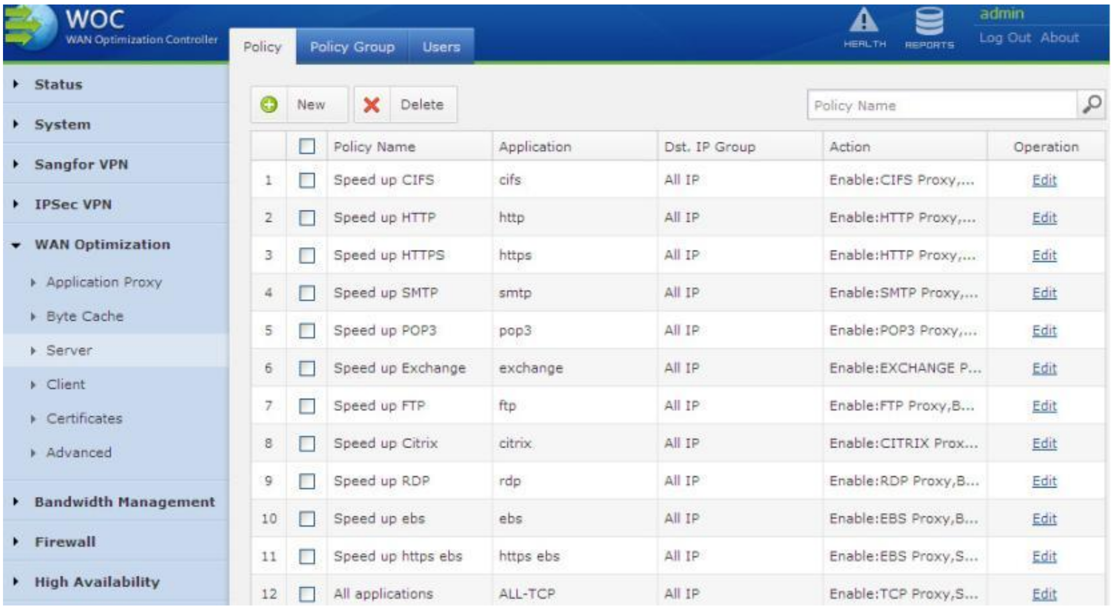
If Maximize Data Reduction is selected, bandwidth savings will be maximized but throughput of the WAN Optimization Controller (WOC) will be lowered down.

If Maximize LAN Throughput is selected, throughput of the WOC will be maximized but data reduction capability will be affected.

Setting Up Inbound Acceleration Connection

To set up an inbound acceleration from a remote WAN optimization Controller (WOC) or mobile worker whose PC is installed Sangfor Portable Acceleration (PACC) client software, you need to perform the Server configuration on the local Sangfor WOC, which includes user, acceleration policy and policy group.

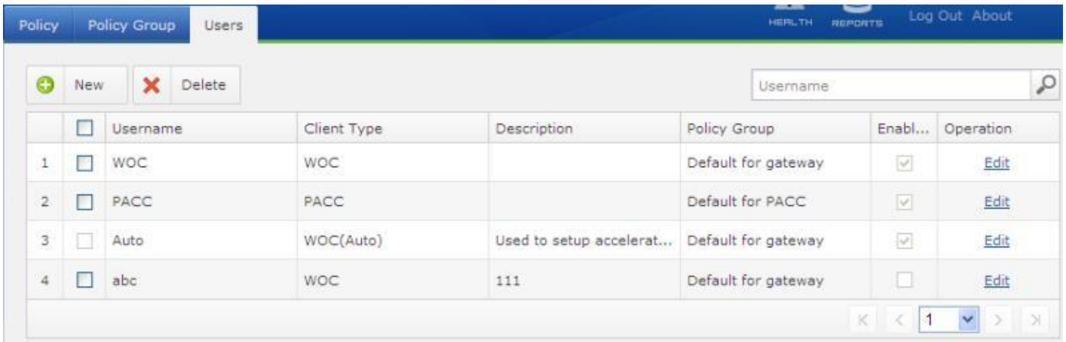
The user account is used by remote WOC or PC to create and establish acceleration connection, and should be associated with certain acceleration policy. For more information, you can refer to the following sections.



	□	Policy Name	Application	Dst. IP Group	Action	Operation
1	□	Speed up CIFS	cifs	All IP	Enable:CIFS Proxy,...	Edit
2	□	Speed up HTTP	http	All IP	Enable:HTTP Proxy,...	Edit
3	□	Speed up HTTPS	https	All IP	Enable:HTTP Proxy,...	Edit
4	□	Speed up SMTP	smtp	All IP	Enable:SMTP Proxy,...	Edit
5	□	Speed up POP3	pop3	All IP	Enable:POP3 Proxy,...	Edit
6	□	Speed up Exchange	exchange	All IP	Enable:EXCHANGE P...	Edit
7	□	Speed up FTP	ftp	All IP	Enable:FTP Proxy,B...	Edit
8	□	Speed up Citrix	citrix	All IP	Enable:CITRIX Prox...	Edit
9	□	Speed up RDP	rdp	All IP	Enable:RDP Proxy,B...	Edit
10	□	Speed up ebs	ebs	All IP	Enable:EBS Proxy,B...	Edit
11	□	Speed up https ebs	https ebs	All IP	Enable:EBS Proxy,S...	Edit
12	□	All applications	ALL-TCP	All IP	Enable:TCP Proxy,S...	Edit

Creating User

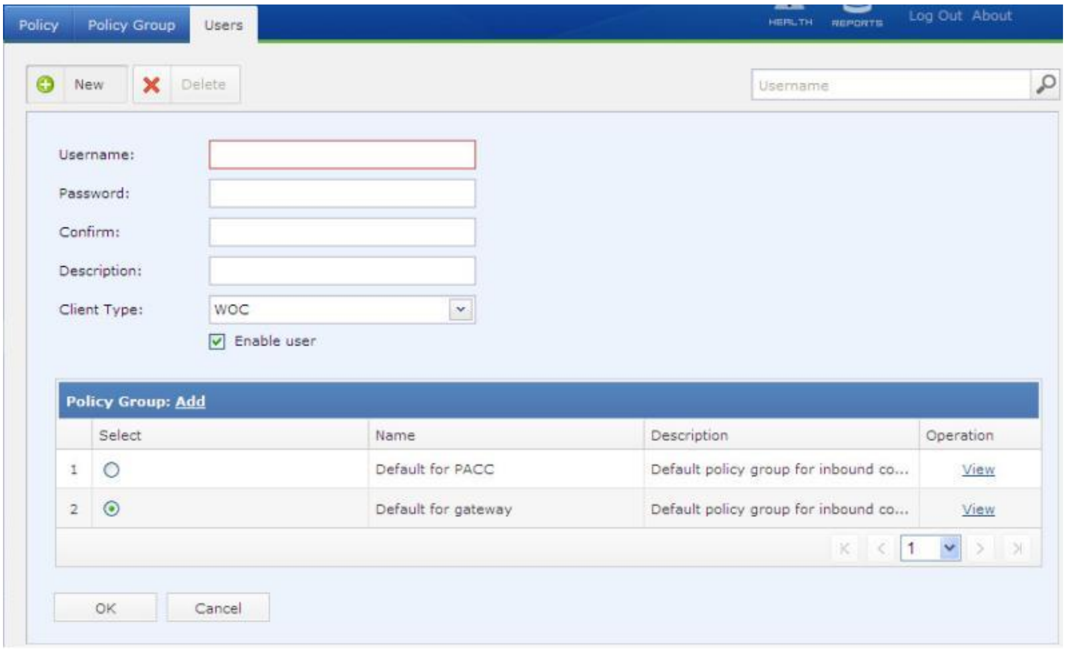
1. Navigate to WAN Optimization > Server > Users.



	□	Username	Client Type	Description	Policy Group	Enabl...	Operation
1	□	WOC	WOC		Default for gateway	☑	Edit
2	□	PACC	PACC		Default for PACC	☑	Edit
3	□	Auto	WOC(Auto)	Used to setup accelerat...	Default for gateway	☑	Edit
4	□	abc	WOC	111	Default for gateway	□	Edit

2. Click the New button and enter the username and password, select client type WOC or PACC. WOC indicates that the peer is a physical WAN Optimization Controller while PACC

indicates that the peer is an ordinary computer on which is installed the Sangfor Portable Acceleration (PACC) client software.



Username:

Password:

Confirm:

Description:

Client Type: WOC

☑ Enable user

Policy Group: Add

	Select	Name	Description	Operation
1	○	Default for PACC	Default policy group for inbound co...	View
2	●	Default for gateway	Default policy group for inbound co...	View

The following are the contents included on the Users page:

Username: Configures name of the user account that will used by the client to create and establish acceleration connection to the local Sangfor WOC.

Password: Configures the password of the user account.

Confirm: Enter the password again.

Description: Give this account a brief description.

Client Type: Configures type of the client by which this user account is used to create and initiate acceleration connection, physical WOC or PACC software. If acceleration is initiated by a remote physical WOC, the client type should be WOC. If acceleration is initiated by a PC that is installed PACC client software (by mobile worker), the client type should be PACC.

Enable user: Select this option to enable this acceleration user account.

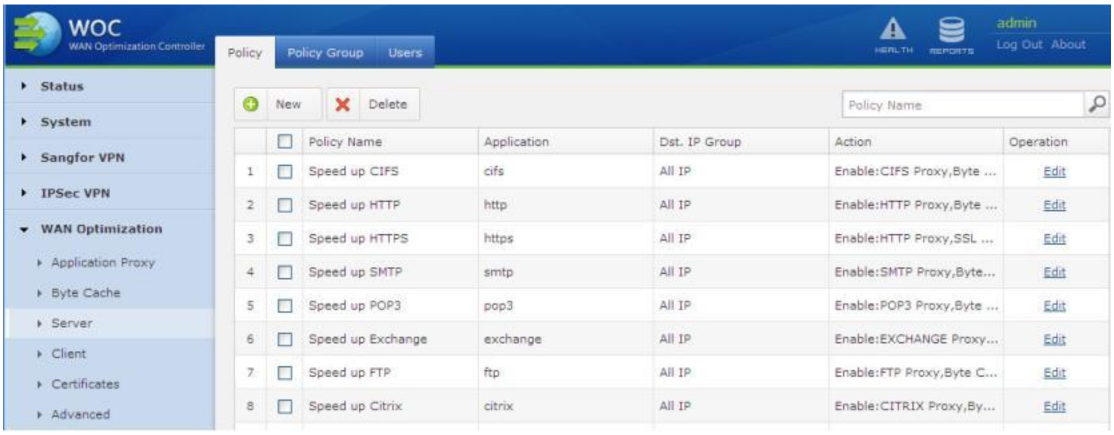
Policy Group: Select the acceleration policy group that is associated with this user account. To add a new acceleration policy group, click Add to enter the Policy Group page.

To view the acceleration policies that are included in the acceleration policy group, click View in the Operation column.

OK: Click this button to save the settings.

Acceleration Policy

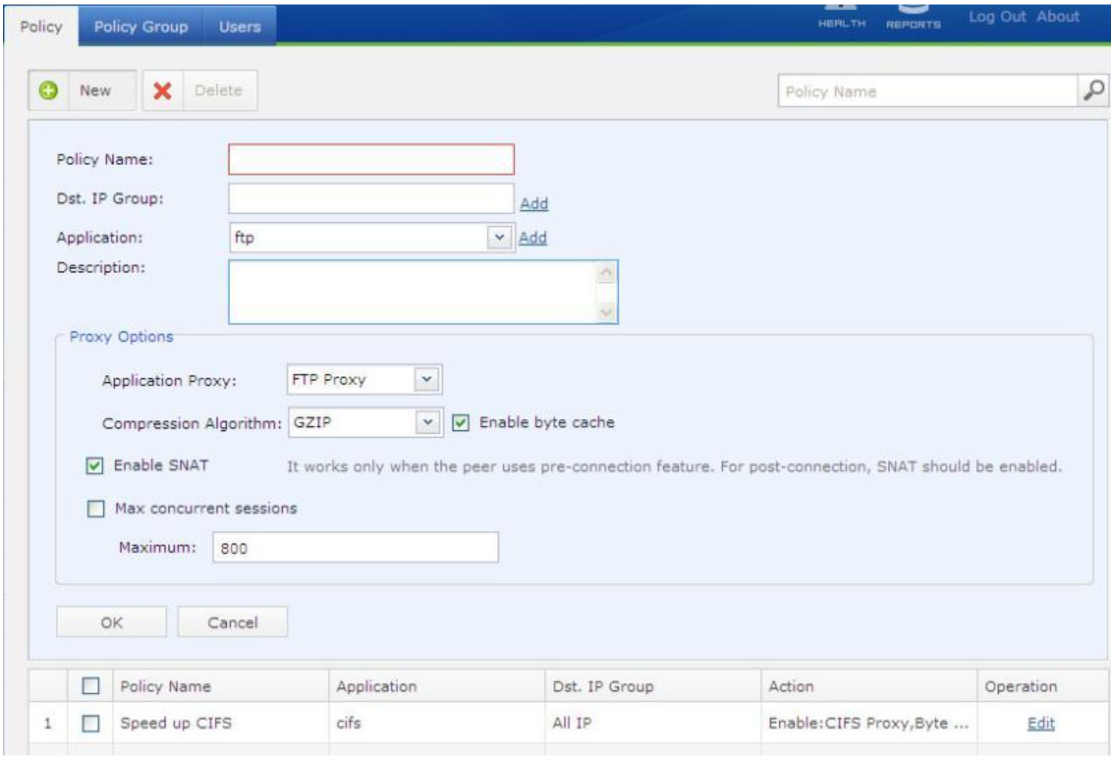
An acceleration policy defines the acceleration related settings, such as destination IP, application, application proxy, compression algorithm and byte cache. Before acceleration policy is associated with a user, the application cannot not be optimized for that user. Some acceleration policies are already built in Sangfor WAN Optimization Controller (WOC). The acceleration page is as shown in the figure below:



	□	Policy Name	Application	Dst. IP Group	Action	Operation
1	□	Speed up CIFS	cifs	All IP	Enable:CIFS Proxy,Byte ...	Edit
2	□	Speed up HTTP	http	All IP	Enable:HTTP Proxy,Byte ...	Edit
3	□	Speed up HTTPS	https	All IP	Enable:HTTP Proxy,SSL ...	Edit
4	□	Speed up SMTP	smtp	All IP	Enable:SMTP Proxy,Byte...	Edit
5	□	Speed up POP3	pop3	All IP	Enable:POP3 Proxy,Byte ...	Edit
6	□	Speed up Exchange	exchange	All IP	Enable:EXCHANGE Proxy...	Edit
7	□	Speed up FTP	ftp	All IP	Enable:FTP Proxy,Byte C...	Edit
8	□	Speed up Citrix	citrix	All IP	Enable:CITRIX Proxy,By...	Edit

To delete an acceleraton poicy, select the policy and click the Delete button.

To create a new acceleration policy, click the New button.



Policy Name:

Dst. IP Group:

Application: ftp

Description:

Application Proxy: FTP Proxy

Compression Algorithm: GZIP ☑ Enable byte cache

☑ Enable SNAT It works only when the peer uses pre-connection feature. For post-connection, SNAT should be enabled.

□ Max concurrent sessions

Maximum: 800

	□	Policy Name	Application	Dst. IP Group	Action	Operation
1	□	Speed up CIFS	cifs	All IP	Enable:CIFS Proxy,Byte ...	Edit

The following are the parameters of an acceleration policy:

Policy Name: Indicates the name of the policy.

Dst. IP Group: Access to the address included in the destination IP group may be accelerated. You can click Add to enter Objects > IP Group page to specify new IP addresses or select the desired IP group which is predefined on the IP Group page. For more information, please refer to Creating IP Group in Chapter 3).

Application: Specifies the application that will be optimized. You can click Add to enter Objects > Application page to create new application or select the desired application which has been defined on the Application page. For more information, please refer to Creating IP Group in Chapter 3).

Description: Gives a brief description to this acceleration policy.

Application Protocol: Indicates the protocol to be proxied; options are Auto proxy, TCP proxy, HTTP proxy, FTP proxy, CIFS proxy, POP3 proxy, SMTP proxy, Exchange proxy, Citrix proxy, RDP proxy and Oracle Forms proxy).

Algorithm: Configures the algorithm used by the acceleration tunnel. Options are No compression, LZO compression and GZIP compression. Compression effect of LZO compression is 15% higher than that of GZIP compression, but it consumes more performance of the WAN Optimization Controller (WOC). GZIP compression is recommended for general cases.

Enable Byte Cache: Decides whether to enable byte cache feature.

Enable SNAT: Select this option, and it will disclose the real source IP address of the data packet when some applications require reserving the source IP; otherwise, the IP address of the local WAN Optimization Controller (WOC) will be taken as the source IP address of the data packet (indicating the data packet is forwarded from this IP address). You have to select this option if the LAN application masquerades the true source IP address of the data packet.

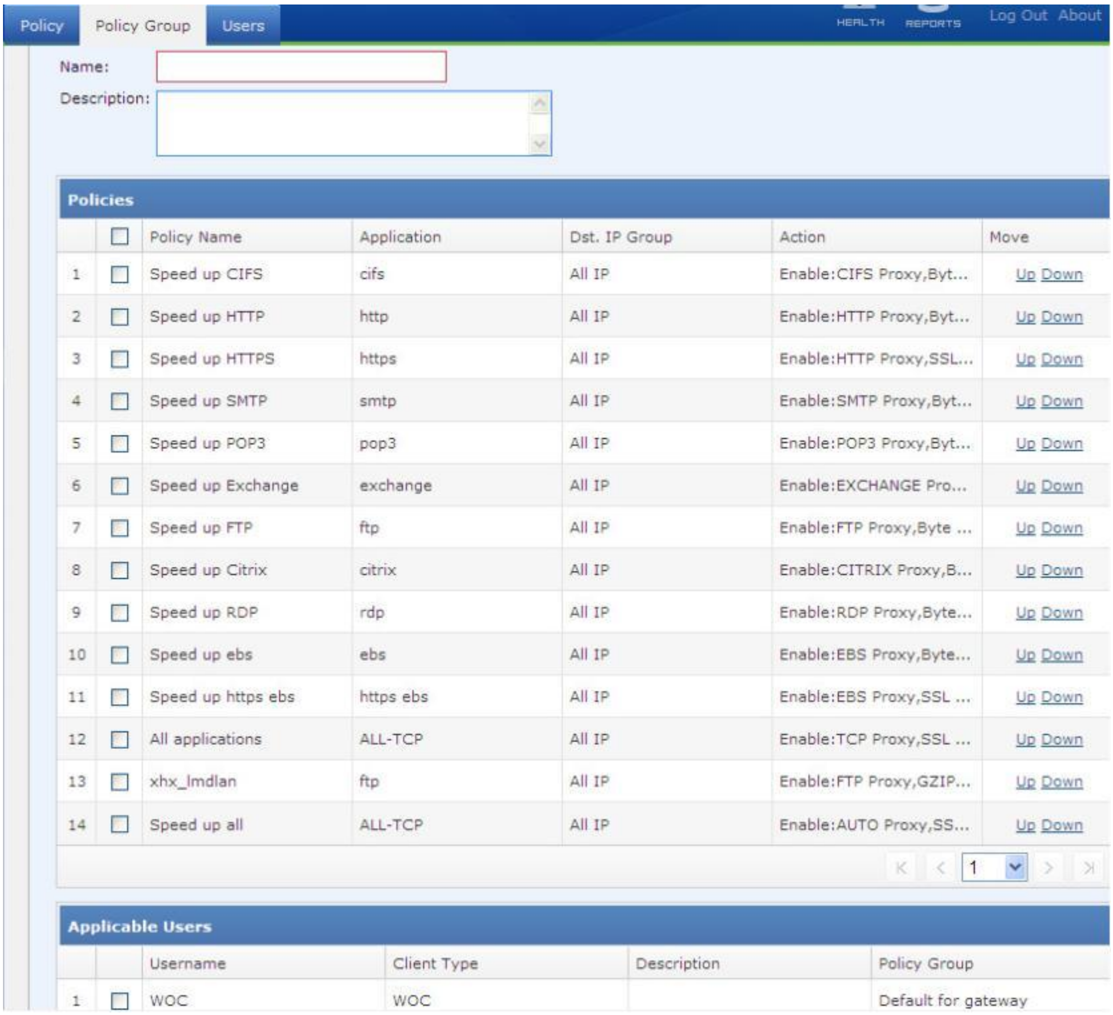
Session Limit: Defines the sessions to be accelerated. The default is the maximum 800. Each policy for PACC user (mobile worker) supports at most 50 sessions and the excessive ones will be bypassed.

To select CIFS proxy, you have to select the Enable SNAT option.

Acceleration Policy Group

An acceleration policy group is a collection of acceleration policies, which should be associated with user. Sangfor WOC is already built in with two default acceleration policies.

Navigate to WAN Optimization > Server > Policy > Policy Group to enter the Policy Group page. Click the New button to add a new acceleration policy group, as shown below:



Name:

Description:

Policies

	□	Policy Name	Application	Dst. IP Group	Action	Move
1	□	Speed up CIFS	cifs	All IP	Enable:CIFS Proxy,Byt...	Up Down
2	□	Speed up HTTP	http	All IP	Enable:HTTP Proxy,Byt...	Up Down
3	□	Speed up HTTPS	https	All IP	Enable:HTTP Proxy,SSL...	Up Down
4	□	Speed up SMTP	smtp	All IP	Enable:SMTP Proxy,Byt...	Up Down
5	□	Speed up POP3	pop3	All IP	Enable:POP3 Proxy,Byt...	Up Down
6	□	Speed up Exchange	exchange	All IP	Enable:EXCHANGE Pro...	Up Down
7	□	Speed up FTP	ftp	All IP	Enable:FTP Proxy,Byte ...	Up Down
8	□	Speed up Citrix	citrix	All IP	Enable:CITRIX Proxy,B...	Up Down
9	□	Speed up RDP	rdp	All IP	Enable:RDP Proxy,Byte...	Up Down
10	□	Speed up ebs	ebs	All IP	Enable:EBS Proxy,Byte...	Up Down
11	□	Speed up https ebs	https ebs	All IP	Enable:EBS Proxy,SSL ...	Up Down
12	□	All applications	ALL-TCP	All IP	Enable:TCP Proxy,SSL ...	Up Down
13	□	xhx_lmdlan	ftp	All IP	Enable:FTP Proxy,GZIP...	Up Down
14	□	Speed up all	ALL-TCP	All IP	Enable:AUTO Proxy,SS...	Up Down

Applicable Users

		Username	Client Type	Description	Policy Group
1	□	WOC	WOC		Default for gateway

The following are attributes of an acceleration policy group:

Name: Configures the name of the acceleration policy group.

Description: Enter descriptive information for this acceleration policy group:

Policies: Includes all the policies created on Policy page. Select the desire acceleration policies that this new policy group includes.

Applicable Users: Select the desired user(s) to associate with the policy.

Scenario: Setting Up Acceleration Connection for Branch User

To enable user at the branch office to set up acceleration connection to the headquarters (HQ) and access 172.16.100.0/24, create an acceleration user named woctest and then associate it with a policy group consisting of HTTP and FTP services.

Perform the following steps:

1. Log in to the Web administrator console of HQ WOC and go to WAN Optimization > Server > Policy page. Create application and destination address. As HTTP and FTP are default applications for acceleration, you need not create acceleration policies for these two

applications.

2. Go to Policy Group page, create an acceleration policy group named woctest group and associate it with the HTTP and FTP applications. In this step, you need not to associate this acceleration policy group with the acceleration user because you have not added the acceleration user yet.

3. Go to WAN Optimization > Server > User page and create a WOC type of user and associate it with the acceleration policy group wanotest group.

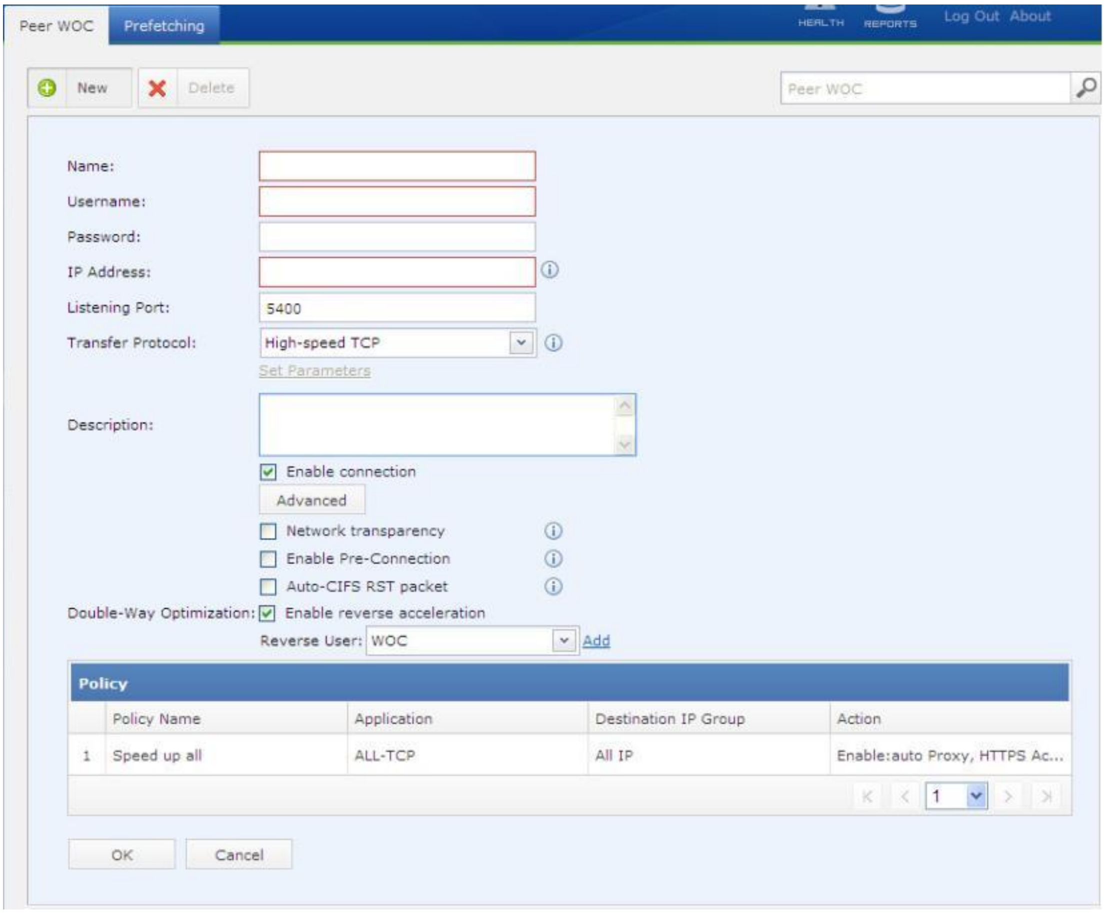
4. User at the head office then can connect to the headquarters with the user account wanotest, having the HTTP and FTP application accelerated.

Setting Up Outbound Acceleration Connection

To set up an outbound acceleration connection, you need to complete the Client setting, namely, adding profile of the remote Sangfor Optimization Controller (WOC) to which you want to connect, and defining the data prefetching time.

Creating Profile of Peer WOC

Navigate to WAN Optimization > Client > Peer WOC page and click the New button to create profile of the peer WOC. In setting up outbound acceleration connection, the local WOC acts as the client, connecting to the server-side Sangfor WOC.



Name:

Username:

Password:

IP Address:

Listening Port: 5400

Transfer Protocol: High-speed TCP

Set Parameters

Description:

☑ Enable connection

Advanced

□ Network transparency

□ Enable Pre-Connection

□ Auto-CIFS RST packet

Double-Way Optimization: ☑ Enable reverse acceleration

Reverse User: WOC Add

Policy

	Policy Name	Application	Destination IP Group	Action
1	Speed up all	ALL-TCP	All IP	Enable:auto Proxy, HTTPS Ac...

OK Cancel

The following are the contents included on Peer WOC page:

Name: Enter name of the peer device to which the local WOC is connecting.

Username: Enter the WOC type of user account configured on the peer WOC for the local WOC to establish acceleration connection.

Password: Enter password of the WOC type of user account configured on the peer WOC for the local WOC.

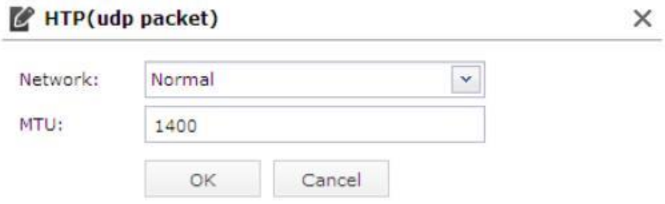
IPAddress: Enter LAN interface IP address or bridge IP address of the peer device.

Listening Port: Enter the listening port of the peer WOC. Listing port of the peer and local Sangfor WOC must be identical; otherwise, the acceleration connection cannot be established.

Transfer Protocol: Configures the encapsulation mode of the data packets that are to be transferred and accelerated. Options are High-speed TCP, HTP (udp packet) and HTP (tcp packet).

High-speed TCP is suitable for network with low latency and no packet loss, HTP (udp packet) is a transfer protocol based on UDP, while HTP (tcp packet) utilizes traffic congestion control algorithm based on TCP protocol and is suitable for network with high packet loss rate or high latency. However, High-speed TCP is recommended in case VPN connection and acceleration connection need to be established simultaneously and transfer protocol TCP is used in VPN connection.

Set Parameters: It is only available when the transfer protocol is HTP (udp packet). You can set network mode to Normal, High packet loss or Low latency and set the Maximum Transfer Unit (MTU) of UDP packets, as shown in the figure below:



HTP(udp packet)

Network: Normal

MTU: 1400

Description: Enter descriptive information for the peer WOC.

Enable connection: Select this option to enable the above settings. This option is unselected initially.

Advanced: Click it and the options Network transparency and Enable Pre-Connection are seen.

Network transparency: Select this option to enable the network transparency mode, and the WOC will reveal the true IP addresses of the source and destination of the packets transmitted in the acceleration channel. This function is suitable for the situation that the access control policy of either Sangfor WOC (local or peer) has referenced the true source IP or destination IP address, and bandwidth is in restriction.

Network transparency should not be selected if Sangfor WOC is deployed and configured in any of the following way: a). Gateway mode and VPN function is enabled; b). Single Arm mode, but the CDP or WCCP function is not enabled.

Pre-Connection: Select this option to enable pre-connection mode.

Pre-connection mode indicates that, when client PC sends request to a server, the client-end WOC receives and responds to the request on behalf of the destination server, in that way, client PC needs not to wait long for the response from the destination server. This feature shortens the time for establishing connection as well as data transmission.

By default, post-connection is applied. Post-connection is opposite to pre-connection, which means the client-side WOC does not respond to the connecting user on behalf of the remote server but only responds after it receives response from the remote server.

For acceleration established between two Sangfor WAN Optimization Controllers (WOC), pre-connection and post-connection are alternative. For acceleration connection established between the Portable Acceleration (PACC) client software and physical Sangfor WOC, pre-connection is the only option.

Auto-CIFS RST packet: Select this option and the CIFS RST packet will be sent to both the client-end and server-end WOCs to disconnect the current CIFS connection when a new acceleration is established between the two WOCs, so that new CIFS connection can get into the acceleration channel and be accelerated.

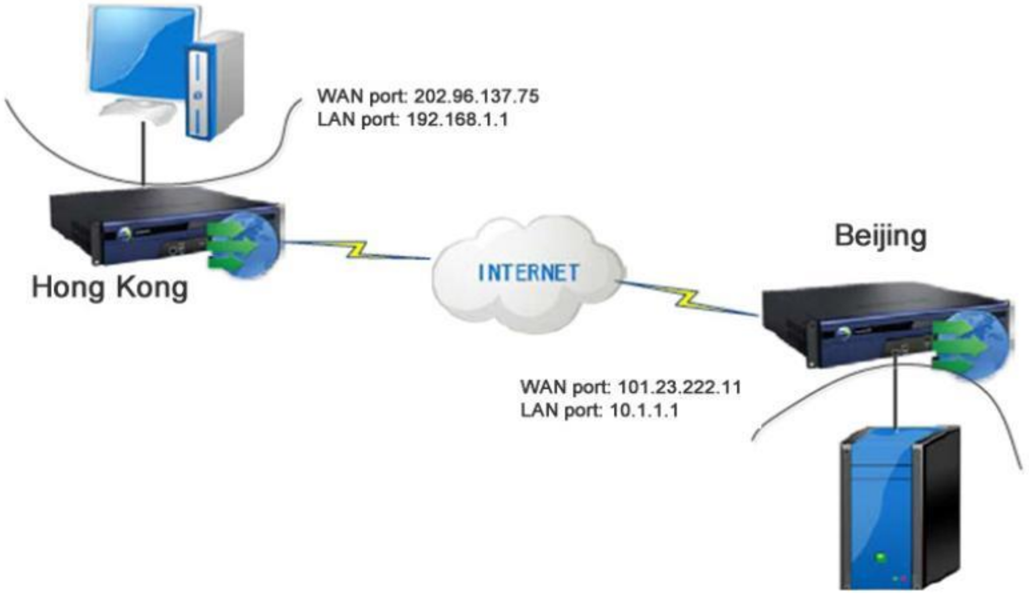
Enable reverse acceleration: Select this option to enable reverse acceleration, and then select a Reverse User that is configured on the peer WOC. Generally, acceleration established between two WOCs is one-way acceleration. To enable the peer WOC to establish acceleration connection to the local WOC proactively without an additional license, you can enable reverse acceleration.

HTP is a high-speed and reliable transmission protocol based on UDP, developed exclusively by SANGFOR. It can deal with networks with high packet loss rate and high latency and achieve good transmission efficiency in wireless and Long-Fat-Pipe environment.

Scenario: Branch Sets Up Acceleration Connection to HQ

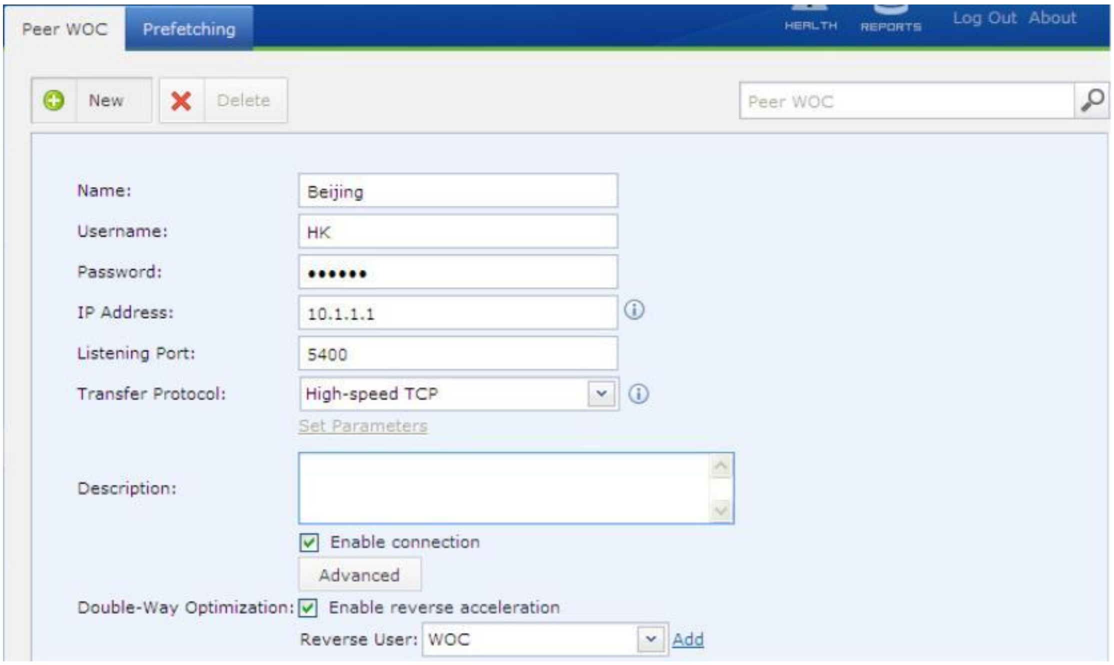
Suppose the Sangfor WAN Optimization Controller (WOC) is deployed on the network of HQ Beijing and the WAN Optimization module is configured already. Now, another WOC needs to be deployed on Hong Kong branch and set up acceleration connection to HQ Beijing WOC.

The network topology is shown in the figure below:



We provide that all other settings are completed. The following only focuses on creating acceleration connection, others being ignored.

Log in to the administrator console of the HK WOC and navigate to WAN Optimization > Client > Peer WOC to create the profile, as shown in the following figure:

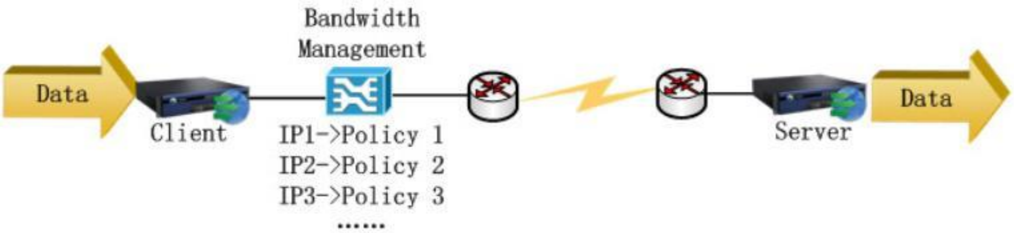


Name:	Beijing
Username:	HK
Password:	••••••
IP Address:	10.1.1.1
Listening Port:	5400
Transfer Protocol:	High-speed TCP
Description:	
	☑ Enable connection
Double-Way Optimization:	☑ Enable reverse acceleration
	Reverse User: WOC

Scenario 22: Enable Network Transparency Mode

The customer deploys the Sangfor WOC in Bridge mode, on the network where a bandwidth management device is deployed at frontend of the WOC. Bandwidth control policies have been configured on the BM device for the internal IP address.

The network topology is as shown in the following figure:



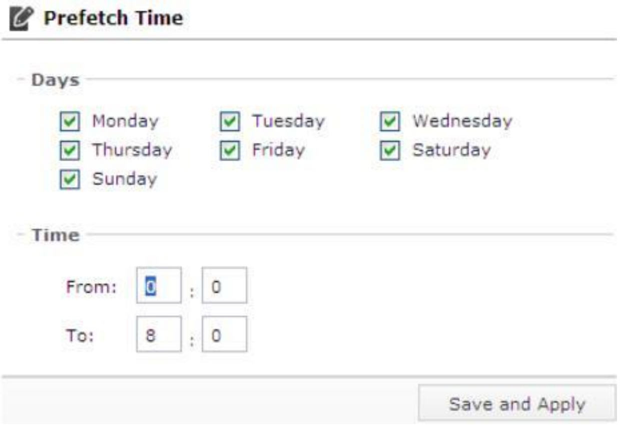
Next, we need to ensure that source IP, source port, destination IP, destination port of the data packets keep unchanged when they flow through the WOC, and bandwidth control policies still take effect.

Log in to the administrator console of the client-end WOC and navigate to WAN Optimization > Client > Peer WOC, edit the related WOC (or create one) and select Enable Network Transparency.

Prefetching

Prefetching is a feature that Sangfor WAN Optimization Controller (WOC) fetches data from remote server and save them to Byte Cache directory on the Sangfor WOC at designated time automatically, before users initiate the request. Therefore, the first users who ask for the data will obtain them from the local Byte Cache directory directly, rather than connecting to the remote sever. Such feature could greatly enhance user experience.

Navigate to WAN Optimization > Client > Prefetching and click the Prefetch Time button to set the time when the data from specified servers will be obtained and saved on the WOC.


Prefetch Time

Days

☑ Monday ☑ Tuesday ☑ Wednesday
☑ Thursday ☑ Friday ☑ Saturday
☑ Sunday

Time

From: 0 : 0

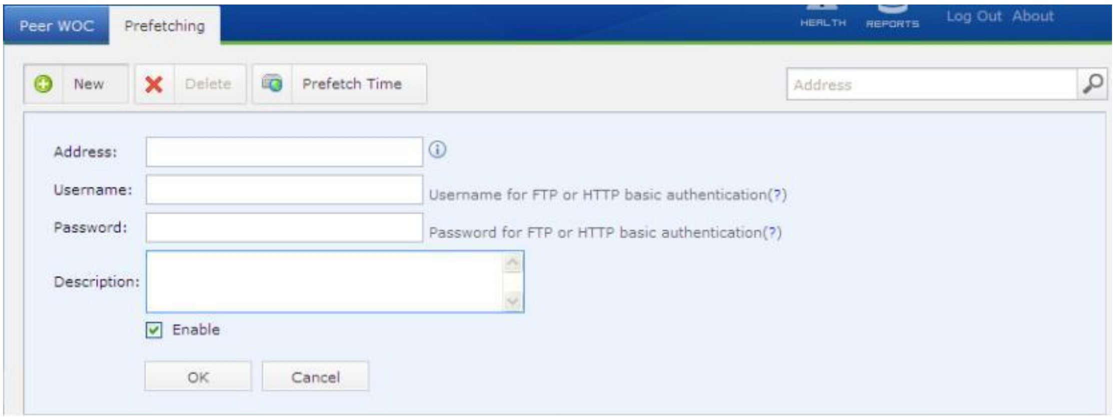
To: 8 : 0

Days: Specifies the weekdays on which prefetching will be implemented.

Time: Specifies the time period during which data will be fetched from the respective servers.

Time is based on WOC system time. Please make sure that the system time of WOC is accurate.

To create a prefetch rule, click the New button.



Address: Specifies the server address on which the desired data are located.

Username, Password: Configures the username and password required for logging in to the server.

Description: Describes the contents to be prefetched.

Enable: Select this option to enable the settings on this page and this prefetch rule.

HTTP and FTP prefetching are supported. Only login to FTP server requires username and password.

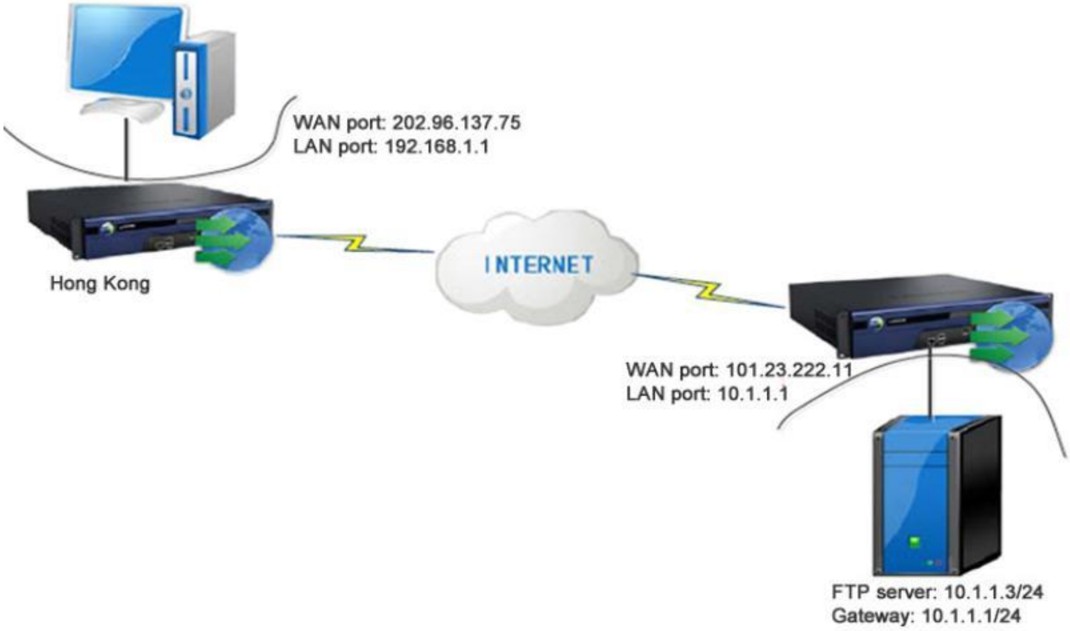
The address and file name should be half-width characters, or else prefetching will fail because of decoding failure.

Scenario: Prefetch Data from FTP Server

Suppose acceleration connection between HQ Beijing and Hong Kong branch has been established. However, the employees at Hong Kong branch frequently download report files of the previous day from the FTP server of HQ Beijing. Since the report files are large and bandwidth is in great shortage, file download is very slow.

To solve this problem, Hong Kong branch enables the prefetching feature on the Sangfor WOC and set the prefetch time (early morning every day) so that report files could be downloaded from the FTP server in HQ Beijing. The downloaded files are cached on the local WOC and will be instantly available to the employees at Hong Kong branch.

The deployment topology is shown below:



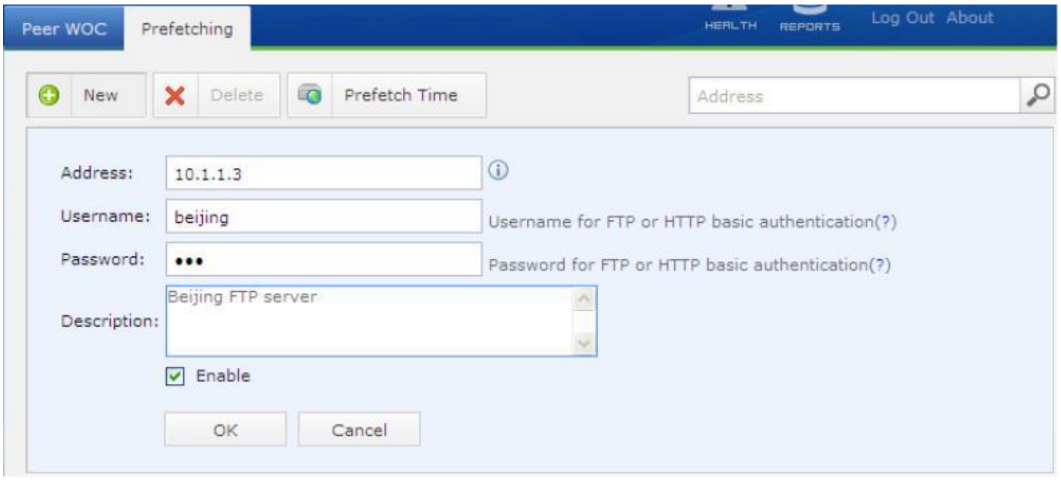
We provide that all other settings are completed. The following only focuses on prefetching settings, others being ignored.

First of all, confirm the following information with the Beijing network administrator:

IP address of FTP server, username and password for logging into the FTP server (not required if authentication is not required). Suppose the IP address of the FTP server is 10.1.1.3, username and password for FTP download are beijing and FTP respectively.

Perform the following steps:

1. Log in to the administrator console of HK WOC and navigate to WAN Optimization > Client > Prefething. Set the Prefetch Time during which the report files will be downloaded from the specified FTP server.
2. Enter the IP address of the FTP server and the username/password, as shown below:



Address: 10.1.1.3

Username: beijing — Username for FTP or HTTP basic authentication(?)

Password: ••• — Password for FTP or HTTP basic authentication(?)

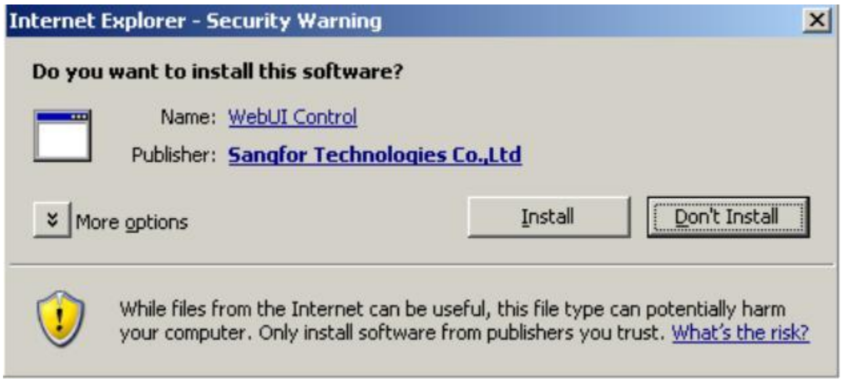
Description: Beijing FTP server

☑ Enable

Certificates

Server Certificate

Through Server Certificate page, you can import the server certificate of the HTTPS server. Before server certificate is imported, you may be asked to install the ActiveX control for importing certificate when visit the login page to the WOC administrator Web console. Click on the pop-up and click the Install button, as shown below:



Internet Explorer - Security Warning

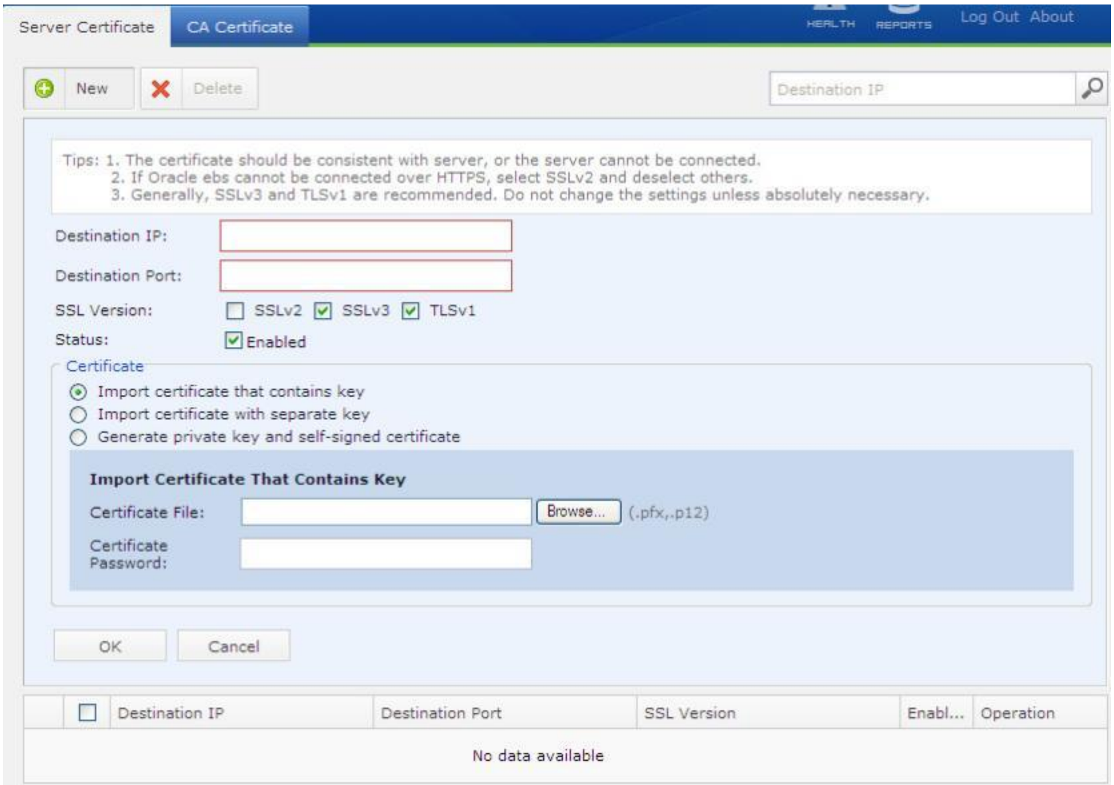
Do you want to install this software?

Name: WebUI Control

Publisher: Sangfor Technologies Co.,Ltd

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Navigate to WAN Optimization > Certificates page to enter the Server Certificate page. Click the New button to add and configure the digital server certificate, as shown in the figure below:



Tips: 1. The certificate should be consistent with server, or the server cannot be connected.
2. If Oracle ebs cannot be connected over HTTPS, select SSLv2 and deselect others.
3. Generally, SSLv3 and TLSv1 are recommended. Do not change the settings unless absolutely necessary.

Destination IP:

Destination Port:

SSL Version: □ SSLv2 ☑ SSLv3 ☑ TLSv1

Status: ☑ Enabled

Certificate

● Import certificate that contains key
○ Import certificate with separate key
○ Generate private key and self-signed certificate

Import Certificate That Contains Key

Certificate File: Browse... (.pfx,.p12)

Certificate Password:

□	Destination IP	Destination Port	SSL Version	Enabl...	Operation
No data available					

The following are the attributes of a server certificate:

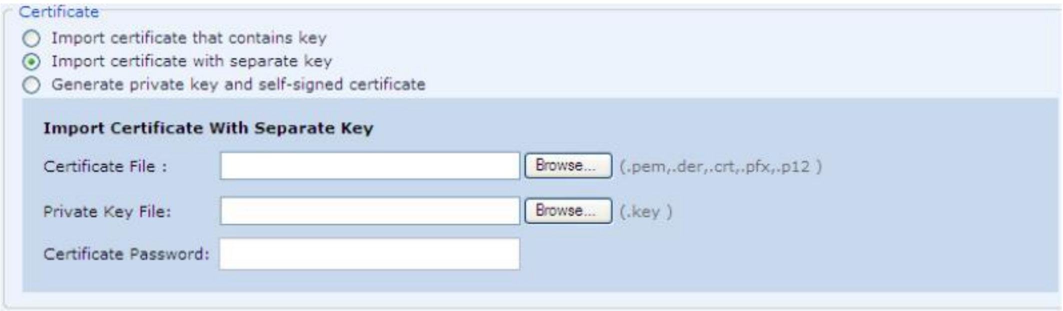
Destination IP: Specifies the IP address and port of the HTTPS server.

SSL Version: This option is intended for Oracle EBS applications. Select the version according to your specific case. If Oracle EBS uses digital certificate, both the WAN Optimization Controller (WOC) and the Oracle server should join the windows domain.

Enable: Select this option to enable the server certificate.

Import certificate that contains key: Select this option, upload the digital certificate through the Certificate File field, and enter the certificate password.

Import certificate with separate key: Select this option if the Certificate Authority (CA) has issued a certificate without key to a HTTPS server. Then import the digital certificate that contains no key, import the private key through the Private Key File field and enter the certificate assword, as shown below:



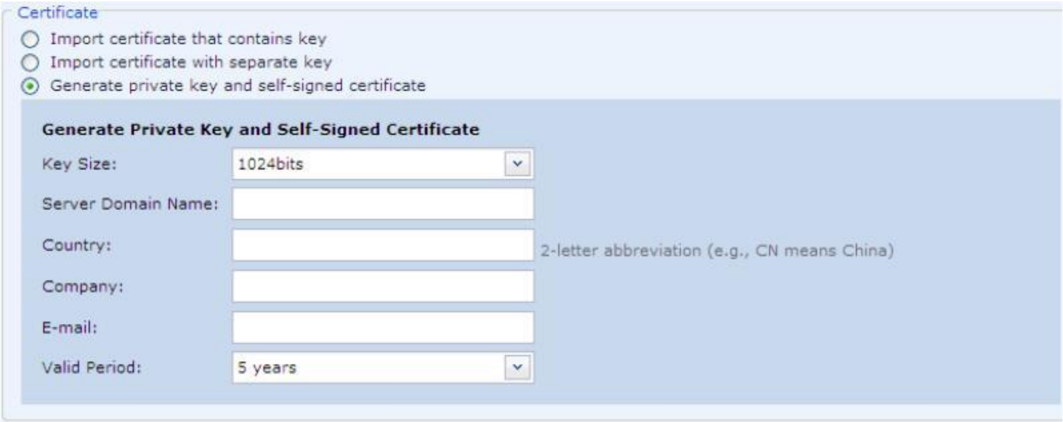
Certificate

○ Import certificate that contains key
● Import certificate with separate key
○ Generate private key and self-signed certificate

Import Certificate With Separate Key

Certificate File :	[Browse...]	(.pem,.der,.crt,.pfx,.p12)
Private Key File:	[Browse...]	(.key)
Certificate Password:		

Generate private key and self-signed certificate: Select this option if you want to generate private key and self-signed certificate with a local CA. Then specify the private key size, domain name of the server, and the certificate parameters. As shown in the figure below:



Certificate

○ Import certificate that contains key
○ Import certificate with separate key
● Generate private key and self-signed certificate

Generate Private Key and Self-Signed Certificate

Key Size:	1024bits	
Server Domain Name:		
Country:		2-letter abbreviation (e.g., CN means China)
Company:		
E-mail:		
Valid Period:	5 years	

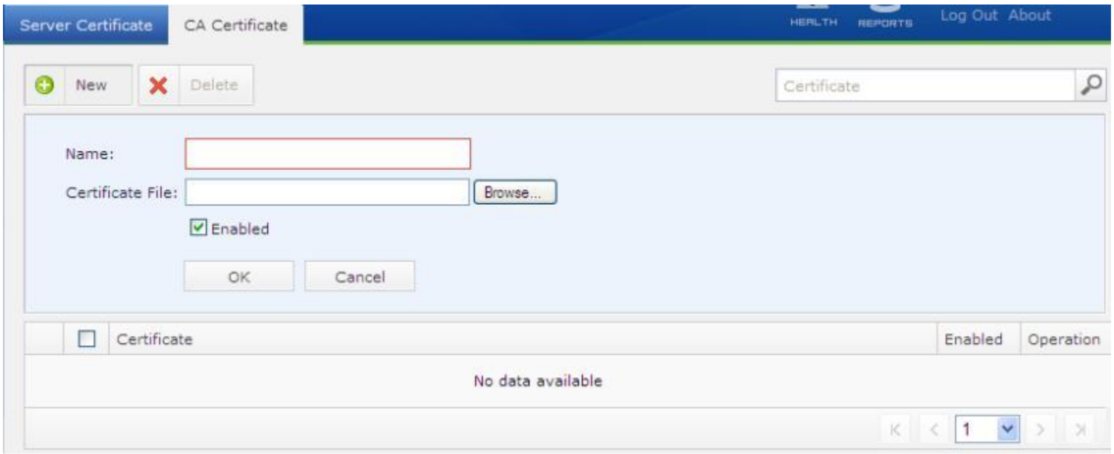
OK: Click this button to save the settings of this server certificate.

This function supports only the HTTPS applications that adopts SSL one-way authentication.

CA Certificate

You can import the root certificate issued by the Certificate Authority (CA) through the CA Certificate page.

Navigate to WAN Optimization > Certificates > CA Certificate, and click the New button:



Name:

Certificate File:

☑ Enabled

□	Certificate	Enabled	Operation

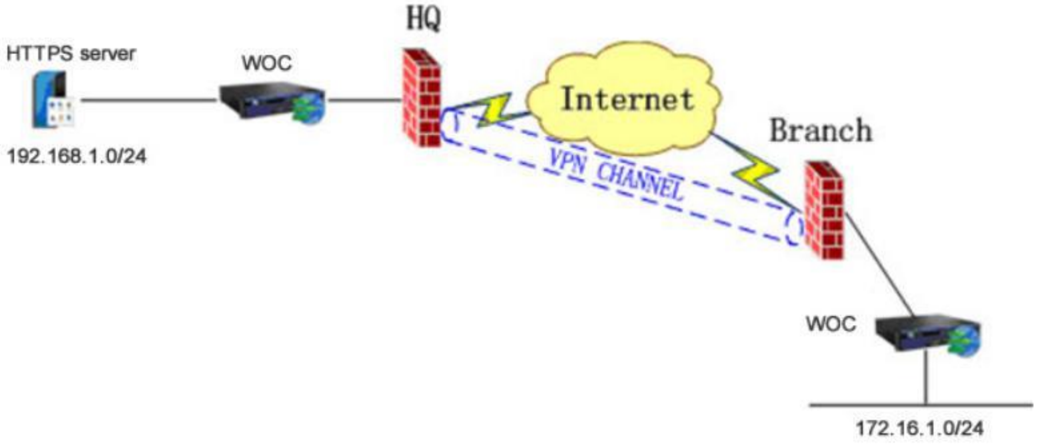
No data available

1

Enter name of the certificate, upload the digital root certificate, select Enable and click OK button to save the settings on this page.

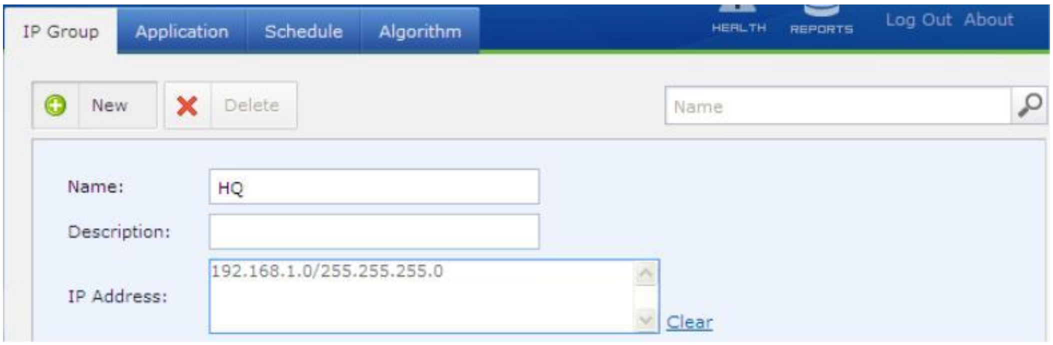
Scenario: Accelerating Access to HTTPS Server

To accelerate the branch user's access to the HTTPS server in the headquarters (HQ), the network and WAN Optimization Controller (WOC) are deployed as follows:



Perform the steps below to configure the HQ WOC:

1. On the System > Objects > IP Group page, create an IP group covering the LAN network segments of the headquarters.

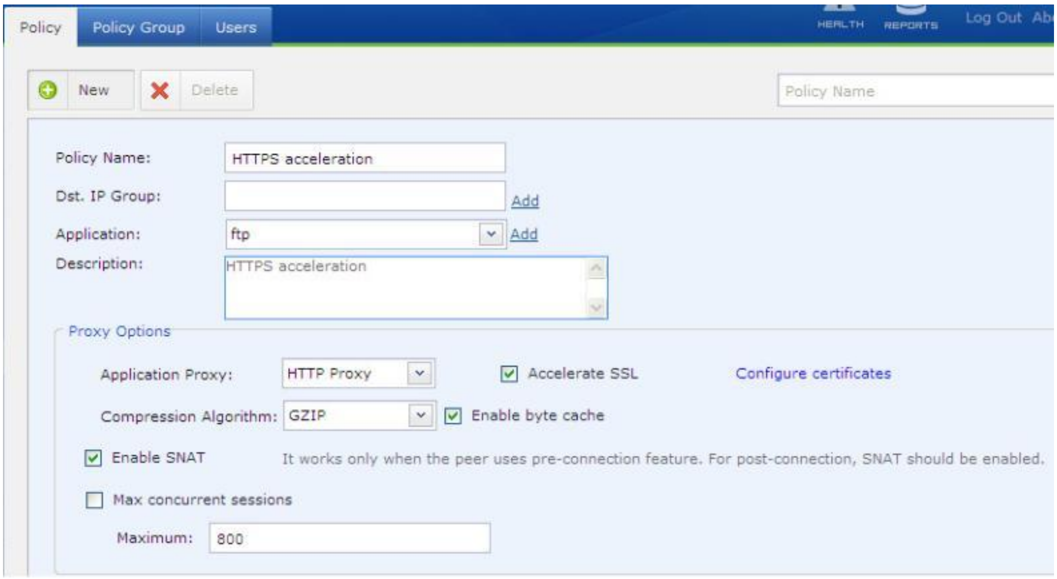


Name: HQ

Description:

IP Address: 192.168.1.0/255.255.255.0

2. On the WAN Optimization > Server > Policy page and create an acceleration policy on HTTPS. Select HTTP Proxy application protocol and Accelerate SSL option, as shown below:



Policy Name: HTTPS acceleration

Dst. IP Group:

Application: ftp

Description: HTTPS acceleration

Proxy Options

Application Proxy: HTTP Proxy ☑ Accelerate SSL

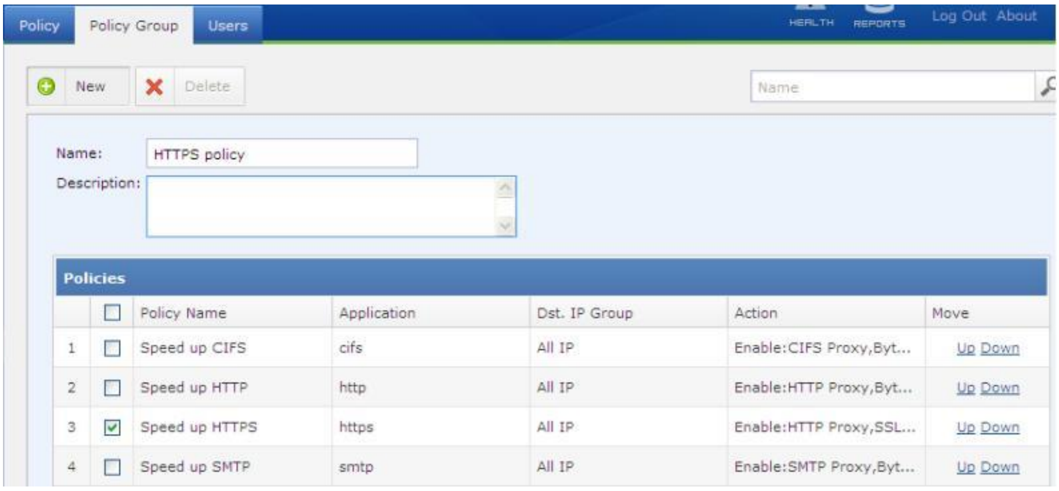
Compression Algorithm: GZIP ☑ Enable byte cache

☑ Enable SNAT It works only when the peer uses pre-connection feature. For post-connection, SNAT should be enabled.

□ Max concurrent sessions

Maximum: 800

3. On the WAN Optimization > Server > Policy Group page, create an acceleration policy group and associate it with the HTTPS acceleration policy, as shown below:



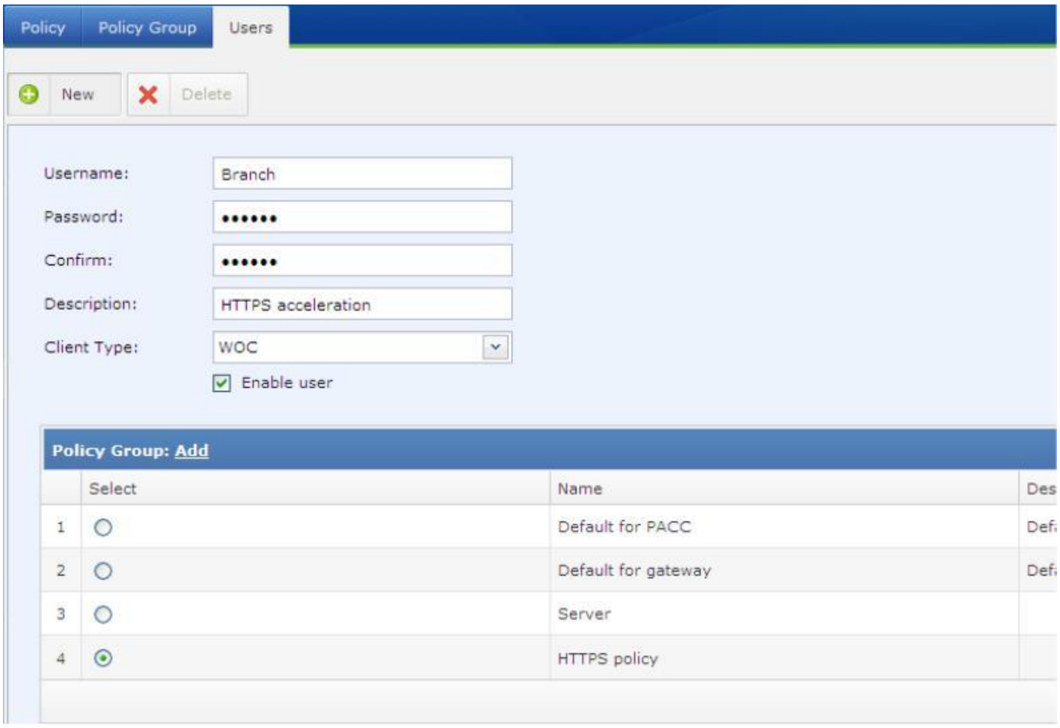
Name: HTTPS policy

Description:

Policies

	□	Policy Name	Application	Dst. IP Group	Action	Move
1	□	Speed up CIFS	cifs	All IP	Enable:CIFS Proxy,Byt...	Up Down
2	□	Speed up HTTP	http	All IP	Enable:HTTP Proxy,Byt...	Up Down
3	☑	Speed up HTTPS	https	All IP	Enable:HTTP Proxy,SSL...	Up Down
4	□	Speed up SMTP	smtp	All IP	Enable:SMTP Proxy,Byt...	Up Down

4. On the WAN Optimization > Server > Users page, create an acceleration user for the branch and associate it with the HTTPS policy group created in the previous step, as shown below:



Username: Branch

Password: ••••••

Confirm: ••••••

Description: HTTPS acceleration

Client Type: WOC

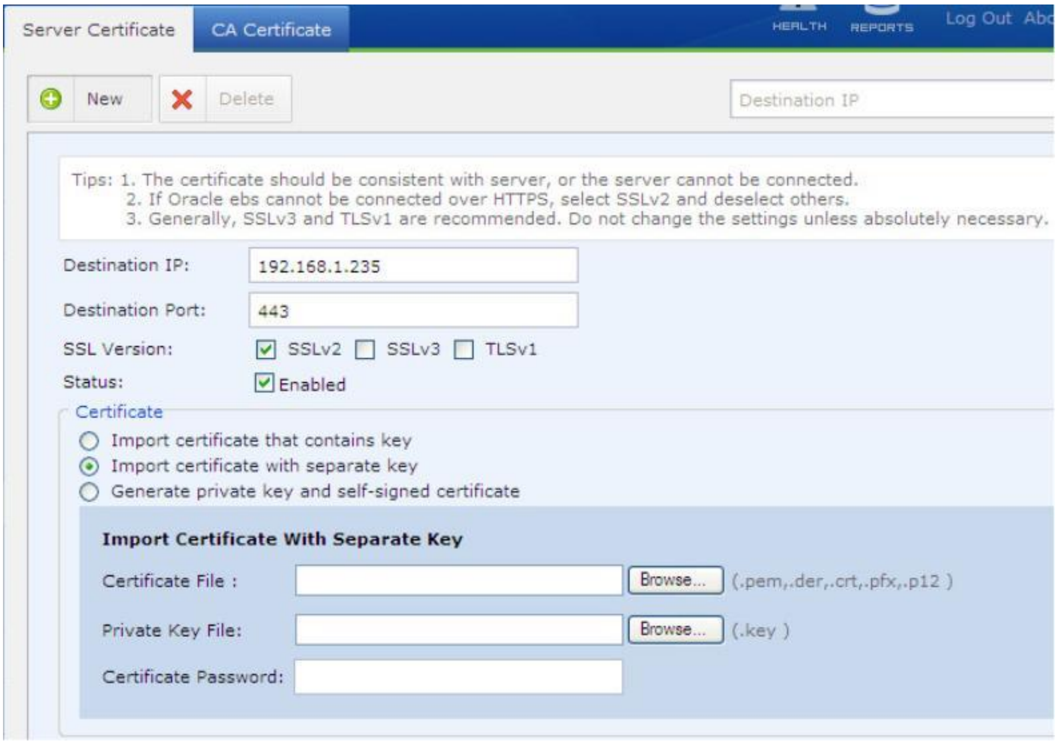
☑ Enable user

Policy Group: Add

	Select	Name	Des
1	○	Default for PACC	Def
2	○	Default for gateway	Def
3	○	Server	
4	●	HTTPS policy	

5. Go to WAN Optimization > Certificates > CA Certificate page, import the CA root certificate of the HTTPS server.

6. Go to WAN Optimization > Certificates > Server Certificate page, import the HTTPS server certificate issued by the CA, as shown below:



Tips: 1. The certificate should be consistent with server, or the server cannot be connected.
2. If Oracle ebs cannot be connected over HTTPS, select SSLv2 and deselect others.
3. Generally, SSLv3 and TLSv1 are recommended. Do not change the settings unless absolutely necessary.

Destination IP: 192.168.1.235

Destination Port: 443

SSL Version: ☑ SSLv2 □ SSLv3 □ TLSv1

Status: ☑ Enabled

Certificate

○ Import certificate that contains key

● Import certificate with separate key

○ Generate private key and self-signed certificate

Import Certificate With Separate Key

Certificate File : Browse... (.pem,.der,.crt,.pfx,.p12)

Private Key File: Browse... (.key)

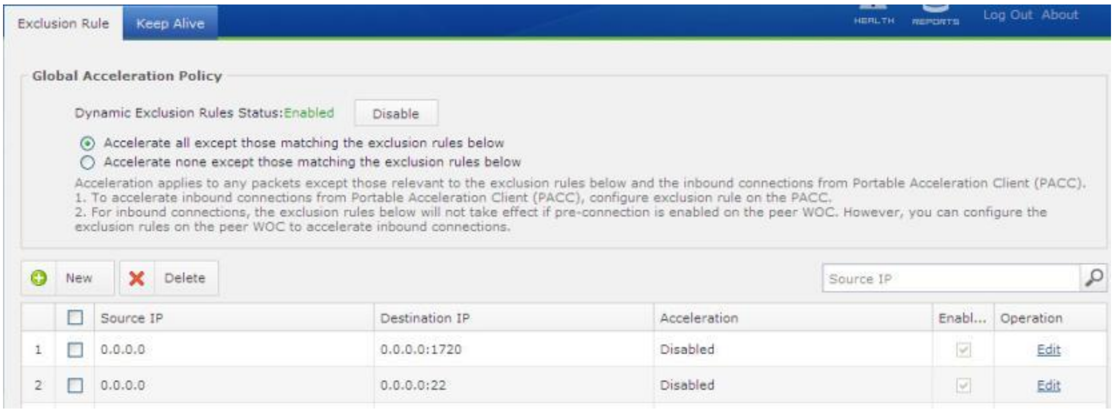
Certificate Password:

In this scenario, the server certificate that the HTTPS server acquired from the CA contains no private key, so we select the Import Certificate With Separate Key option, and import the server certificate and the private key file.

Exclusion Rule

By configuring exclusion rules, you can exclude connections to or from some IP address, subnets or network segments from the global acceleration policy. By default, connections to or from all of the IP addresses are accelerated.

Navigate to WAN Optimization > Advanced to enter the Exclusion Rule page, as shown below:



Global Acceleration Policy

Dynamic Exclusion Rules Status:Enabled Disable

● Accelerate all except those matching the exclusion rules below

○ Accelerate none except those matching the exclusion rules below

Acceleration applies to any packets except those relevant to the exclusion rules below and the inbound connections from Portable Acceleration Client (PACC).
1. To accelerate inbound connections from Portable Acceleration Client (PACC), configure exclusion rule on the PACC.
2. For inbound connections, the exclusion rules below will not take effect if pre-connection is enabled on the peer WOC. However, you can configure the exclusion rules on the peer WOC to accelerate inbound connections.

New Delete Source IP

	□	Source IP	Destination IP	Acceleration	Enabl...	Operation
1	□	0.0.0.0	0.0.0.0:1720	Disabled	☑	Edit
2	□	0.0.0.0	0.0.0.0:22	Disabled	☑	Edit

The following are the contents included on the Exclusion Rule page:

Dynamic Exclusion Rules Status: This feature is intended for debugging only.

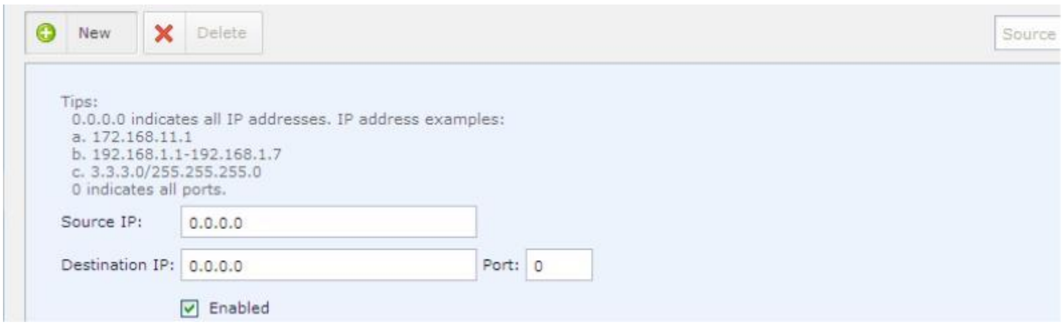
Accelerate all except those matching the exclusion rules below: Select this option and all the data packets will be accelerated except those matching any of the exclusion rules.

Accelerate none except those matching the exclusion rules below: Select this option and no data packet will be accelerated except those matching any of the exclusion rules.

There are exclusion rules already built in the Sangfor WOC that define the source/destination IP address and some common ports. The first entry (source IP 0.0.0.0, destination IP 0.0.0.0:1720) indicates that data packets sent from any IP address and destined for any IP address on port 1720 will not be accelerated, but be bypassed.

Creating Exclusion Rule

1. Navigate to WAN Optimization > Advanced > Exclusion Rule and click the New button.



Tips:
0.0.0.0 indicates all IP addresses. IP address examples:
a. 172.168.11.1
b. 192.168.1.1-192.168.1.7
c. 3.3.3.0/255.255.255.0
0 indicates all ports.

Source IP: 0.0.0.0

Destination IP: 0.0.0.0 Port: 0

☑ Enabled

2. Enter source IP address, destination address and destination port. So that data packets sent from the source IP address and destined for destination IP address on the specified port will be excluded from the global acceleration policy.

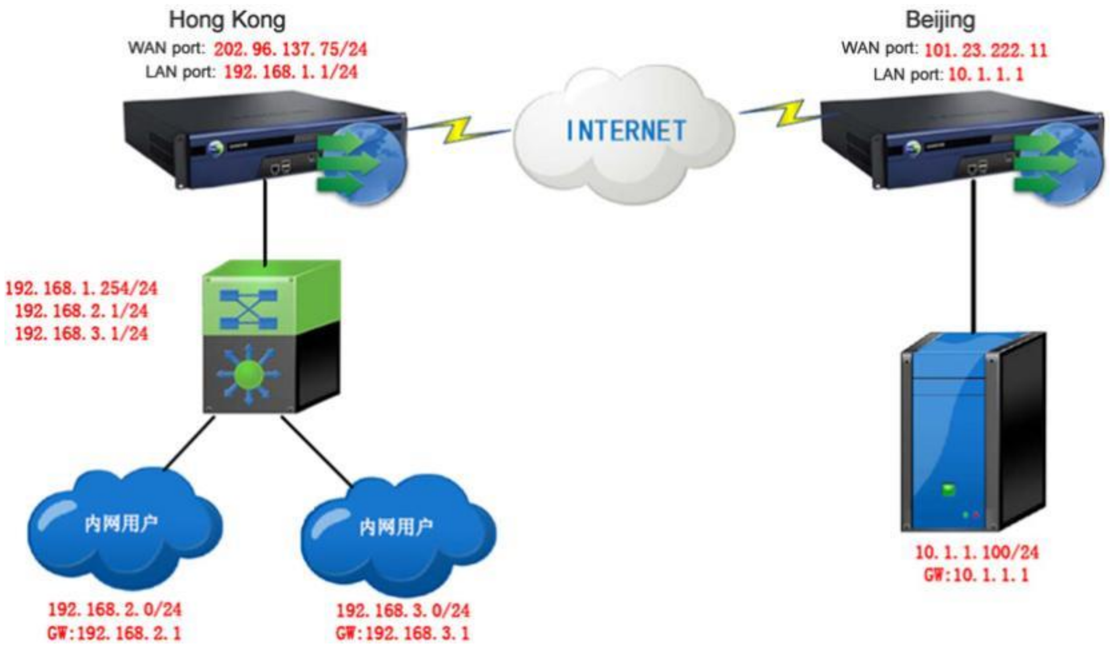
3. Select Enable.

4. Click OK and click Save and Apply.

Scenario: Acceleration Exclusion Rule for Specific Subnet

Provided the customer has established a VPN connection between HQ Beijing and Hong Kong branch. However, it is required that only Hong Kong accountants' (on network segment 192.168.30.0/24) access to Beijing server be accelerated.

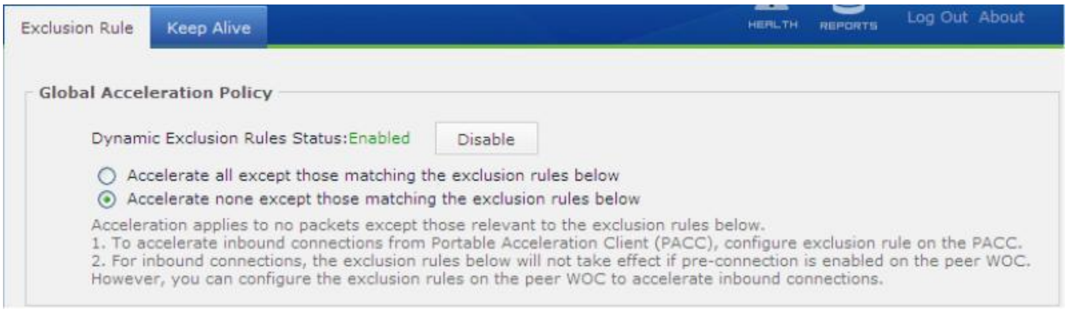
The network topology is as shown below:



We provide that all other settings are completed. The following only focuses on creating exclusion policy, others being ignored.

Perform the following steps:

1. Log in to the administrator console of HK WOC and navigate to WAN Optimization > Advanced > Exclusion Rule. Select the option Acceleration none except those matching the exclusion rules below, as shown below:



Global Acceleration Policy

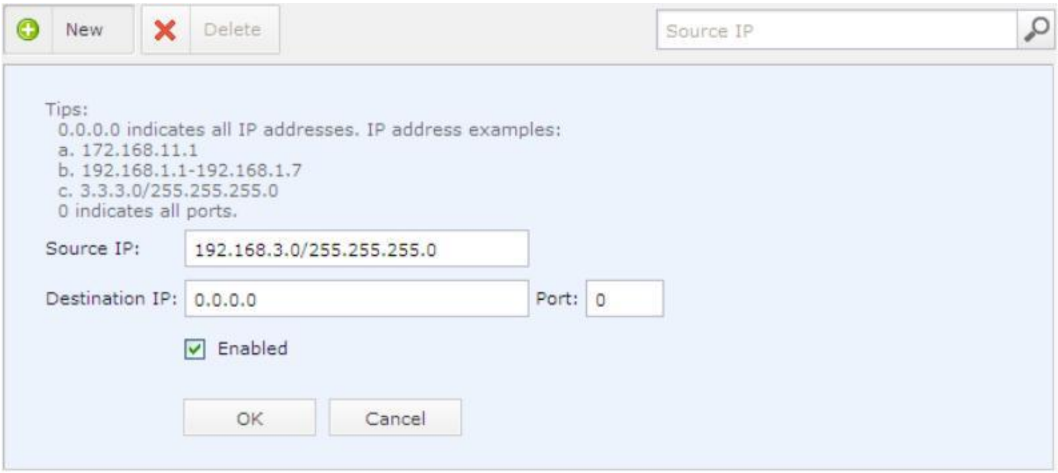
Dynamic Exclusion Rules Status:Enabled

○ Accelerate all except those matching the exclusion rules below

● Accelerate none except those matching the exclusion rules below

Acceleration applies to no packets except those relevant to the exclusion rules below.
1. To accelerate inbound connections from Portable Acceleration Client (PACC), configure exclusion rule on the PACC.
2. For inbound connections, the exclusion rules below will not take effect if pre-connection is enabled on the peer WOC. However, you can configure the exclusion rules on the peer WOC to accelerate inbound connections.

2. Click the New button to create a exclusion rule, as shown in the following figure:



Tips:
0.0.0.0 indicates all IP addresses. IP address examples:
a. 172.168.11.1
b. 192.168.1.1-192.168.1.7
c. 3.3.3.0/255.255.255.0
0 indicates all ports.

Source IP: 192.168.3.0/255.255.255.0

Destination IP: 0.0.0.0 Port: 0

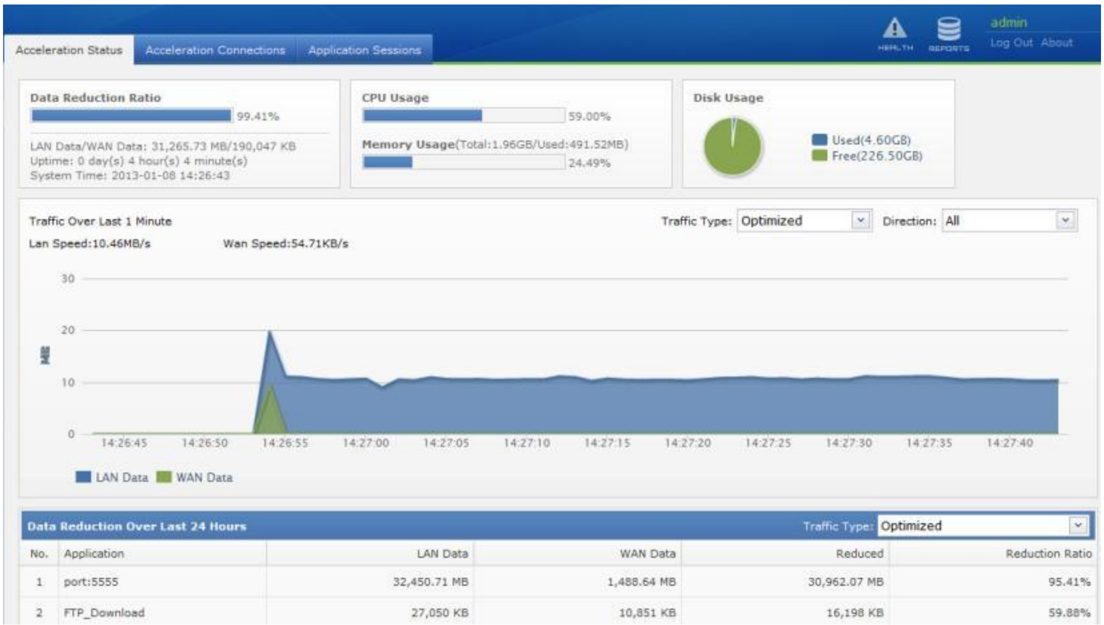
☑ Enabled

3. Click the OK and Save and Apply buttons.

If pre-connection is enabled, the exclusion rule should be configured on the peer WOC or the Portable Acceleration (PACC) client software. If pre-connection is not enabled, you can either configure the exclusion rule on the local WOC or peer WOC/PACC.

Viewing WAN Optimization Status

WAN optimization status is available on the home page of the Web administrator console.



Data Reduction Ratio 99.41%

LAN Data/WAN Data: 31,265.73 MB/190,047 KB
Uptime: 0 day(s) 4 hour(s) 4 minute(s)
System Time: 2013-01-08 14:26:43

CPU Usage 59.00%

Memory Usage(Total:1.96GB/Used:491.52MB) 24.49%

Disk Usage
🟦 Used(4.60GB)
🟩 Free(226.50GB)

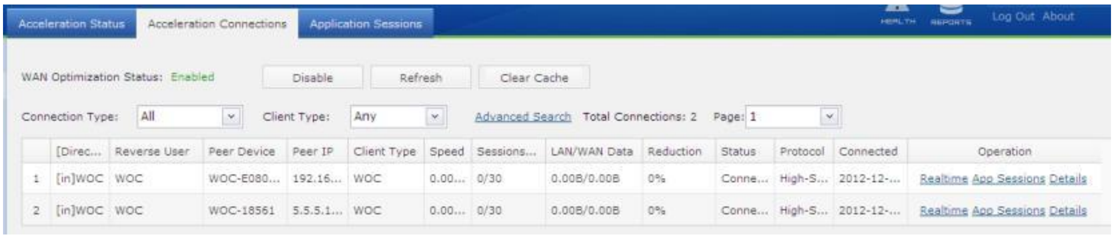
Traffic Over Last 1 Minute
Lan Speed:10.46MB/s Wan Speed:54.71KB/s
Traffic Type: Optimized Direction: All

Data Reduction Over Last 24 Hours
Traffic Type: Optimized

No.	Application	LAN Data	WAN Data	Reduced	Reduction Ratio
1	port:5555	32,450.71 MB	1,488.64 MB	30,962.07 MB	95.41%
2	FTP_Download	27,050 KB	10,851 KB	16,198 KB	59.88%

The overlaid chart in the above figure shows the overall WAN data and LAN data flow through the Sangfor WOC. While the table presents the top applications that contribute the most reduced data over the past 24 hours. Ranking is based on reduced data.

To view all the acceleration connections currently established, click the Acceleration Connections tab:

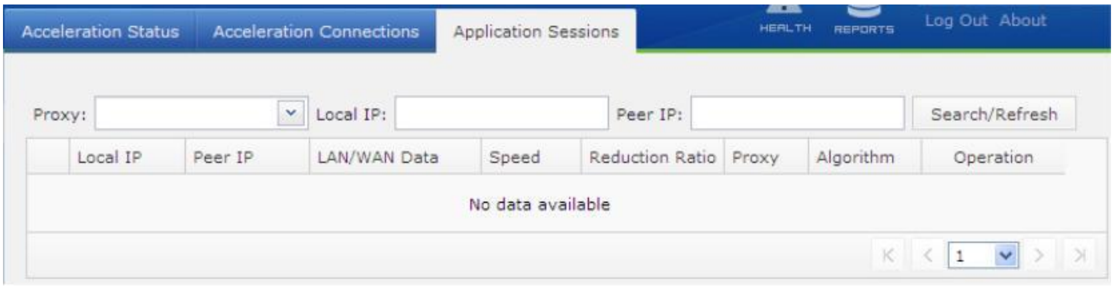


WAN Optimization Status: Enabled

Connection Type: All Client Type: Any Total Connections: 2 Page: 1

	[Direc...	Reverse User	Peer Device	Peer IP	Client Type	Speed	Sessions...	LAN/WAN Data	Reduction	Status	Protocol	Connected	Operation
1	[in]WOC	WOC	WOC-E080...	192.16...	WOC	0.00...	0/30	0.00B/0.00B	0%	Conne...	High-S...	2012-12-...	Realtime App Sessions Details
2	[in]WOC	WOC	WOC-18561	5.5.5.1...	WOC	0.00...	0/30	0.00B/0.00B	0%	Conne...	High-S...	2012-12-...	Realtime App Sessions Details

To view all the sessions currently established, click the Acceleration Sessions tab:



Proxy: Local IP: Peer IP:

	Local IP	Peer IP	LAN/WAN Data	Speed	Reduction Ratio	Proxy	Algorithm	Operation
	No data available							

Chapter 6 Bandwidth Management

For the data flowing through the Sangfor WAN Optimization Controller (WOC), data can be categorized automatically and be blocked based on the bandwidth channel settings and bandwidth control policies configured on the WOC. With this feature, you can guarantee core enterprise businesses with enough bandwidth while use of non-work-related applications are restrained or totally blocked. Bandwidth management feature is only available when the Sangfor WOC is deployed in Gateway mode, Bridge mode, Double Bridge mode or Single Arm mode.

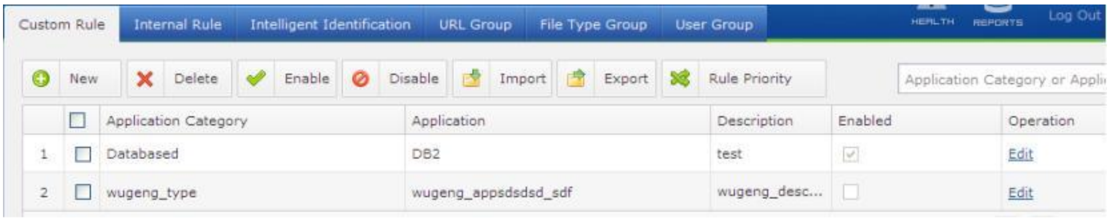
Application Identification

It is well known that download software, such as BT, Emule, etc., consume a great deal of bandwidth resources, and use of IM software, such as QQ, MSN, during office hours lowers down work efficiency and workforce productivity. Though company seniors issue regulations or set firewall to stop their employees from using these software tools, their efforts are still in vain, for these software tools are designed to be able to shy away from ordinary firewalls. A kind of solution is needed badly that employees are allowed to access the Internet but are under restrictions.

Sangfor application identification feature came into being for this reason. You can set application identification rules to identify all the data packets (including P2P traffic) flowing through the Sangfor WOC and achieve granular traffic control, by specifying packet feature, including but not limited to transfer protocol, port, packet direction and data packets size. Data packets with any the specified feature that are sent from or destined for external networks will be blocked or bypassed according to the application identification rule referenced by the associated bandwidth channel or access control policy. For the introduction of how to configure bandwidth channel and access control policy, please refer to the following two sections, Access Control Policy and Bandwidth Channel.

Application identification rule falls into internal rule and custom rule. The internal rules cannot be exported or modified except the category, while the custom rule can be added, deleted and edited.

If conflict exists between any custom rule and internal rule, only one of them will take the precedence, which is determined by the rule priority setting in Rule Priority page. You can click the Rule Priority button and modify the rule priority.



	□	Application Category	Application	Description	Enabled	Operation
1	□	Databased	DB2	test	☑	Edit
2	□	wugeng_type	wugeng_appsdsdsd_sdf	wugeng_desc...	□	Edit

To add an application identification rule, click the New button.

To delete an application identification rule, select the rule and click the Delete button.

To enable or disable an application identification rule, select the rule and click the Enable or Disable button.

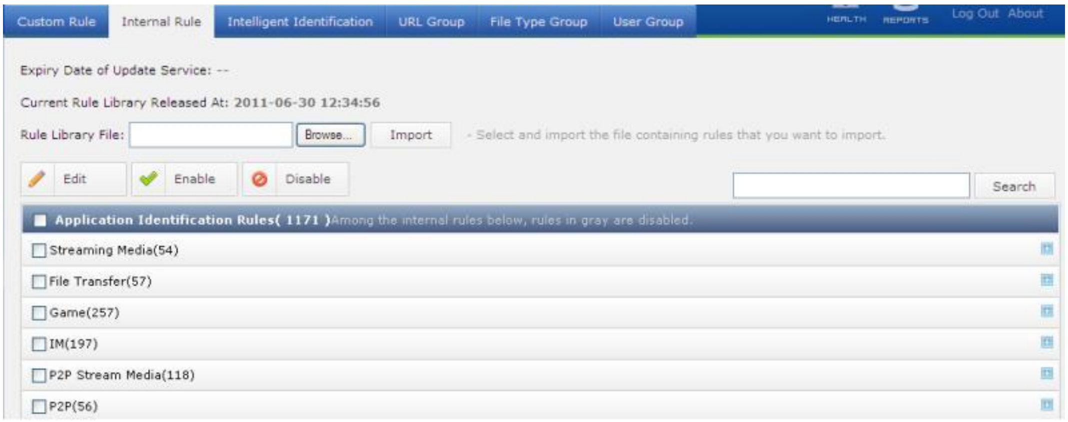
To import application identification rules from a file, click the Import button. File extension should be ccf).

To export the application identification rules, select the rules and click Export.

To search for a specific rule, enter the keyword of a rule name into the search field and click the search icon.

Add Application Identification Rule

1. Navigate to Bandwidth Management > Objects to enter Custom Rule page.



Expiry Date of Update Service: --

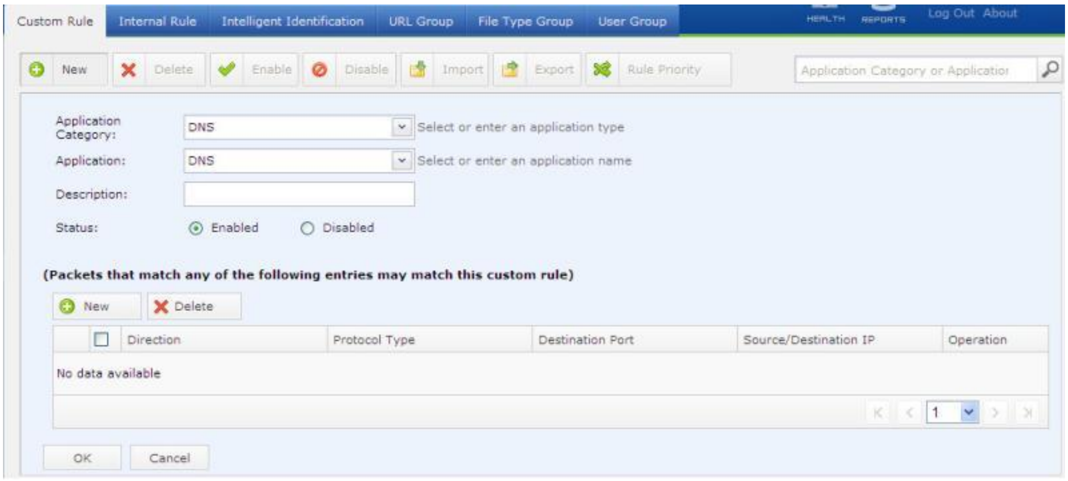
Current Rule Library Released At: 2011-06-30 12:34:56

Rule Library File:

- Select and import the file containing rules that you want to import.

□ Application Identification Rules(1171)Among the internal rules below, rules in gray are disabled.
□ Streaming Media(54)
□ File Transfer(57)
□ Game(257)
□ IM(197)
□ P2P Stream Media(118)
□ P2P(56)

2. Click the New button to add a new application identification rule, as shown below:



Application Category: DNS Select or enter an application type

Application: DNS Select or enter an application name

Description:

Status: ● Enabled ○ Disabled

(Packets that match any of the following entries may match this custom rule)

□	Direction	Protocol Type	Destination Port	Source/Destination IP	Operation
No data available					

3. Configure the following:

Application Category: Select or enter the application category.

Application: Select or enter the application name.

Description: Enter descriptive information of the application identification rule.

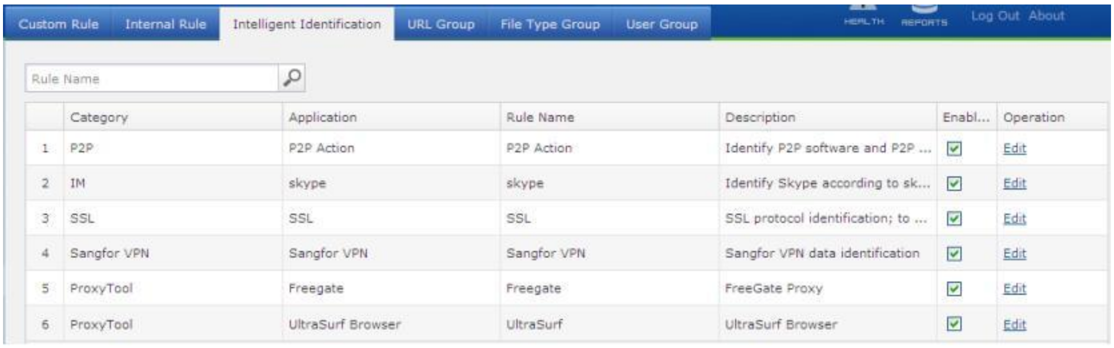
Status: Select Enabled to enable this rule.

4. Click the New button (above the table) to specify packet features.
5. Click OK to save the settings.

Since BT and IM software tools differ from each other and keep updating always, some application identification rules may get invalid for some latest versions of these software tools. SANGFOR will periodically update the internal rule library regularly. To ensure the internal rule to be auto-updated timely, please make sure that the Auto-Update page is configured properly, Application Identification/URL Library license is valid and your Sangfor WOC is connected to the Internet.

Intelligent Identification

Intelligent identification rule identifies P2P applications in clear text or cipher text, encrypted Skype data according to the Skype behaviors, and SSL certificate, Sangfor VPN data and data related by proxy. Navigate to Bandwidth Management > Objects > Intelligent Identification, and you will see the intelligent identification rules.



	Category	Application	Rule Name	Description	Enabl...	Operation
1	P2P	P2P Action	P2P Action	Identify P2P software and P2P ...	☑	Edit
2	IM	skype	skype	Identify Skype according to sk...	☑	Edit
3	SSL	SSL	SSL	SSL protocol identification; to ...	☑	Edit
4	Sangfor VPN	Sangfor VPN	Sangfor VPN	Sangfor VPN data identification	☑	Edit
5	ProxyTool	Freegate	Freegate	FreeGate Proxy	☑	Edit
6	ProxyTool	UltraSurf Browser	UltraSurf	UltraSurf Browser	☑	Edit

Application identification rule can also identify P2P applications, but it is only limited to plaintext P2P data. However, the intelligent identification rule P2P Action can identify both plaintext and encrypted P2P data.

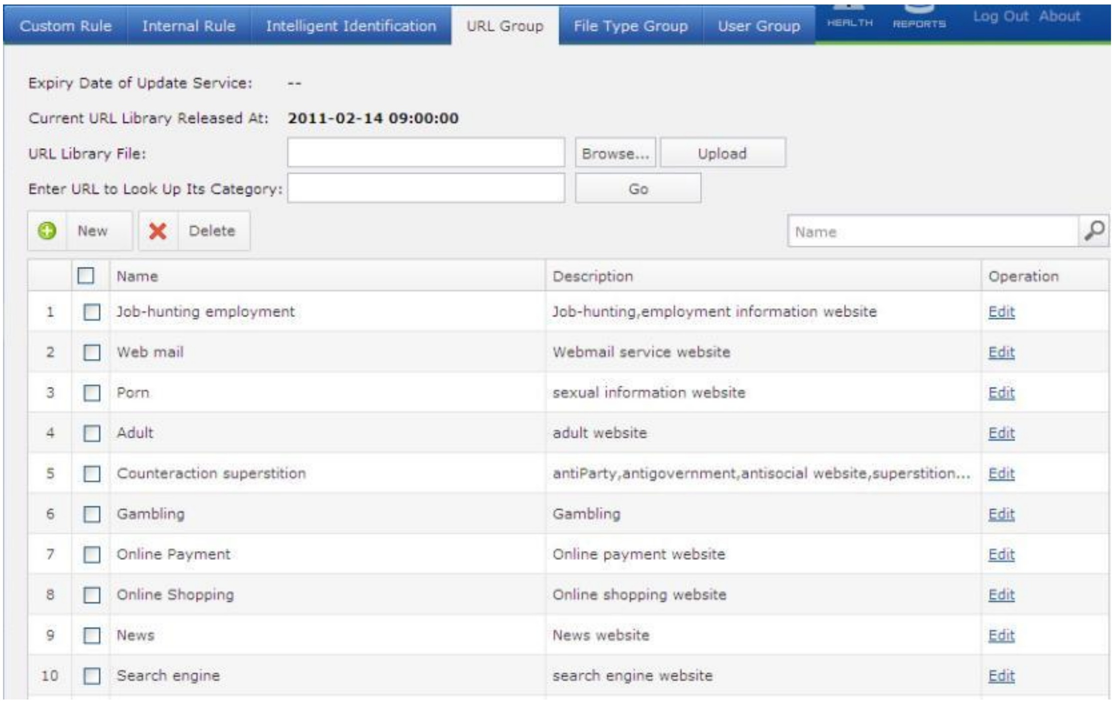
Skype data are also encrypted. To filter Skype data, you need to enable the Skype intelligent identification rule.

URL Group

URL group needs to be associated with access control policy and bandwidth channel to achieve URL filtering and bandwidth management.

Sangfor WOC is built in with some URL groups when it is delivered from the factory. You can also add new URL into the URL library.

Navigate to Bandwidth Management > Objects > URL Group to enter the following page:



Expiry Date of Update Service: --

Current URL Library Released At: 2011-02-14 09:00:00

URL Library File:

Enter URL to Look Up Its Category:

	□	Name	Description	Operation
1	□	Job-hunting employment	Job-hunting,employment information website	Edit
2	□	Web mail	Webmail service website	Edit
3	□	Porn	sexual information website	Edit
4	□	Adult	adult website	Edit
5	□	Counteraction superstition	antiParty,antigovernment,antisocial website,superstition...	Edit
6	□	Gambling	Gambling	Edit
7	□	Online Payment	Online payment website	Edit
8	□	Online Shopping	Online shopping website	Edit
9	□	News	News website	Edit
10	□	Search engine	search engine website	Edit

The following are the contents included on the URL Group page:

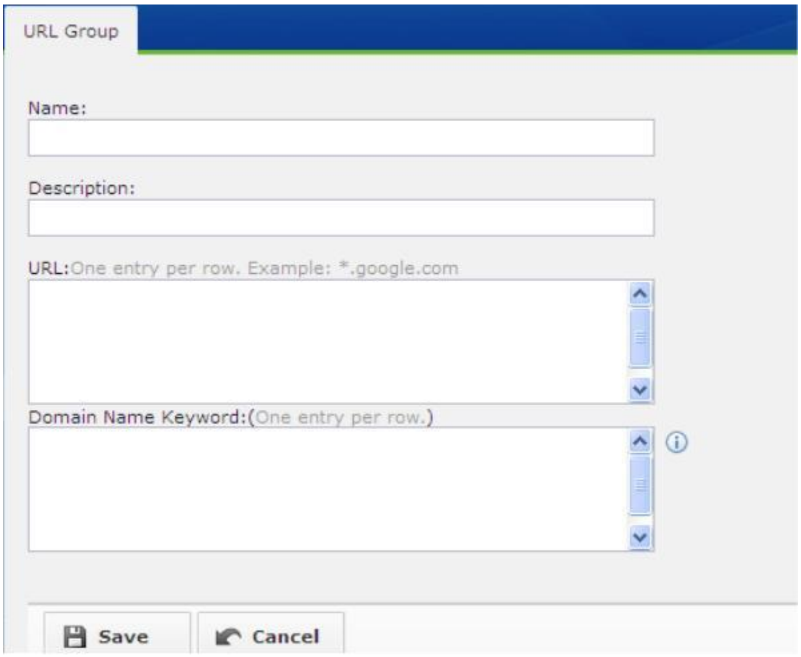
Expiry Date of Update Service: Indicates the date on which update service for URL library will expire.

Current URL Library Released At: Indicates the time when the current URL library is released to public.

URL Library File: Click the Browse button to select the URL library file from the local PC and then click Upload to update the current URLs manually if your Sangfor WOC cannot connect to the Internet.

Enter URL to Look Up Its Category: Enter a domain name and click the Go button to look up what category does the URL belongs to in the URL library. For instance, enter www.sina.com and click Go, and the search result shows News.

To add a new URL group, click the New button.



URL Group

Name:

Description:

URL:One entry per row. Example: *.google.com

Domain Name Keyword:(One entry per row.)

Name: Enter a name for the URL group.

Description: Enter descriptive information for the URL group.

URL: Enter the URL address(es). Wildcard character is supported.

Domain Name Keyword: If this field is configured, the URL group will be matched in case the domain name keyword is included in the URL address.

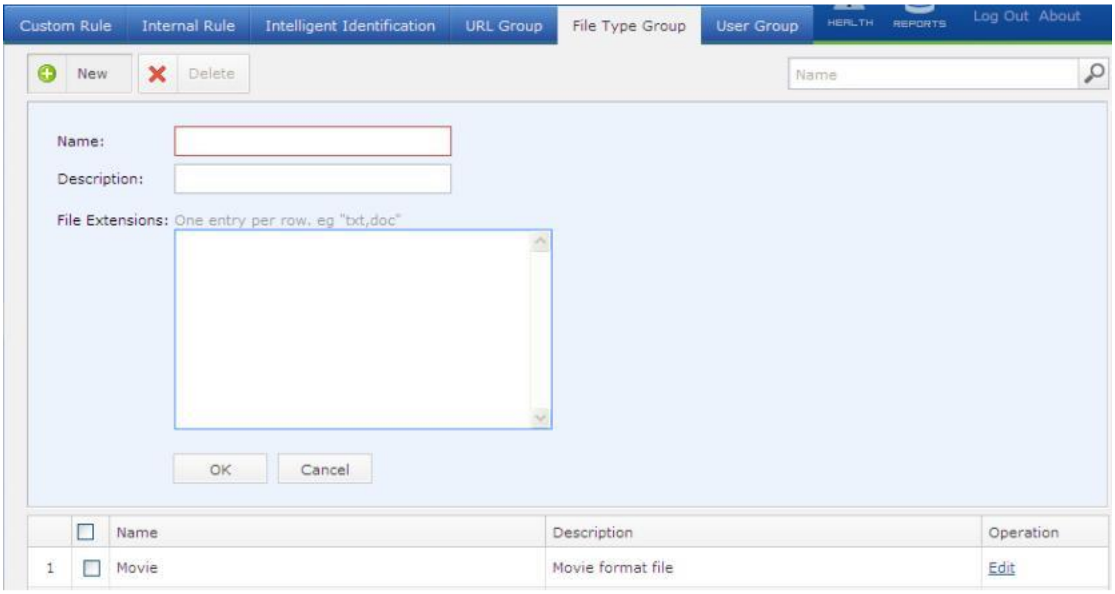
Up to 100 URL groups (internal and custom URL groups) are supported. As to the custom URL groups, you can have as many as 10 URL groups enabled at the same time. Multiple URL groups can be disabled as well.

File Type Group

File type group needs to be associated with access control policy to control HTTP/FTP upload and download and bandwidth channel to control the upload and download bandwidth of the configured file types (in the file type group).

Sangfor WOC is built in with file type groups when it is delivered from the factory. You can also add new file type group.

To add a new file type group, navigate to Bandwidth Management > Objects > File Type Group and click the New button.



Name:

Description:

File Extensions: One entry per row. eg "txt,doc"

	□	Name	Description	Operation
1	□	Movie	Movie format file	Edit

Name: Defines the name of the new file type group.

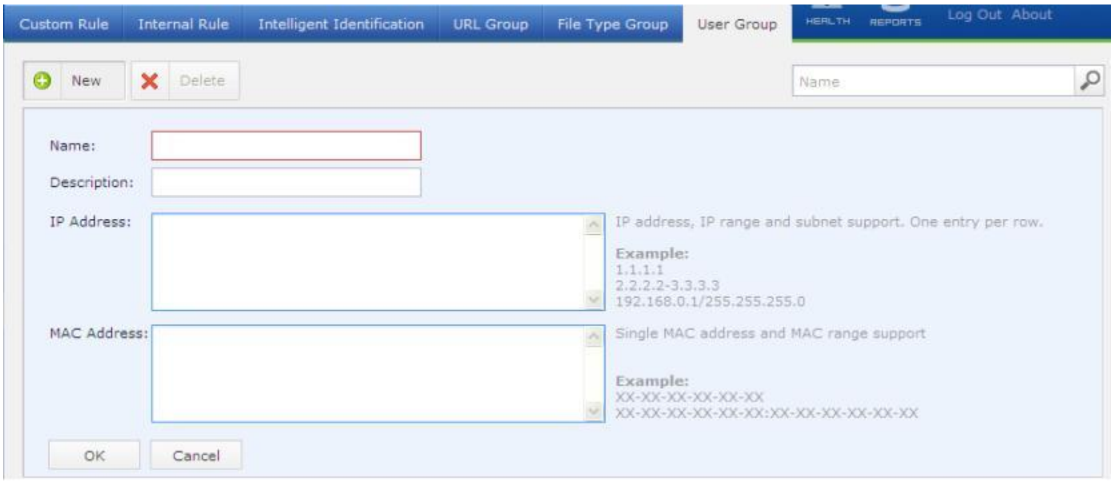
Description: Gives a brief description to this file type group.

File Extension: Configures the extension of file type, one entry per row.

A file type cannot be included in two groups.

User Group

Users in internal network can be divided and included in a user group, based the IP address or MAC address. To add a new user group, navigate to Bandwidth Management > Objects > User Group and click the New button.



Name:

Description:

IP Address: IP address, IP range and subnet support. One entry per row.

Example:
1.1.1.1
2.2.2.2-3.3.3.3
192.168.0.1/255.255.255.0

MAC Address: Single MAC address and MAC range support

Example:
XX-XX-XX-XX-XX-XX
XX-XX-XX-XX-XX-XX:XX-XX-XX-XX-XX-XX

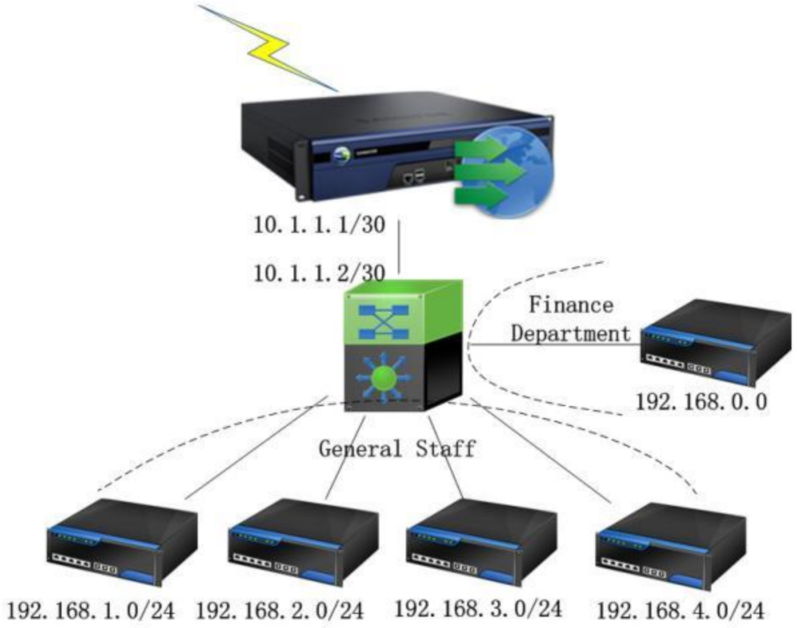
As shown on the above page, you create user group based on IP address or MAC address.

The IP address can be single IP address, IP range and subnet; MAC address can be single MAC address and MAC range. IP address and MAC address are with OR logic, which means, if data packet matches either IP address or MAC address of this user group, the related user will be regarded as a user in this user group and may match the policies associated with this user group.

If there is a layer 3 switch in the local area network, the MAC address contained in the header of the data packet will be the MAC address of the layer 3 switch. In that case, you need to add a user group based on IP address, for the MAC address will NOT take effect then.

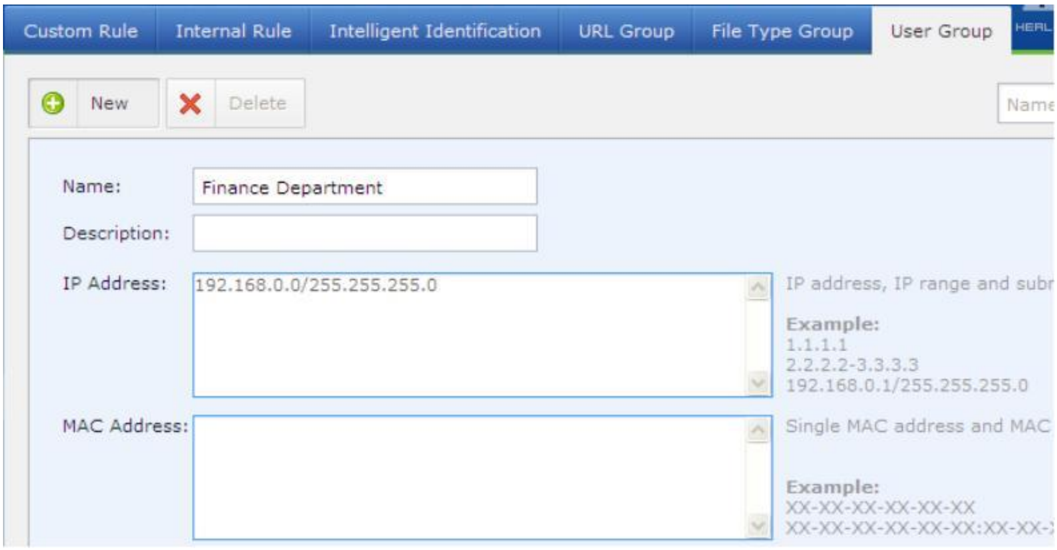
Scenario: Creating User Group

The network topology is as shown in the figure below:



To add the following three user groups, Finance Department (192.168.0.0/24), Managers (192.168.1.100, 192.168.2.100, 192.168.3.100 and 192.168.4.100) and General Staff (all other IP addresses), perform the following steps:

1. Go to Bandwidth Management > Objects > User Group and create a user group named Finance Department.



Name: Finance Department

Description:

IP Address: 192.168.0.0/255.255.255.0

IP address, IP range and subr

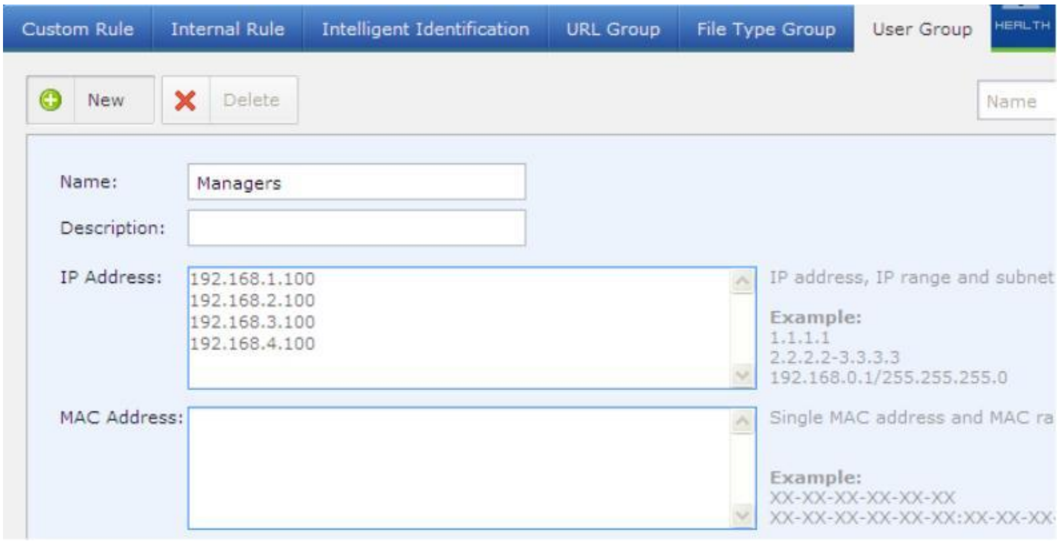
Example:
1.1.1.1
2.2.2.2-3.3.3.3
192.168.0.1/255.255.255.0

MAC Address:

Single MAC address and MAC

Example:
XX-XX-XX-XX-XX-XX
XX-XX-XX-XX-XX-XX:XX-XX-

2. Create a user group named Managers.



Name: Managers

Description:

IP Address:
192.168.1.100
192.168.2.100
192.168.3.100
192.168.4.100

IP address, IP range and subnet

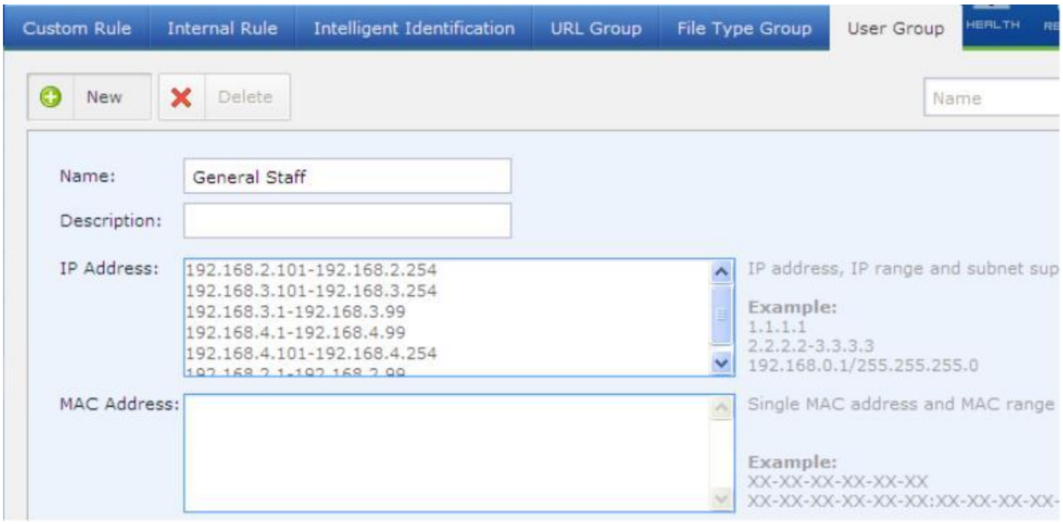
Example:
1.1.1.1
2.2.2.2-3.3.3.3
192.168.0.1/255.255.255.0

MAC Address:

Single MAC address and MAC ra

Example:
XX-XX-XX-XX-XX-XX
XX-XX-XX-XX-XX-XX:XX-XX-XX-

3. Create a user group named General Staff, as shown below:



Name: General Staff

Description:

IP Address:
192.168.2.101-192.168.2.254
192.168.3.101-192.168.3.254
192.168.3.1-192.168.3.99
192.168.4.1-192.168.4.99
192.168.4.101-192.168.4.254
192.168.2.1-192.168.2.99

IP address, IP range and subnet sup

Example:
1.1.1.1
2.2.2.2-3.3.3.3
192.168.0.1/255.255.255.0

MAC Address:

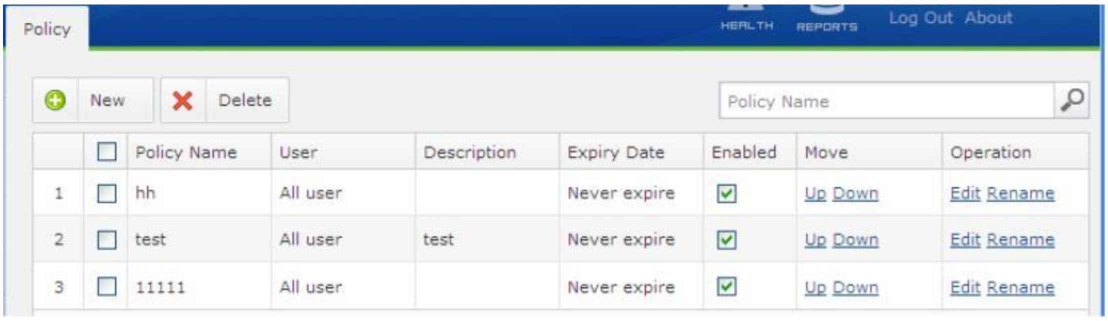
Single MAC address and MAC range

Example:
XX-XX-XX-XX-XX-XX
XX-XX-XX-XX-XX-XX:XX-XX-XX-XX-

While creating a new user group, please note that an IP address or MAC address can belong to several user groups. If you want to distinguish some users from a subnet, a user group covering most of IP addresses of the subnet must be composed of some shorter ranges of IP addresses.

Access Control Policy

An access control policy specifies the Internet access privilege of LAN users, such as what applications, services and URLs are accessible, which types of files are allowed to be uploaded or downloaded, etc.



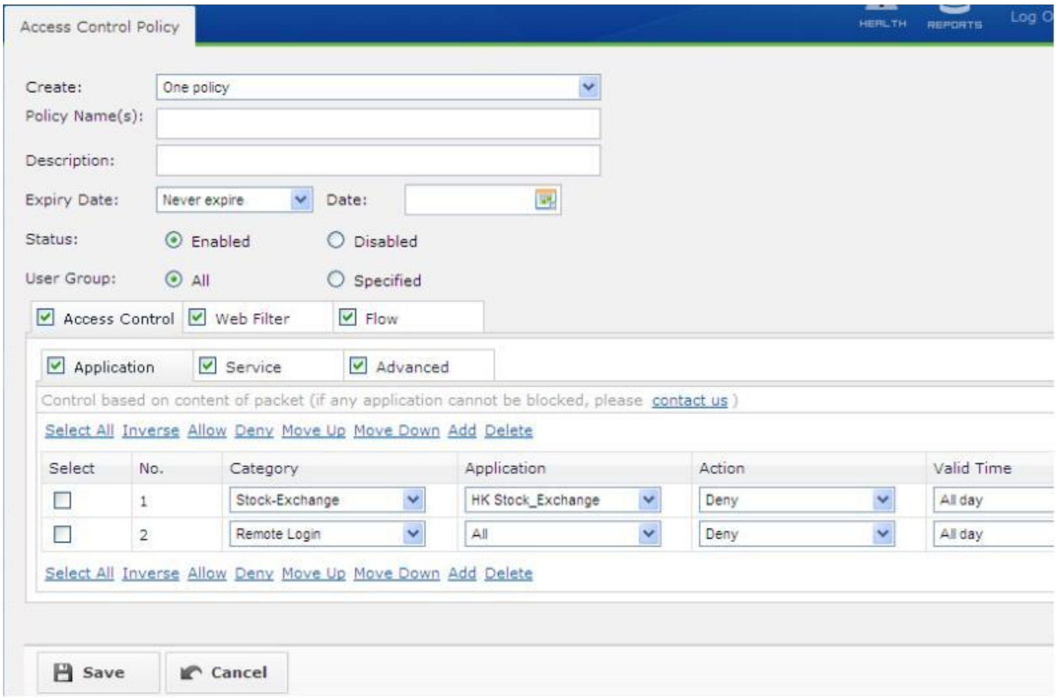
	□	Policy Name	User	Description	Expiry Date	Enabled	Move	Operation
1	□	hh	All user		Never expire	☑	Up Down	Edit Rename
2	□	test	All user	test	Never expire	☑	Up Down	Edit Rename
3	□	11111	All user		Never expire	☑	Up Down	Edit Rename

To have an access control policy take effect, you need to associate it with some user group. For information about user group, please refer to the above section.

Creating Access Control Policy

1. Navigate to Bandwidth Management > Access Control to enter the Access Control Policy page.

2. Click the New button to add a new access control policy.



Create: One policy
Policy Name(s):
Description:
Expiry Date: Never expire Date:
Status: ● Enabled ○ Disabled
User Group: ● All ○ Specified

☑ Access Control ☑ Web Filter ☑ Flow

☑ Application ☑ Service ☑ Advanced

Control based on content of packet (if any application cannot be blocked, please contact us)

Select All Inverse Allow Deny Move Up Move Down Add Delete

Select	No.	Category	Application	Action	Valid Time
□	1	Stock-Exchange	HK Stock_Exchange	Deny	All day
□	2	Remote Login	All	Deny	All day

Select All Inverse Allow Deny Move Up Move Down Add Delete

3. Configure the following:

Create: Select One policy or Multiple policies to create one or multiple policies based on the settings on the current page. If Multiple policies is selected, you need to enter more than one entries in the Policy Name(s) field.

Policy Name: Enter name for the access control policy (policies) you want to create.

Description: Enter descriptive information for the access control policy.

Expiry Date: Specify on which date the access control policy will expire. You can also select Never expire to set the valid period of the policy as infinite.

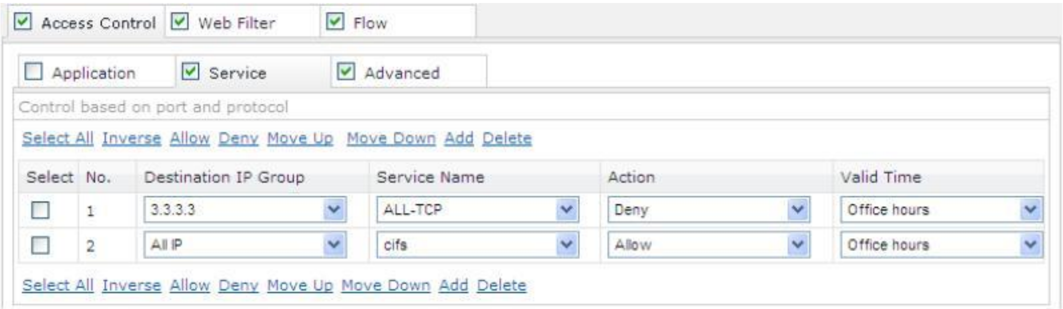
Status: Select Enabled to enable the policy, otherwise, the policy will never take effect.

User Group: Select the user group to which the access control policy is applied, All or Specified. If Specified is selected, you need to select the desired user group from the Available textbox and move them to the Selected textbox.

4. Specify the application, services, proxy types on Access Control tab.

The applications on Access Control > Application tab come from the internal application identification library and custom application identification rules. Data packet flowing through the Sangfor WOC will be inspected and analyzed based on the packet feature. If it matches any of the application entries, it may be allowed or denied according to the specified action.

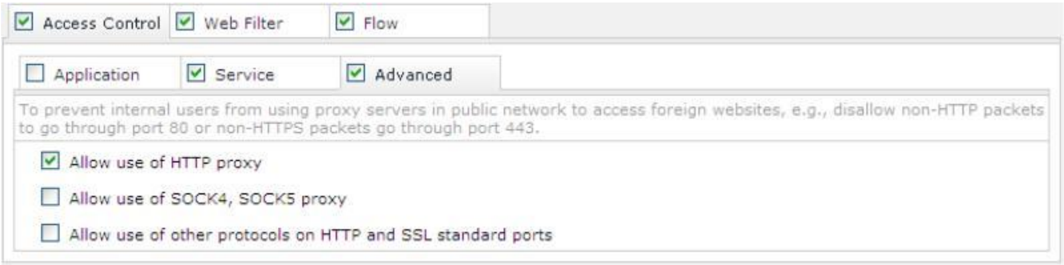
The services in Access Control > Service come from the applications predefined in System > Objects > Applications, while destination IP addresses come from the IP groups predefined in System > Objects > IP Group. Data packets flowing through the Sangfor WOC will inspected and analyzed based on the packet feature. If it matches any of the service entries, it may be allowed or denied according to the specified action.


☑ Access Control
☑ Web Filter
☑ Flow
□ Application
☑ Service
☑ Advanced
Select All Inverse Allow Deny Move Up Move Down Add Delete
Select All Inverse Allow Deny Move Up Move Down Add Delete

Control based on port and protocol

Select	No.	Destination IP Group	Service Name	Action	Valid Time
□	1	3.3.3.3	ALL-TCP	Deny	Office hours
□	2	All IP	cifs	Allow	Office hours

On Access Control > Advanced tab, you can decide whether to allow users to use proxy server (HTTP proxy and SOCK proxy) in public networks or certain ports. If use of proxy server is allowed, the users will shy away from Sangfor WOC.



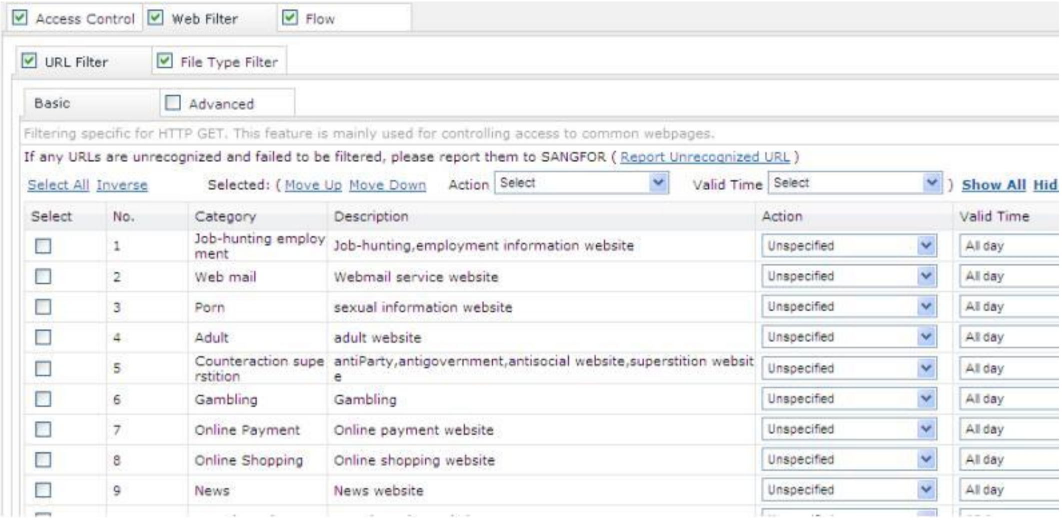
To prevent internal users from using proxy servers in public network to access foreign websites, e.g., disallow non-HTTP packets to go through port 80 or non-HTTPS packets go through port 443.

☑ Allow use of HTTP proxy

□ Allow use of SOCK4, SOCK5 proxy

□ Allow use of other protocols on HTTP and SSL standard ports

5. Specify URL categories and file types on Web Filter tab.



Filtering specific for HTTP GET. This feature is mainly used for controlling access to common webpages.

If any URLs are unrecognized and failed to be filtered, please report them to SANGFOR (Report Unrecognized URL)

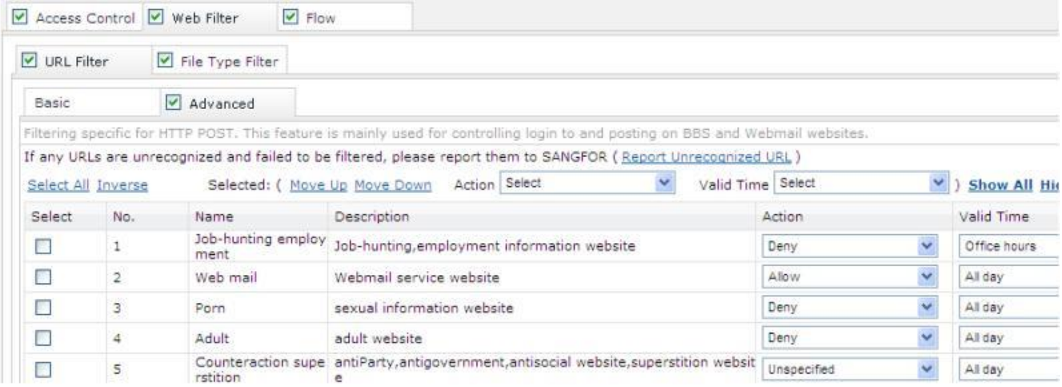
Select All Inverse Selected: (Move Up Move Down Action Select Valid Time Select) Show All Hid

Select	No.	Category	Description	Action	Valid Time
□	1	Job-hunting employment	Job-hunting,employment information website	Unspecified	All day
□	2	Web mail	Webmail service website	Unspecified	All day
□	3	Porn	sexual information website	Unspecified	All day
□	4	Adult	adult website	Unspecified	All day
□	5	Counteraction superstition	antiParty,antigovernment,antisocial website,superstition website	Unspecified	All day
□	6	Gambling	Gambling	Unspecified	All day
□	7	Online Payment	Online payment website	Unspecified	All day
□	8	Online Shopping	Online shopping website	Unspecified	All day
□	9	News	News website	Unspecified	All day

The URL categories on Web Filter > URL Filter tab come from the URL groups predefined in Bandwidth Management > Objects > URL Group. Select the action Deny, and you can prevent the associated LAN users from using HTTP GET or HTTP POST to access the websites that are categorized into that URL category.

Sangfor WOC is integrated with a bunch of URL groups. To update the URL groups in the URL library, you need to purchase the Application Identification/URL Library license or add URL groups by yourself.

Different from the Web Filter > URL Filter > Basic tab that includes rules filtering web browsing behaviors, Web Filter > URL Filter > Advanced tab includes rules restraining user's HTTP POST behaviors. In other words, if you want to allow users to browse a website but cannot write post at the website, configure a URL filter rule in Web Filter > URL Filter > Advanced.



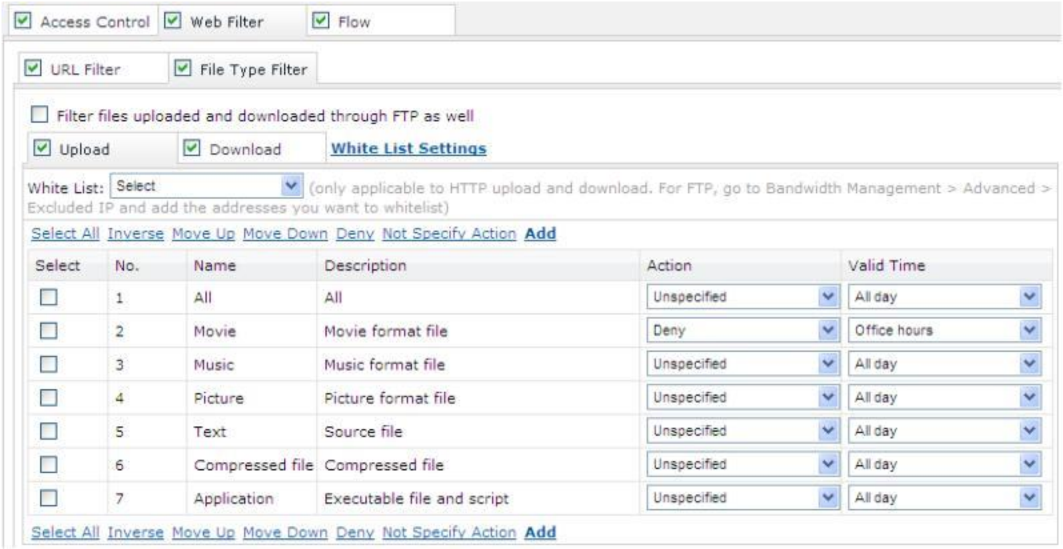
Filtering specific for HTTP POST. This feature is mainly used for controlling login to and posting on BBS and Webmail websites.

If any URLs are unrecognized and failed to be filtered, please report them to SANGFOR (Report Unrecognized URL)

Select All Inverse Selected: (Move Up Move Down Action Select Valid Time Select) Show All Hi

Select	No.	Name	Description	Action	Valid Time
□	1	Job-hunting employment	Job-hunting,employment information website	Deny	Office hours
□	2	Web mail	Webmail service website	Allow	All day
□	3	Porn	sexual information website	Deny	All day
□	4	Adult	adult website	Deny	All day
□	5	Counteraction superstition	antiParty,antigovernment,antisocial website,superstition website	Unspecified	All day

By configuring file type filter rule, you can prevent users from uploading and downloading certain types of files through HTTP/FTP from any website except the whitelisted websites. The available file types are predefined in Bandwidth Management > Objects > File Type Group.



☑ Access Control ☑ Web Filter ☑ Flow

☑ URL Filter ☑ File Type Filter

□ Filter files uploaded and downloaded through FTP as well

☑ Upload ☑ Download White List Settings

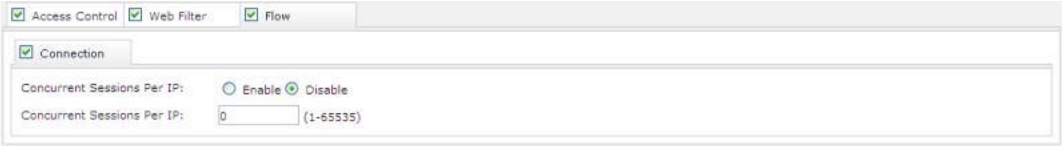
White List: Select (only applicable to HTTP upload and download. For FTP, go to Bandwidth Management > Advanced > Excluded IP and add the addresses you want to whitelist)

Select All Inverse Move Up Move Down Deny Not Specify Action Add

Select	No.	Name	Description	Action	Valid Time
□	1	All	All	Unspecified	All day
□	2	Movie	Movie format file	Deny	Office hours
□	3	Music	Music format file	Unspecified	All day
□	4	Picture	Picture format file	Unspecified	All day
□	5	Text	Source file	Unspecified	All day
□	6	Compressed file	Compressed file	Unspecified	All day
□	7	Application	Executable file and script	Unspecified	All day

Select All Inverse Move Up Move Down Deny Not Specify Action Add

6. Specify number of concurrent sessions that an IP address can keep in a connection.



☑ Access Control ☑ Web Filter ☑ Flow

☑ Connection

Concurrent Sessions Per IP: ○ Enable ● Disable

Concurrent Sessions Per IP: 0 (1-65535)

On Flow > Connection tab, you can enable and set the maximum number of sessions of a single IP can keep with the external networks. If number of concurrent sessions exceeds the maximum, the excessive sessions will be disconnected.

Scenario: Creating Access Control Policy for Specific Users

The requirements are as follows:

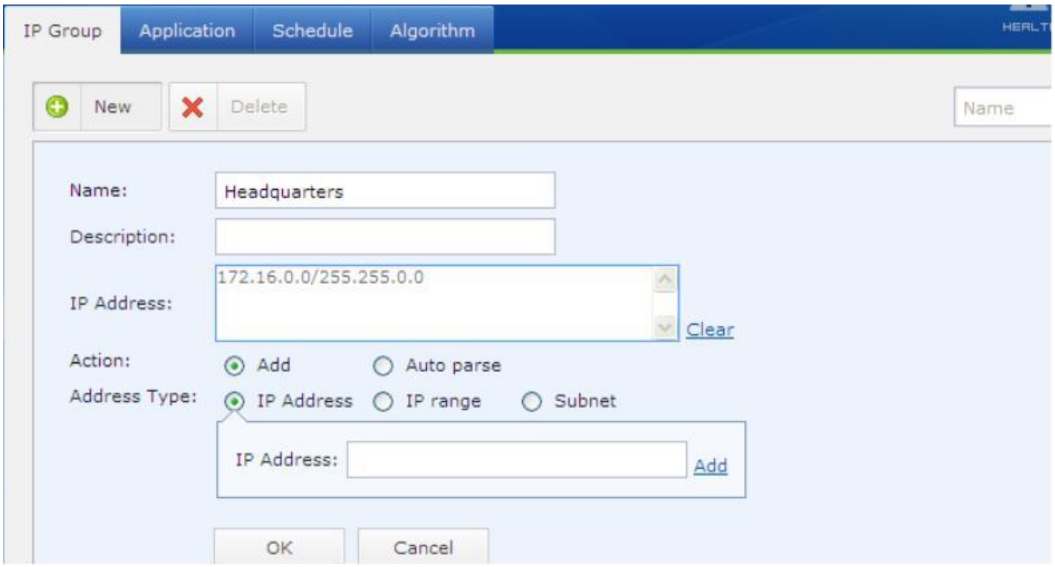
a.) Finance Department: Deny these employees to access the Internet but allow their access to the Intranet of the Headquarters (172.16.0.0/16).

b.) General Staff: Allow these employees to access the Internet but deny them to use P2P download tools; each user can have maximum 300 concurrent sessions.

c.) Managers: Allow these employees to access the Internet.

Perform the following steps:

1. Go to System > Objects > IP Group and click the New button to create an IP group, which covers the hosts at the head office.



Name: Headquarters

Description:

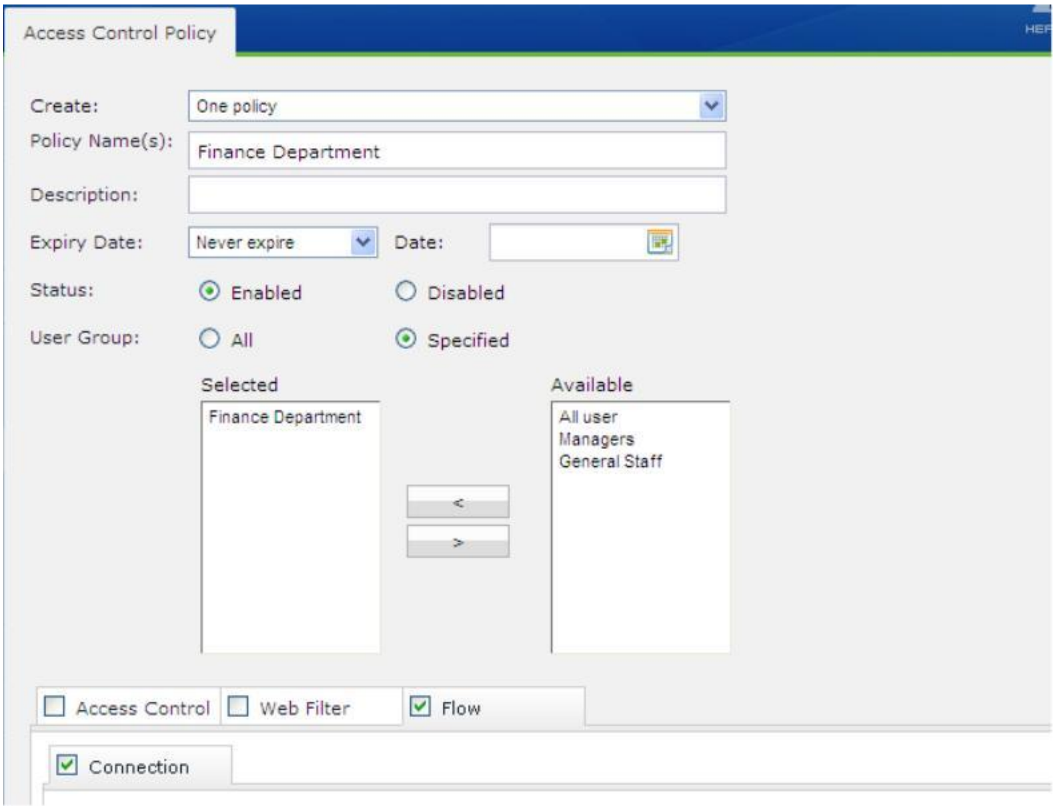
IP Address: 172.16.0.0/255.255.0.0

Action: ● Add ○ Auto parse

Address Type: ● IP Address ○ IP range ○ Subnet

IP Address:

2. Go to Bandwidth Management > Access Control > Policy to create an access control policy named Finance Department; select the user group Finance Department (suppose the group has been created), as shown below:



Create: One policy

Policy Name(s): Finance Department

Description:

Expiry Date: Never expire Date:

Status: ● Enabled ○ Disabled

User Group: ○ All ● Specified

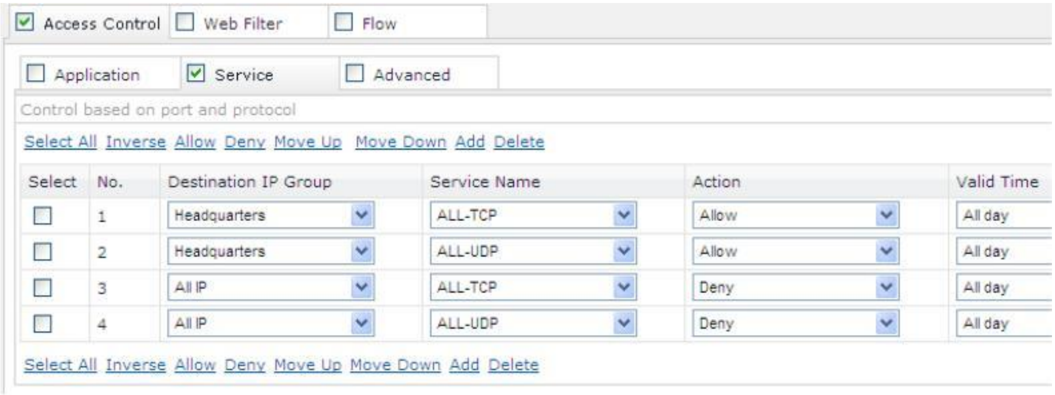
Selected: Finance Department

Available: All user, Managers, General Staff

□ Access Control □ Web Filter ☑ Flow

☑ Connection

3. Configure a rule to deny the user group Finance Department to access the Internet, as shown below:



☑ Access Control ☐ Web Filter ☐ Flow

☐ Application ☑ Service ☐ Advanced

Control based on port and protocol

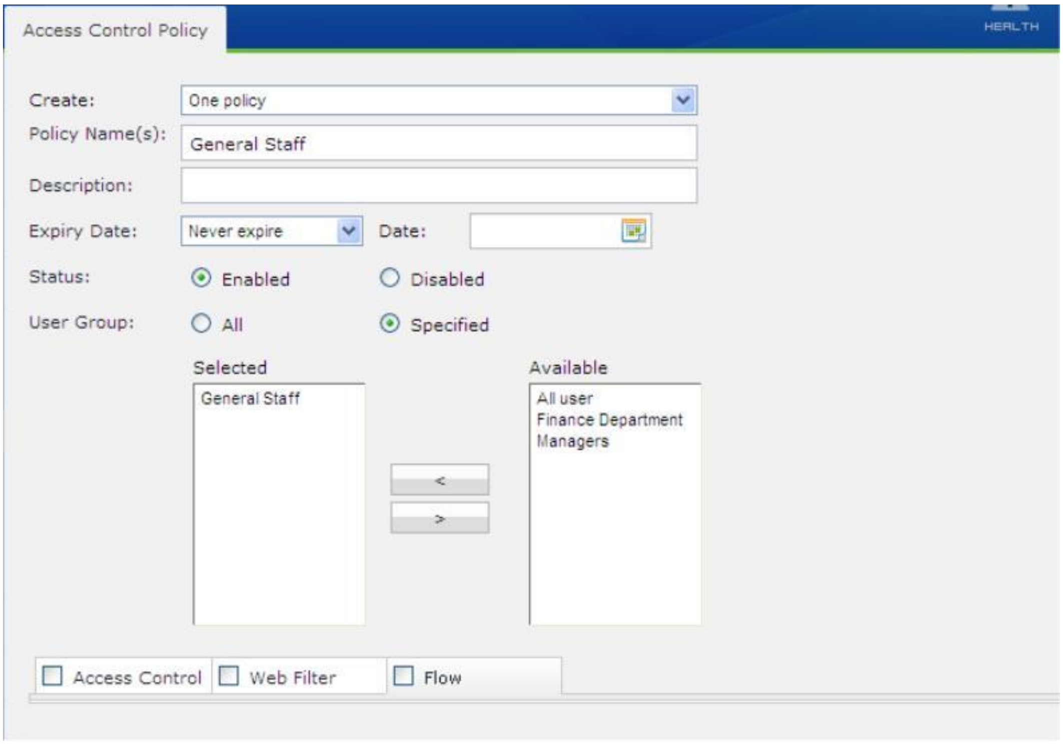
Select All Inverse Allow Deny Move Up Move Down Add Delete

Select	No.	Destination IP Group	Service Name	Action	Valid Time
☐	1	Headquarters	ALL-TCP	Allow	All day
☐	2	Headquarters	ALL-UDP	Allow	All day
☐	3	All IP	ALL-TCP	Deny	All day
☐	4	All IP	ALL-UDP	Deny	All day

Select All Inverse Allow Deny Move Up Move Down Add Delete

Internet behaviors of the users in a group can only be distinguished based on IP addresses instead of their behaviors. For instance, they may use the ping command, browse webpage, access FTP server or even video when accessing the head office and public networks. For this reason, Service rules have to be configured to control their access to specific services.

4. Configure an access control policy named General Staff, and select the user group General Staff (suppose the group has been created), as shown below:



Access Control Policy

Create: One policy

Policy Name(s): General Staff

Description:

Expiry Date: Never expire Date:

Status: ● Enabled ○ Disabled

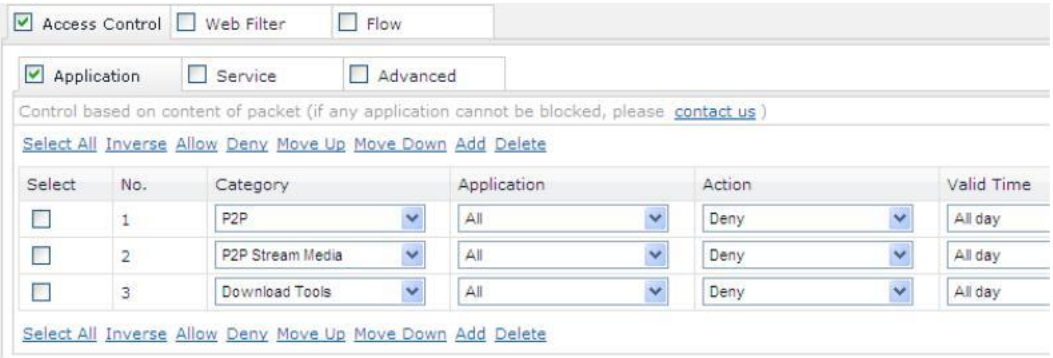
User Group: ○ All ● Specified

Selected: General Staff

Available: All user, Finance Department, Managers

☐ Access Control ☐ Web Filter ☐ Flow

5. Configure a rule to deny the user group General Staff to use the P2P download tools, as shown below:



☑ Access Control □ Web Filter □ Flow

☑ Application □ Service □ Advanced

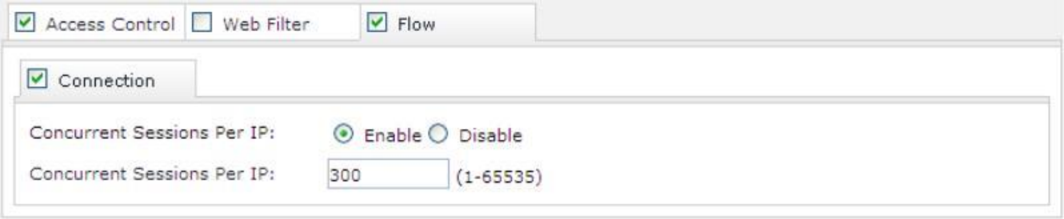
Control based on content of packet (if any application cannot be blocked, please contact us)

Select All Inverse Allow Deny Move Up Move Down Add Delete

Select	No.	Category	Application	Action	Valid Time
□	1	P2P	All	Deny	All day
□	2	P2P Stream Media	All	Deny	All day
□	3	Download Tools	All	Deny	All day

Select All Inverse Allow Deny Move Up Move Down Add Delete

6. Click on Flow > Connection tab and enable sessions control and configure Concurrent Sessions Per IP to 300, as shown below:



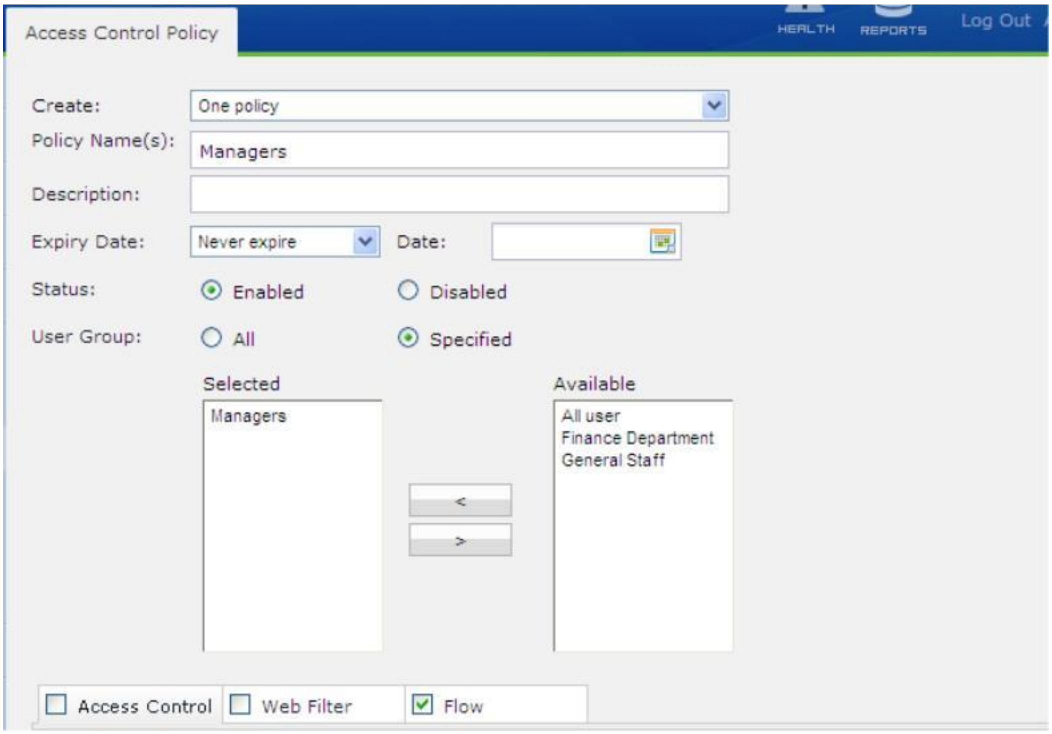
☑ Access Control □ Web Filter ☑ Flow

☑ Connection

Concurrent Sessions Per IP: ● Enable ○ Disable

Concurrent Sessions Per IP: 300 (1-65535)

7. Create an access control policy named Managers and configures no rule.



Access Control Policy

Create: One policy

Policy Name(s): Managers

Description:

Expiry Date: Never expire Date:

Status: ● Enabled ○ Disabled

User Group: ○ All ● Specified

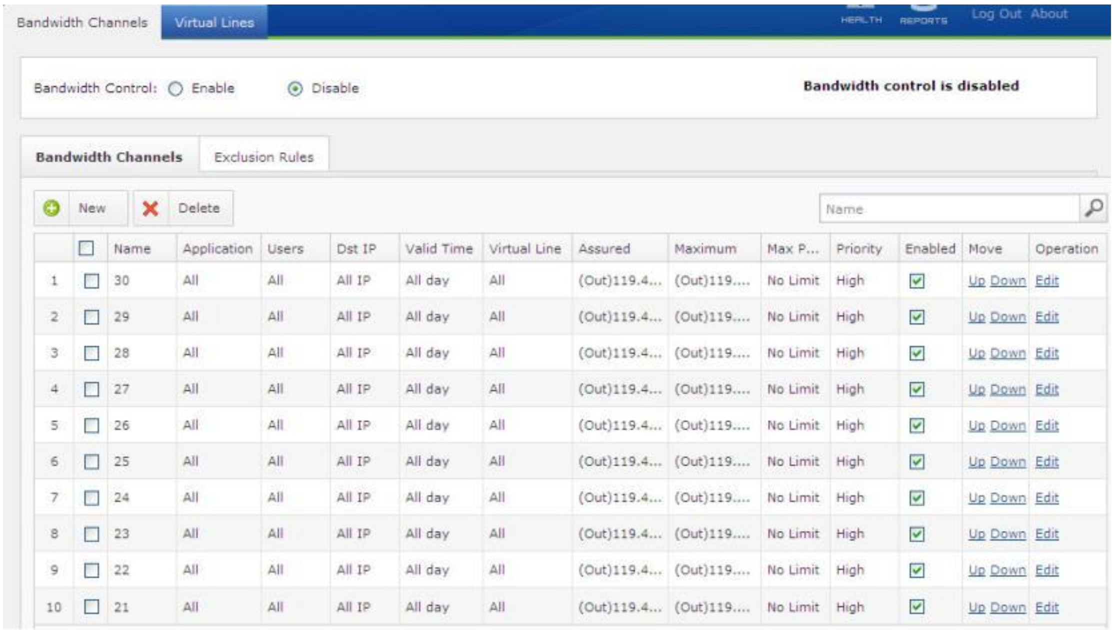
Selected: Managers

Available: All user, Finance Department, General Staff

□ Access Control □ Web Filter ☑ Flow

Bandwidth Control

Control over bandwidth is achieved by building bandwidth channels to restrain the amount of bandwidth that can be occupied by specific applications and users. It, however, can be either minimum amount of bandwidth (assured bandwidth) or maximum amount of bandwidth (maximum bandwidth) that is available to the associated users. The use of assured bandwidth is to guarantee enough bandwidth is available to some key applications. The use of maximum bandwidth is to set upper bandwidth limits for less important applications or users, so that majority of bandwidth is not occupied by non-work-related applications.



Bandwidth Control: ○ Enable ● Disable

Bandwidth control is disabled

	□	Name	Application	Users	Dst IP	Valid Time	Virtual Line	Assured	Maximum	Max P...	Priority	Enabled	Move	Operation
1	□	30	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
2	□	29	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
3	□	28	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
4	□	27	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
5	□	26	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
6	□	25	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
7	□	24	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
8	□	23	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
9	□	22	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit
10	□	21	All	All	All IP	All day	All	(Out)119.4...	(Out)119....	No Limit	High	☑	Up Down	Edit

Some Basic Concepts

Bandwidth channel: We divide the total bandwidth into many uneven portions in proportion, based on application, source and destination. Each portion is taken as a bandwidth channel, Assured Channel or Limited Channel.

Limited channel: Defines the maximum amount of bandwidth the associated applications and users can use. Even when the network is busy, the bandwidth assigned to this channel will be no more than the preset maximum amount.

Assured channel: In addition to defining the maximum amount of bandwidth, an assured bandwidth channel also specifies the minimum amount of bandwidth (assured) that is available to the associated applications and users. Even when the network is busy, this channel will be assigned no less than the minimum amount of bandwidth and no more than the preset maximum amount.

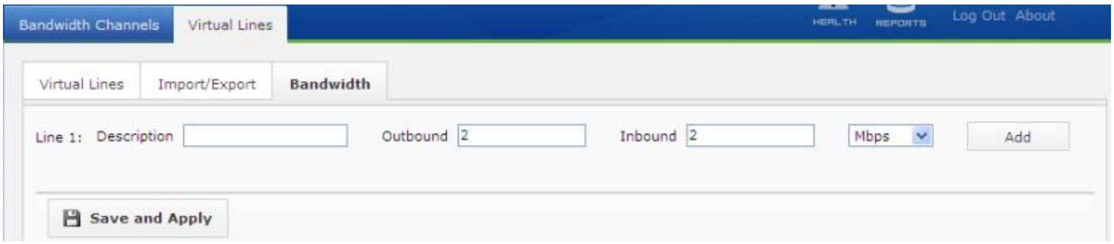
Virtual line: Virtual line is applicable to Sangfor WOC deployed in Bridge mode. The truth is that Internet line is split into several lines virtually and allocates a portion of its total bandwidth to each virtual line. These virtual lines then are associated with bandwidth channels that play a role of restraining bandwidth of specific applications and users.

Priority: If the bandwidth control feature is enabled, the data packet going through the WOC will try to match a bandwidth channel, according to the packet features. If satisfied, the data packet will match the bandwidth channel. A same data packet can match only one bandwidth channel. Since the bandwidth channels are been matched from top to bottom, you should better move the bandwidth channels with more detailed and specific features to the top of the bandwidth channel list.

Virtual Line

Under Bridge mode, all the data packets are taken as data of a same link from the viewpoint of the Sangfor WOC, no matter how many Internet lines the frontend device is connected to, or whether Sangfor WOC is in Double Bridge mode and has two egresses. What's more, the bandwidth control is only specific for all Internet lines as a whole. Therefore, if you want to distinguish the links in granular bandwidth management, you need create virtual lines and associate virtual line with bandwidth channel.

For example, if there is only one virtual line (Line 1) configured in Bandwidth Management > Bandwidth Control > Virtual Line > Bandwidth, the Outbound and Inbound bandwidth of the Line 1 should be the total of all the Internet lines (provided that the frontend device is connected to several Internet lines, or the WOC is in Double Bridge with multiple egresses). In that case, you cannot accomplish bandwidth control over the multiple Internet lines unless another or more virtual lines are added.



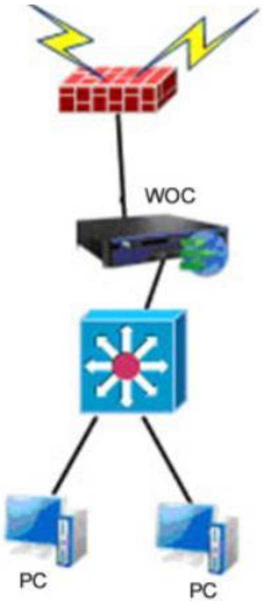
Line 1: Description
Outbound 2
Inbound 2
Mbps

To import or export virtual lines, click the Import/Export tab and perform the corresponding operations. The file that contains virtual line information should be ini file.

Creating Virtual Line

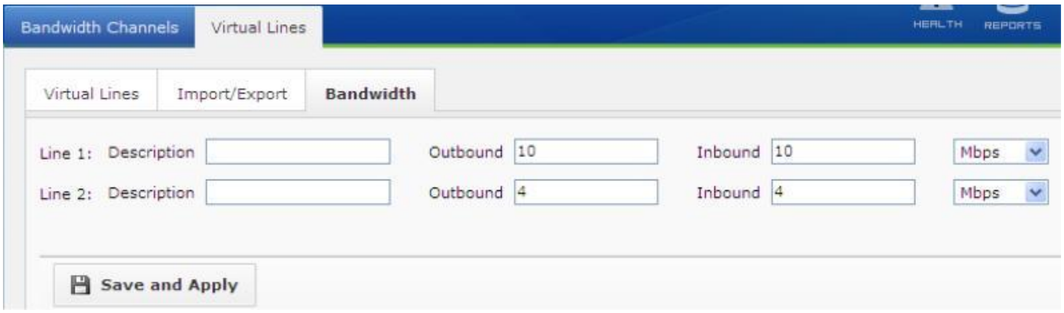
Suppose the Sangfor WOC is deployed in Bridge mode, and the firewall has two egresses, Line 1 (10Mb/s) and Line 2 (4Mb/s). Routing policies on the firewall are: 202.96.0.0/24---Line1, 58.251.0.0/24----Line2.

The network deployment is as shown in the following figure:



To achieve bandwidth control over P2P traffic on the two Internet lines, that P2P traffic on each Internet line should not occupy more than 20% of total bandwidth, perform the following steps:

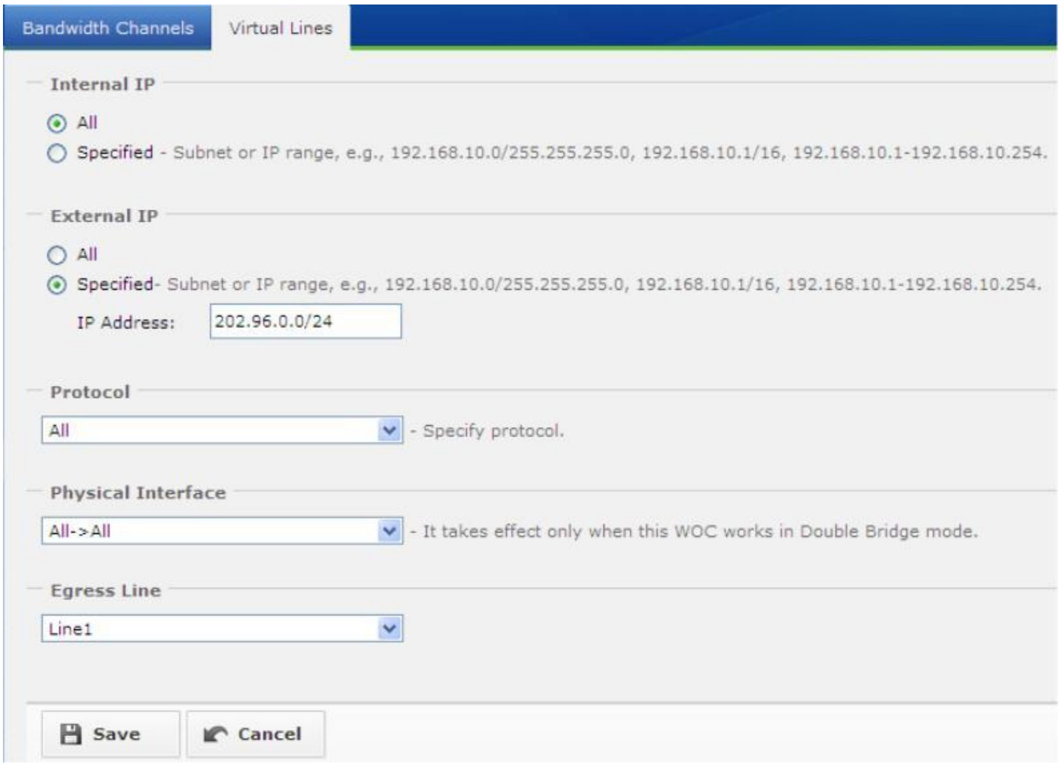
1. Go to the Bandwidth Management > Bandwidth Control > Virtual Lines > Bandwidth to add two virtual lines representing the two physical Internet lines respectively, one line 10Mb/s and the other line 4Mb/s (the actual bandwidth of the two Internet lines), as shown below:



Line 1:	Description		Outbound	10	Inbound	10	Mbps
Line 2:	Description		Outbound	4	Inbound	4	Mbps

2. Go to the Bandwidth Management > Bandwidth Control > Virtual Lines > Virtual Lines and click the New button to configure the two virtual lines.

   To configure rule for virtual line is to have the data go to different virtual lines according to the line selection rule, and to have the virtual lines and external lines be well associated. Generally, the frontend device is configured with line selection rule; therefore, you need only to configure the virtual line rule with the frontend device’s route settings. Just follow the route settings on the firewall to configure the virtual line rule. In this scenario, since the data on Line 1 are forwarded to 202.96.0.0/24, we configure Line 1 as follows.



Internal IP

● All

○ Specified - Subnet or IP range, e.g., 192.168.10.0/255.255.255.0, 192.168.10.1/16, 192.168.10.1-192.168.10.254.

External IP

○ All

● Specified- Subnet or IP range, e.g., 192.168.10.0/255.255.255.0, 192.168.10.1/16, 192.168.10.1-192.168.10.254.

IP Address: 202.96.0.0/24

Protocol

All - Specify protocol.

Physical Interface

All->All - It takes effect only when this WOC works in Double Bridge mode.

Egress Line

Line1

Internal IP: Configures the source IP address and source port of the data packets.

External IP: Configures the destination IP address and destination port of the data packet.

Protocol: Specifies the transfer protocol.

Physical Interface: Configures the bridge pair that forwards the matching data packet (in multi-bridge mode).

Egress Line: Configures a virtual line on which the packets will transmitted if the above four conditions are satisfied.

3. Repeat the above steps to configure another virtual line, Line 2, so that the virtual line rules exactly the same as the routing rules on the firewall device.

The virtual lines on Virtual Lines tab are matched from top to button.

Bandwidth Channel

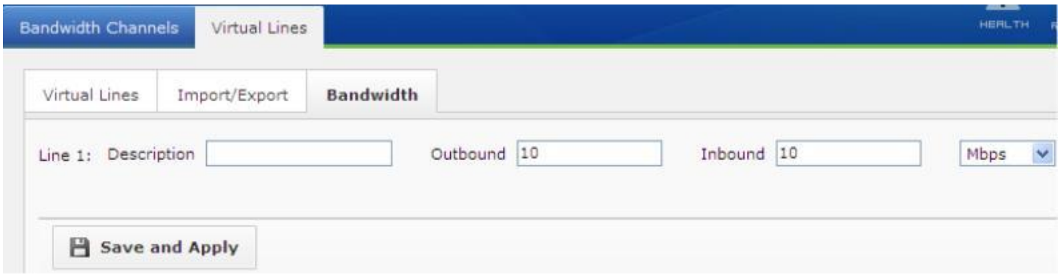
Bandwidth channel falls into assured bandwidth channel and limited bandwidth channel.

Creating Assured Bandwidth Channel

Assured channel can guarantee the normal running of some key applications. In addition to defining the maximum amount of bandwidth, you can also specify the minimum amount of bandwidth (assured) that is available to the applications and users. Even when the network is busy, this channel will be assigned no less than the minimum amount of bandwidth and no more than the preset maximum amount.

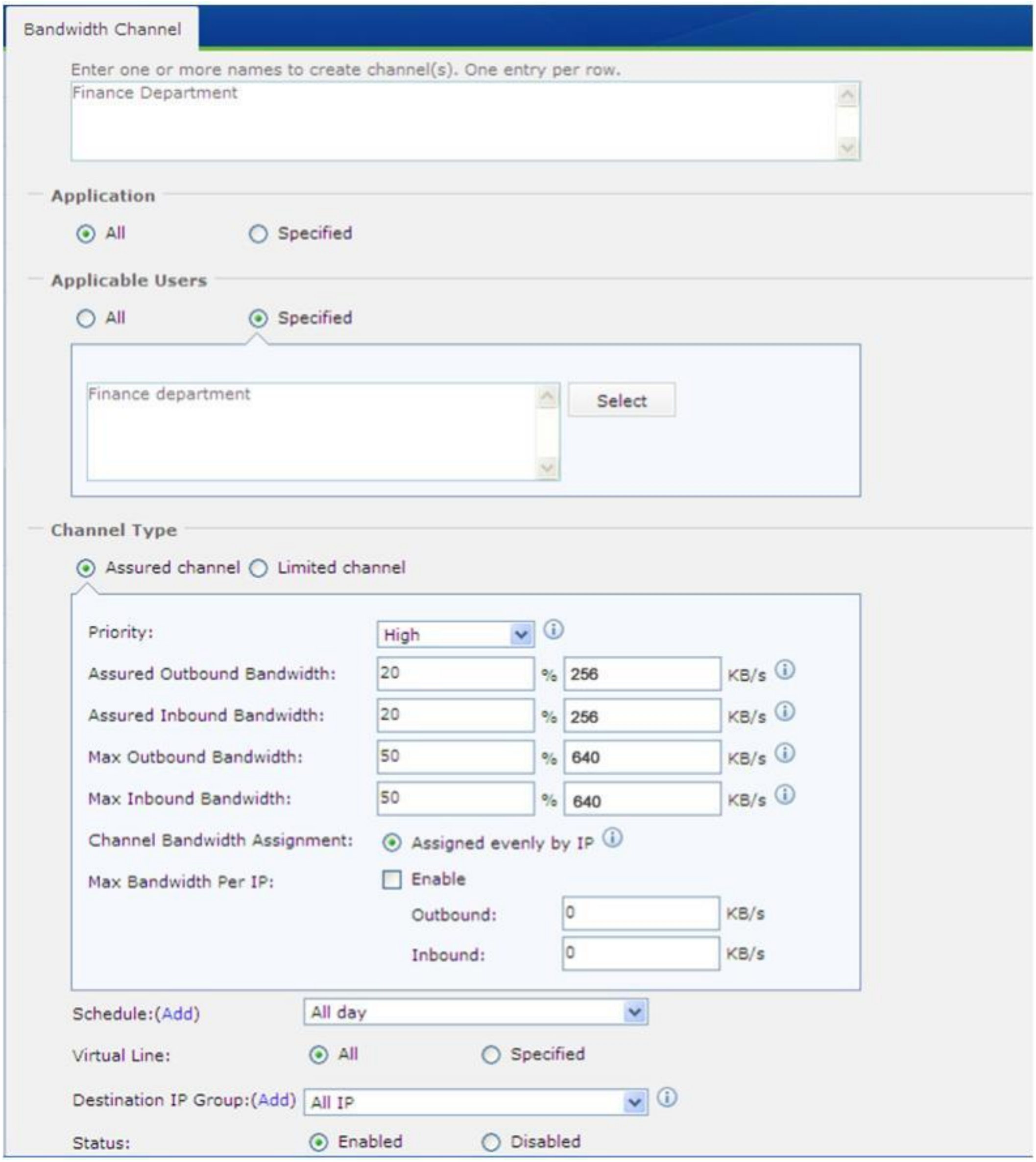
Provided that a company have a leased line (10Mb/s), to ensure members in Finance Department with bandwidth no less than 2Mb/s to access to the remote HQ even when the network is busy, yet transfer rate is no more than 5Mb/s, perform the following steps:

1. Navigate to Bandwidth Management > Bandwidth Control > Virtual Lines > Bandwidth, to add a virtual lines and the bandwidth is 10 Mb/s, as shown below:



Line 1: Description Outbound 10 Inbound 10 Mbps

2. Navigate to Bandwidth Management > Bandwidth Control > Bandwidth Channels to enable bandwidth control.
3. On Bandwidth Channels page, click New to configure an assured bandwidth channel named Finance Department, as shown below:



Bandwidth Channel

Enter one or more names to create channel(s). One entry per row.

Finance Department

Application

● All ○ Specified

Applicable Users

○ All ● Specified

Finance department

Channel Type

● Assured channel ○ Limited channel

Priority: High

Assured Outbound Bandwidth: 20 % 256 KB/s

Assured Inbound Bandwidth: 20 % 256 KB/s

Max Outbound Bandwidth: 50 % 640 KB/s

Max Inbound Bandwidth: 50 % 640 KB/s

Channel Bandwidth Assignment: ● Assigned evenly by IP

Max Bandwidth Per IP: □ Enable

Outbound: 0 KB/s

Inbound: 0 KB/s

Schedule:(Add) All day

Virtual Line: ● All ○ Specified

Destination IP Group:(Add) All IP

Status: ● Enabled ○ Disabled

Channel Name: Enter name for the bandwidth channels. Multiple names supported, one entry per row, and each name cannot exceed 96 characters. In this scenario, it is Finance Department.

Application: Configures the specific applications applied to this bandwidth channel.

Applicable User: Configures the valid users and user groups. You can select All to have all the users and groups applied to this policy, or select Specified to have some of the users or user groups applied to this policy. In this scenario, it is the members in Finance Department. If you have not added the members into the user group Finance Department, go to Bandwidth Management > Objects > User Group to add the user group.

Channel Type: Configured the type of bandwidth channel, Assured Channel or Limited Channel. In this scenario, we need to create Assured channel, the members of the Finance Department need to be assured with at least 2Mb/s yet not more than 5Mb/s.

Assured Outbound Bandwidth and Assured Inbound Bandwidth are 20%, and Max Outbound Bandwidth and Max Inbound Bandwidth ratio are 50%, because the total bandwidth is 10Mb/s, assured bandwidth is 2Mb/s and maximum bandwidth is 5Mb/s.

Priority: Options are High, Medium and Low. The bandwidth channel with higher priority is preferred to be assigned with idle bandwidth (from other bandwidth channels).

Channel Bandwidth Assignment: Configures the bandwidth for the users and the specific service/application that apply to this bandwidth chancel (policy). The only option is Assign evenly by IP. Please note that the user indicates the user who is producing traffic on this channel, excluding the users that apply to this channel but are not producing any traffic.

Max Bandwidth Per IP: Click the Enable option and configure the Outbound and Inbound bandwidth. In this scenario, it does not require such bandwidth limit, therefore, there is no need to select and configure this option.

Schedule: Configures the time period during which this bandwidth channel will be valid.

Virtual Line: Configures the virtual line to which this bandwidth channel applies.

Destination IP Group: Configures the destination IP address to which this bandwidth channel applies.

4. Click the Save button.

The ratio sum of the assured bandwidth ratio might be over 100%. When it is over 100%, the assured bandwidth of each channel will reduce according to the proportions. For example, if we configure two channels, Line 1 is assured with 30% and Line2 is assured with 90%, the bandwidth actually allocated to Line1 is 30/(90+30)%, that is, 25%, and the bandwidth actually allocated to Line2 is 90/(90+30)%, that is, 75%.

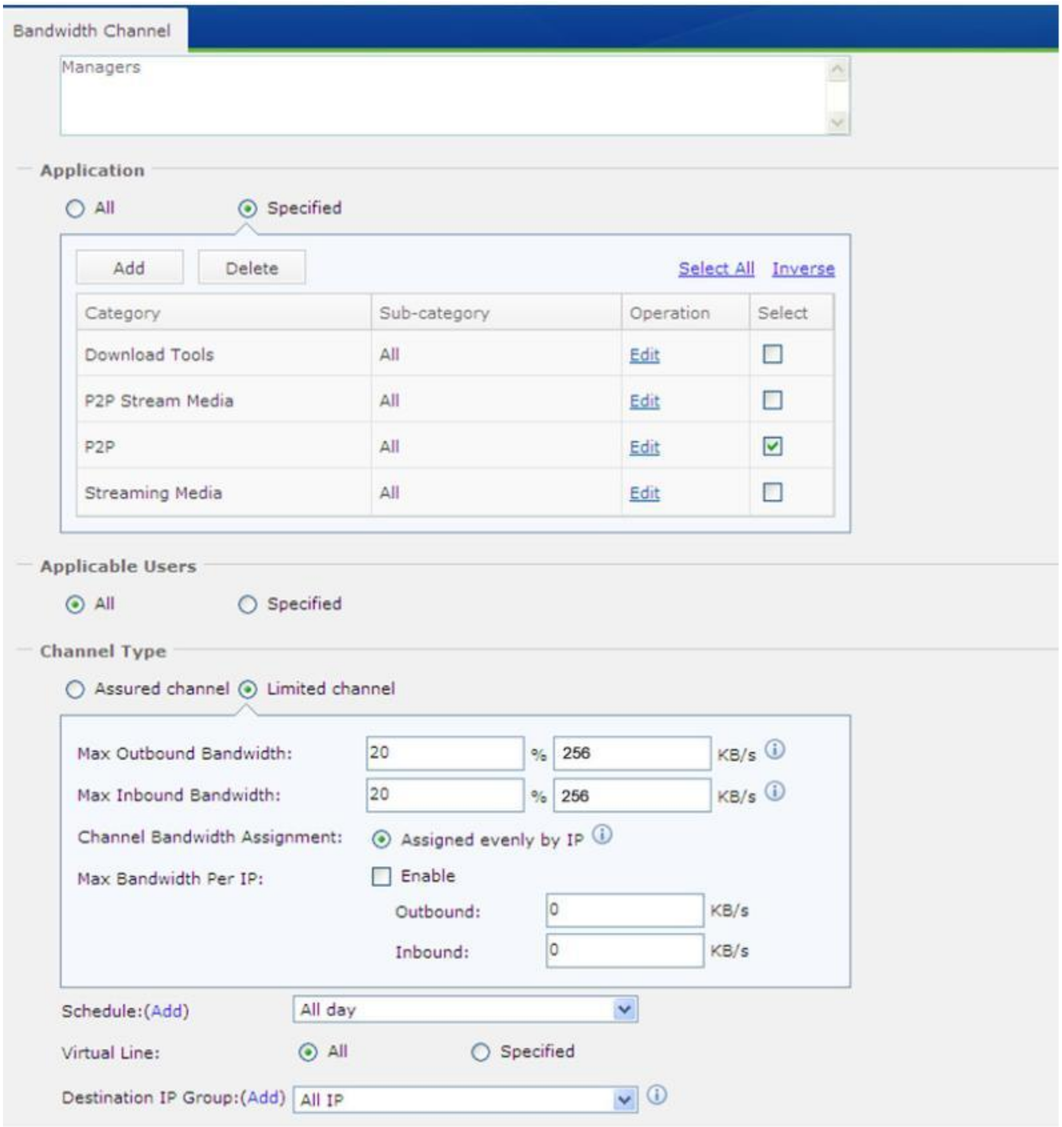
Channel with higher priority would preferentially use the idle bandwidth of other bandwidth channels.

Creating Limited Bandwidth Channel

Limited channel defines the maximum amount of bandwidth the associated applications and users can use. Even when the network is busy, the bandwidth assigned to this channel will be no more than the preset maximum amount.

Provided that a company have a leased line (10Mb/s), to keep P2P traffic by the managers who often use download software (such as Thunder) to occupy no more than 2Mb/s and not to influence businesses of other departments, perform the following steps:

1. Navigate to Bandwidth Management > Bandwidth Control > Virtual Lines > Bandwidth, to add a virtual lines and the bandwidth is 10 Mb/s.
2. Navigate to Bandwidth Management > Bandwidth Control > Bandwidth Channels to enable bandwidth control.
3. On Bandwidth Channels page, click New to configure a limited bandwidth channel named Managers, as shown below:



Bandwidth Channel

Managers

Application

○ All ● Specified

Add Delete Select All Inverse

Category	Sub-category	Operation	Select
Download Tools	All	Edit	□
P2P Stream Media	All	Edit	□
P2P	All	Edit	☑
Streaming Media	All	Edit	□

Applicable Users

● All ○ Specified

Channel Type

○ Assured channel ● Limited channel

Max Outbound Bandwidth: 20 % 256 KB/s

Max Inbound Bandwidth: 20 % 256 KB/s

Channel Bandwidth Assignment: ● Assigned evenly by IP

Max Bandwidth Per IP: □ Enable

Outbound: 0 KB/s

Inbound: 0 KB/s

Schedule:(Add) All day

Virtual Line: ● All ○ Specified

Destination IP Group:(Add) All IP

Channel Name: Enter name for the bandwidth channels. Multiple names supported, one entry per row and each name cannot exceed 96 characters. In this scenario, the name is Managers.

Application: Configures the specific applications applied to this bandwidth channel. In this scenario, it should be Download Tool/All, P2P/All, P2P Stream Media/All, Streaming Media/All. What is more, you can select Website Type or File Type. The former helps to filter the access to specific type of websites, and the later helps to filter file downloaded using HTTP and FTP.

Applicable User: Configures the valid users and groups. You can select All to have all the users and user groups applied to this policy, or select Specified to have some of the users or user groups applied to this policy. In this scenario, it is the members in Managers. If you have not added the members into the user group Managers, go to Bandwidth Management > Objects > User Group to add the user group.

Channel Type: Configures the type of bandwidth channel, Assured Channel or Limited Channel. In this scenario, we need to create Limited channel, to assign no more than 2Mb/s to the user group Managers to use P2P applications.

Max Outbound Bandwidth and Max Inbound Bandwidth is 20% of the total bandwidth.

Channel Bandwidth Assignment: Configures the bandwidth for the users and the specific application that apply to this bandwidth chancel. The only option is Assign evenly by IP. Please note that the users include only the applicable users who are producing traffic on this channel.

Max Bandwidth Per IP: Click the Enable option and configure the Outbound and Inbound bandwidth. In this scenario, it does not require such bandwidth limit, therefore, we do not need to select and configure this option.

Schedule: Configures the time period during which this bandwidth channel will be valid.

Virtual Line: Configures the virtual line to which this bandwidth channel applies.

Destination IP Group: Configures the destination IP address to which this bandwidth channel applies.

5. Click the Save button.

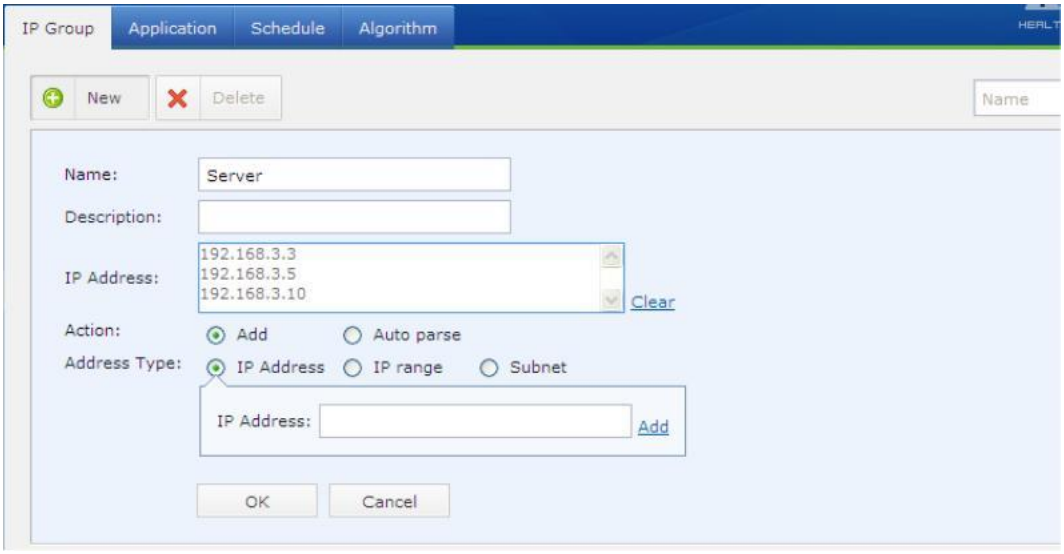
Creating Bandwidth Control Exclusion Rule

Exclusion rule works in the situation that some data do not need any bandwidth control.

For instance, if the Sangfor WOC is deployed in Bridge mode and some servers is located on DMZ, requests sent to these servers from the internal users do not need to go through the WOC nor across the Wide Area Network (WAN), and therefore bandwidth control does not need apply to such data traffic. To exclude such data from global bandwidth channels, you can configure a corresponding exclusion rule.

Provided that the Sangfor WOC works in Bridge mode and some servers (IP addresses are 192.168.3.3, 192.168.3.5, 192.168.3.10) are in DMZ, to have the access data to these servers excluded from the existing bandwidth channels, perform the steps below:

1. Navigate to System > Objects > IP Group page and click New to add the IP group named Server that includes the server IP addresses 192.168.3.3, 192.168.3.5 and 192.168.3.10, as shown below:



Name: Server

Description:

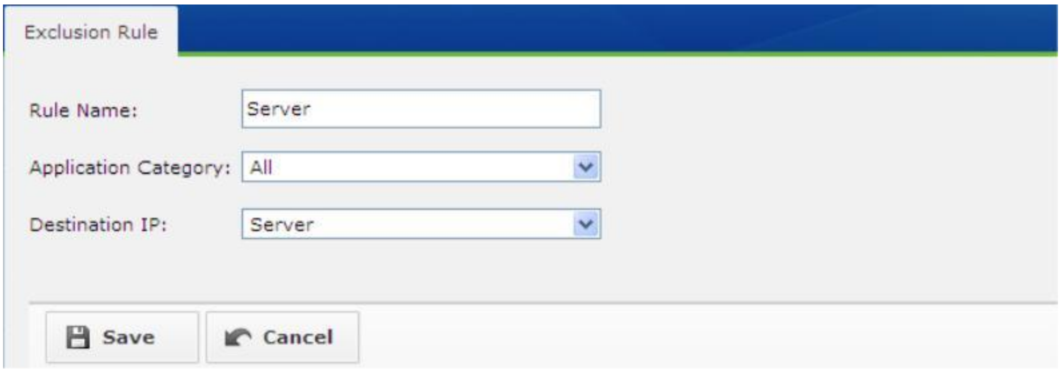
IP Address:
192.168.3.3
192.168.3.5
192.168.3.10

Action: ● Add ○ Auto parse

Address Type: ● IP Address ○ IP range ○ Subnet

IP Address:

2. Navigate to Bandwidth Management > Bandwidth Control > Bandwidth Channels > Exclusion Rules and click the New button to add an exclusion rule named Server.



Rule Name: Server

Application Category: All

Destination IP: Server

3. Configure the following contents on the above page.

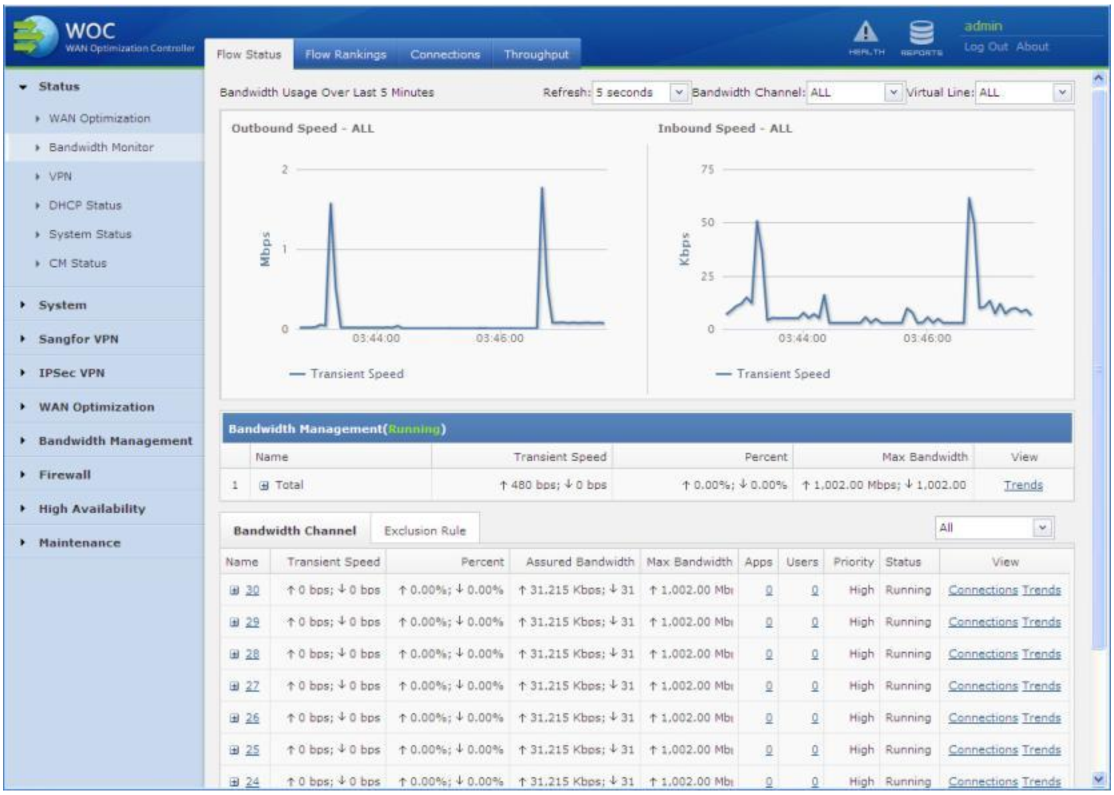
   Rule Name: Enter a name for the exclusion rule. In this scenario, the name is Server.

   Application Category: Select the application category which you want to exclude from the existing bandwidth channels.

   Destination IP: Select the IP group. In this scenario, it is Server. Packets sent to or coming from the addresses in this IP group will shy away from limitations by the bandwidth channels.

4. Click the Save button.

Viewing Bandwidth Usage



Bandwidth Usage Over Last 5 Minutes

Refresh: 5 seconds Bandwidth Channel: ALL Virtual Line: ALL

Bandwidth Management(Running)

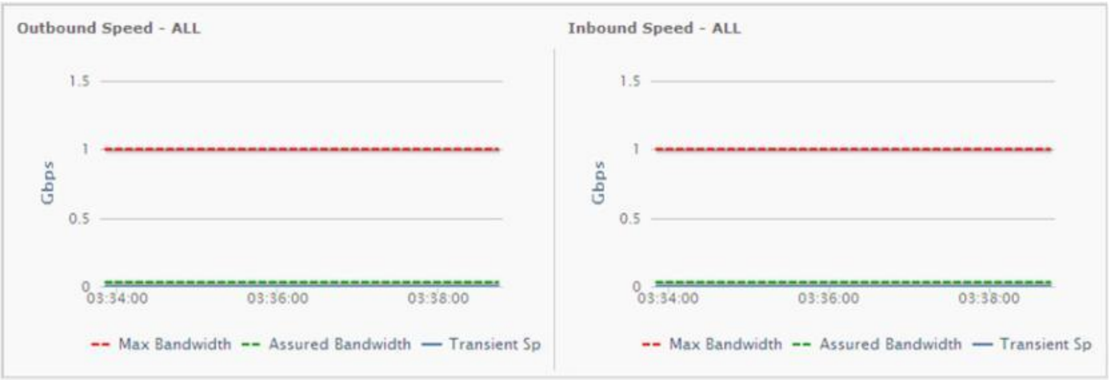
	Name	Transient Speed	Percent	Max Bandwidth	View
1	⊞ Total	↑ 480 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 1,002.00 Mbps; ↓ 1,002.00	Trends

Bandwidth Channel | Exclusion Rule | All

Name	Transient Speed	Percent	Assured Bandwidth	Max Bandwidth	Apps	Users	Priority	Status	View
⊞ 30	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends
⊞ 29	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends
⊞ 28	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends
⊞ 27	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends
⊞ 26	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends
⊞ 25	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends
⊞ 24	↑ 0 bps; ↓ 0 bps	↑ 0.00%; ↓ 0.00%	↑ 31.215 Kbps; ↓ 31	↑ 1,002.00 Mb	0	0	High	Running	Connections Trends

The graphs in the above screenshot shows the outbound and inbound bandwidth usage the on specified bandwidth channel and virtual line over the past 5 minutes.

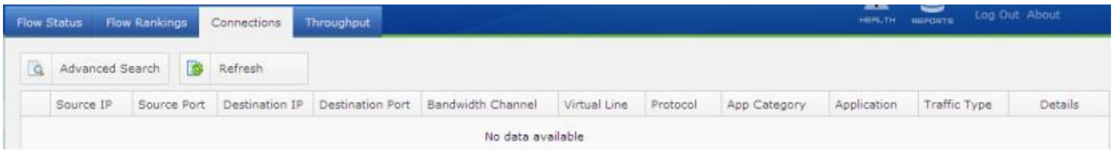
To view detailed traffic status of a bandwidth channel, click the Trends link in the Bandwidth Management table, as shown below:



To view the number of total and dropped packets and queue length information on certain bandwidth channel, click the name in the Bandwidth Channel table.

To view the active applications or users on a bandwidth channel, click the number link on Apps or Users column in the Bandwidth Channel table.

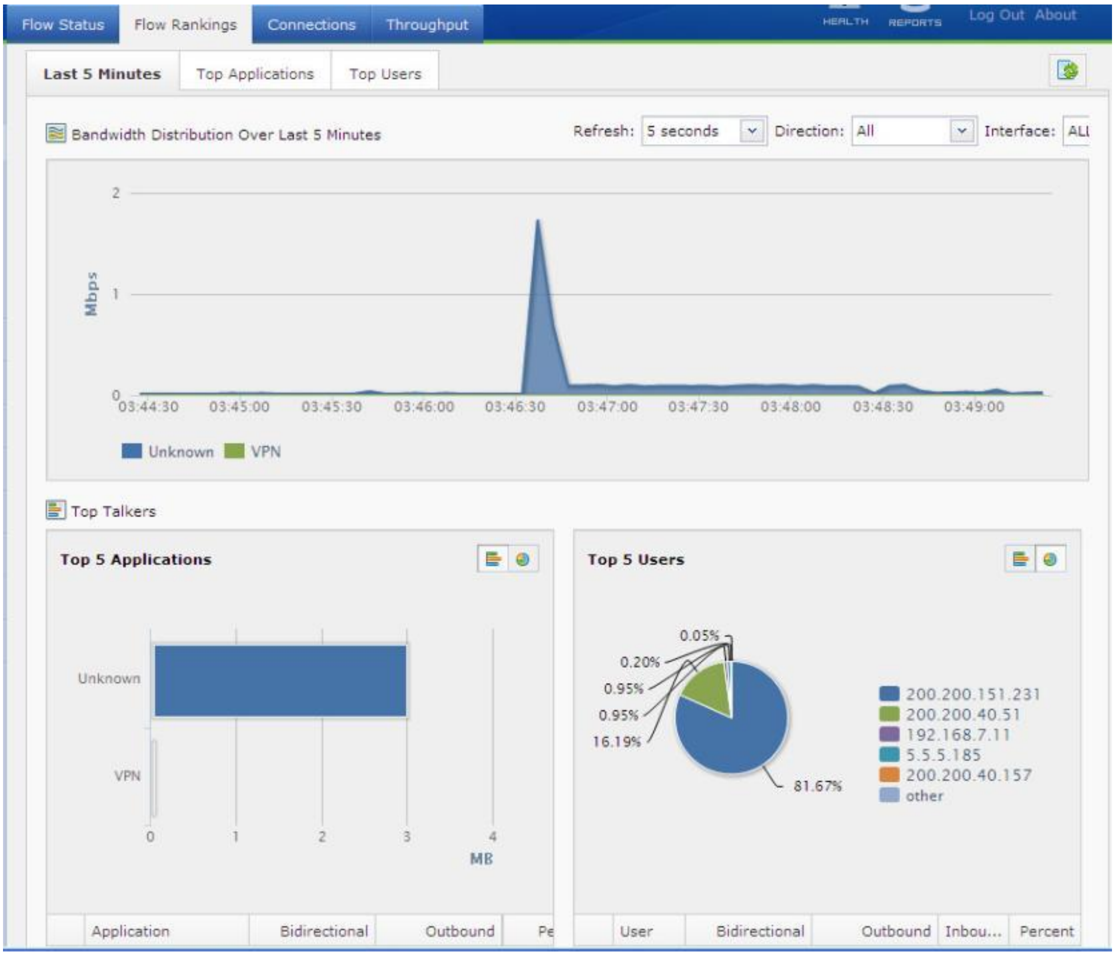
To view the connections established over a bandwidth channel, click the Connections link in the Bandwidth Channel table and enter into the Connections tab, as shown in the following figure:



Source IP	Source Port	Destination IP	Destination Port	Bandwidth Channel	Virtual Line	Protocol	App Category	Application	Traffic Type	Details

No data available

To view the most active application categories, applications and users in specified direction or on certain network interface over the past 5 minutes or at real time, go to Bandwidth Monitor > Flow Rankings > Last 5 Minutes or Top Applications and Top Users tab respectively.



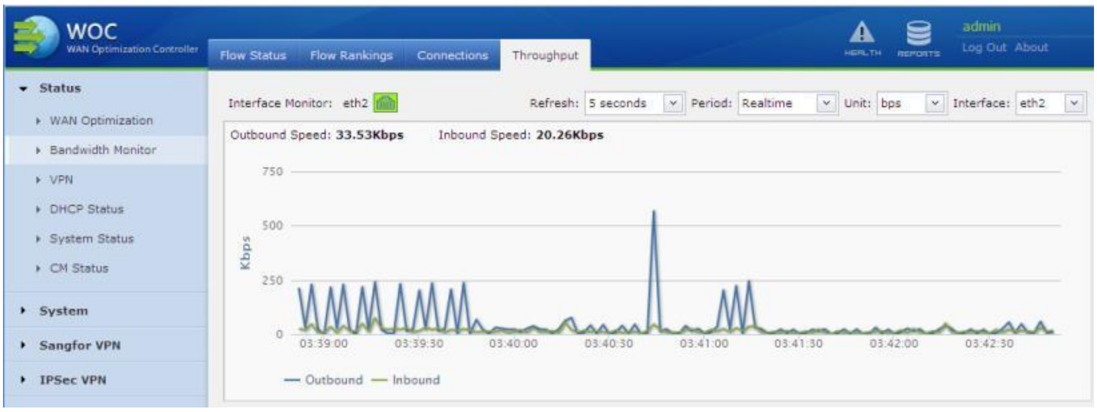
Refresh: 5 seconds Direction: All Interface: ALL

Application	Bidirectional	Outbound	Pe

User	Bidirectional	Outbound	Inbou...	Percent

All unrecognizable traffic is categorized into Unknown and VPN traffic into VPN.

To view data traffic on certain network interface, go to Bandwidth Monitor > Throughput tab:



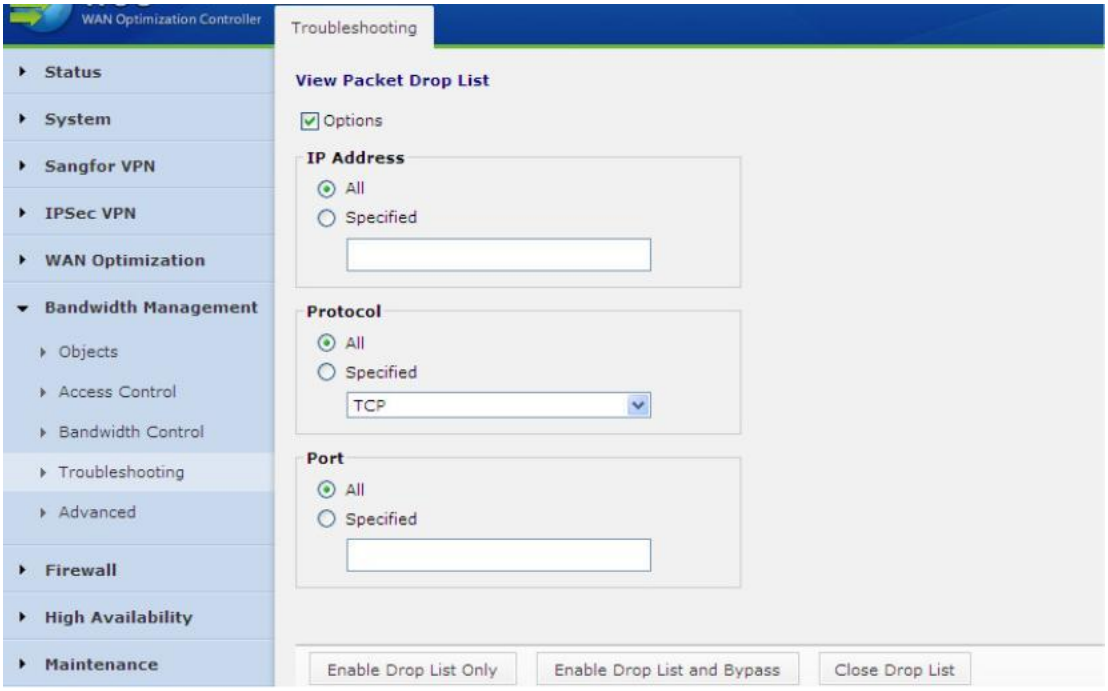
Interface Monitor: eth2 Refresh: 5 seconds Period: Realtime Unit: bps Interface: eth2

Outbound Speed: **33.53Kbps** Inbound Speed: **20.26Kbps**

Troubleshooting

Troubleshooting feature enables you to check in which stage a data packet is denied, for what reason, and to quickly find and correct the configuration mistakes made on certain module.

Navigate to Bandwidth Management > Troubleshooting to enter the Troubleshooting page:



View Packet Drop List

☑ Options

IP Address
● All
○ Specified

Protocol
● All
○ Specified
TCP

Port
● All
○ Specified

Select Options and the filtering criteria appear. The following are the filtering criteria:

IP Address: Specify the IP addresses so that the packets sent to or coming from these addresses will be dropped and referred to in the Packet Drop List. By default, All (network segments) is selected.

Protocol Type: Specify the transfer protocol so that matching packets will be dropped.

Port: Specify the port so that matching packets will be dropped.

Enable Drop List Only: Click this button to enable the Packet Drop List. In that case, access control policy still takes effect normally, and packets that are expected to be rejected will be dropped. You can view information of the dropped data packets by clicking the link View Packet Drop List. To refresh the packet drop list, press the F5 key.

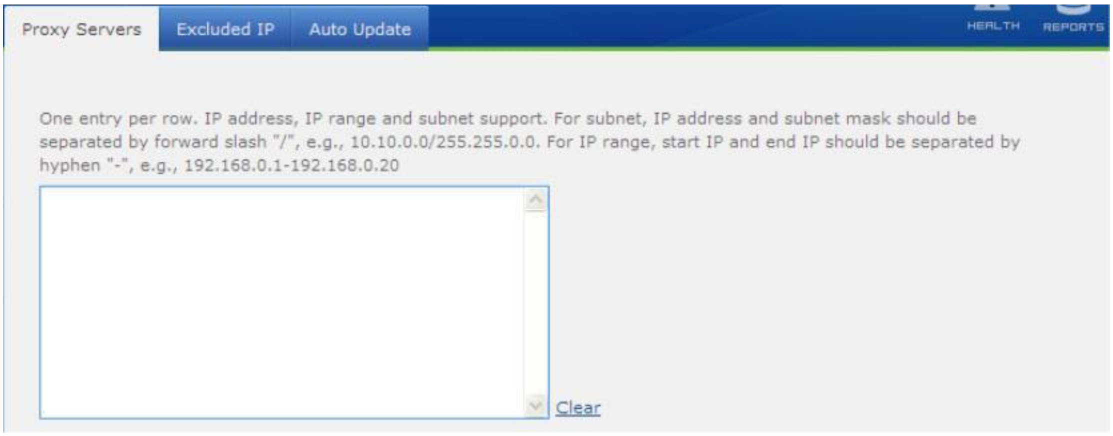
Enable Drop List and Bypass: Click this button to enable the packet drop list and bypass. In that case, the access control policy becomes invalid, even the data packets that expected to be dropped will pass through the Sangfor WOC. However, you can still view the information of the data packets that should be dropped (but bypassed) by clicking the link View Packet Drop List. To refresh the packet drop list, press the F5 key.

Close Drop List: Click this button to disable the packet drop list and bypass.

Proxy Server

It turns out that majority of the firewall features on Sangfor WAN Optimization Controller (WOC) will become invalid if internal users use proxy tools to access the Internet, for firewall allows or rejects connection only based on destination IP address and port of the data packet.

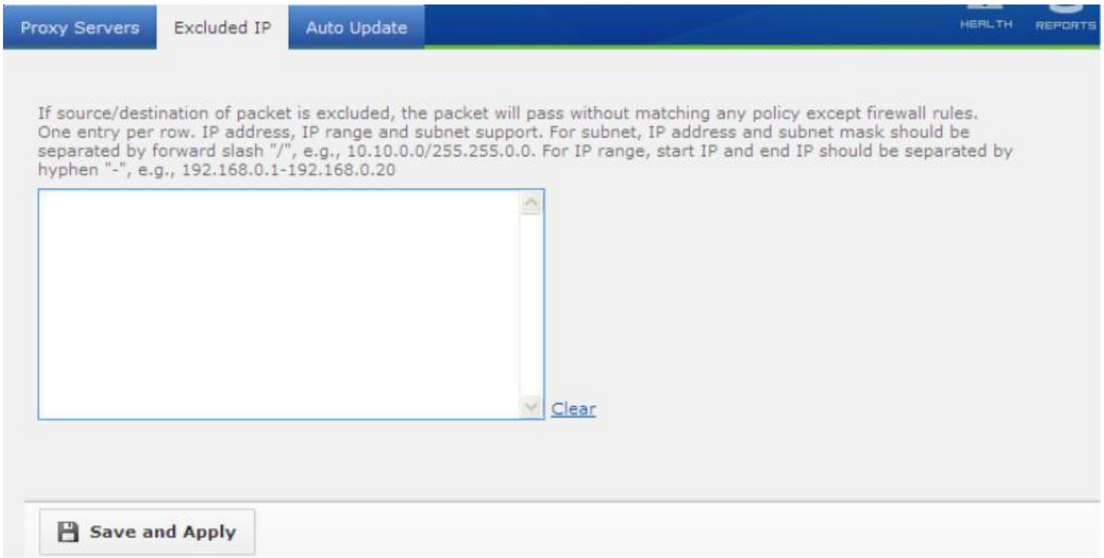
To have the firewall work in that situation, you need add the proxy server IP addresses in Bandwidth Management > Advanced > Proxy Server, so that the Sangfor WOC can identify the data forwarded to those proxy servers, tell the real destination IP addresses and ports, and apply the rule to those IP addresses and ports accordingly.



One entry per row. IP address, IP range and subnet support. For subnet, IP address and subnet mask should be separated by forward slash "/", e.g., 10.10.0.0/255.255.0.0. For IP range, start IP and end IP should be separated by hyphen "-", e.g., 192.168.0.1-192.168.0.20

Excluded IP

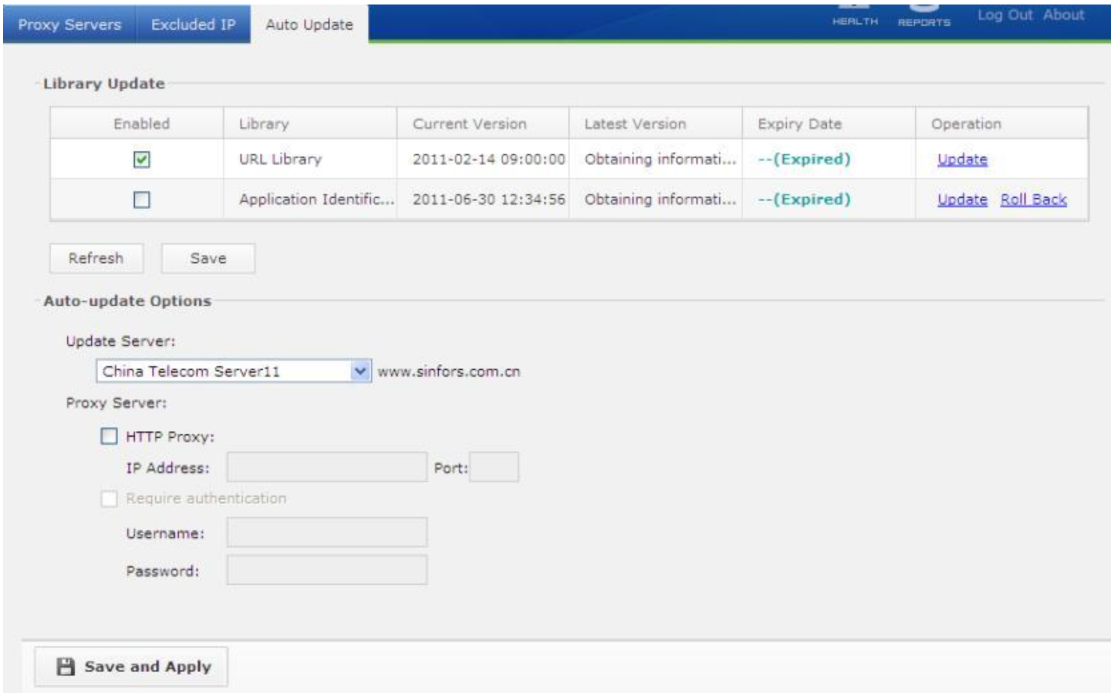
Packet whose source or destination is in any of the excluded IP addresses in Bandwidth Management > Advanced > Excluded IP will pass through the Sangfor WOC, without being monitored or being controlled by the WOC.



If source/destination of packet is excluded, the packet will pass without matching any policy except firewall rules.
One entry per row. IP address, IP range and subnet support. For subnet, IP address and subnet mask should be separated by forward slash "/", e.g., 10.10.0.0/255.255.0.0. For IP range, start IP and end IP should be separated by hyphen "-", e.g., 192.168.0.1-192.168.0.20

Internal Rule Auto Update

The auto update settings in Bandwidth Management > Advanced > Auto Update are intended for the update of the internal application identification rule and URL library, as shown below:



Library Update

Enabled	Library	Current Version	Latest Version	Expiry Date	Operation
☑	URL Library	2011-02-14 09:00:00	Obtaining informati...	--(Expired)	Update
□	Application Identific...	2011-06-30 12:34:56	Obtaining informati...	--(Expired)	Update Roll Back

Auto-update Options

Update Server:

China Telecom Server11 www.sinfors.com.cn

Proxy Server:

□ HTTP Proxy:

IP Address: Port:

□ Require authentication

Username:

Password:

The following are the contents included on the Auto Update page:

Library Update: Select the checkbox under Enabled, so that the internal URL library and application identification rules can be updated automatically. You can also click Update to update immediately the library if it has not expired or click Roll Back to restore to the previous version of library.

Proxy Server: To update the internal URL library and application identification rules regularly automatically, you need to ensure that the Sangfor WAN Optimization Controller (WOC) can connect to the Internet. If the Sangfor WOC cannot connect to the Internet directly and needs HTTP proxy, select and configure the HTTP proxy server, among which proxy server IP address and port are required. If the proxy server requires authentication, select Require authentication and configure the Username and Password fields.

Update Server: To ensure update speed, select an update server that receives Internet services from the same ISP as the Sangfor WOC.

Chapter 7 Firewall

The Sangfor WAN Optimization Controller (WOC), integrated the enterprise-level stateful firewall with high availability, can protect enterprise network against attacks initiated from Internet or other external networks connected through VPN.

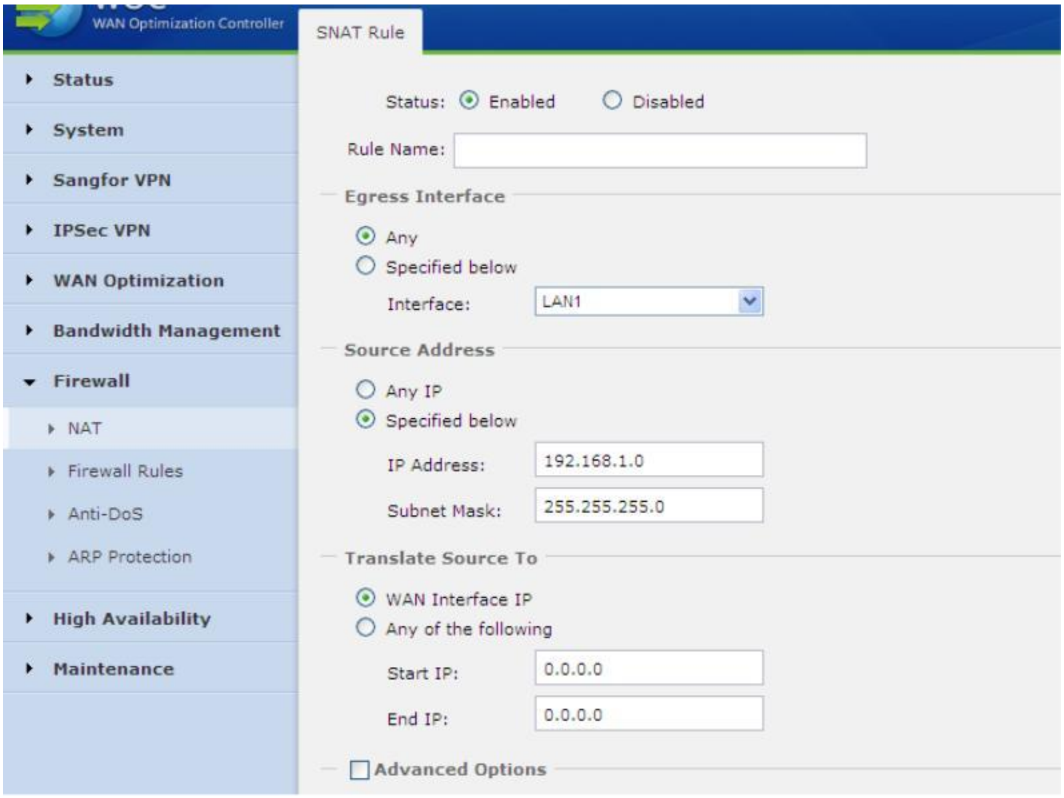
What is more, the built-in anti-DoS feature defend Sangfor WOC against DoS attacks from extranet as well as inside the intranet.

Configuring Source NAT Rule

SNAT is Source Network Address Translation in short. A source NAT rule can convert the source IP addresses of the outgoing packets forwarded to external networks by the Sangfor WOC. There is no built-in source NAT rule on Sangfor WOC. You need to add SNAT rule manually.

Provided that a network segment of the local area network is 192.168.1.0/24, to proxy the LAN users on this network segment to the Internet, perform the following steps to add a source NAT rule:

1. Navigate to Firewall > NAT to enter the SNAT Rule page. Click the New button and configure the rule, as shown in the figure below:



Status: ● Enabled ○ Disabled

Rule Name:

Egress Interface

● Any
○ Specified below

Interface: LAN1

Source Address

○ Any IP
● Specified below

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Translate Source To

● WAN Interface IP
○ Any of the following

Start IP: 0.0.0.0

End IP: 0.0.0.0

□ Advanced Options

Status: Select Enabled to enable this source NAT rule.

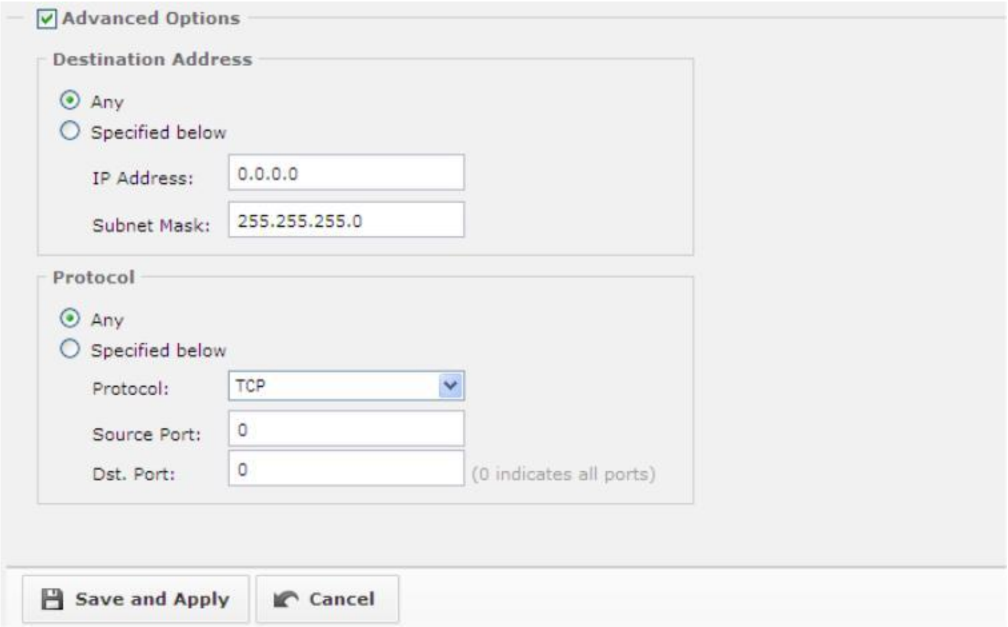
Rule Name: Specifies name of the source NAT rule.

Egress Interface: Select a network interface of the Sangfor WOC. Data packets sent through this network interface may match this SNAT rule. In this scenario, it should be Any.

Source Address: Specifies the source IP address. If the source IP address in the data packet is as specified, it may match this rule. In this scenario, the source IP address is 192.168.1.0 and subnet mask is 255.255.255.0.

Translate Source To: Specifies the public IP address to which the source IP address will be translated. You can select WAN Interface IP, which means the IP address of any WAN interface of the Sangfor WOC, or specify an IP address or IP range.

2. Select the option Advanced Options to expand more settings, such as Destination Address and Protocol, as shown below:



☑ Advanced Options

Destination Address

● Any

○ Specified below

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Protocol

● Any

○ Specified below

Protocol: TCP

Source Port: 0

Dst. Port: 0 (0 indicates all ports)

Destination Address: Specifies the destination IP address. Only when the destination IP address in the data packet is as specified may the source IP address be translated to the specified public IP address.

Protocol: Select the transfer protocol. Only when transfer protocol is as specified may the source IP address be translated to the specified public IP address.

3. Click the Save and Apply button.

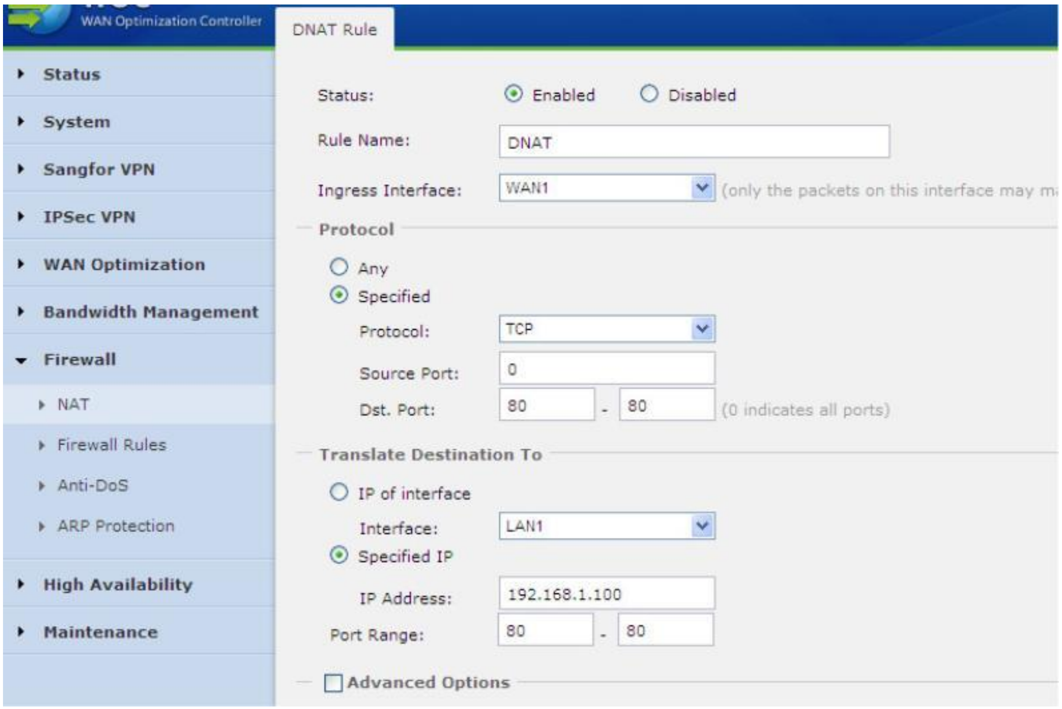
Configuring Destination NAT Rule

DNAT is Destination Network Address Translation in short. A destination NAT rule can convert the destination IP addresses of the incoming packets forwarded to internal network by the Sangfor

WOC. There is no built-in destination NAT rule on Sangfor WOC. You need to add DNAT rule manually.

Provided that a server (IP address: 192.168.1.100) on local area network needs to provide Web services for external networks on port 80, to achieve application delivery, follow the steps below to configure a destination NAT rule:

1. Navigate to Firewall > Firewall Rules to add a new firewall rule, which allows Web services. For detailed guide, Please refer to the following section Creating Firewall Rule.
2. Navigate to Firewall > NAT > DNAT Rules page and click the New button to add a new DNAT rule, as shown in the figure below:



DNAT Rule

Status: ● Enabled ○ Disabled

Rule Name: DNAT

Ingress Interface: WAN1 (only the packets on this interface may m

Protocol

○ Any

● Specified

Protocol: TCP

Source Port: 0

Dst. Port: 80 - 80 (0 indicates all ports)

Translate Destination To

○ IP of interface

Interface: LAN1

● Specified IP

IP Address: 192.168.1.100

Port Range: 80 - 80

□ Advanced Options

Status: Select Enabled to enable this destination NAT rule.

Rule Name: Specifies name of the destination NAT rule.

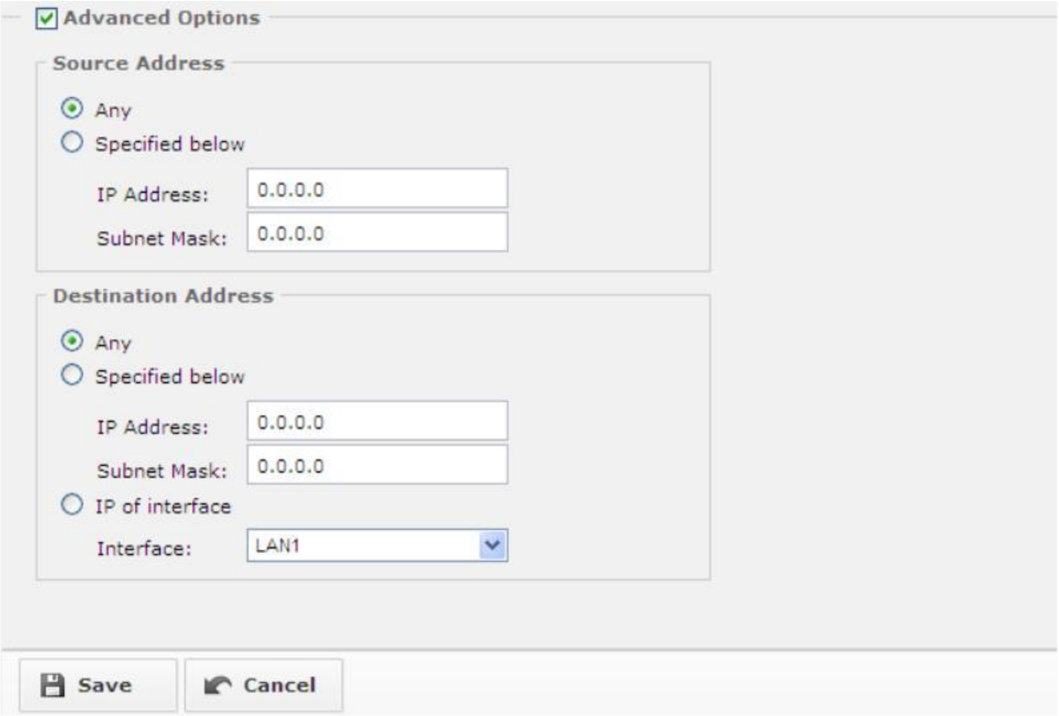
Ingress Interface: Select a network interface of the Sangfor WOC. Data packets received on this network interface may match this DNAT rule. In this scenario, it should be a WAN interface.

Protocol: Select the transfer protocol. In this scenario, it should be TCP and source port be 0 and destination port be 80.

Translate Destination To: Specifies the public IP address to which the destination IP address will be translated. You can select IP of Interface and select a WAN interface, or specify an IP address or IP range. In this scenario, the address is 192.168.1.100 and port is 80.

Source Address: Specifies the source IP address. If the source IP address in the data packet is as specified, it may match this rule. In this scenario, the source IP address is 192.168.1.0 and subnet mask is 255.255.255.0.

3. Select the option Advanced Options to expand more settings, such as Source Address and Destination Address, as shown below:



☑ Advanced Options

Source Address

● Any
○ Specified below

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Destination Address

● Any
○ Specified below

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

○ IP of interface

Interface: LAN1

Source Address: Specifies the source IP address. Only when the source IP address in the data packet is as specified may the destination IP address be translated to the specified IP address.

Destination Address: Specifies the destination IP address. Only when the destination IP address in the data packet is as specified may the destination IP address be translated to the specified IP address.

4. Click the Save and Apply button.

⚠

For the destination NAT rule configured for internal hosts to provide services for external networks, those internal hosts must take the Sangfor WOC as the gateway or ultimate gateway to the Internet. Otherwise, the DNAT rule will not take effect.

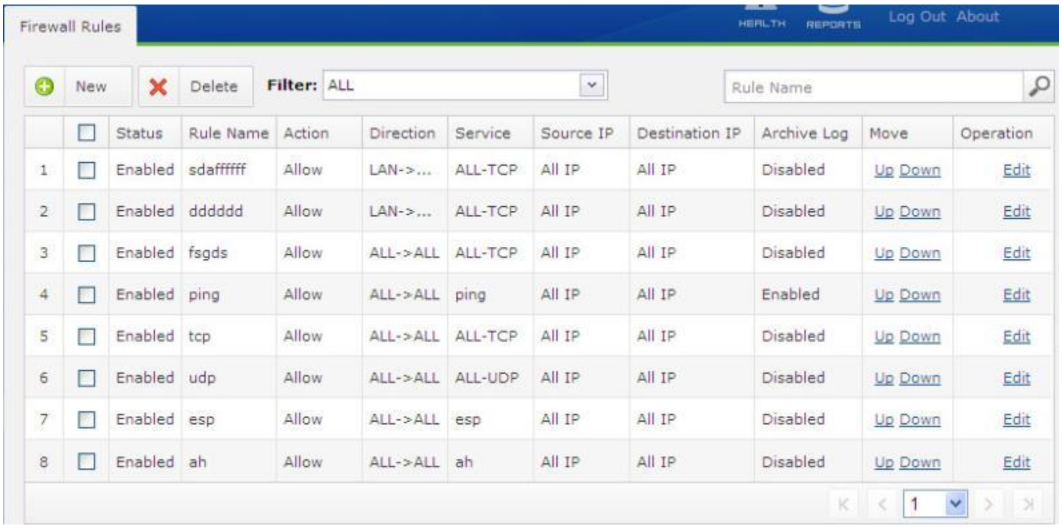
Creating Firewall Rule

The Sangfor WAN Optimization Controller (WOC) is integrated with stateful inspection packet filtering technology, which helps to filter data packets during a specified time schedule based on protocol, source IP address and destination IP address.

The firewall rules cover the rules applied to access to the local Sangfor WOC, and rules applied to access among the LAN, DMZ, WAN and VPN interfaces.

Perform the following steps to add a firewall rule:

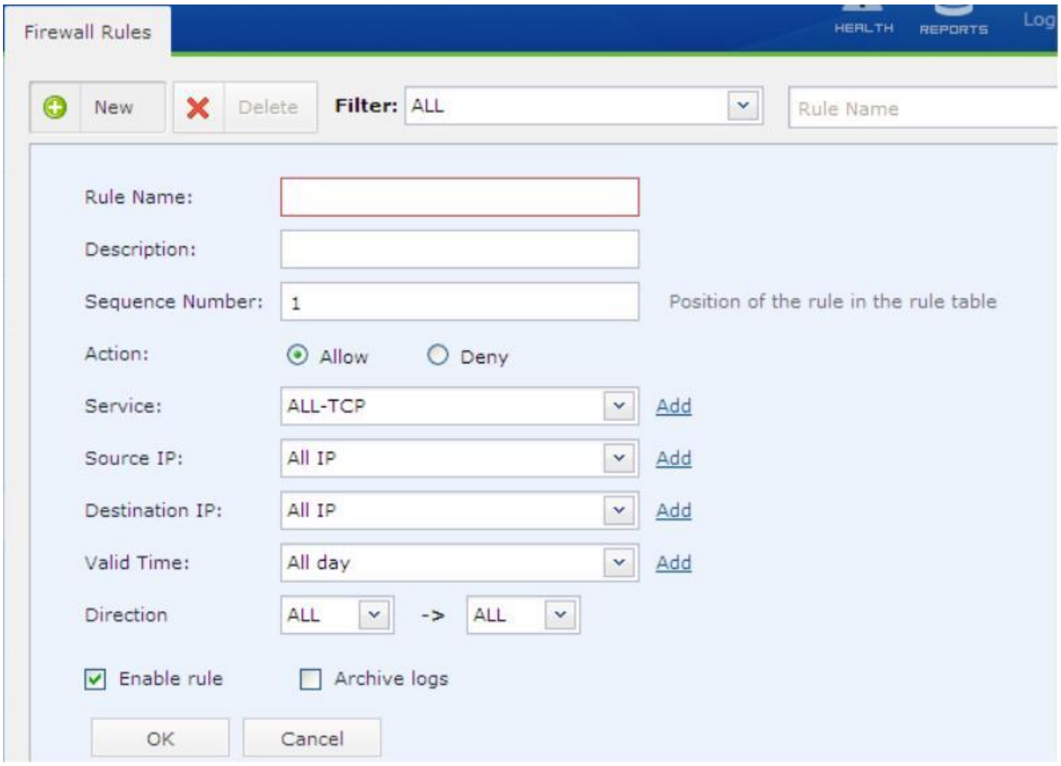
1. Navigate to Firewall > Firewall Rules.



Filter: ALL

	□	Status	Rule Name	Action	Direction	Service	Source IP	Destination IP	Archive Log	Move	Operation
1	□	Enabled	sdaffffff	Allow	LAN->...	ALL-TCP	All IP	All IP	Disabled	Up Down	Edit
2	□	Enabled	dddddd	Allow	LAN->...	ALL-TCP	All IP	All IP	Disabled	Up Down	Edit
3	□	Enabled	fsgds	Allow	ALL->ALL	ALL-TCP	All IP	All IP	Disabled	Up Down	Edit
4	□	Enabled	ping	Allow	ALL->ALL	ping	All IP	All IP	Enabled	Up Down	Edit
5	□	Enabled	tcp	Allow	ALL->ALL	ALL-TCP	All IP	All IP	Disabled	Up Down	Edit
6	□	Enabled	udp	Allow	ALL->ALL	ALL-UDP	All IP	All IP	Disabled	Up Down	Edit
7	□	Enabled	esp	Allow	ALL->ALL	esp	All IP	All IP	Disabled	Up Down	Edit
8	□	Enabled	ah	Allow	ALL->ALL	ah	All IP	All IP	Disabled	Up Down	Edit

2. Click the New button to add a new rule, as shown below:



Filter: ALL

Rule Name:

Description:

Sequence Number: 1 Position of the rule in the rule table

Action: ● Allow ○ Deny

Service: ALL-TCP

Source IP: All IP

Destination IP: All IP

Valid Time: All day

Direction ALL -> ALL

☑ Enable rule □ Archive logs

Rule Name, Description: Enter a name for the rule.

Description: Enter descriptive information for the rule.

Sequence Number: Configures the position of this firewall rule in the rule table.

Action: Specifies the action to be taken if packets match the criteria of the firewall rule.

Application: Select the application to which this firewall rule applies. The available applications are predefined in System > Objects > Application. You can click Add to add a new application (please refer to the section Creating Application in Chapter 3).

Source IP: Select the source IP group of the packets to which this firewall rule applies. The IP groups available here are predefined in System > Objects > IP Group. You can click Add to add a new IP group (please refer to the section Creating IP Group in Chapter 3).

Destination IP: Select the destination IP group of the packets to which this firewall rule applies. The IP groups available here are predefined in System > Objects > IP Group. You can click Add to add a new IP group (please refer to the section Creating IP Group in Chapter 3).

Valid Time: Select a schedule during which this firewall rule is in effect. The schedules available here are predefined in System > Objects > Schedule (please refer to section Creating Schedule in Chapter 3).

Direction: Select the data forwarding direction. The following are the possible directions:

LAN<->DMZ: Data access between the LAN interface and DMZ interface of the Sangfor WOC.

DMZ<->WAN: Data access between the DMZ interface and WAN interface of the Sangfor WOC.

WAN<->LAN: Data access between the WAN interface and LAN interface of the Sangfor WOC.

VPN<->LAN: Data access between the VPN interface and LAN interface of the Sangfor device. There are six filter rules built in each Sangfor device, which allow all TCP, UDP and ICMP data from VPN interface to LAN interface and from LAN interface to VPN interface.

VPN<->WAN: Data access between the VPN interface and WAN interface of the Sangfor WOC. If the peer Sangfor WOC has configured a tunnel route to access the local Sangfor WOC or access Internet through the local Sangfor WOC, to control the Internet access of the peer, you can configure the firewall rules with VPN<->WAN direction on the local Sangfor WOC.

VPN<->DMZ: Data access between the VPN interface and DMZ interface of the Sangfor WOC.

Enable rule: Select it to enable the current firewall rule.

Archive logs: Select it to achieve the firewall rule event if the data packets matching this firewall rule go through the Sangfor WOC. We recommend you deselect this option to for fear of generating massive logs.

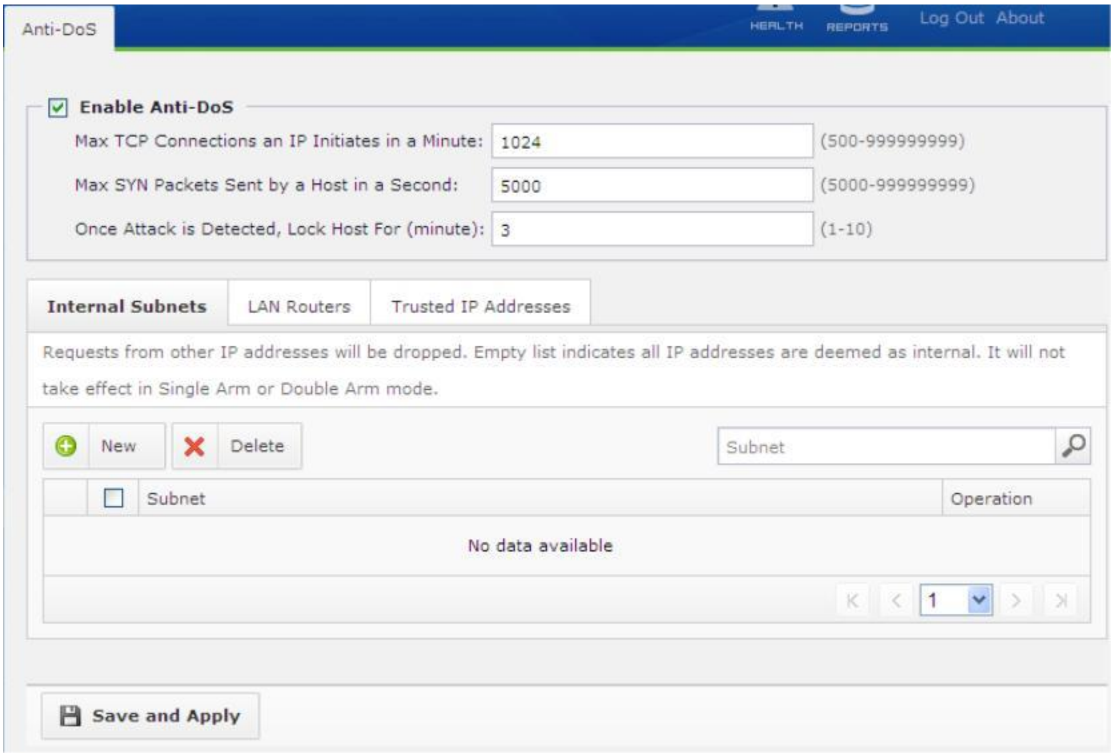
3. Click Save to save the settings.

Anti-DoS

The firewall shoulders the responsibilities of protecting the local area network (LAN) from being attacked by external users. However, apart from outside attacks, attacks from the LAN may also bring the security issues. For instance, it often happens that a virus-infected computer sends massive data packets to the gateway, which may result in bandwidth congestion or gateway crash.

The anti-DOS feature built in the Sangfor WOC can effectively solve this issue. It can monitor the number of data packets sent from a certain IP address to the gateway. When the number reaches the threshold specified, the requests will be regarded as DoS attack and IP address will locked for a certain period of time.

Navigate to Firewall > Anti-DoS to enter the Anti-DoS page, as shown below:



☑ Enable Anti-DoS

Max TCP Connections an IP Initiates in a Minute: 1024 (500-999999999)

Max SYN Packets Sent by a Host in a Second: 5000 (5000-999999999)

Once Attack is Detected, Lock Host For (minute): 3 (1-10)

Requests from other IP addresses will be dropped. Empty list indicates all IP addresses are deemed as internal. It will not take effect in Single Arm or Double Arm mode.

□	Subnet	Operation
	No data available	

The following are the contents included on the Anti-DoS page:

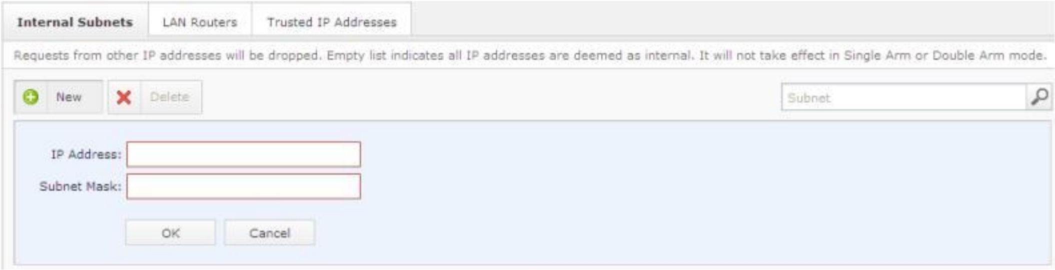
Enable Anti-DoS: Select this option to enabled anti-DoS feature.

Max TCP connections an IP initiates in a minute: Specifies the maximum of TCP connections that each IP address is allowed to initiate to the same port of an IP address in one minute. If the threshold here is reached, the IP address will be locked for a specified period.

Max SYN packets sent by a host in a minute: Specifies the maximum of SYN packets that each host is allowed to send in one minute. If the threshold here is reached, the IP/MAC address will be locked for a specified period.

Once attack is detected, lock host for (minute): Specifies the period that the attacking host will be locked after the attack is detected.

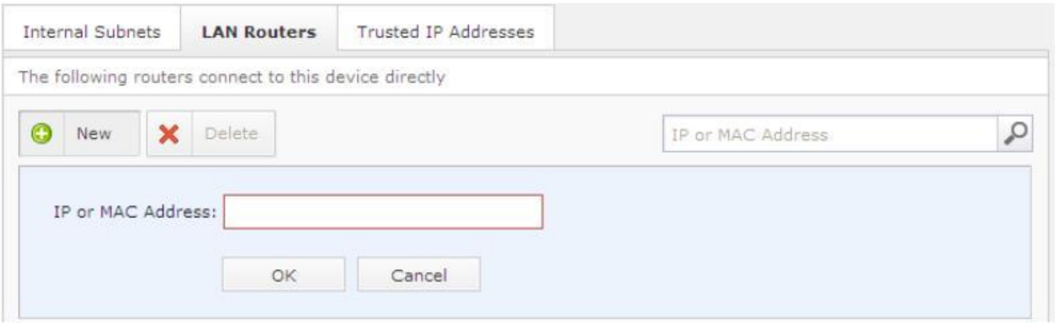
Internal Subnets: Indicates the subnets in the local area network that can access the Internet through the Sangfor WOC. When a data packet is sent from an internal IP address, the WOC will first check whether the source IP address of the packet is in the Internal Subnets list. If not, the packet will be dropped. If yes, the Sangfor device will further monitor and calculate the number of data packets from that IP address. Once the number of data packets reaches the above threshold, IP address will be locked for a period of time.



Requests from other IP addresses will be dropped. Empty list indicates all IP addresses are deemed as internal. It will not take effect in Single Arm or Double Arm mode.

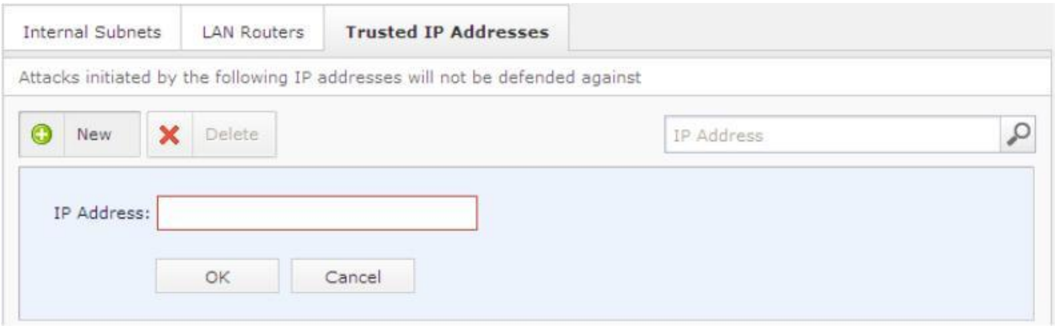
Null list indicates all IP addresses are regarded as internal addresses, which means the Sangfor WOC will skip checking for source IP address, directly monitor and calculate the number of outgoing packets.

LAN Routers: The function of LAN Routers is similar to that of Internal Subnets.



The following routers connect to this device directly

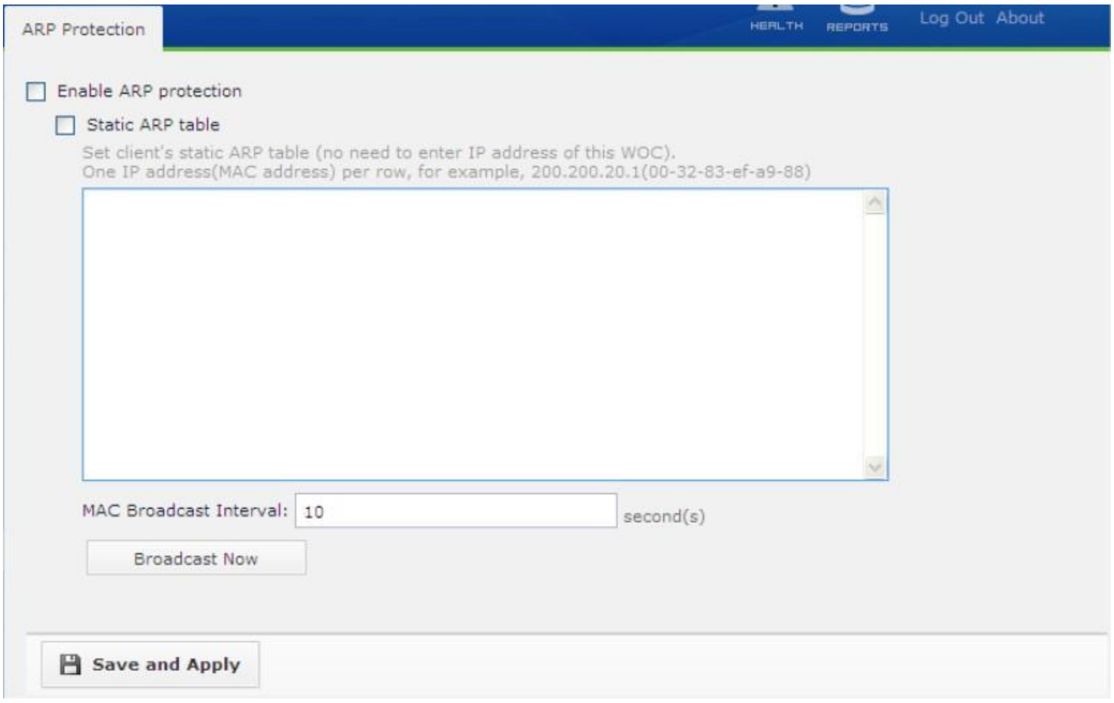
Trusted IP Addresses: The attacks initiated by any IP addresses in the list will not be defended against. If no entry is added, the attack initiated from any IP address will not be defended against.



Attacks initiated by the following IP addresses will not be defended against

ARP Protection

To protect the local area network from ARP spoofing, you can configure the static ARP table and broadcast interval of the local MAC address on the ARP Protection page, as shown below:



□ Enable ARP protection

□ Static ARP table

Set client's static ARP table (no need to enter IP address of this WOC).
One IP address(MAC address) per row, for example, 200.200.20.1(00-32-83-ef-a9-88)

MAC Broadcast Interval: 10 second(s)

The following are the contents included on ARP Protection page:

Enable ARP protection: Select this option to enable the ARP protection.

Static ARP table: Select the option and add the IP/MAC address of the machine in the local area network.

MAC Broadcast Interval: Indicates the time interval that interface IP address and MAC address of the local Sangfor WOC are broadcasted across the local area network. To broadcast the interface IP address and MAC address right now, click the Broadcast Now button.

Save and Apply: Click this button to save and apply the above settings.

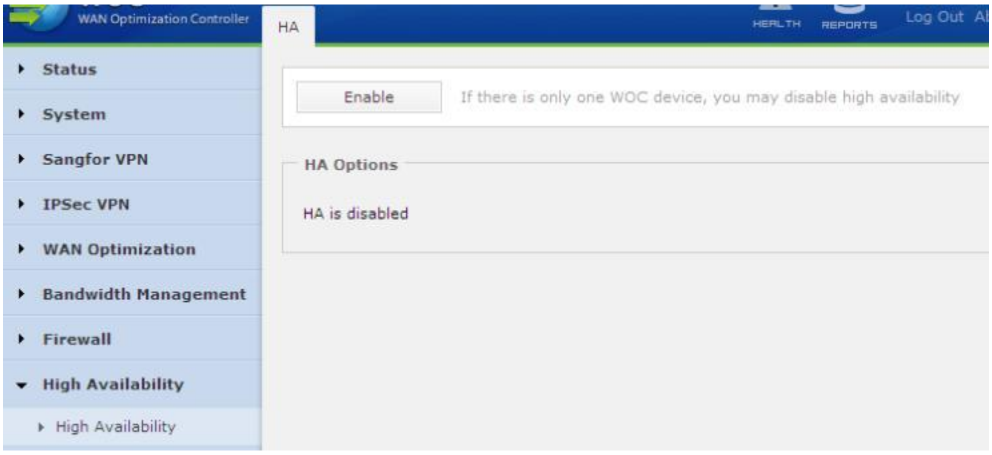
Chapter 8 High Availability

To ensure the robustness and stability of your network, SANGFOR allows you to deploy up to two Sangfor WAN Optimization Controllers (WOC) in your enterprise network. HA feature is only available and works when,

a. Two Sangfor WOCs are deployed in the enterprise network, one acting as active device and the other as standby device.

b. The separate HA software package has been installed on both Sangfor WOCs.

After deploying the physical WOCs, navigate to High Availability > HA to enable HA and configure the HA options, as shown in the figure below:



If there is only one WOC device, you may disable high availability

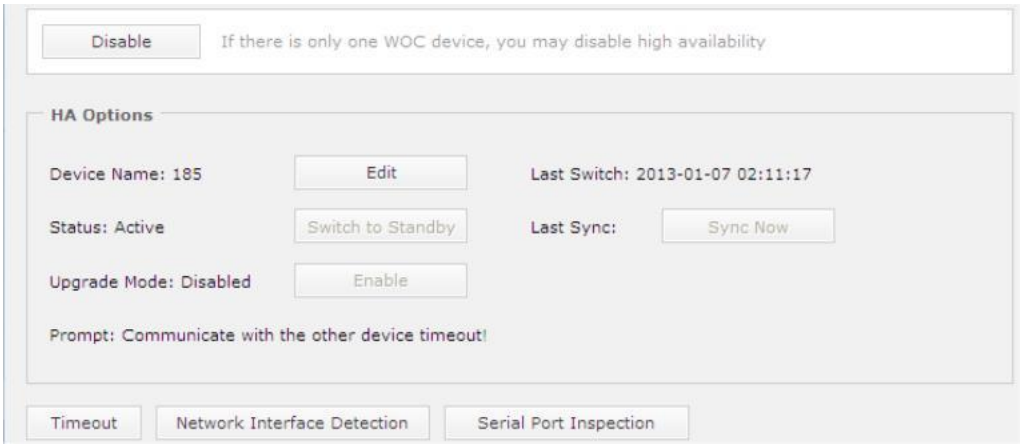
HA Options

HA is disabled

To enable high availability, the Sangfor WOC should be deployed in Route mode or Single Arm mode.

Both Sangfor WOCs should enable high availability.

Click the Enable button to enable HA and configure the following:



If there is only one WOC device, you may disable high availability

HA Options

Device Name: 185

Last Switch: 2013-01-07 02:11:17

Status: Active

Last Sync:

Upgrade Mode: Disabled

Prompt: Communicate with the other device timeout!

Device Name: Displays the name of the current Sangfor WOC. To edit the name, click Edit.

Status: Displays whether the active device and standby device communicate with each other smoothly. Click the Switch to Standby or Switch to Active button switch the status.

Last Switch: The previous time that status of the two Sangfor WOCs is switched.

Update Mode: Indicates the mode when the device can be upgraded. When the update mode is enabled, active/standby status of cannot be altered. Thus, it is recommended to enable the update mode only when you want to update the two Sangfor WOCs. After updating is completed, close the update mode.

Timeout: Click this button to specify the timeout for automatic switch between the active device and standby device. The default value is 10 seconds.

Network Interface Detection: Click this button and select the network interfaces. This setting will detect the connection status of the selected interface(s). Once any interface is disconnected, the active/standby switch will occur, ensuring smooth running of the network.

Serial Port Inspection: Click this button and enable serial port fault detection. When the serial port fails (for example, serial cable falls out), it probably causes that both Sangfor devices become active simultaneously. To avoid the IP conflict, this function (if enabled) will detect the status of the peer device according to the network packets transferred through the selected interface and automatically switch a device to standby and the other to active.

⚠

The interfaces selected on both Sangfor WOCs should be connected to a same layer-2 switch, or else, this function will not work.

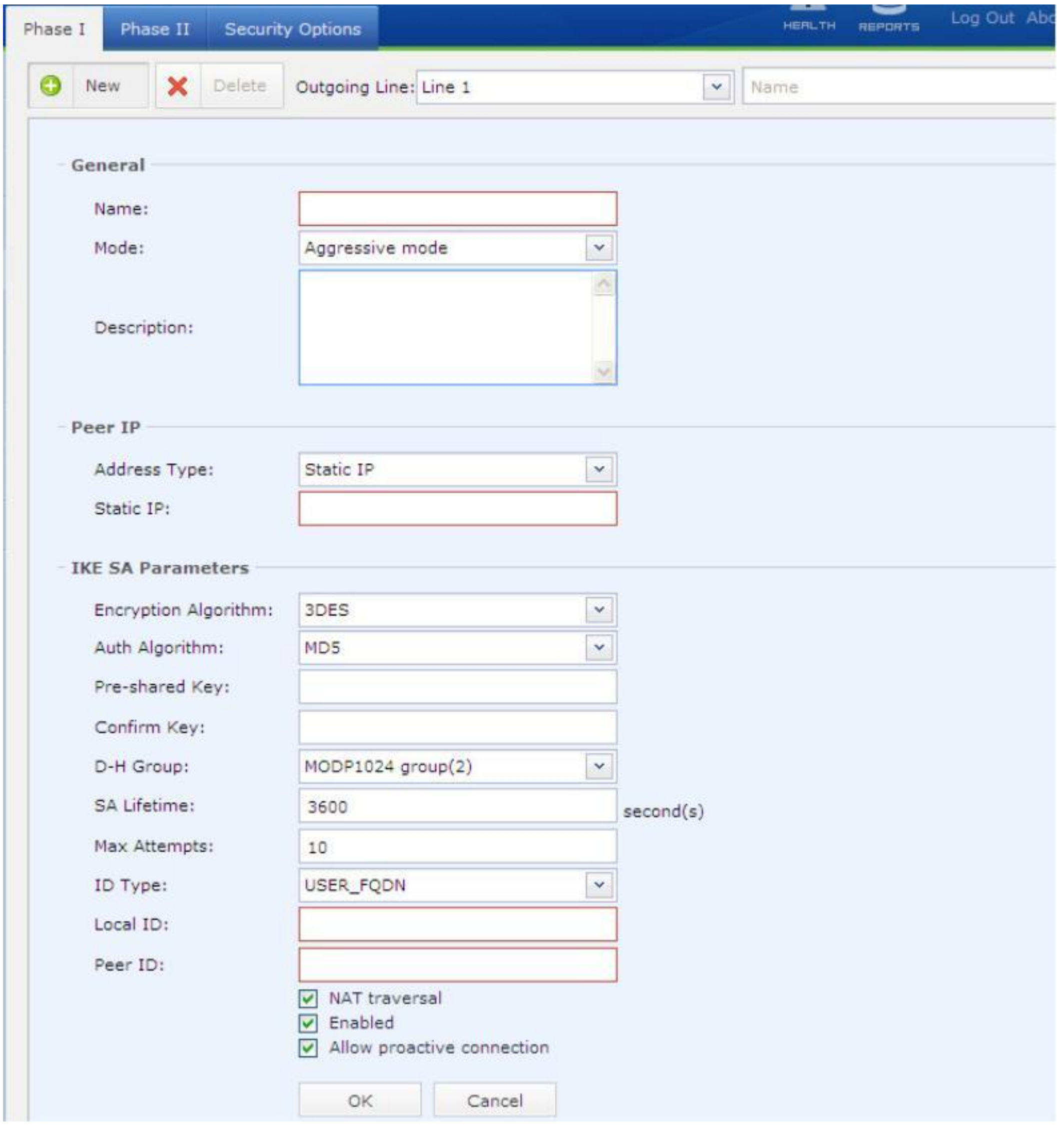
Chapter 9 IPSec VPN

Sangfor WAN Optimization Controller (WOC) allows third-party VPN device to interconnect with the existing networks, establishing a standard IPSec VPN connection. To set up IPSec VPN connection with a third party, you need to configure the parameters used in Phase I, Phase II.

Configuring Peer Device (Phase I)

In Phase I, you configure the profile of the peer VPN device that needs to establish standard IPSec VPN connection with the local Sangfor WOC. This is the first phase of the standard IPSec negotiation.

1. Navigate to IPSec VPN > IPSec VPN and click the New button to add profile of the peer VPN device:



Outgoing Line: Line 1

General

Name:

Mode: Aggressive mode

Description:

Peer IP

Address Type: Static IP

Static IP:

IKE SA Parameters

Encryption Algorithm: 3DES

Auth Algorithm: MD5

Pre-shared Key:

Confirm Key:

D-H Group: MODP1024 group(2)

SA Lifetime: 3600 second(s)

Max Attempts: 10

ID Type: USER_FQDN

Local ID:

Peer ID:

☑ NAT traversal

☑ Enabled

☑ Allow proactive connection

2. Configure the fields on the above page. The followings are the contents when Main mode is selected:

   Name: Specifies name of the first phase.

   Mode: Specifies the mode of negotiation in Phase I. Options are Main mode and Aggressive mode.

   Standard IPSec VPN connections can only be set up with Sangfor WOC deployed in Route mode. Bridge mode and Single Arm mode are not supported.

   Both parties cannot use dynamic IP address simultaneously.

   Description: Enter descriptive information.

   Address Type: Select Static IP, Dynamic IP or Dynamic Name, and configure the pop-up field.

   Encryption Algorithm: Specifies encryption algorithm for Phase I. Options are DES, 3DES, AES and SANGFOR_DES.

   We recommend you select the encryption algorithm SANGFOR_DES if both parties are Sangfor devices.

   Auth Algorithm: Select authentication algorithm for Phase I. Options are MD5 and SHA-1.

   Pre-shared Key, Confirm Key: Configures and confirm the shared key of the two parties.

   D-H group: Specifies Differ-Hellman group of the two negotiating parties.

   SA Lifetime: Specifies the lifetime of the Phase I, in unit of second.

   Max Attempts: Configures the maximum number of attempts of Phase I negotiation.

   Enabled: Select this option to enable the peer device.

   Allow proactive connection: Select this option and the other party can initiate IPSec VPN connection to the local Sangfor WOC.

3. Click the OK button.

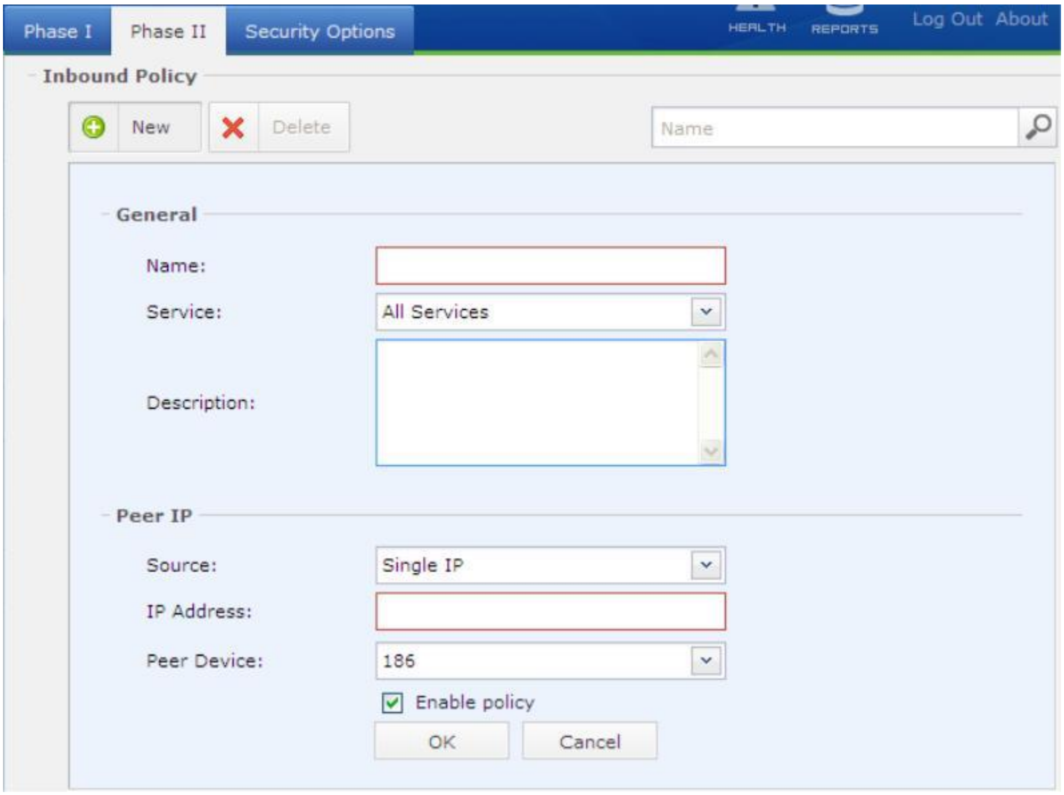
Creating Inbound/Outbound Policy (Phase II)

Phase II covers the configurations of outbound policies and inbound policies for establishing standard IPSec VPN connection.

Inbound policy defines the rules for the packets sent from the peer device to the local Sangfor WOC, while outbound policy defines the rules for the packets sent from the local Sangfor WOC to the peer device.

To add an inbound policy,

1. Navigate to IPSec VPN > Phase II and click the New button under Inbound Policy, as shown in the figure below:



2. Configure the fields on the above page. The followings are the contents:

   Name: Specifies the name of the inbound policy.

   Service: Specifies the LAN services. The LAN services are predefined in Sangfor VPN > Advanced > LAN Service.

   Description: Enter descriptive information for the inbound policy.

   Source: Select the type of source, Single IP or IP range, of the peer device, and then enter the IP address or IP range accordingly.

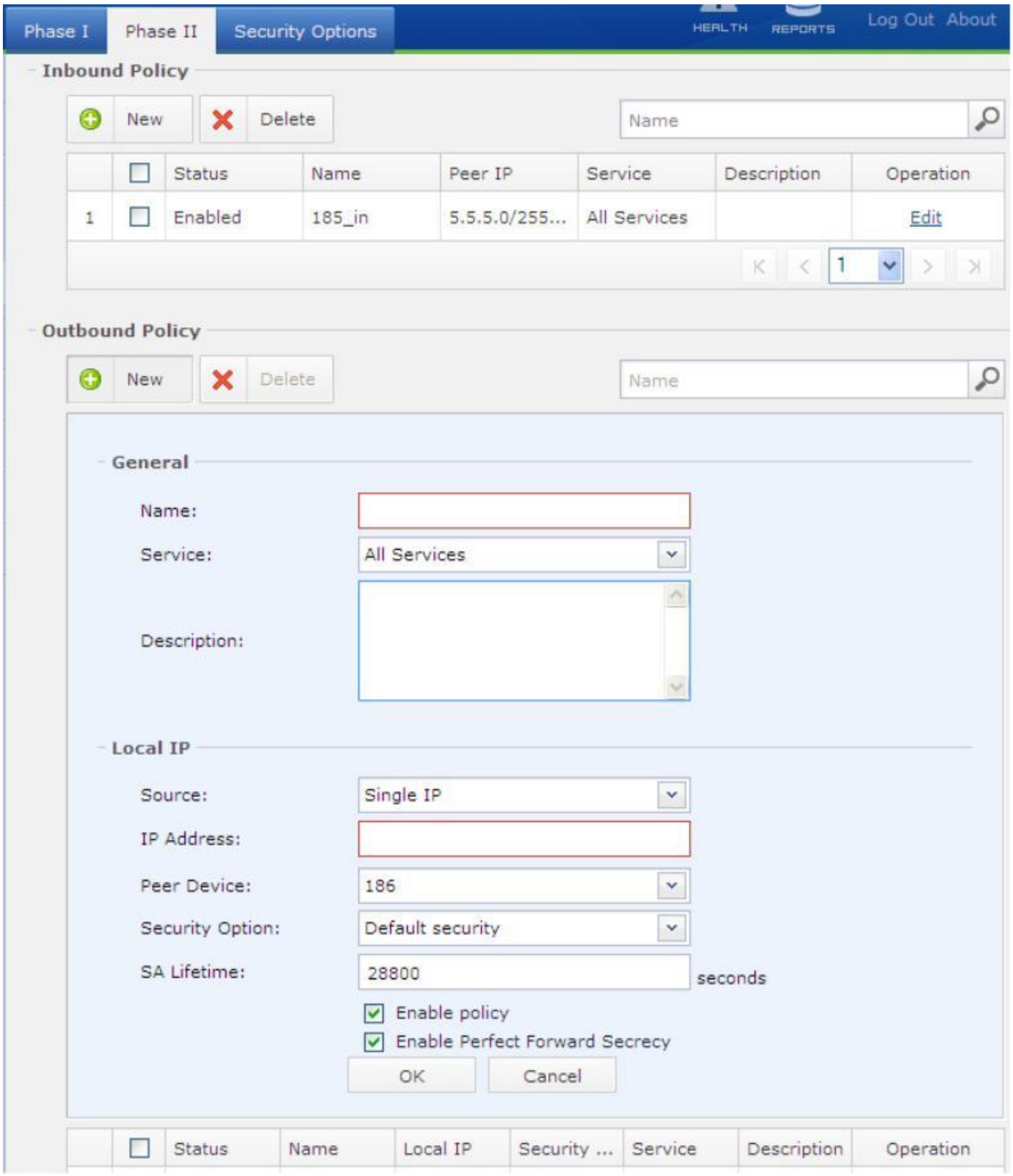
   Peer Device: Select a peer device. The peer device is predefined in Phase I.

   Enable policy: Select it to enable this inbound policy.

3. Click the OK button to save the settings.

To add an outbound policy,

1. Navigate to IPSec VPN > Phase II and click the New button under Outbound Policy, as shown in the figure below:



Inbound Policy

	□	Status	Name	Peer IP	Service	Description	Operation
1	□	Enabled	185_in	5.5.5.0/255...	All Services		Edit

Outbound Policy

General

Name:

Service: All Services

Description:

Local IP

Source: Single IP

IP Address:

Peer Device: 186

Security Option: Default security

SA Lifetime: 28800 seconds

☑ Enable policy

☑ Enable Perfect Forward Secrecy

	□	Status	Name	Local IP	Security ...	Service	Description	Operation

2. Configure the fields on the above page. The followings are the contents:

   Name: Specifies the name of the outbound policy.

   Service: Specifies the LAN services. The services are predefined in Sangfor VPN > Advanced > LAN Service.

   Description: Enter descriptive information for the outbound policy.

   Source: Select the type of source, Single IP or IP range, of the peer device, and then enter the IP address or IP range accordingly.

   Peer Device: Select a peer device. The peer device is predefined in Phase I.

Security Option: Select the security policy for negotiation of the two parties. The security policies are predefined on the Security Option page. For detailed guide, please refer to the following section.

SA Lifetime: Configures the lifetime of this outbound policy.

Enable policy: Select it to enable this outbound policy.

Enable Perfect Forward Secrecy: If the peer device is configured with PFS, select this option.

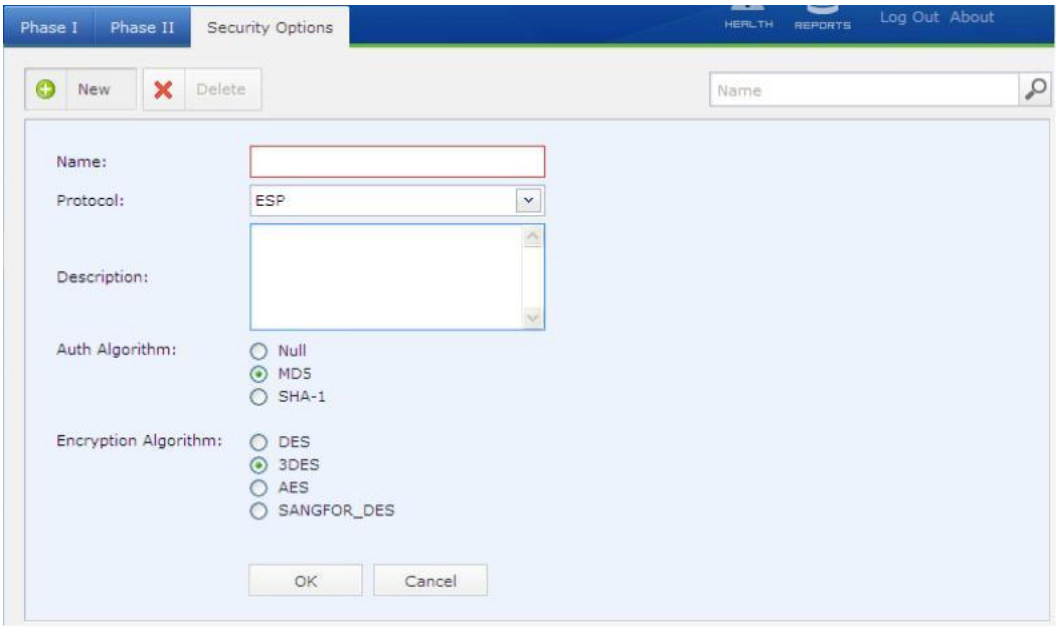
3. Click the OK button to save the above settings.

Security Options

Security options are the parameters used for establishing the standard IPSec VPN connection.

Perform the following steps to add new entry of security options.

1. Navigate to IPSec VPN > Security Options and click the New button, as shown below:



Name:

Protocol: ESP

Description:

Auth Algorithm: ○ Null ● MD5 ○ SHA-1

Encryption Algorithm: ○ DES ● 3DES ○ AES ○ SANGFOR_DES

2. Configure the fields on the above page. The followings are the contents:

Name: Specifies the name of the security options.

Protocol: Specifies the data transmission protocol used in Phase II, AH or ESP.

Description: Enter descriptive information for the security options.

Auth Algorithm: Specifies the authentication algorithm used in negotiation in phase II, MD5 or SHA-1.

Encryption Algorithm: Specifies the encryption algorithm used in negotiation in phase II, DES, 3DES, AES or SANGFOR_DES.

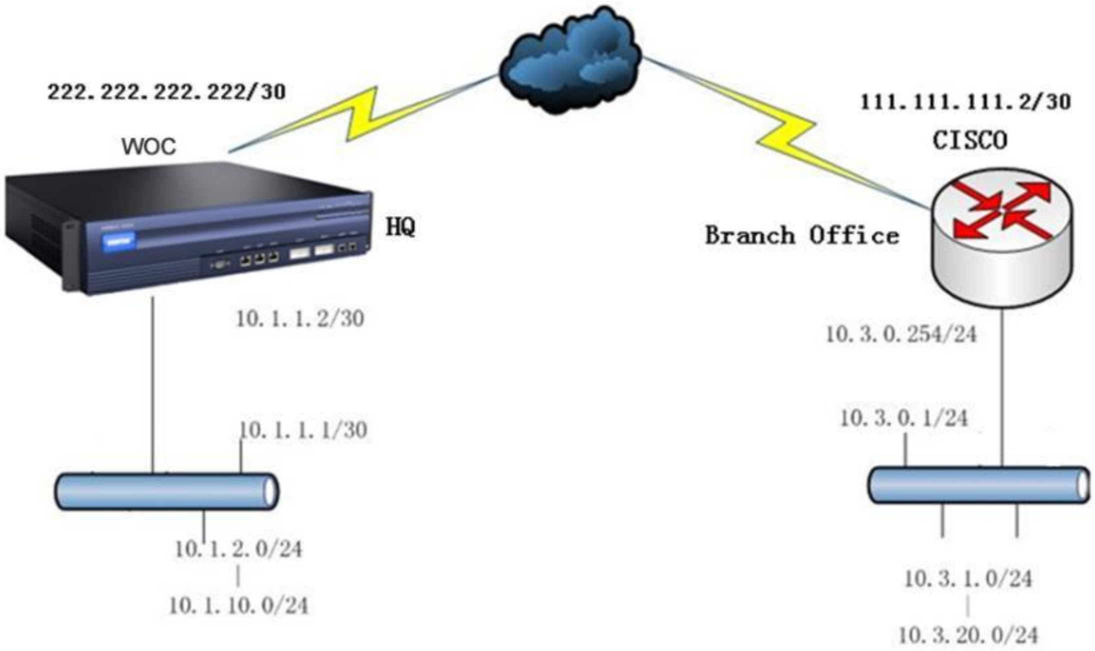
3. Click the OK button to save the settings.

The encryption algorithm in a security options is for the use of the connection negotiation in phase II. If the security policies on different connecting peer devices vary, you need to add all those policies into the Security Options page.

Scenario: Setting Up IPSEC VPN Connection with CISCO PIX

Cisco device and Sangfor WAN Optimization Controller (WOC) are connected through standard IPSec VPN. The branch (10.3.0.0/16) needs to access the server on the headquarters (HA) network (10.1.10.0/24). Network segment of the headquarters is 10.1.0.0/16).

The network topology is as shown in the figure below:

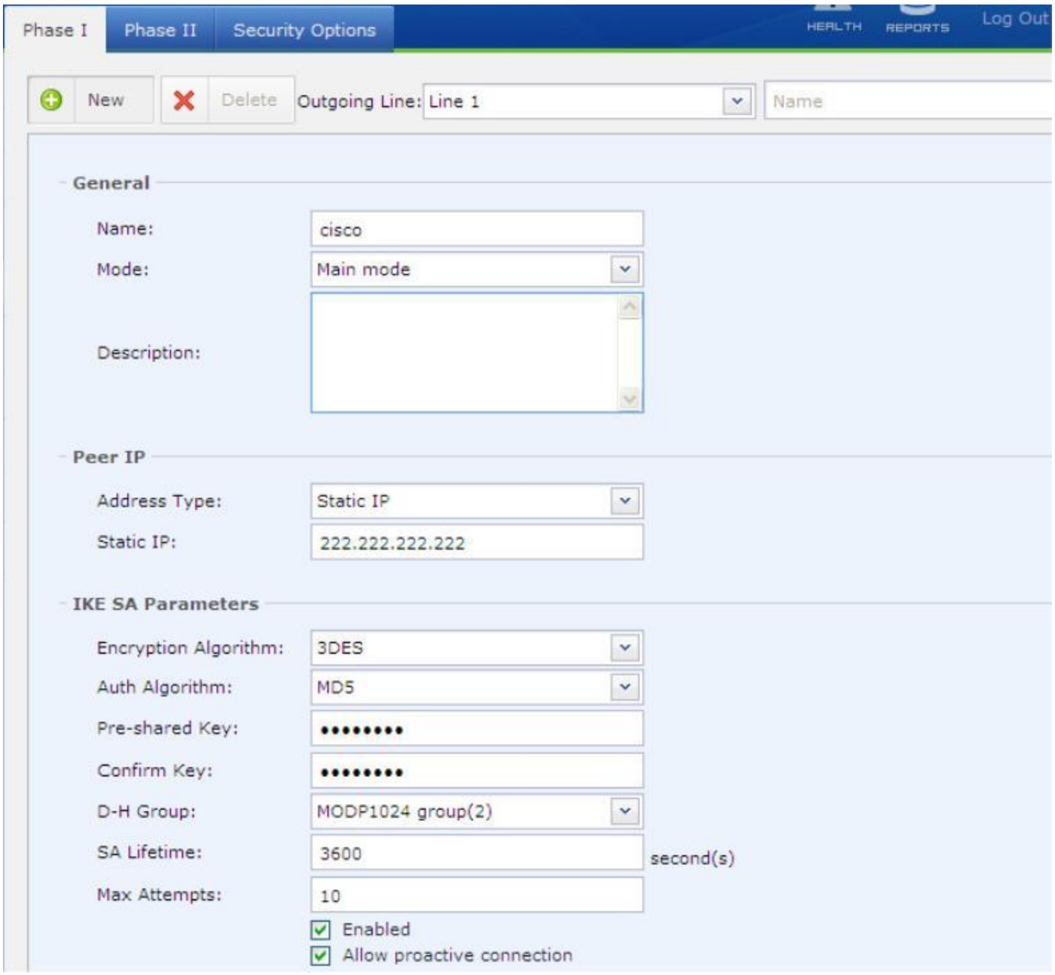


The following are configurations on the Cisco VPN device:

```
crypto ipsec transform-set sangfor esp-des esp-md5-hmac crypto map mymap 10
ipsec-isakmp
crypto map mymap 10 match address 102
crypto map mymap 10 set pfs group2
crypto map mymap 10 set peer 111.111.111.111
crypto map mymap 10 set transform-set sangfor
crypto map mymap interface outside
isakmp enable outside
isakmp key test123 address 222.222.222.222 netmask  255.255.255.252
isakmp identity  address
isakmp policy 10 authentication  pre-share
isakmp policy 10 encryption  des
isakmp policy 10 hash  md5
isakmp policy 10 group  2
isakmp policy 10 lifetime  28800
access-list 102 permit ip 10.3.0.0 255.255.0.0 10.1.0.0 255.255.0.0
access-list  nonat   permit   ip  10.3.0.0   255.255.0.0  10.1.0.0   255.255.0.0  global   (outside)  1
222.222.222.222
nat (inside) 0 access-list  nonat
nat (inside) 1 10.3.0.0 255.255.0.0 0 0
```

Perform the steps below to configure the IPSec VPN parameters on Sangfor WOC:

1. Navigate to IPSec VPN > Phase I and add the profile of Cisco VPN device, as shown below:



Outgoing Line: Line 1

General

Name: cisco

Mode: Main mode

Description:

Peer IP

Address Type: Static IP

Static IP: 222.222.222.222

IKE SA Parameters

Encryption Algorithm: 3DES

Auth Algorithm: MD5

Pre-shared Key: ••••••••

Confirm Key: ••••••••

D-H Group: MODP1024 group(2)

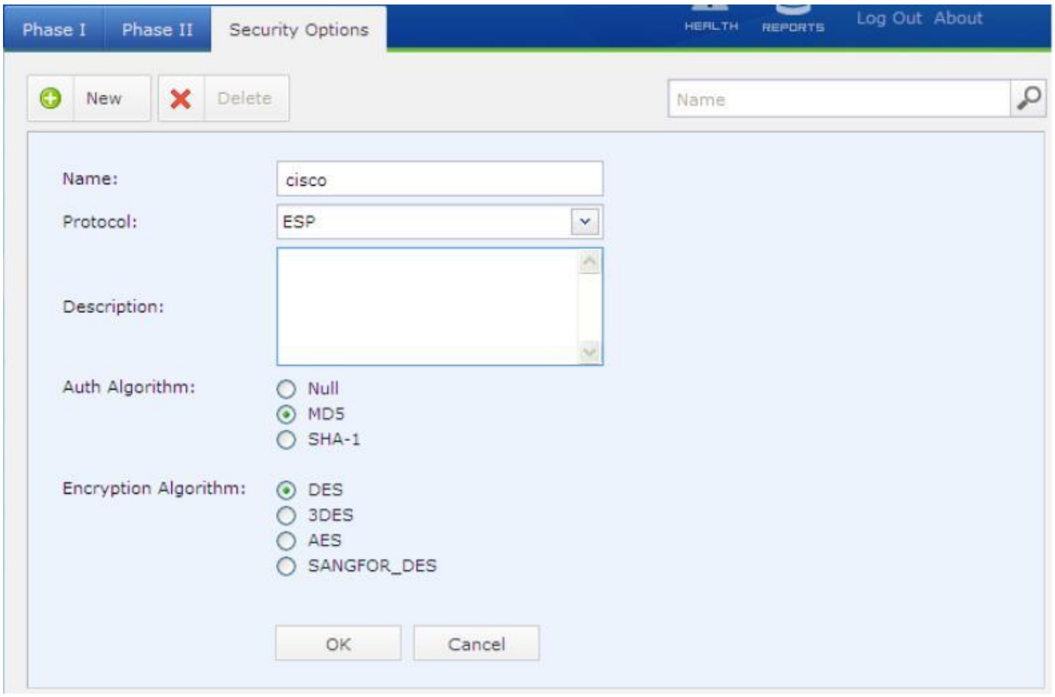
SA Lifetime: 3600 second(s)

Max Attempts: 10

☑ Enabled

☑ Allow proactive connection

2. Configure security options, as shown below:



Name: cisco

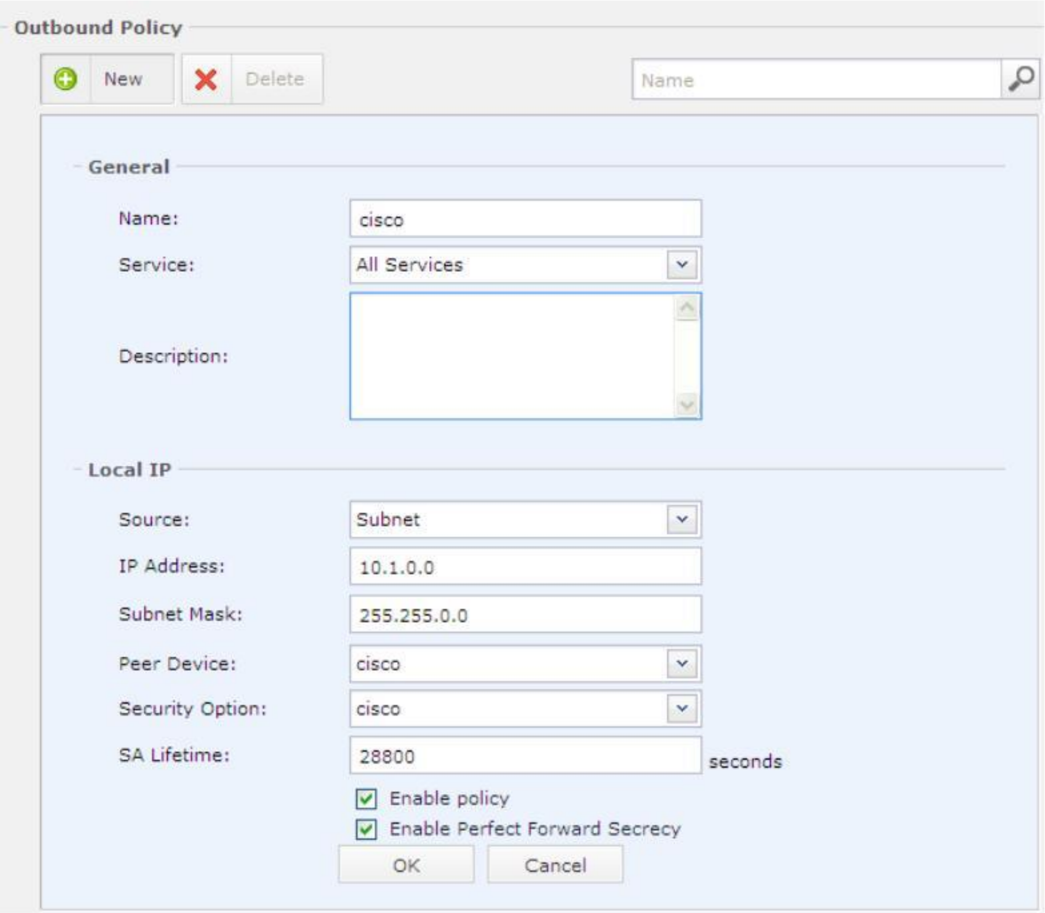
Protocol: ESP

Description:

Auth Algorithm: ○ Null ● MD5 ○ SHA-1

Encryption Algorithm: ● DES ○ 3DES ○ AES ○ SANGFOR_DES

3. Configure Phase II, outbound and inbound policy, as shown in the figures below:



Outbound Policy

General

Name: cisco

Service: All Services

Description:

Local IP

Source: Subnet

IP Address: 10.1.0.0

Subnet Mask: 255.255.0.0

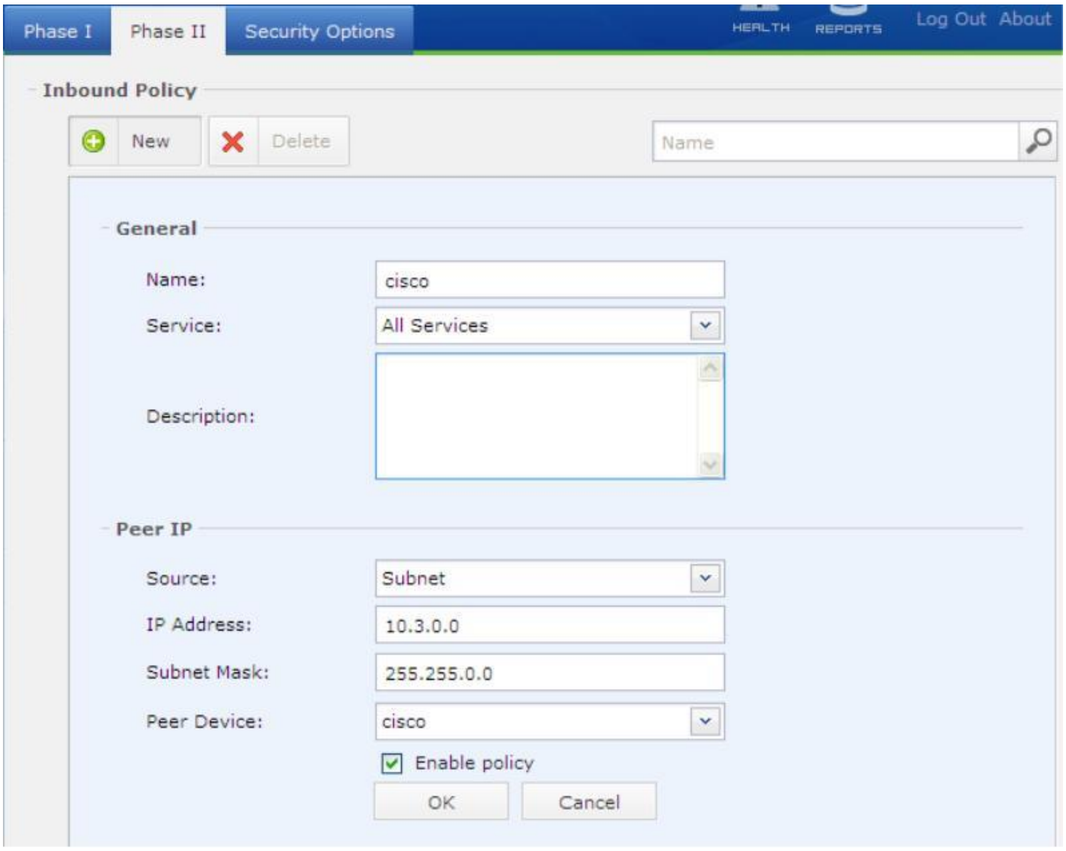
Peer Device: cisco

Security Option: cisco

SA Lifetime: 28800 seconds

☑ Enable policy

☑ Enable Perfect Forward Secrecy



General

Name: cisco

Service: All Services

Description:

Peer IP

Source: Subnet

IP Address: 10.3.0.0

Subnet Mask: 255.255.0.0

Peer Device: cisco

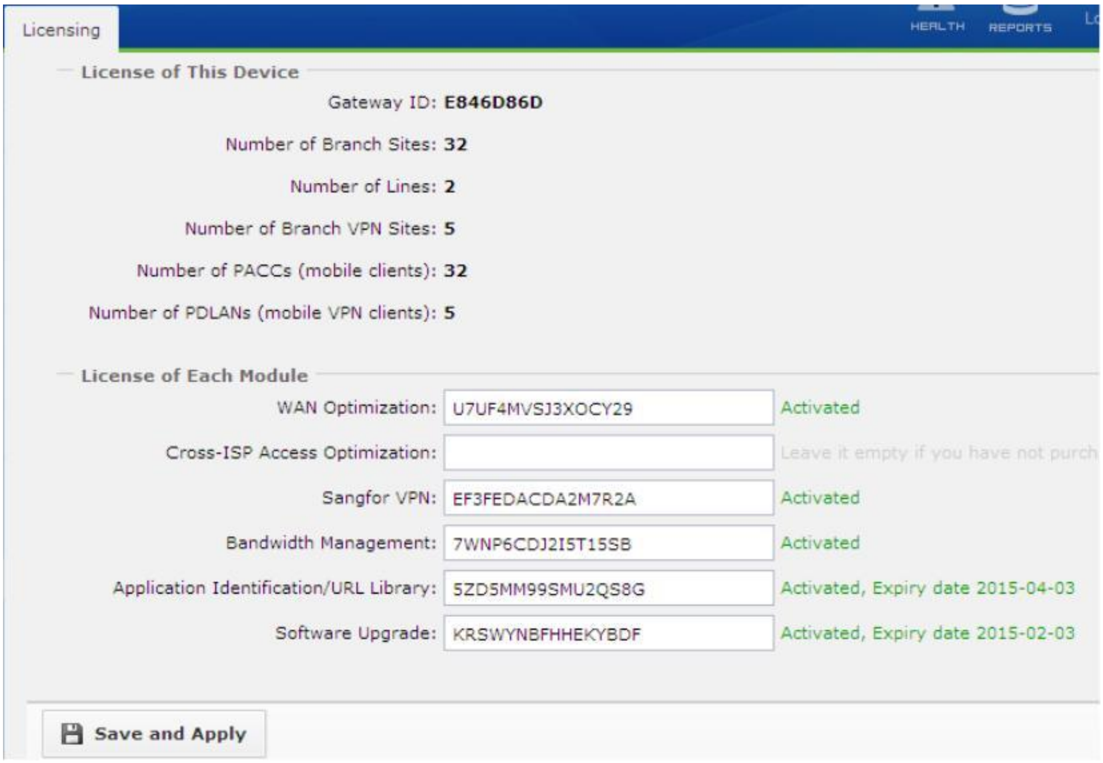
☑ Enable policy

Chapter 10 Maintenance

Licensing Sangfor WOC and Function Modules

Though the device license is attached to the purchase of Sangfor WAN Optimization Controller (WOC), the availability of some other function modules, such as WAN optimization, Sangfor VPN, IPSec VPN, bandwidth management, application identification/URL library update service and software update service are activated with separate license keys respectively.

You can go to the Maintenance > Licensing page, license the device and each function module, as shown in the figure below:



License of This Device

Gateway ID: **E846D86D**

Number of Branch Sites: **32**

Number of Lines: **2**

Number of Branch VPN Sites: **5**

Number of PACCs (mobile clients): **32**

Number of PDLANs (mobile VPN clients): **5**

License of Each Module

WAN Optimization:	U7UF4MVSJ3XOCY29	Activated
Cross-ISP Access Optimization:		Leave it empty if you have not purch
Sangfor VPN:	EF3FEDACDA2M7R2A	Activated
Bandwidth Management:	7WNP6CDJ2I5T15SB	Activated
Application Identification/URL Library:	5ZD5MM99SMU2QS8G	Activated, Expiry date 2015-04-03
Software Upgrade:	KRSWYNBFHHEKYBDF	Activated, Expiry date 2015-02-03

Save and Apply

The following are the contents included on the Licensing page:

Gateway ID: This is one of the identities of a Sangfor device and delivered to the customer together with the product suit.

Number of Branch Sites: This is the maximum number of Sangfor WAN Optimization Controllers deployed in remote networks that this WOC can support.

Number of Lines: This is the maximum number of Internet lines that the purchased Sangfor WOC can support.

Number of Branch VPN Sites: This is the maximum number of VPN sites that the purchased Sangfor WOC can support. A type of license related to Sangfor VPN.

Number of PACCs: This is the maximum number of Portable Acceleration (PACC) client software users that the purchased Sangfor WOC can support. To have accelerated access to the enterprise network, the mobile workers need only to install the PACC on their PCs and establish acceleration connection with the physical Sangfor WOC deployed in that network.

Number of PDLANs: This is the maximum number of mobile VPN users that the purchased Sangfor WOC can support. Sangfor VPN allows mobile workers to securely connect to the enterprise network, meanwhile being accelerated. To establish secure and accelerated connection to the enterprise network, the mobile workers need only to install the Sangfor Mobile VPN Client software on their PCs and initiate VPN connection to that Sangfor WOC (for more information, please refer to Appendix B: PACC & Mobile VPN Client .

WAN Optimization: Enter the license key and click the Save and Apply button to activate the WAN optimization feature. Activated means the function is available.

Cross-ISP Access Optimization: Enter the license key and click the Save and Apply button to activate the module.

Sangfor VPN: Enter the license key and click the Save and Apply button to activate the Sangfor VPN module. For more information about Sangfor VPN, please refer to Chapter 4 Sangfor VPN.

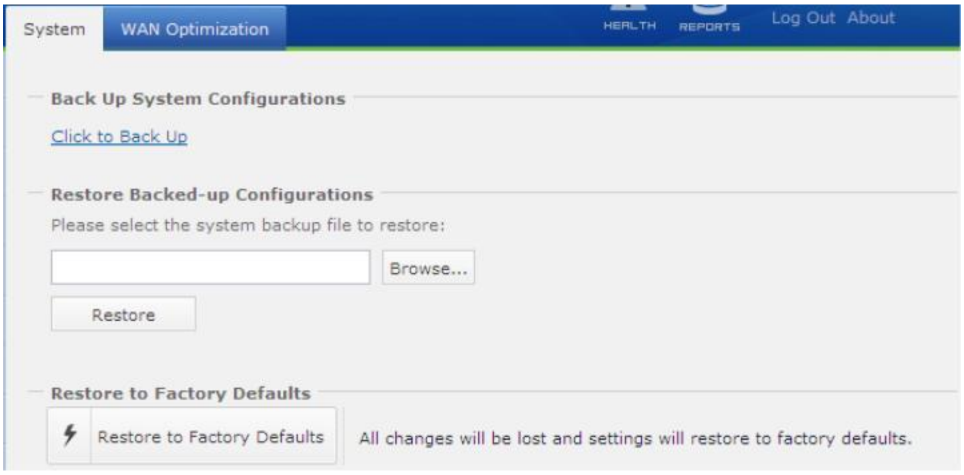
Bandwidth Management: Enter the license key and click the Save and Apply button to activate the BM module.

Application Identification/URL Library: Enter the license key and click the Save and Apply button to activate the update service of the internal application identification rule and URL library.

Software Upgrade: Enter the license key and click the Save and Apply button to activate the software upgrade service, so that you can update your Sangfor WOC if there is any new version available.

Backing Up or Restoring System Settings

Navigate to Maintenance > Backup/Restore > System to back up or restore system settings.



Back Up System Configurations

Restore Backed-up Configurations

Please select the system backup file to restore:

Restore to Factory Defaults

All changes will be lost and settings will restore to factory defaults.

To back up the current system settings, click on the Click to Back Up link under Back Up System Configurations and select a directory on the local PC.

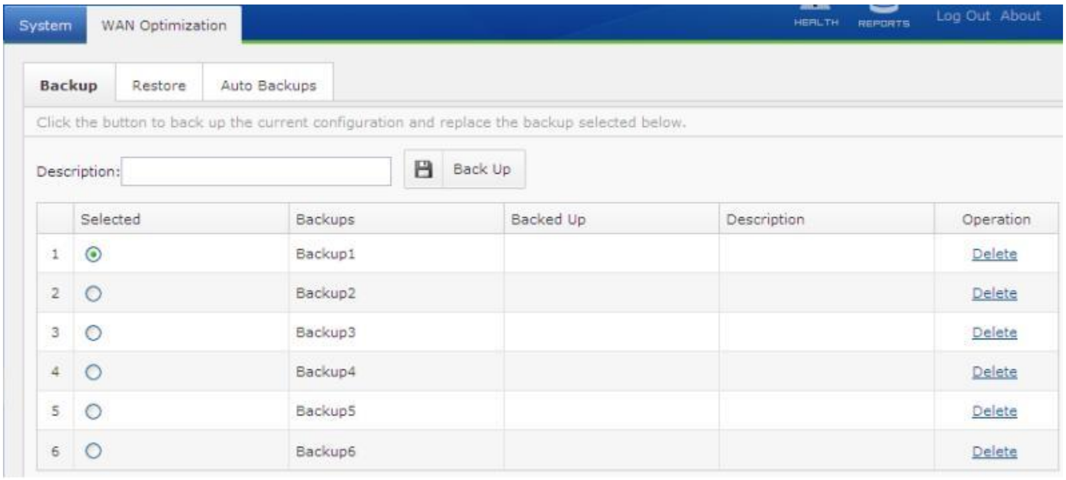
If you have ever backed up system settings onto your PC and want to restore the current system settings to that version, click the Browse button under Restore Backed-up Configuration, select and upload the backup file.

The system settings saved onto the local PC include WAN Optimization settings.

Backing Up or Restoring WANO Settings

You can back up WAN optimization settings and save them onto the Sangfor WOC separately (rather than onto the local PC), or restore the current WANO settings to the backup, without exerting any impact on system or other function modules.

1. Navigate to Maintenance > Backup/Restore > WAN Optimization.
2. To back up the current WAN optimization configuration, click the Backup tab, select the desired backup and click the Back Up button. The newly backed up configuration will replace the selected one, as shown below:

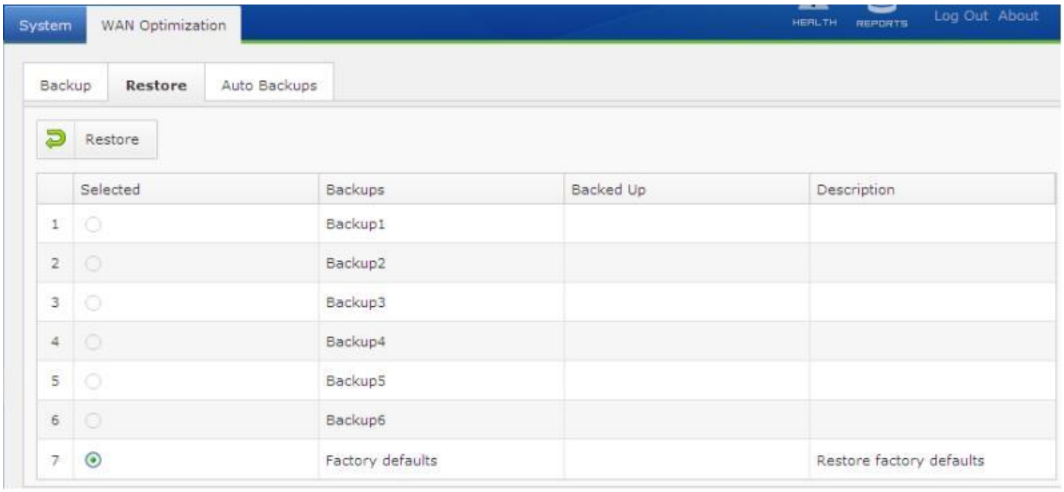


Click the button to back up the current configuration and replace the backup selected below.

Description:

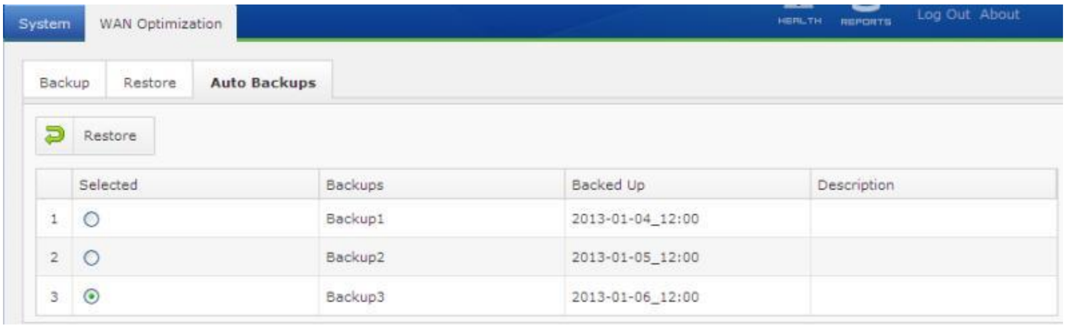
	Selected	Backups	Backed Up	Description	Operation
1	●	Backup1			Delete
2	○	Backup2			Delete
3	○	Backup3			Delete
4	○	Backup4			Delete
5	○	Backup5			Delete
6	○	Backup6			Delete

3. To replace the current WAN optimization configuration with backed up file, click the Restore tab, select the desired backup or factory defaults and click the Restore button, to as shown in the following figure:



	Selected	Backups	Backed Up	Description
1	○	Backup1		
2	○	Backup2		
3	○	Backup3		
4	○	Backup4		
5	○	Backup5		
6	○	Backup6		
7	●	Factory defaults		Restore factory defaults

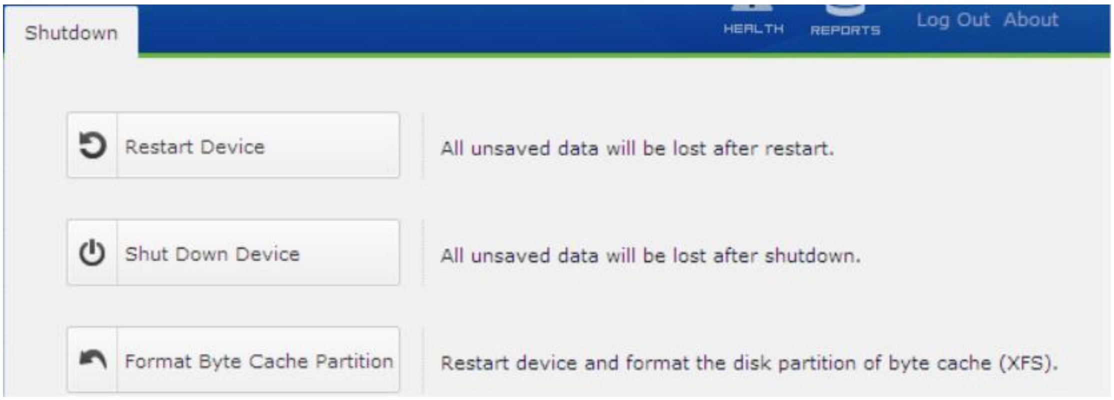
4. To replace the current WAN optimization configuration with auto-backup file, click the Auto Backups tab, select the desired backup and click the Restore button, to as shown in the following figure



	Selected	Backups	Backed Up	Description
1	○	Backup1	2013-01-04_12:00	
2	○	Backup2	2013-01-05_12:00	
3	●	Backup3	2013-01-06_12:00	

Shutdown

To soft restart or shut down to Sangfor WOC, navigate to Maintenance > Shutdown and click Restart Device or Shut Down Device button respectively. You can also format the partition allocated to byte cache.



All unsaved data will be lost after restart.

All unsaved data will be lost after shutdown.

Restart device and format the disk partition of byte cache (XFS).

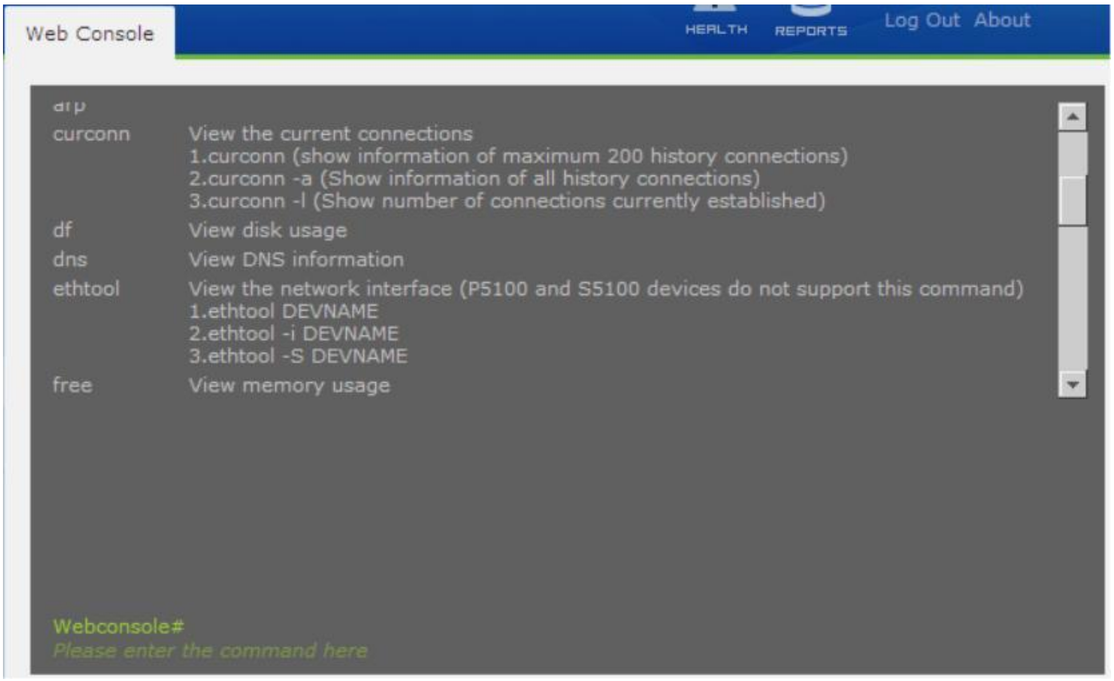
⚠

Some WOC models DO NOT support soft shutdown.

Web Console

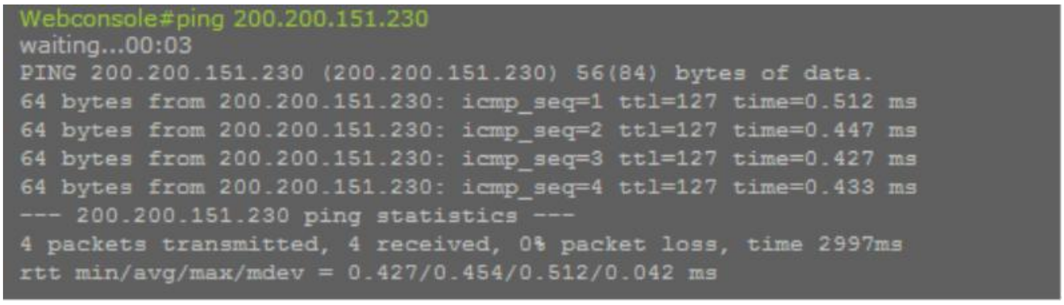
Through Web Console, you can execute some common commands, including but not limited to Ping, arp, ip route, and to check the connectivity with remote host, inspect network failure or device fault, and so on.

To view all the commands supported on Web Console, enter help into the Webconsole# field, as shown in the following figure:



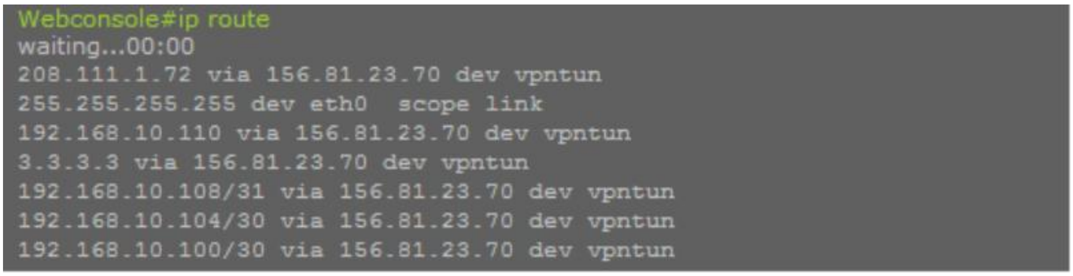
```
arp
curconn      View the current connections
             1.curconn (show information of maximum 200 history connections)
             2.curconn -a (Show information of all history connections)
             3.curconn -l (Show number of connections currently established)
df           View disk usage
dns          View DNS information
ethtool      View the network interface (P5100 and S5100 devices do not support this command)
             1.ethtool DEVNAME
             2.ethtool -i DEVNAME
             3.ethtool -S DEVNAME
free         View memory usage

Webconsole#
Please enter the command here
```

Scenario: executing Ping command



```
Webconsole#ping 200.200.151.230
waiting...00:03
PING 200.200.151.230 (200.200.151.230) 56(84) bytes of data.
64 bytes from 200.200.151.230: icmp_seq=1 ttl=127 time=0.512 ms
64 bytes from 200.200.151.230: icmp_seq=2 ttl=127 time=0.447 ms
64 bytes from 200.200.151.230: icmp_seq=3 ttl=127 time=0.427 ms
64 bytes from 200.200.151.230: icmp_seq=4 ttl=127 time=0.433 ms
--- 200.200.151.230 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.427/0.454/0.512/0.042 ms
```

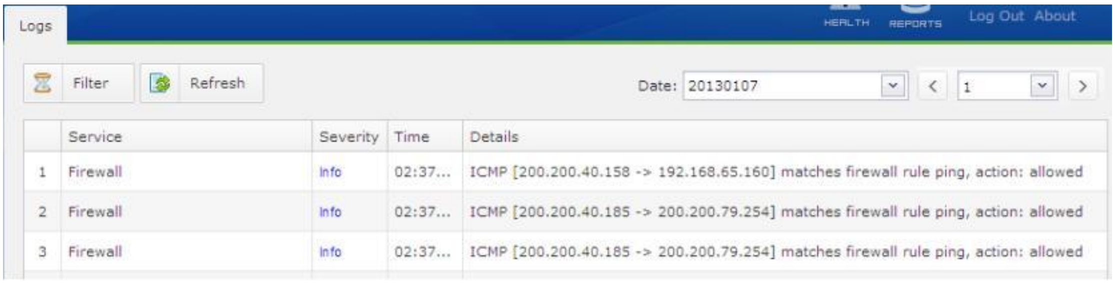
Scenario: executing ip route command



```
Webconsole#ip route
waiting...00:00
208.111.1.72 via 156.81.23.70 dev vpntun
255.255.255.255 dev eth0  scope link
192.168.10.110 via 156.81.23.70 dev vpntun
3.3.3.3 via 156.81.23.70 dev vpntun
192.168.10.108/31 via 156.81.23.70 dev vpntun
192.168.10.104/30 via 156.81.23.70 dev vpntun
192.168.10.100/30 via 156.81.23.70 dev vpntun
```

Viewing Logs

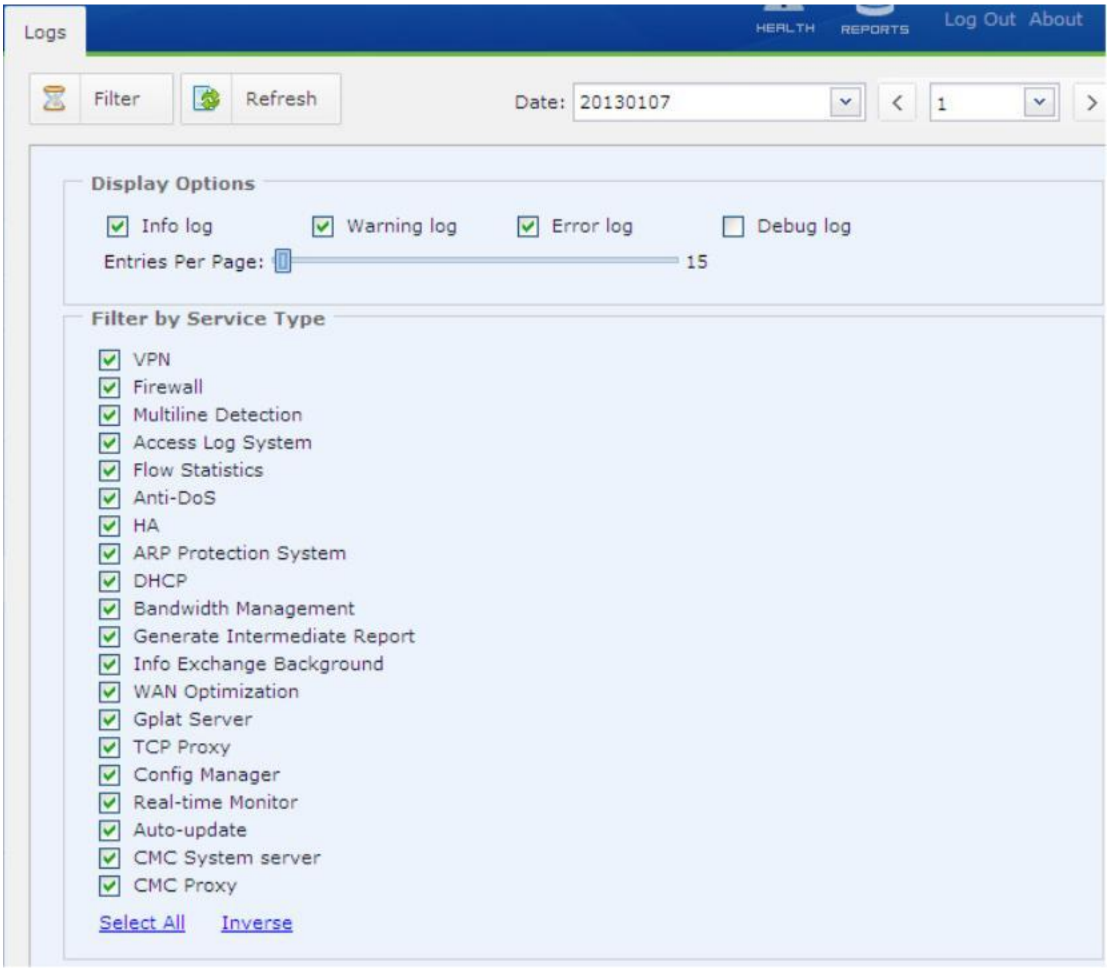
Running events and error message about the Sangfor WOC can be logged and viewed in Maintenance > Logs, as shown in the following figure:



Date: 20130107 1

	Service	Severity	Time	Details
1	Firewall	Info	02:37...	ICMP [200.200.40.158 -> 192.168.65.160] matches firewall rule ping, action: allowed
2	Firewall	Info	02:37...	ICMP [200.200.40.185 -> 200.200.79.254] matches firewall rule ping, action: allowed
3	Firewall	Info	02:37...	ICMP [200.200.40.185 -> 200.200.79.254] matches firewall rule ping, action: allowed

To view a specific log, select the date on which the event occurred approximately, or click the Filter button to specify the Display Options and service types, as shown below:



Date: 20130107 1

Display Options

☑ Info log ☑ Warning log ☑ Error log □ Debug log

Entries Per Page: 15

Filter by Service Type

- ☑ VPN
- ☑ Firewall
- ☑ Multiline Detection
- ☑ Access Log System
- ☑ Flow Statistics
- ☑ Anti-DoS
- ☑ HA
- ☑ ARP Protection System
- ☑ DHCP
- ☑ Bandwidth Management
- ☑ Generate Intermediate Report
- ☑ Info Exchange Background
- ☑ WAN Optimization
- ☑ Gplat Server
- ☑ TCP Proxy
- ☑ Config Manager
- ☑ Real-time Monitor
- ☑ Auto-update
- ☑ CMC System server
- ☑ CMC Proxy

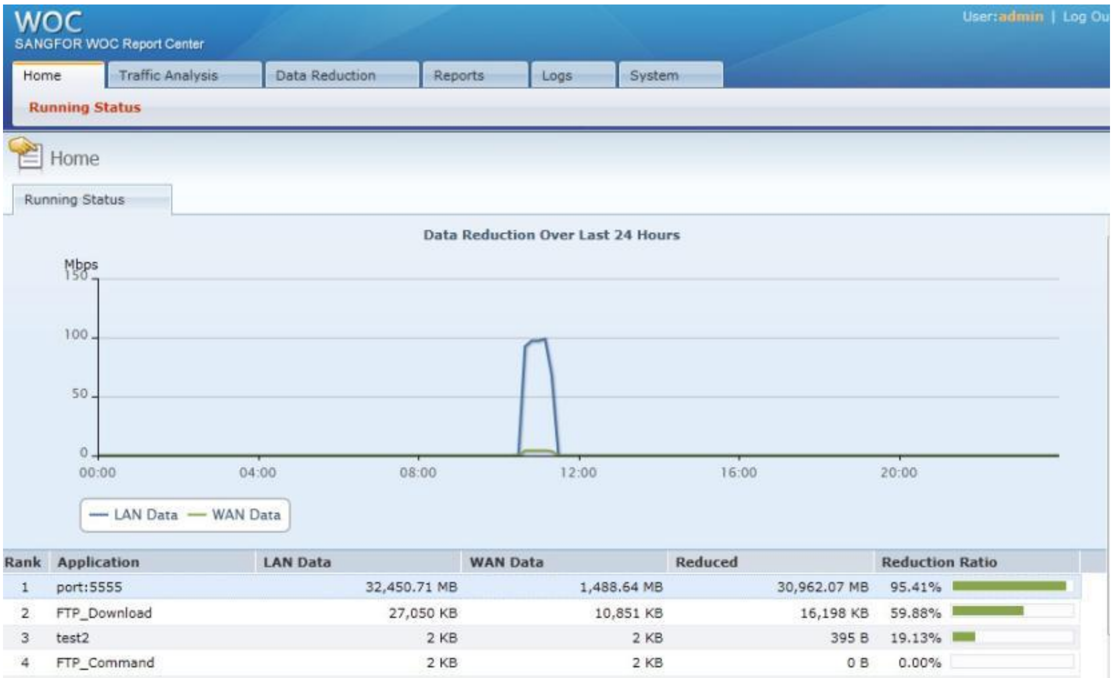
⚠

The Sangfor WAN Optimization Controller (WOC) will only save the logs for 14 days, the logs generated in earlier days will be deleted automatically.

Appendix A: Internal Report Center

Sangfor WAN Optimization Controller (WOC) is built in with a Report Center, in which you can make traffic analysis, data reduction reports based on the data transmitted through and optimized by the Sangfor WOC.

To enter the Report Center, click on the REPORTS icon at the upper right page of the Web administrator console of Sangfor WOC.



Rank	Application	LAN Data	WAN Data	Reduced	Reduction Ratio
1	port:5555	32,450.71 MB	1,488.64 MB	30,962.07 MB	95.41%
2	FTP_Download	27,050 KB	10,851 KB	16,198 KB	59.88%
3	test2	2 KB	2 KB	395 B	19.13%
4	FTP_Command	2 KB	2 KB	0 B	0.00%

The above is the homepage of Sangfor WOC Report Center, presenting the following information:

Data reduction over the past 24 hours in graph

Top 10 applications that have contributed the most reduced data

To retrieve most active applications, subnets and hosts, and generate reports, click the Traffic Analysis tab.

To get data reduction ratio based on application, subnet and internal host, click the Data Reduction tab.

To subscribe to reports on daily, weekly or monthly basis or make custom report, click on the Reports tab.

To view admin logs or firewall logs related to the Web administrator console, click on the Logs tab.

To clean up the database and configure the SMTP server and other logging options, click on the System tab.

Appendix B: PACC & Mobile VPN Client

VPN connection and/or acceleration connection can be established between two physical Sangfor WAN Optimization Controllers (WOC), or between physical WOC and computer that is installed Sangfor client software. The client software corresponding to WAN optimization is Portable Acceleration (PACC) client, while the client software corresponding to Sangfor VPN is Mobile VPN Client (or PDLAN). You can install the individual version of PACC and PDLAN, or the integrated version of PACC and PDLAN.

Network topology, software installation and configuration of them are slightly different. We only describe software installation, network topology and configuration of the integrated version, and the network topology of the use of PACC. Before installing the client software, please ensure that your PC meets the following requirements:

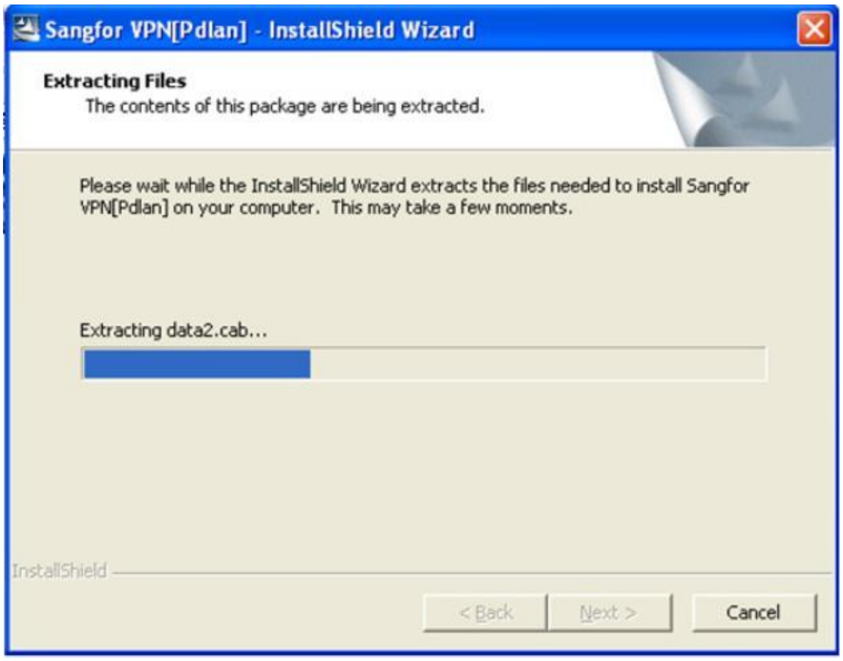
Memory: 256MB or above (VPN-only Client); 512MB or above (PACC&PDLAN Client)

Hard disk: remaining partition is 50MB or above (VPN-only Client); 1GB or above (PACC&PDLAN Client)

Operating system: Windows 2000 server, Windows XP, Windows 2003 server, Windows Vista and Windows 7 (32bit and 32bit)

Software Installation

1. Double-click the executable file to install the integrated version of Portable Acceleration (PACC) client and Mobile VPN client software, as shown below:



Sangfor VPN[Pdlan] - InstallShield Wizard

Extracting Files

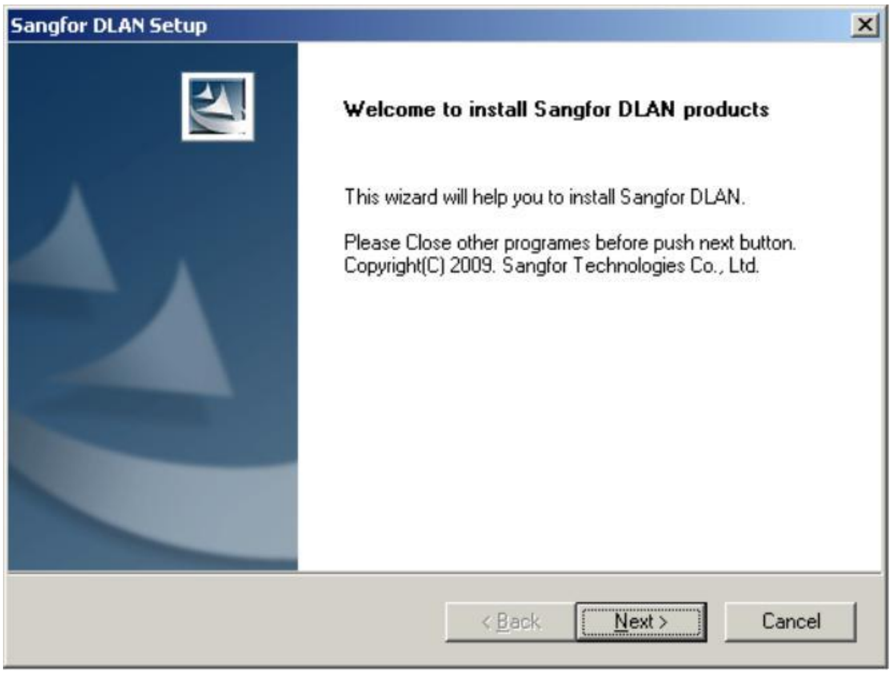
The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install Sangfor VPN[Pdlan] on your computer. This may take a few moments.

Extracting data2.cab...

Before installing the client software, terminate the antivirus program running on your computer; otherwise, installation may fail. You can run the antivirus software after the installation finishes.

2. Follow the instructions and the Wizard to install the client software, as shown below:



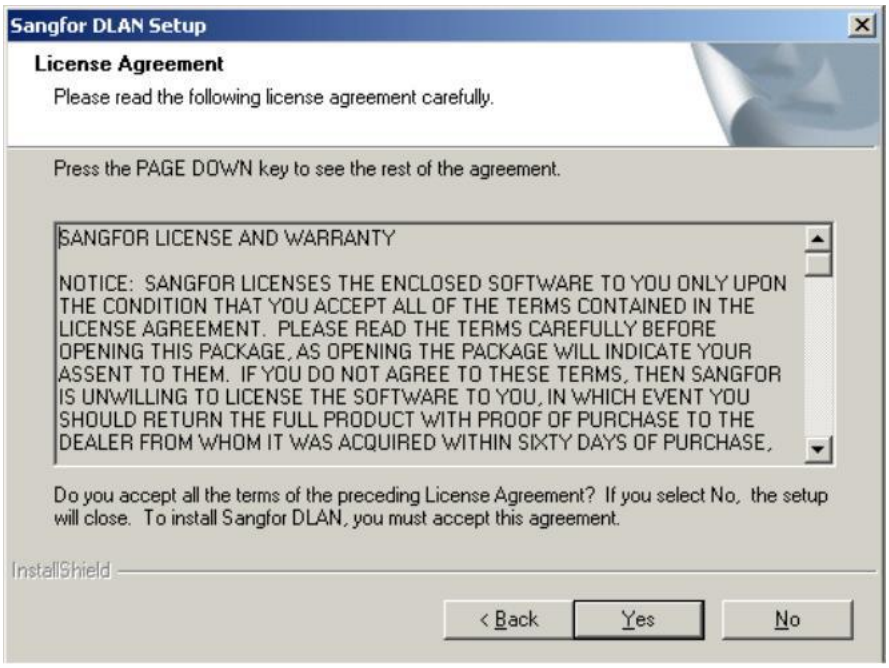
Sangfor DLAN Setup

Welcome to install Sangfor DLAN products

This wizard will help you to install Sangfor DLAN.

Please Close other programes before push next button.
Copyright(C) 2009. Sangfor Technologies Co., Ltd.

3. Click the Next button to go on the next step, as shown below:



Sangfor DLAN Setup

License Agreement

Please read the following license agreement carefully.

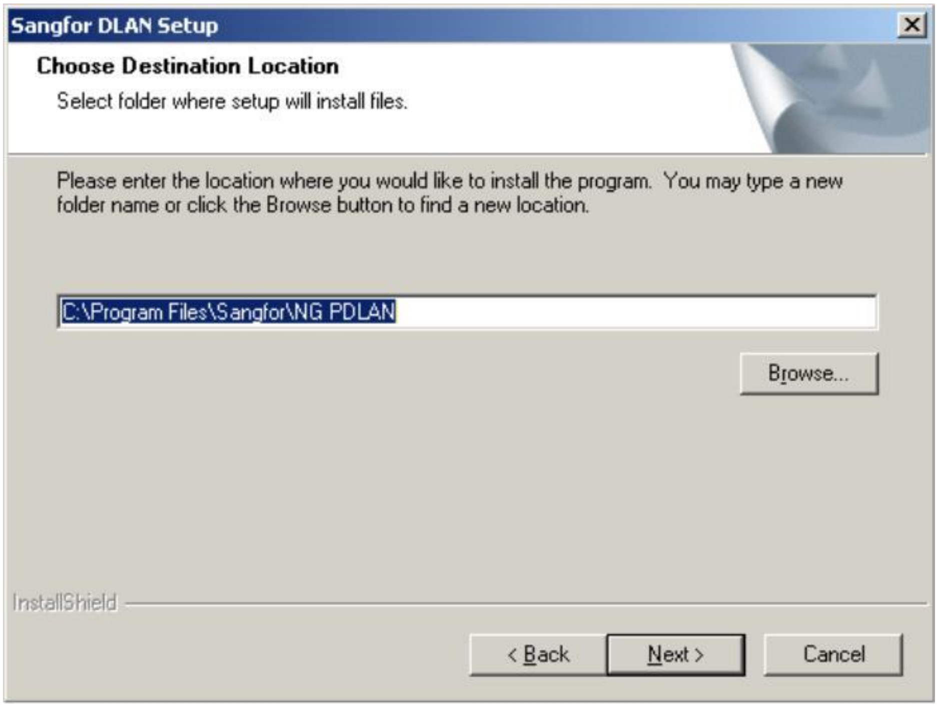
Press the PAGE DOWN key to see the rest of the agreement.

SANGFOR LICENSE AND WARRANTY

NOTICE: SANGFOR LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THE LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SANGFOR IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE,

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Sangfor DLAN, you must accept this agreement.

4. Click the Yes button to accept all the terms in the License Agreement and go on the next step, as shown below:



Sangfor DLAN Setup

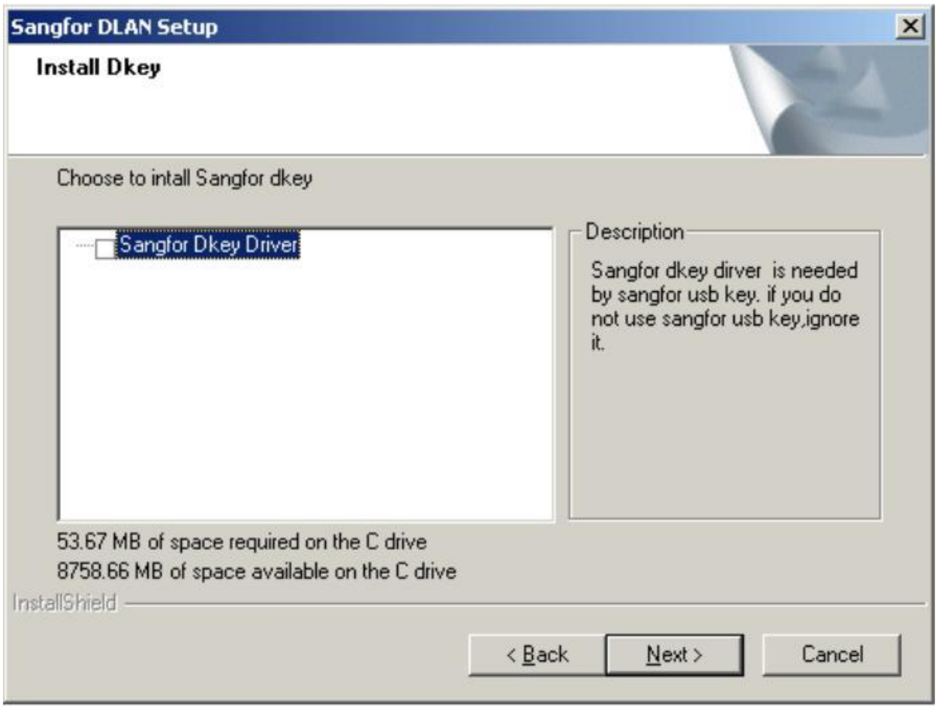
Choose Destination Location

Select folder where setup will install files.

Please enter the location where you would like to install the program. You may type a new folder name or click the Browse button to find a new location.

C:\Program Files\Sangfor\NG PDLAN

5. Click the Browse button to select an installation directory and then click the Next button to go on the next step, as shown below:



Sangfor DLAN Setup

Install Dkey

Choose to intall Sangfor dkey

□ Sangfor Dkey Driver

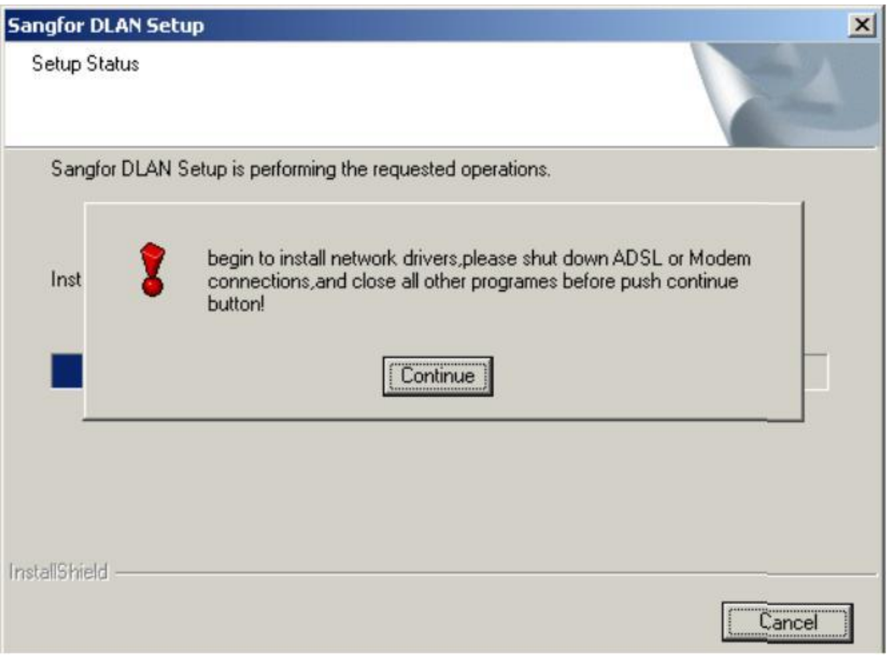
Description

Sangfor dkey dirver is needed by sangfor usb key. if you do not use sangfor usb key,ignore it.

53.67 MB of space required on the C drive

8758.66 MB of space available on the C drive

6. Select Sangfor Dkey Driver if the user is to use DKey. Click the Next button to go on the next step, as shown below:

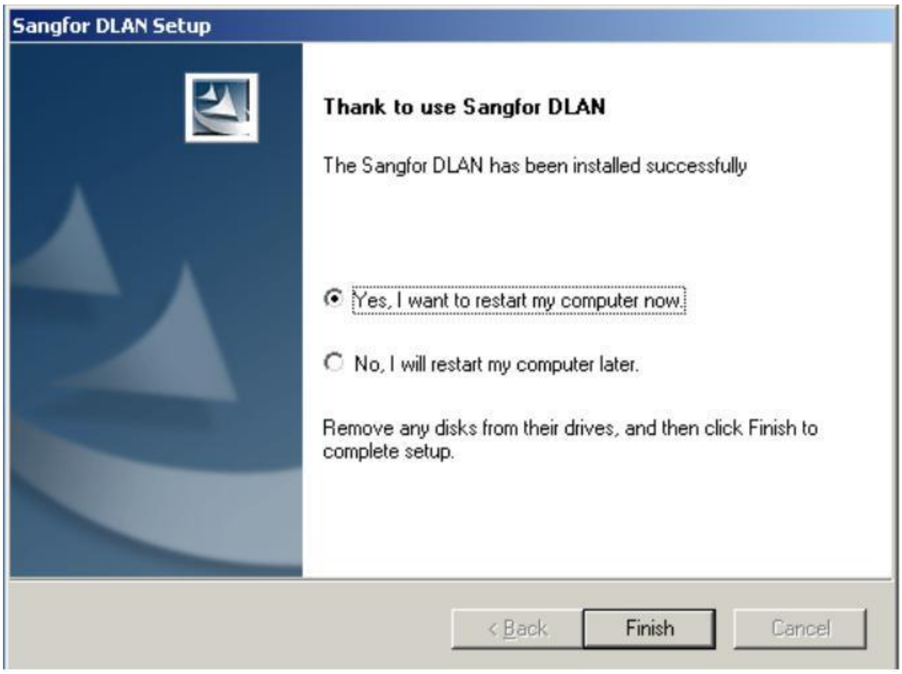


Sangfor DLAN Setup is performing the requested operations.

begin to install network drivers,please shut down ADSL or Modem connections,and close all other programes before push continue button!

During installing process, it will require disconnecting from the Internet. To ensure that installation goes smoothly, disable the Local Area Connection of the computer. You can enable it after installation completes.

7. Click the Continue button and installation process completes. Restart your computer.



Thank to use Sangfor DLAN

The Sangfor DLAN has been installed successfully

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

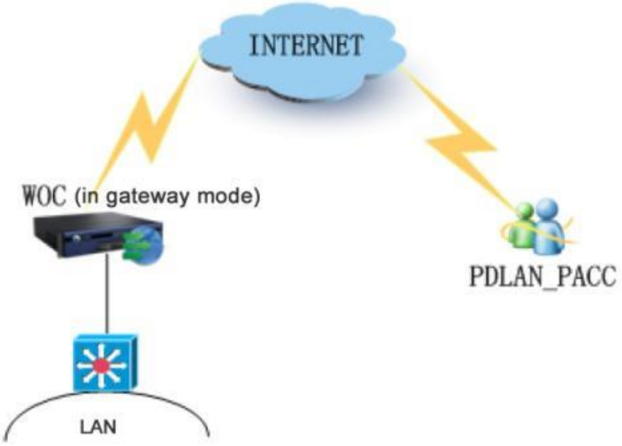
8. Enable the Local Area Connection to have the computer connect to the Internet.

Network Deployment

Deployment of WOC for Use of PACC&PDLAN

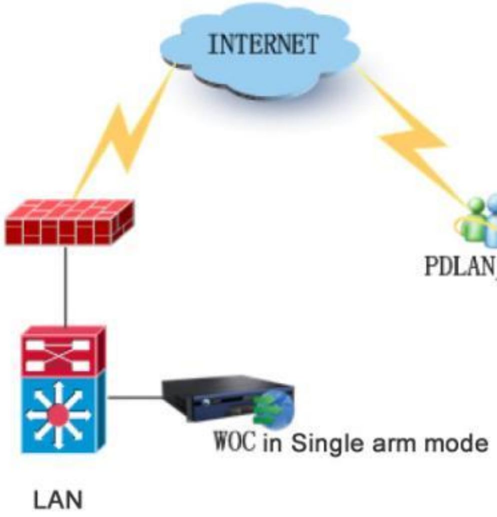
HQ WOC in Gateway Mode

The Sangfor WOC at head office is deployed in Gateway mode, and mobile worker establishes VPN and acceleration connection to the HQ WOC simultaneously, as shown in the following network topology:



HQ WOC in Single-Arm Mode

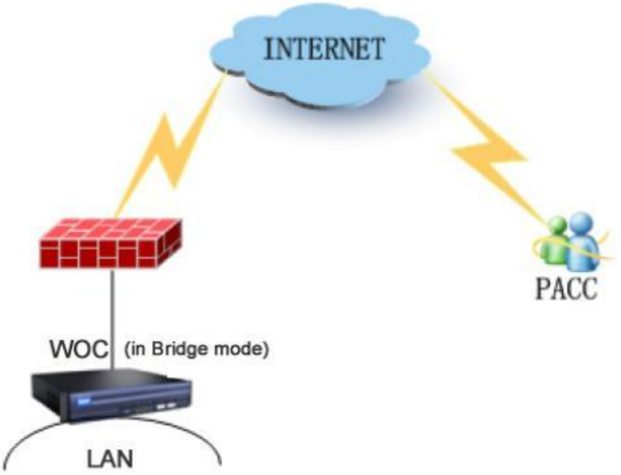
The HQ WOC is deployed in Single arm mode, on the local area network. The front-end firewall maps the TCP/UDP 4009 (default) port to the WOC, and the mobile worker establishes VPN and acceleration connection to the WOC simultaneously, as shown in the following network topology:



Deployment of WOC for Use of PACC

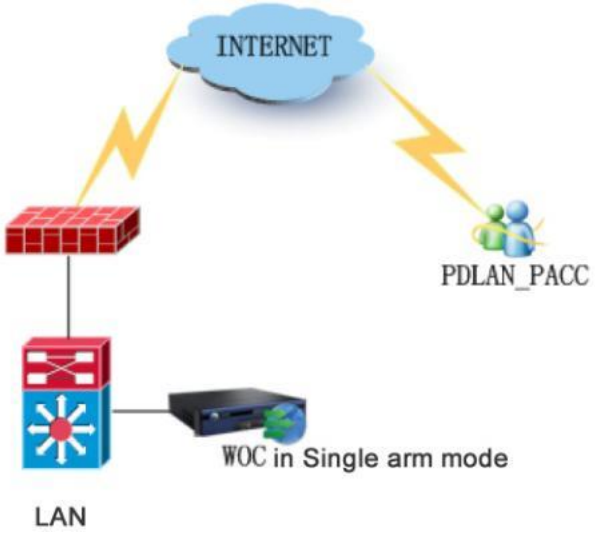
HQ WOC in Bridge Mode

The Sangfor WOC at head office is deployed in Bridge mode, and mobile worker establishes acceleration connection to the HQ WOC. The frontend firewall maps the TCP and UDP port (5400 by default) to the WOC, as shown in the following network topology:



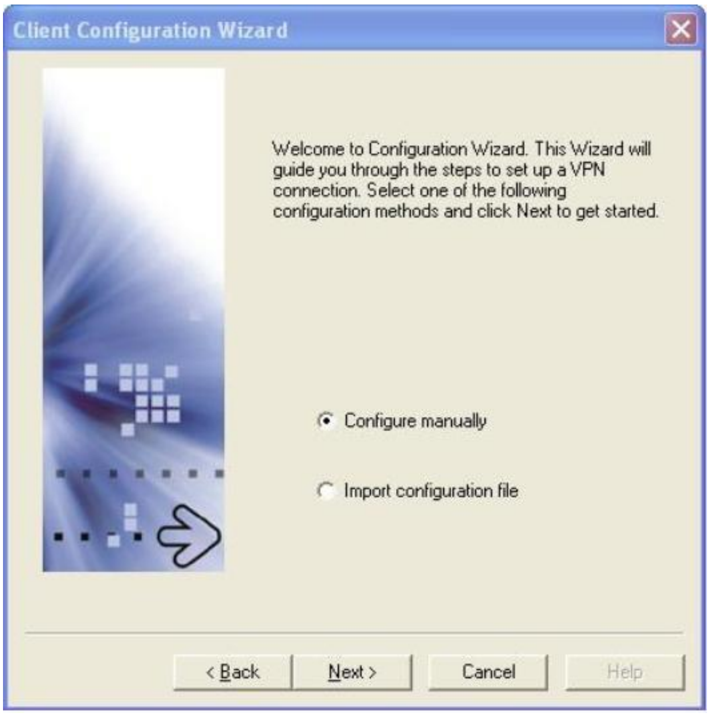
HQ WOC in Single Arm Mode

The Sangfor WOC at head office is deployed in Single Arm mode, and mobile worker establishes acceleration connection to the HQ WOC. The frontend firewall maps the TCP and UDP port (5400 by default) to the WOC, as shown in the following network topology:



Configuration

The first time you run the integrated version of Portable Acceleration (PACC) client and Mobile VPN Client software, the Configuration Wizard will pop up. Follow the instructions to complete the basic configuration of WAN optimization and Sangfor VPN.



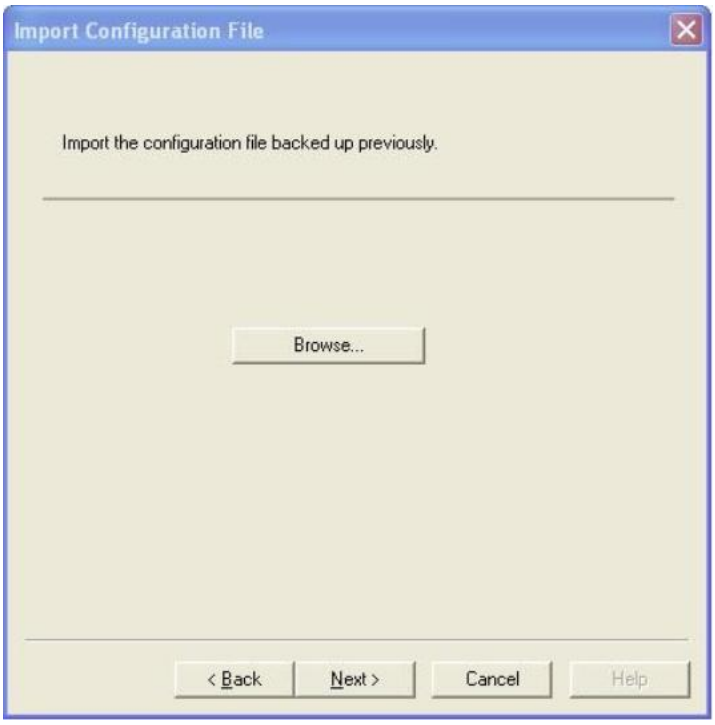
Client Configuration Wizard

Welcome to Configuration Wizard. This Wizard will guide you through the steps to set up a VPN connection. Select one of the following configuration methods and click Next to get started.

● Configure manually

○ Import configuration file

1. Select Configure Manually if you have not backed up any configuration, or select Import configuration file to simply import configuration to set up outbound VPN connection to the remote Sangfor WOC. The latter is recommended for general cases, as shown below:

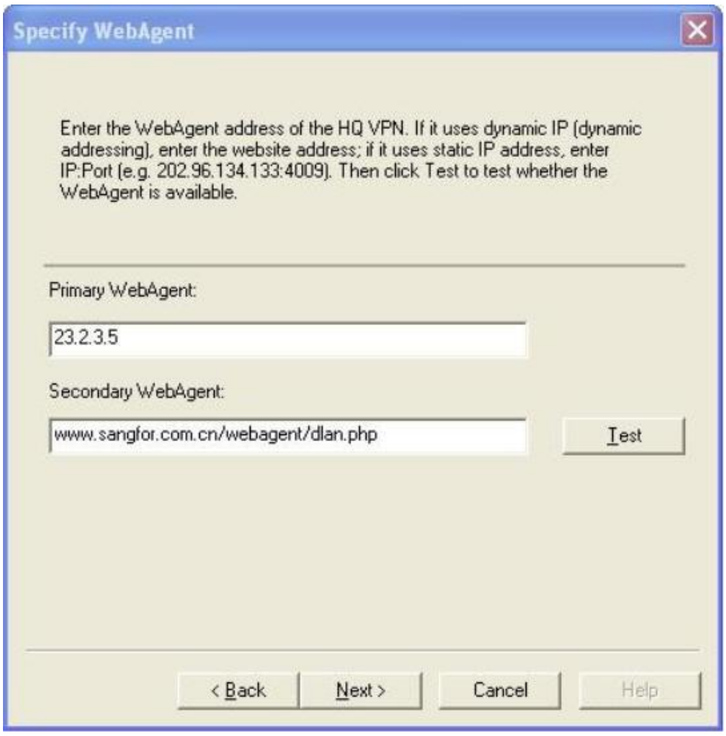


Import Configuration File

Import the configuration file backed up previously.

The file should be the one exported from the HQ WOC that contains the user account created for this mobile user.

2. If Configure Manually is selected, click the Next button to enter the Specify Webagent page.



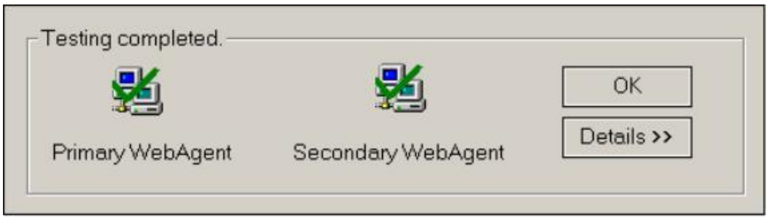
Specify WebAgent

Enter the WebAgent address of the HQ VPN. If it uses dynamic IP (dynamic addressing), enter the website address; if it uses static IP address, enter IP:Port (e.g. 202.96.134.133:4009). Then click Test to test whether the WebAgent is available.

Primary WebAgent: 23.2.3.5

Secondary WebAgent: www.sangfor.com.cn/webagent/dlan.php

3. Enter the primary and secondary Webagent of the HQ WOC and click the Test button to check the validity of the WebAgent, as shown below:

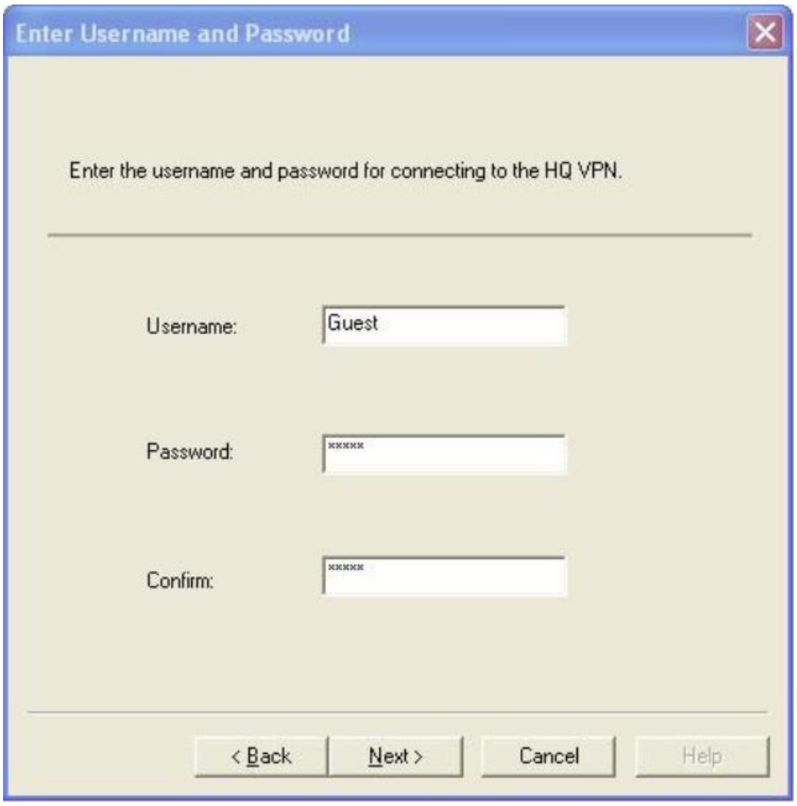


Testing completed.

If HQ WOC uses a static IP address, enter the IP address in format of IP:port. If HQ WOC uses multiple static IP addresses, enter the IP addresses in format of IP1#IP2:port.

For the Webagent address(es), contact the network administrator of the head office.

4. Click Next and enter the username/password that will be used by this mobile worker to connect to the HQ VPN site, as shown below:



Enter Username and Password

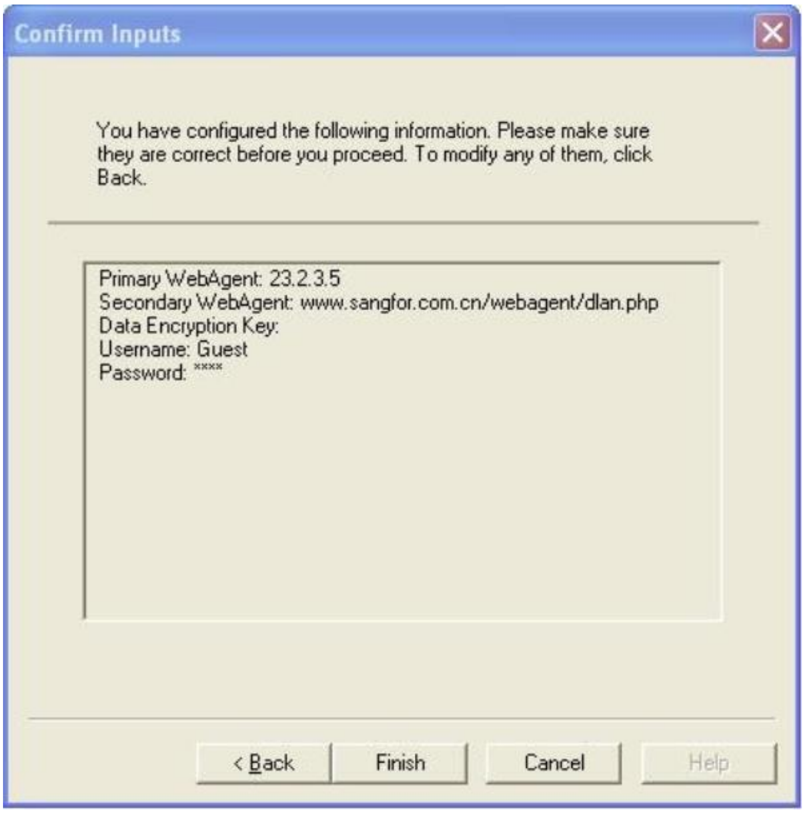
Enter the username and password for connecting to the HQ VPN.

Username: Guest

Password: *****

Confirm: *****

5. Click the Next button and then confirm the correctness of settings, as shown below:

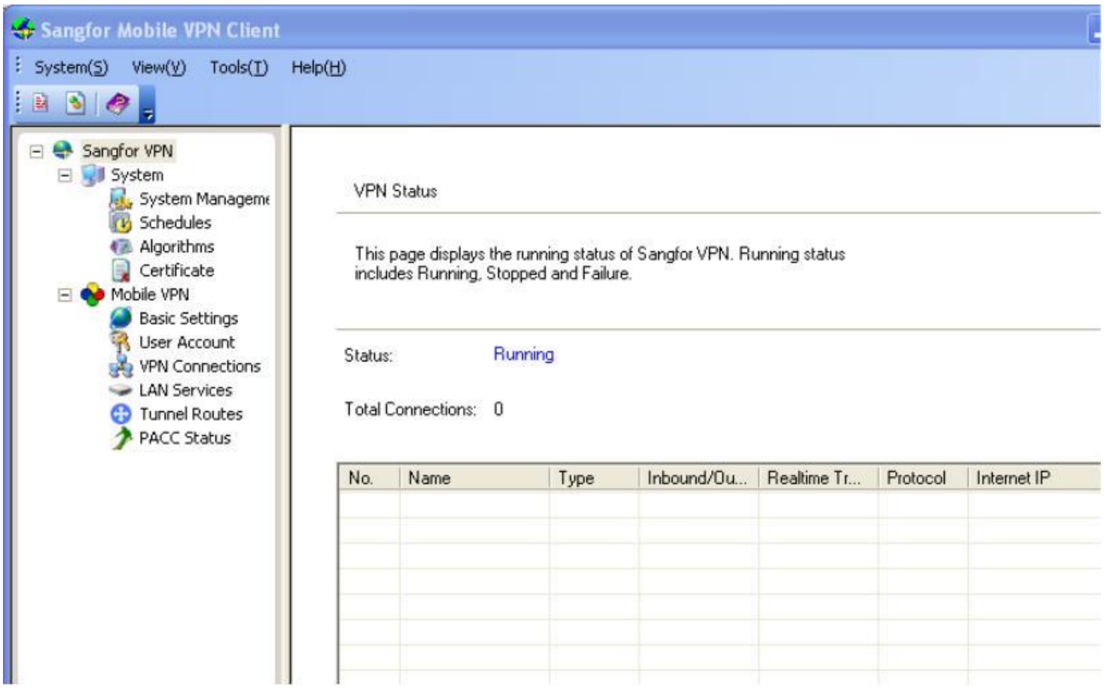


Confirm Inputs

You have configured the following information. Please make sure they are correct before you proceed. To modify any of them, click Back.

Primary WebAgent: 23.2.3.5
Secondary WebAgent: www.sangfor.com.cn/webagent/dlan.php
Data Encryption Key:
Username: Guest
Password: ****

6. Click the Finish button and confirm changes to the new configuration. Open the software and the console appears, as shown below:



VPN Status

This page displays the running status of Sangfor VPN. Running status includes Running, Stopped and Failure.

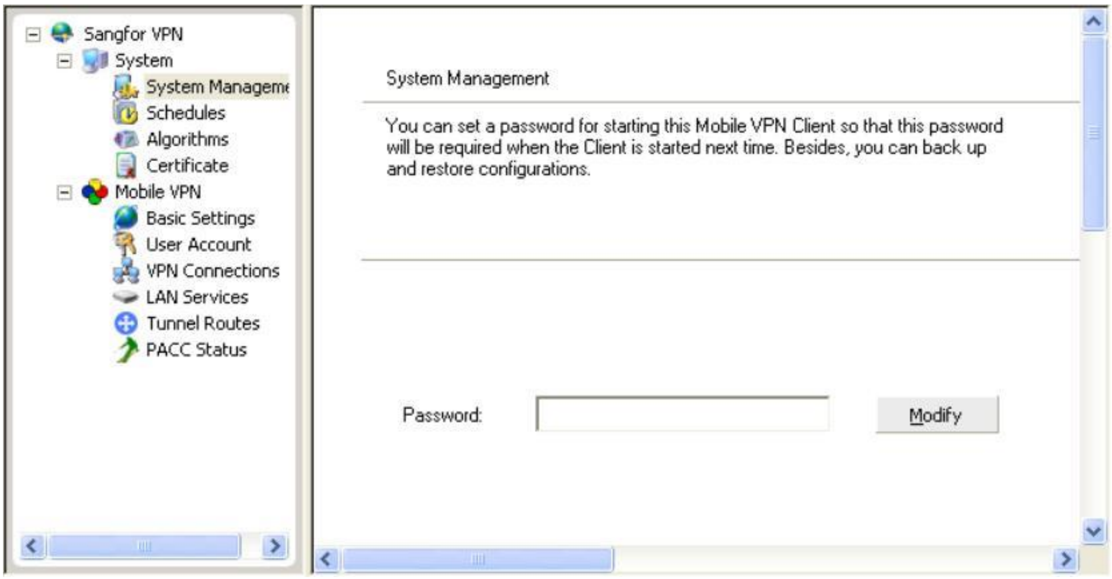
Status: Running

Total Connections: 0

No.	Name	Type	Inbound/Ou...	Realtime Tr...	Protocol	Internet IP

System Settings

System settings are global, which involves login to the client software and creating objects (such as schedule, algorithm and certificate) that may be referenced by other VPN or PACC settings.



System Management

You can set a password for starting this Mobile VPN Client so that this password will be required when the Client is started next time. Besides, you can back up and restore configurations.

Password:

System Management: You can set password for starting the client software, back up the current configuration, set password for the backup file, and restore to backup configurations

Password: Click the Modify button to configure or modify the password. Next time you start the client software, you need to enter this password. If you do not want to set password, leave the new password fields empty.

Backup Config, Restore Config: Click the button to back up or restore configuration. To backup configuration, click the Backup Config button and set password for the backup file. If you do not set password, the file will not be encrypted. To restore configuration from a backup file, click the Restore Config button and browse the configuration file you previously backed up.

Schedules: You can combine commonly used time ranges into a schedule that will be referenced by the LAN service. To add a schedule, click Add and to enter the Add Schedule page. Drag over the grids to select the desired time ranges and enable them.

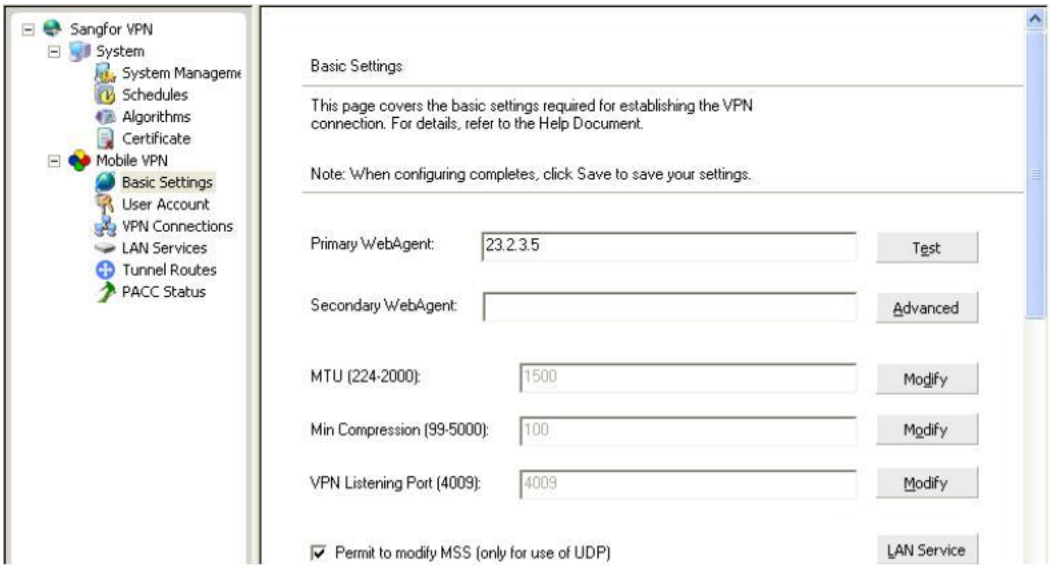
Algorithms: Configures the VPN encryption and authentication algorithms. To add an algorithm, click the Upload button and select the DLL file of the algorithm. To remove an algorithm, select the algorithm and click the Delete button. The built-in algorithms cannot be deleted.

If you want to add and use your own encryption or authentication algorithm, please make sure the encryption/authentication algorithms used on the HQ VPN and the client software are the same. Different encryption/authentication algorithms will incur failure in establishing VPN channel.

Certificates: Generate digital certificate for your computer, which is intended for authentication if you are asked to go through hardware based authentication by the HQ VPN administrator. This certificate should be sent to the HQ network administrator and imported to the HQ VPN device. Only after the HQ administrator has had the hardware-featured certificate bound with the user account, can this user establish VPN connection with the HQ VPN site smoothly.

Mobile VPN Settings

By completing the mobile VPN settings, you can establish VPN connection between the local computer and the remote Sangfor WOC.



Basic Settings

This page covers the basic settings required for establishing the VPN connection. For details, refer to the Help Document.

Note: When configuring completes, click Save to save your settings.

Primary WebAgent: 23.2.3.5

Secondary WebAgent:

MTU (224-2000): 1500

Min Compression (99-5000): 100

VPN Listening Port (4009): 4009

☑ Permit to modify MSS (only for use of UDP)

Primary/Secondary WebAgent: Configures the URL address to fulfill addressing. You can enter the URL of the trial version provided by SANGFOR. For the URL of the official version, enter the URL of your Web server.

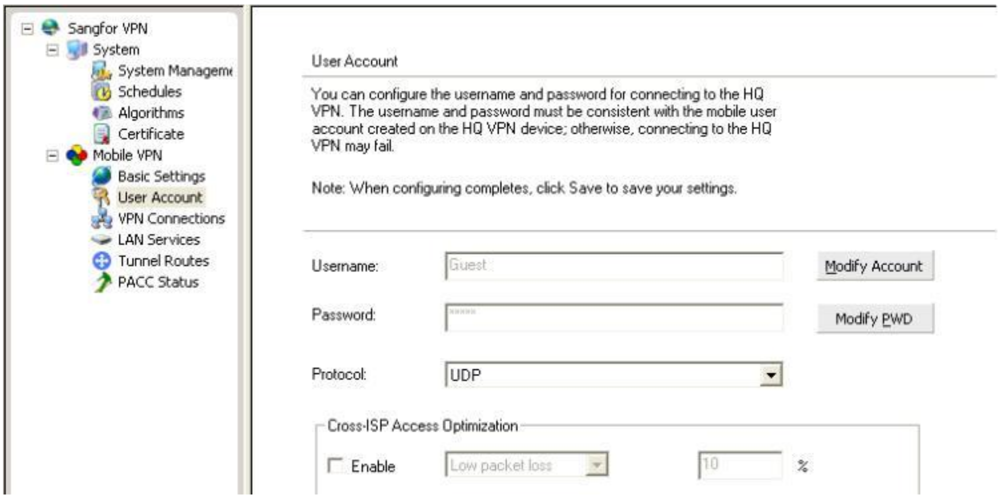
Advanced: Click this button to enter Shared Key page and configure the shared key of the WebAgent.

LAN Service: Click this button to configure the LAN services that will be accessible to the HQ VPN network.

⚠

We recommend you adopt the default MTU, Min Compression Value in general cases. If you need change these values, contact SANGFOR technical support technician.

User Account: Configures the user account and other parameters of a VPN connection. The settings on this page, in association with those on Basic Settings page, will be taken as the defaults, connecting the local computer to the specified Sangfor device.



User Account

You can configure the username and password for connecting to the HQ VPN. The username and password must be consistent with the mobile user account created on the HQ VPN device; otherwise, connecting to the HQ VPN may fail.

Note: When configuring completes, click Save to save your settings.

Username: Guest

Password: *****

Protocol: UDP

Cross-ISP Access Optimization

□ Enable Low packet loss 10 %

Username, Password: Enter the username and password configured for on HQ WOC for this user.

Protocol: Configures the transfer protocol of the VPN data. Options are TCP and UDP. When the VPN connection appears unstable, try altering the protocol.

Cross-ISP Access Optimization: If different Internet Service Providers (ISP) are providing services to the HQ VPN site and your network, and the Cross-ISP Access Optimization License of the HQ VPN WOC is activated, you may select this option to optimize cross-ISP access based on the current packet loss rate. Packet loss rate must first be assessed by other means.

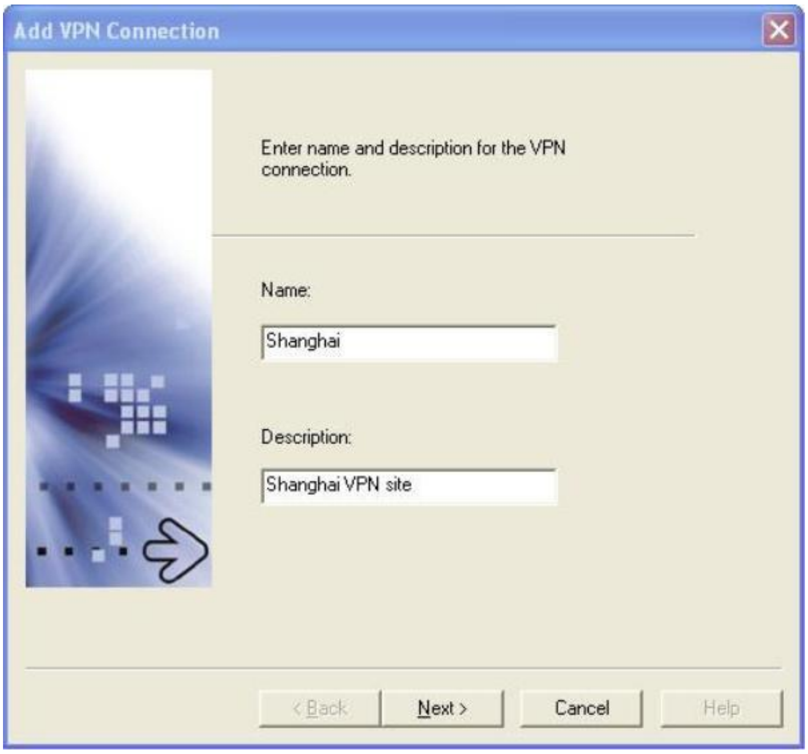
VPN Connections: Configures the profile of the VPN connection, so that the mobile worker can connect to remote VPN site.

Setting Up Outbound VPN Connection

Since the settings in Basic Settings and User Account can establish outbound VPN connection to only one remote Sangfor device, you need to add profile of another VPN connection in Mobile VPN > VPN Connections if you want to establish outbound VPN connection to another remote Sangfor device.

To add a new VPN connection, perform the steps below:

1. Go to Mobile VPN > VPN Connection and click the New button to add a new VPN connection, as shown below:



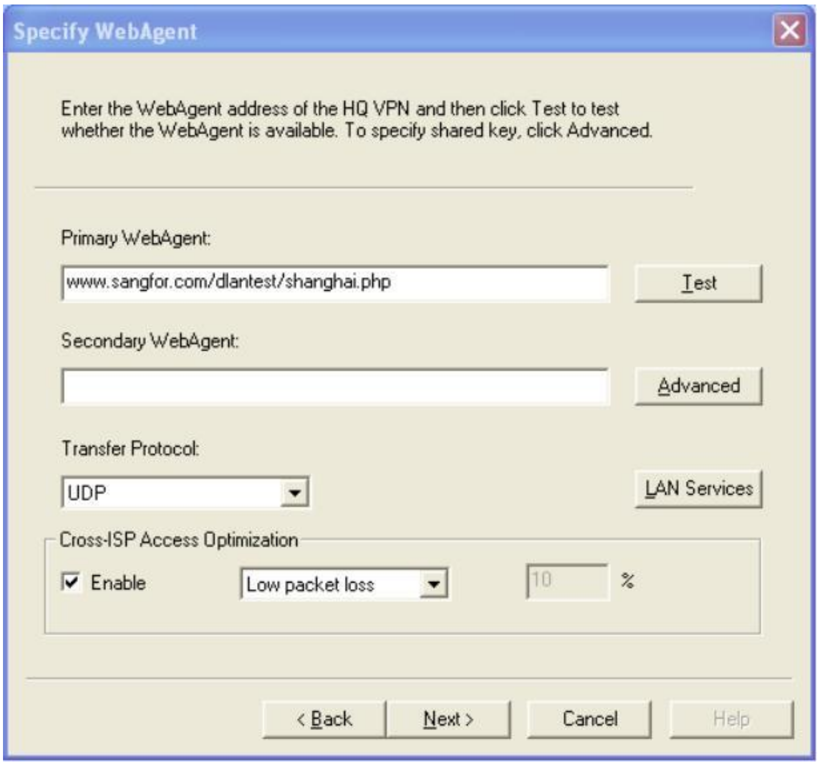
Enter name and description for the VPN connection.

Name: Shanghai

Description: Shanghai VPN site

2. Enter name and description for this VPN connection (better the name of the HQ VPN site),

and then click the Next button to go on the next step, as shown below:



Specify WebAgent

Enter the WebAgent address of the HQ VPN and then click Test to test whether the WebAgent is available. To specify shared key, click Advanced.

Primary WebAgent: www.sangfor.com/dlantest/shanghai.php

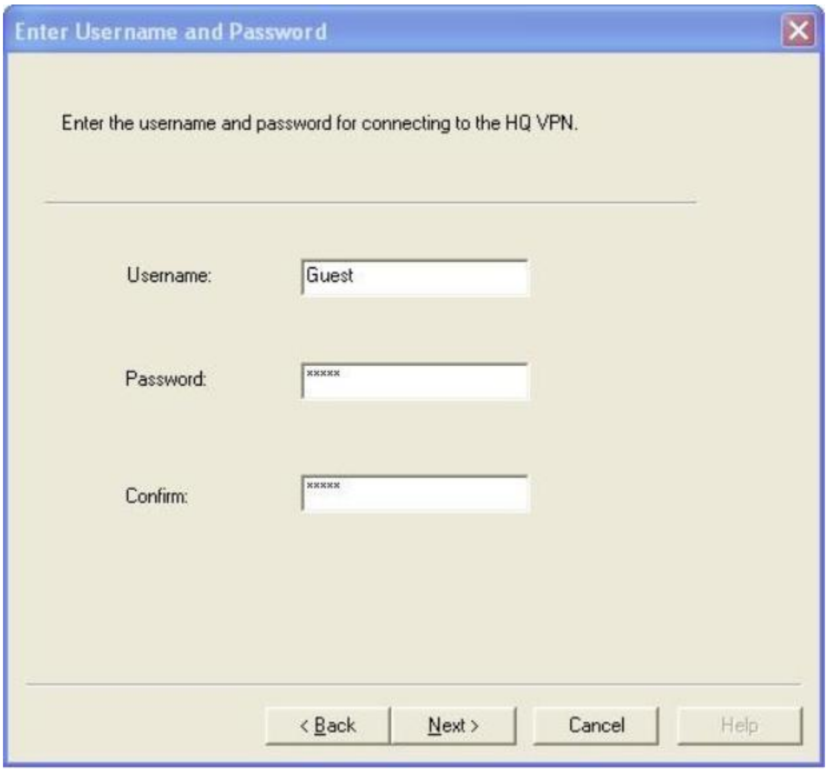
Secondary WebAgent:

Transfer Protocol: UDP

Cross-ISP Access Optimization

☑ Enable Low packet loss 10 %

3. Configure Webagent and transfer protocol, LAN services and then click the Next button to go on the next step, as shown below:



Enter Username and Password

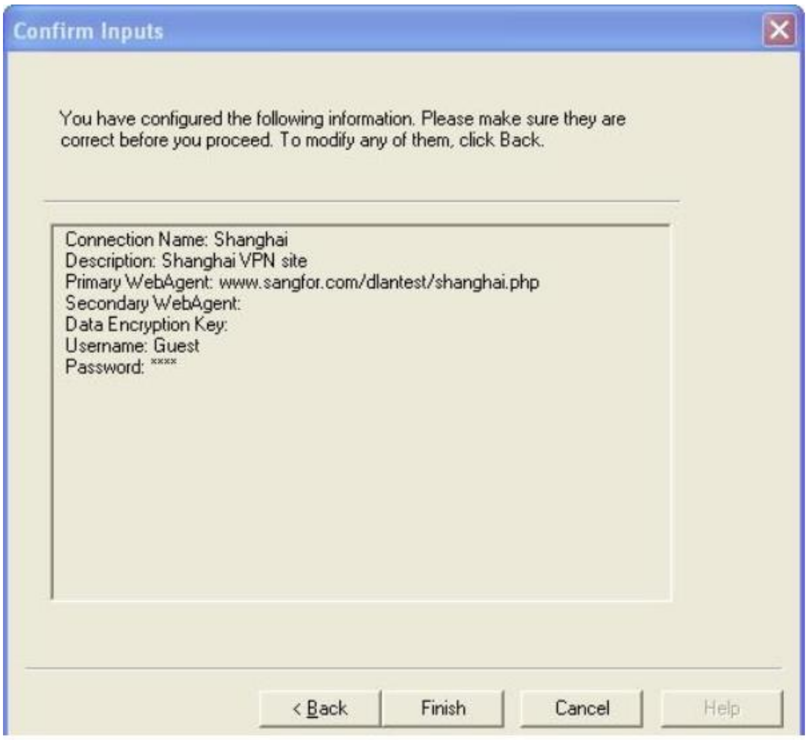
Enter the username and password for connecting to the HQ VPN.

Username: Guest

Password: *****

Confirm: *****

4. Enter the username and password used for establishing outbound VPN connection and click the Next button, as shown below:



You have configured the following information. Please make sure they are correct before you proceed. To modify any of them, click Back.

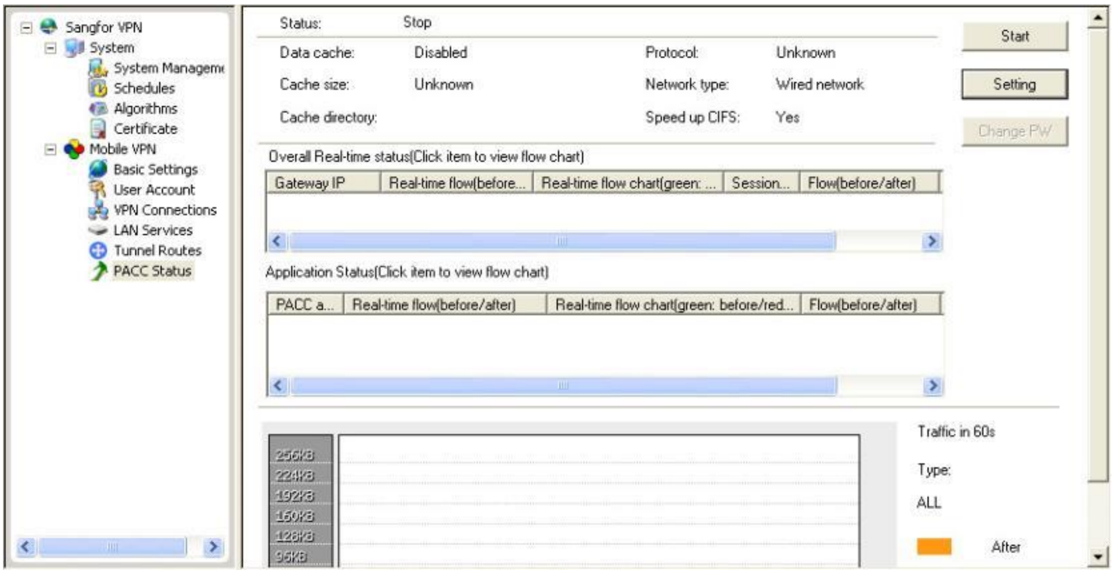
Connection Name: Shanghai
Description: Shanghai VPN site
Primary WebAgent: www.sangfor.com/dlantest/shanghai.php
Secondary WebAgent:
Data Encryption Key:
Username: Guest
Password: ****

5. Check the correctness of the information and then click the Finish button.

If the mobile worker needs only to connect to one Sangfor device, no connection needs to be added in Mobile VPN > VPN Connections.

PACC Settings & WAN Optimization Status

You can view WAN optimization status and configure optimization related options.



Status: Stop

Data cache: Disabled
Cache size: Unknown
Cache directory:
Protocol: Unknown
Network type: Wired network
Speed up CIFS: Yes

Overall Real-time status(Click item to view flow chart)

Gateway IP	Real-time flow(before...	Real-time flow chart(green: ...	Session...	Flow(before/after)

Application Status(Click item to view flow chart)

PACC a...	Real-time flow(before/after)	Real-time flow chart(green: before/red...	Flow(before/after)

Type:
ALL

The following are the contents included on the PACC Status page:

Status: Shows the running status of PACC.

Data cache: Indicates whether data cache feature is enabled.

Cache size: Indicates the current size of data cache.

Cache directory: Indicates the current directory of data cache.

Protocol: Indicates the protocol currently used.

Network type: Indicates how your network is connected to the Internet currently.

Speed up CIFS: Indicates whether CIFS optimization is enabled.

Overall Real-time Status: Shows the information of connected Sangfor WOC, such as IP address, real-time flow(chart), sessions, flow before/after acceleration and data reduction ratio.

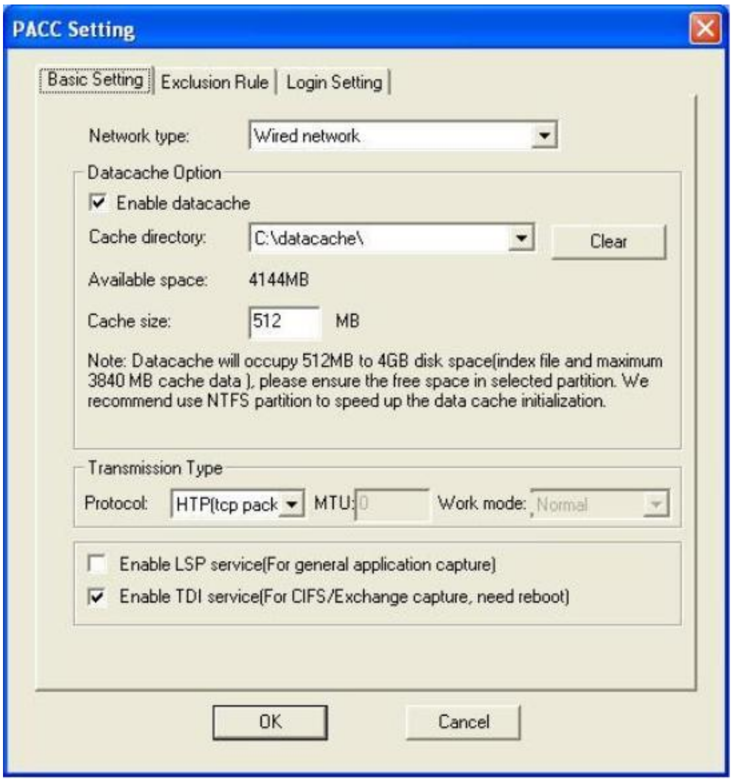
Application Status: Shows the optimization status of applications.

Real-time flow in 60 seconds: Shows the real-time traffic going through PACC in the past 60 seconds. Grey stands for the traffic amount before acceleration and Orange stands for the traffic amount after acceleration.

Start, Stop: Click the button to start or stop the Portable Acceleration (PACC) client software.

Change PW: After the acceleration connection is established, you can click this button to modify the login password.

Setting: Click this button to enter the PACC Setting dialog and configure the PACC client software.



Network type: Wired network

Datacache Option

☑ Enable datacache

Cache directory: C:\datacache\

Available space: 4144MB

Cache size: 512 MB

Note: Datacache will occupy 512MB to 4GB disk space(index file and maximum 3840 MB cache data), please ensure the free space in selected partition. We recommend use NTFS partition to speed up the data cache initialization.

Transmission Type

Protocol: HTP(tcp pack MTU: 0 Work mode: Normal

☐ Enable LSP service(For general application capture)

☑ Enable TDI service(For CIFS/Exchange capture, need reboot)

Network type: Specifies how user's PC connects to the Internet. If it is connected wirelessly (through CDMA, GPRS, etc.; yet excluding WiFi, etc), choose the corresponding option (Wireless network) and it will optimize the wireless networks. Auto detect is the default selection.

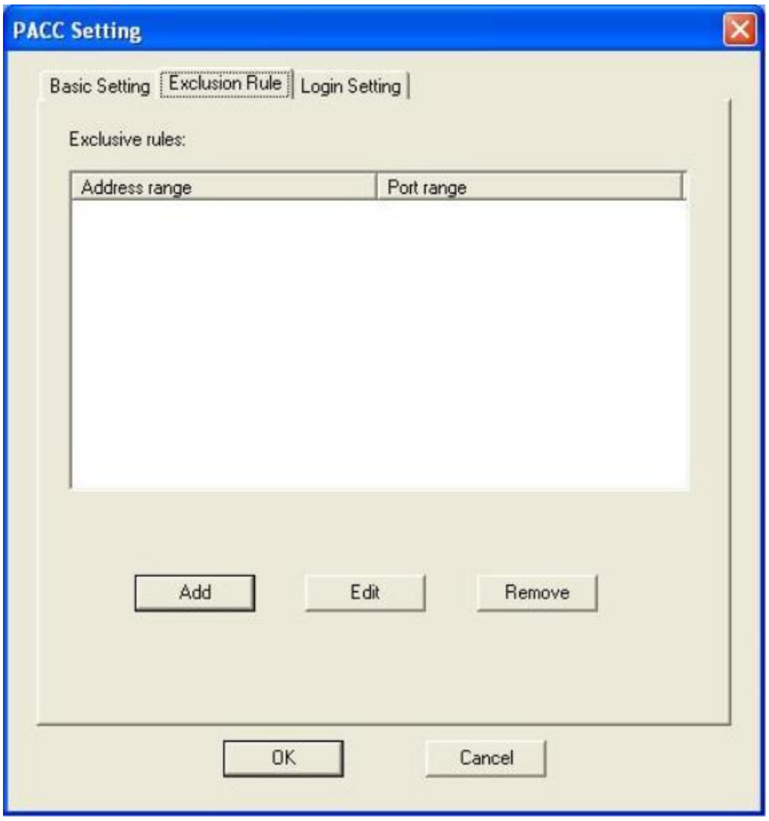
Enable datacache: Select this option and select a directory to enable byte cache function.

Clear: Click it to clear the files in the Cache directory.

Cache size: Configures the size of the local hard disk space allocated for use of byte cache.

Enable LSP Service: Select this option and it will capture the data packets of the applications that are being accelerated, except those of My Network Places and Exchange.

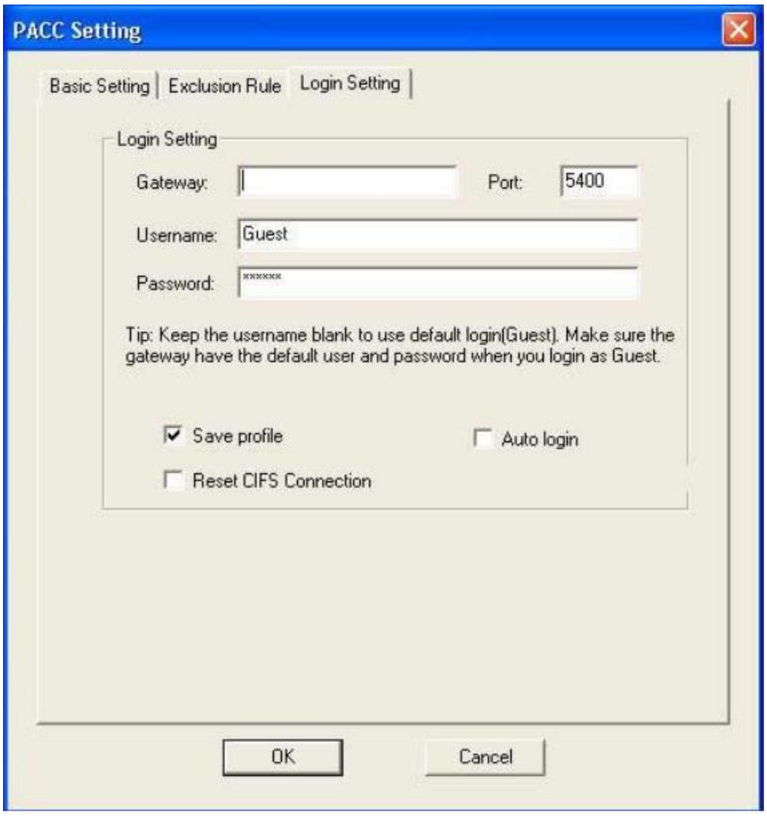
Enable TDI Service: Select this option and it will optimize My Network Places and Exchange. The option takes effect after computer reboot.



Exclusion Rule: Configures the server-end IP addresses whose data transmission will not be optimized. The PACC users' requests of accessing these excluded IP addresses will not get into the acceleration channel. To add an exclusion rule, click Add and configure the following :

Port Range: Enter the ports to be excluded from the acceleration policies.

IP Type: Specifies the type of the IP addresses to be excluded from the acceleration policies.



Login Setting

Gateway: |

Port: 5400

Username: Guest

Password: ******

Tip: Keep the username blank to use default login(Guest). Make sure the gateway have the default user and password when you login as Guest.

☑ Save profile

☐ Auto login

☐ Reset CIFS Connection

Gateway: Indicates IP address or URL of the remote Sangfor WOC.

Port: Indicates the listening port of server. By default, it is 5400.

Username, Password: Type in the correct username and password that have been configured on the remote Sangfor WOC for this user.

Save profile: Save the information you have specified above for next login, so that you will not be bothered to enter the information again next time you log in.

Auto login: Select it so that you can log in automatically next time when you double-click the icon to start the client software.

Appendix C: Sangfor Firmware Updater

Sangfor Firmware Updater is intended to update version and restore configurations of any Sangfor device, IAM, SSL VPN, WANO, AD. The following are feature of Sangfor Firmware Updater.

1. Simplified update process

   Firmware Updater works as an update wizard, support online update feature that helps search for updates and analyze versions of available updates for the connected Sangfor device in the local area network.

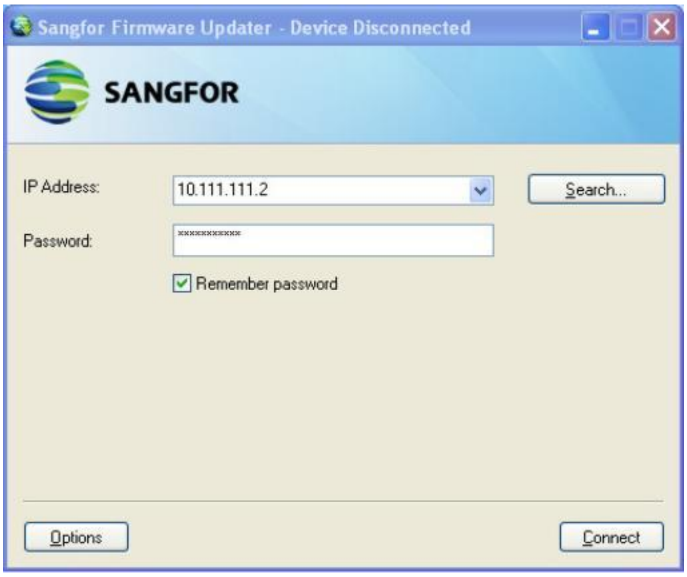
   Using online update method to update Sangfor device, network administrators need not handle some troubles such as preparing Sangfor device, checking current version of their Sangfor device, downloading update package, etc., but only choose an available version and click buttons.

   In addition to online update, administrators can browse and upload an existing package from the computer to update the Sangfor device manually or restore the configuration if the package is backed up previously.

2. The program file that can launch Sangfor Firmware Updater is included in a compressed file and available once the compressed file is decompressed, without being installed on the computer.

Updating Your Sangfor Device

1. Download the SANGFOR-Updater6.0.zip file from the Sangfor official website.
2. Double-click the executive file SANGFOR Firmware Updater.exe, and then specify or search for the Sangfor device that you want to connect to and update, as shown below:



Sangfor Firmware Updater - Device Disconnected

IP Address: 10.111.111.2

Password: ***********

☑ Remember password

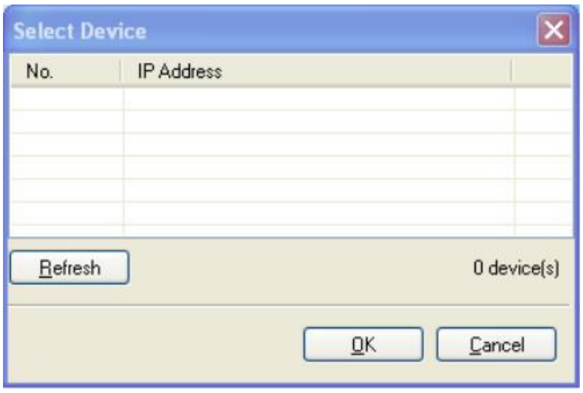
The following are the contents included on the above page:

IP Address: Enter the LAN interface IP address of the Sangfor device that you want to connect to and update. IP:Port format is supported.

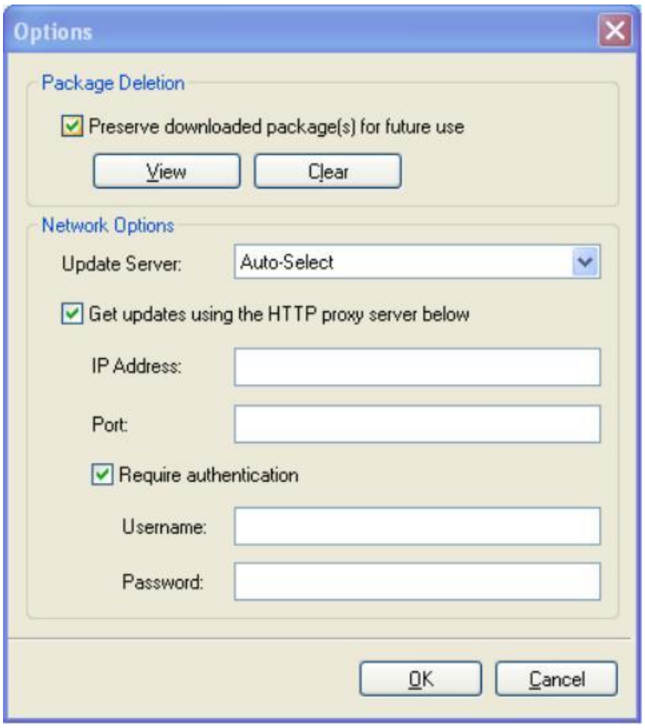
Password: Enter the password for connecting to the Sangfor device specified above. The default password is dlanrecover (case-sensitive), or password of the default administrator account (Admin or admin) for connecting to the administrator console.

Remember password: Select this option to remember the password so that the password need not be entered once again when you connect to this device via Sangfor Firmware Updater next time.

Search: Click this button to search for Sangfor devices in the local area network. If any Sangfor device is found, it will be displayed on Select Device page, as shown below:



3. Click the Options button to configure Package Deletion option and network related settings, as shown below:



☑ Preserve downloaded package(s) for future use

Update Server: Auto-Select

☑ Get updates using the HTTP proxy server below

☑ Require authentication

The following are the contents included on the Options page:

Preserve downloaded package(s) for future use: Select this option and the previously downloaded packages (in Download folder) will be preserved and can be used for future update or configuration restoring.

To open Download folder and view the downloaded package(s), click the View button.

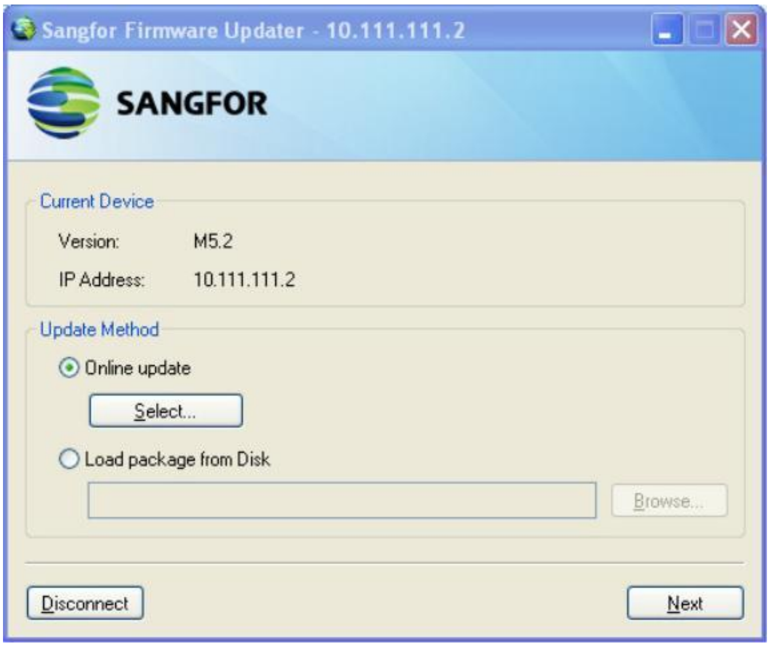
To delete all the downloaded packages in Download folder, click the Clear button.

Update Server: Select an update server, Shenzhen or Shanghai, which will always be used to get updates, or select Auto-Select to have the system select update server every time. This option only works when update method is online update.

Get updates using the HTTP proxy server below: To specify a HTTP proxy server to get updates for the connected Sangfor device, select this option and enter the IP address and port of the HTTP proxy server in the IPAddress and Port fields respectively.

Require authentication: To have the HTTP proxy server require authentication, select this option and enter the username and password into the Username and Password fields respectively.

4. Click the Connect button to connect to the specified Sangfor device and select Online update method or Load package from Disk, as shown in the figure below:



Sangfor Firmware Updater - 10.111.111.2

Current Device

Version: M5.2

IP Address: 10.111.111.2

Update Method

● Online update

○ Load package from Disk

Under Current Device are the version information (e.g., M5.2 of SSL VPN) and IP address (e.g., 10.111.111.2) of the currently connected Sangfor device.

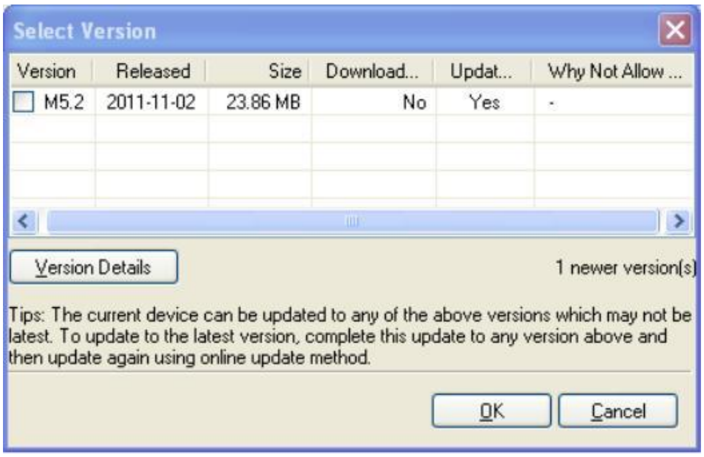
Under Update Method are two options, Online update and Load package from Disk. The former is the previously mentioned feature that can automatically get updates for the connected Sangfor device, and the latter enables administrator to choose a package to update the current device or restore the configurations on the current Sangfor device with those contained in the chosen package.

Currently, online update only supports update of version SSL M5.0 and above. For update of lower versions and other series of Sangfor devices, please select the update method Load package from Disk.

5. Search for newer version and download update package, or load package.

Select new version and download package. It happens when method is Online update.

a. Click the Select button and the firmware updater will check for updates. After updates checking and analyzing, the available and updatable version(s) are displayed on the Select Version page, as shown in the figure below:



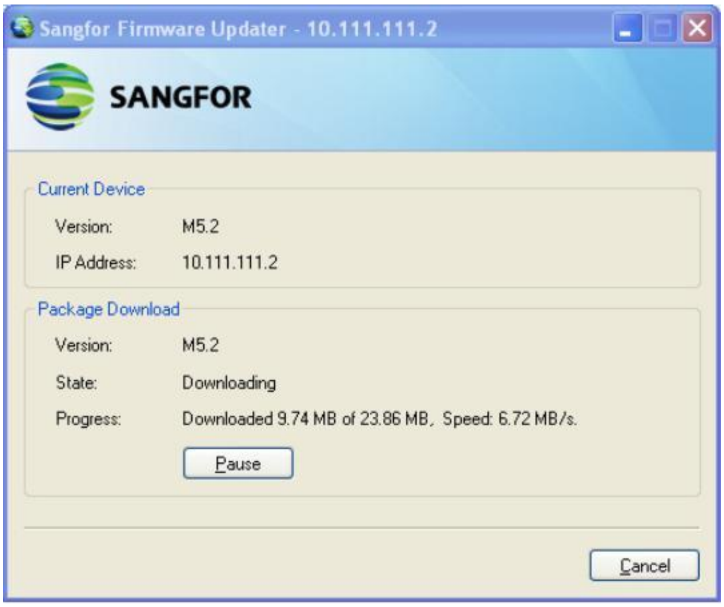
Version	Released	Size	Download...	Updat...	Why Not Allow ...
□ M5.2	2011-11-02	23.86 MB	No	Yes	-

1 newer version(s)

Tips: The current device can be updated to any of the above versions which may not be latest. To update to the latest version, complete this update to any version above and then update again using online update method.

b. Select the checkbox next to a version and click the OK button to close this page.

c. Click the Next button to download package of the selected version. The download process is as shown in the figure below:



Current Device

Version: M5.2

IP Address: 10.111.111.2

Package Download

Version: M5.2

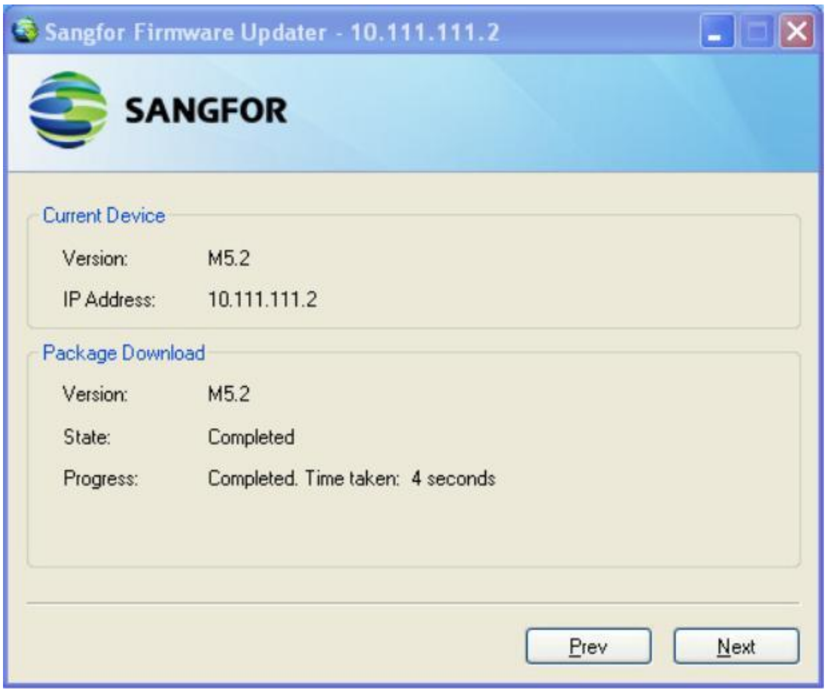
State: Downloading

Progress: Downloaded 9.74 MB of 23.86 MB, Speed: 6.72 MB/s.

To stop downloading the package, click the Pause button which will then turn to a Resume button.

To cancel downloading the package, click the Cancel button.

d. While package download is completed, click the Next button to confirm version information and update the current device, as shown in the figure below:



Current Device

Version: M5.2

IP Address: 10.111.111.2

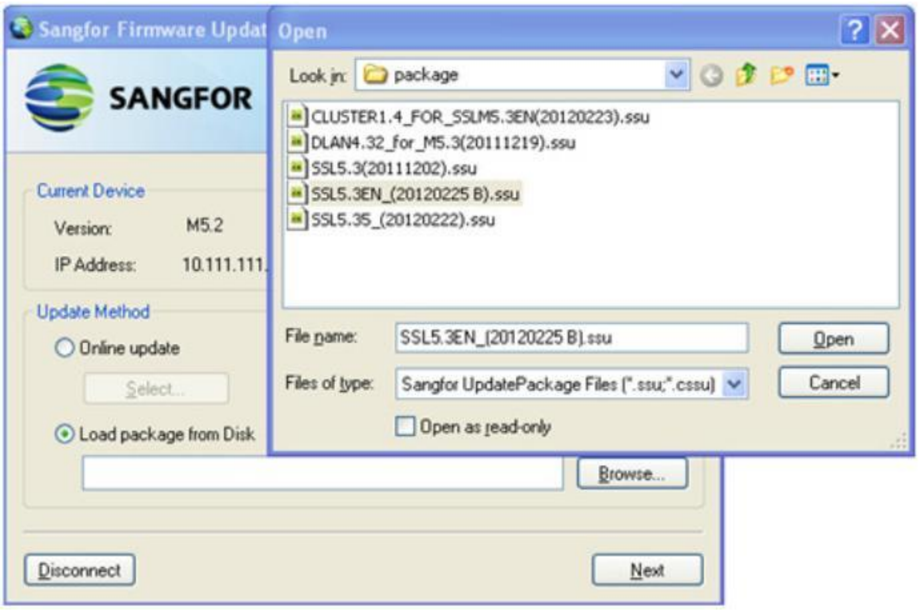
Package Download

Version: M5.2

State: Completed

Progress: Completed. Time taken: 4 seconds

Load update package. It happens when update method is Load package from Disk. Browse a package from local PC, click the Open button and Next button, as shown below:



Current Device

Version: M5.2

IP Address: 10.111.111.

Update Method

○ Online update

● Load package from Disk

Look in: package

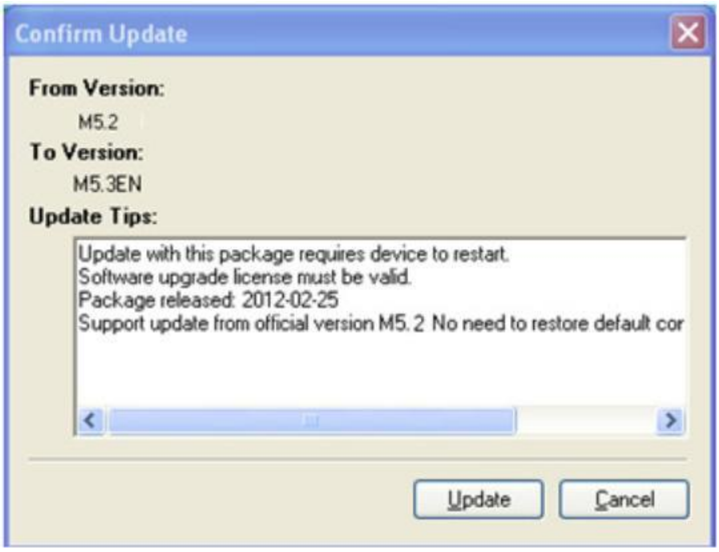
CLUSTER1.4_FOR_SSLM5.3EN(20120223).ssu
DLAN4.32_for_M5.3(20111219).ssu
SSL5.3(20111202).ssu
SSL5.3EN_(20120225 B).ssu
SSL5.35_(20120222).ssu

File name: SSL5.3EN_(20120225 B).ssu

Files of type: Sangfor UpdatePackage Files (*.ssu;*.cssu)

□ Open as read-only

6. Confirm the update information and click the Update button to update the current Sangfor device, as shown in the figure below:



From Version:
M5.2
To Version:
M5.3EN
Update Tips:

Update with this package requires device to restart.
Software upgrade license must be valid.
Package released: 2012-02-25
Support update from official version M5. 2 No need to restore default cor

⚠

Please DO NOT cancel updating during the update process. Otherwise, the current device will meet unexpected error.

Appendix D: Acronyms and Abbreviations

AC	Alternating Current
ARP	Address Resolution Protocol
BM	Bandwidth Management
CA	Certificate Authority
CPU	Central Processing Unit
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DNS	Domain Name Server
DoS	Denial of Service Attack
HQ HTTP	Headquarters Hyper Test Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IM	Instant Message
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MTU	Maximum Transmission Unit
NIC	Network Interface Card
OS	Operating System
RADIUS	Remote Authentication Dial In User Service
SMTP	Simple Message Transfer Protocol
SNAT	Source Network Address Translation
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP UI	User Datagram Protocol User Interface
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WANO	Wide Area Network Optimization
WCCP	Web Cache Communication Protocol