Cisco Small Business Pro
SA 520 Security Appliance with Wireless
SA 520 Security Appliance
SA 540 Security Appliance
235168

ADMINISTRATION GUIDE

Cisco Small Business

SA500 Series Security Appliances

Contents

1

Getting Started

This chapter describes the SA500 and provides scenarios to help you to begin configuring your security appliance to meet the needs of your business.

- **Feature Overview**
- **Installation Options**
- **Hardware Installation**
- **Getting Started with the Configuration Utility**
- **About the Default Settings**
- **Basic Tasks**
- **Common Configuration Scenarios**

Feature Overview

The features of the SA520, SA520W, and the SA540 are compared in the following table.

Table 1 Comparison of SA500 Series Security Appliance Models

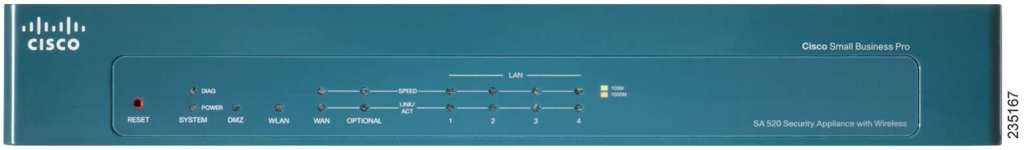
Feature	SA520	SA520W	SA540
Firewall Performance	200 Mbps	200 Mbps	300 Mbps
UTM	200 Mbps	200 Mbps	300 Mbps
VPN Performance	65 Mbps	65 Mbps	85 Mbps
Connections	15,000	15,000	40,000

Feature	SA520	SA520W	SA540
LAN Ports	4	4	8
Wireless (802.11n)	No	Yes	No
IPsec (# seats)	Yes (50)	Yes (50)	Yes (100)
SSL (# seats)	Includes 2 seats. With license, up to 25 seats.	Includes 2 seats. With license, up to 25 seats.	Included (50)

Device Overview

Before you begin to use the security appliance, become familiar with the LEDs on the front panel and the ports on the rear panel. Refer to the following illustrations and descriptions.

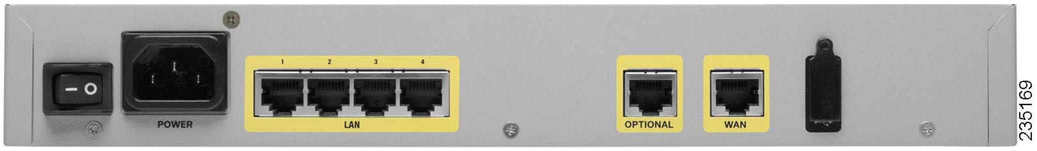
Front Panel



- **RESET Button**—To reboot the security appliance, push and release the Reset button. To restore the factory default settings, press and hold the Reset button for 5 seconds.
- **DIAG LED**—(Orange) When lit, indicates the appliance is performing the power-on diagnostics. When off, indicates the appliance has booted properly.
- **POWER LED**—(Green) When lit, indicates the appliance is powered on.
- **DMZ LED**—(Green) When lit, indicates the Optional port is configured as a Demilitarized Zone or Demarcation Zone, which allows public services such as web servers, without exposing your LAN.
- **SPEED LED**—(Green or Orange) Indicates the traffic rate for the associated port. Off = 10 Mbps, Green = 100 Mbps, Orange = 1000 Mbps.

- **LINK/ACT LED—**(Green) When lit, indicates that a connection is being made through the port. When flashing, the port is active.
- **WLAN LED—**(Green) When lit, indicates that wireless is enabled (SA520W).

Rear Panel



- **POWER Switch—**Turns the security appliance on or off.
- **POWER Connector—**Connects the security appliance to power using the supplied power cable.
- **LAN Ports—**Connect computers and other network appliances to the security appliance. The SA520 and SA520W have 4 LAN ports. The SA540 has 8.
- **OPTIONAL Port—**Can be configured to operate as a WAN, LAN, or DMZ port. A DMZ (Demilitarized Zone or Demarcation Zone) can be configured to allow public access to services such as web servers without exposing your LAN.
- **WAN Port—**Connects the security appliance to DSL, a cable modem, or another WAN connectivity device.
- **USB Port—**Connects the security appliance to a USB device. You can use a USB device to store configuration files for backup and restore operations.

NOTE The back panel of the SA520W includes three threaded connectors for the antennas.

Installation

This section guides you through the installation of your security appliance. Refer to the following topics:

- **Installation Options, page 13**
- **Hardware Installation, page 16**

Installation Options

You can place your security appliance on a desktop, mount it on a wall, or mount it in a rack.

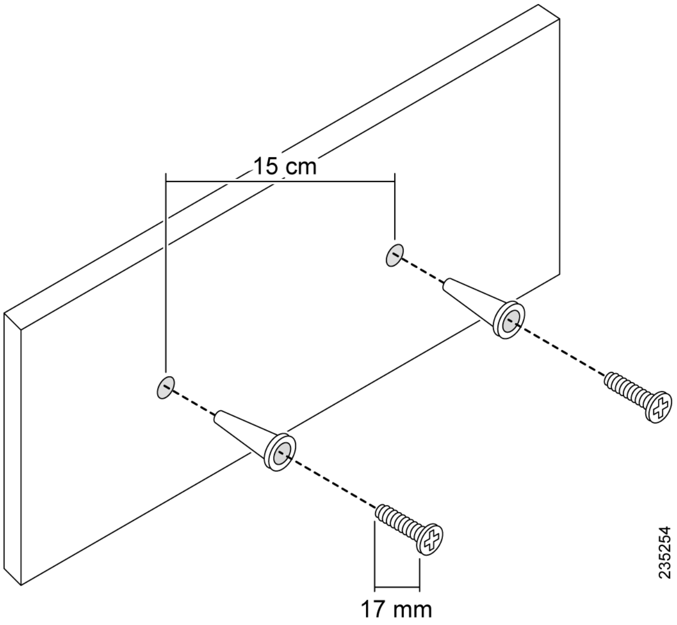
Placement Tips

- **Ambient Temperature—**To prevent the security appliance from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).
- **Air Flow—**Be sure that there is adequate air flow around the device.
- **Mechanical Loading—**Be sure that the security appliance is level and stable to avoid any hazardous conditions.

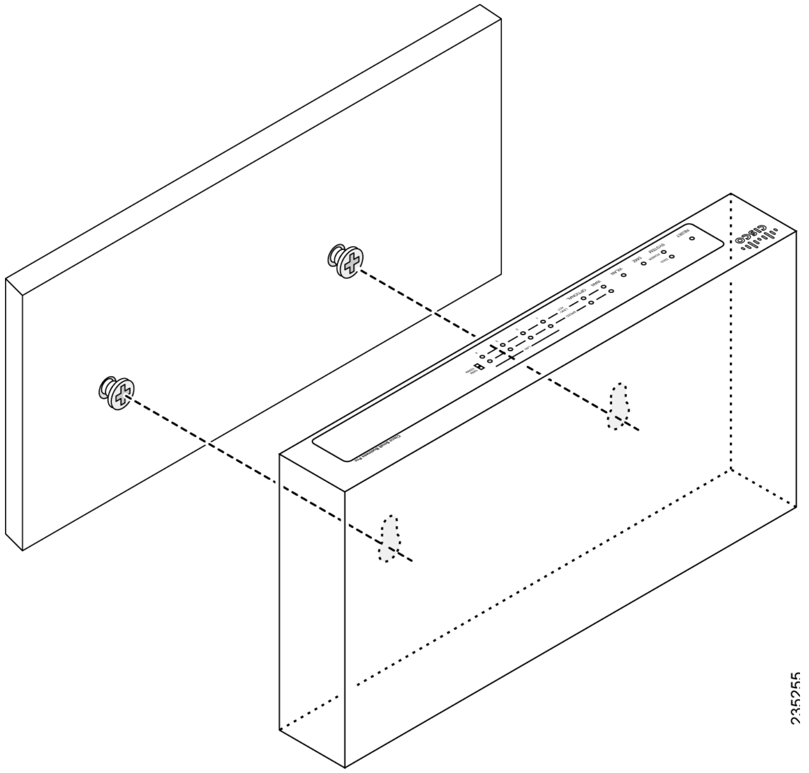
To place the security appliance on a desktop, install the four rubber feet (included) on the bottom of the security appliance. Place the device on a flat surface.

Wall Mounting

STEP 1 Insert two 17 mm screws, with anchors, into the wall 15 cm apart (about 5.9 inches). Leave 3-4 mm (about 1/8 inch) of the head exposed.



STEP 2 Position the unit so that the wall-mount slots are over the two screws. Slide the unit down until the screws fit snugly into the wall-mount slots.



Rack Mounting

You can mount the security appliance in any standard size, 19-inch (about 48 cm) wide rack. Each security appliance requires 1 rack unit (RU) of space, which is 1.75 inches (44.45 mm) high.

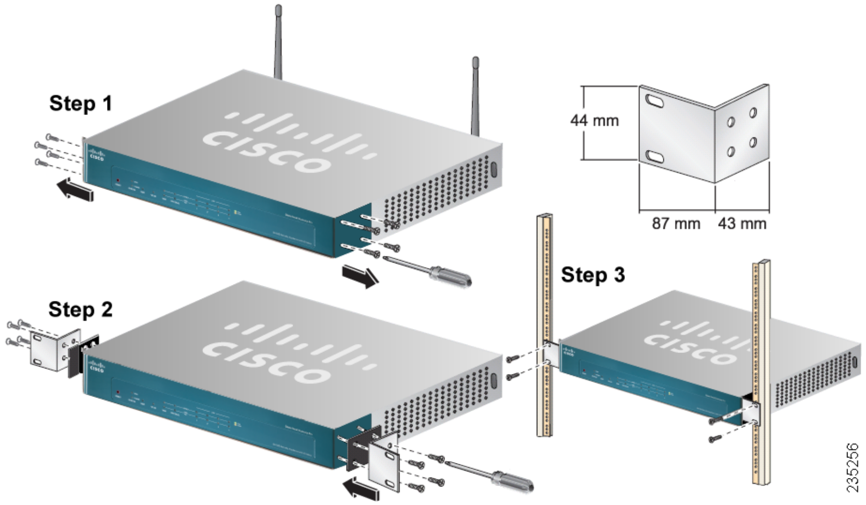
CAUTION Do not overload the power outlet or circuit when installing multiple devices in a rack.

STEP 1 Remove the four screws from each side of the security appliance.

STEP 2 Place one of the supplied spacers on the side of the security appliance so that the four holes align to the screw holes. Place a rack mount bracket next to the spacer and reinstall the screws.

NOTE If the screws are not long enough to reattach the bracket with the spacer, attach the bracket directly to the case without the spacer.

STEP 3 Install the security appliance into a standard rack as shown.



Hardware Installation

Follow these steps to connect the equipment:

STEP 1 Connect the security appliance to power.

STEP 2 If you are installing the SA520W, screw each antenna onto a threaded connector on the back panel. Orient each antenna to point upward.

STEP 3 For DSL, a cable modem, or other WAN connectivity devices, connect an Ethernet network cable from the device to the WAN port on the back panel. Cisco strongly recommends using Cat5E or better cable.

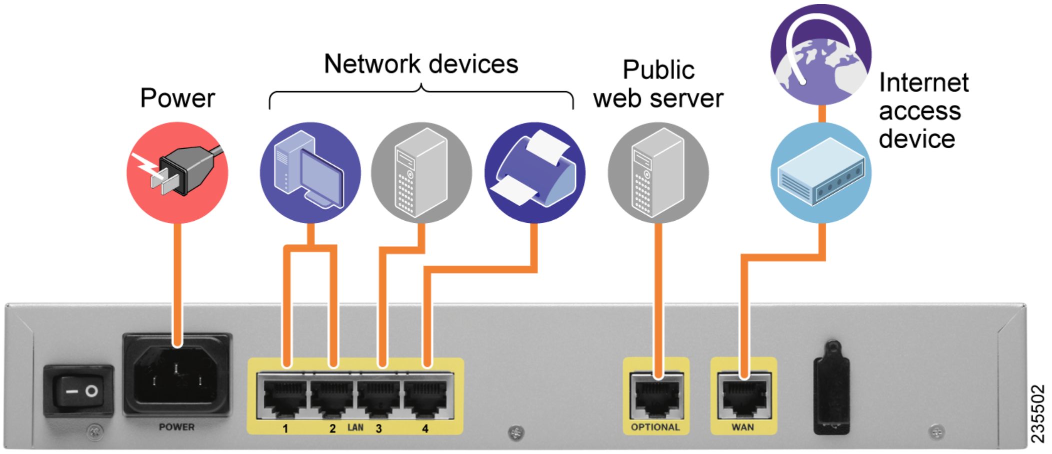
STEP 4 For network devices, connect an Ethernet network cable from the network device to one of the dedicated LAN ports on the back panel.

STEP 5 If you are using a UC500, connect an Ethernet network cable from the WAN port of the UC500 to an available LAN port of the security appliance.

STEP 6 Power on the security appliance.

STEP 7 Power on the connected devices. Each LED lights to show an active connection.

A sample configuration is illustrated below.



Congratulations! The installation of the security appliance is complete.

Getting Started with the Configuration Utility

The Configuration Utility web page is a web based device manager that is used to provision the SA500 Series Security Appliances. To use this utility, you must be able to connect to the SA500 Series Security Appliances from your administration PC or laptop. You can access the security appliance by using any web browser (such as Microsoft Internet Explorer or Mozilla Firefox).

Connecting to the Configuration Utility

STEP 1 Connect your computer to an available LAN port on the back panel of the security appliance.

STEP 2 Start a web browser, and enter the following address: **192.168.75.1**

This address is the factory default LAN address of the security appliance. If you change this setting in the LAN configuration, you will need to enter the new IP address to connect to the Configuration Utility.

STEP 3 When the Security Alert appears, accept or install the certificate:

- **Internet Explorer:** Click **Yes** to proceed, or click **View Certificate** for details. On the Certificate page, click **Install the Certificate**. Follow the instructions in the Wizard to complete the installation.
- **Firefox:** Click the link to add an exception. Click the **Add Exception** button. Click **Get Certificate**, and then click **Confirm Security Exception**.
- **Safari:** Click **Continue** to proceed, or click **Show Certificate**. On the Certificate page, click **Install the Certificate**. Follow the instructions in the Wizard to complete the installation.

STEP 4 Enter the default user name and password:

- Username: **cisco**
- Password: **cisco**

STEP 5 Click **Log In**. The Getting Started (Basic) window opens. For more information, see **Using the Getting Started Pages, page 19**.

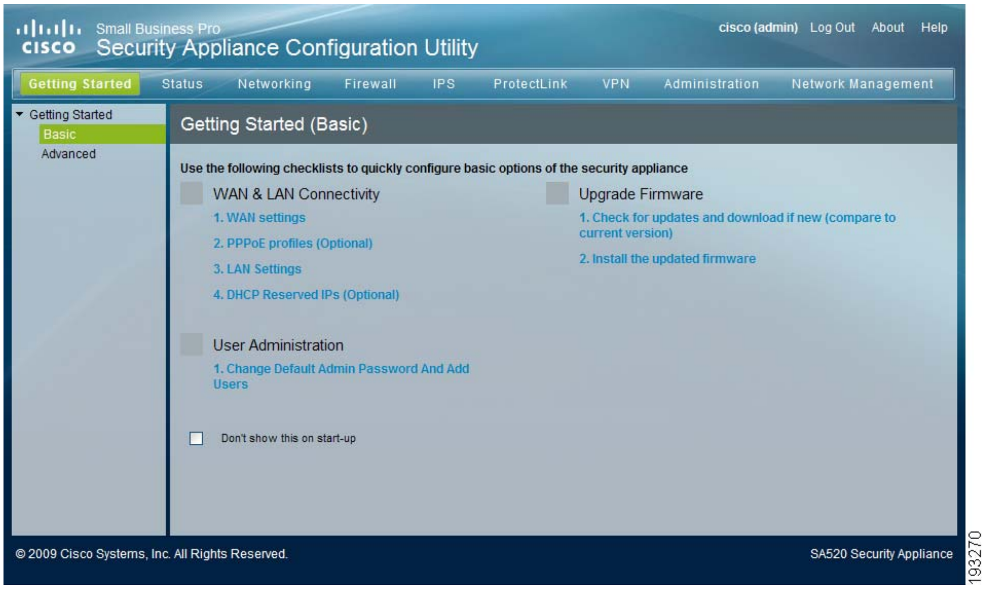
NOTE You can use the Cisco Configuration Assistant (CCA) t to launch the Configuration Utility if you are using the security appliance with a CCA-supported device, such as the UC500. For more information about CCA, see: www.cisco.com/go/configassist.

Using the Getting Started Pages

The Getting Started pages provide help with common configuration tasks.

- Find a task that you need to perform, and then click a link to get started. Proceed in order through the listed links.
- For help with advanced configuration tasks, such as firewall/NAT configuration, optional WAN configuration, DMZ configuration, and VPN setup, click the **Getting Started > Advanced** link in the navigation pane, and click the links to perform the tasks that you want to complete.
- To return to the Getting Started (Basic) page at any time, click the **Getting Started** button in the menu bar.
- To prevent the Getting Started (Basic) page from appearing automatically after you log in, check the **Don't show this on start-up** box.

Getting Started (Basic) Page



Getting Started (Basic)

Use the following checklists to quickly configure basic options of the security appliance

WAN & LAN Connectivity

1. WAN settings
2. PPPoE profiles (Optional)
3. LAN Settings
4. DHCP Reserved IPs (Optional)

Upgrade Firmware

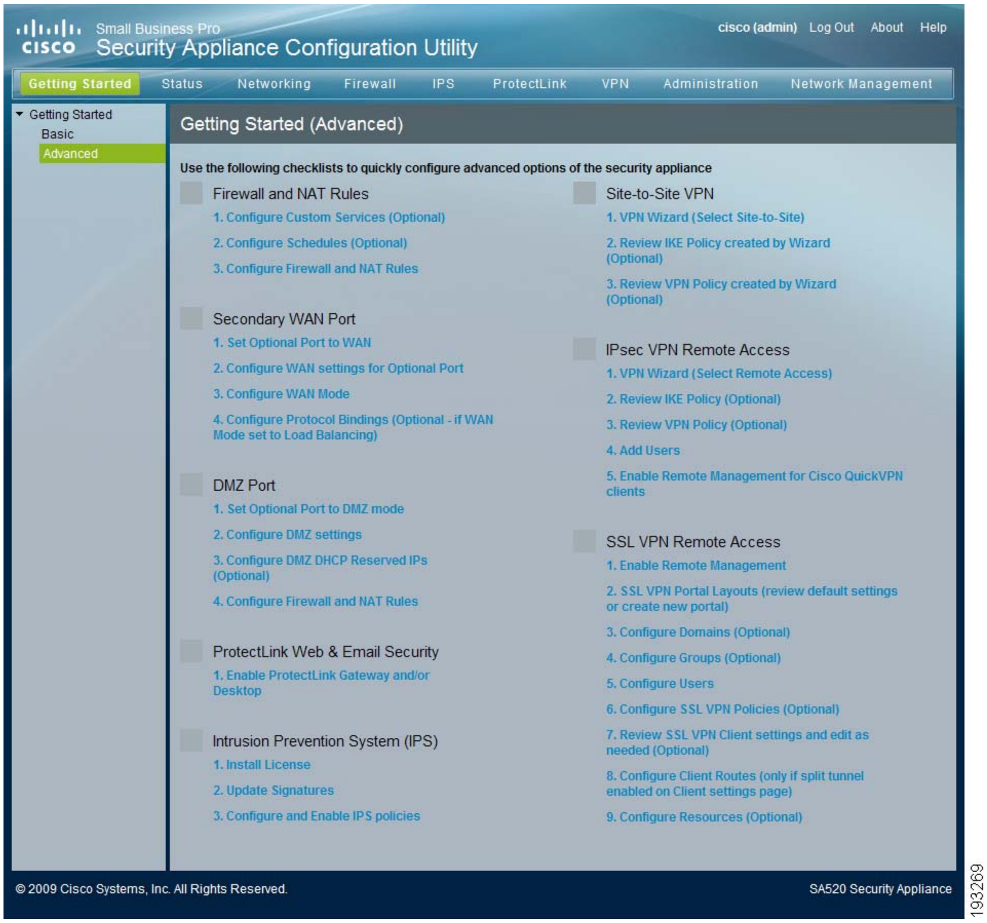
1. Check for updates and download if new (compare to current version)
2. Install the updated firmware

User Administration

1. Change Default Admin Password And Add Users

□ Don't show this on start-up

Getting Started (Advanced) Page


Small Business Pro
Security Appliance Configuration Utility
cisco (admin) Log Out About Help
Getting Started Status Networking Firewall IPS ProtectLink VPN Administration Network Management
Getting Started
Basic
Advanced
193269

Getting Started (Advanced)

Use the following checklists to quickly configure advanced options of the security appliance

Firewall and NAT Rules

1. Configure Custom Services (Optional)
2. Configure Schedules (Optional)
3. Configure Firewall and NAT Rules

Secondary WAN Port

1. Set Optional Port to WAN
2. Configure WAN settings for Optional Port
3. Configure WAN Mode
4. Configure Protocol Bindings (Optional - if WAN Mode set to Load Balancing)

DMZ Port

1. Set Optional Port to DMZ mode
2. Configure DMZ settings
3. Configure DMZ DHCP Reserved IPs (Optional)
4. Configure Firewall and NAT Rules

ProtectLink Web & Email Security

1. Enable ProtectLink Gateway and/or Desktop

Intrusion Prevention System (IPS)

1. Install License
2. Update Signatures
3. Configure and Enable IPS policies

Site-to-Site VPN

1. VPN Wizard (Select Site-to-Site)
2. Review IKE Policy created by Wizard (Optional)
3. Review VPN Policy created by Wizard (Optional)

IPsec VPN Remote Access

1. VPN Wizard (Select Remote Access)
2. Review IKE Policy (Optional)
3. Review VPN Policy (Optional)
4. Add Users
5. Enable Remote Management for Cisco QuickVPN clients

SSL VPN Remote Access

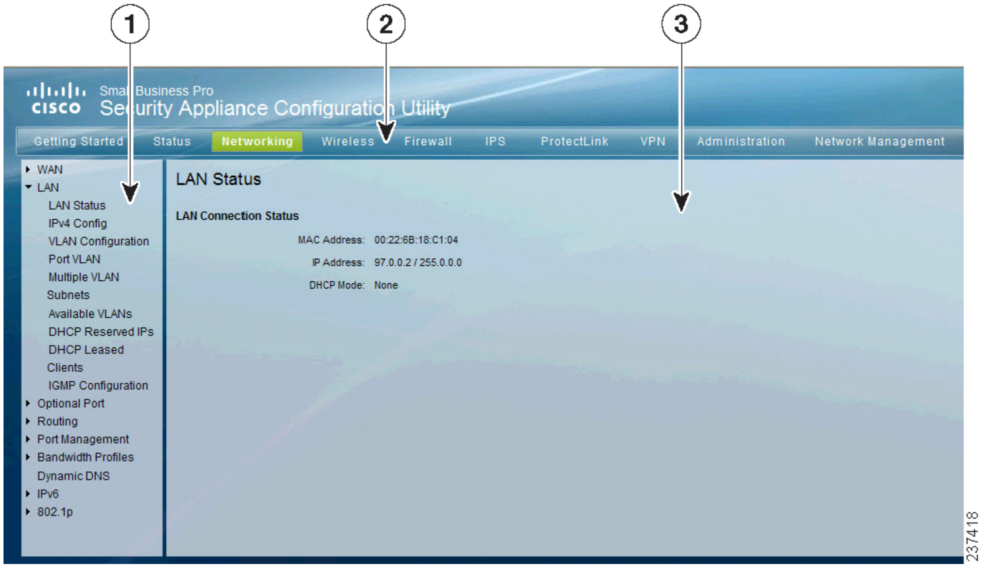
1. Enable Remote Management
2. SSL VPN Portal Layouts (review default settings or create new portal)
3. Configure Domains (Optional)
4. Configure Groups (Optional)
5. Configure Users
6. Configure SSL VPN Policies (Optional)
7. Review SSL VPN Client settings and edit as needed (Optional)
8. Configure Client Routes (only if split tunnel enabled on Client settings page)
9. Configure Resources (Optional)

© 2009 Cisco Systems, Inc. All Rights Reserved. SA520 Security Appliance

Navigating Through the Configuration Utility

Use the menu bar and the navigation pane to perform tasks in the Configuration Utility.

Menu Bar and Navigation Pane



LAN Status

LAN Connection Status

MAC Address: 00:22:6B:18:C1:04

IP Address: 97.0.0.2 / 255.0.0.0

DHCP Mode: None

Number	Component	Description
1	Menu Bar	Contains the major function categories. Click a menu item to change to another category.
2	Navigation Pane	Provides easy navigation through the configurable device features.The main branches expand to provide the subfeatures. Click on the triangle next to the main branch title to expand or contract its contents. Click on the title of a feature or subfeature to open it.
3	Main Content	The main content of the feature appears in this area.

Using the Help System

The Configuration Utility includes detailed Help files for all configuration tasks. To view a Help page, click the **Help** link in the top right corner of the screen. A new window opens with information about the page that you are currently viewing.

About the Default Settings

The SA500 Series Security Appliances are pre-configured with settings that allow you to start using the device with minimal changes needed. Depending on the requirements of your Internet Service Provider (ISP) and the needs of your business, you might need to modify some of these settings. You can use the Configuration Utility to customize all settings, as needed.

Settings of particular interest are described below. For a full list of all factory default settings, see **Appendix D, “Factory Default Settings.”**

- **IPv4 Addressing:** By default, the security appliance is in IPv4 Only mode. If you want to use IPv6 addressing, first enable IPv6 mode and then configure your IPv6 WAN and your IPv6 LAN. See **Configuring IPv6 Addressing, page 77**.

- **WAN Configuration:** By default, the security appliance is configured to obtain an IP address from your ISP by using Dynamic Host Configuration Protocol (DHCP). If your ISP assigned a static IP address, you will need to configure it. In addition, if your ISP requires a login every time that you connect to the Internet, you will need to enter the account information. You can change other WAN settings as well. For more information, see **Scenario 1: Basic Network Configuration with Internet Access, page 26**.

- **LAN Configuration:** By default, the LAN interface acts as a DHCP server for all connected devices. For most deployment scenarios, the default DHCP and TCP/IP settings of the security appliance should be satisfactory. However, you can change the subnet address, or the default IP address of the security appliance. You can assign static IP addresses to connected devices rather than allowing the security appliance to act as a DHCP server. For more information, see **Scenario 1: Basic Network Configuration with Internet Access, page 26**.

- **Optional Port:** This port is preset to act as a secondary WAN port. Alternatively, you can configure the Optional port for use as a DMZ port or an extra LAN port. See **Scenario 1: Basic Network Configuration with**

Internet Access, page 26 or **Scenario 7: DMZ for Public Websites and Services, page 29**.

- **Wireless Network (SA520W only):** The SA520W is configured with an access point named AP1, which has the default network name of Cisco_1. The access point is enabled by default. The security profile has Open security and identifies itself to all wireless devices that are in range. These settings make it easy for you to begin using your wireless network. However, for security purposes, it is strongly recommended that you configure the profile with the appropriate security settings. See **Scenario 10: Wireless Networking, page 35**.
- **Administrative Access:** You can access the Configuration Utility by using a web browser and entering the default IP address of 192.168.75.1. You can log on by entering *cisco* for the username and *cisco* for the password. You are strongly encouraged to change the default username and password. You can also change the default Idle Timeout setting. The default setting requires logging in again after 10 minutes of inactivity. For more information about these settings, see **Changing the Default User Name and Password, page 23**.

Basic Tasks

We strongly recommend that you complete the following basic tasks before you begin configuring your security appliance.

Changing the Default User Name and Password

To prevent unauthorized access, immediately change the user name and password for the default Administrator account.

STEP 1 In the **User Administration** section of the Getting Started (Basic) page, click **Change Default Admin Password And Add Users**.

The Users window opens.

STEP 2 In the first row of the table, find the default Administrator account.

STEP 3 Click the button in the **Edit** column. The User Configuration window opens, displaying the default information.

STEP 4 Enter the following information:

- **User Name:** Enter a unique identifier for the user. It can include any alphanumeric characters.
- **First Name:** Enter the user’s first name.
- **Last Name:** Enter the user’s last name.

  The **User Type** and **Group** cannot be changed for this account.
- **Check to Edit Password:** Check this box to enable the password fields.
- **Enter Your Password:** Enter the current password. The default password for this new security appliance is **cisco**.
- **New Password:** Enter a password that contains alphanumeric, ‘—’ or ‘_’ characters.
- **Confirm Password:** Enter the password again.
- **Idle Timeout:** Enter the time in minutes that the user can be inactive before the login expires. You can enter any value from 0 to 999.

STEP 5 Click **Apply** to save your settings.

Backing Up Your Configuration

At any point during the configuration process, you can back up your configuration. Later, if you make changes that you want to abandon, you easily can easily revert to a saved configuration. For more information, see **Upgrading Firmware and Working with Configuration Files, page 176**.

Upgrading the Firmware

Before you do any other tasks, you should upgrade your firmware to ensure that you are using the latest version. You can upgrade from a file stored on your computer, your network, or a USB key.

STEP 1 In the **Upgrade Firmware** section of the Getting Started (Basic) page, click the link: **Check for updates and download if new**

STEP 2 When the web page opens, download the latest software.

STEP 3 In the **Upgrade Firmware** section of the Getting Started (Basic) page, click the **Install the updated firmware** link.

The Firmware & Configuration (Network) window opens.

STEP 4 In the **Firmware Upgrade** area, click **Browse**. Find the file that you downloaded.

STEP 5 Click **Upload**.

NOTE Wait while the firmware is upgraded.
1. Do NOT close the browser window.
2. Do NOT go online.
3. Do NOT turn off or power-cycle the router.
4. Do NOT shutdown the computer.

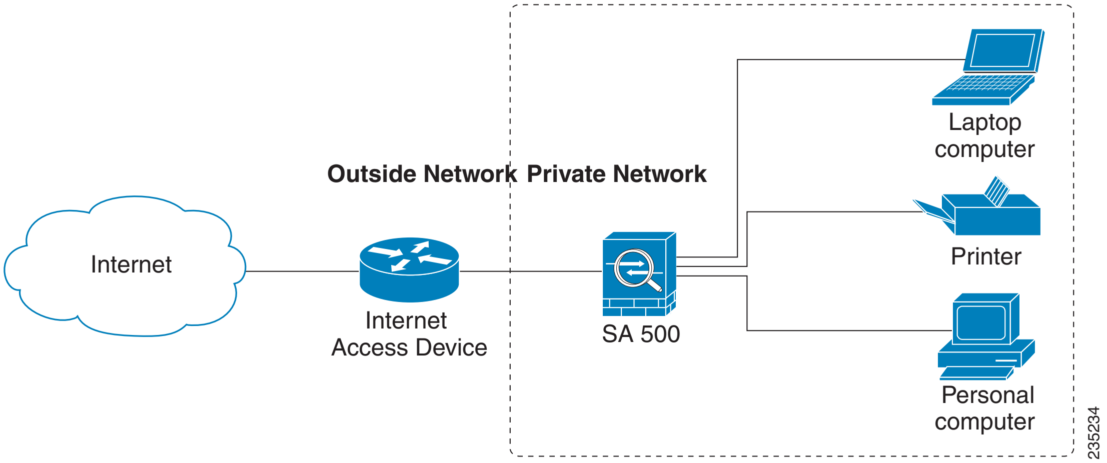
The router will take several minutes to complete the upgrade. While the upgrade is in progress, the Test LED on the front panel of the router is lit. When the upgrade is complete, the router automatically restarts.

Common Configuration Scenarios

The SA500 Series Security Appliances can be deployed to address the security concerns of your business. As you get started using your security appliance, consider the following configuration scenarios:

- **Scenario 1: Basic Network Configuration with Internet Access, page 26**
- **Scenario 8: Cisco Smart Business Communications System Configuration, page 28**
- **Scenario 7: DMZ for Public Websites and Services, page 29**
- **Scenario 6: Firewall for Controlling Inbound and Outbound Traffic, page 29**
- **Scenario 9: Site-to-Site Networking and Remote Access, page 31**
- **Scenario 10: Wireless Networking, page 35**

Scenario 1: Basic Network Configuration with Internet Access



In a basic deployment for a small business, the security appliance enables communication between the devices on the private network and also allows computers to access the Internet. With the default settings, the security appliance gets its WAN address dynamically from the ISP. All devices on the LAN receive their IP addresses dynamically from the security appliance. All devices have access to the Internet, but no inbound traffic is allowed from the Internet to any LAN devices.

Configuration tasks for this scenario:

The default configuration is sufficient for many small businesses, and you might not need to change any of the WAN or LAN settings. However, depending on the requirements of your ISP, as well your preferences for your LAN configuration, you can make changes, as needed.

NOTE Before you configure your network, make sure that you have upgraded the firmware (see **Upgrading the Firmware, page 24**) and changed the default Administrator password (see **Changing the Default User Name and Password, page 23**).

Consider the following first steps:

1. Review the WAN configuration and make any changes that are needed to set up your Internet connection.

   In the **WAN & LAN Connectivity** section of the Getting Started (Basic) page, click the **WAN settings** link. For more information, see **Configuring the WAN Connection, page 37**.

2. Review the LAN configuration and make any changes that are needed to support your network. The default DHCP and TCP/IP settings should be satisfactory in most cases. However, you can change the subnet address or the default IP address, or assign static IP addresses to your devices.

   In the **WAN & LAN Connectivity** section of the Getting Started (Basic) page, click the **LAN Settings** link. For more information, see **Configuring the LAN, page 43**.

3. If you are going to use your security appliance with your Cisco Smart Business Communications System (SBCS), install and configure your UC500.

   See **Scenario 8: Cisco Smart Business Communications System Configuration, page 28**.

4. Consider how you want to use the Optional port:

   - If you need to host public services such as websites, you will need a DMZ. For more information, see **Scenario 7: DMZ for Public Websites and Services, page 29**. For information about using the optional port as an extra LAN port, see **Configuring the Optional Port as a LAN Port, page 53**.

   - If you have two ISP links and do not need a DMZ, you can use the Optional port as a secondary WAN port to provide backup connectivity or load balancing. To configure the port, use the links in the **Secondary WAN Port** section of the Getting Started (Advanced) page. For more information, see **Configuring the Optional WAN, page 54**.

   - If you do not need a DMZ or a secondary WAN, you can use the Optional port as an extra LAN port. For more information, see **Configuring the Optional Port as a LAN Port, page 53**.

5. If you want to allow inbound access from the Internet, or if you want to restrict some types of outbound traffic to the Internet, configure your firewall rules.

   See **Scenario 6: Firewall for Controlling Inbound and Outbound Traffic, page 29**.

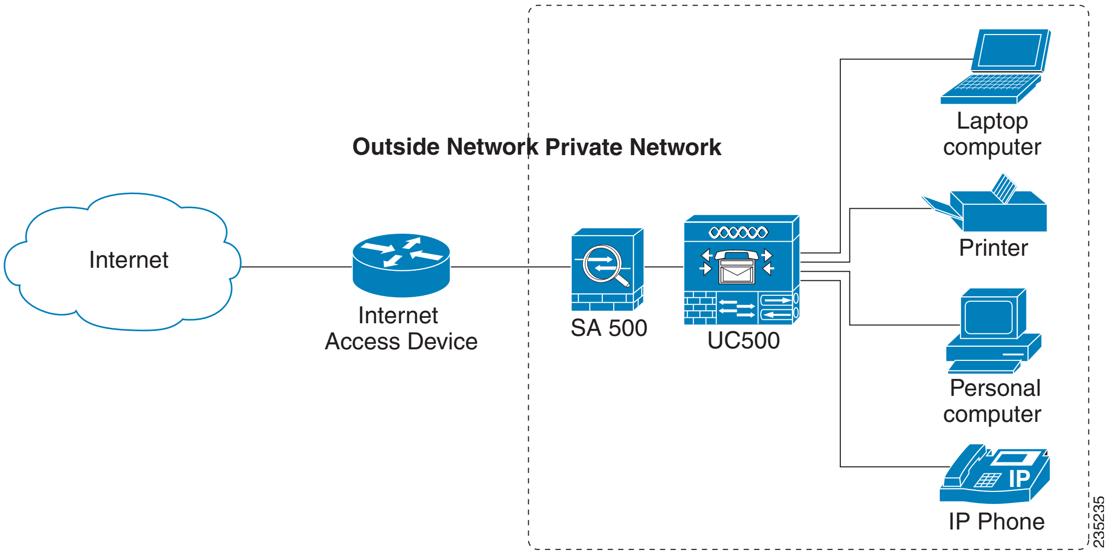
6. Consider whether you need to allow access to your network from remote sites or remote workers.

   See **Scenario 9: Site-to-Site Networking and Remote Access, page 31**.

7. Consider whether you need to enable features such as logging or remote access to the configuration utility. See **Configuring the Logging Options, page 185** and **RMON (Remote Management), page 197**.

Scenario 8: Cisco Smart Business Communications System Configuration

You can use the security appliance to protect your Cisco Smart Business Communications System network.



Configuration tasks for this scenario:

1. Configure the WAN and LAN settings for your security appliance, as needed. See **Scenario 1: Basic Network Configuration with Internet Access, page 26**.
2. Connect a cable from the WAN port of the UC500 to an available LAN port of the security appliance.

   With the default configuration, the security appliance acts as a DCHP server that assigns IP addresses in the range of 192.168.75.x. IP Phones are assigned IP addresses in the address range 10.1.1.x/24.
3. If you want to assign a static IP address to the UC500 or other LAN devices, click the **DHCP Reserved IPs** link under **WAN & LAN Connectivity** on the Getting Started (Basic) page. For more information, see **DHCP Reserved IPs, page 52**.
4. Configure a static IP route from the security appliance to the UC 500 data VLANs (192.168.10.x). For more information, see **Static Routing, page 68**.
5. Because the security appliance will provide the firewall, Network Address Translation (NAT), and SIP Application Layer Gateway (SIP-ALG) for your network, disable those functions on the UC500. For instructions, refer to the documentation or online Help for the Cisco Configuration Assistant (CCA).

Scenario 6: Firewall for Controlling Inbound and Outbound Traffic

By default, all outbound traffic is allowed and all inbound traffic is denied. If you want to deny some outbound traffic or allow some inbound traffic, you will need to configure a firewall rule. To prevent unwanted traffic from the Internet, and to ensure that your employees are using the Internet for approved business purposes, you can configure various levels of firewall rules. You can configure rules that apply to a specified IP address, a range of IP addresses, or to everyone globally.

Consider the following examples of firewall rules:

- Block outbound traffic to certain websites
- Restrict Internet access for certain users
- Allow inbound traffic to your DMZ
- Configure advanced NAT routing

For these scenarios and all situations in which you need an exception from the default firewall policy, you need to configure firewall rules.

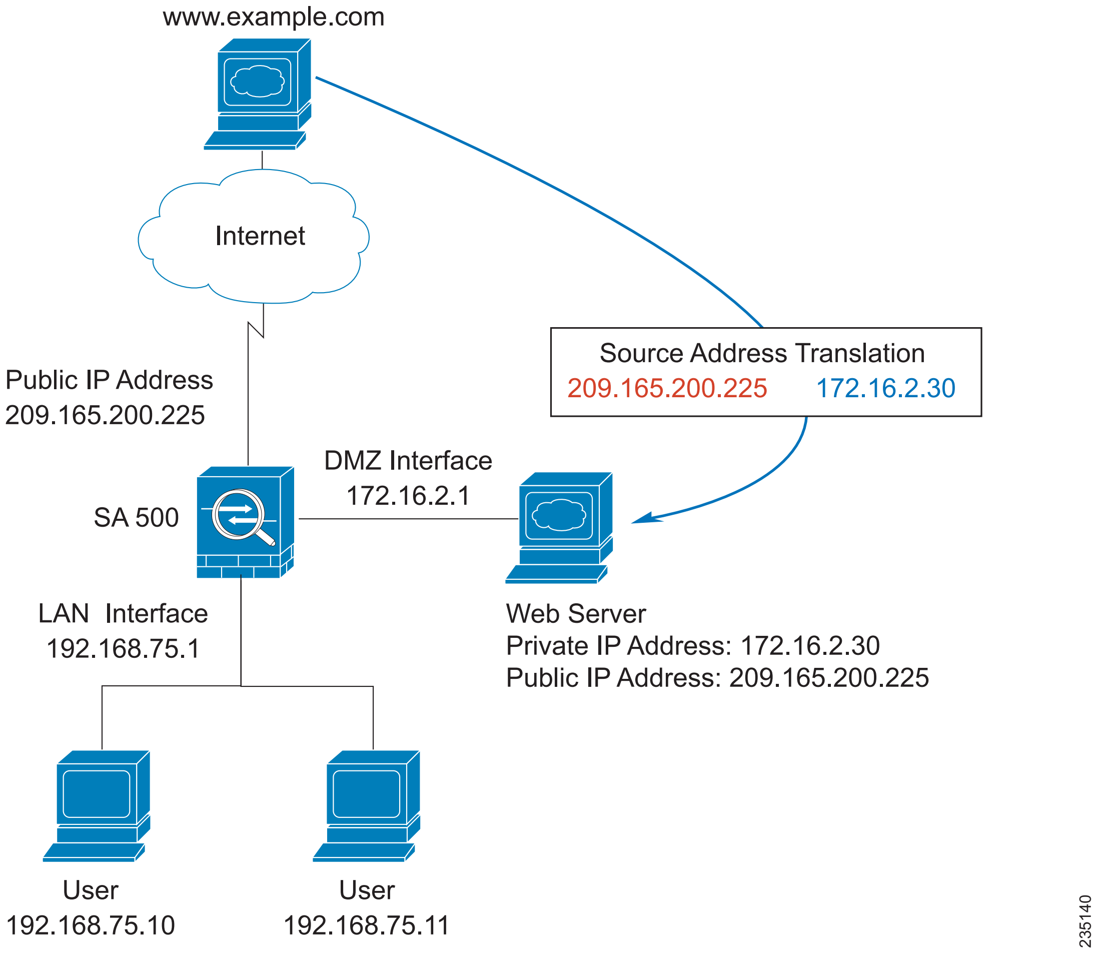
NOTE The default WAN and LAN settings might be sufficient for your deployment, but consider the steps outlined in **Scenario 1: Basic Network Configuration with Internet Access, page 26**.

Configuration tasks for this scenario:

To start configuring your firewall rules, use the **Firewall and NAT Rules** links on the Getting Started (Advanced) page. For more information, see **Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 103**.

Scenario 7: DMZ for Public Websites and Services

If your business hosts public services such as websites, you need a way to allow access to those services without exposing your LAN. You can address this concern by configuring the Optional port of the security appliance for use as a DMZ (Demarcation Zone or Demilitarized Zone). This zone acts as a separate network between your private LAN and the Internet. After you configure your DMZ, you can configure the firewall rules that enable traffic to connect only to the services that you specify.



NOTE The default WAN and LAN settings might be sufficient for your deployment, but consider the steps outlined in **Scenario 1: Basic Network Configuration with Internet Access, page 26**.

Configuration tasks for this scenario:

To start configuring a DMZ, use the links in the **DMZ Port** section of the Getting Started (Advanced) page. For more information, see **Configuring a DMZ, page 61**.

Scenario 8: Configuring ProtectLink Web & Email Security

For added protection against web and email threats, the security appliance supports Cisco ProtectLink Security services. By using these services, your network is protected from email threats in the Internet “cloud” and web threats in the Cisco security appliance, providing access only to email and websites that are appropriate for your business.

Configuration tasks for this scenario:

In the **ProtectLink Web & Email Security** section of the Getting Started (Advanced) page, click **Enable ProtectLink Gateway and/or Endpoint**. The Protect Link window opens. For more information, see **Chapter 6, “Using Cisco ProtectLink Security Services.”**

Scenario 9: Site-to-Site Networking and Remote Access

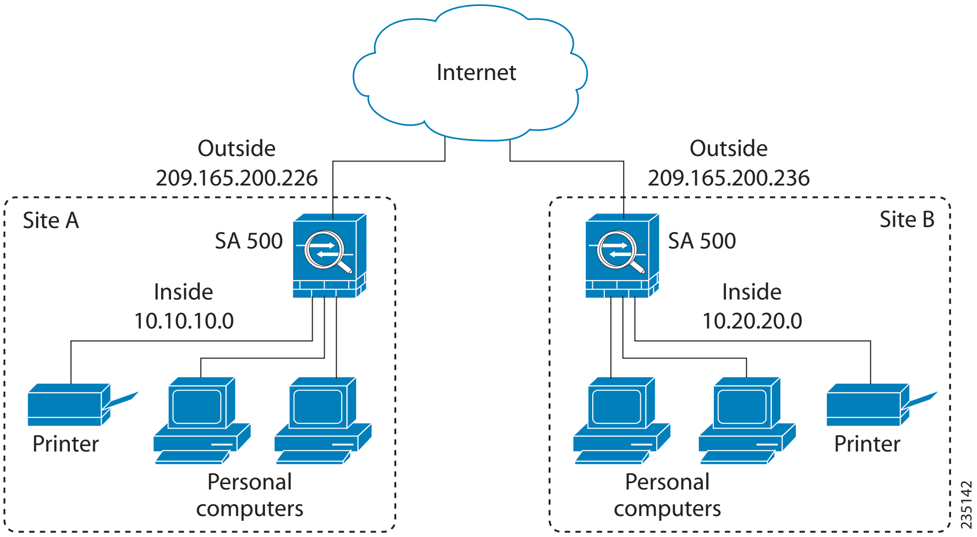
You can configure a Virtual Private Network (VPN) to extend your network to other sites or to allow business partners and teleworkers to access applications and network resources.

You can configure the following types of VPNs:

- IPsec VPN for a Site-to-Site Tunnel
- IPsec VPN for Remote Access with a VPN Client
- SSL VPN for Remote Access with a Web Browser

IPsec VPN for Site-to-Site VPN

For site-to-site VPN, you can configure an IPsec tunnel with advanced encryption to maintain network security.

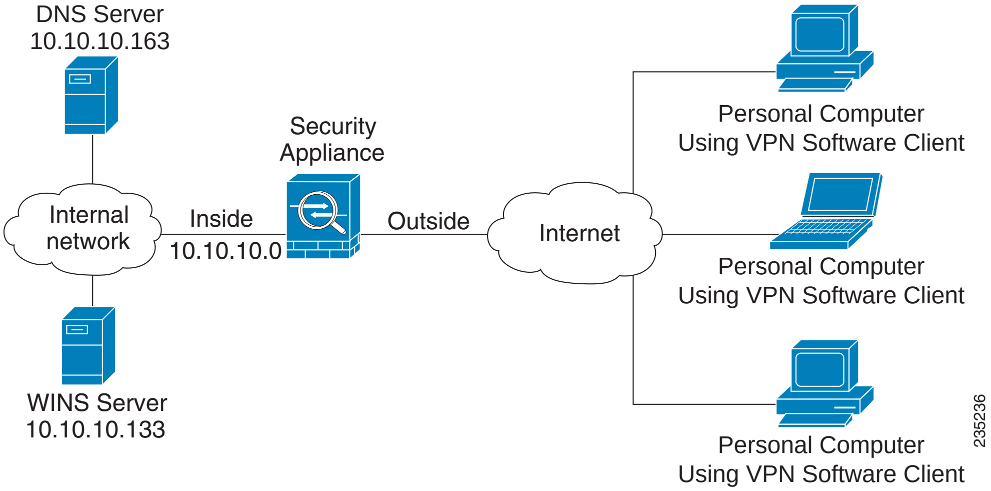


Configuration tasks for this scenario:

In the **Site-to-Site VPN** section of the Getting Started (Advanced) page, click the **VPN Wizard** link. When the VPN Wizard appears, choose the **Site-to-Site** option and enter the other settings. Optionally, you can use other links on the Getting Started (Advanced) page to review and modify the policies that were created by the Wizard. For more information, see **Configuring an IPsec VPN Tunnel for Remote Access with a VPN Client, page 139**.

IPsec VPN Remote Access with a VPN Client

For remote access by users who have an IPsec VPN client on the PC, you can configure an IPsec VPN client tunnel for secure access. This option requires installing and maintaining the VPN client software for these remote sites and users.

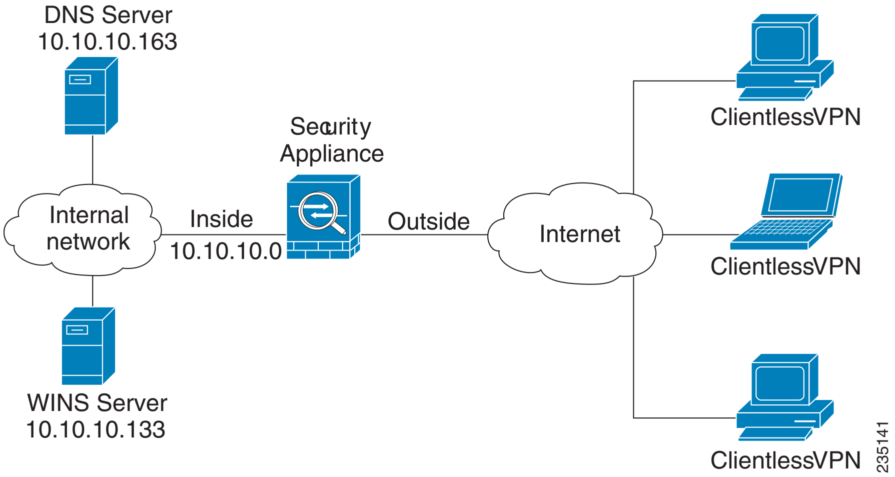


Configuration tasks for this scenario:

In the **IPsec VPN Remote Access** section of the Getting Started (Advanced) page, click the **VPN Wizard** link. When the VPN Wizard appears, choose the **Remote Access** option and complete the fields on the page. Return to the Getting Started (Advanced) page and click **Add Users** to add your VPN users. Optionally, you can use other links on the Getting Started (Advanced) page to review and modify the policies that were created by the Wizard. For more information, see **Configuring an IPsec VPN Tunnel for Remote Access with a VPN Client, page 139**.

SSL VPN Remote Access With a Web Browser

For remote access by users who have no special software on the PC, such as contractors who need access to some or all of your network resources, SSL VPN is a flexible and secure way to extend your network resources. You are not responsible for any VPN client software, since the VPN tunnel can be accessed by anyone with a web browser, Internet access, and the correct login credentials.

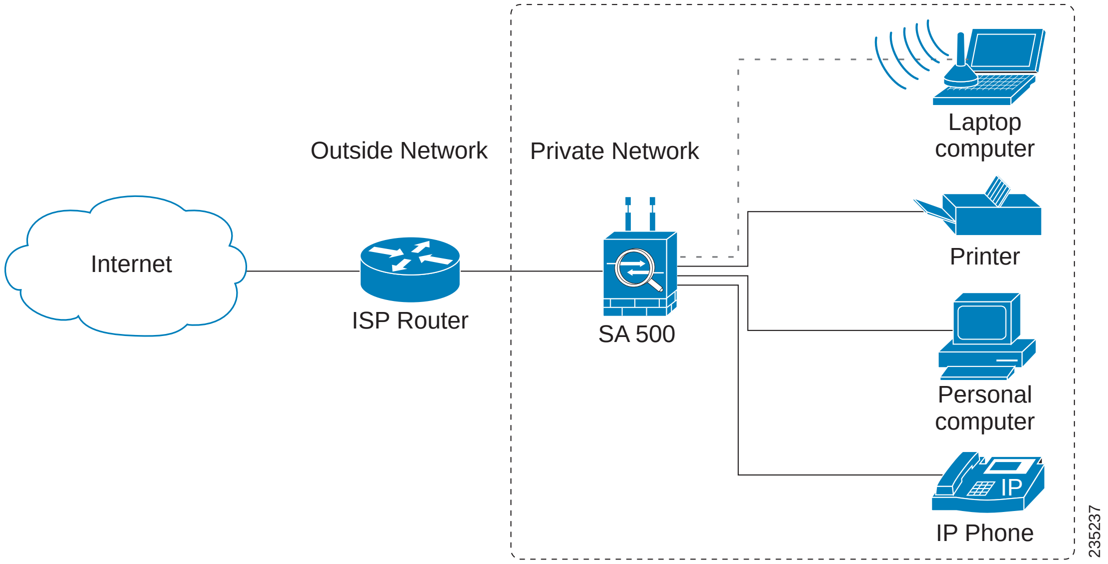


Configuration tasks for this scenario:

In the **SSL VPN Remote Access** section of the Getting Started (Advanced) page, click the **SSL VPN Portal Layouts** link to review the default settings for the user portal. Create new portals for different user groups, if needed. Return to the Getting Started (Advanced) page and click the **Configure Users** link to add your VPN users. Optionally, you can use other links to configure the policies, client settings, routes, and resources for your SSL VPN. For more information, see **Configuring SSL VPN for Browser-Based Remote Access, page 154**.

Scenario 10: Wireless Networking

With the SA520W, you can configure your wireless network to meet the demands of your physical environment and to control access to your network resources.



Configuration tasks for this scenario:

1. The default WAN and LAN settings might be sufficient for your deployment, but consider the steps outlined for **Scenario 1: Basic Network Configuration with Internet Access, page 26**.
2. Although you can begin using your wireless network right away, you should configure the security settings to protect your network and the data that you transmit. To configure your wireless network, see **Chapter 3, "Wireless Configuration for the SA520W."**

2

Networking

This chapter describes how to configure the Networking features for your router. It includes the following sections:

- **Configuring the WAN Connection**
- **Configuring the LAN**
- **Configuring the Optional WAN**
- **Configuring a DMZ**
- **VLAN Configuration**
- **Routing**
- **Port Management**
- **QoS Bandwidth Profiles**
- **Dynamic DNS**
- **Configuring IPv6 Addressing**

To access the Networking pages click ***Networking*** from the Configuration Utility menu bar.

Configuring the WAN Connection

By default, your security appliance is configured to receive a public IP address from your ISP automatically through DHCP. Depending on the requirements of your ISP, you may need to modify these settings to ensure Internet connectivity. For example, your ISP may have assigned a static IP address or may require a login.

NOTE To configure IPv6 addressing, see **Configuring IPv6 Addressing, page 77**.

Use the account information provided by your ISP to complete the fields in this section.

STEP 1 Click **Networking** > **WAN > IPv4 Config**, or from the Getting Started (Basic) page, under **WAN & LAN Connectivity**, click **WAN settings**.

The IPv4 WAN Configuration window opens.

If a login is required, continue to **Step 2** to complete the fields under ISP Connection Type. If not, check, continue to **Step 5**

STEP 2 If your Internet connection requires a login, complete these fields under **ISP Connection Type**:

- **ISP Connection Type:** Choose the connection type, as specified by your service provider (PPTP, PPPoE, or L2TP), and complete the required fields.
- **PPPoE Profile Name:** Choose a PPPoE profile. To manage the profiles in the drop-down list, see **Creating PPPoE Profiles, page 40**.
- **User Name:** Enter user name required to log in
- **Password:** Enter the password required to log in
- **Secret (Optional):** Enter the secret phrase to log into the server (if applicable).
- **Connectivity Type:** Choose one of the following options:
    - **Keep Connected:** The connection is always on, regardless of the level of activity. Choose this option if you pay a flat fee for your Internet service.
    - **Idle Time:** The security appliance disconnects from the Internet after a specified period of inactivity (Idle Time). Choose this option if your ISP fees are based on the time that you spend online. If you select option, also enter the Idle Time in minutes

- **My IP Address:** Enter the IP address assigned to you by the ISP.
- **Server IP Address:** Enter the IP address of the PPTP, PPPoE, or other server.

STEP 3 Enable VLAN Tagging (Applies to PPPoE configurations only).

- **Enable VLAN Tagging**: Check this box to enable a connection on a VLAN tagged WAN interlace.
- **VLAN ID**: Specify the VLAN ID.

STEP 4 Reset the PPPoE/L2TP/PPTP connection by schedule. Choose one of the following options:

- **Never**: Disables Reset Connection by Schedule.
- **Daily**: Resets the connection daily.
- **Weekly**: Resets the connection weekly on a specific day. If you choose this option, enter the **Day** and **Time** you want to restart the WAN connection.

STEP 5 If your ISP does not require a login, enter the following information under **Internet (IP) Address** and **Dynamic Name System (DNS) Servers**:

- **IP Address Source:** Your ISP assigns you an IP address that is either dynamic (newly generated each time you log in) or static (permanent).
  - **Get Dynamically from ISP**: Choose this option if your ISP has not assigned an IP address to you.
  - **Use Static IP Address**: Choose this option if your ISP has assigned an IP address to you. Also enter the **IP Address**, **IP Subnet Mask**, and the **Gateway IP Address** that were provided by your ISP.
- **DNS Server Source:** DNS servers map Internet domain names (example: www.cisco.com) to IP addresses. You can get DNS server addresses automatically from your ISP or use ISP-specified addresses.
  - **Get Dynamically from ISP**: Choose this option if you have not been assigned a static DNS IP address.
  - **Use These DNS Servers.**: Choose this option if your ISP assigned a static DNS IP address. Also enter the addresses for the **Primary DNS Server** and the **Secondary DNS Server**.

STEP 6 If required by your ISP, configure the following settings in the **MTU Size** area:

- **MTU Type:** The Maximum Transmission Unit is the size, in bytes, of the largest packet that can be passed on. Choose **Default** to use the default MTU size, 1500 bytes. Choose **Custom** if you want to specify another size.

- **MTU Size:** If you chose **Customer** for the MTU Type, enter the custom MTU size in bytes.

The MTU (Maximum Transmit Unit) is the size of the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes. For PPPoE connections, it is 1492 Bytes. Unless a change is required by your ISP, it is recommended that the MTU values be left as is.

STEP 7 Click **Apply** to save your settings.

NOTE Next steps:

- If you are using the Getting Started (Basic) page, click **Getting Started** in the menu bar, and then continue with the list of configuration tasks.
- To check the WAN status, click **WAN > WAN Status**. For more information, see **Viewing the WAN Status, page 39**.
- If you need to create PPPoE profiles, click **WAN > PPPoE Profiles**. For more information, see **Creating PPPoE Profiles, page 40**.
- If you need to configure another ISP link, click **Optional Port > Optional Port Mode** and choose **WAN** for the port mode. After saving your settings on that page, click **Optional Port > WAN** to configure the WAN connection. For more information, see **Configuring the Optional WAN, page 54**.
- If you are having problems with your WAN connection, see the **Internet Connection, page 217** in **Appendix A, “Troubleshooting.”**

Viewing the WAN Status

You can check the WAN status, renew the connection, or release the connection.

STEP 1 Click **Networking** >**WAN > WAN Status**.

The WAN Status window opens. This page displays the following types of information about the dedicated WAN and the optional WAN (if applicable):

- Connection Time
- Connection Type: Dynamic IP (DHCP) or Static IP
- Connection State: Connected or Disconnected
- Link State: Up or Down

- WAN state: Up or Down
- DHCP Server
- Lease Obtained
- Lease Duration
- IP Address
- Subnet Mask
- Gateway
- DNS Server
- Secondary DNS
- MAC Address

STEP 2 If the WAN is configured using DHCP, you can use buttons on the WAN Status page to renew or release the connection.

- Click **Renew** to renew the connection.
- Click **Release** to release the connection.
- If the WAN is configured with a Static IP address, click **Disable** to disable the connection.

NOTE If you are having problems with your WAN connection, see the **Internet Connection, page 217** in **Appendix A, "Troubleshooting."**

Creating PPPoE Profiles

If you have multiple PPPoE accounts, you can use this page to maintain the information. You can then associate a profile with the WAN interface as part of the WAN configuration.

STEP 1 Click **Networking** > **WAN > PPPoE Profiles**, or from the Getting Started (Basic) page, under **WAN & LAN Connectivity**, click **PPPoE profiles**.

The PPPoE profiles window opens.

STEP 2 Click **Add** to create a new profile.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the PPPoE Profile Configuration window opens.

STEP 3 Enter the following information:

- **Profile Name:** Enter a name for the profile.
- **User Name:** Enter the user name that is required to login to the ISP account.
- **Password:** Enter the password that is required to login to the ISP account.
- **Authentication Type:** Choose the authentication type, as specified by your ISP.
- **Connectivity Type:** Choose one of the following options:
  - **Keep Connected:** The connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service.
  - **Idle:** The security appliance disconnects from the Internet after a specified period of inactivity (Idle Time). If you choose this option, also enter the Idle Time in minutes. This choice is recommended if your ISP fees are based on the time that you spend online.

STEP 4 Click **Apply** to save your settings.

Configuring an IP Alias

A single WAN Ethernet port can be accessed through multiple IP addresses by adding an IP alias to the port.

STEP 1 Click **Networking** > **WAN > IP Alias**.

The IP Aliases window opens.

Any currently configured WAN IP aliases used by the WAN port appear in the List of IP Aliases table.

STEP 2 Click **Add** to add a new alias.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the IP Aliases window opens.

STEP 3 Enter the following information:

- Interface Name: Choose an interface name on which the alias is created.
- IP Address: The IP address alias added to this WAN port of the router.
- Mask: The IPv4 subnet mask.

STEP 4 Click **Apply** to save your changes.

The new alias appears in the List of IP Aliases table.

Configuring the LAN

For most applications, the default DHCP and TCP/IP settings of the security appliance are satisfactory. However, you can use the LAN Configuration page to change these and other settings.

- **About the Default LAN Settings**
- **Configuring the LAN**
- **Viewing the LAN Status**
- **VLAN Configuration**
- **DHCP Reserved IPs**
- **DHCP Leased Clients**
- **Configuring an IGMP Proxy**
- **Configuring the Optional Port as a LAN Port**

About the Default LAN Settings

- By default the LAN of the router is configured in the 1**92.168.75.0** subnet and the LAN IP address of the router is **192.168.75.1**.
- By default, the security appliance acts as a Dynamic Host Configuration Protocol (DHCP) server to the hosts on the WLAN or LAN network. It can automatically assign IP addresses and DNS server addresses to the PCs and other devices on the LAN. With DHCP enabled, the IP address of the security appliance is the gateway address to your LAN. If you want another PC on your network to be the DHCP server or if you are manually configuring the network settings of all of your PCs, disable DHCP and enter the appropriate settings.
- Instead of using a DNS server, you can use a Windows Internet Naming Service (WINS) server. A WINS server is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. The security appliance includes the WINS server IP address in the DHCP configuration when acknowledging a DHCP request from a DHCP client.
- By default, your LAN is configured for IPv4 addressing. If you need to enable IPv6 addressing, see **Configuring IPv6 Addressing, page 77** and **Configuring the IPv6 LAN, page 80**.

Configuring the LAN

STEP 1 Click **Networking** > **LAN > IPv4 Config**, or from the Getting Started (Basic) page, under **WAN & LAN Connectivity**, click **LAN Settings**.

The IPv4 LAN Configuration window opens.

STEP 2 In the **LAN TCP/IP Setup** area, enter this information for your security appliance:

- **IP address:** Enter the LAN IP address for the security appliance.

  NOTE If you change the IP address in this field and click **Apply**, the security appliance will no longer be at the IP address that you entered in your web browser to launch the Configuration Utility, and your computer will not longer be on the same subnet as the security appliance (having received an IP address through DHCP based on the former address).

  After you click **Apply**, wait a few seconds to allow your computer to obtain a new IP address from newly assigned IP address pool (or unplug and re-insert the Ethernet cable to release and renew your IP address). Then enter the new IP address of the security appliance in the Address bar of the browser, and log in again.

- **Subnet mask:** Enter the subnet mask for this IP address.

STEP 3 In the **DHCP** area, configure these settings:

- **DHCP Mode:** Choose one of the following modes:
  - **None:** Choose this option if the computers on the LAN are configured with static IP addresses or are configured to use another DHCP server.
  - **DHCP Server:** Choose this option to allow the security appliance to act as a DCHP server and to assign IP addresses within the specified range. Also complete the fields that are highlighted with white backgrounds.

    If you want to reserve certain IPs for particular devices, complete this procedure and then configure the reserved IP addresses. See **DHCP Reserved IPs, page 52**.
  - **DHCP Relay:** Choose this option to allow the security appliance to use a DHCP Relay. If you choose this mode, also enter the IP address of the Relay Gateway.
- **Domain Name (optional):** Enter a name for the domain.

- **Starting IP Address** and **Ending IP Address**: Enter the range of addresses in the IP address pool for this security appliance. Any new DHCP client that joins the LAN is assigned an IP address in this range. The default starting address is 192.168.75.2. The default ending address is 192.168.75.100. You can save part of the range for PCs with fixed addresses. These addresses should be in the same IP address subnet as the LAN IP address of the security appliance.

- **Primary DNS Server** and **Secondary DNS Server (Optional)**: Optionally, enter the IP address of the primary DNS server and secondary DNS server for your service provider.

- **Primary Tftp Server and Secondary Tftp Server (Optional):** Optionally, enter the IP address of the primary Tftp server and secondary Tftp server for your service provider.

- **WINS Server (Optional):** Enter the IP address for the WINS server or, if present in your network, the Windows NetBios server.

- **Lease Time:** Enter the maximum connection time in hours that a dynamic IP address is “leased” to a network user. When the time elapses, the user is automatically assigned a new dynamic IP address. The default is 24 hours.

- **Relay Gateway:** If you chose DHCP Relay as the DHCP mode, enter the IP address of the relay gateway.

STEP 4 In the **LAN Proxies** section, specify the proxy settings:

- **Enable DNS Proxy:** Check this box to allow the security appliance to act as a proxy for all DNS requests and to communicate with the DNS servers of the ISP. When this feature is disabled, all DHCP clients receive the DNS IP addresses of the ISP.

STEP 5 Click **Apply** to save your settings.

NOTE Next steps:

- If you are using the Getting Started (Basic) page, click **Getting Started** in the menu bar, and then continue with the list of configuration tasks.

- To check the LAN connection status, click **LAN > LAN Status**. For more information, see **Viewing the LAN Status, page 46**.

- To reserve certain IP addresses always to be used by particular devices, click **LAN > DHCP Reserved IPs**. For more information, see **DHCP Reserved IPs, page 52**.

- To view a list of the connected devices, click **LAN > DHCP Leased Clients**. For more information, see **DHCP Leased Clients, page 53**.
- If you need an extra LAN port and are not planning to configure either an optional WAN or a DMZ, click **Optional Port > Optional Port Mode** and choose **LAN** for the port mode. For more information, see **Configuring the Optional Port as a LAN Port, page 53**.
- If you are having problems with your LAN connection, see **Pinging to Test LAN Connectivity, page 221** in **Appendix A, "Troubleshooting."**

Viewing the LAN Status

STEP 1 Click **Networking > LAN > LAN Status**.

The LAN Status window opens. This page displays the following types of information:

- MAC address of the LAN interface
- IP address and subnet mask of the interface
- DHCP server mode

STEP 2 Click **Apply** to save your settings.

VLAN Configuration

The security appliance supports Virtual LANs (VLANs), which allow you to segregate the network into LANs that are isolated from one another. The default configuration provides for a data VLAN and a voice VLAN, which can be treated like two separate networks.

You can change the settings for the default VLANs, and you can add new VLANs, for up to a total of 16 VLANs. For example, if you need a guest network for visitors to your site, you can create new VLAN. Any PC that is connected to the specified LAN port is on a separate VLAN and cannot access other VLANs, unless you enable inter VLAN routing.

This section includes the following topics:

- **Default VLAN Settings**
- **Enabling or Disabling VLAN Support**
- **Creating VLAN IDs**
- **Assigning VLANs to LAN Ports**

Default VLAN Settings

By default, the data VLAN and the voice VLAN are enabled with the following settings:

- Data VLAN: The VLAN is enabled with the VLAN ID 1
  - VLAN - Data, VLAN Number (untagged packets): 1
  - VLAN - Data, IP Address: See Product Tab
  - VLAN - Data, IP Address Distribution: DHCP Server
  - VLAN - Data, Start IP Address: 192.168.75.50 (assuming LAN IP address is 192.168.75.1)
  - VLAN - Data, End IP Address: 192.168.75.254 (assuming LAN IP address is 192.168.75.1)
  - VLAN - Data, Subnet Mask: 255.255.255.0
  - VLAN - Data, Lease Time in Minutes: 1440 (24hours)
  - Lease Time in Minutes: 1440 (24hours)
  - HTTP Remote Access: disable
  - HTTPS Remote Access: disable
- Voice VLAN: The VLAN is enabled with the VLAN ID 100.
  - IP Address: 10.1.1.1
  - IP Address Distribution: DHCP Server
  - Start IP Address: 10.1.1.50
  - End IP Address: 10.1.1.254
  - Subnet Mask: 255.255.255.0

Enabling or Disabling VLAN Support

By default, VLAN support is enabled. If you do not want VLANs, you can disable VLAN support.

STEP 1 Click **Networking > VLAN > VLAN Configuration**.

The VLAN Configuration window opens.

STEP 2 To enable VLAN support, check the **Enable VLAN** box. To disable VLAN support, uncheck the box.

STEP 3 Click **Apply** to save your settings.

NOTE Next steps:

Create VLAN IDs. For more information, see **Creating VLAN IDs, page 48**.

Creating VLAN IDs

Before you can configure a new VLAN, you need to create the VLAN IDs. Later you will assign VLAN IDs to ports on the Port VLANs page.

STEP 1 Click **Networking > VLAN > Available VLANs**.

The Available VLANs window opens. The default VLAN and any other VLANs appear in the List of available VLANs table. The default VLAN ID is 1.

STEP 2 To add a VLAN, click **Add**.

Other options: To delete an entry, check the box, and then click **Delete**. To edit an entry, check the box, and then click the **Edit** button. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the VLAN Configuration window opens.

STEP 3 Enter the following information:

- **Name:** Enter a descriptive name, for reference.
- **ID:** Enter a unique identification number, which can be any number from 2 to 4091.

NOTE VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 4092 is reserved and cannot be used.

- **Inter VLAN Routing Enable:** Check the box if you want to allow the SA500 to route traffic between this VLAN and other VLANs that also have inter-VLAN routing enabled. Uncheck the box to disable inter-VLAN routing for this VLAN.

STEP 4 Click **Apply** to save your settings.

NOTE Next steps:

- Assign the VLANs to LAN ports. For more information, see **Assigning VLANs to LAN Ports, page 49**.
- Set up VLAN subnets. For more information, see **Multiple VLAN Subnets, page 50**.

Assigning VLANs to LAN Ports

To assign a VLAN to a LAN port, choose the mode and assign VLAN membership.

STEP 1 Click **Networking > LAN > Port VLAN**.

The Port VLANs window opens. The existing port VLAN settings appear in the Port VLANs table.

STEP 2 To update the settings for a port, click the **Edit** button.

STEP 3 In the **VLAN Configuration** area, enter the following information:

- **Mode:** Choose one of the following options:
  - **Access:** The access port is a member of a single VLAN. All data going into and out of the access port is untagged. By default, all VLAN ports are in access mode. Access mode is recommended if the port is connected to a single end-user device which is VLAN unaware.
    If you choose this option, also enter a VLAN ID for the port, in the **PVID** field.
  - **General:** The port is a member of a specified set of VLANs. The port sends and receives both tagged and untagged data. Untagged data coming into the port is assigned the specified PVID. Data that is sent out of the port from the same PVID is untagged. All other data is tagged.

General mode is recommended if the port is connected to an unmanaged switch with a mix of VLAN-aware and VLAN-unaware devices.
If you choose this option, also enter a **PVID** number for the port, and configure the **VLAN Membership** in the lower half of the page.

  - **Trunk:** The port is a member of a specified set of VLANs. All data going into and out of the port is tagged. Untagged data coming into the port is not forwarded, except for the default VLAN with PVID=1, which is untagged. Trunk mode is recommended if the port is connected to a VLAN-aware switch or router.
If you choose this option, also configure the **VLAN Membership** in the lower half of the page.

- **PVID**: If you chose Access or General mode, enter the Port VLAN ID to be used to forward or filter the untagged packets coming into port.

STEP 4 In the **VLAN Membership Configuration** area, check the box for each VLAN that you want to associate with this port.

STEP 5 Click **Apply** to save your settings.

Multiple VLAN Subnets

Typically, VLANs are isolated such that the traffic generated by any one of these networks is not seen by the others. However there are instances where you want to enable communication between VLANs. When you configure VLAN subnets, the security appliance routes traffic between VLANs and provides services such as a DHCP server for the members of each VLAN.

STEP 1 Click **Networking > VLAN > Multiple VLAN Subnets**.

The Multiple VLAN Subnets window opens. All VLANs from the **Networking > LAN > Available VLANs** page appear in the List of available Multiple VLAN Subnets table.

The Multiple VLAN Subnet Configuration window opens.

STEP 2 In the **Multiple VLAN Subnet** section of the page, enter the following settings:

- **IP Address:** Enter the VLAN subnet IP address.

- **Subnet Mask:** Enter the subnet mask for this VLAN.

STEP 3 In the **DHCP** section of the page, choose the DHCP mode:

- **None:** Choose this option if you do not want to enable a DHCP server for this VLAN.
- **DHCP Server:** Choose this option to allow the security appliance to act as a DHCP server for this VLAN. If you choose this option, complete the other fields in this section of the page.
- **DHCP Relay:** Choose this option to allow the security appliance to use a DHCP Relay for this VLAN. If you choose this mode, also enter the IP address of the **Relay Gateway**.

STEP 4 If you chose DHCP Server for the DHCP Mode, enter the following information:

- **Domain Name:** *(optional)* Enter a domain name for this VLAN.
- **Starting IP Address:** Enter the first IP address in the DHCP range. Any new DHCP client joining the VLAN is assigned an IP address between this address and the Ending IP Address.
- **Ending IP Address:** Enter the last IP address in the DHCP range. Any new DHCP client joining the LAN is assigned an IP address between the Starting IP Address and this IP address.

  NOTE The Starting and Ending DHCP addresses should be in the same IP address range as the LAN TCP/IP address (as configured on the LAN > IPv4 LAN Configuration page, LAN TCP/IP Setup section).

- **Primary DNS Server** and **Secondary DNS Server (Optional)**: Enter the IP address of the primary DNS server for the VLAN. Optionally, enter the IP address of a secondary DNS server.
- **Primary Tftp Server** and **Secondary Tftp Server (Optional)**: Enter the IP address of the primary and secondary Tftp servers for the VLAN
- **WINS Server (Optional):** Enter the IP address for the WINS server or, if present in your network, the Windows NetBios server.
- **Lease Time:** Enter the maximum connection time in hours that a dynamic IP address is “leased” to a network user. When the time elapses, the user is automatically assigned a new dynamic IP address. The default is 24 hours.

STEP 5 In the **LAN Proxies** section, check the **Enable DNS Proxy** box to allow the VLAN to act as a proxy for all DNS requests and to communicate with the DNS servers of the ISP. When this feature is disabled, all DHCP clients on the VLAN receive the DNS IP addresses of the ISP.

This feature is particularly useful in Auto Rollover mode. For example, if the DNS servers for each connection are different, then a link failure may render the DNS servers inaccessible. However, when the DNS proxy is enabled, then clients can make requests to the router and the router, in turn, sends those requests to the DNS servers of the active connection. You also can enable the IGMP proxy on the respective LAN.

STEP 6 Click **Apply** to save your settings.

DHCP Reserved IPs

Even when the security appliance is configured to act as a DHCP server, you can reserve certain IP addresses always to be assigned to specified devices. To do so, add the MAC address of the device, along with the desired IP address, to the list of DHCP Reserved IPs. Whenever the LAN DHCP server receives a request from a device, the hardware address is compared with the database. If the device is found, then the reserved IP address is used. Otherwise, an IP address is assigned automatically from the DHCP pool.

NOTE The reserved IPs need to be outside the pool of the DHCP addresses that the DHCP server assigns dynamically.

STEP 1 Click **Networking > LAN > DHCP Reserved IPs**, or from the Getting Started (Basic) page, under **WAN & LAN Connectivity**, click **DHCP Reserved IPs (Optional)**.

The DHCP Reserved IPs (LAN) window opens. Any existing reserved IPs are listed in the Available DHCP Assigned IPs (LAN) table.

STEP 2 To add a reserved IP address, click **Add**. The DHCP Reserved IP for LAN window opens.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

STEP 3 Enter the IP address and the MAC address of the device that you want to add.

Each reserved IP address should be outside the configured DHCP pool addresses.

STEP 4 Click **Apply** to save your settings.

DHCP Leased Clients

This page displays a list of the DHCP-assigned IP addresses and hardware addresses of the LAN clients. Click **Networking > LAN > DHCP Leased Clients**.

Configuring an IGMP Proxy

You can configure the router to act as a proxy for all IGMP requests and to communicate with the IGMP servers of the ISP.

STEP 1 Click **Networking > LAN > IGMP Configuration**.

The IGMP Proxy window opens.

STEP 2 Check the box to enable an IGMP proxy.

STEP 3 Click **Apply** to save your changes.

Configuring the Optional Port as a LAN Port

If you are not planning to configure an optional WAN or a DMZ, you can configure the Optional port for use as a LAN port.

STEP 1 Click **Networking > Optional Port > Optional Port Mode**.

The Optional Port Mode window opens.

STEP 2 Choose **LAN**.

STEP 3 Click **Apply** to save your settings.

Configuring the Optional WAN

You can configure the Optional port for use as an optional WAN, allowing you to set up two ISP links for your network. You can use one link as the primary link and one for backup purposes, or you can configure load balancing to use both links at the same time.

STEP 1 First configure the Optional port for use as a WAN port:

a. Click **Networking > Optional Port > Optional Port Mode**, or from the Getting Started (Advanced) page, under **Secondary WAN Port**, click **Set Optional Port to WAN**.

   The Optional Port Mode window opens.

b. Choose **WAN**.

c. Click **Apply** to save your settings.

   If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to return to the list of configuration tasks.

STEP 2 Click **Networking > Optional Port > WAN**, or from the Getting Started (Advanced) page, under **Secondary WAN Port**, click **Configure WAN settings for Optional Port**.

STEP 3 The WAN Configuration window opens.In the **ISP Configuration** area, check the **Internet Connection Require a Login** box if your ISP requires a login every time you connect to the Internet.

- If you checked the box, complete the fields in the ISP Connection Type area.
- If you did not check the box, continue complete the fields in the Internet (IP) Address area and Dynamic Name System (DNS) Servers area.

STEP 4 If your Internet connection requires a login, enter the settings in **ISP Connection Type** area:

- **ISP Connection Type:** Choose the connection type, as specified by your service provider: PPTP, PPPoE, or L2TP. Then complete all fields that are highlighted with white backgrounds.
- **PPPoE Profile Name:** Choose a PPPoE profile. To manage the profiles in the drop-down list, see **Creating PPPoE Profiles, page 40**.
- **User Name:** The user name that is required to log in

- **Password:** The password that is required to log in
- **Secret:** Enter the secret phrase to log into the server (if applicable).
- **Connectivity Type:** Choose one of the following options:
  - **Keep Connected:** The connection is always on, regardless of the level of activity. Choose this option if you pay a flat fee for your Internet service.
  - **Idle Time:** The security appliance disconnects from the Internet after a specified period of inactivity (Idle Time). If you choose this option, also enter the Idle Time in minutes. Choose this option if your ISP fees are based on the time that you spend online.
- **My IP Address:** Enter the IP address assigned to you by the ISP.
- **Server IP Address:** Enter the IP address of the PPTP, PPPoE, or other server.

STEP 5 If your ISP does not require a login, enter the following information in the **Internet (IP) Address** and **Dynamic Name System (DNS) Servers** areas:

- **IP Address Source:** Your ISP assigns you an IP address that is either dynamic (newly generated each time you log in) or static (permanent).
  - **Get Dynamically from ISP**: Choose this option if your ISP has not assigned an IP address to you.
  - **Use Static IP Address**: Choose this option if your ISP has assigned an IP address to you. Also enter the **IP Address**, **IP Subnet Mask**, and the **Gateway IP Address** that were provided by your ISP.
- **DNS Server Source:** DNS servers map Internet domain names (example: www.cisco.com) to IP addresses. You can get DNS server addresses automatically from your ISP or use ISP-specified addresses.
  - **Get Dynamically from ISP**: Choose this option if you have not been assigned a static DNS IP address.
  - **Use These DNS Servers.**: Choose this option if your ISP assigned a static DNS IP address. Also enter the addresses for the **Primary DNS Server** and the **Secondary DNS Server**.

STEP 6 If required by your ISP, configure the following settings in the **MTU Size** area:

- **MTU Type:** The Maximum Transmission Unit is the size, in bytes, of the largest packet that can be passed on. Choose **Default** to use the default MTU size, 1500 bytes. Choose **Custom** if you want to specify another size.

- **MTU Size:** If you chose **Customer** for the MTU Type, enter the custom MTU size in bytes.

  The MTU (Maximum Transmit Unit) is the size of the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes. For PPPoE connections, it is 1492 Bytes. Unless a change is required by your ISP, it is recommended that the MTU values be left as is.

STEP 7 If a MAC address source is required by your ISP, enter the following information in the **Router's MAC Address** area:

- **MAC Address Source:** Typically, you use the unique 48-bit local Ethernet address of the security appliance as your MAC address source. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, you can enter a different MAC address to use for this purpose.
  - **Use Default Address:** Choose this option to use the default MAC address.
  - **Use this computer's MAC address:** Choose this option if you want to use the MAC address of your computer as the MAC address source.
  - **Use This MAC Address:** Choose this option if you want to enter a MAC address that your ISP requires for this connection (sometimes called MAC address cloning). Enter the **MAC Address** in the format XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or an alphabetical letter between A and F (inclusive), as in the following example: `01:23:45:67:89:ab`

STEP 8 Click **Apply** to save your settings.

STEP 9 Next steps:

- If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to continue with the list of configuration tasks.
- To check the WAN status, click **WAN > WAN Status**. For more information, see **Viewing the WAN Status, page 39**.
- **Recommended:** To configure auto-rollover, load balancing, and failure detection for your ISP links, click **Optional Port > WAN Mode**. For more information, see **Configuring Auto-Rollover, Load Balancing, and Failure Detection, page 57**.

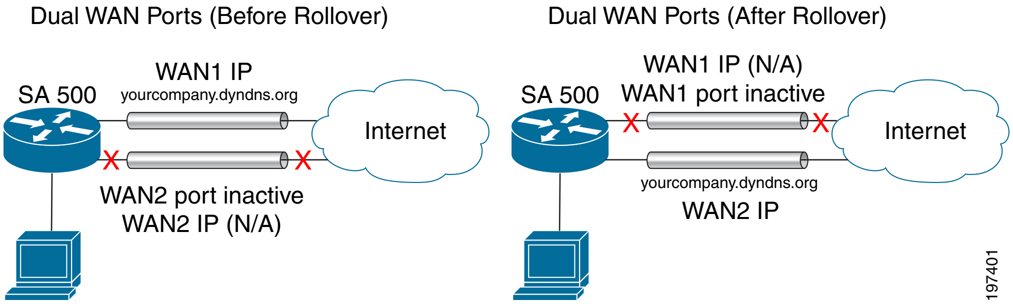
- If you are having problems with your WAN connection, see the **Internet Connection, page 217** in **Appendix A, "Troubleshooting."**

Configuring Auto-Rollover, Load Balancing, and Failure Detection

If you configured two ISP links, one for the dedicated WAN and one for the optional WAN, you can configure the WAN Mode to determine how the two ISP links are used. You can choose from these features:

- **Auto-Rollover:** Enable this feature when you want to use one ISP link as a backup. If a failure is detected on the link that you specify as the primary link, then the security appliance directs all Internet traffic to the backup link. When the primary link regains connectivity, all Internet traffic is directed to the primary link, and the backup link becomes idle. You can designate either the Dedicated WAN port or the Optional WAN port as the primary link. **Figure 1** shows an example of Dual WAN ports configured with Auto-Roller.

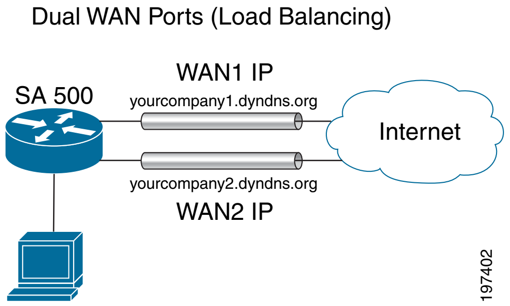
Figure 1 Example Dual WAN Ports with Auto-Roller



- **Load Balancing:** Enable this feature when you want to use both ISP links simultaneously. The two links will carry data for the protocols that are bound to them. You can use this feature to segregate traffic between links that are not of the same speed. For example, bind high-volume services through the port that is connected to a high speed link, and bind low-volume services to the port that is connected to the slower link.

  Load balancing is implemented for outgoing traffic and not for incoming traffic. To maintain better control of WAN port traffic, consider making the WAN port Internet addresses public and keeping the other one private. **Figure 2** shows an example of Dual WAN Ports configured with Load Balancing.

Figure 2 Example of Dual WAN Ports with Load Balancing



NOTE When configuring load balancing, make sure that you configure both WAN ports with the Connectivity Type set to Keep Connection. If the WAN is configured to time out after a specified period of inactivity, then load balancing is not applicable.

- **Failure Detection:** Enable this feature to allow the security appliance to detect the failure of a WAN link. You can specify the detection method. In the event of a failure, traffic for the unavailable link is diverted to the available link.

NOTE Before you perform this procedure, you must configure the optional WAN connection. See **Configuring the Optional WAN, page 54**.

STEP 1 Click **Networking > Optional Port > WAN Mode**, or from the Getting Started (Advanced) page, under **Secondary WAN Port**, click **Configure WAN Mode**.

The WAN Mode window opens.

STEP 2 In the **Port Mode** area, choose one of the following modes:

- **Auto-Rollover with Primary port as:** Choose this option If you have two ISP links and you want to use one link as a backup. From the drop-down list, choose the WAN port that you want to designate as the primary link: **Dedicated WAN** or **Optional WAN**.

  When Auto Failover mode is enabled, the link status of the primary WAN port is checked at regular intervals as defined by the failure detection settings.

- **Load Balancing:** Choose this option if you have two ISP links that you want to use simultaneously. After you complete this procedure by clicking the **Apply** button, you need to configure the protocol bindings. See **Configuring the Protocol Bindings for Load Balancing, page 60**.

When the security appliance is configured in Load Balancing mode, it checks the connection of both the links at regular intervals to detect the status.

NOTE You can click the **Protocol Bindings** link to view, add, or edit the protocol bindings, but save your settings on this page first.

- **Use only single WAN port:** Choose this option if you are connected to only one ISP. Also select the WAN port that is connected to your ISP: **Dedicated WAN** or **Optional WAN**. This option may be useful for debugging connection issues.

STEP 3 If you chose Auto-Rollover or Load Balancing for the Port Mode, configure the **WAN Failure Detection Method**:

- **None:** Choose this option to have no check for detecting WAN failure. This option is valid only if the port mode is set to Load Balancing.
- **DNS lookup using WAN DNS Servers:** Choose this option to detect a failure of a WAN link by using the DNS servers that are configured for the Dedicated WAN or Optional Port WAN.
- **DNS lookup using these DNS Servers:** Choose this option to detect a failure of a WAN link by using the DNS servers that you specify in the fields below.
  - **Dedicated WAN**: Enter the IP address of the DNS servers for the Dedicated WAN.
  - **Optional WAN**: Enter the IP address of the DNS server for the WAN interface on the Optional port.
- **Ping these IP addresses:** Choose this option to detect WAN failure by pinging the IP addresses that you specify in the fields below.
  - **Dedicated WAN**: Enter a valid IP address to ping from the Dedicated WAN.
  - **Optional WAN**: Enter a valid IP address to ping from the WAN interface on the Optional port.
- **Retry Interval is:** Specify how often, in seconds, the security appliance should run the above configured failure detection method.
- **Failover after:** Specify the number of retries after which failover is initiated.

STEP 4 Click **Apply** to save your settings.

NOTE Next steps:

- If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to continue with the list of configuration tasks.
- **Required for load balancing:** If you chose the Load Balancing option, click **Optional Port > Protocol Bindings** to configure your protocol bindings. For more information, see **Configuring the Protocol Bindings for Load Balancing, page 60**.

Configuring the Protocol Bindings for Load Balancing

If you chose Load Balancing as the Port Mode for your Optional WAN, you configure protocol bindings to determine how the traffic is balanced between the two ISP links. This feature can be used to segregate traffic between links that are not of the same speed. High volume traffic can be routed through the port connected to a high speed link and low volume traffic can be routed through the port connected to the slow link.

For example, you can bind the HTTP protocol to the Dedicated WAN and bind the FTP protocol to the Optional WAN. In this scenario, the security appliance automatically channels FTP data through the Optional WAN. All HTTP traffic is routed through the Dedicated WAN.

NOTE Before you can enter the protocol bindings, you must configure the optional port, the WAN connection, and the WAN port mode. For more information, see **Configuring Auto-Rollover, Load Balancing, and Failure Detection, page 57**.

If you want to enter a protocol binding for a custom service, you must first add the custom service to the database. See **Creating Custom Services, page 104**.

STEP 1 Click **Networking > Optional Port > Protocol Bindings**, or from the Getting Started (Advanced) page, under **Secondary WAN Port**, click **Configure Protocol Bindings (Optional - if WAN Mode set to Load Balancing)**.

The Protocol Bindings window opens. Any existing protocol bindings appear in the List of Available Protocol Bindings table.

STEP 2 Click **Add**.

Other options: Click **Edit** to edit an entry. To enable a protocol binding, click **Enable**. To disable a protocol binding, click **Disable**. To delete an entry, check the box, and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the Protocol Bindings Configuration window opens.

STEP 3 Enter the following information:

- **Service:** Choose a service from the list.

  The security appliance is configured with a list of standard services. For information about adding your own custom services to the list, see **Creating Custom Services, page 104**.

- **Local Gateway:** Choose the interface that you want to use: **Dedicated WAN** or **Configured WAN**.

- **Source Network:** To identify the source network, choose **Any**, **Single Address**, or **Address Range**. If you choose **Single Address**, enter the address in the Start Address field. If you choose **Address Range**, enter the Start Address and the End Address to specify the range.

- **Destination Network:** To identify the destination network, choose **Any**, **Single Address**, or **Address Range**. If you choose **Single Address**, enter the address in the Start Address field. If you choose **Address Range**, enter the Start Address and the End Address to specify the range.

STEP 4 Click **Apply** to save your settings.

STEP 5 When you are ready, enable the new protocol bindings that you added. A new protocol binding is disabled until you enable it.

Configuring a DMZ

A DMZ (Demarcation Zone or Demilitarized Zone) is a subnetwork that is behind the firewall but that is open to the public. By placing your public services on a DMZ, you can add an additional layer of security to the LAN. The public can connect to the services on the DMZ but cannot penetrate the LAN. You should configure your DMZ to include any hosts that must be exposed to the WAN (such as web or email servers).

DMZ configuration is identical to the LAN configuration. There are no restrictions on the IP address or subnet assigned to the DMZ port, other than the fact that it cannot be identical to the IP address given to the LAN interface of this gateway.

In this scenario, the business has one public IP address, 209.165.200.225, which is used for both the router's public IP address and the web server's public IP address. The administrator configures the Optional port to be used as a DMZ port. A firewall rule allows inbound HTTP traffic to the web server at 172.16.2.30. Internet users can enter the domain name that is associated with the IP address 209.165.200.225, and they are connected to the web server. The same IP address is used for the WAN interface.

Figure 3 Example DMZ with One Public IP Address for WAN and DMZ

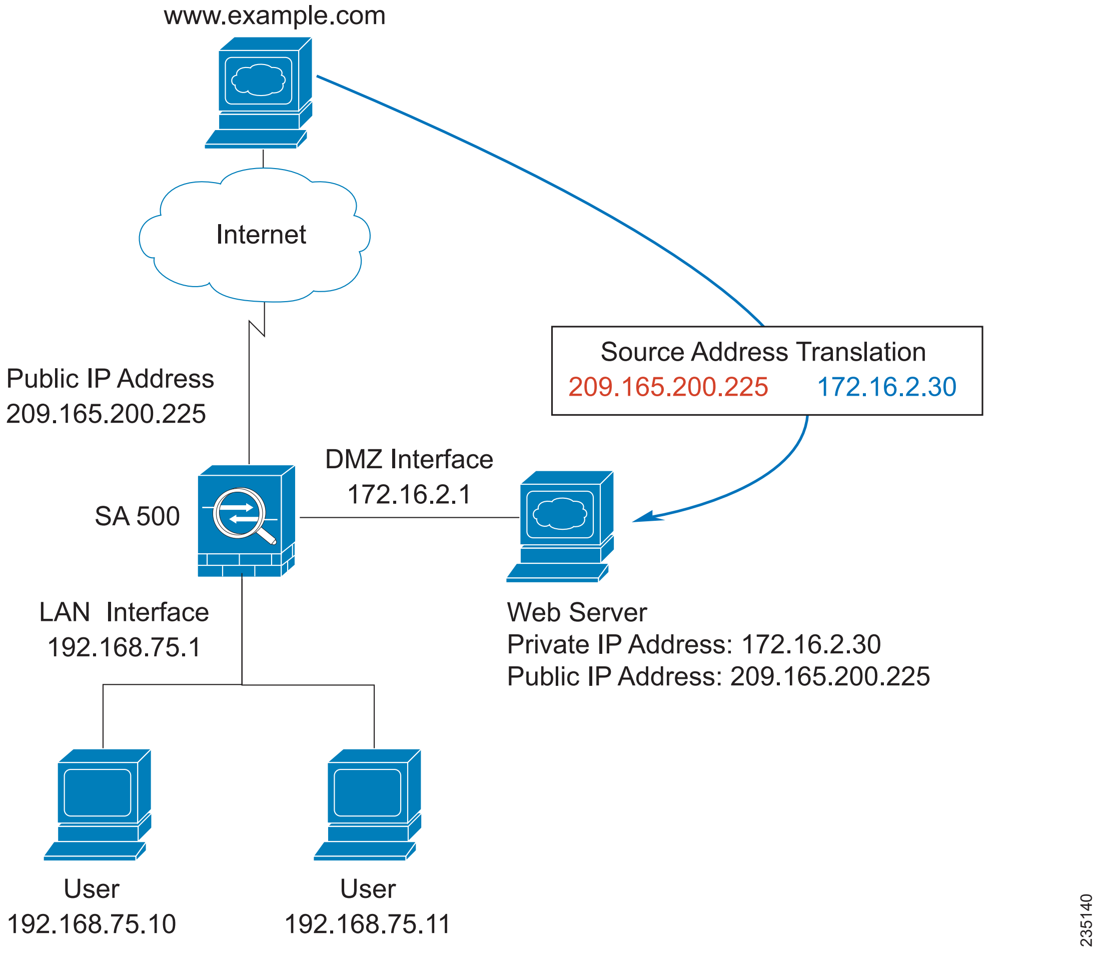
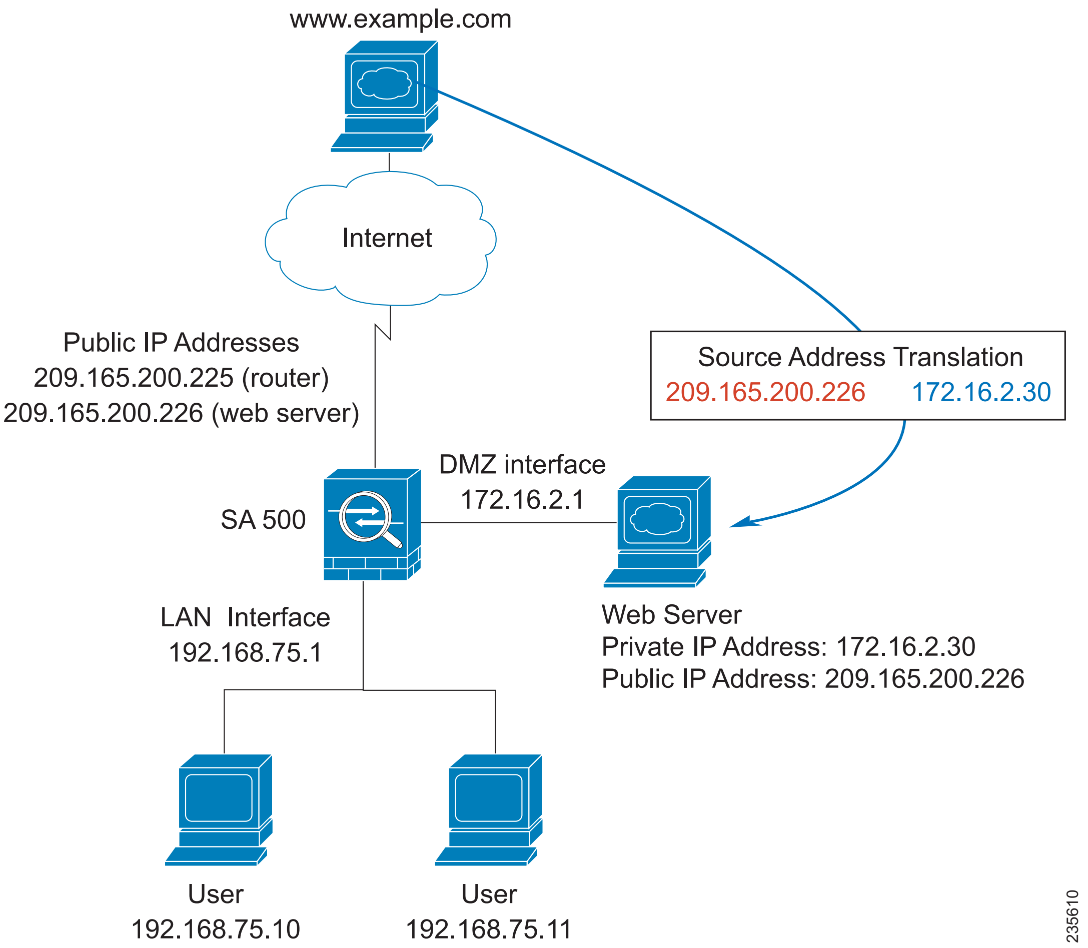


Figure 4 Example DMZ with Two Public IP Addresses



In this scenario, the ISP has supplied two static IP addresses: 209.165.200.225 and 209.165.200.226. The address 209.165.200.225 is used for the router's public IP address. The administrator configures the Optional port to be used as a DMZ port and created a firewall rule to allow inbound HTTP traffic to the web server at 172.16.2.30. The firewall rule specifies an external IP address of 209.165.200.226. Internet users can enter the domain name that is associated with the IP address 209.165.200.226, and they are connected to the web server.

Configuring the DMZ Settings

Follow this procedure to configure your DMZ port settings, and then create firewall rules to allow traffic to access the services on your DMZ.

STEP 1 First configure the Optional port for use as a DMZ:

a. Click **Networking > Optional Port > Optional Port Mode**, or from the Getting Started (Advanced) page, under DMZ Port, click **Set Optional Port to DMZ mode**.

The Optional Port Mode window opens.

b. Choose **DMZ**.

c. Click **Apply** to save your settings.

If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to return to the list of configuration tasks.

STEP 2 Click **Networking > Optional Port > DMZ Config**, or from the Getting Started (Advanced) page, under **DMZ Port**, click **Configure DMZ settings**.

The DMZ Configuration window opens.

STEP 3 In the **DMZ Port Setup** area, enter an **IP Address** and the **Subnet Mask** for the DMZ port on the internal network. Devices on the DMZ network communicate with the router by using this IP address.The default DMZ IP address of 172.16.2.1 is shown on the screen.

STEP 4 In the **DHCP for DMZ Connected Computers** area, enter the following information:

- **DHCP Mode:** Choose one of the following modes:
    - **None:** Choose this option if If the computers on the DMZ are configured with static IP addresses or are configured to use another DHCP server.
    - **DHCP Server:** Choose this option to allow the security appliance to act as a DHCP server and to assign IP addresses to all devices that are connected to the DMZ network. Also complete the fields that are highlighted with white backgrounds.
    - **DHCP Relay:** Choose this option to allow the security appliance to use a DHCP Relay. If you choose this mode, also enter the IP address of the Relay Gateway.
- **Domain Name (optional):** Enter a name for the domain.

- **Starting IP Address** and **Ending IP Address**: Enter the range of addresses in the IP address pool for this security appliance. Any new DHCP client that joins the DMZ is assigned an IP address in this range.
- **Primary DNS Server** and **Secondary DNS Server (Optional)**: Enter the IP address of the primary DNS server for the DMZ. Optionally, enter the IP address of a secondary DNS server.
- **Primary Tftp Server** and **Secondary Tftp Server (Optional)**: Enter the IP address of the primary and secondary Tftp servers for the DMZ
- **WINS Server (Optional):** Enter the IP address for the WINS server or, if present in your network, the Windows NetBios server.
- **Lease Time:** Enter the maximum connection time in hours that a dynamic IP address is "leased" to a network user. When the time elapses, the user is automatically assigned a new dynamic IP address. The default is 24 hours.
- **Relay Gateway:** If you chose DHCP Relay as the DHCP mode, enter the IP address of the relay gateway.

STEP 5 In the **DMZ Proxies** section, check the box to allow the DMZ to act as a proxy for all DNS requests and to communicate with the DNS servers of the ISP. When this feature is disabled, all DHCP clients on the DMZ receive the DNS IP addresses of the ISP.

STEP 6 Click **Apply** to save your settings.

NOTE Next steps:

- If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to continue with the list of configuration tasks.
- **Required:** You must configure a firewall rule to allow inbound traffic to access your DMZ. Also use the firewall rule to specify a public IP address for a server on your DMZ, if applicable. To get started, click **Firewall** on the menu bar. For more information, see **Configuring a Firewall Rule for Inbound Traffic, page 110**.
- If you want to reserve certain IP addresses for specified devices, click **Optional Port > DMZ Reserved IPs**. For more information, see **DMZ Reserved IPs, page 66**.

- If you want to see a list of the DMZ DHCP clients, click **Optional Port > DMZ DHCP Clients**. For more information, see **DMZ DHCP Leased Clients, page 67**.

DMZ Reserved IPs

If you configured your DMZ to act as a DHCP server, you can reserve certain IP addresses always to be assigned to specified devices. To do so, add the hardware address of the device, along with the desired IP address, to the list of DMZ Reserved IPs. Whenever the DMZ DHCP server receives a request from a device, the hardware address is compared with the database. If the device is found, then the reserved IP address is used. Otherwise, an IP address is assigned automatically from the DHCP pool.

NOTE Before you can perform this procedure, you must enable DCHP Server mode or DHCP Relay mode on the DMZ Configuration page. For more information, see **Configuring a DMZ, page 61**.

STEP 1 Click **Networking > Optional Port > DMZ Reserved IPs**, or from the Getting Started (Advanced) page, under **DMZ Port**, click **Configure DMZ DHCP Reserved IPs (Optional)**.

The DMZ Reserved IPs window opens. Any existing DMZ reserved IP addresses appear in the Available DHCP Assigned IPs (DMZ) table.

NOTE The reserved IPs need to be outside the pool of the DHCP addresses that the DMZ DHCP server assigns dynamically.

STEP 2 Click **Add**.

Other options: Click **Edit** to edit an entry. To delete an entry, check the box, and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the DMZ Reserved IPs Configuration window opens.

STEP 3 Enter the IP Address and the MAC Address.

STEP 4 Click **Apply** to save your settings.

DMZ DHCP Leased Clients

This page displays a list of the DHCP-assigned IP addresses and hardware addresses of the DMZ clients.

Click **Networking > Optional Port > DMZ DHCP Clients**.

Routing

If needed, you can change the routing mode, configure static routing, or configure dynamic routing on your security appliance.

- **Routing, page 67**
- **Static Routing, page 68**
- **Dynamic Routing, page 69**

Routing

Depending on the requirements of your ISP, you can configure the security appliance in NAT routing mode or Classic routing mode. By default, NAT is enabled.

Network Address Transalation (NAT) is a technique that allows several computers on a LAN to share an Internet connection. The computers on the LAN use a private IP address range while the WAN port on the router is configured with a single public IP address. Along with connection sharing, NAT also hides internal IP addresses from the computers on the Internet.

STEP 1 Click **Networking > Routing > Routing**.

The Routing Mode window opens.

STEP 2 Choose one of the following options:

- **NAT:** Choose this option if your ISP has assigned only one IP address to you or if you are sharing IP addresses across several devices such as your LAN, and using the other dedicated devices for DMZ. NAT is the default option.
- **Classic Routing:** Choose this option if your ISP has assigned an IP address for each of the computers that you use.

STEP 3 Click **Apply** to save your settings.

Static Routing

To configure static routes, enter a route name and specify the IP address and related information for the destination. Also assign a priority, which determines the route that is chosen when there are multiple routes to the same destination.

You can add static routes for your IPv4 network or your IPv6 network, if IPv6 mode is enabled.

STEP 1 Click **Networking > Routing > Static**.

The Static Routing window opens.

STEP 2 Click **Add** to add a new static route.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the Static Routing Configuration window opens.

STEP 3 Enter the following information:

- **Name:** Enter a name for identification and management purposes.
- **Active:** Check this box to activate the route, or clear the box to deactivate a route that is not in use but that you do not want to delete. An inactive route is not broadcast if Routing Information Protocol (RIP) is enabled.
- **Private:** Determines whether the route can be shared with other routers when RIP is enabled. If it is selected, then the route will not be shared in a RIP broadcast or multicast. This is only applicable for IPv4 static routes.
- **Destination IP Address:** Enter the IP address of the host or the network that the route leads to.
- **IP Subnet Mask:** Enter the subnet mask for the destination network.
- **Interface:** From the list, choose the physical network interface (Dedicated WAN, Optional WAN, DMZ or LAN), through which this route is accessible.
- **Gateway IP Address:** Enter the IP address of the gateway router through which the destination host or network can be reached.

- **Metric:** Enter a number from 2 to 15 to manage the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.

STEP 4 Click **Apply** to save your settings.

Dynamic Routing

Dynamic Routing or RIP, is an Interior Gateway Protocol (IGP) that is commonly used in internal networks. It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network.

NOTE RIP is disabled by default.

STEP 1 Click **Networking > Routing > Dynamic**.

The Dynamic Routing (RIP) window opens.

STEP 2 In the **RIP Configuration** area, enter the following information:

- **RIP Direction:** Determines how the router sends and receives RIP packets:
  - **Both:** The router both broadcasts its routing table and also processes RIP information received from other routers.
  - **Out Only:** The router broadcasts its routing table periodically but does not accept RIP information from other routers.
  - **In Only:** The router accepts RIP information from other routers, but does not broadcast its routing table.
  - **None:** The router neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.
- **RIP Version:** Choose one of the following options:
  - **Disabled:** If RIP is disabled, this is selected.
  - **RIP-1** is a class-based routing version that does not include subnet information. This is the most commonly supported version.
  - **RIP-2** includes all the functionality of RIPv1 plus it supports subnet information. Though the data is sent in RIP-2 format for both RIP-2B and RIP-2M, the mode in which packets are sent is different.

- **RIP-2B** broadcasts data in the entire subnet.
- **RIP-2M** sends data to multicast addresses.

STEP 3 In the **Authentication for RIP 2B/2M** area, enter the following information:

- **Enabled Authentication for RIP 2B/2M:** Check this box to enable authentication for RIP-2B or RIP-2M.
- **First Key Parameters and Second Key Parameters**
  - **MD5 Key ID:** Input the unique MD-5 key ID.
  - **MD5 Auth Key:** Input the auth key for this MD5 key.
  - **Not Valid Before:** Start date of the First Key for MD5 based authentication between routers.
  - **Not Valid After:** End date of the First Key for MD5 based authentication between routers.

STEP 4 Click **Apply** to save your settings.

Port Management

You can enable or disable ports, set the duplex mode and speed, and enable or disable port mirroring. Refer to the following topics.

- **Configuring the Ports, page 70**
- **Configuring SPAN (Port Mirroring), page 71**

Configuring the Ports

STEP 1 Click **Networking > Port Management > Port Management**.

The Port Management window opens.

STEP 2 Choose the following options for each port:

- **Enable:** Check this box to enable the port. To disable the port, uncheck the box. By default all ports are enabled.

- **Auto:** Check this box to let the gateway and network to determine the optimal port settings.
- **Duplex:** Choose either Half Duplex and Full Duplex based on the port support. The default is Full Duplex for all ports.
- **Speed:** Choose the port speed. The default setting is 1000 Mbps for all ports.

STEP 3 Click **Apply** to save your settings.

Configuring SPAN (Port Mirroring)

Port mirroring, sometimes called Switched Port Analyzer, allows the traffic on one port to be visible on another port. This feature may be useful for debugging or for traffic monitoring by an external application. You can choose one LAN port to monitor the traffic on all other LAN ports.

STEP 1 Click **Networking > Port Management > SPAN (Port Mirroring)**.

The SPAN (Port Mirroring) window opens.

STEP 2 Enter the following information:

- **Do you want to enable Port Mirroring:** Check this box to enable port mirroring.
- **Mirror all LAN Ports to:** Choose the LAN port that will monitor all of the other LAN ports.

STEP 3 Click **Apply** to save your settings.

QoS Bandwidth Profiles

You can configure Quality of Service (QoS) Bandwidth Profiles for the WAN and the LAN.

For traffic from the secure zone to the insecure zone, QoS is determined by limiting the speed as well assigning a priority. To do so, create bandwidth profiles and assign traffic classes to them. The traffic selector identifies the stream of traffic that is subject to the specified bandwidth management profile.

NOTE Bandwidth limiting is not applicable to a DMZ interface.

Creating QoS Bandwidth Profiles for WAN Interfaces

STEP 1 Click **Networking > QoS > WAN QoS**.

The Bandwidth Management window opens. Any existing profiles appear in the Bandwidth Profiles table.

STEP 2 To enable this feature check the box at the top of the page and click **Apply**.

STEP 3 In the **WAN Configuration** area, specify the **Upstream Bandwidth in Kbps** and the **Downstream Bandwidth in Kbps** for each WAN interface by entering the values provided by your ISP. Then click **Apply**.

STEP 4 In the **Bandwidth Profiles Enable** area, do the following:

- Check the box to enable the bandwidth profiles.
- Click **Apply** to save your settings.

STEP 5 Click **Add** to add a new bandwidth profile.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the Bandwidth Profile Configuration window opens.

STEP 6 Enter the parameters to define a bandwidth profile. for a WAN interface.

- **Profile Name:** Enter a name to identify this profile.
- **Priority:** Choose a priority: Low, Medium, or High, Urgent. You can use Urgent for latency sensitive traffic such as voice. It is recommended that you set only one bandwidth profile to Urgent.
- **Maximum Bandwidth:** Enter the maximum bandwidth to associate with this profile.
- **Minimum Bandwidth:** Enter the minimum bandwidth to associate with this profile.
- **WAN Interface:** Choose the interface to which this bandwidth profile is applicable.

STEP 7 Click **Apply** to save your settings.

STEP 8 Repeat as needed to create additional profiles.

Traffic Selectors

After you create a bandwidth profile, you can associate it with a traffic flow.

NOTE Before you can create traffic selectors, you must enable bandwidth profiles and create at least one bandwidth profile. For more information, see **Creating QoS Bandwidth Profiles for WAN Interfaces, page 72**.

STEP 1 Click **Networking > Bandwidth Profiles > Traffic Selectors**.

The Traffic Selectors window opens. Any existing traffic selectors are listed in the List of Traffic Selectors table.

STEP 2 Click **Add** to add a new traffic selector.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the Traffic Selector Configuration window opens.

STEP 3 Enter the following information:

- **Available Profiles:** Select the bandwidth profile which will applied to this traffic.
- **Service:** Chose a service from the drop down list. If you do not see a service that you want, you can configure a custom service through Firewall custom services page.
- **Traffic Selector Match Type:** Choose the method for identifying the host to which the traffic selector will apply. Then enter the **IP Address**, **MAC Address**, **Port Name**, or **VLAN**, based on the chosen match type.

STEP 4 Click **Apply** to save your settings.

LAN QoS

The security appliance provides QoS-based IEEE 802.1p class of service (CoS) values and DSCP values for implementing Quality of Service at the Media Access Control level. This QoS method specifies priority values that can be used to differentiate traffic and give preference to higher-priority traffic, such as telephone calls.

Enabling LAN QoS

STEP 1 Click **Networking > QoS > LAN QoS**.

STEP 2 To enable quality of service on the LAN ports, check the box at the top of the page. Uncheck the box to disable this feature.

STEP 3 For each port, choose the type of value to use to classify the traffic. You can choose either DSCP, which is a layer 3 IP field, or CoS, which is a layer 2 Ethernet header field, depending on your requirements.

STEP 4 Click **Apply** to save your settings.

Port CoS Mapping

Use the Port CoS Mapping page to map each CoS value to a QoS priority queue.

STEP 1 Click **Networking > Qos > Port CoS Mapping**.

The Port CoS Mapping window opens.

STEP 2 For each **CoS Value**, use the drop-down list to choose the corresponding **Priority Queue**: **Lowest**, **Low**, **Medium** or **High**.

STEP 3 Click **Apply** to save your settings.

Port DSCP Mapping

Use the Port DSCP Mapping page to map each DSCP value to a QoS priority queue.

STEP 1 Click **Networking > Qos > Port DSCP Mapping**.

The Port DSCP Mapping window opens.

STEP 2 For each DSCP value, use the drop-down list to choose the corresponding **Queue**: **Lowest**, **Low**, **Medium** or **High**.

STEP 3 Click **Apply** to save your settings.

DSCP Remarking

DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Use the Remark CoS to DSCP page to map CoS values to DSCP values.

STEP 1 Click **Networking > Remark CoS to DSCP**.

The Remark CoS to DSCP window opens.

STEP 2 For each CoS value, use the drop-down list to choose the corresponding DSCP value.

STEP 3 Click **Apply** to save your settings.

Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. If your ISP has not provided you with a static IP, and your WAN connection is configured to use DHCP to get an IP address dynamically, then DDNS allows you to have a virtual static address for your website. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.com.

STEP 1 Click **Networking > Dynamic DNS**.

The Dynamic DNS window opens.

STEP 2 In the **WAN Mode** area, the Current WAN Mode is displayed.

STEP 3 In the **Dedicated WAN (DDNS Status)** area or the **Optional WAN (DDN Status)** area, enter the following information:

- **Select the Dynamic DNS Service:** Choose None or choose DynDNS.com.
- **Host and Domain Name:** Specify the complete Host Name and Domain Name for the DDNS service.
- **User Name:** Enter the DynDNS account User Name.
- **Password:** Enter the password for the DynDNS account.
- **Use wildcards:** Check this box to allow all subdomains of your DynDNS Host Name to share the same public IP as the Host Name. This option can be enabled here if not done on the DynDNS website.
- **Update every 30 days:** Check this box to allow the security appliance to update the host information on DynDNS and keep the subscription active after the 30 day trial.

STEP 4 Click **Apply** to save your settings.

Configuring IPv6 Addressing

Internet Protocol Version 6 (IPv6) is a new IP protocol designed to replace IPv4, the Internet protocol that is predominantly deployed and extensively used throughout the world. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, resulting in an exponentially larger address space. You can configure the security appliance to support IPv6 addressing on the LAN and the Dedicated WAN.

NOTE IPv6 is not supported on the Optional port.

First enable IPv6 mode, and then configure your WAN connection, LAN connection, routing, and tunneling.

- **IP Routing Mode**
- **Configuring the IPv6 WAN Connection**
- **Configuring the IPv6 LAN**
- **IPv6 LAN Address Pools**
- **IPv6 Multi LAN**
- **IPv6 Static Routing**
- **Routing (RIPng)**
- **6to4 Tunneling**
- **IPv6 Tunnels Status**
- **ISATAP Tunnels**
- **MLD Tunnels**
- **Configuring Router Advertisement**
- **Adding RADVD Prefixes**

IP Routing Mode

To get started with the IPv6 configuration, first enable IPv4/IPv6 mode. IPv4 and IPv6 addressing are supported.

STEP 1 Click **Networking > IPv6 > Routing Mode**.

The Routing Mode window opens.

STEP 2 Click **IPv4/IPv6 mode** to enable IPv6 addressing, or click **IPv4 only mode** to enable only IPv4 addressing.

STEP 3 Click **Apply** to save your settings.

STEP 4 When the warning appears "An IP Mode change will cause the device to reboot," click **OK** to continue. If you do not want to change the IP mode, click **Cancel**.

NOTE Next steps:

- To configure the WAN connection, click **IPv6 > IPv6 WAN Config**. For more information, see **Configuring the IPv6 WAN Connection, page 78**.
- To configure the LAN, click **IPv6 > IPv6 LAN Config**. For more information, see **Configuring the IPv6 LAN, page 80**.

Configuring the IPv6 WAN Connection

By default, when you enable IPv6 mode, your security appliance is configured to be a DHCPv6 client of the ISP, with stateless autoconfiguration. If your ISP assigned a static IPv6 address, or if you need to change the DHCP autoconfiguration mode, configure the settings on this page.

STEP 1 Click **Networking > IPv6 > IPv6 WAN Config**.

The IPv6 WAN Configuration window opens.

STEP 2 In the **Internet(IPv6) Address** area, choose **Static IPv6** if your service provider assigned a fixed (static or permanent) IP address. If you were not assigned a static IP address, choose **DHCPv6**.

STEP 3 If you are configuring a static address, enter the following information in the **Static IP Address** area of the page.

- **IPv6 Address:** Enter the static IP address that was provided by your Service Provider.
- **IPv6 Prefix Length:** The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. All hosts in the network have the identical initial bits for their IPv6 address. Enter the number of common initial bits in the network's addresses. The default prefix length is 64.
- **Default IPv6 Gateway:** Enter the IPv6 address of the gateway for your ISP. This is usually provided by the ISP or your network administrator.
- **Primary DNS Server** and **Secondary DNS Server**: Enter a valid IP address of a primary DNS Server and optionally a secondary DNS Server.

STEP 4 If you need to change the DHCPv6 autoconfiguration mode, choose the mode in the **DHCPv6** area of the page**:**

- **Stateless Address Auto Configuration:** If you choose this option, the security appliance can generate its own addresses using a combination of locally available information and information advertised by routers.
- **Stateful Address Auto Configuration:** If you choose this option, the security appliance connects to the DHCPv6 server at the ISP to obtain a leased address.

STEP 5 Click **Apply** to save your settings.

NOTE Next steps:

To configure the LAN, click **IPv6 > IPv6 LAN Config**. For more information, see **Configuring the IPv6 LAN, page 80**.

Configuring the IPv6 LAN

In IPv6 mode, the LAN DHCP server is enabled by default (similar to IPv4 mode). The DHCPv6 server will serve IPv6 addresses from configured address pools with the IPv6 Prefix Length assigned to the LAN. For more information, see **IPv6 LAN Address Pools, page 82**.

STEP 1 Click **Networking > IPv6 > IPv6 LAN Config**.

The IPv6 LAN Configuration window opens.

STEP 2 In the **LAN TCP/IP Settings** section, enter the following information:

- **IPv6 Address:** Enter the IPv6 address. The default IPv6 address for the gateway is fec0::1. You can change this 128-bit IPv6 address based on your network requirements.

  NOTE If you change the IP address and click **Apply**, then the browser connection is lost. Wait a few seconds to allow your administration computer to obtain a new IP address from newly assigned IP address pool (or release and renew if connected via DHCP). Then enter the new IP address of the security appliance in the Address bar of the browser, and log in again.

- **IPv6 Prefix Length:** Enter the number of characters in the IPv6 prefix.

  The IPv6 network (subnet) is identified by the prefix, which consists of the initial bits of the address. The default prefix length is 64 bits. All hosts in the network have the identical initial bits for the IPv6 address. The number of common initial bits in the addresses is set by the prefix length field.

STEP 3 In the **DHCPv6** area, enter the following information:

- **DHCP Status:** If you do not want the security appliance to act as a DHCP server, click **Disable DHCPv6 Server** (the default setting). If you want the security appliance to act as a DHCP server that dynamically assigns IP addresses to all connected devices, click **Enable DHCPv6 Server**, and then complete all fields that are highlighted with white backgrounds.

- **DHCP Mode:** Choose the appropriate option for your configuration:
  - **Stateless:** Choose this option to allow the security appliance to autoconfigure the IPv6 LAN hosts by using ICMPv6 router discovery messages. There are no managed addresses to serve the LAN nodes.

    NOTE For the stateless mode, you also need to configure the Router Advertisement Daemon (RADVD). See **Router Advertisement Daemon (RADVD), page 88**.
  - **Stateful:** Choose this option to allow the IPv6 LAN host to rely on an external DHCPv6 server to provide required configuration settings.
- **Domain Name (optional):** Enter a domain name for the DHCPv6 server.
- **Server Preference:** Enter a value from 0 to 255 to indicate the preference level for this DHCP server. DHCPv6 clients will pick up the DHCPv6 server which has highest preference value. The default is 255.
- **DNS Servers:** Choose one of the following options:
  - **Use DNS Proxy:** Check this box to enable DNS proxy on this LAN. The security appliance will act as a proxy for all DNS requests and will communicate with the DNS servers of the ISP (as configured in the WAN settings page).
  - **Use DNS from ISP:** Check this box allows the ISP to define the DNS servers (primary/secondary) for the LAN DHCP client.
  - **Use below:** Check this box to use the Primary DNS Server and the Secondary DNS Server that you enter in the fields below.
- **Lease/Rebind Time:** Enter the number of seconds that IP addresses are leased to clients. The default is 86400, which is 24 hours.

STEP 4 Click **Apply** to save your settings.

NOTE Next steps:

- **Required for stateless autoconfiguration:** If you chose stateless autoconfiguration mode, click **IPv6 > Router Advertisement** to configure the Router Advertisement Deamon (RADVD). For more information, see **Router Advertisement Daemon (RADVD), page 88**.
- If you want to configure the LAN address pools, click **IPv6 > IPv6 Address Pools**. For more information, see **IPv6 LAN Address Pools, page 82**.

- If you need to configure a LAN alias address, click **IPv6 > IPv6 Multi LAN**. For more information, see **IPv6 Multi LAN, page 83**.
- If you need to configure static routing, click **IPv6 > IPv6 Multi LAN**. For more information, see **IPv6 Static Routing, page 83**.

IPv6 LAN Address Pools

You can define the IPv6 delegation prefix for a range of IP addresses to be served by the DHCPv6 server. By using a delegation prefix, you can automate the process of informing other networking equipment on the LAN of the DHCP information for the assigned prefix.

STEP 1 Click **Networking > IPv6 > IPv6 Address Pools**.

The IPv6 Address Pools window opens. Any existing address pools are listed in the List of Available Pools table.

STEP 2 Click **Add** to create a new address pool.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the IPv6 Address Prefix & Pools Configuration window opens.

STEP 3 Enter the following information:

- **Start IPv6 Address:** Enter the first address in the range of addresses for this pool.
- **End IPv6 Address:** Enter the final address in the range of addresses for this pool.
- **IPv6 Prefix Length:** Enter the number of characters in the IPv6 prefix.

  The IPv6 network (subnet) is identified by the prefix, which consists of the initial bits of the address. All hosts in the network have the identical initial bits for the IPv6 address. The number of common initial bits in the addresses is set by the prefix length field.

STEP 4 Click **Apply** to save your settings.

IPv6 Multi LAN

You can use this page to configure an IPv6 LAN alias address.

STEP 1 Click **Networking > IPv6 > IPv6 Multi LAN**.

The IPv6 Multi LAN window opens. Any existing alias addresses are listed in the Available Multi IPv6 Addresses table.

STEP 2 Click **Add** to add a new alias address.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the IPv6 Multi LAN Configuration window opens.

STEP 3 Enter the following information:

- **IPv6 Address:** Enter the IPv6 LAN Alias address to be added.
- **Prefix Length:** Enter the prefix length of the IPv6 address.

  The IPv6 network (subnet) is identified by the prefix, which consists of the initial bits of the address. All hosts in the network have the identical initial bits for the IPv6 address. The number of common initial bits in the addresses is set by the prefix length field.

STEP 4 Click **Apply** to save your settings.

IPv6 Static Routing

STEP 1 Click **Networking > IPv6 > IPv6 Static Routing**.

The IPv6 Static Routing window opens. Any existing static routes are listed in the List of IPv6 Static Routes table.

STEP 2 Click **Add** to add a new static route.**Other options:** Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the IPv6 Static Route Configuration window opens.

STEP 3 Enter the following information:

- **Route Name:** Enter the name of the route, for identification and management purposes.
- **Active:** Check this box to enable the route, or uncheck this box to disable the route. When a route is added in inactive state, it is listed in the table, but will not be used for routing. This feature allows you to configure the routes even before the destination network is ready to receive traffic. Enable the routes when ready.
- **IPv6 Destination:** Enter the IPv6 address of the destination host or network for this route.
- **IPv6 Prefix Length:** Enter the number of prefix bits in the IPv6 address to define the subnet.
- **Interface:** Choose the physical network interface for this route (Dedicated WAN, Optional WAN, DMZ or LAN), through which this route is accessible.
- **Gateway IP Address:** Enter the IP Address of the gateway through which the destination host or network can be reached.
- **Metric:** Specify the priority of this route by entering a value between 2 and 15. If multiple routes to the same destination exist, the security appliance chooses route with the lowest metric.

STEP 4 Click **Apply** to save your settings.

Routing (RIPng)

RIPng (Routing Information Protocol - next generation, RFC 2080) is a routing protocol that uses UDP packets to exchange routing information through port 521. The distance to a destination is measured by the hop count, as follows:

- The hop count from a router to a directly connected network is 0.
- The hop count between two directly connected routers is 1.
- When the hop count is greater than or equal to 16, the destination network or host is unreachable.

By default, the routing update is sent every 30 seconds. If the security appliance receives no routing updates from a neighbor after 180 seconds, the routes learned from the neighbor are considered as unreachable. After another 240 seconds, if no routing update is received, the security appliance remove these routes from the routing table.

NOTE RIPng is disabled by default.

STEP 1 Click **Networking > IPv6 > Routing (RIPng)**.

The Routing (RIPng) window opens.

STEP 2 Check the **Enable RIPNG** box to enable RIPng. Uncheck the box to disable this protocol.

STEP 3 Click **Apply** to save your settings.

6to4 Tunneling

Automatic tunneling allows traffic from a LAN IPv6 network to be tunneled through to a WAN IPv4 network, and vice versa. You should enable this feature if you have an end site or end user that needs to connect to the IPv6 Internet using the existing IPv4 network.

STEP 1 Click **Networking > IPv6 > 6to4 Tunneling**.

The 6to4 Tunneling window opens.

STEP 2 Check the box to enable automatic tunneling, or uncheck the box to disable this feature.

STEP 3 Click **Apply** to save your settings.

IPv6 Tunnels Status

You can use this page to view information about the automatic tunnel set up through the dedicated WAN interface. The table shows two fields the name of tunnel and the IPv6 address that is created on the device.

To open this page, click **Networking > IPv6 > IPv6 Tunnels Status**.

ISATAP Tunnels

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is used to transmit IPv6 packets between dual-stack nodes over an IPv4 network. The security appliance is one endpoint (a node) for the tunnel. You must set a local endpoint as well as the ISATAP Subnet Prefix that defines the logical ISATAP subnet to configure a tunnel.

STEP 1 Click **Networking > IPv6 > ISATAP Tunnels**.

The **ISATAP Tunnels** window opens. Any existing tunnels are listed in the List of Available ISATAP Tunnels table.

STEP 2 To add an ISATAP tunnel, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the ISATAP Tunnel Configuration window opens.

STEP 3 Enter the following information:

- **ISATAP Subnet Prefix:** Enter the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet. You can get the prefix from your ISP or Internet registry, or derive it from RFC 4193.
- **Local End Point Address:** Enter the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address.
- **IPv4 Address:** Enter the local end point address if not the LAN IPv4 address.

STEP 4 Click **Apply** to save your settings.

MLD Tunnels

Multicast Listener Discovery (MLD) is an IPv6 protocol that discovers listeners for a specific multicast group. This protocol is similar to IGMP in IPv4.

STEP 1 Click **Networking > IPv6 > MLD Tunnels**.

The MLD Tunnels window opens.

STEP 2 Check the box to enable MLD when this router is in IPv6 mode. Then enter the following information:

- **Maximum query response time:** Enter the maximum amount of time (in milliseconds) that can elapse between this router sending a host-query message and the host replying back to it. By varying the Query Response Interval, an administrator can tune the burstiness of MLD messages on the link; larger values make the traffic less bursty, as host responses are spread out over a larger interval. The minimum value of this parameter is 5000 ms (5 seconds) and maximum value is 1800000 ms (30 mins).

- **Robustness Variable:** Enter a value from 2 to 8 to allow tuning for the expected packet loss on a link. Enter a higher value if a link is expected to be lossy. The default value is 2. The minimum value of Robustness Variable is 2 and maximum value is 8.

- **Query Interval:** Enter the number of seconds to elapse between General Queries sent by the device. The default value is 125 seconds. By varying the Query Interval, an administrator can tune the number of MLD messages on the link; larger values cause MLD Queries to be sent less often. The minimum value of Query interval is 100 seconds and maximum value is 1800 seconds.

STEP 3 Click **Apply** to save your settings.

Router Advertisement Daemon (RADVD)

If you configured the security appliance to use IPv4/IPv6 mode, you can configure the Router Advertisement Daemon (RADVD) on this device. The RADVD listens for router solicitations in the IPv6 LAN and responds with router advertisements as required. This is stateless IPv6 auto configuration as it distributes IPv6 prefixes to all nodes on the network.

First configure RADVD, and then add your RADVD prefixes as described in the following sections:

- **Configuring Router Advertisement**
- **Adding RADVD Prefixes**

Configuring Router Advertisement

Use this page to enable RADVD and to choose the advertise mode.

STEP 1 Click **Networking > IPv6 > Router Advertisement**.

The RADVD window opens.

STEP 2 Enter the following information:

- RADVD Status: Enable or disable the RADVD process. If you enable RADVD, complete the fields that are highlighted with white backgrounds.
- Advertise Mode: Choose one of the following modes:
  - Unsolicited Multicast: Choose this option to send router advertisements to all interfaces belonging to the multicast group. Also enter the Advertise Internal.
  - Unicast only: Choose this option to restrict advertisements to well known IPv6 addresses only (advertisements are sent only to the interface of the known address).
- Advertise Interval: If you chose Unsolicited Multicast mode, enter a value between the Minimum Router Advertisement Interval and Maximum Router Advertisement Interval. MinRtrAdvInterval = 0.33 * MaxRtrAdvInterval. The default is 30 seconds.
- RA Flags: Choose one of the following options:
  - **Managed:** Choose this option to use the administered/stateful protocol for address auto configuration.

- **Other:** Choose this option to allow the host to use the administered/ stateful protocol of other (i.e. non-address) information auto configuration.

- Router Preference: Chose **Low, Medium, or High** for the preference associated with this router's RADVD process. This setting is useful if there are other RADVD enabled devices on the LAN. The default setting is High.
- MTU: If required by your ISP, you can change this value, which is used in advertisements to ensure that all nodes on the network use the same MTU value in the cases where the LAN MTU is not well known. The default is 1500.
- Router Lifetime: Enter the lifetime in seconds of the route. The default is 3600 seconds.

STEP 3 Click **Apply** to save your settings.

Adding RADVD Prefixes

NOTE Before you can perform this procedure, you must enable RADVD. For more information, see **Configuring Router Advertisement, page 88**.

STEP 1 Click **Networking > IPv6 > Advertisement Prefixes**.

The Advertisement Prefixes window opens. Any existing prefixes appear in the List of Prefixes to Advertise table.

STEP 2 To add a prefix to the table, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries in the table, check the box at the left side of the heading row.

After you click Add or Edit, the RADVD Prefixes window opens.

STEP 3 Enter the following information:

- **IPv6 Prefix Type:** Choose whether to select the prefix type as **6to4** or **Global/Local/ISATAP**. Also complete the fields that are highlighted with white backgrounds.
- **SLA ID**. The SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent.
- **IPv6 Prefix:** Specify the IPv6 network address.

- **IPv6 Prefix Length:** Enter a decimal value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address.
- **Prefix Lifetime:** Enter the maximum number of seconds that the requesting router is allowed to use the prefix.

STEP 4 Click **Apply** to save your settings.

3

Wireless Configuration for the SA520W

This chapter describes how to configure the access points and the radio for the SA520W. It includes the following sections:.

- **Configuring an Access Point**
- **Configuring the Radio**’

NOTE The router is configured with default settings for a simple wireless network. However, you must enable the access point before any wireless devices can connect.

Configuring an Access Point

By default, your SA520W is configured with an access point named AP1, which is has the default network name of Cisco_1. The access point is enabled by default. The security profile has Open security and is identifying itself to all wireless devices that are in range. These settings make it easy for you to begin using your wireless network. However, for security purposes, it is strongly recommended that you configure each profile with the highest level of security that is supported by the wireless devices that you want to allow into your network.

You can create multiple access points to segment the wireless LAN into multiple broadcast domains. This configuration helps you to maintain better control over broadcast and multicast traffic, which affects network performance. For each access point, you can customize the security mode, the Quality of Service settings, and the radio.

Step 1: Configuring the Wireless Profiles

A wireless profile specifies the security settings. Optionally, you can configure advanced wireless settings, QoS settings, and MAC filtering. After you configure a wireless profile, you can assign it to any access point.

NOTE Cisco strongly recommends WPA2 for wireless security. Other security modes are vulnerable to attack.

STEP 1 Click **Wireless > Profiles**.

The Profiles window opens. The existing profiles appear in the List of Profiles table.

STEP 2 In the first row of the table, click the button in the **Edit** column to configure the default profile.

Other options: Click **Add** to add an entry. Click the button in the **Adv Config** column, the **QoS Config** column, or the **Configure MAC Filter** column to edit other settings (more information later in this chapter). To delete a profile, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Profile Configuration window opens.

STEP 3 Enter the following information in the **Profile Configuration** area:

- **Profile Name:** For a new profile, enter a unique (alphanumeric) identifier for this wireless profile. For the default profile, the name default1 cannot be changed.
- **Security:** Choose the type of security to be configured in this profile:
  - **OPEN:** No security. Any wireless device can connect (subject to access point ACL policy).
  - **WEP (Wired Equivalent Privacy):** WEP encryption is an older encryption method that is not considered to be secure and can easily be broken. Select this option only if you need to allow access to devices that do not support WPA or WPA2.
  - **WPA (Wi-Fi Protected Access):** WPA provides better security than WEP because it uses dynamic key encryption. This standard was implemented as an intermediate measure to replace WEP, pending final completion of the 802.11i standard for WPA2. WPA supports TKIP or

TKIP+CCMP encryption (default is TKIP) and PSK/RADIUS authentication. This option is a good choice if you need to allow access to devices that do not support WPA2.

- **WPA2:** WPA2 provides the best security for wireless transmissions. This method implements the security standards specified in the final version of 802.11i. WPA2 supports CCMP or CCMP+TKIP encryption (default is CCMP) and PSK/RADIUS authentication. WPA2 is recommended, although some devices may not support this security mode. To protect your information as it is transmitted over the airwaves, you should enable the highest level of encryption supported by your network equipment.
- **WPA + WPA2:** This mode allows both WPA and WPA2 clients to connect simultaneously. This option is a good choice to enable a higher level of security while allowing access by devices that might not support WPA2.

- **Encryption:** Select the encryption method to be used. For WPA, the choices are TKIP or TKIP+CCMP. For WPA, the choices are CCMP or CCMP+TKIP. CCMP is stronger than TKIP and is recommended. However, some wireless devices may support only TKIP.
- **Authentication:** For WPA/WPA2, select the WPA/WPA2 authentication method to be used: RADIUS, PSK, or PSK + RADIUS.
- **WPA Password:** For PSK authentication, enter a pre-shared key. The key can include up to 64 ASCII characters. The clients also need to be configured with the same password.
- **Enable Pre-Authentication:** If you chose RADIUS as the Authentication method, you can check this box to enable Pre-Authentication for this profile.
- **AP Isolation:** Check this box to create a separate virtual network for the clients that use this profile. When this feature is enabled, each client is in its own virtual network and will not be able to communicate with other clients.

STEP 4 If you chose WEP as the Security Type, enter the following information in the **WEP Index and Keys** area:

- **Authentication:** Select either **Open System** or **Shared Key** scheme. Shared key is recommended.
- **Encryption:** Select the encryption type - 64 WEP or 128 WEP. The larger size keys provide stronger encryption, thus making the key more difficult to crack (i.e. 64 WEP has a 40-bit key which is less secure than the 128 WEP which has a 104-bit key).

- **WEP Passphrase:** Choose any alphanumeric phrase (longer than 8 characters for optimal security) and click **Generate key** to generate 4 unique WEP keys. Select one of the four to use as the static key that devices must have in order to use the wireless network.
- **WEP Key 1-4:** If WEP Passphrase is not specified, a key can be entered directly in one of the WEP Key boxes. The length of the key should be 5 ASCII characters (or 10 hex characters) for 64-bit WEP and 13 ASCII characters (or 26 hex characters) for 128-bit WEP.
- **WEP Key Index:** Based on which WEP key box is used, WEP key index is derived. Different clients can have different numbering scheme for index. For clients which have indexing starting with 0, WEP Key 1 to WEP Key 4 corresponds to index 0 to 3. Clients which have indexing starting with 1, WEP Key 1 to WEP Key 4 correspond to index 1 to 4.

STEP 5 Click **Apply** to save your settings.

STEP 6 Repeat this procedure as needed to add more wireless profiles.

NOTE Next steps:

- **Required for each access point:** Configure and enable the access point. See **Step 2: Configuring the Access Points, page 98**.
- If you need to configure advanced settings, click the **Advanced Config** button in the List of Profiles table. For more information, see **Profile Advanced Configuration, page 95**.
- If you need to configure QoS settings, click the **QoS Config** button in the List of Profiles table. For more information, see **Configuring the QoS Settings for a Wireless Profile, page 95**.
- If you want to configure MAC Filtering, click the **MAC Filtering** button in the List of Available Access Points table. For more information, see **Controlling Wireless Access Based on MAC Addresses, page 96**.
- For RADIUS authentication, configure the RADIUS settings. See **Configuring RADIUS Server Records, page 193**.

Profile Advanced Configuration

STEP 1 Click **Wireless > Profiles**.

The Profiles window opens. The existing profiles appear in the List of Profiles table.

STEP 2 Find the profile that you want to edit, and click the button in the **Adv Config** column.

The Profile Advanced Configuration window opens.

STEP 3 As needed, change the following settings:

- **Group Key Refresh Interval (Seconds):** This specifies the timeout interval after which group keys are generated (only used if profile is configured with WPA or WPA2 security).
- **PMKSA Life Time (Seconds):** WPA2 security standard has an option called PMKSA caching which means that the master keys derived from successful RADIUS authentication are cached for some time to avoid long RADIUS authentication every time a client connects. This timeout interval specifies for how long this PMKSA is stored in the access point. A client reconnecting within this interval (after successful RADIUS authentication) can skip the RADIUS authentication.
- **802.1X Re-authentication Interval (Seconds):** The timeout interval after which the access point should re-authenticate with the RADIUS server.

STEP 4 Click **Apply** to save your settings.

Configuring the QoS Settings for a Wireless Profile

Quality of Service (QoS) is used to prioritize different types of traffic. It gives the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. The default QoS settings should be sufficient, but advanced users can map the DSCP/ToS values to Classes of Service, as needed.

You can choose from four Class of Service queues to prioritize the data traffic over the wireless link:

- **Voice:** Highest priority queue, minimum delay. Used typically to send time-sensitive data such as Voice over IP (VoIP).

- **Video:** High priority queue, minimum delay. Used typically to send time-sensitive data such as Video and other streaming media.
- **Best Effort:** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- **Background:** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is typically sent to this queue (FTP data, for example).

STEP 1 Click **Wireless > Profiles**.

The Profiles window opens. The existing profiles appear in the List of Profiles table.

STEP 2 Find the profile that you want to edit, and click the button in the **QoS Config** column.

The QoS Configuration window opens.

STEP 3 Enter the following settings.

- **QoS Enable:** Check this box to enable QoS for this profile. The settings on this page apply only if this box is checked.
- **Default Class Of Service:** Use this setting to specify the default Class of Service for all traffic on the access point.
- **IP DSCP/TOS to Service Mapping:** For each IP DSCP/TOS value, leave **Default** in the field to apply the selected Default Class of Service, or choose a particular Class of Service to prioritize the traffic.

STEP 4 Click **Apply** to save your settings.

Controlling Wireless Access Based on MAC Addresses

This page allows you to define specific MAC addresses to permit or deny access to the selected access point. The default is “open” access, which means that MAC filtering is not enabled. Any device can use this access point.

MAC Filtering provides additional security, but it also adds to the complexity and maintenance. Be sure to enter each MAC address correctly to ensure that the policy is applied as intended.

Before performing this procedure, decide whether you want to enter a list of addresses that will be denied access or a list that will be allowed access. Generally it is easier and more secure to use this feature to allow access to the specified MAC addresses, thereby denying access to unknown MAC addresses.

You will enter the MAC addresses into the MAC Address table first, and then set the ACL Policy Status.

IMPORTANT: Any time that you add or delete addresses from the MAC Address table, click the **Apply** button to save your settings. The policy applies only to the addresses that are in the table when you click **Apply**.

STEP 1 Click **Wireless > Access Point**.

The Access Points window opens. Existing access points are listed in the List of Available Access Points table.

STEP 2 Find the access point that you want to edit, and click the button in the **Configure MAC Filter** column.

The MAC Filtering Configuration window opens.

STEP 3 To add an address to the MAC Address table, complete the following tasks:

a. Click **Add**.

Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading. After making changes in the table, be sure to click **Apply** to apply the ACL policy to the new list.

After you click Add or Edit, the New MAC Filter window opens.

b. Enter the **MAC Address** of the device that you want to add to the table.

c. Click **Apply** to save your settings.

STEP 4 Repeat the previous step for each MAC address that you want to add to the table.

STEP 5 At the top of the MAC Filtering page, set the **ACL Policy Status**. From the list, choose one of the following options:

- **Open:** MAC filtering is not enabled. Any device can use this access point.
- **Allow:** All of the devices in the MAC Address table are allowed to use this access point. All other devices are denied access.
- **Deny:** All of the devices in the MAC Address table are prevented from using this access point. All other devices are allowed access.

STEP 6 Click **Apply** to save your settings.

Step 2: Configuring the Access Points

Use the Access Point page to configure up to four access points to allow access to your wireless network. For each access point, assign a profile, specify a Service Set Identifier (SSID) or network name, set the maximum number of clients, and, optionally, specify a schedule.

STEP 1 Click **Wireless > Access Point**.

The Access Points window opens. Existing access points are listed in the List of Available Access Points table.

STEP 2 In the first row of the table, click the button in the **Edit** column to configure the default access point.

Other options: Click **Add** to add an entry. To view the status, click the button in the **Status** column. To enable an access point, check the box and then click **Enable**. To disable an access point, check the box and then click **Disable**. To delete an access point, check the box and then click **Delete**. To select all access points, check the box in the first column of the table heading.

After you click Add or Edit, the Access Point Configuration window opens.

STEP 3 Enter the following information:

- **Profile Name:** Choose a profile, which determines the security and optional advanced settings for this access point. For more information, see **Step 1: Configuring the Wireless Profiles, page 92**.
- **Active Time:** Check this box to activate the access point only during specified hours of the day. Then enter the Start Time and Stop Time.
  - **Start Time:** Enter the hour and minute when the active period begins. Choose AM or PM from the drop-down list.
  - **Stop Time:** Enter the hour and minute when the active period ends. Choose AM or PM from the drop-down list.
- **Max Associated Clients:** Enter the maximum number of clients that can connect to this access point at any time. The default is 8 clients.

- **SSID:** Specify the Service Set Identifier, or network name, that clients use to connect to the access point. It is a good practice to replace the default SSID with a unique identifier.
- **Broadcast SSID:** Check this box to allow the security appliance to broadcast the SSID. All wireless devices within range are able to see the SSID when they scan for available networks. Uncheck this box to prevent auto-detection of the SSID. In this case, users must know the SSID to set up a wireless connection to this access point.

STEP 4 Click **Apply** to save your settings.

STEP 5 Repeat this procedure as needed to add or edit other access points within your SA520W.

NOTE Next steps:

To view the status of the access point, click the button in the List of Available Access Points table. For more information, see **Wireless Statistics for the SA520W, page 208**.

Configuring the Radio

Basic Radio Configuration

The radio card is preconfigured with standard settings. Use this page to modify the settings, as needed.

For example, you can set a manual channel for operation to resolve issues with interference from other access points in the area. You also can change the mode (g & b, g only, n only, ng) to suit the devices in your network.

STEP 1 Click **Wireless > Radio Settings > Radio Settings**.

The Radio Settings window opens.

STEP 2 Enter the following information:

- **Region:** Choose a geographic region from the drop-down list of regions.

- **Country:** Choose a country from the drop-down list of countries. This list is populated according to the region selected. This impacts the available Wi-Fi™ channels as determined by wireless authorities in the corresponding country/region.
- **Mode:** Choose the 802.11 modulation technique.
  - **g & b:** Select this mode if some devices in the wireless network use 802.11g and others use 802.11b.
  - **g only:** Select this mode if all devices in the wireless network can support 802.11g.
  - **n only:** Select this mode if all devices in the wireless network can support 802.11n.
  - **ng:** Select this mode to allow 802.11n, 802.11g and 802.11b clients to connect to this access point.
- **Channel Spacing:** Select either 20 MHz or 40 MHz channel bonding (spacing), or choose “auto” to let system determine the best channel spacing to use. This setting is specific to 802.11n traffic.
- **Control Side Band:** If you chose 40 MHz channel spacing, choose Lower Upper.
- **Current Channel:** Displays the channel currently in use by the radio.
- **Channel:** Select a channel from the list of channels or choose “auto” to let system determine the best channel to use based on the environmental noise levels for the available channels.
- **Default Transmit Power:** Enter a value in dBm as the default transmitted power level for all APs that use this radio. The default is 20 dBm.

STEP 3 Click **Apply** to save your settings.

Advanced Radio Configuration

This page is used to specify advanced configuration settings for the radio.

STEP 1 Click **Wireless > Radio Settings > Advanced Settings**.

The Advanced Radio Settings window opens.

STEP 2 Enter the following information:

- **Beacon Interval:** Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. Set the interval by entering a value in milliseconds. The default setting is 100, which means that beacon frames are sent every 100 milliseconds (10 seconds).
- **Dtim Interval:** The Delivery Traffic Information Map (DTIM) message is an element that is included in some beacon frames. It indicates the client stations that are currently sleeping in low-power mode and have buffered data on the access point awaiting pickup. Set the interval by entering a value in beacon frames. The default setting is 2, which means that the DTIM message is included in every second beacon frame.
- **RTS Threshold:** Determines the packet size that requires a Request To Send (RTS)/Clear To Send (CTS) handshake before sending. A low threshold setting can be useful in areas where many client devices are associating with the wireless device, or in areas where the clients are far apart and can detect only the access point but not other clients. Although a low threshold value consumes more bandwidth and reduces the throughput of the packet, frequent RTS packets can help the network to recover from interference or collisions. Set the threshold by entering the packet size in bytes. The default value is 2346, which effectively disables RTS.
- **Fragmentation Threshold:** Frame length that requires packets to be broken up (fragmented) into two or more frames. Setting a lower value can reduce collisions because collisions occur more often in the transmission of long frames, which occupy the channel for a longer time. Use a low setting in areas where communication is poor or where there is a great deal of radio interference. Set the threshold by entering the frame length in bytes. The default value is 2346, which effectively disables fragmentation.
- **Preamble mode:** 802.11b requires that a preamble be appended to every frame before it is transmitted through the air. The preamble can be either the traditional long preamble, which requires 192 μs for transmission, or it can be an optional short preamble that requires only 96 μs. The long preamble is needed for compatibility with the legacy 802.11 systems operating at 1 and 2 Mbps. The default is Long.

- **Protection Mode:** Select **RTS/CTS protection** if you want the security appliance to perform a RTS/CTS handshake before transmitting a packet. This mode can minimize collisions among hidden stations.
- **U-APSD:** Check this box to conserve power by enabling the Unscheduled Automatic Power Save Delivery (also referred to as WMM Power Save) feature.
- **Short Retry Limit**, **Long Retry Limit:** Enter the number of times the security appliance will retry a frame transmission that fails. Retries are used for both long and short frames, of size less than or equal to the RTS threshold.

STEP 3 Click **Apply** to save your settings.

4

Firewall Configuration

This chapter describes how to configure firewall rules that control outbound and inbound traffic and to specify other settings that protect your network. It includes the following sections:

To access the Firewall pages click *Firewall* from the Configuration Utility menu bar.

Configuring Firewall Rules to Control Inbound and Outbound Traffic

By default, your firewall prevents inbound access and allows all outbound access. If you want to allow some inbound access or prevent some outbound access, you must configure firewall rules. You can choose how and to whom the rules apply and can specify these settings:

- Services or traffic types (examples: web browsing, VoIP, other standard services and also custom services that you define)
- Direction of the traffic
- Days of the week and times of day
- Keywords in a domain name or on a URL of a web page
- MAC addresses of devices

- Port triggers

This section includes these topics:

- **Preliminary Tasks for Firewall Rules**
- **Configuring the Default Outbound Policy**
- **Configuring a Firewall Rule for Outbound Traffic**
- **Configuring a Firewall Rule for Inbound Traffic**

NOTE For detailed examples, see **Firewall Rule Configuration Examples, page 114**.

Preliminary Tasks for Firewall Rules

Depending on the firewall settings that you want to apply, you might need to complete these tasks before you can configure your firewall rule:

- If you want to create rules that apply to custom services, first create the records for the services. See **Creating Custom Services, page 104**.
- If you want to create rules that apply only on specified days and times, first create the schedules. See **Creating Schedules for a Firewall Rules, page 105**.
- If you want to use additional public IP addresses (typically assigned by your ISP) for firewall rules other than the IP address configured on the WAN interface. See **Configuring IP Aliases for WAN interfaces, page 106**.

Creating Custom Services

The security appliance is configured with a long list of standard services that you can use to configure firewall rules and port forwarding rules. (See **Appendix B, “Standard Services.”**) If you need to configure a firewall rule for a service that is not on the standard list, first you must identify the service by entering a name, specifying the type, and assigning the port range.

STEP 1 Click **Firewall > Firewall > Services**, or from the Getting Started (Advanced) page, under **Firewall and NAT Rules**, click **Configure Custom Services**.

The Custom Services window opens. Any existing custom services appear in the List of Available Custom Services table.

STEP 2 To add a custom service, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Custom Services Configuration window opens.

STEP 3 Enter the following information:

- **Name:** Enter a name for this service.
- **Type:** Specify the protocol.
  - If you choose ICMP or ICMPv6, also enter the ICMP Type.
  - If you choose TCP or UDP, also specify the port range by entering the Start Port and the Finish Port.

STEP 4 Click **Apply** to save your settings.

If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to continue with the list of configuration tasks under **Firewall and NAT Rules**.

Creating Schedules for a Firewall Rules

You can create a schedule and then apply it to one or more firewall rules. For example, to create a firewall rule that applies only on the weekend, you could create a schedule named Weekend that is active all day on Saturday and Sunday.

For more information about the time settings for your security appliance, see **Configuring the Time Settings, page 184**.

STEP 1 Click **Firewall > Firewall > Schedules**, or from the Getting Started (Advanced) page, under Firewall and NAT Rules, click **Configure Schedules (Optional)**.

The Firewall Schedules window opens. Any existing schedules appear in the List of Available Schedules table.

STEP 2 To create a new schedule, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Schedules window opens.

STEP 3 Enter the following information:

- **Schedule Name:** Enter a name for the schedule. The name will appear in the Select Schedule drop-down list on the Firewall Rule Configuration page.
- **Scheduled Days:** From the drop-down list, choose **All Days** or **Specific Days**. If you choose **Specific Days**, also check the days for this schedule.
- **Schedule Time of Day:** From the drop-down list, choose **All Day** or **Specific Times**. If you choose **Specific Times**, also enter the **Start Time** and the **End Time** by entering the hour, minute, and AM or PM.

STEP 4 Click **Apply** to save your settings.

If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to continue with the list of configuration tasks under **Firewall and NAT Rules**.

Configuring IP Aliases for WAN interfaces

IP aliases are useful when you have additional public IP address provided by your ISP and you want to these addresses to reach devices on your local network.

STEP 1 Click **Networking > WAN > IP Alias**.

STEP 2 To add IP Aliases, click **Add.**

STEP 3 Choose the **WAN** interface from the Interface drop-down menu. This is the interface where you will add the IP address to.

STEP 4 Click **Apply** to save your settings.

Configuring the Default Outbound Policy

The default outbound policy is used whenever there is no specified firewall rule that applies to the source, destination, service, or other characteristics of the outbound traffic. This policy applies to all traffic that is directed from the LAN to the WAN.

STEP 1 Click **Firewall > Firewall > Default Outbound Policy**.

STEP 2 Select **Allow Always** to allow outbound traffic, or choose **Block Always** to block outbound traffic.

STEP 3 Click **Apply** to save your settings.

NOTE Next steps:

- To configure a firewall rule for outbound traffic, see **Configuring a Firewall Rule for Outbound Traffic, page 107**.
- To configure a firewall rule for outbound traffic, see **Configuring a Firewall Rule for Inbound Traffic, page 110**.

Configuring a Firewall Rule for Outbound Traffic

This procedure explains how to configure a firewall rule for the following traffic flows:

- From the LAN to the WAN
- From the LAN to the DMZ
- From the DMZ to the WAN

For examples, see **Firewall Rule Configuration Examples, page 114**.

NOTE In addition to firewall rules, there are two other methods for controlling access to the Internet:

- You can allow access to approved websites. For more information, see **Configuring Approved URLs to Allow Access to Websites, page 126**.
- You can block URLs that contain specified keywords. For more information, see **Configuring Blocked URLs to Prevent Access to Websites, page 127**.

STEP 1 Click **Firewall > Firewall > IPv4 Rules** or **IPv6 Rules**, or for IPv4 rules, you can use the Getting Started (Advanced) page. In the **Firewall and NAT Rules** section, click **Configure Firewall and NAT Rules**.

STEP 2 The Firewall Rules window opens. Any existing rules appear in the List of Available Firewall Rules table.

For IPv4 rules, you can view the list of available rules by zone. Choose the source and destination from the **From Zone** and **To Zone** drop-down menus and click **Display Rules**.

STEP 3 To add a rule, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To change the status of a rule, check the box and then click **Enable** or **Disable**. To select all entries, check the box in the first column of the table heading.

The IPv4 Firewall Rules page includes the option to move a rule up, move a rule down, or move it to a specified location in the firewall rules list. For more information, see **Prioritizing Firewall Rules, page 113**.

If you click **Add** or **Edit**, the Firewall Rules Configuration window opens.

STEP 4 In the **Firewall Rule Configuration** area, enter the following information:

- **From Zone:** Chose the source of the traffic that is covered by this rule. For an outbound rule, choose **SECURE (LAN)** if the traffic is coming from your LAN users or choose **DMZ** if the traffic is coming from a server on your DMZ.
- **To Zone:** For an outbound rule, choose **INSECURE (WAN)** if the traffic is going to the Internet, or choose **DMZ** if the traffic is going to a server on your DMZ.
  - If the From Zone is the WAN, the To Zone can be the public DMZ or secure LAN.

  - If the From Zone is the LAN, then the To Zone can be the public DMZ or insecure WAN.

- **Service**: Choose from a list of common services or a custom defined service. For more information, see **Appendix B, “Standard Services”** and **Creating Custom Services, page 104**.

- **Action:** Choose how and when to apply the rule.

- **Select Schedule:** If you choose one of the “by schedule” actions, choose a schedule from the list.

  For more information about schedules, see **Creating Schedules for a Firewall Rules, page 105**.

- **Source Hosts**: You can apply the rule to all users or you can specify users by entering an IP address or address range.

  - If you choose Single Address, enter an IP address in the **From** field.

  - If you choose Address Range, enter the first address in the **From** field and enter the last address in the **To** field.

- **Destination Hosts**: You can apply the rule to all users or you can specify users by entering an IP address or address range.

  - If you choose Single Address, enter an IP address in the **From** field.

  - If you choose Address Range, enter the first address in the **From** field and enter the last address in the **To** field.

- **Log:** You can choose whether or not to log the packets for this rule. Click **Never** if you do not want to log the packets, or click **Always** to log the packets.

- **QoS Priority:** You can use this rule to prioritize traffic. Each priority level corresponds to a Term of Service (ToS) value.

  - **Normal-Service:** ToS=0 (lowest QoS)

  - **Minimize-Cost:** ToS=1

  - **Maximize-Reliability:** ToS=2

  - **Maximize-Throughput:** ToS=4

  - **Minimize-Delay:** ToS=8 (highest QoS)

STEP 5 For a LAN to WAN rule only, enter the following information in the **Source NAT Settings** area:

- **SNAT IP Type:** Source Network Address Translation (SNAT) requires re-writing the source or destination IP address of incoming IP packets as they pass through the firewall. Choose one of the following options:
  - **WAN Interface Address:** Choose this option to use the IP address of the WAN interface.
  - **Single Address:** Choose this option to map outbound traffic to an external IP address (usually provided by your ISP), and select the IP alias configured for the WAN interface. If no IP alias is configured, the list is empty.

STEP 6 Click **Apply** to save your settings.

Configuring a Firewall Rule for Inbound Traffic

This procedure explains how to configure a firewall rule for the following traffic flows:

- From the WAN to the LAN
- From the WAN to the DMZ
- From the DMZ to the LAN

If you want to allow incoming traffic, you must make the security appliance's WAN port IP address known to the public. This is called "exposing your host." However, this public IP address does not necessarily have to be your WAN address. The security appliance supports multiple public IP addresses on a single WAN interface. When you create your firewall rule, you can choose whether to associate the public service with the dedicated WAN address, the optional WAN address, or another IP address that your ISP has provided to you.

For examples, see **Firewall Rule Configuration Examples, page 114**.

NOTE In addition to configuring firewall rules, you can use the following methods to control inbound traffic:

- You can prevent common types of attacks. For more information, see **Configuring Attack Checks, page 118**.

- You can allow or block traffic from specified MAC addresses. For more information, see **Configuring MAC Filtering to Allow or Block Traffic, page 119**
- You can associate IP addresses with MAC addresses to prevent spoofing. For more information, see **Configuring IP/MAC Binding to Prevent Spoofing, page 128**

STEP 1 Click **Firewall > Firewall > IPv4 Rules** or **IPv6 Rules**, or for IPv4 rules, you can use the Getting Started (Advanced) page. In the **Firewall and NAT Rules** section, click **Configure Firewall and NAT Rules**.

The Firewall Rules window opens. Any existing rules appear in the List of Available Firewall Rules table.

For IPv4 rules, you can view the list of available rules by zone. Choose the source and destination from the **From Zone** and **To Zone** drop-down menu and click **Display Rules**.

STEP 2 To add a rule, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To change the status of a rule, check the box and then click **Enable** or **Disable**. To select all entries, check the box in the first column of the table heading.

The IPv4 Firewall Rules page includes the option to move a rule up, move a rule down, or move it to a specified location in the firewall rules list. For more information, see **Prioritizing Firewall Rules, page 113**.

If you click **Add** or **Edit**, the Firewall Rules Configuration window opens.

STEP 3 In the **Firewall Rule Configuration** area, enter the following information:

- **From Zone:** Chose the source of the traffic that is covered by this rule. For an inbound rule, choose **INSECURE (WAN)** if the traffic is coming from the Internet or choose **DMZ** if the traffic is coming from a server on your DMZ.
- **To Zone:** For an inbound rule, choose **SECURE (LAN)** if the traffic is going to the LAN, or choose **DMZ** if the traffic is going to a server on your DMZ.
  - If the From Zone is the WAN, the To Zone can be the public DMZ or secure LAN.
  - If the From Zone is the LAN, then the To Zone can be the public DMZ or insecure WAN.

- **Service**: Choose from a list of common services or a custom defined service. For more information, see **Appendix B, "Standard Services"** and **Creating Custom Services, page 104**.
- **Action:** You can choose to block or to allow and to apply the rule always or only on a specified schedule. Choose BLOCK always, ALLOW always, BLOCK by schedule, or ALLOW by schedule.
- **Select Schedule:** If you choose one of the "by schedule" actions, choose a schedule from the list.

  For more information about schedules, see **Creating Schedules for a Firewall Rules, page 105**.
- **Source Hosts**: You can apply the rule to all users or you can specify users by entering an IP address or address range.
  - If you choose Single Address, enter an IP address in the **From** field.
  - If you choose Address Range, enter the first address in the **From** field and enter the last address in the **To** field.
- **Destination Hosts** (available only if the traffic flow is from DMZ to LAN**)**: You can apply the rule to all users or you can specify users by entering an IP address or address range.
  - If you choose Single Address, enter an IP address in the **From** field.
  - If you choose Address Range, enter the first address in the **From** field and enter the last address in the **To** field.
- **Local Server:** Shows the IP address of the local server (only applies to IPv4 Firewall rules.)
- **Log:** You can choose whether or not to log the packets for this rule. Click **Never** if you do not want to log the packets, or click **Always** to log the packets.

STEP 4 For a WAN-to-LAN or a WAN-to-DMZ rule, enter the following information in the **Destination NAT Settings** area:

- **Internal IP Address:** Enter the IP address of the server that is hosting the service.
- **Enable Port Forwarding:** Check the box to forward traffic to a particular port.
- **Translate Port Number:** If you enabled port forwarding, enter the port number that will be the destination for the forwarded traffic.

- **External IP Address:** Select one of the following options to specify the IP address that is exposed to the public:
  - **Dedicated WAN:** The public will connect to this service by using the IP address that is associated with your WAN interface.
  - **Optional WAN:** The public will connect to this service by using the IP address that is associated with the WAN interface on the Optional port.
  - **Other:** The public will connect to this service by using another IP address that your ISP has provided to you. If you choose this option, enter the address in the **Other IP Address** field.

STEP 5 Click **Apply** to save your settings.

The firewall rule appears on the Firewall Rules page.

Prioritizing Firewall Rules

If a firewall policy contains more than one rule that permits traffic, you can reorder them by priority. You can move a rule up, move a rule down, or move it to a specified location in the firewall rules list.

NOTE This feature only applies to IPv4 firewall rules.

STEP 1 Click **Firewall > Firewall > IPv4 Rules**, or you can use the Getting Started (Advanced) page. In the **Firewall and NAT Rules** section, click **Configure Firewall and NAT Rules**.

The IPv4 Firewall Rules window opens.

The firewall rules appear in the List of Available Firewall Rules table. The list includes all firewall rules for controlling traffic from a particular zone to a particular destination.

STEP 2 To view the list of rules belonging to the same group, choose the source and destination from the **From Zone** and **To Zone** drop-down menus and click **Display Rules**. Only the rules for the specified security zones appear.

For example: If you choose WAN and LAN from the Zone drop-down menus, only the rules for the WAN to LAN security zones appear.

STEP 3 To reorder the rules, click **Move**.

The Move Firewall Rules window opens.

STEP 4 In the List of Available Firewall Rules table, check the box next the rule you want to reorder and select one of the following:

- **MoveUp**: Moves the rule up one position.
- **MoveDown**: Moves the rule down one position.
- **Move To**: Moves the rule to a specified location. Enter the target index number to move the selected rule to.

  For example: A target index of 2 moves the rule to position 2 and moves the other rules down to position 3 in the list.

STEP 5 When finished, you are returned to the IPv4 Firewall Rules page.

STEP 6 Verify that the rules were reordered by choosing the appropriate source and destination the Zone drop-down menus and click **Display Rules.**

Firewall Rule Configuration Examples

Allowing Inbound Traffic to a Web Server Using the WAN IP Address

Situation: You host a public web server on your DMZ. You want to allow inbound HTTP requests from any outside IP address. The inbound traffic is addressed to your WAN IP address but is directed to a web server.

Solution: Create an inbound rule as follows:

Parameter	Value
From Zone	Insecure (WAN1)
To Zone	DMZ
Service	HTTP
Action	ALLOW always
Source Hosts	Any
Internal IP Address	192.168.5.2
External IP Address	Dedicated WAN

Allowing Inbound Traffic to a Web Server Using a Specified Public IP Address

Situation: You host a public web server on your local DMZ network. You want to allow inbound HTTP requests from any outside IP address. Your ISP has provided a static IP address that you want to expose to the public as your web server address.

Solution: Add the static IP address (provided by the ISP), to the WAN interface as an alias and create an inbound rule as For information about configuring aliases, see **Configuring IP Aliases for WAN interfaces, page 106**.

Parameter	Value
From Zone	Insecure (WAN1)
To Zone	DMZ
Service	HTTP
Action	ALLOW always
Source Hosts	Any
Internal IP Address	192.168.5.2
External IP Address	Dedicated WAN-209.165.201.225

Allowing Inbound Traffic from Specified Range of Outside Hosts

Situation: You want to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses (132.177.88.2 - 132.177.88.254).

Solution: Create an inbound rule as shown below. In the example, connections for CU-SeeMe (an Internet video-conferencing client) are allowed only from a specified range of external IP addresses.

Parameter	Value
From Zone	INSECURE (Dedicated WAN/Optional WAN)
To Zone	Secure (LAN)
Service	CU-SEEME:UDP

Parameter	Value
Action	ALLOW always
Source Hosts	Address Range
From	132.177.88.2
To	134.177.88.254
Send to Local Server (DNAT IP)	192.168.75.11 (internal IP address)

Blocking Outbound Traffic By Schedule and IP Address Range

Use Case: Block all weekend Internet usage if the request originates from a specified range of IP addresses.

Solution: Set up a schedule called “Weekend” to define the time period when the rule is in effect. Configure an outbound rule that applies to traffic from marketing group, which has an IP address range of 10.1.1.1 to 10.1.1.100.

Parameter	Value
From Zone	Secure (LAN)
To Zone	INSECURE (Dedicated WAN/Optional WAN)
Service	HTTP
Action	BLOCK by schedule
Schedule	Weekend
Source Hosts	Address Range
From	10.1.1.1
To	10.1.1.100
Destination Hosts	Any

Blocking Outbound Traffic to an Offsite Mail Server

The following rule blocks access to the SMTP service to prevent a user from sending email through an offsite mail server.

Parameter	Value
From Zone	Secure (LAN)
To Zone	INSECURE (Dedicated WAN/Optional WAN)
Service	SMTP
Action	BLOCK Always
Source Hosts	Any

Using Other Tools to Prevent Attacks, Restrict Access, and Control Inbound Traffic

In addition to firewall rules, the security appliance provides a number of other tools to help you to protect your network from undesired inbound traffic.

- **Configuring Attack Checks**
- **Configuring MAC Filtering to Allow or Block Traffic**
- **Configuring IP/MAC Binding to Prevent Spoofing**
- **Configuring a Port Triggering Rule to Direct Traffic to Specified Ports**

Configuring Attack Checks

Use this page to specify how you want to protect your network against common types of attacks including discovery, flooding, and echo storms.

STEP 1 Click **Firewall > Attacks**. The *Attack Checks* window opens.

STEP 2 In the **WAN Security Checks** area, check the box for each feature that you want to enable:

- **Block Ping to WAN interface:** Check this box to prevent attackers from discovering your network through ICMP Echo (ping) requests. Cisco recommends that you uncheck this box only if you need to allow the security appliance to respond to pings for diagnostic purposes.

  This setting is overridden in these cases:

  - A firewall rule that directs ping requests to a particular computer on the LAN. See **Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 103**.
  - WAN Mode settings that ping specified IP addresses for failure detection. See **Configuring Auto-Rollover, Load Balancing, and Failure Detection, page 57**.

- **Enable Stealth Mode:** Check this box to prevent the security appliance from responding to port scans from the WAN. In Stealth Mode, your network is less susceptible to discovery and attacks.

- **Block TCP Flood:** Check this box to drop all invalid TCP packets. This feature protects your network from a SYN flood attack, in which an attacker sends a succession of SYN (synchronize) requests to a target system.

STEP 3 In the **LAN Security Checks** section, check the **Block UDP Flood** box to prevent the security appliance from accepting more than 25 simultaneous, active UDP connections from a single computer on the LAN.

STEP 4 In the **ICSA Settings** area, enter the following information:

- **Block ICMP Notification:** Check this box to silently block without sending an ICMP notification to the sender. Some protocols, such as MTU Path Discovery, require ICMP notifications.

- **Block Fragmented Packets:** Check this box to block fragmented packets from ANY to ANY.

- **Block Multicast Packets:** Check this box to block multicast packets.

STEP 5 In the **DoS Attacks** area, enter the following information:

- **SYN Flood Detect Rate (max/sec):** Enter the maximum number of SYN packets per second that will cause the security appliance to determine that a SYN Flood Intrusion is occurring. This value can range between 1 and 10,000 packets per second. The default is 128 SYN packets per second.
- **Echo Storm (ping pkts/sec):** Enter the number of pings per second that will cause the security appliance to determine that an echo storm intrusion event is occurring. Echo storm intrusion events are not blacklisted. This value can range between 1 and 10,000 ping packets per second. The default is 15 ping packets per second.
- **ICMP Flood [ICMP pkts./sec]:** Enter the number of ICMP packets per second, not including PING packets, that will cause the security appliance to determine that an ICMP flood intrusion event is occurring. ICMP flood events are not blacklisted. This value can range between 1 and 10,000 ICMP packets per second. The default is 100 ICMP packets per second.

STEP 6 Click **Apply** to save your settings.

Configuring MAC Filtering to Allow or Block Traffic

You can restrict (block or allow) traffic to the WAN and DMZ from the LAN based on the MAC address of the device. The first step is to populate the list of MAC addresses to be covered by the filtering policy. You can configure the policy either to block all MAC addresses in the list and permit the rest, or to permit only the configured MAC addresses and block the rest.

STEP 1 Click **Firewall > MAC Filtering > MAC Filtering**. The Source MAC Filter window opens.

Before you can add any addresses to the table, you must check the box to enable MAC filtering, and then click **Apply.**

STEP 2 In the **MAC Filtering Enable** area, enter the following information:

- **Enable MAC Address Filtering?:** Check the box to enable Source MAC Address Filtering.
- **Policy for MAC Addresses listed below:** Choose one of the following options:

- **Block and permit the rest:** All addresses in the MAC Addresses table are blocked. All other addresses are allowed.
- **Permit and block the rest:** All addresses in the MAC Addresses table are permitted. All other addresses are blocked.
- Click **Apply** to save your settings.

STEP 3 To add a MAC address to the table, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the MAC Filtering Configuration window opens.

STEP 4 Enter the MAC Address.

STEP 5 Click **Apply** to save your settings.

Configuring IP/MAC Binding

IP/MAC Binding allows you to bind IP addresses to a MAC address and vice-versa. Some systems are configured with static addresses. To prevent the user from changing static IP addresses, the router needs to enable IP/MAC Binding. If the router sees packets with matching IP addresses but inconsistent MAC addresses or vice-versa, it will drop these packets.

STEP 1 Click **Firewall > MAC Filtering > IP/MAC Binding**. The IP/MAC Binding window opens.

All currently defined rules appear in the IP/MAC Binding table.

STEP 2 To add a new IP/MAC rule, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To change the status of a rule, check the box and then click **Enable** or **Disable**. To select all entries, check the box in the first column of the table heading.

STEP 3 If you click **Add** or **Edit**, the IP MAC Binding Configuration window opens.

STEP 4 Enter the following information:

- **Name:** Specify a unique name for this rule.
- **MAC Address:** Specify the MAC address for this rule.
- **IP Address**: Specify the IP address for this rule.
- **Log Dropped Packets**: Choose whether to Enable or Disable dropped packets.

STEP 5 Click **Apply** to save your changes.

The new rule appears in the IP/MAC Binding table.

Port Triggering

Port triggering opens an incoming port for a specified type of traffic on a defined outgoing port. When a LAN device makes a connection on one of the defined outgoing ports, the security appliance opens the specified incoming port to support the exchange of data. When the exchange is completed, the ports are closed.

Port triggering is more flexible than the static port forwarding that you can configure in a firewall rule. Port triggering rules do not have to reference specific LAN IP addresses or IP addresses ranges. In addition, the ports are not left open when they are not in use, thereby providing a level of security that static port forwarding does not offer.

Port triggering is required for some applications. Such applications require that, when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The security appliance must send all incoming data for that application only on the required port or range of ports. The gateway has a list of common applications and games with corresponding outbound and inbound ports to open. You can also specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled. See **Appendix B, “Standard Services.”**

NOTE Port triggering is not appropriate for servers on the LAN, since the LAN device must make an outgoing connection before an incoming port is opened.

Configuring a Port Triggering Rule to Direct Traffic to Specified Ports

STEP 1 Click **Firewall > Port Triggering > Port Triggering**. The Port Triggering window opens.

The Port Triggering window opens. Any existing rules are listed in the List of Available Port Triggering Rules table.

STEP 2 To add a new port triggering rule, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Port Triggering Configuration window opens.

STEP 3 In the **Port Triggering Rule** area, enter the following information:

- **Name:** Enter a name for this rule.
- **Enable:** Check this box to enable this rule.
- **Protocol:** Choose the protocol (TCP or UDP).
- **Interface**: Choose the interface (LAN or DMZ).

STEP 4 In the **Outgoing (Trigger) Port Range** area, enter the Start Port and End Port to specify the outgoing port range for this rule.

STEP 5 In the Incoming (Response) Port Range area, enter the Start Port and End Port to specify the incoming port range for this rule.

STEP 6 Click **Apply** to save your settings.

Viewing the Port Triggering Status

The Port Triggering Status page provides information on the ports that have been opened as per the port triggering configuration rules. The ports are opened dynamically whenever the security appliance detects traffic that matches a port triggering rule.

To view this page, click **Firewall > Port Triggering > Port Triggering Status**. The following information appears:

- **LAN/DMZ IP Address:** Displays the LAN IP address of the device which caused the ports to be opened.
- **Open Ports:** Displays the ports that have been opened so that traffic from WAN destined to the LAN IP address can flow through the security appliance.
- **Time Remaining:** This field displays the time for which the port will remain open when there is no activity on that port. The time is reset when there is activity on the port.

Configuring Session Settings to Analyze Incoming Packets

Use this page to configure how incoming packets are analyzed.

STEP 1 Click **Firewall > Session Setting**.

The Session Settings window opens.

STEP 2 Enter the following information:

- **Maximum Unidentified Sessions:** This value defines the maximum number of unidentified sessions for the ALG identification process. This value can range between 2 and 128. The default is 32 sessions.
- **Maximum Half Open Sessions:** The gateway preserves resources by limiting the number of half-open sessions at any given time. A half-open session is the session state between receipt of a SYN packet and the SYN/ACK packet. Under normal circumstances, a session is allowed to remain in the half-open state for 10 seconds. The maximum value can range between 0 and 3,000. The default is 1,024 sessions.
- **TCP Session Timeout Duration (seconds):** Inactive TCP sessions are removed from the session table after this duration. Most TCP sessions terminate normally when the RST or FIN flags are detected. This value can range between 0 and 4,294,967 seconds. The default is 1,800 seconds (30 minutes).
- **UDP Session Timeout Duration (seconds):** Inactive UDP sessions are removed from the session table after this duration. This value can range between 0 and 4,294,967 seconds. The default is 120 seconds (2 minutes).
- **Other Session Timeout Duration (seconds):** Inactive non-TCP/UDP sessions are removed from the session table after this duration. This value can range between 0 and 4,294,967 seconds. The default is 60 seconds.

- **TCP Session Cleanup Latency (seconds):** Maximum time for a session to remain in the session table after detecting both FIN flags. This value can range between 0 and 4,294,967 seconds. The default is 10 seconds.

STEP 3 Click **Apply** to save your settings.

Using Other Tools to Control Access to the Internet

The gateway offers some standard web filtering options to allow the admin to easily create internet access policies between the secure LAN and insecure WAN. Instead of creating policies based on the type of traffic (as is the case when using firewall rules), web based content itself can be used to determine if traffic is allowed or dropped.

Refer to the following topics:

- **Configuring Content Filtering to Allow or Block Web Components**
- **Configuring Approved URLs to Allow Access to Websites**
- **Configuring Blocked URLs to Prevent Access to Websites**
- **Configuring IP/MAC Binding to Prevent Spoofing**

Configuring Content Filtering to Allow or Block Web Components

The security appliance supports a content filtering option that you can use to block access to certain Internet sites. Up to 32 key words can be specified for filtering. The type of keywords you can specify include website URL, newsgroup name, etc.

STEP 1 Click **Firewall > Content Filtering > Content Filtering**.

The Content Filtering window opens.

STEP 2 In the **Content Filtering Enable** area, enable or disable the following:

- **Enable Content Filtering:** Check the box to enable content filtering. Enable this feature when you want to configure and use features such as a list of Trusted Domains, keyword filtering, and so on.

- **Enable Check Referrer:** Check the box to check the HTTP referrer header when allowing access to URLs that match keywords. When enabled, this feature allows access to links that are referred to on a website, but do not match the name of the domain of the main page.
- **HTTP Ports:** Enter the HTTP ports on which content filtering will act. The default port is 80. If your networking using an external HTTP proxy server which listens on other ports, they can be added here. Multiple ports can be specified in a comma separated list.

STEP 3 In the **Web Components** area, check the box for any component that you want to block. Certain commonly used web components can be blocked for increased security. Some of these components can be used by malicious websites to infect computers that access them.

- **Proxy**: Check this box to proxy servers, which can be used to circumvent certain firewall rules and thus present a potential security gap.

  For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective.

- **Java**: Check this box to block Java applets that can be downloaded from pages that contain them.

  Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computer

- **ActiveX**: Check this box to prevent ActiveX applets from being downloaded through Internet Explorer.

  Similar to Java applets, ActiveX controls are installed on a Windows computer while running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers.

- **Cookies:** For added security, check this box to block cookies.

  Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option filters out cookies from being created by a website.

STEP 4 Click **Apply** to save your settings.

Configuring Approved URLs to Allow Access to Websites

Use this page to create a list of websites that your users are allowed to access. You can specify exact domain names or keywords.

NOTE This page is available only if you enabled Content Filtering. See **Configuring Content Filtering to Allow or Block Web Components, page 124**.

STEP 1 Click **Firewall > Content Filtering > Approved URLs**.

The Approved URLs window opens.

STEP 2 In the **Approved URLs List Enable** area, enable or disable this feature:

a. **Do you want to Enable Approved URLs List?:** Check the box to enable the list of approved URLs, or uncheck the box to disable this feature.

b. Click **Apply** to save your settings.

STEP 3 To add a domain name or keyword to the Approved URLs List, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Approved URL Configuration window opens.

STEP 4 Enter the following information:

- **URL:** Enter the domain name or keywords for a website that you want to approve. Separate multiple entries with semicolons (;).
- **Match Type:** Specify the method for applying this rule:
  - **Website:** Choose this option to allow access only to the exact URL that you entered in the URL box. For example, if you entered *www.yahoo.com*, then your users can access www.yahoo.com, but they will be blocked from www.yahoo.com.uk or www.yahoo.co.jp.
  - **URL keyword:** Choose this option to allow access to any URL that contains the keyword that you entered in the URL box. For example, if you entered *yahoo*, then your users can access websites such as www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk, and www.yahoo.co.jp.

STEP 5 Click **Apply** to save your settings.

Configuring Blocked URLs to Prevent Access to Websites

Use this page to create a list of websites that your users are prevented from accessing. You can specify exact domain names or keywords.

NOTE This page is available only if you enabled Content Filtering. See **Configuring Content Filtering to Allow or Block Web Components, page 124**.

STEP 1 Click **Firewall > Content Filtering > Blocked URLs**.

The Blocked URLs window opens.

STEP 2 To add a domain name or keyword to the Blocked URLs List, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Blocked URLs Configuration window opens.

STEP 3 Enter the following information:

- **URL:** Enter the domain name or keywords for a website that you want to approve. Separate multiple entries with semicolons (;).
- **Match Type:** Specify the method for applying this rule:
  - **Website:** Choose this option to block access to the domain name exactly as shown. For example, if you enter *www.yahoo.com* for the URL, then your users are prevented from accessing www.yahoo.com, but they can access www.yahoo.com.uk or www.yahoo.co.jp.
  - **URL Keyword:** Choose this option to block access to any website with a domain name that contains the configured keyword. For example, if you enter *yahoo* for the URL, then your users are prevented from accessing websites such as www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk, and www.yahoo.co.jp.

STEP 4 Click **Apply** to save your settings.

Configuring IP/MAC Binding to Prevent Spoofing

You can use IP/MAC binding to allow traffic from the LAN to the WAN only when the host has an IP address that matches a specified MAC address. By requiring the gateway to validate the source traffic's IP address with the unique MAC address of device, the administrator can ensure that traffic from the specified IP address is not spoofed. In the event of a violation (the traffic's source IP address doesn't match up with the expected MAC address having the same IP address), the packets will be dropped and can be logged for diagnosis.

STEP 1 Click **Firewall > MAC Filtering > IP/MAC Binding**.

The IP/MAC Binding window opens.

STEP 2 To add an IP/MAC binding to the table, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the IP MAC Binding Configuration window opens.

STEP 3 Enter the following information:

- **Name:** Enter a name for this IP/MAC binding.
- **MAC Address:** Enter the MAC address.
- **IP Address:** Enter the IP address.
- **Log Dropped Packets:** Choose **Enable** to keep a log of all packets that are dropped as a result of this security feature. Otherwise, choose **Disable**.

  NOTE After you enable the logging, you can view these logs by clicking **Status** on the menu bar, and then clicking **View Log > View All Logs**.

STEP 4 Click **Apply** to save your settings.

SIP

SIP ALG (Session Initiation Protocol Application-level gateway) can rewrite information within the SIP messages (SIP headers and SDP body) to make signaling and audio traffic between the client behind NAT and the SIP endpoint possible.

NOTE SIP-ALG should be enabled when voice devices such as the UC 500 or SIP phones are connected to the network behind the security appliance.

STEP 1 Click **Firewall > SIP**.

The SIP ALG window opens.

STEP 2 Check the box to enable SIP ALG support or uncheck the box to disable this feature. If this feature is disabled, the router will not allow incoming calls to the UAC (User Agent Client) behind the router.

STEP 3 Click **Apply** to save your settings.

5

Intrusion Prevention System

The SA500 Series uses an Intrusion Prevention System (IPS) to protect the security zones for a given set of categories. IPS monitors network traffic for malicious or unwanted behavior on the device and can react, in real-time, to block or prevent those activities.

When an attack is detected, offending packets are dropped or alerts are logged depending on the administrative settings, but all other traffic is unaffected. Unlike traditional firewalls, an IPS makes access control decisions based on application content, rather than IP address or ports.

You can configure IPS to protect network services such as web, instant messaging applications, email, file transfer, Windows services and DNS. It also protects applications against vulnerabilities such as viruses and worms, peer-to-peer (P2P) applications, and backdoor exploits.

This chapter describes how to configure the IPS features. It includes the following sections:

- **Configuring IPS**
- **Configuring the IPS Policy**
- **Configuring the Protocol Inspection Settings**
- **Configuring Peer-to-Peer Blocking and Instant Messaging**

To access the IPS pages click *IPS* from the Configuration Utility menu bar.

Configuring IPS

You configure IPS from the IPS Setup page. From this page you can enable IPS for the security zone you want to protect (LAN or DMZ), update the IPS signatures, and view the IPS status.

STEP 1 Click **IPS > IPS Setup**, or from the Getting Started (Advanced) page, under Intrusion Prevention System, click **Update Signatures**.

The IPS Configuration window opens.

- **IPS Enable**: By default, IPS is disabled. To enable IPS for a particular zone, select either LAN or DMZ or both for the zone(s) that you want to protect. For example: Enabling IPS protection on the LAN zone enforces IPS on all incoming and outgoing LAN traffic.

  Click **Apply** to save your settings.

- **IPS Status**: Displays the IPS Signatures status including the IPS license expiration date, the signature file version, and the date that the security device last checked for signature updates.

  - Click the **View IPS Logs** link to view the IPS log messages. To display messages generated by IPS, you must choose IPS as the facility. For more information see **Active Users, page 213**.

- **Automatic Signature Updates:** IPS uses signature files to identify an attack in progress. You can configure the security appliance to automatically update the IPS signatures when they become available.

  - To enable the auto update option, check the **Automatically Update Signatures** box.

    Enter your Cisco.com **User Name** and **Password** to authenticate to the signature update server. These credentials are only required once. Click **Apply** to save your settings.

    NOTE The Cisco username and password details once applied are applicable to all other services on the router which use them. For example, the Cisco username and login used in Administration is automatically updated for IPS signature downloads.

  - Click **Update Now** to immediately update new signatures if they are available. This option is only active if the Automatically Update Signature box is checked.

  - Click **Reset** to revert to the previous settings.

- **Manual Signature Updates**: To manually update the latest signature file, click the Cisco.com link to obtain the file and download it to your computer. Browse to the location of the signature file on the local PC and then click **Upload**.

Configuring the IPS Policy

You can configure the IPS Policy settings to protect the network against threats such as Denial-of-Service attacks, malware, and backdoor exploits.

STEP 1 Click **IPS > IPS Policy**, or from the Getting Started (Advanced) page, under Intrusion Prevention System, click **Configure and Enable IPS Policies.**

STEP 2 Choose the policy for each category or for each signature within each category.

- To select a policy for an IPS category, click an option in the category heading row.
- To expand the signatures under a category, click the **+** button next to the category heading. To hide the signatures, click the **-** button.
- To select a policy for an individual signature, click an option in the entry row for that signature.

Options:

- **Disabled**: Choose this option to disable checking for this category.
- **Detect Only**: Choose this option to check for attacks on this category and to log a message upon detection.This option is mostly used for troubleshooting purposes.
- **Detect and Prevent**: Choose this option to check for and prevent attacks on this category. Upon detection, a message is logged and a preventative action is taken.

  For IPS messages to be logged, you must configure IPS as the facility. For more information, see **Logs Facility and Severity, page 189**.

STEP 3 Click **Apply** to save your settings.

Configuring the Protocol Inspection Settings

You can configure the Protocol Inspection settings to detect suspicious behavior and attacks on various types of protocols.

STEP 1 Click **IPS> IPS Protocol Inspection**.

STEP 2 Choose the inspection settings for each category or for each signature within each category.

- To select an inspection setting for an IPS category, click an option in the category heading row.
- To expand the signatures under a category, click the **+** button next to the category heading. To hide the signatures, click the **-** button.
- To select an inspection setting for an individual signature, click an option in the entry row for that signature.

Options:

- **Disabled**: Choose this option to disable inspection checking for this protocol.
- **Detect Only**: Choose this option to check for attacks on this protocol and to log a message upon detection.This option is mostly used for troubleshooting purposes.
- **Detect and Prevent**: Choose this option to check for and prevent attacks on this protocol. Upon detection, a message is logged and a preventative action is taken.

  For IPS messages to be logged, you must configure IPS as the facility. For more information, see **Logs Facility and Severity, page 189**

STEP 3 Click **Apply** to save your settings.

Configuring Peer-to-Peer Blocking and Instant Messaging

You can configure the appliance to block Peer-to-Peer (P2P) and Instant Message (IM) traffic on the security appliance. From the IM and P2P blocking page, you can specify what type of P2P and IM applications (such as Gnutella, BitTorrent, AOL, or Yahoo) are blocked.

STEP 1 Click **IPS > IM and P2P Blocking**.

STEP 2 Choose the inspection settings for each category or for each signature within each category.

- To select an inspection setting for an IPS category, click an option in the category heading row.
- To expand the signatures under a category, click the **+** button next to the category heading. To hide the signatures, click the **-** button.
- To select an inspection setting for an individual signature, click an option in the entry row for that signature.

Options:

- **Disabled**: Choose this option to disable checking for this service.
- **Detect Only**: Choose this option to check for attacks on this service and to log a message upon detection.This option is mostly used for troubleshooting purposes
- **Detect and Prevent**: Choose this option to check for and prevent attacks for this service. Upon detection, a message is logged and a preventative action is taken.

  For IPS messages to be logged, you must configure IPS as the facility. For more information, see **Logs Facility and Severity, page 189**

STEP 3 Click **Apply** to save your settings.

6

Using Cisco ProtectLink Security Services

The SA500 Series supports Cisco ProtectLink Security Services. These services provide layers of protection against different security threats on your network.

- **Cisco ProtectLink Web** provides all users with web threat protection to prevent access to dangerous websites and URL filtering to control employee access to non-business related websites.
- **Cisco ProtectLink Gateway** provides the web security features of ProtectLink Web and combines it with email security to prevent spam, viruses, and phishing attacks in email.
- **Cisco ProtectLink Endpoint** protects desktops, laptops, and servers from viruses, spyware, and other web threats without running software on a server.

For information about these services, click **ProtectLink** on the menu bar. To buy, register, or activate the service, click **Administration** on the menu bar, and then click **License Management**.

After you activate your service, use the links in the navigation pane to configure the ProtectLink services. For more information, see the Cisco ProtectLink Security documentation at: www.cisco.com/go/protectlink.

7

Configuring VPN

This chapter describes how to configure a Virtual Private Network (VPN) to allow other sites and remote workers to access your network resources. It includes the following sections:

- **About VPN**
- **Configuring a Site-to-Site VPN Tunnel**
- **Configuring an IPsec VPN Tunnel for Remote Access with a VPN Client**
- **Configuring SSL VPN for Browser-Based Remote Access**
- **VeriSign™ Identity Protection configuration**

To access the VPN pages click *VPN* from the Configuration Utility menu bar.

About VPN

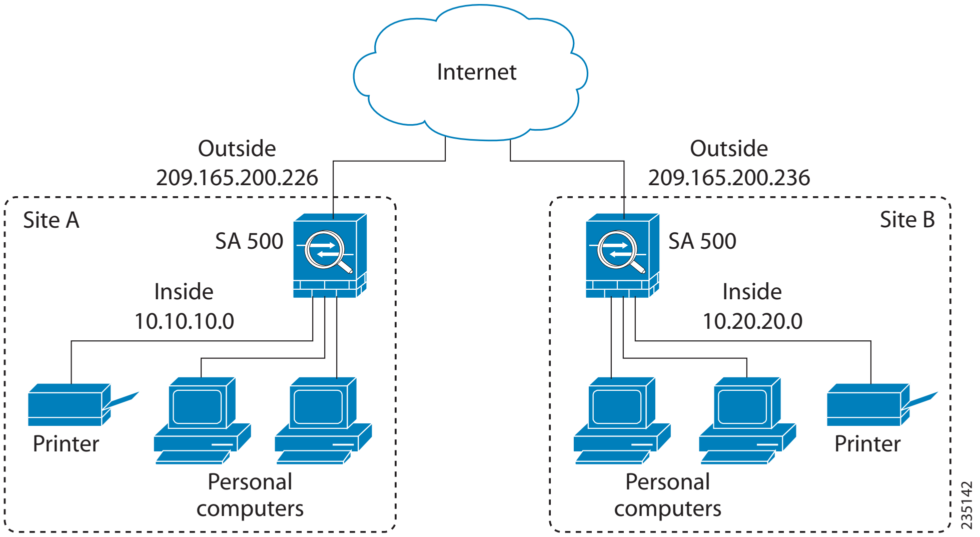
A VPN provides a secure communication channel (“tunnel”) between two gateway routers or between a remote PC and a gateway router, as in the following scenarios:

- **Site-to-Site VPN:** The VPN tunnel connects two routers to secure traffic between two sites that are physically separated. See **Configuring a Site-to-Site VPN Tunnel, page 137**.
- **Remote Access with IPsec VPN Client Software:** A remote worker uses a secure VPN client software to access the corporate network. See **Configuring a Site-to-Site VPN Tunnel, page 137**.
- **Remote Access with a Web Browser:** A remote worker uses a web browser to initiate a VPN tunnel to access the available services on the corporate network. See **Configuring SSL VPN for Browser-Based Remote Access, page 154**.

Configuring a Site-to-Site VPN Tunnel

The configuration utility includes a VPN Wizard that makes it easy for you to configure the VPN settings to allow other sites to connect to your network.

Figure 5 Site-to-Site VPN



The VPN Wizard helps you to set up an IPsec VPN tunnel. The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can update any of the parameters by using the other options in the navigation pane.

NOTE For information about the VPNC recommendations, visit the following website: www.vpnc.org/vpn-standards.html

STEP 1 Click **VPN > IPsec > VPN Wizard**, or from the Getting Started (Advanced) page, under **Site-to-Site VPN**, click **VPN Wizard**.

The VPN Wizard window opens.

STEP 2 In the **About VPN Wizard** area, choose **Site-to-Site** to create a site-to-site VPN tunnel from the security appliance to another VPN gateway.

STEP 3 In the **Connection Name and Remote IP Type** area, enter the following information:

- **What is the new connection name?:** Enter a name for the connection. The name is used for management and identification purposes.

- **What is the pre-shared Key?:** Enter the desired value, which the peer device must provide to establish a connection. The length of the pre-shared key is between 8 characters and 49 characters and must be entered exactly the same here and on the remote VPN gateway or client.

  NOTE When the security appliance at the other site is configured, the same pre-shared key has to be entered on that device. Do not use the double-quote character (“) in the pre-shared key.

- **Local WAN Interface:** Choose the WAN interface that you want to use for this VPN tunnel: **Dedicated WAN** or **Optional WAN**.

STEP 4 In the **Remote & Local WAN Addresses** area, enter the following information about the remote server and the local server:

- **Remote Gateway Type:** Choose **IP Address** if you want to enter the IP address of the remote device, or choose **Fully Qualified Domain Name (FQDN)** if you want to enter the domain name of the remote network, such as vpn.company.com. Then enter that address or name in the **Remote WAN’s IP Address or Internet Name** field.

  For the example illustrated in Figure 5, the remote site, Site B, has a public IP address of 209.165.200.236. You would choose IP Address for the type, and you would enter 209.165.200.236 in the IP Address or Internet Name field.

- **Local Gateway Type:** This field can be left blank if you are not using a different FQDN or IP address than the one specified in the WAN port’s configuration. Choose **IP Address** if you want to enter an IP address, or choose **Fully Qualified Domain Name (FQDN)** if you want to enter a domain name, such as vpn.company.com. Then enter that address or name in the **Local WAN’s IP Address or Internet Name** field.

  For the example illustrated in Figure 5, the local site, Site A, has a public IP address of 209.165.200.226. You would choose IP Address for the type, and you would enter 209.165.200.226 in the IP Address or Internet Name field.

STEP 5 In the **Secure Connection Remote Accessibility** area, enter the following information about the LAN at the remote site:

- **Remote LAN IP Address:** Enter the IP address of the remote LAN.

  For the example illustrated in Figure 5, the remote site, Site B, has a LAN IP address of 10.20.20.0.

- **Remote LAN Subnet Mask:** Enter the associated subnet mask for the above entered subnet IP Address.

For the example illustrated in Figure 5, the remote site, Site B, has a subnet mask of 255.0.0.0.

NOTE The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

STEP 6 Click **Apply** to save your settings.

The settings are not saved on the Wizard page. The Wizard creates a VPN policy and an IKE policy based on your entries.

NOTE **Next steps**:

- If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to return to the list of configuration tasks for **Site-to-Site VPN**.
- To review or update the configured VPN policy click **IPsec > VPN Policies**. For more information, see **Configuring the IPsec VPN Policies, page 148**.
- To review or update the configured IKE policy, click **IPsec > IKE Policies**. For more information, see **Configuring the IKE Policies for IPsec VPN, page 144**.
- To configure IPsec passthrough, click **IPsec > Passthrough**. For more information, see **Configuring IPsec Passthrough, page 153**.

Configuring an IPsec VPN Tunnel for Remote Access with a VPN Client

This section describes how to configure an IPsec VPN tunnel for remote access with a VPN client, or by using Standard IPsec (Xauth). The VPN Wizard helps you to set up a tunnel to allow workers to connect to your network from remote locations by using an IPsec VPN client. After creating the policies through the Wizard, you can update any of the parameters by using the other options in the navigation pane.

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup For information about the VPNC recommendations, see: www.vpnc.org/vpn-standards.html.

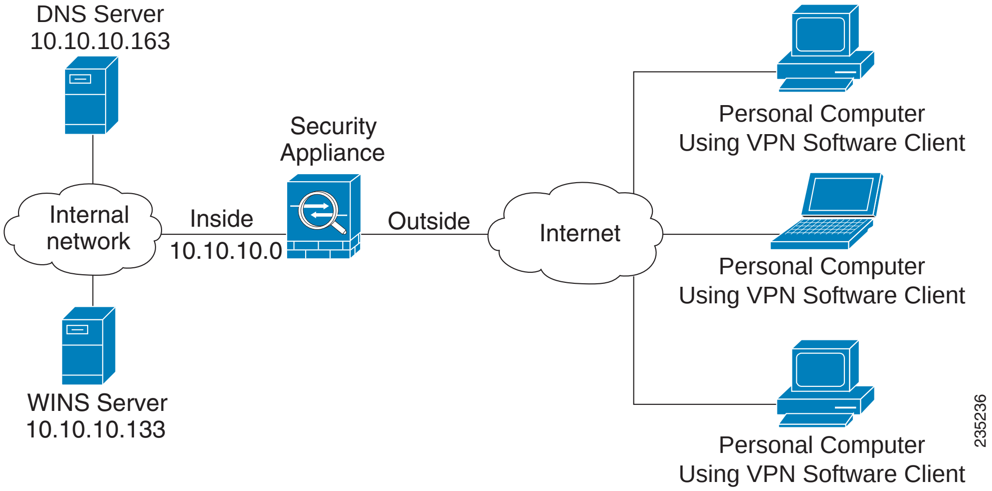
With the Wizard's default settings, you will need to add VPN users through the IPsec VPN users page after you complete the Wizard. Alternatively, you can edit the IKE policy to allow Extended Authentication (XAUTH) from user records stored on an external authentication server such as a RADIUS server.

For detailed information about configuring an IPsec tunnel between an SA500 and Cisco VPN Client, see the Application Note located under Technical Documentation at: www.cisco.com/go/sa500resources.

The Cisco VPN client software is available for download at: www.cisco.com/go/ciscovpnclient. For Windows, select Cisco VPN Client v5.x. For Mac OS, select Cisco VPN Client v4.x.

NOTE A 3-year Cisco Small Business Support Service Contract (CON-SBS-SVC2) is required to download the client software. If you don't have one, contact your partner or reseller, or Cisco Support for more information.

Figure 6 IPsec VPN Remote Access with a VPN Client



STEP 1 Click **VPN > IPsec > VPN Wizard**, or from the Getting Started (Advanced) page, under **IPsec VPN Remote Access**, click **VPN Wizard**.

The VPN Wizard window opens.

STEP 2 In the **About VPN Wizard** area, choose **Remote Access** to allow the security appliance to be accessed by remote PCs that are running VPN client software.

STEP 3 In the **Connection Name and Remote IP Type** area, enter the following information:

- **What is the new connection name?:** Enter a name for the connection. The name is used for management and identification purposes.

- **What is the pre-shared Key?:** Enter the desired value, which the peer device must provide to establish a connection. The length of the pre-shared key is between 8 characters and 49 characters and must be entered exactly the same here and on the remote client.

  NOTE Do not use the double-quote character (“) in the pre-shared key.

- **Local WAN Interface:** If you have configured two WANs, choose the interface that you want to use for this VPN tunnel. If you have only one WAN configured, choose Dedicated WAN.

STEP 4 In the **Remote & Local WAN Addresses** area, enter the following information about the remote server and the local server:

- **Remote Gateway Type:** Choose **Fully Qualified Domain Name (FQDN)**, and then enter a name **Remote WAN's IP Address or Internet Name** field to identify the VPN client to the gateway.
- **Local Gateway Type:** This field can be left blank if you are not using a different FQDN or IP address than the one specified in the WAN port's configuration. Choose **IP Address** if you want to enter an IP address, or choose **Fully Qualified Domain Name (FQDN)** if you want to enter a domain name, such as vpn.company.com. Then enter that address or name in the **Local WAN's IP Address or Internet Name** field.

STEP 5 Click **Apply** to save your settings.

NOTE **Next steps:**

- If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to return to the list of configuration tasks for **IPsec Remote Access VPN**.
- **Required:** Configure the VPN users.
  - To add users to the user database, continue with the procedure **Configuring the User Database for the IPsec Remote Access VPN, page 142**.
  - To allow Extended Authentication (XAUTH) from user records stored on an external authentication server such as a RADIUS server, see **Configuring the IKE Policies for IPsec VPN, page 144**.
- To review or update the configured VPN policy click **IPsec > VPN Policies**. For more information, see **Configuring the IPsec VPN Policies, page 148**.

- To review or update the configured IKE policy, click **IPsec > IKE Policies**. For more information, see **Configuring the IKE Policies for IPsec VPN, page 144**.
- To configure IPsec passthrough, click **IPsec > Passthrough**. For more information, see **Configuring IPsec Passthrough, page 153**.

Configuring the User Database for the IPsec Remote Access VPN

If you are using IPsec VPN for remote access by remote workers, use this page to manage the users (both XAUTH and Cisco QuickVPN). The VPN gateway authenticates the users in this list when XAUTH is used in an IKE policy.

Alternatively, you can enable Extended Authentication (XAUTH) from user records stored on an external authentication server such as a RADIUS server, see **Configuring the IKE Policies for IPsec VPN, page 144**.

If you are using the using the Cisco VPN Client, see the Application Note located under Technical Documentation at: www.cisco.com/go/sa500resources.

STEP 1 Click **VPN > IPsec > IPsec Users**.

The IPsec Users window opens. Any existing users are listed in the List of IPsec Users table.

STEP 2 Click **Add** to add a user.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the IPsec User Configuration window opens.

STEP 3 Enter the following information:

- **User Name:** Enter a unique identifier for the XAUTH user.
- **Remote Peer Type:** Choose one of the following options:
  - Standard IPsec (XAuth)

  - Cisco QuickVPN

    X-Auth is an IPsec standard that extends the authentication in native IPsec to provide user credentials. XAUTH can be used when additional client security is required with IPsec clients such as Greenbow. QuickVPN is a propriety Cisco/Linksys client which uses user authentication but the implementation is specific only to Quick VPN. This option should be selected when the clients use QuickVPN Client.

- **Allow user to change password?:** If you chose Cisco QuickVPN for the Remote Peer Type, you can check this box to allow the user to change the password.
- **Password:** Enter an alphanumeric password for this user.
- **Confirm Password:** Re-enter the characters that you entered in the Password field.
- **LAN IP address:** Enter the LAN IP subnet to which the remote user will have access. The subnet should be part of the LAN or VLAN IP addresses.
- **Subnet Mask**: Enter the subnet mask for the local subnet.

STEP 4 Click **Apply** to save your settings.

STEP 5 Repeat as needed for each user that you need to add.

NOTE **Next steps:**

- If you are using the Getting Started (Advanced) page, click **Getting Started > Advanced** to return to the list of configuration tasks for **IPsec VPN Remote Access**.
- Optionally, review and modify the default settings and policies. See **Advanced Configuration of IPsec VPN, page 144**.
- For Cisco QuickVPN, you also must enable Remote Management. See **RMON (Remote Management), page 197**.

Advanced Configuration of IPsec VPN

The following topics are helpful for users who want to review and modify the settings that are created by the VPN Wizard.

- **Viewing the Basic Setting Defaults for IPsec VPN**
- **Configuring the IKE Policies for IPsec VPN**
- **Configuring the IPsec VPN Policies**

Viewing the Basic Setting Defaults for IPsec VPN

To view the basic setting defaults that are configured by the Wizard, click **VPN** on the menu bar, and then click **IPsec > Basic Setting Defaults**.

Configuring the IKE Policies for IPsec VPN

The Internet Key Exchange (IKE) protocol is a negotiation protocol that includes an encryption method to protect data and ensure privacy. It is also an authentication method to verify the identity of devices that are trying to connect to your network. You can create IKE policies to define the security parameters such as authentication of the peer, encryption algorithms, etc. to be used in this process.

You can choose whether to authenticate users from the User Database (see **Configuring the User Database for the IPsec Remote Access VPN**) or an external authentication server such as a RADIUS server (by choosing the IPsec Host option in the XAUTH field of this page.

NOTE The VPN Wizard is the recommended method to create the corresponding IKE and VPN policies for a VPN tunnel. After the Wizard creates the matching IKE and VPN policies, you can make changes, as needed. Advanced users can create an IKE policy from **Add** but must be sure to use compatible encryption, authentication, and key-group parameters for the VPN policy.

STEP 1 Click **VPN > IPsec > IKE Policies**. The existing entries appear in the List of IKE Policies table.

The IKE Policies window opens. Any existing policies are listed in the List of IKE Policies table.

STEP 2 Click **Edit** to edit an entry.

Other options: Click **Add** to add an entry. To delete an entry, check the box, and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the IKE Policy Configuration window opens.

STEP 3 In the **General** area, enter the following information:

- **Policy Name:** Enter a unique name for identification and management purposes.
- **Direction/Type:** Choose one of the following options:
  - **Initiator:** The security appliance initiates the connection to the remote end.
  - **Responder:** The security appliance waits passively and responds to remote IKE requests.
  - **Both:** The security appliance works in either Initiator or Responder mode.
- **Exchange Mode:** Choose one of the following options:
  - **Main Mode:** Choose this option if you want higher security, but with a slower connection. Main Mode relies upon two-way key exchanges between the initiator and the receiver. The key-exchange process slows down the connection but increases security.
  - **Aggressive Mode:** Choose this option if you want a faster connection, but with lowered security. In Aggressive Mode there are fewer key exchanges between the initiator and the receiver. Both sides exchange information even before there is a secure channel. This feature creates a faster connection but with less security than Main Mode.

    NOTE If you choose **Main Mode**, then you must use an IP address as the identifier type for both the Local device and the Remote device, below. If FQDN, User FQDN or DER ASN1 DN is selected as the identifier type, then Main Mode is disabled and Aggressive Mode is applied.

STEP 4 In the **Local** area, enter the following information:

- **Identifier Type** and **Identifier:** Choose the type of identifier for the local device, and then enter the ID in the text box.

  - Local WAN IP
  - Internet Address/FQDN
  - User FQDN
  - DER ASN1 DN.

  NOTE Typically, an IP address is used for site-to-site connections since the IP address or FQDN is well known. An IP address is required if you want to use Main Mode. For remote client connections, the User FQDN is never resolved but provides a means of identifying a client that can have different IP address depending on network that is used to make the connection. The DER ASN1 DN is used as an identifier when certificates are used for authentication.

STEP 5 In the **Remote** area, enter the following information:

- **Identifier Type** and **Identifier:** Choose the type of identifier for the local device, and then enter the ID in the text box.

  NOTE An IP address is required if you want to use Main Mode.

STEP 6 In the **IKE SA Parameters** area, enter the information about the Security Association (SA) parameters, which define the strength and the mode for negotiating the SA.

- **Encryption Algorithm:** The algorithm used to negotiate the SA. There are five algorithms supported by this router: DES, 3DES, AES-128, AES-192, and AES-256.

- **Authentication Algorithm:** Specify the authentication algorithm for the VPN header. There are five algorithms supported by this router: MD5, SHA-1, SHA2-256, SHA2-384 and SHA2-512.

  NOTE Ensure that the authentication algorithm is configured identically on both sides.

- **Authentication Method:** Select Pre-shared key for a simple password based key. Selecting RSA-Signature disables the pre-shared key text box and uses the Active Self Certificate uploaded in the Certificates page. In that case, a certificate must be configured in order for RSA-Signature to work. See **Managing Certificates for Authentication, page 190**.

NOTE The double-quote character (“) is not permitted for the shared key.

- **Pre-shared key:** Enter the alpha-numeric key to be shared with IKE peer.
- **Diffie-Hellman (DH) Group:** Choose the Diffie-Hellman algorithm to use when exchanging keys. The DH Group sets the strength of the algorithm in bits.
- **SA Lifetime (seconds):** Enter the number of seconds for the Security Association to remain valid.
- **Enable Dead Peer Detection:** Check this box to enable the security appliance to detect whether a peer is alive or not. If a peer is detected as dead, then the security appliance deletes the IPsec and IKE Security Association.
- **Detection Period (seconds):** Detection Period is the interval between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPsec traffic is idle.
- **Reconnect after failure count:** Maximum number of DPD failures allowed before tearing down the connection.

STEP 7 In the **Extended Authentication (XAUTH)** area, you can enable the VPN gateway router to authenticate users from the User Database (default choice) or an external authentication server such as a RADIUS server. Choose one of the following **XAUTH Types**:

- **None:** Choose this option to disable XAUTH.
- **User Database:** Choose this option if you want to authenticate users based on the accounts that you create in this Configuration Utility. If you choose this option, be sure to add the users on the IPsec Users page. See **Configuring the User Database for the IPsec Remote Access VPN, page 142**.
- **IPsec Host:** Choose this option if you want the security appliance to be authenticated with a username and password combination. In this mode, the security appliance acts as a VPN Client of the remote gateway. If you choose this option, also enter a Username and Password.
  - **Username:** If you chose IPsec Host as the XAUTH Type, enter the user name for the security appliance to use when connecting to the remote server. The username can include any alphanumeric characters.
  - **Password:** Enter the password for the security appliance to use when connecting to the remote server.

STEP 8 Click **Apply** to save your settings.

NOTE **Next Steps**

- To review or update the configured VPN policy click **IPsec > VPN Policies**. For more information, see **Configuring the IPsec VPN Policies, page 148**.
- To review or update the configured IKE policy, click **IPsec > IKE Policies**. For more information, see **Configuring the IKE Policies for IPsec VPN, page 144**.
- To configure IPsec passthrough, click **IPsec > Passthrough**. For more information, see **Configuring IPsec Passthrough, page 153**.
- To configure the VPN users (for remote access VPN only), click **IPsec > IPsec Users**. See **Configuring the User Database for the IPsec Remote Access VPN, page 142**.
- To configure the security appliance to work with your RADIUS server, see **Configuring RADIUS Server Records, page 193**.

Configuring the IPsec VPN Policies

You can use this page to manage the VPN policies. This page contains two tables List of VPN Policies and List of back up Policies. These tables list the policies that have been added and allows several operations on the policies.

NOTE Before you create an Auto Policy, first create an IKE policy. Then you can apply the IKE policy on this page. For more information, see **Configuring the IKE Policies for IPsec VPN, page 144**.

STEP 1 Click **VPN > IPsec > VPN Policies**.

The VPN Policies window opens. Two tables are displayed:

- **List of VPN Policies:** Lists all the VPN policies except the backup policies. Auto and Manual policies are included.
- **List of back up Policies:** Lists all the policies that are configured as a backup policy. These policies are created when you create a new IKE policy and select the **Enable Redundant Gateway** option. The policy comes into effect only if the primary policy fails. You cannot enable, disable, edit, or delete the backup policies. You can only take actions on the primary policy, by using the buttons in the List of VPN Policies table.

STEP 2 To add a VPN policy, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the VPN Policy Configuration window opens.

STEP 3 In the **General** area, enter the following information:

- **Policy Name:** Enter a unique name to identify the policy.
- **Policy Type:** Choose one of the following types:
  - **Auto:** Some parameters for the VPN tunnel are generated automatically. The IKE (Internet Key Exchange) protocol is used to perform negotiations between the two VPN endpoints. To create an Auto VPN Policy, you need to first create an IKE policy and then add the corresponding Auto Policy for that IKE Policy.
  - **Manual:** All settings (including the keys) for the VPN tunnel are manually input for each end point. No third party server or organization is involved.
- **Select Local Gateway:** If you configured the Optional Port for use as a WAN port, choose which WAN interface will act as one end of the tunnel: **Dedicated WAN** or **Optional WAN**.
- **Remote End Point:** Choose to identify the remote end point by the IP address or the Internet Name/FQDN of the remote gateway or the client PC. Also enter the IP address or the Internet Name/FQDN in the field below the drop-down list.
- **Enable NetBIOS:** Check this box to enable NetBIOS, which is a program that carries out name resolution. This option allows NetBIOS broadcasts to travel over the VPN tunnel.
- **Enable RollOver:** This option is applicable if you have two ISP links and if you have enabled Auto-Rollover (see **Configuring Auto-Rollover, Load Balancing, and Failure Detection, page 57**). In this case, you can check the **Enable RollOver** box to ensure that VPN traffic rolls over to the backup link whenever the primary link fails. The security appliance will automatically update the local WAN gateway for the tunnel based on the optional WAN link configuration. For this type of configuration, Dynamic DNS has to be configured because the IP address will change due to failover. See **Dynamic DNS, page 76**.

STEP 4 In the **Local Traffic Selection** area and the **Remote Traffic Selection** area, enter the following information to specify the IP addresses that are on either side of the tunnel:

- **Local IP** or **Remote IP:** Choose one of the following options:
    - **Any:** Allows all traffic from the given end point. Note that selecting **Any** for both local and remote end points is not valid.
    - **Single:** Allows only one host to connect to the VPN. If you choose this option, also enter the IP address of the host in the Start IP Address field.
    - **Range:** Allows all computers within an IP address range to connect to the VPN. If you choose this option, also specify the range by entering the Start IP Address and the End IP address.
    - **Subnet:** Allows all computers on a subnet to connect to the VPN. If you choose this option, also enter the network address and the subnet mask.

STEP 5 If you chose Manual Policy for the Policy Type, create an SA (Security Association) by entering the following static inputs in the **Manual Policy Parameters** area:

- **SPI-Incoming** or **SPI-Outgoing:** Enter a hexadecimal value between 3 and 8 characters. For example: 0a1234.
- **Encryption Algorithm:** Choose the algorithm that is used to encrypt the data.
- **Key-In:** Enter the encryption key of the inbound policy.
- **Key-Out:** Encryption key of the outbound policy.

    The length of the keys depends on the chosen algorithm:

    - **DES:** 8 characters
    - **3DES:** 24 characters
    - **AES-128:** 16 characters
    - **AES-192:** 24 characters
    - **AES-256:** 32 characters
    - **AES-CCM:** 16 characters

- **Integrity Algorithm:** Choose the algorithm that is used to verify the integrity of the data.
- **Key-In:** Enter the integrity key (for ESP with Integrity-mode) for the inbound policy.
- **Key-Out:** Enter the integrity key (for ESP with Integrity-mode) for the inbound policy.

  The length of the key depends on the chosen algorithm:

  - **MD5:** 16 characters
  - **SHA-1:** 20 characters
  - **SHA2-256:** 32 characters
  - **SHA2-384:** 48 characters
  - **SHA2-512:** 64 characters

STEP 6 If you chose Auto Policy as the Policy type, enter the following information in the **Auto Policy Parameters** area:

- **SA Lifetime:** Enter the lifetime of the Security Association, and specify whether it is in seconds or kilobytes.
  - **Seconds:** If you specify the SA Lifetime in seconds, this value represents the interval after which the Security Association becomes invalid. The SA is renegotiated after this interval. The default value is 3600 seconds.
  - **Kilobytes:** If you specify the SA Lifetime in kilobytes, the SA is renegotiated after the specified number of kilobytes of data is transferred over the original SA. The minimum value is 300 seconds or 1920000 KB.

    NOTE For every policy, two SAs are created, one for inbound traffic and one for outbound traffic. When using a lifetime configured in kilobytes (also known as lifebyte) along with a lifetime in seconds, the SA expires asymmetrically. For example, the lifebyte for a download stream expires frequently if the downstream traffic is very high, but the lifebyte of the upload stream expires less frequently or only when it reaches its timeout period. When setting the lifetime in both seconds and kilobytes, you should reduce the difference in expiry frequencies of the SAs; otherwise the system could eventually run out of resources as a result of this asymmetry. The lifebyte specifications are generally recommended for advanced users only.

- **Encryption Algorithm:** Choose the algorithm that is used to encrypt the data.
- **Integrity Algorithm:** Choose the algorithm that is used to verify the integrity of the data.
- **PFS Key Group:** Check this box to enable Perfect Forward Secrecy (PFS) to improve security. While this option is slower, it ensures that a Diffie-Hellman exchange is performed for every phase-2 negotiation.
- **Select IKE Policy:** Choose the IKE policy to define the characteristics of phase-1 of the negotiation. **Configuring the IKE Policies for IPsec VPN, page 144**.

STEP 7 In the **Redundant VPN Gateway Parameters** area, enter the following information to create a backup policy for this policy:

- **Enable Redundant Gateway for this policy?:** Check this box to make a backup policy for this policy. When the tunnel for this policy is down, the backup tunnel automatically becomes active.
- **Select Back- up Policy:** Choose a policy to act as a backup of this policy. This list includes only those policies that can be configured as back up policies.

  NOTE A backup policy should meet the following conditions:
  1. The Type should be Auto.
  2. The DPD should be enabled.
  3. The Direction should be either initiator or both.
  4. The XAuth configuration should be None or IPsec Host.
  5. The policy should be Gateway only, not client.
- **Failback time to switch from back-up to primary:** Enter the number of seconds that must pass to confirm that primary tunnel has recovered from a failure. If the primary tunnel is up for the specified number of seconds, the security appliance will switch to the primary tunnel by disabling the backup tunnel.

STEP 8 Click **Apply** to save your settings.

NOTE **Next steps:**

- To view the status of the VPN tunnels, click **Status > VPN Status > IPsec Status**. For more information, see **IPsec VPN Status, page 210**.
- To view IPsec VPN logs, click **Status > View Logs > IPsec VPN Logs**. For more information, see **IPsec VPN Logs, page 215**.

- To configure IPsec passthrough, click **IPsec > Passthrough**. For more information, see **Configuring IPsec Passthrough, page 153**.
- To configure a range for a dynamic IP address, see **Configuring a Dynamic IP Range, page 153**.
- To add the users for remote access VPN, see **Configuring the User Database for the IPsec Remote Access VPN, page 142**.
- If you enabled rollover, be sure to configure Dynamic DNS. See **Dynamic DNS, page 76**.

Configuring IPsec Passthrough

You need to configure IPsec passthrough if there are devices behind the security appliance that need to set up IPsec tunnels independently, for example, to connect to another router on the WAN.

STEP 1 Click **VPN > IPsec > Passthrough**.

The Passthrough window opens.

STEP 2 Check the box for each type of traffic that you want to allow to pass through the VPN tunnel.

STEP 3 Click **Apply** to save your settings.

Configuring a Dynamic IP Range

The IP address is defined by the Dynamic IP Range and is automatically set by default. However, you can use the Dynamic IP Range page to manually specify a starting and ending range for the IP address.

The Dynamic IP Range is used by IPsec VPN clients connecting to the router using Mode- Config.

NOTE If you are creating a VPN policy and want to change the dynamic IP address, change it before you create the policy. Otherwise, the changes will not take affect.

STEP 1 Click **VPN > IPsec > Dynamic IP Range.**

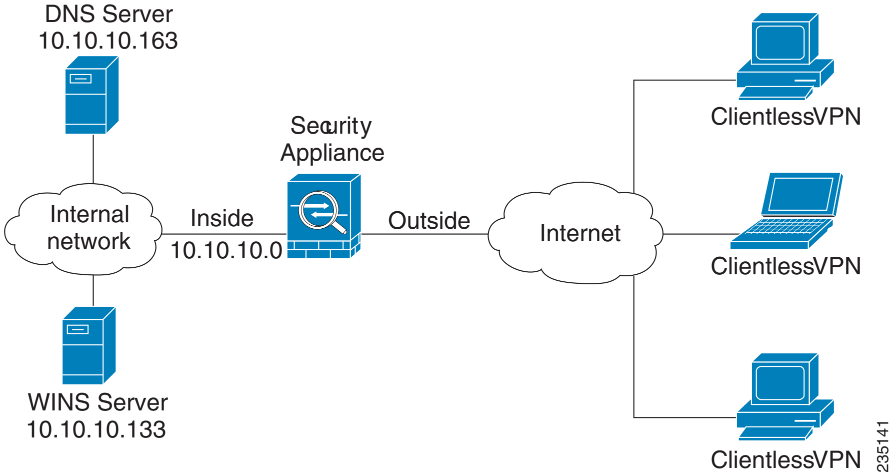
The Dynamic IP Range window opens.

STEP 2 Enter a Start IP range and End IP range for the IP address.

Click **Apply** to save your settings.

Configuring SSL VPN for Browser-Based Remote Access

SSL VPN is a flexible and secure way to extend network resources to virtually any remote user who has access to the Internet and a web browser. A benefit is that you do not have to install and maintain VPN client software on the remote machines.



Users can remotely access the network by using a web browser. When the tunnel is established, each user will have an IP address on the internal network, such as 10.10.10.x, in the above example.

You can use SSL VPN to provide access to the following types of services on your network:

- Internal websites
- Web-enabled applications
- NT/Active Directory and FTP file shares
- E-mail proxies, including POP3S, IMAP4S, and SMTPS
- MS Outlook Web Access
- MAPI

- Applications (that is, port forwarding for access to other TCP-based applications)

The security appliance supports multiple concurrent sessions to allow remote users to access the LAN over an encrypted link through a customizable user portal interface. You can specify the user privileges and you can control each user's access to network resources. You can streamline the setup process by organizing VPN users into domains and groups that share VPN policies.

NOTE Remote Management (RMON) must be enabled, or SSL VPN access will be blocked. For more information, see **RMON (Remote Management), page 197**.

Access Options for SSL VPN

The remote user can be given different options for SSL service:

- **VPN Tunnel**: The remote user's SSL enabled browser is used in place of a VPN client on the remote host to establish a secure VPN tunnel. A SSL VPN client (Active-X or Java based) is installed in the remote host to allow the client to join the corporate LAN with pre-configured access/policy privileges. At this point a virtual network interface is created on the user's PC and it is assigned an IP address and DNS server address from the security appliance.

  To create a VPN tunnel, see **Elements of the SSL VPN, page 156**.

- **Port Forwarding**: Port Forwarding service supports TCP connections between the remote user and the security appliance. A web-based (ActiveX or Java) client is installed on the client machine. The administrator can define the services and applications that are available to remote port forwarding users. Users do not have access to the full LAN.

  To configure port forwarding, see **Configuring SSL VPN Port Forwarding, page 163**.

Security Tips for SSL VPN

To minimize the risks involved with SSL certificates:

- Configure a group policy that consists of all users who need Clientless SSL VPN access and enable it only for that group policy.

- Limit Internet access for Clientless SSL VPN users, for example, by limiting which resources a user can access using a clientless SSL VPN connection. To do this, you could restrict the user from accessing general content on the

Internet. Then, you could configure links to specific targets on the internal network that you want users of Clientless SSL VPN to be able to access.

- Educate users. If an SSL-enabled site is not inside the private network, users should not visit this site over a Clientless SSL VPN connection. They should open a separate browser window to visit such sites, and use that browser to view the presented certificate.

Elements of the SSL VPN

Several elements work together to support SSL VPN.

- **Portal:** To access your network, user starts a web browser and then enters the URL for your portal. The security appliance is pre-configured with a portal that you can use for all users. You can modify title, banner heading, banner message, security settings, and access type (VPN tunnel, port forwarding, or both). In addition, you can create different portal layouts for different groups of users. For example, you could create two portal layouts for two groups that have access to different resources. On each portal layout, you would customize the banner message to provide customized information for the portal users.

  IMPORTANT: If you plan to create different portal layouts for different user domains, you must create the portal layouts first. In the scenario, start with **Scenario Step 1: Customizing the Portal Layout, page 157**. If you are not going to create different portal layouts, you can start the scenario with this step so that you can review the default settings and modify, as needed. In addition, the Portal Layouts page shows you the URL that you need to provide to the portal users.

- **Users:** Create your VPN users. You can use the default domain and group or configure your own domains and groups. As you create each user record, be sure to select SSL VPN User as the User Type. Instructions are included in the scenario, or for complete details about domains, groups, and users, see **Chapter 8, "Administration."**.

- **VPN Policies:** The default VPN policies should be sufficient for most purposes. As needed, you can create more complex policies. See **Creating the SSL VPN Policies, page 160**.

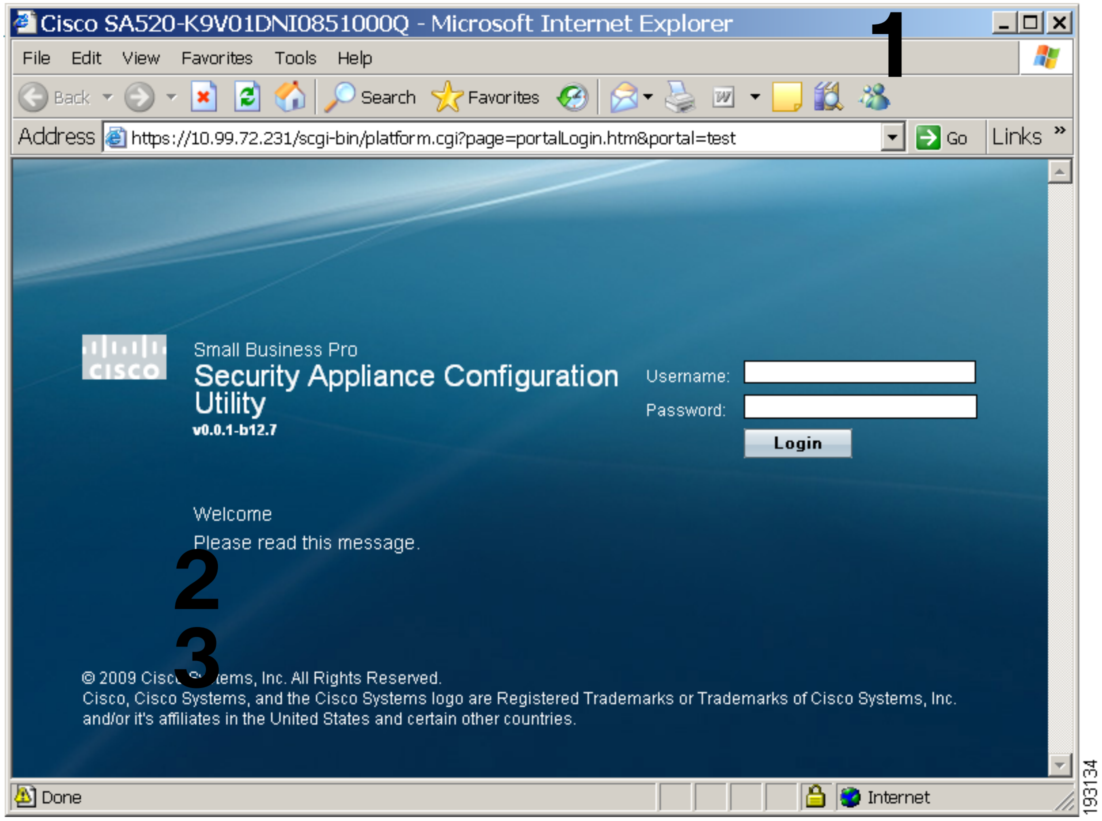
- **Port Forwarding:** You can configure port forwarding to allow access to a limited set of resources. For example, you may want the SSL VPN users to access the email service only. See **Configuring SSL VPN Port Forwarding, page 163**.

Scenario Step 1: Customizing the Portal Layout

When a remote user wants to access your private network through an SSL tunnel, the user starts a web browser and enters a URL. The browser displays a login page with several features that you can configure:

1. Portal Site Title: appears at the top browser
2. Banner Title
3. Banner Message

Configurable Areas of the SSL VPN Portal Layout


Cisco SA520-K9V01DNI0851000Q - Microsoft Internet Explorer

https://10.99.72.231/scgi-bin/platform.cgi?page=portalLogin.htm&portal=test

Small Business Pro
Security Appliance Configuration Utility
v0.0.1-b12.7

Welcome
Please read this message.

© 2009 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are Registered Trademarks or Trademarks of Cisco Systems, Inc. and/or it's affiliates in the United States and certain other countries.

STEP 1 Click **VPN > SSL VPN Server > Portal Layouts**.

The Portal Layouts window opens.

STEP 2 To modify the default portal layout, click the pencil button in the **Edit** column.

Other options: To add a portal layout, click **Add**. To delete a portal layout, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading. To designate a layout as the default layout, click the star (*) button. To view a portal layout, click the hyperlink in the **Portal URL** column.

After you click Add or Edit, the Portal Layout Configuration window opens.

STEP 3 In the **Portal Layout and Theme Name** area, enter the following information:

- **Portal Layout Name:** Enter a descriptive name for the portal that is being configured. The name will appear in the URL for the portal. Do not enter spaces or special characters. Only alphanumeric characters, hyphens ('-'), and underscore ('_') characters are allowed for this field.

- **Portal Site Title:** Enter the title that will appear at the top of the web browser window for the portal.

- **Banner Title:** Enter one word for the banner title. Spaces and special characters are not allowed.

- **Banner Message:** Enter the message text to display along with the banner title. For example, enter instructions or information about the resources that the users can access after logging in. Empty space and characters are not allowed.

- **Display banner message on login page:** Check the box to show the banner title and banner message on the portal layout.

- **HTTP meta tags for cache control (recommended):** Check the box to enable this security feature, which is strongly recommended. This feature ensures that the SSL VPN portal pages and other web content cannot be cached. The HTTP meta tags cache control directives prevent out-of-date web pages and data from being stored on the client's web browser cache.

- **ActiveX web cache cleaner:** Check this box to load an ActiveX cache control whenever users login to this SSL VPN portal.

STEP 4 In the **SSL VPN Portal Pages to Display** area, check the box for each SSL VPN Portal page that users can access through this portal.

Any page that is not selected will not be visible from the SSL VPN portal navigation menu. However, users can still access the hidden pages unless SSL VPN access policies are created to prevent access to these pages

STEP 5 Click **Apply** to save your settings.

STEP 6 To view your new page, click the link in the Portal URL column of the table. This URL also is the URL that you will provide to your users.

STEP 7 Repeat as needed to add more portal layouts.

NOTE Next step (required)

Configure the SSL VPN Users. Proceed to the next section **Scenario Step 2: Adding the SSL VPN Users**.

Scenario Step 2: Adding the SSL VPN Users

Authentication of the remote SSL VPN user is done by the security appliance by using either a local database on the security appliance or external authentication servers (i.e. LDAP or RADIUS). The user domain determines the authentication method (local user database, external server) to be used when validating the remote user's connection.

In this scenario, you add all users to the default domain and group. However, you can create different domains and groups if you want to have different portal layouts and different SSL VPN policies for different users. For complete details about domains, groups, and users, as well as user policies that you can configure see **Chapter 8, "Administration."** For information about adding users, see **Adding or Editing User Settings, page 173**.

STEP 1 Click **Administration > Users > Users**. The List of Users table appears.

The User window opens. The default Administrator and Guest users appear in the List of Users table, along with any new users that you add.

STEP 2 To add a user, click **Add**.

The User Configuration window opens.

STEP 3 Enter the following information:

- **User Name:** Enter a unique identifier for the user. It can include any alphanumeric characters.
- **First Name:** Enter the user's first name.
- **Last Name:** Enter the user's last name.
- **User Type:** Choose **SSL VPN User**.
- **Select Group:** Choose **SSLVPN**.
- **Password:** Enter a password that contains alphanumeric, '—' or '_' characters.
- **Confirm Password:** Enter the password again.
- **Idle Timeout:** Enter the time in minutes that the user can be inactive before the session is disconnected. Enter any value from 0 to 999. The timeout value for the individual user has precedence over the timeout for the group. If the user's timeout value is set to 0, the group timeout setting applies.

  NOTE Every user is added as a local user with password, and when the user is assigned to an external authentication mechanism based on the group, certain attributes such as the local password are ignored.

STEP 4 Click **Apply** to save your settings.

Creating the SSL VPN Policies

SSL VPN Policies give configured SSL users access to services and network resources. A policy applies to a specific network resource, IP address, or IP address range on the LAN, or to other SSL VPN services that are supported by the security appliance.

By default, a global PERMIT policy (not displayed) is preconfigured over all addresses and over all services and ports.

You can create user, group, and global policies. Policies are applied based on the following levels of precedence:

- User-level policies take precedence over Group-level policies.
- Group-level policies take precedence over Global policies.

- When two policies are in conflict, a more specific policy takes precedence over a general policy. For example, a policy for a specific IP address takes precedence over a policy for a range of addresses that includes this IP address.

A policy can be offered to the VPN Tunnel, Port Forwarding, or both.

After you define a policy, it goes into effect immediately. However, if Remote Management (RMON) is not enabled, SSL VPN access will be blocked. See **RMON (Remote Management), page 197**.

If you are creating a policy that applies to a network resource, you first need to configure a record for the network resource. See **Specifying the Network Resources for SSL VPN, page 163**.

STEP 1 Click **VPN > SSL VPN Server > SSL VPN Policies**.

The SSL VPN Policies window opens.

STEP 2 In the **Query** area, choose which policies to display in the List of SSL VPN Policies table.

- **View List of SSL VPN Policies for:** Choose **Global** for all users, **Group** for a particular group, or **User** for a particular user.
- **Available Groups:** If you chose **Group** as the query type, choose the name from this list.
- **Available Users:** If you chose **User** as the query type, choose the name from this list.
- Click **Display** to run the query.

STEP 3 To add an SSL VPN policy, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the SSL VPN Policy Configuration window opens.

STEP 4 In the **Policy For** area, enter the following information:

- **Policy For:** Choose the type of policy: Global, Group, or User. If you choose Group, also choose the group from the Available Groups list. If you choose User, also choose the user from the Available Users list.

STEP 5 In the **SSL VPN Policy** area, enter the following information:

- **Apply Policy to:** Choose to apply the policy to a Network Resource, an IP address, an IP network, or All Addresses that are managed by the device. Also complete the fields that are highlighted with white backgrounds.
- **Policy Name:** Enter a name to identify this policy.

  NOTE If you create a policy with same name as that of any existing policy, the newly policy overwrites the existing one.

- **IP Address:** If you chose IP Address or Network Resource in the Apply Policy to field, enter the IP address of the device.
- **Mask Length:** If you chose IP Network in the Apply Policy to field, enter the length of the subnet mask.
- **Port Range / Port Number (Begin & End):** Specify a port or a range of ports to apply the policy to all TCP and UDP traffic with those ports. Leave the fields empty to apply the policy to all traffic.
- **Service:** Choose **VPN Tunnel**, **Port Forwarding**, or **All Services Defined**.
- **Defined Resources:** Choose the services for a particular policy. This option is available only for policies that are applied to a Network Resource.
- **Permission:** Choose either Permit or Deny for this policy.

STEP 6 Click **Apply** to save your settings.

NOTE Next steps:

Enable Remote Management (RMON), if you have not done so previously. If RMON is disabled, SSL VPN access is blocked. See **RMON (Remote Management), page 197**.

Specifying the Network Resources for SSL VPN

Network resources are services or groups of LAN IP addresses that are used to easily create and configure SSL VPN policies. This shortcut saves time when creating similar policies for multiple remote SSL VPN users.

STEP 1 Click **VPN > SSL VPN Server > Resources**.

The Resources window opens.

STEP 2 To add a network resource, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

STEP 3 Enter the following information:

- **Resource Name:** Enter a unique name to identify this resource.
- **Service:** Choose one of the supported SSL VPN services to associate with this resource.

STEP 4 Click **Apply** to save your settings.

Configuring SSL VPN Port Forwarding

Port Forwarding is used when you want to allow access only to a limited set of resources. For example, you may want the SSL VPN users to access the email service only. Port forwarding is different from split and full tunnel modes, which allow access to all ports for a give subnet.

The following table lists some common applications and corresponding TCP port numbers:

TCP Application	Port Number
FTP Data (usually not needed)	20
FTP Control Protocol	21
SMTP (send mail)	25

TCP Application	Port Number
HTTP (web)	80
POP3 (receive mail)	110
NTP (network time protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

Adding a TCP Application Configuration for Port Forwarding

TCP Application Configuration is required for port forwarding.

STEP 1 Click **VPN > SSL VPN Server > Port Forwarding**.

The Port Forwarding window opens. This page includes two tables:

- List of Configured Applications for Port Forwarding
- List of Configured Host Names for Port Forwarding

STEP 2 To add an application, click **Add** in the List of Configured Applications for Port Forwarding table.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

STEP 3 Enter the following information:

- **Local Server IP Address:** Enter the IP address of the internal host machine or local server.
- **TCP Port Number:** Enter the port number of the TCP application that enables port forwarding.

STEP 4 Click **Apply** to save your settings.

Configuring Host Name Resolution for Port Forwarding

Optionally, you can configure a hostname (FQDN) for the network server to give users an easy way to connect to the server without having to remember and enter an IP address.

NOTE The local server IP address of the configured hostname must match the IP address of the configured application for port forwarding.

STEP 1 Click **VPN > SSL VPN Server > Port Forwarding**.

The Port Forwarding window opens. This page includes two tables:

- List of Configured Applications for Port Forwarding
- List of Configured Host Names for Port Forwarding

STEP 2 To add a configured host name, click **Add** in the List of Configured Host Names for Port Forwarding table.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

STEP 3 Enter the following information:

- **Local Server IP Address:** Enter the IP address of the internal host machine or local server.
- **Fully Qualified Domain Name:** Enter the fully qualified domain name for the TCP application.

STEP 4 Click **Apply** to save your settings.

SSL VPN Tunnel Client Configuration

An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this security appliance. When a SSL VPN client is launched from the user portal, a “network adapter” with an IP address from the corporate subnet, DNS and WINS settings is automatically created. This feature allows access to services on the private network without any special network configuration on the remote SSL VPN client machine.

Make sure that the virtual (PPP) interface address of the VPN tunnel client does not conflict with the address of any physical devices on the LAN. The IP address range for the SSL VPN virtual network adapter should be either in a different subnet or non-overlapping range as the corporate LAN.

If the SSL VPN client is assigned an IP address in a different subnet than the corporate network, a client route must be added to allow access to the private LAN through the VPN tunnel. In addition, a static route on the private LAN's firewall (typically this security appliance) is needed to forward private traffic through the VPN Firewall to the remote SSL VPN client.

NOTE As in any IPsec tunnel deployment, the two networks that are joined by the tunnel must use different IP address ranges in their subnets.

The security appliance allows Full Tunnel and Split Tunnel support.

- **Full Tunnel Mode:** The VPN Tunnel handles all traffic that is sent from the client.
- **Split Tunnel Mode:** The VPN Tunnel handles only the traffic that is destined for the specified destination addresses in the configured client routes. These client routes give the SSL client access to specific private networks, thereby allowing access control over specific LAN services.

Configuring the SSL VPN Client

STEP 1 Click **VPN > SSL VPN Client > SSL VPN Client**.

The SSL VPN Client window opens.

STEP 2 Enter the following information:

- **Enable Split Tunnel Support:** Check this box to enable Split Tunnel Mode Support, or uncheck this box for Full Tunnel Mode Support. With Full Tunnel Mode, all of the traffic from the host is directed through the tunnel. By comparison, with Split-Tunnel Mode, the tunnel is used only for the traffic that is specified by the client routes.

  NOTE If you enable Split Tunnel Support, you also will need to configure SSL VPN Client Routes. After you complete this procedure, see **Configuring Client Routes for Split Tunnel Mode, page 167**.

- **DNS Suffix (Optional):** Enter the DNS Suffix for this client.
- **Primary DNS Server (Optional):** Enter the IP address of the primary DNS Server for this client.

- **Secondary DNS Server (Optional):** Enter the IP address of the secondary DNS Server for this client.
- **Client Address Range Begin:** Enter the first IP address that will be assigned to SSL VPN clients.
- **Client Address Range End:** Enter the last IP address that will be assigned to SSL VPN clients.

  NOTE Configure an IP address range that does not directly overlap with any of addresses on your local network. For example, the default range is 192.168.251.1 to 192.168.251.254.

STEP 3 Click **Apply** to save your settings.

NOTE **Next steps:**
If you enable Split Tunnel Support, you also will need to configure SSL VPN Client Routes. After you complete this procedure, see **Configuring Client Routes for Split Tunnel Mode, page 167**.

Configuring Client Routes for Split Tunnel Mode

If Full Tunnel support is disabled on the SSL VPN Client page, then you must configure client routes for Split Tunnel Mode.

The Configured Client Routes entries are added by the SSL VPN Client such that only traffic to these destination addresses is redirected through the SSL VPN tunnels, and all other traffic is redirected using the hosts (SSL VPN Clients) native network interface. For example if the SSL VPN Client attempts to access this device's LAN network then in Split Tunnel mode, the user should add the LAN subnet as the Destination Network using this page.

NOTE You can configure client routes only if Split Tunnel support is enabled on the SSL VPN Client page. See **Configuring the SSL VPN Client, page 166**.

STEP 1 Click **VPN > SSL VPN Client > Configured Client Routes**.

The Configured Client Routes window opens. Any configured routes are listed in the Configured Client Routes table.

STEP 2 To add a configured client route, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

The SSL VPN Client Route Configuration window opens.

STEP 3 Enter the following information:

- **Destination Network:** Enter the destination subnet to which a route is added on the SSL VPN Client.
- **Subnet Mask:** Enter the subnet mask for the destination network.

STEP 4 Click **Apply** to save your settings.

Viewing the SSL VPN Client Portal

To view the SSL VPN Client Portal, click **VPN> SSL VPN Client > SSL VPN Client Portal**.

NOTE Remote users will use the Portal URL to access the VPN portal.

The client portal provides remote access to the corporate network through the following options in the navigation pane:

- **VPN Tunnel:** After the user clicks the link in the navigation pane, the VPN Tunnel information window opens. The user can click the Launcher icon to connect to the remote network.
- **Port Forwarding:** After the user clicks the link in the navigation pane, the Port Forwarding information window opens. The user can click the Launcher icon to connect to the remote servers.
- **Change Password:** The user can click this link to change his or her password.

NOTE

1. The Change Password section is available only for users who belong to the local data base.
2. The administrator can enable or disable certain features.
3. The user must ensure that Java, Java Script, Active-X controls are enabled or allowed in the web browser settings.

VeriSign™ Identity Protection configuration

Use this page to configure the optional VeriSign™ Identity Protection (VIP) two-factor authentication to authenticate SSL VPN users, providing an enhanced level of security.

NOTE For more information or to order the VeriSign Identity Protection service, go to: www.cisco.com/go/viptoken.

Configuring VeriSign Identity Protection

STEP 1 Click **VPN > VeriSign ID Protection > VIP Configuration**.

The VIP Configuration window opens.

STEP 2 To activate or disable your service, complete the following tasks in the **VeriSign Identity Protection Configuration** area:

a. **Enable VeriSign Identity Protection:** Check this box to enable VIP, or uncheck the box to disable this feature.

b. **Service Type:** Choose the type of service that you acquired from VeriSign:

   - **VIP Pilot/Developer Test Drive:** Choose this option if pilot tokens were provided to you to test and understand VIP service during the initial stages of deployment.
   - **VIP Production:** Choose this option if you have purchased VeriSign service. The service will use VIP production servers to authenticate your users.

c. Click **Apply** to save your settings.

STEP 3 In the **Upload Certificate area**, complete the following tasks:

a. **Certificate File:** Click **Browse**, and then find your VeriSign certificate (RA) file.

a. **Password for the certificate file:** Enter the password that was provided to you along with the certificate (RA) file. The password encrypts the private key provided in the certificate and is required to decrypt and use it.

b. Click **Upload** to upload the certificate.

Managing User Credentials for VeriSign Service

Use this page to associate VeriSign tokens with your users.

NOTE Your users must be configured in Administration first. See **Users, page 171**.

STEP 1 Click **VPN > VeriSign ID Protection > Credential Management**.

The VeriSign Credential Management window opens.

STEP 2 To add a credential, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the VeriSign Credential Configuration window opens.

STEP 3 Enter the following information:

- **Credential Id:** Enter the 6-digit alphanumeric number, which is typically found on the back of the physical token. Each credential identifier must be unique and must not be added if it is already present in the token configuration table.
- **User Name:** Choose the user to associate with the token number. Each credential identifier can be associated with only one user. After the user has been associated with a credential, the same user cannot be associated with a different credential. Only available users are shown in the user list.

STEP 4 Click **Apply** to save your settings.

8

Administration

This chapter describes how to manage users, perform maintenance operations such as firmware upgrade and configuration backup, and how to configure logging and other features for the router. It includes the following sections:

To access the Administration pages, click *Administration* on the Configuration Utility menu bar.

Users

You can use the Users page to assign user names, passwords, and access policies.

There are two default accounts. You can change the user name and password for these accounts but you cannot change the user policies.

- **admin:** The administrator account, which has read-write access to all settings.

- **guest:** A guest account, which has read-only access. This account is disabled by default. To enable the account, edit the User Login Policies. See **Adding or Editing User Login Policies, page 175**.
- **SSL VPN:** An SSL VPN account, which allows access to the services specified in the SSL VPN configuration.

Domains

All SSL VPN users are members of a group, and all groups are members of an authentication domain. The domain must be configured first before any groups and individual users can be assigned to it.

STEP 1 Click **Administration > Users > Domains**.

The Domains window opens.

STEP 2 To add a Domain, click **Add** in the List of Domains table.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Domains Configuration window opens.

STEP 3 Enter the following information:

- **Domain Name:** Enter a unique identifier for the domain.
- **Authentication Type:** Choose the authentication type for this domain.
- **Portal Layout Name:** Choose a portal layout. Layouts are configured through the SSL VPN Portal menu. See **Scenario Step 1: Customizing the Portal Layout, page 157**.

STEP 4 Click **Apply** to save your settings.

When you create a domain, a group is created automatically. It has the same name as the domain and is associated with the domain. To edit the group settings, see **Groups, page 173**.

Groups

Groups are used to create a logical grouping of SSL VPN users that share the authentication domain, LAN and service access rules, and idle timeout settings. They are associated to authenticating domains.

STEP 1 Click **Administration > Users > Groups**.

The Groups window opens.

STEP 2 To add a group, click **Add** in the List of Groups table.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Groups Configuration window opens.

STEP 3 Enter the following information:

- **Group Name:** Enter a unique identifier for the group. You can use any alphanumeric characters.
- **Domain:** Assign a domain from the drop-down list of authentication domains.
- **Idle Timeout:** Enter the number of minutes that a device can be idle before the session is disconnected.

  NOTE The group timeout setting is used as the default timeout setting for all users in the group. You can assign a different idle timeout setting to a user on the Users page. The user settings have precedence over the settings group settings. See **Adding or Editing User Settings, page 173**.

STEP 4 Click **Apply** to save your settings.

Adding or Editing User Settings

The users are part of a group which in turn is a part of an authenticating domain.

NOTE Before you configure users, configure the groups. See **Groups, page 173**.

NOTE For security, a password should contain no dictionary words from any language, and should include a mixture of uppercase and lowercase letters, numbers, and symbols. The password can be up to 30 characters.

STEP 1 Click **Administration > Users > Users**. The List of Users table appears.

The Users window opens.

STEP 2 To add a user, click **Add**, or to edit a user's information, click the button in the **Edit** column. The User Configuration window opens.

The Users Configuration window opens.

STEP 3 Enter the following information:

- **User Name:** Enter a unique identifier for the user. It can include any alphanumeric characters.
- **First Name:** Enter the user's first name.
- **Last Name:** Enter the user's last name.
- **User Type:** Identify the type of account.
- **Select Group:** Choose a group.
- If you are adding a new user, complete the following fields:
  - **Password:** Enter a password that contains alphanumeric, '—' or '_' characters.
  - **Confirm Password:** Enter the password again.
- If you are updating a user's settings, complete the following fields:
  - **Check to Edit Password:** Check this box to enable the password fields.
  - **Enter Your Password:** Enter your password, as a security check before you can change a password.
  - **New Password:** Enter a password that contains alphanumeric, '—' or '_' characters.
  - **Confirm Password:** Enter the password again.
- **Idle Timeout:** Enter the time in minutes that the user can be inactive before the session is disconnected. Enter any value from 0 to 999. The timeout value for the individual user has precedence over the timeout for the group. If you want to ensure that the group's timeout settings are used, set this value to 0.

  NOTE Every user is added as a local user with password, and when the user is assigned to an external authentication mechanism based on the group, certain attributes such as the local password are ignored.

STEP 4 Click **Apply** to save your settings.

Adding or Editing User Login Policies

STEP 1 To add or edit user login policies, click **Administration > Users > Users**.

The Users window opens.

You cannot configure these settings for the system default users, only for the users that you add.

STEP 2 Proceed as needed, based on the type of policy:

- **User Login Policy:** Click the first button in the Edit User Policies column. When the User Login Policies window opens, enter the following information:
  - **Disable Login:** Check this box to disable the account, or uncheck this box to enable the account. This setting cannot be changed for the default admin account.
  - **Deny Login from WAN Interface:** Check this box to prevent the user from logging in from the WAN, or uncheck this box to allow the user to log in from the WAN. This setting cannot be changed for the default admin account.
- **User Login Policy By Browser:** Click the second button in the Edit User Policies column. When the User Policy By Client Browser window opens, enter the following information:
  - In the User Policy By Client Browser area, choose whether to **Deny Login from Defined Browsers** or to **Allow Login only from Defined Browsers**.
  - To add a browser, click **Add**, choose the browser, and then click **Apply**.
  - To delete a browser, check the box, and then click **Delete**.
- **User Login Policy By IP Address:** Click the third button in the Edit User Policies column. When the User Policy By Source IP Address window opens, enter the following information:
  - In the User Policy By Source IP Address area, choose whether to **Deny Login from Defined Addresses** or to **Allow Login only from Defined Addresses**.

- To add an address, click **Add**, enter the type and the address, and then click **Apply**.
- To delete an address, check the box, and then click **Delete**.

STEP 3 Click **Apply** to save your settings.

Firmware and Configuration

This section describes the following maintenance tasks:

- **Upgrading Firmware and Working with Configuration Files**
- **Maintaining the USB Device**
- **Using the Secondary Firmware**

Upgrading Firmware and Working with Configuration Files

You can use the Firmware & Configuration page to perform the following tasks:

- Upgrade the firmware version and check for new availability.
- Backup custom configuration settings for later restoration.
- Restore your saved settings from a backup file or revert to the factory default settings.
- Reboot the security appliance.

  IMPORTANT! During a restore operation or firmware upgrade, do NOT try to go online, turn off the device, shut down the PC, or interrupt the process in anyway until the operation is complete. This process should take only two minutes or so including the reboot process. Interrupting the upgrade process at specific points when the flash is being written to can corrupt the flash memory and render the router unusable without a low-level process of restoring the flash firmware (not through the Configuration Utility).

STEP 1 Click **Administration > Firmware & Configuration > Network**.

The Firmware & Configuration (Network) window opens.

STEP 2 Perform the following tasks, as needed:

- **Status**

  Displays the firmware status. Includes the primary and secondary firmware version, the time when the firmware check was last performed, the latest available image for your device, and a link to latest firmware release notes on Cisco.com. See Release Notes located under Technical Documentation at: www.cisco.com/go/sa500resource.

  If a firmware upgrade is available, select one of the following:

  - **Upload:** Check this option to upgrade the firmware.
  - **Upload & Factory Reset:** Check this option to upgrade your firmware and reset your security appliance to the default settings.

    If you choose not to upgrade, you are reminded that a new firmware is available every 24 hours.

    You can also view the firmware status from the Status pages. See **Device Status, page 204**.

- **Check for New Firmware & Download**:

  - **Check Periodically**: Check this option to automatically check for firmware updates on a daily basis (every 24 hours). Enter your Cisco **User Name** and **Password** and click **Apply** to save your settings.

    NOTE The Cisco username and password details once applied are applicable to all other services on the router which use them. For example, the Cisco username and login used in Administration is automatically updated for IPS signature downloads.

    If new firmware is available it is automatically downloaded to your device and you are prompted to install it. Click **OK** to close the notification window and then click **Upgrade or Upgrade & Factory Reset.**

  - To see if an upgraded version of the firmware is immediately available, click **Check Now**.

- **Firmware Upgrade**
  - To manually upgrade your firmware, click **Browse**, locate and select the configuration file, and then click **Upload**. When the operation is completed, the security appliance restarts automatically with the new settings.
  - To upgrade your firmware and reset your security appliance to the factory default settings, click **Browse**, locate and select the configuration file, and then click **Upload & Factory Reset**. When the operation is complete, the security appliance restarts automatically with the new settings.
- **Backup/Restore Settings:**
  - To save a copy of your current settings, click **Backup**. Read the warning that appears, and then click **OK**. When the Download window opens, click **Save**, and then choose a location where you want to save the file.
  - To restore your saved settings from a backup file, click **Browse**, locate and select the file, and then click **Restore**. When the operation is completed, the security appliance restarts automatically with the restored settings.
  - To erase your current settings and revert to the factory default settings, click **Default**. After the restore, the security appliance restarts automatically with the restored settings. For more information, see **Appendix D, "Factory Default Settings."**
- **Reboot:** To reboot the security appliance, click **Reboot**.

Maintaining the USB Device

You can use this page to perform the following maintenance tasks on the USB device:

- Mount or unmount the USB device safely.
- Upgrade the firmware for the security appliance.
- Back up and restore the configuration settings for the USB device.

IMPORTANT! Restoring a saved configuration will remove your current settings. Firewall rules, VPN policies, LAN/WAN settings and all other settings will be lost. Back up your settings to ensure that you can restore them later if needed.

Wait until the process is complete.

1. Do NOT close the browser window.
2. Do NOT go online.
3. Do NOT turn off or power-cycle the router.
4. Do NOT shut down the computer.
5. Do NOT remove or unmount the USB device.

STEP 1 Click **Administration > Firmware & Configuration > USB**.

The Firmware & Configuration (USB) window opens.

STEP 2 Perform the following tasks, as needed:

- **Mount/Unmount:**
  - To mount a USB device, insert the device into the USB port. Then click the Refresh button on the browser toolbar. The Mount button is enabled. Click **Mount**.
  - To safely remove a USB device, click **Unmount**.
- **Backup / Restore Settings / Software Upgrade**
  - To save a backup copy of current settings and digital certificates, click **Backup**. The file is saved as cisco.cfg.
  - To restore the settings from a previously saved configuration file, click **Restore**. Locate and select the backup file from the connected USB storage device. A progress bar indicating the status of the restore operation will appear. The security appliance automatically restarts.
  - To upgrade the firmware, select an upgrade file, and then click **Upload** to upload the file, or **Upload & Factory Reset** to upload the file and reset the security appliance to the factory default settings. A progress bar will appear to display the upgrade status.

    For information about downloading firmware upgrade files, see **Upgrading the Firmware, page 24**.

    The router takes several minutes to complete the upgrade. While the upgrade is in progress, the Test LED on the front panel of the router will light up. Wait until the light goes off before accessing the router again. When the image upload is complete, the router automatically restarts.

After a successful upgrade, log in. To verify the firmware version, go to **Status > Device Status**. The Firmware Version (Primary) should be the same as the version that you attempted to install. If the upgrade was unsuccessful, see **Appendix A, "Troubleshooting."**

- **Reboot:** Click **Reboot** if it is necessary to reboot the router.

Using the Secondary Firmware

You can use this feature to revert to the previous firmware version that was in use.

STEP 1 Click **Administration > Firmware & Configuration > Swap Firmware**.

The Swap Firmware window opens.

STEP 2 Click **Switch** to reboot the security appliance by using the secondary firmware image.

NOTE Do not try swap images if a secondary firmware image is not present. Doing so can cause the to router to not boot up.

Diagnostics

You can use the Diagnostics page to assess configuration of the security appliance and to monitor the overall network health.

NOTE These features require an active WAN connection.

STEP 1 Click **Administration > Diagnostics**.

The Diagnostics window opens.

STEP 2 Perform the following tasks, as needed:

- **Ping or Trace an IP Address:** You can use these tools to test your network.
  - **Ping through VPN tunnel:** Check the box to enable pinging through the VPN tunnel. Otherwise, uncheck the box.

  - To test connectivity between the security appliance and a connected device on the network, enter the **IP Address** of the device and then click **Ping**. The results appear in the Command Output page. Click **Back** to return to the Diagnostics page.

  - To view the route between the security appliance and a destination, enter the **IP Address** of the destination, and then click **Traceroute**. The results appear in the Command Output page. The report includes up to 30 “hops” (intermediate routers) between this security appliance and the destination. Click **Back** to return to the Diagnostics page.

- **DNS Lookup:** To retrieve the IP address of any server on the Internet, type the **Internet Name** in the text box and then click **Lookup**. If the host or domain entry exists, you will see a response with the IP address. A message stating “Unknown Host” indicates that the specified Internet Name does not exist.

- **Router Options:** Choose from the following options:

  - To view an IPv4 routing table or an IPv6 routing table, click the **Display** button. The results appear in the Command Output page. Click **Back** to return to the Diagnostics page.

  - To capture all packets that pass through a selected interface, click **Packet Trace**. When the Capture Packets window opens, choose the interface: **LAN**, **Dedicated WAN**, or **Optional WAN**. Click **Start** to begin capturing packets. Click **Stop** to stop the capture. To download the report, click **Download**.

Measuring and Limiting Traffic with the Traffic Meter

Traffic metering allows you to measure and limit the traffic routed by this router. You can set traffic metering for both the dedicated WAN and the optional WAN.

STEP 1 Click **Administration > Traffic Meter > Dedicated WAN** to configure the dedicated WAN, or click **Traffic Meter > Optional WAN** to configure the optional WAN.

The Traffic Meter window opens.

STEP 2 In the **Enable Traffic Meter** area, enter the following information:

- **Enabled Traffic Metering:** Check this box to enable traffic metering on the port. The security appliance will keep a record of the volume of traffic going from this interface. You also can configure the security appliance to place a restriction on the volume of data being transferred.
- **Traffic Limit Type:** Choose one of the following options:
  - **No Limit:** The default option, where no limits on data transfer are imposed.
  - **Download Only:** Limits the amount of download traffic. Enter the maximum allowed data (in Megabytes) that can be downloaded for a given month in the Monthly Limit text box. Once the limit is reached, no traffic is allowed from the WAN side.
  - **Both Directions:** For this setting, the router will calculate traffic for both upload and download directions. The traffic limit typed into the Monthly Limit field is shared by both upload and download traffic. For example, for a 1GB limit, if a 700 MB file is downloaded then the remaining 300 MB must be shared between both upload and download traffic. The amount of traffic downloaded will reduce the amount of traffic that can be uploaded and vice-versa.
- **Monthly Limit:** Enter the volume limit in the Monthly Limit field that is applicable for this month. This limit will apply to the type of direction (Download Only or Both) selected above.
- **Increase This Month's Limit:** If the monthly traffic limit has been reached and you need to temporarily increase the limit, check this option and type in the amount of the increase.

- **This Month's Limit:** Displays the data transfer limit applicable for this month which is the sum of the value in the Monthly Limit field and the Increase this Month's Limit field.

STEP 3 In the **Traffic Counter** area, enter the following information.

- **Traffic Counter:** Specify the type of action to be taken on the traffic counter.
  - **Restart Now:** Choose this option and then click **Apply** to reset the counter immediately.
  - **Specific Time:** Choose this option if you want the counter to restart at a specified date and time. Then enter the time in hours (HH) and minutes (MM) and select the day of the month (1st to Last).
- **Send E-mail Report before restarting counter:** Choose this option to send an email report before the traffic counter is restarted. The email is sent to the address configured in the Logging section, if logging is enabled. See **Remote Logging, page 188**.

STEP 4 In the **When Limit is Reached** area, specify the action that occurs when the traffic counter limit is reached.

- **Block All Traffic:** Choose this option to block all traffic to and from the WAN when the traffic limit is reached.
- **Block All Traffic Except E-mail:** Choose this option to block all traffic to and from the WAN except email traffic.

STEP 5 If traffic metering is enabled, the **Internet Traffic Statistics** area displays the following information:

Start Date/Time	Date on which the traffic meter was started or the last time when the traffic counter was reset.
Outgoing Traffic Volume	Volume of traffic, in Megabytes, that was uploaded through this interface.
Incoming Traffic Volume	Volume of traffic, in Megabytes, that was downloaded through this interface.
Total Traffic Volume	Amount of traffic, in Megabytes, that passed through this interface in both directions.
Average per day	Average volume of traffic that passed through this interface.

% of Standard Limit	Amount of traffic, in percent that passed through this interface against the Monthly Limit.
% of Monthly Limit	Amount of traffic, in percent that passed through this interface against this Month's Limit (if the month's limit has been increased).

Configuring the Time Settings

Use the Time Zone window to configure your time zone, adjust for Daylight Savings Time, and to specify which Network Time Protocol (NTP) server to synchronize the date and time.

STEP 1 Click **Administration > Time Zone**.

The Time Zone window opens.

STEP 2 Enter the following information:

- **Date/Time:** Enter the time zone relative to Greenwich Mean Time (GMT).
- **Automatically Adjust for Daylight Savings Time:** Select this option to automatically adjust the time for Daylight Savings Time.
- **Use Default NTP Servers or Use Custom NTP Servers:** Select either default NTP servers, or enter the IP addresses of up to four custom NTP servers. The default NTP Server settings are as follows:
  - 0.ciscosb.pool.ntp.org
  - 1.ciscosb.pool.ntp.org
  - 2.ciscosb.pool.ntp.org
  - 3.ciscosb.pool.ntp.org

STEP 3 Click **Apply** to save your settings.

Configuring the Logging Options

You can configure logs for various events that occur on your network. Refer to the following topics:

- **Local Logging Config**
- **IPv6 Logging**
- **Remote Logging**
- **Logs Facility and Severity**

For information about viewing the system event logs, IPsec VPN Logs, and Policy Enforcement Logs, see **Active Users, page 213**.

Local Logging Config

You can configure the router to log events such as unicast or broadcast traffic passing through the router, or packets that are dropped due to source MAC filtering.

NOTE Enabling logging options can generate a significant volume of log messages and is recommended for debugging purposes only.

STEP 1 Click **Administration > Logging > Logging Config**.

The Local Logging Config window opens.

STEP 2 Check the box for each logging option that you want to enable, or uncheck the box to disable the specified logging option.

- **Routing Logs:** For each type of traffic, choose the types of packets to be logged (Accepted Packets and Dropped Packets) as described in the **Routing Logs** table.
- **System Logs:** Choose the types of system events to be logged.
  - **All Unicast Traffic:** All unicast packets directed to the router are logged.
  - **All Broadcast/Multicast Traffic:** All broadcast or multicast packets directed to the router are logged.
- **Other Event Logs**: Choose the other types of events to be logged.
  - **Source MAC Filter:** If checked, logs packets matched due to source MAC filtering. Uncheck to disable source MAC filtering logs.

- **Output Blocking Event Log**: If checked, the device displays logs for packets blocked by the ProtectLink service.
- **Bandwidth Limit:** If checked, displays logs related to packets dropped due to Bandwidth Limiting.

STEP 3 Click **Apply** to save your settings.

Routing Logs	
LAN to WAN	Enable logging for firewall rules matching LAN to WAN source and destination. Logging for individual firewall rules should be enabled.
LAN to DMZ	Enable logging for firewall rules matching LAN to DMZ source and destination. Logging for individual firewall rules should be enabled.
DMZ to WAN	Enable logging for firewall rules matching DMZ to WAN source and destination. Logging for individual firewall rules should be enabled.
WAN to LAN	Enable logging for firewall rules matching WAN to LAN source and destination. Logging for individual firewall rules should be enabled.
DMZ to LAN	Enable logging for firewall rules matching DMZ to LAN source and destination. Logging for individual firewall rules should be enabled.
WAN to DMZ	Enable logging for firewall rules matching WAN to DMZ source and destination. Logging for individual firewall rules should be enabled.

IPv6 Logging

This page allows enabling logging rules for IPv6 traffic logging.

STEP 1 Click **Administration > Logging > IPv6 Logging**.

The IPV6 Logging window opens.

STEP 2 Check the box for each logging option that you want to enable, or uncheck the box to disable the specified logging option.

- **Accepted Packets:** This logs packets that were successfully transferred through the segment. This option is useful when the Default Outbound Policy is “Block Always” (see the Firewall Rules page under the Firewall menu).

  For example, let’s say that you want a record of every successful SSH connection from the LAN to the WAN. You would check the **LAN to WAN** box under **Accepted Packets**. Whenever a LAN machine makes an SSH connection to the WAN, a message is logged. (This example assumes that your default outbound policy is “Block Always” and you have enabled a firewall rule to allow SSH traffic from the LAN to the WAN. The firewall rule also must allow logging. For more information, see **Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 103**.)

- **Dropped Packets:** Logs packets that were blocked from being transferred through the segment. This option is useful when the Default Outbound Policy is “Allow Always” (see the Firewall Rules page under the Firewall menu).

  For example, let’s say that you want a record of every blocked SSH connection from the LAN to the WAN. You would check the **LAN to WAN** box under **Dropped Packets**. Whenever a machine on the LAN attempts to make an SSH connection to the WAN, a message is logged. This example assumes that your default outbound policy is “Allow Always” and you have enabled a firewall rule to block SSH traffic from the LAN to the WAN. The firewall rule also must allow logging. For more information, see **Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 103**.

STEP 3 Click **Apply** to save your settings.

Remote Logging

Use this page to enable and configure email logs for various types of logs to a specified email address or to a syslog server.

STEP 1 Click **Administration > Logging > Remote Logging**.

The Remote Logging Config window opens.

STEP 2 In the **Log Options** area, enter a name to identify the device in the remote logs. Every logged message will include this identifier as a prefix for easier identification of the source of the message. The log identifier is added to email and syslog messages.

STEP 3 In the **Enable E-Mail Logs** area, enter the following information:

- **Enable E-Mail Logs:** Check this box to enable email logs.
- **E-mail Server Address:** Enter the IP address or Internet Name of an email server. The router will connect to this server to send email logs when required.
- **Return E-mail Address:** Type the email address where the replies from the SMTP server are to be sent (required for failure messages).
- **Send To E-mail Address:** Type the email address where the logs and alerts are to be sent.
- **Authentication with SMTP server:** If the SMTP server requires authentication before accepting connections, choose either **Login Plain** or **CRAM-MD5** authentication from the drop-down menu and enter the user account name and password. To disable authentication, select **None**.
- **Respond to Identd from SMTP Server:** Check this box to configure the router to respond to an IDENT request from the SMTP server.

STEP 4 In the **Send E-mail logs by Schedule** area, configure the following settings to receive e-mail logs according to a schedule:

- **Unit:** Select the period of time that you need to send the log: Hourly, Daily, or Weekly. To disable sending of logs, select Never.

  This option is useful when you do not want to receive logs by email, but want to keep email options configured so that you can use the Send Log function from the **Status > View Logs** pages.

- **Day:** If logs are to be sent on a weekly basis, choose the day of the week.
- **Time:** Select the time of day when logs should be sent.

STEP 5 If you want the security appliance to send logs to a syslog server, enter the IP address or the Internet name of the server in the **SysLog Server** field.

STEP 6 Click **Apply** to save your settings.

Logs Facility and Severity

A variety of events can be captured and logged for review. These logs can be sent to a syslog server or emailed to a specified address. You can also specify which system messages are logged based on the facility that generated the message and its severity level.

STEP 1 Click **Administration> Logging > Logs Facility and Severity**.

The Logs Facility and Severity window opens.

STEP 2 Select the logging severity level and as defined in the **Log Severity Levels** table.

STEP 3 Check the box for each event that you want to display in the local log or to send to the syslog server.

STEP 4 Click **Apply** to save your settings.

Log Severity Levels	
Emergency (level 0)	System unusable. Syslog definition is LOG_EMERG.
Alert (level 1)	Immediate action needed. Syslog definition is LOG_ALERT.
Critical (level 2)	Critical conditions. Syslog definition is LOG_CRIT.
Error (level 3)	Error conditions. Syslog definition is LOG_ERR.
Warning (level 4)	Warning conditions. Syslog definition is LOG_WARNING.
Notification (level 5)	Normal but significant condition. Syslog definition is LOG_NOTICE.

Information (level 6)	Informational messages only. Syslog definition is LOG_INFO.
Debugging (level 7)	Debugging messages. Syslog definition is LOG_DEBUG. For example: If you select Critical, all messages listed under the Critical, Emergency, and Alert categories are logged.

Managing Certificates for Authentication

Digital Certificates (also known as X509 Certificates), are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CAs) such as such as VeriSign, Thawte and other organizations. Digital Certificates are used by this router during the Internet Key Exchange (IKE) authentication phase as an alternative authentication method. Self certificates are issued to you by various CAs. You create and manage certificates from the Authentication (Certificates) page.

Trusted Certificates (CA Certificate)	Used to verify the validity of certificates generated and signed by the CA. The Trusted Certificates table contains the certificates for each CA and includes this information: **CA Identity (Subject Name)**: The organization or person to whom the certificate is issued. ▪ **Issuer Name**: The name of the CA that issued the certificate. ▪ **Expiry Time**: The date after which the certificate becomes invalid.

Active Self Certificates	Lists the certificates issued to you by a trusted CA and are available for use by the remote IKE servers. The remote IKE server validates the router by using these certificates. To use a self certificate you must first request a certificate from the CA and then download and activate the certificate on your system. The Active Self Certificates table for each certificate includes this information: ▪ **Name.** Name used to identify this certificate. ▪ **Subject Name.** Name which other organizations will see as the holder (owner) of this certificate. Enter the registered business name or official company name. ▪ **Serial Number:** Serial number maintained by the CA and used for identification purposes. ▪ **Issuer Name:** Name of the CA that issued the certificate. ▪ **Expiry Time**: Date on which the certificate expires. It is advisable to renew the certificate before it expires.
Certification Signing Request (CSR)	Contains all the information required to create your digital certificate including the contact information, the common name for which the signed certificate is issued, and the public key of the server that will use the certificate. The Certificate Signing Request table lists the name of the certificates you request and the certificate status.

STEP 1 : Click **Administration > Authentication**.

The Authentication (Certificates) window opens.

STEP 2 For each type of certificate, perform the following actions, as needed:

- To add a certificate, click **Upload**. You can upload the certificate from the PC or the USB device. Click **Browse**, find and select the certificate, and then click **Upload**.
- To delete a certificate, check the box to select the certificate, and then click **Delete**.
- To download the router's certificate (.pem file), click the **Download** button under the Download Settings area.

STEP 3 To request a certificate from the CA, click **Generate CSR**.

The Generate Certification Signing Request window opens.

a. Enter the distinguished name information in the **Generate Self Certificate Request** fields.

  - **Name**: Unique name used to identify a certificate.
  - **Subject**: Name of the certificate holder (owner). The subject field populates the CN (Common Name) entry of the generated certificate and can contain these fields:

    - CN=Common Name
    - O=Organization
    - OU=Organizational unit
    - L= Locality
    - ST= State
    - C=Country

      For example: CN=router1, OU=my_dept, O=my_company, L=SFO, C=US

    Whatever name you choose will appear in the subject line of the generated CSR. To include more than one subject field, enter each subject separated by a comma. For example: CN=hostname.domain.com, ST=CA, C=USA

  - **Hash Algorithm**: Algorithm used by the certificate. Choose between MD5 and SHA-1
  - **Signature Algorithm**: Algorithm (RSA) used to sign the certificate.
  - **Signature Key Length**: Length of the signature, either 512 or 1024.
  - **(Optional)** IP Address, Domain Name, and Email Address

b. Click **Generate**.

   A new certificate request is created and added to the Certification Signing Request (CSR) table. To view the request, click the **View** button next to the certificate you just created.

Configuring RADIUS Server Records

This page allows the user to configure details of any RADIUS servers that are used for authentication.

STEP 1 Click **Administration> RADIUS Server**.

STEP 2 To add a server, click **Add**.

Other options: Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

After you click Add or Edit, the Radius Server Configuration window opens.

STEP 3 Enter the following information:

- **Authentication Server IP Address:** Enter the IP address of the authenticating Radius Server.
- **Authentication Port:** Enter the port number on the Radius server that is used to send the Radius traffic.
- **Secret:** Enter the shared key that is configured on the Radius server. The Secret can contain all characters except for single quote, double quote and space.
- **Timeout:** Enter the number of seconds that the connection can exist before re-authentication is required.
- **Retries:** Enter the number of retries for the device to re-authenticate with the Radius server.

STEP 4 Click **Apply** to save your settings.

License Management

You install and manage licenses from the License Management page. Depending on the type of license, you can upload it, automatically install it by using a Product Authorization Key (PAK), or activate it from Cisco.com.

Supported Licenses	
SSL VPN	Provides remote access for employees, partners, and consultants. This is a permanent license with no usage period or renewal required. The default number of supported seats is 2. ▪ For the SA540 model, a free upgrade to 50 seats is available. You must download a license key from Cisco to enable these seats. To obtain the license key, click the **Upgrade to 50 Seats** link on the License Management page. ▪ For the SA520 and SA520W models, you can increase the seat count from 2 users to 25 users. To add seats, you must purchase an SSL VPN license from Cisco at: www.cisco.com/go/license.
ProtectLink Services (Web/Gateway and Endpoint)	▪ **ProtectLink Web** provides unlimited number of users with web threat protection to prevent access to dangerous websites, and URL filtering to control employee access to non-business related websites. ▪ **ProtectLink Gateway** provides the web security features of ProtectLink Web and combines it with email security to prevent spam, viruses and phishing attacks in email. It is available in a 25 seat or 100 seat license. To download a free trail license for ProtectLink (30-day trial), click the **Free Trial** link on the License Management page. ▪ **ProtectLink Endpoint**: protects Windows PCs and servers against spyware, viruses and other malware.
IPS (Intrusion Prevention System)	Provides protection against worms, attacks, and malware. This license is valid for one year. For more information about IPS, see **Configuring IPS, page 131**.

STEP 1 Click **Administration > License Management,** or from the Getting Started (Advanced) page, under Intrusion Prevention System (IPS), click **Install License**.

The License Management window opens.

The License Status table includes this information:

- **Feature**: Displays the available licenses. Click the **Feature** link to see a description of the license.
- **Status**: Shows if the license is installed or not installed. Licenses cannot be transferred or revoked once they are installed.
- **Seats Available**: Current number of licenses installed.
- **Expiration**: Date on which the license expires shown in MM/DD/YYYY format. For example: 04/23/2010.

  For the ProtectLink licenses, the system automatically updates the seat count and expiration date every 24 hours based on changes made to the licensing server. However, if you want to retrieve this information immediately, click the **Update** button.
- **Action**: Use to perform a next step action. Depending on what you want to do, click one of these links:
  - **Install**: Install and activate the license.
  - **Free Trial**: Download a trial license from Cisco.com.
  - **Renew**: Renew your existing license if your license is about to expire or has already expired.
  - **Upgrade to 25 Seats:** Upgrade the license to enable users. (Only applies to the SA520 and SA520W)
  - **Upgrade to 50 Seats:** Upgrade the license to enable users. Only applies to the SA540)
  - **Device Credentials**: Read-Only. Click this button to display the product ID and serial number of the device and the device credentials.

STEP 2 To install a license, select the feature, and click **Install**.

The License Management Install License window opens.

a. For an IPS license, select one of these installation methods from the Install License page:

   - Installation License Type

     - **License Code (PAK) from cisco.com**: Automatically retrieves and installs the license on the device from the Cisco server. To use this option, enter your PAK ID and Cisco.com username and password. These credentials are required for the device to authenticate to the Cisco server.

       Make sure that the security appliance is set to the current time, or the license will not install properly. See **Configuring the Time Settings, page 184**.

     - **License File downloaded from cisco.com**: Installs a license that was previously downloaded to your PC.

   - **Select Transfer File**: If the license file is located on your PC, or on a USB device, you can download it to the security device. Click **Browse** to locate and select the license file.

     After you finish entering the information in the required fields, click **Validate License**. Click **Back** to return to the License Management page.

b. To install and activate a ProtectLink Web/Gateway or Endpoint license, click **Install** and follow the steps provided on the Install License page.

9

Network Management

This chapter describes how to configure the remote management features for the router. It includes the following sections:

- **RMON (Remote Management)**
- **CDP**
- **SNMP**
- **UPnP**
- **Bonjour**

To access the Network Management pages, click ***Network Management*** from the Configuration Utility menu bar.

RMON (Remote Management)

The primary means to configure this gateway via the browser-independent GUI. The GUI can be accessed from LAN node by using the gateway's LAN IP address and HTTP, or from the WAN by using the gateway's WAN IP address and HTTPS (HTTP over SSL).

The Remote Management page allows you to access the router from a remote WAN network. The security appliance allows remote management securely using HTTPS, i.e. https://.

NOTE Disabling Remote Management prevents SSL VPN access.

IMPORTANT: When remote management is enabled, the router is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the router and misuse it in many ways, it is *highly recommended* that you change the admin and guest passwords before continuing.

STEP 1 Click **Network Management > Remote Management**.

The Remote Management (RMON) window opens.

STEP 2 Enter the following information:

- **Enable Remote Management?:** By default, Remote management is disabled. To enable WAN access to the configuration GUI check the box.

  IMPORTANT: When you enable remote management, the security appliance is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the security appliance and misuse it in many ways, we strongly recommend that you change the admin and guest passwords before continuing.

- **Access Type:** Choose the level of permission for remote management:
  - **All IP Addresses:** If this option is selected, make sure that you change the default password.
  - **IP Address Range:** If this option is selected, enter the **From**: starting IP address for the allowed range and **To**: ending IP address for the allowed range.
- **Only this PC:** If this option is selected, set the following:
  - **IP Address:** IP Address of the PC given remote management permissions
- **Port Number:** Displays the port number used for the remote connection.
- **Remote SNMP Enable**: Check the box to enable SNMP for the remote connection.

STEP 3 Click **Apply** to save your settings.

CDP

Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco manufactured equipment. Each CDP enabled device sends periodic messages to a multicast address and also listens to the periodic messages sent by others in order to learn about neighboring devices and determine the status of these devices. This page provides the configuration options to control CDP.

NOTE Enabling CDP is not recommended on the Dedicated WAN port and the Optional ports because they are connected to insecure networks.

STEP 1 Click **Network Management > CDP**.

The CDP window opens.

STEP 2 Enter the following information:

- **CDP:** Choose one of the following options:
  - **Enable All:** Enable CDP on all port supported by the Device.
  - **Disable All:** Disable CDP
  - **Per Port:** Configure CDP on selective ports, displayed in the port information table.
- **CDP Timer:** This is the time interval between any successive CDP packets sent by the router.
- **CDP Hold Timer:** The hold timer is the amount of time the information sent in the CDP packet should be cached by the device which receives the CDP packet, after which the information is expires.

STEP 3 Click **Apply** to save your settings.

SNMP

Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The router supports the SNMPv2c protocol version and can send traps to a specified community.

Configuring SNMP

STEP 1 Click **Network Management > SNMP > SNMP**.

The SNMP window opens.

STEP 2 To add an entry, click **Add**.

NOTE Click the **Edit** button to edit an entry. To delete an entry, check the box and then click **Delete**. To select all entries, check the box in the first column of the table heading.

The SNMP Configuration window opens.

STEP 3 Enter the following information:

- **IP Address:** Enter the IP Address of the SNMP manager or trap agent.
- **Subnet Mask:** Enter the network mask used to determine the list of allowed SNMP managers.
- **Port:** Enter the SNMP trap port of the IP address to which the trap messages will be sent.

STEP 4 Click **Apply** to save your settings.

Configuring SNMP System Info

You can use this page to configure the MIB (Management Information Base) fields.

STEP 1 Click **Network Management > SNMP > SNMP System Info**.

The SNMP System Info window opens.

STEP 2 Enter the following information:

- **SysContact:** The name of the contact person for this security appliance.
- **SysLocation:** The physical location of the security appliance.
- **SysName:** A name given for easy identification of the security appliance.

STEP 3 Click **Apply** to save your settings.

UPnP

UPnP (Universal Plug and Play) is a feature that allows for automatic discovery of devices that can communicate with this security appliance.

The UPnP Portmap Table displays the IP addresses and other settings of the UPnP devices that have accessed the security appliance.

STEP 1 Click **Network Management > UPnP.**

The UPnP window opens.

STEP 2 Enter the following information:

- **Do you want to enable UPnP?:** Check this box to enable UPnP support and uncheck to disable it. If disabled, the router will not allow for automatic device configuration.
- **Advertisement Period:** This is the period (in seconds) of how often this router will broadcast its UPnP information to all devices within range.
- **Advertisement Time to Live:** This is expressed in hops for each UPnP packet. This is the number of steps a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range.

STEP 3 Click **Apply** to save your settings.

Bonjour

Bonjour is a service advertisement and discovery protocol. Bonjour only advertises the default services configured on the router when Bonjour is enabled.

Configuring Bonjour

STEP 1 To enable Bonjour, click **Firewall > Attacks**. Uncheck the **Block Multicast Packets** box and then click **Apply** to save your savings.

STEP 2 Click **Network Management** on the menu bar, and then click **Bonjour > Bonjour Configuration**.

The Bonjour Configuration window opens.

STEP 3 Check the **Enable Bonjour** box to enable the default services. The available services are csco-sb, http, and https.

On an SA500, you cannot disable a particular service. You can either enable Bonjour or disable it.

STEP 4 Click **Apply** to save your settings.

Associating VLANs

After you enable a Bonjour service, you need to select an available VLAN for the default services to bind with.

STEP 1 Click **Network Management > Bonjour > VLAN Association**.

The VLAN Association window opens.

STEP 2 Select the VLAN from the Available VLANs drop-down menu.

The default services will only be visible to the hosts belonging to the associated VLANs. By default, LAN/Default-VLAN is the broadcasting domain.

STEP 3 Click **Apply** to add the VLAN.

The VLAN associated to the service appears in the List of VLANs table.

To dissociate the VLAN from the service, check the box next the appropriate VLAN and click **Delete**.

.

10

Status

This chapter describes how view the status of your router. It includes the following sections:

- **Device Status**
- **VPN Status**
- **Active Users**
- **View Logs**
- **CDP Neighbor**
- **LAN Devices**
- **Reports**

To access the Status pages click ***Status*** from the Configuration Utility menu bar.

Device Status

The Device Status section consist of the following pages:

- **Device Status**
- **Resource Utilization**
- **Interface Statistics**
- **Port Statistics**
- **Wireless Statistics for the SA520W**

Device Status

Use this Dashboard page to view the current system information.

Status > ***Device Status***

Router Information	
System Name	Unit name of the device.
Firmware (Primary & Secondary)	Version of the firmware that the router is currently using (primary), and the version that the router was previously running (secondary). By default, the router will boot with the primary router information
Serial Number	Serial number of this device, unique per security appliance.
Users (Admin/Guest)	Number of administrative and guest users configured on the system
Resource Utilization	
CPU Utilization	Total CPU usage by the system
Memory Utilization	Total memory usage by the system.
System Up Time	Duration for which the device has been running.
Licenses	
Displays the license status of various licensed features in the system. These features are ProtectLink Gateway, ProtectLink Endpoint, SSL VPN and Intrusion Prevention System.	
Syslog Summary	
Displays the summary of the system event log. Syslog entries can be of different severity levels. The number of logs in each level is displayed.	
Routing Mode	
Displays the routing mode of the router (NAT or Classical routing),	
WAN Mode	
Displays the WAN configuration mode of the router (Single WAN port, Auto-rollover, or Load Balancing).	

LAN Interface	
IP Address	LAN IP address of the router,.
DHCP Mode:	Displays the router’s DHCP server mode. The mode can be Disabled, Server, or Relay.
WAN Interface	
IP Address	IP address for the primary (dedicated) WAN port.
State	Indicates if the WAN connection is UP or DOWN. State will be UP if the link is up and the WAN interface has an IP.
Optional Port (WAN/DMZ/LAN)	
IP address	IP address of the Optional Port. When the Optional Port is in LAN mode, this field will not be displayed.
State	Indicates if the connection is UP or DOWN. When the Optional Port is in LAN or DMZ mode, this field is not displayed. In WAN mode, the state will be UP if the link is up and the WAN interface has an IP.
Access Points	(only applies to SA 520W) Shows how many access points are configured on the SA 520W and how many users are associated with each SSID.
Site to Site VPN	
All Tunnels	Number of active Site-to-Site VPN tunnels and the total number of configured Site-to-Site VPN tunnels.
Remote Access VPN	
SSL Users	Number of active SSL users.
IPsec Users	Number of IPsec users.

Resource Utilization

Use this page to view the resource information for the router.

Device Status > Resource Utilization

CPU Utilization	Displays the CPU statistics of the system including CPU usage by user and kernel, CPU idle, and CPU waiting for IO.
Memory Utilization	Displays the memory status of system (total, used, free, cached, and buffer memory).

Interface Statistics

Use this page to view the data transfer statistics for the Dedicated WAN, Optional, LAN, and WLAN ports. This page is updated every 10 seconds.

Device Status > Interface Statistics

Tx Packets	Number of IP packets leaving the port.
Rx Packets	Number of packets received by the port.
Collisions	Number of signal collisions that have occurred on this interface. A collision occurs when the interface tries to send data at the same time as a port on the other router or computer that is connected to this port.
Tx B/s	Number of bytes leaving the port per second.
Rx B/s	Number of bytes received by the port per second.
Up Time	Duration for which the port has been active. The uptime will be reset to zero when the security appliance or the port is restarted.
Poll Interval	Enter a value in seconds for the poll interval. To modify the poll interval, click the **Stop** button and then click **Start** to restart the automatic refresh using the specified poll interval.
Start	Enables the automatic page refresh.
Stop	Disables the automatic page refresh feature.

Port Statistics

Use this page to view current statistics for an individual port. This page is updated every 10 seconds.

Device Status > Port Statistics

Port Id	Indicates the physical port IDs of the Device (switch).
Tx Bytes	Number of good bytes of data transmitted by a port (including FCS). The preamble is excluded.
Tx Drop Pkts	This counter is incremented each time a packet is dropped due to lack of resources (such as transmit FIFO overflow).
Rx Bytes	Number of data bytes received by a port, including FCS and bad packets. The preamble is excluded.
Rx Drop Pkts	Displays the number of good packets received by a port dropped due to a lack of resources (such as lack of input buffers.
Poll Interval	Enter a value in seconds for the poll interval. This causes the page to re-read the statistics from the security appliance and refresh the page automatically. To modify the poll interval, click the **Stop** button and then click **Start** to restart automatic refresh.
Start	Enables the automatic page refresh.
Stop	Disables the automatic page refresh.

Wireless Statistics for the SA520W

This page shows a cumulative total of relevant wireless statistics for the radio and the access points configured on it. The counters are reset when the device is rebooted.

Radio Statistics

The radio can have multiple virtual access points configured and active concurrently. This table indicates cumulative statistics for the radio.

Device Status > Radio Statistics

Radio	Numerical identification of the radio.
Packets	Number of transmitted/received (tx/rx) wireless packets reported to the radio, over all configured access points.
Bytes	Number of transmitted/received (tx/rx) bytes of information reported to the radio, over all configured access points.
Errors	Number of transmitted/received (tx/rx) packet errors reported to the radio, over all configured access points.
Dropped	Number of transmitted/received (tx/rx) packets dropped by the radio, over all configured access points.
Multicast	Number of multicast packets sent over the radio.

Access Point Statistics

This table displays transmit/receive data for a given access point.

Device Status > Access Point Statistics

SSID Name	Name of the access point.
Radio	Radio number on which the access point is configured.
Packets	Number of transmitted/received (tx/rx) wireless packets on the access point.
Bytes	Number of transmitted/received (tx/rx) bytes of information on the access point.
Errors	Number of transmitted/received (tx/rx) packet errors reported to the access point.
Dropped	Number of transmitted/received (tx/rx) packets dropped by the access point.
Multicast	Number of multicast packets sent over this access point.

Poll Interval	Enter a value in seconds for the poll interval. To modify the poll interval, click the **Stop** button and then click **Start** to restart the automatic refresh using the specified poll interval.

VPN Status

IPsec VPN Status

Use this page to view current statistics for the IPsec connections. You can use buttons on the page to start or stop a connection. The page also refreshes automatically to display the most current status for an SA.

Status > ***VPN Status > IPsec Status***

Policy Name	Name of the IKE or VPN policy.
Endpoint	Displays the IP address of the remote VPN gateway or client.
Tx (KB)	Data transmitted in Kilobytes.
Tx (Packets)	Number of IP packets transmitted.
State	Displays the current status for IKE policies. The status can be either Not Connected or IPsec SA Established.
Action	Click **Connect** to establish an inactive SA (connection) or **Drop** to terminate an active SA (connection). When a VPN policy is in place and is enabled, a connection is triggered by any traffic that matches the policy, and the VPN tunnel is set up automatically. However, you can use the Connect/ Disconnect button to manually connect or disconnect the VPN tunnel.

SSL VPN Status

This page displays the current statistics for the SSL VPN Tunnel connections. You can use the buttons on the page to either start or stop connections.

Status > VPN Status > SSL VPN Status

User Name	Username of the logged in user.
IP Address	Internet IP address from where tunnel establishment was initiated.
Tunnel Specific Fields	
Local ppp interface	Name of ppp interface on the router associated to sslvpn tunnel.
Peer PPP Interface IP	IP address assigned to ppp interface at the remote client side from where the tunnel is established.
Tx Packets	Number of packets associated with the tunnel transferred by the remote client.
Tx Dropped Packets	Number of packets associated with the tunnel dropped while transfering, by the remote client.
Tx Bytes (KB)	Total volume of sent traffic (in Kilobytes) associated with the tunnel.
Rx Packets	Number of packets associated with the tunnel received by the remote client.
Rx Dropped Packets	Number of packets associated with the tunnel dropped while receiving, by the remote client.
Rx Bytes (KB)	Total volume of received traffic (in Kilobytes) associated with the tunnel.
Connection Status	Click **Disconnect** to terminate an active user's session and hence the associated SSLVPN-Tunnel(if any). **NOTE** If the tunnel is not established by the user, the tunnel specific fields will have no values.

Poll Interval	Enter a value in seconds for the poll interval. To modify the poll interval, click the **Stop** button and then click **Start** to restart the automatic refresh using the specified poll interval.
Start	Click to enable the automatic page refresh feature.
Stop	Click **Stop** to disable the automatic page refresh feature.

Quick VPN Status

This page displays the status of QuickVPN connections and allows you to DROP any existing active (ONLINE) connections.

Status > VPN Status > Quick VPN Status

User Name	Name of the IPsec User associated with the QuickVPN tunnel.
Remote IP	Displays the IP address of the remote QuickVPN client. This could be NAT/Public IP if the client is behind the NAT router.
Status	Displays the current status of the QuickVPN client. OFFLINE means that the QuickVPN tunnel is NOT initiated/established by the IPsec user. ONLINE means that QuickVPN Tunnel, initiated/established by the IPsec user, is active.
Action	Click **Drop** to terminate an active/ONLINE connection and hence to change the status of QuickVPN client to OFFLINE.
Poll Interval	Time in seconds, after which the page will automatically reload.To modify the poll interval click the Stop button and use Start to restart automatic refresh.
Start	Click to enable automatic page refresh feature.
Stop	Click Stop to disable the automatic page refresh feature.

Active Users

This page lists the administrator and SSL VPN users who are currently logged into the device. A button on the page allows you to disconnect any user.

Status > Active Users

User Name	A unique identifier for the user.
Group	A group to which the logged-in user belongs.
IP address	IP Address of the host from which the user accessed the Router.
Login Time	Timestamp of when the user first logged into the Router.
Disconnect	Terminates an active user's session and the associated SSLVPN-Tunnel (if any).

View Logs

View All Logs

Use this page to view the system message log contents generated by severity level and facility type.

For information about configuring the logs, see **Configuring the Logging Options, page 185**.

STEP 1 Click **Status > View Logs > View All Logs**.

STEP 2 Select the logs to view.

Log Severity: Choose a log severity level.You can choose from one of these levels: Emergency, Alert, Critical, Error, Warning, Notification, Information, or Debugging. For a description of these levels, see **Logs Facility and Severity, page 189**.

For example: If you select Critical, all messages listed under the Critical, Error Warning, Notification, Information, and Debugging are displayed. Emergency, and Alert categories will not be displayed.

Log Facility: Choose the facility from which the logs are to be viewed.

All	Displays all facility logs.
Kernel logs	Displays logs that are a part of the kernel code.
System logs	Displays user-space applications logs such as NTP, Session and DHCP.
Wireless	Displays logs related to wireless.
IPS	Displays logs generated by the Intrusion Prevention System (IPS).
ProtectLink	Displays logs for ProtectLink Gateway and Endpoint services.
VPN	Displays IKE and SSL VPN related logs.
Firewall	Displays logs related to firewall rules, attacks, and content filtering.
Network	Displays routing, DHCP, WAN, LAN and QoS logs.

STEP 3 Enter the Source and Destination IP address for filtering the firewall logs.

Wildcard characters such as asterisk (*) and dot (.) are allowed in the source and destination address fields

STEP 4 Click **Apply** to save your settings.

The log information is displayed in the Log Area. It includes this information:

Date	Date and time of corresponding log.
Severity	Severity of corresponding log.
Facility	Facility of corresponding log.
Source IP	Source IP address of corresponding log.
Destination IP	Destination IP address of corresponding log.
Log Data	Contents of each log.

- Click **Refresh Logs** to see the entries added after the page was opened.
- Click **Clear Logs** to delete all entries in the log window.
- Click **Send Logs** to email the log messages that are currently displayed in the log window. The logs are sent to the email addresses that you configured in

Remote Logging Configuration page. For more information, see **Remote Logging, page 188**

IPsec VPN Logs

Use this page to view the log contents generated by all IPsec VPN policies. The logs are generated automatically and need not be enabled explicitly. This page shows the status of the recent IPsec VPN activity.

Status > View Logs > IPsec VPN Logs

- Click **Refresh Logs** to see the entries added after the page was opened.
- Click **Clear Logs** to delete all entries in the log window.

ProtectLink Logs

Use this page to displays the logs for ProtectLink services events.

Status > View Logs > ProtectLink Logs

- Click **Clear Logs** to delete all entries in the log window
- Click **Refresh Logs** to view the entries added after the page was opened.
- Click **Send Logs** to e-mail the log messages currently displayed in the log window. Ensure that the e-mail address and server information are configured on the Firewall Logs & E-mail page (under Administration menu) before clicking Send Log.

CDP Neighbor

The Cisco Discovery Protocol (CDP) provides information about other devices that are connected to this device and that support the CDP protocol. The page displays information specific to the device and identifies the network interface of this device on which the neighbor was discovered. For more information about CDP Global Configuration, see **CDP, page 199**.

Status > CDP Neighbor

Device Id	Displays the device identifier advertised by the neighbor
Local Port	Interface on which the neighbor was discovered.

Duration	The number of minutes a device has been connected.
Function	The type of device, R-Router, T-Switch Bridge, S-Switch, H-Host, I-IGMP, r-repeater.
Platform	Platform name of the neighboring device.
Interface ID	Interface identifier of the neighbor.

LAN Devices

The LAN Devices page displays all the hosts that are connected to the LAN network. For each device, the page displays the IP address and the associated MAC address. The Name field is also displayed for hosts that identify themselves using NETBIOS. For all other devices the name is displayed as “Unknown.”

Reports

Use the Reports page to display the top 10 websites that have been visited or the top 10 websites that have been blocked by content filtering or ProtectLink URL filtering components. The page is only active when Content Filtering or ProtectLink URL filtering components are enabled. To open this page, click **Status** > **Reports**.

From the **Report View** list, choose the type of report to view from the drop-down list, either Website Hits or Website Blocks. Then click **Apply** to save your changes.

- Click **Refresh Data** to update the data on the screen.
- Click **Reset Data** to reset the values to 0.

NOTE *Elapsed Collection Time* indicates the period of time in which the data was collected.

A

Troubleshooting

Internet Connection

Symptom: You cannot access the Configuration Utility from a PC on your LAN.

Recommended action:

STEP 1 Check the Ethernet connection between the PC and the security appliance.

STEP 2 Ensure that the IP address of your PC is on the same subnet as the security appliance. If you are using the recommended addressing scheme, your PC's address should be in the range 192.168.75.2 to 192.168.75.254.

STEP 3 Check the IP address of your PC. If the PC cannot reach a DHCP server, some versions of Windows and MacOS generate and assign an IP address. These auto-generated addresses are in the range 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.

STEP 4 If your IP address has changed and you don't know what it is, reset the security appliance to the factory default settings (including firewall IP address 192.168.75.1).

If you do not want to reset to factory default settings and lose your configuration, reboot the security appliance and use a packet sniffer (such as Ethereal™) to capture packets sent during the reboot. Look at the Address Resolution Protocol (ARP) packets to locate the LAN interface address.

STEP 5 Launch your browser and ensure that Java, JavaScript, or ActiveX is enabled. If you are using Internet Explorer, click **Refresh** to ensure that the Java applet is loaded. Close the browser and launch it again.

STEP 6 Ensure that you are using the correct login information. The factory default login name is **cisco** and the password is **cisco**. Ensure that CAPS LOCK is off when entering this information.

Symptom: The security appliance does not save my configuration changes.

Recommended action:

STEP 1 When entering configuration settings, click **Apply** before moving to another menu or tab; otherwise your changes are lost.

STEP 2 Click **Refresh** or **Reload** in the browser, which will clear a cached copy of the old configuration.

Symptom: The security appliance cannot access the Internet.

Possible cause: If you use dynamic IP addresses, your security appliance is not requesting an IP address from the ISP.

Recommended action:

STEP 1 Launch your browser and determine if you can connect to an external site such as www.google.com.

STEP 2 Launch the Configuration Utility.

STEP 3 Click **Status > Device Status > Device Status**.

STEP 4 In the **Dedicated WAN Info** area, find the **IPv4 Address**. If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP. See the next symptom.

Symptom: The security appliance cannot obtain an IP address from the ISP.

Recommended action:

STEP 1 Turn off power to the cable or DSL modem.

STEP 2 Turn off the security appliance.

STEP 3 Wait 5 minutes, and then reapply power to the cable or DSL modem.

STEP 4 When the modem LEDs indicate that it has resynchronized with the ISP, reapply power to the security appliance. If the security appliance still cannot obtain an ISP address, see the next symptom.

Symptom: The security appliance still cannot obtain an IP address from the ISP.

Recommended action:

STEP 1 Click **Networking > WAN > IPv4 Config**.

STEP 2 Ask your ISP the following questions:

- Is a login required for your Internet connection? If so, which type? On the IPv4 WAN Configuration page, check the box for **Internet Connection Requires a Login**. Choose the correct ISP Connection Type, and then enter the account information as specified by the ISP (User Name, Password, and Secret, if applicable).
- Does your ISP checks for your PC's hostname? If yes, in the **User Name** field, enter the PC hostname that is required for your ISP account.
- Is your ISP expecting you to login from a particular Ethernet MAC address? If yes, in the **Router's MAC Address** area, choose **Use this MAC Address** for the **MAC Address Source**, and then enter the required MAC address in the field provided.

Symptom: The security appliance can obtain an IP address, but PC is unable to load Internet pages.

Recommended action:

STEP 1 Ask your ISP for the addresses of its designated Domain Name System (DNS) servers. Configure your PC to recognize those addresses. For details, see your operating system documentation.

STEP 2 On your PC, configure the security appliance to be its TCP/IP gateway.

Date and Time

Symptom: Date shown is January 1, 2000.

Possible cause: The security appliance has not yet successfully reached a network time server (NTS).

Recommended action:

STEP 1 If you have just configured the security appliance, wait at least 5 minutes, click **Administration > Time Zone**.

STEP 2 Review the settings for the date and time.

STEP 3 Verify your Internet access settings.

Symptom: The time is off by one hour.

Possible cause: The security appliance does not automatically adjust for Daylight Savings Time.

Recommended action:

STEP 1 Click **Administration > Time Zone**.

STEP 2 Check or uncheck **Automatically adjust for Daylight Savings Time**.

STEP 3 Click **Apply** to save your settings.

Pinging to Test LAN Connectivity

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an ICMP echo-request packet to the designated device. The device responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your PC or workstation.

Testing the LAN path from your PC to your security appliance

STEP 1 On your PC, click the Windows **Start** button, and then click **Run**.

STEP 2 Type ping <IP_address> where <IP_address> is the IP address of the security appliance. Example: ping 192.168.75.1.

STEP 3 Click **OK**.

STEP 4 Observe the display:

- If the path is working, you see this message sequence:

  ```
  Pinging <IP address> with 32 bytes of data
  Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
  ```

- If the path is not working, you see this message sequence:

  ```
  Pinging <IP address> with 32 bytes of data
  Request timed out
  ```

STEP 5 If the path is not working, test the physical connections between the PC and the security appliance:

- If the LAN port LED is off, go to the “LED displays” section on page B-1 and follow instructions for “LAN or Internet port LEDs are not lit.”
- Verify that the corresponding link LEDs are lit for your network interface card and for any hub ports that are connected to your workstation and firewall.

STEP 6 If the path is still not up, test the network configuration:

- Verify that the Ethernet card driver software and TCP/IP software are installed and configured on the PC.
- Verify that the IP address for the security appliance and PC are correct and on the same subnet.

Testing the LAN path from your PC to a remote device

STEP 1 On your PC, click the Windows **Start** button, and then click **Run**.

STEP 2 Type ping -n 10 <IP_address> where -n 10 specifies a maximum of 10 tries and <IP address> is the IP address of a remote device such as your service provider's DNS server. Example: ping -n 10 10.1.1.1.

STEP 3 Click **OK** and then observe the display (see the previous procedure).

STEP 4 If the path is not working, do the following:

- Check that the PC has the IP address of your firewall is listed as the default gateway. (If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel.)
- Verify that the network (subnet) address of your PC is different from the network address of the remote device.
- Verify that the cable or DSL modem is connected and functioning.
- Call your ISP and go through the questions listed in **Symptom: The security appliance still cannot obtain an IP address from the ISP.**
- Ask your ISP if it rejects the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic from the MAC address of only your broadband modem. Some ISPs additionally restrict access to the MAC address of just a single PC connected to that modem. If this is the case, configure your firewall to clone or spoof the MAC address from the authorized PC. For more information, see **Configuring the WAN Connection, page 37**.

Restoring Factory Default Configuration Settings

To restore factory default configuration settings, take one of the following actions:

- Launch the Configuration Utility and login. Click **Administration > Firmware & Configuration > Network**. In the **Backup/Restore Settings** area, click **Default**.

  OR

- Press and hold the Reset button on the front panel about the security appliance for about 10 seconds, until the test LED lights and then blinks. Release the button and wait for the security appliance to reboot. If the security appliance does not restart automatically; manually restart it to make the default settings effective.

After a restore to factory defaults, the following settings apply:

- LAN IP address: **192.168.75.1**
- Username: **cisco**
- Password: **cisco**
- DHCP server on LAN: **enabled**
- WAN port configuration: **Get configuration via DHCP**

B

Standard Services

The security appliance is configured with the following list of standard services that are available for port forwarding and firewall configuration. If you want to configure a port forwarding rule or a firewall rule for a service that is not on this list, you can create a custom service for that purpose. See **Creating Custom Services, page 104**.

ANY

AIM

BGP

BOOTP_CLIENT

BOOTP_SERVER

CU-SEEME:UDP

CU-SEEME:TCP

DNS:UDP

DNS:TCP

FINGER

FTP

HTTP

HTTPS

ICMP-TYPE-3

ICMP-TYPE-4

ICMP-TYPE-5

ICMP-TYPE-6

ICMP-TYPE-7

ICMP-TYPE-8

ICMP-TYPE-9

ICMP-TYPE-10

ICMP-TYPE-11

ICMP-TYPE-13

ICQ

IMAP2

IMAP3

IRC

NEWS

NFS

NNTP

PING

POP3

PPTP

RCMD

REAL-AUDIO

REXEC

RLOGIN

RTELNET

RTSP:TCP

RTSP:UDP

SFTP

SMTP

SNMP:TCP

SNMP:UDP

SNMP-TRAPS:TCP

SNMP-TRAPS:UDP

SQL-NET

SSH:TCP

SSH:UDP

STRMWORKS

TACACS

TELNET

TFTP

VDOLIVE

C

Technical Specifications and Environmental Requirements

Feature	SA520	SA520W	SA540
Standards	IEEE 802.3 CSMA1CD IEEE 802.3i 10BASE-T IEEE 802.3U 100BASE-TX IEEE 802.3x (full duplex flow Control) IEEE 802.3ab (1000BASE-T) Auto MDI1MDIX IEEE 802.3Z (1000BASE-X)	IEEE 802.3 CSMA1CD IEEE 802.3i 10BASE-T IEEE 802.3U 100BASE-TX IEEE 802.3x (full duplex flow Control) IEEE 802.3ab (1000BASE-T) Auto MDI1MDIX IEEE 802.3Z (1000BASE-X) IEEE 802.11n IEEE 802.1b, g, and n	IEEE 802.3 CSMA/CD IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3x (full-duplex flow control) Auto MDI/MDIX
Physical Interfaces	4 X RJ-45 Connectors for LAN port 1 X RJ-45 Connector for WAN port 1 X RJ-45 Connector for LAN, WAN or DMZ port 1 X USB Connector for USB 2.0 1 X Power switch	4 X RJ-45 Connectors for LAN port 1 X RJ-45 Connector for WAN port 1 X RJ-45 Connector for LAN, WAN or DMZ port 1 X USB Connector for USB 2.0 1 X Power switch 3 X external antennas	8 X RJ-45 connectors for 10BASE-T, 100BASE-TX, 1000BASE-T 1 X RJ-45 connector be able to be a LAN, WAN or DMZ port 1 X RJ-45 connector for WAN port 1 X USB connector for USB 2.0
Operating Temperature	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)

Feature	SA520	SA520W	SA540
Storage Temperature	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)
Operating Humidity	10 to 90 percent relative humidity, non-condensing	10 to 90 percent relative humidity, non-condensing	10 to 90 percent relative humidity, non-condensing
Storage Humidity	5 to 95 percent relative humidity, non-condensing	5 to 95 percent relative humidity, non-condensing	5 to 95 percent relative humidity, non-condensing
Internal Power Supply			
Voltage Range	90 to 264 VaC, Single PHASE	90 to 264 VaC, Single PHASE	90 to 264 VaC, Single PHASE
Input Frequency Range	47 HZ To 63 HZ	47 HZ To 63 HZ	47 HZ To 63 HZ
Output Voltage Regulation	11.4V ~ 12.6 V	11.4V ~ 12.6 V	11.4V ~ 12.6 V
Output Current	MAX 2.5A	MAX 2.5A	MAX 2.5A
Transmit (TX) Power (default)	N/A	11dBm	N/A
Physical Specifications			
Form Factor	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable	1 RU, 19-in. rack-mountable
Dimensions (H x W x D)	1-3/4 x 12-1/8 x 7-1/8 inches (44 x 308 x 180 mm)	1-3/4 x 12-1/8 x 7-1/8 inches (44 x 308 x 180 mm) Antenna adds approximately 6-3/4 inches (171 mm) to height and 1-2/8 inches (30 mm) to depth.	1-3/4 x 12-1/8 x 7-1/8 inches (44 x 308 x 180 mm)
Weight (with Power Supply)	4.91 lb	5.15	5.14 lb

D

Factory Default Settings

General Settings

Feature	Setting
Host Name	Model number
Device Name	Model number
Administrator Username	cisco
Administrator Password	cisco
Allow ICMP echo replies (good for validating connectivity)	disable
Date and Time - Automatic Time Update	enable
Date and Time - Daylight Savings Time	enable
Date and Time - Protocol	NTP
Date and Time - Time Zone	Pacific Time (US & Canada)
DDNS	disable
HTTP Remote Access	enable
HTTPS Remote Access	enable
SNMP - Trusted Peer	IP address
SNMP Agent	disable

Feature	Setting
SNMP Version	SNMP V1 & V2c, SNMP V3
SNMP Read-Only Community String	public
SNMP Read-Write Community String	private
SNMP Traps	disable
System Logging - Notify Level	Informational
System Logging	disable
System Logging - Log UnAuthorized Login Attempts	enable
System Logging - Log Authorized Login Attempts	enable
System Logging - Log System Errors	enable
System Logging - Configuration Changes	enable
Email Server Requires Authentication	disable
Cisco Discovery Protocol	enabled on LAN / disabled on WAN port
Bonjour	enabled on LAN / disabled on WAN port
UPnP	disable
Radius Server Port	1812

Router Settings

Feature	Setting
VLAN - Voice, Name	Voice VLAN
VLAN - Voice, VLAN Number (802.1q tagged packets)	100
VLAN - Voice, IP Address	10.1.1.1
VLAN - Voice, IP Address Distribution	DHCP Server
VLAN - Voice, Start IP Address	10.1.1.50
VLAN - Voice, End IP Address	10.1.1.254
VLAN - Voice, Subnet Mask	255.255.255.0
VLAN - Data, Lease Time in Minutes	1440
HTTP Remote Access	disable
HTTPS Remote Access	disable
VLAN - Data, Name	Data VLAN
VLAN - Data, VLAN Number (untagged packets)	1
VLAN - Data, IP Address	See Product Tab
VLAN - Data, IP Address Distribution	DHCP Server
VLAN - Data, Start IP Address	192.168.x.50
VLAN - Data, End IP Address	192.168.x.254
VLAN - Data, Subnet Mask	255.255.255.0
VLAN - Data, Lease Time in Minutes	1440
HTTP Remote Access	enable

Feature	Setting
HTTPS Remote Access	enable
WAN1 IP address assignment	DHCP client
WAN1 - MTU	1500
WAN1- Outgoing Traffic Bandwidth Limit	disable
Allow ICMP echo replies (good for validating connectivity)	disable
HTTPS Remote Access	disable
WAN2 IP address assignment	DHCP client
WAN2 - MTU	1500
WAN2- Outgoing Traffic Bandwidth Limit	disable
Allow ICMP echo replies (good for validating connectivity)	disable
HTTPS Remote Access	disable
Routing (RIP1/2)	disable
Inter-VLAN routing	enable / disable on DMS VLAN
Static Routing	disable
IPv4 and IPv6	IPv4 Only
IPSec - Signaling Authentication - Key Exchange Method	Automatic
IPSec - Signaling Authentication - Auto Reconnect	enable
IPSec - Signaling Authentication - Local Subnet (Data VLAN subnet)	192.168.10.0
IPSec - Signaling Authentication - Local Subnet (Data VLAN subnet mask)	255.255.255.0

Feature	Setting
IPSec - Signaling Authentication - Keying Mode	IKE with PSK
IPSec - Signaling Authentication - Phase 1 - Mode	Main Mode
IPSec - Signaling Authentication - Phase 1 - Encryption Algorithm	3DES-CBC, AES 256
IPSec - Signaling Authentication - Phase 1 - Hash Algorithm	SHA1
IPSec - Signaling Authentication - Phase 1 - Group Description Attribute	DH Group 2 (1024 bit)
IPSec - Signaling Authentication - Phase 1 - Lifetime in Seconds	28800
IPSec - Signaling Authentication - Phase 1 - Rekey Margin	540
IPSec - Signaling Authentication - Phase 1 - Rekey Fuzz Percent	100
IPSec - Signaling Authentication - Phase 1 - Negotiation Attempts	Infinite
IPSec - Signaling Authentication - Phase 2 - Encryption Algorithm	3DES-CBC, AES 256
IPSec - Signaling Authentication - Phase 2 - Authentication Algorithm	SHA1
IPSec - Signaling Authentication - Phase 2 - Use PFS	disable
IPSec - Signaling Authentication - Phase 2 - Group Description Attribute	DH Group 2 (1024 bit)
IPSec - Signaling Authentication - Phase 2 - Hash Algorithm	SHA1

Feature	Setting
IPSec - Signaling Authentication - Phase 2 - Lifetime in Seconds	3600
IPSec Pass through	enable
PPTP Pass through	enable
L2TP Pass through	enable

Wireless Settings

Feature	Setting
VLAN - Voice, VLAN Number (802.1q tagged packets)	100
VLAN - Voice, Name (optional)	Voice VLAN
SSID Name	cisco-voice
SSID Broadcast	disable
Wireless Isolation (within SSID):	disable
802.1q Priority	5
802.11e Priority	6
VLAN - Data, VLAN Number (untagged packets)	1
VLAN - Data, IP Address Assignment (Management)	DHCP Client
VLAN - Data, IP Address (Failover when no DHCP Server Available)	See Product Tab
VLAN - Data, Subnet Mask (Failover when no DHCP Server Available)	255.255.255.0
VLAN - Data, Name (optional)	Data VLAN

Feature	Setting
SSID Name	cisco-data
SSID Broadcast	disable
Wireless Isolation (within SSID):	disable
802.1q Priority	0
Radius Server Port	1812
Key Renewal Timeout	3600
Connection Control (MAC address filtering)	Disabled
Wireless Isolation (between SSIDs):	enabled
Wireless Network Mode	Mixed (802.11b,g,n)
Wireless Channel	Auto
CTS Protection Mode	disabled
Basic Data Rates (Advertised)	All
Beacon Interval	100 ms
DTIM Interval	2 ms
RTS Threshold	2347
Fragmentation Threshold	2346
Power Output	100%
Radio	disabled
802.1x supplicant	disabled
Clustering of Access Points - unique to AP54x	disabled
Broadcast / Multicast Rate Limiting	disabled
Broadcast / Multicast Rate Limit	50pps
Multicast traffic rate per radio	auto

Feature	Setting
MAC Authentication Default Action	Permit
Load Balancing Mode	disabled
802.1d Spanning tree mode on wired / WDS link	disabled
Country or Band code for Radio such as FCC, ETSI etc.	Depends on SKU
Channel Bandwidth	40Mhz
Maximum associations supported	200
Antenna Selection, automatically selects best antenna	Auto
WMM APSD Power mode setting	On
AP Detection for neighbor AP - both rogue and known APs	enabled
For a multiple-radio AP, which radio this WDS link is using	Radio 1
Arbitration Inter Frame Spacing (AIFS)	4 queues = 1ms, 1ms, 3ms, 7ms
Minimum contention window	4 queues = 3ms, 7ms, 15ms, 15ms
Maximum Burst	4 queues - 1.5ms, 3ms, 0ms, 0ms
Maximum contention window	4 queues = 7ms, 15ms, 15ms, 15ms

Storage

Feature	Setting
VLAN - Data, IP Address Assignment (Management)	DHCP Client
VLAN - Data, IP Address (Failover when no DHCP Server Available)	See Product Tab
VLAN - Data, Subnet Mask (Failover when no DHCP Server Available)	255.255.255.0
Windows workgroup name	WORKGROUP
HTTP Access Administration	80
HTTP File Access	8080
FTP File Access	21
HTTPS Administration Access	443
Dual Link Mode (802.3ad Link Aggregation, Active Backup)	Active Backup
Idle Drive Spin Down (1-8 hours, 1 day)	8 hours
Public access to share	Read-only
Idle Disconnect Timeout	5 minutes
Banner	Welcome to the Cisco Small Business FTP Server
Allow Anonymous Access	disable
Allow Anonymous File Upload	disable
Allow Anonymous File Download	enable
Maximum Anonymous Transfer Rate (0 - unlimited) in KB/s	0
Disconnect Idle Sessions	5 minutes

Feature	Setting
Disconnect Stalled Sessions	5 minutes
Maximum Connections per IP Address	5
Default File Creation Attributes (Group Read/Write, Everyone Read/Write	enable
Enable users to delete and rename other's files and folders	enable

Security Settings

Feature	Setting
UpNP	Disabled
Remote Management	Disabled
CDP. Enabled on LAN, disabled on WAN	Disabled on WAN
Firewall	Inbound Deny / Outbound Allow
Respond to Ping on internet	Disabled
Enable Stealth Mode	Enable
Block TCP Flood	Enable
Block UDP Flood	Enable
Block ICMP Notification	Enable
Block Fragmented Packets	Enable
Block Multicast Packets	Enable
SYN Flood Detect Rate	128 max/sec
Echo Storm (ping packets/sec)	15 packets/sec

Feature	Setting
ICMP Flood (ICMP packets/sec)	100 packets/sec

E

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the SA500 Series Security Appliances.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation	www.cisco.com/support (Log in required)
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Software	
Quick VPN Software	www.cisco.com/go/qvpn
Cisco VPN Client	www.cisco.com/go/ciscovpnclient
SA500 Firmware Downloads	www.cisco.com/go/sa500software
Product Documentation	
SA500 Technical Documentation	www.cisco.com/go/sa500resources
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb