2

Configuration Wizards

This chapter describes how to use the configuration wizards to configure the security appliance. It includes the following sections:

To access the Configuration Wizards pages, click **Configuration Wizards** in the left hand navigation pane.

Using the Setup Wizard for the Initial Configuration

Use the Setup Wizard to quickly configure the primary features of your security appliance, such as Cisco.com account credentials, security license, remote administration, port, WAN, LAN, DMZ, WAN redundancy, WLAN (for ISA550W and ISA570W only), and security services. Refer to the following steps:

- **Starting the Setup Wizard, page 37**
- **Configuring Cisco.com Account Credentials, page 37**
- **Enabling Firmware Upgrade, page 38**
- **Validating Security License, page 39**
- **Enabling Bonjour and CDP Discovery Protocols, page 39**
- **Configuring Remote Administration, page 40**
- **Configuring Physical Ports, page 41**
- **Configuring the Primary WAN, page 42**
- **Configuring the Secondary WAN, page 42**
- **Configuring WAN Redundancy, page 42**
- **Configuring Default LAN Settings, page 43**
- **Configuring DMZ, page 44**
- **Configuring DMZ Services, page 45**
- **Configuring Wireless Radio Settings, page 47**
- **Configuring Intranet WLAN Access, page 48**
- **Configure Security Services, page 49**
- **Viewing Configuration Summary, page 50**

NOTE Before you use the Setup Wizard to configure your security appliance, we recommend that you have the following requirements:

- An active WAN connection for verifying your Cisco.com account credentials, validating the security license, and upgrading your firmware to the latest version from Cisco.com.

- A valid Cisco.com account for validating the security license and upgrading your firmware to the latest version from Cisco.com. To register a Cisco.com account, go to https:// tools.cisco.com/RPF/register/register.do.
- The Product Authorization Key (PAK), or license code, for validating the security license and activating security services. You can find the license code from the Software License Claim Certificate that Cisco provides upon purchase of the security appliance.

Starting the Setup Wizard

STEP 1 When you log in to the Configuration Utility for the first time, the Setup Wizard may launch automatically. To launch the Setup Wizard at any time, click **Configuration Wizards > Setup Wizard**.

The Getting Started page appears If you have applied a configuration, a warning message appears saying “Continuing with the Setup Wizard will overwrite some of your previously modified parameters.” Read the warning message carefully before you start configuring.

STEP 2 Click **Next**.

Configuring Cisco.com Account Credentials

STEP 3 Use the Cisco.com Credentials page to configure your Cisco.com account credentials.

A valid Cisco.com account is required to download the latest firmware image from Cisco.com, validate the security license, and check for signature updates from Cisco’s signature server for IPS, Application Control, and Anti-Virus. If you do not already have one, go to https:// tools.cisco.com/RPF/register/register.do by clicking the **Create a Cisco.com Account** link to register a Cisco.com account.

- **Username:** Enter the username of your Cisco.com account.
- **Password:** Enter the password of your Cisco.com account.

STEP 4 Click **Next**.

If you can access the Internet, the Setup Wizard will validate your Cisco.com account credentials through the Internet after you click **Next**.

If you cannot access the Internet, the Setup Wizard will assume that your Cisco.com account credentials are valid and proceed to next step.

NOTE: You can configure your Cisco.com account credentials on the Device Management > Cisco Services & Support > Cisco.com Account page after the Setup Wizard is complete. See Configuring Cisco.com Account, page 424.

STEP 5 If your Cisco.com account credentials are invalid, click **OK** to return to the Cisco.com Credentials page. Correct your Cisco.com account credentials and then click **Next** to verify them again.

STEP 6 If your Cisco.com account credentials are valid, proceed to the Upgrade Firmware page.

Enabling Firmware Upgrade

STEP 7 Use the Upgrade Firmware page to enable the device to check for firmware updates or to manually upgrade the firmware.

- To automatically check for firmware updates, check the box next to **Check for firmware update when Setup Wizard completes**. The security appliance will immediately check for firmware updates after the Setup Wizard is complete. This feature requires that you have an active WAN connection.
- To manually upgrade the firmware from a firmware image stored on your PC, uncheck the box next to **Check for firmware update when Setup Wizard completes**. Uncheck this box when you do not have an active WAN connection and you have already downloaded the latest firmware image from Cisco.com to your local PC.

STEP 8 If you uncheck the box, click **Browse** to locate and select the firmware image from your PC, and then click **Upgrade**.

After you click Upgrade, the security appliance starts installing the firmware. This process will take several minutes. Do not disconnect the power or reset the device. Doing so will cancel the firmware upgrade process and could possibly corrupt. The security appliance reboots after the firmware is upgraded. You will be redirected to the login screen when the security appliance boots up.

STEP 9 If you choose to automatically check for firmware updates, click **Next**.

Validating Security License

STEP 10 Use the License Installation page to validate the security license, which is used to activate security services on the device.

STEP 11 If the security license is already installed on the security appliance, click **Next** to proceed next step.

STEP 12 If the security license is not installed on the security appliance, enter the following information to validate the security license:

- **Email Address:** Enter the registered email address to receive the PAK ID.
- **PAK ID:** Enter your Product Authorization Key in this field. You can find the license code from the Software License Claim Certificate that Cisco provides upon purchase of the security appliance.

  NOTE: A valid Cisco.com account is required to validate the security license. If your Cisco.com account credentials are not configured, go back to the Cisco.com Credentials page to configure them.

NOTE: If you want to continue the Setup Wizard configuration without installing the security license, check the box next to **Continue without installing license (not recommended)**. The security services cannot be activated without installing the security license.

STEP 13 After you are finished, click **Next**.

Enabling Bonjour and CDP Discovery Protocols

STEP 14 Use the Discovery page to enable Bonjour and/or CDP discovery protocols on the security appliance. For optimal device discovery and topology support via the OnPlus portal, enable both discovery protocols.

- **Enable Bonjour Discovery Protocol:** Check this box to enable Bonjour discovery protocol, or uncheck this box to disable it.
- **Enable Cisco Discovery Protocol (CDP):** Check this box to enable Cisco Discovery Protocol (CDP), or uncheck this box to disable it.

  NOTE: Discovery protocols are only operational on the LAN ports of the security appliance.

STEP 15 After you are finished, click **Next**.

Configuring Remote Administration

STEP 16 Use the Remote Administration page to configure the remote management settings. The security appliance allows remote management securely by using HTTPS and HTTP, for example https://xxx.xxx.xxx.xxx:8080.

- **Remote Administration:** Click **On** to enable remote management by using HTTPS, or click **Off** to disable it. We recommend that you use HTTPS for secure remote management.
- **HTTPS Listen Port Number:** If you enable remote management by using HTTPS, enter the port number. By default, the listen port number for HTTPS is 8080.
- **HTTP Enable:** Click **On** to enable remote management by using HTTP, or click **Off** to disable it.
- **HTTP Listen Port Number:** If you enable remote management by using HTTP, enter the port number. By default, the listen port number for HTTP is 80.
- **Allow Address:** To specify the devices that can access the configuration utility through the WAN interface, choose an Address Object or enter an address.
    - **Address Objects:** These objects represent known IP addresses and address ranges, such as the GUEST VLAN and the DHCP pool. After completing the wizard, you can view information about Address Objects on the Networking > Address Management page.
    - **Create new address:** Choose this option to enter an IP address or address range. In the pop-up window, enter a **Name** and specify the **Type** (Host or Range). For a single host, enter the IP address. For a range, enter the **Starting IP Address** and the **Ending IP Address**.
- **Remote SNMP:** Click **On** to enable SNMP for remote connection, or click **Off** to disable SNMP. Enabling SNMP allows remote users to use the SNMP protocol to access the Configuration Utility.

STEP 17 After you are finished, click **Next**.

Configuring Physical Ports

STEP 18 Use the Port Configuration page to specify the port configuration.

If you are using the ISA570 or ISA570W, choose one of the following options:

- **1 WAN, 9 LAN switch:** One WAN port (WAN1) and nine LAN ports are configured.
- **1 WAN, 1 DMZ, 8 LAN switch:** One WAN port (WAN1), one DMZ port, and eight LAN ports are configured. The configurable port GE10 is set as a DMZ port.
- **1 WAN, 1 WAN backup, 8 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN) and eight LAN ports are configured. The configurable port GE10 is set as the secondary WAN port.
- **1 WAN, 1 WAN backup, 1 DMZ, 7 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN), one DMZ port, and seven LAN ports are configured. The configurable port GE10 is set as the secondary WAN port and the configurable port GE9 is set as a DMZ port.

If you are using the ISA550 or ISA550W, choose one of the following options:

- **1 WAN, 6 LAN switch:** One WAN port (WAN1) and six LAN ports are configured.
- **1 WAN, 1 DMZ, 5 LAN switch:** One WAN port (WAN1), one DMZ port, and five LAN ports are configured. The configurable port GE7 is set as a DMZ port.
- **1 WAN, 1 WAN backup, 5 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN) and five LAN ports are configured. The configurable port GE7 is set as the secondary WAN port.
- **1 WAN, 1 WAN backup, 1 DMZ, 4 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN), one DMZ port, and four LAN ports are configured. The configurable port GE7 is set as the secondary WAN port and the configurable port GE6 is set as a DMZ port.

NOTE: If you have two ISP links, we recommend that you set a backup WAN so that you can provide backup connectivity or load balancing. If you need to host public services, we recommend that you set a DMZ port.

STEP 19 After you are finished, click **Next**.

Configuring the Primary WAN

STEP 20 Use the Primary WAN Connection page to configure the primary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the primary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the primary WAN port. The security appliance supports DHCP Client, Static IP, PPPoE, PPTP, and L2TP. For complete details, see Network Addressing Mode, page 125.

STEP 21 After you are finished, click **Next**.

Configuring the Secondary WAN

STEP 22 If only one WAN port is configured, proceed to **Configuring Default LAN Settings, page 43**. If two WAN ports are configured, use the Secondary WAN Connection page to configure the secondary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the secondary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the secondary WAN port. For complete details, see Network Addressing Mode, page 125.

STEP 23 After you are finished, click **Next**.

Configuring WAN Redundancy

STEP 24 If you have two WAN links, use the WAN Redundancy page to determine how the two ISP links are used.

- **Equal Load Balancing (Round Robin):** Choose this option if you want to re-order the WAN ports for Round Robin selection. The order is as follows: WAN1 and WAN2. The Round Robin will then be back to WAN1 and continue the order.
- **Weighted Load Balancing:** Choose this option if you want to distribute the bandwidth to two WAN ports by the weighted percentage or by the weighted link bandwidth. The two links will carry data for the protocols that are bound to them.

  - **Weighted By Percentage:** If you choose this option, specify the percentage of bandwidth for each WAN, such as 80% for WAN1 and 20% for WAN2.
  - **Weighted by Link Bandwidth:** If you choose this option, specify the amount of bandwidth for each WAN, such as 80 Mbps for WAN1 and 20 Mbps for WAN2.

  NOTE: The Weighted by Link Bandwidth option has the same effect as the Weighted by Percentage option. However, it provides more percentage options than in the Weighted by Percentage field.

- **Failover:** Choose this option if you want to use one ISP link as a backup. If a failure is detected on 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.
  - **Select WAN Precedence:** Choose one of the following options:

    Primary: WAN1; Secondary: WAN2: If you choose this option, WAN1 is set as the primary link and WAN2 is set as the backup link.

    Primary: WAN2; Secondary: WAN1: If you choose this option, WAN2 is set as the primary link and WAN1 is set as the backup link.
  - **Preempt Delay Timer:** Enter the time in seconds that the security appliance will preempt the primary link from the backup link after the primary link is up again. The default is 5 seconds.

STEP 25 After you are finished, click **Next**.

Configuring Default LAN Settings

STEP 26 Use the LAN Configuration page to configure the default LAN settings.

- **IP Address:** Enter the subnet IP address for the default LAN.
- **Netmask:** Enter the subnet mask for the default LAN.
- **DHCP Mode:** Choose one of the following DHCP modes:
  - **Disable:** 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:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the LAN. Any new DHCP client joining the LAN is assigned an IP address of the DHCP pool.
- **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 27 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet as the LAN IP address.
- **Lease Time:** Enter the maximum connection time that a dynamic IP address is “leased” to a network user. When the time elapses, the user is automatically renewed the dynamic IP address.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.
- **WINS2:** Optionally, enter the IP address of the secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the default LAN.
- **Default Gateway:** Enter the IP address of default gateway.

STEP 28 After you are finished, click **Next**.

Configuring DMZ

STEP 29 If you have not configured a DMZ port, proceed to **Configuring Wireless Radio Settings, page 47**. If you configured a DMZ port, use the DMZ Configuration page to configure a DMZ network.

- **IP Address:** Enter the subnet IP address for the DMZ.
- **Netmask:** Enter the subnet mask for the DMZ.

- **DHCP Mode:** Choose one of the following DHCP modes:
  - **Disable:** Choose this option if the computers on the DMZ are configured with static IP addresses or are configured to use another DHCP server.
  - **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the DMZ. Any new DHCP client joining the DMZ is assigned an IP address of the DHCP pool.
  - **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 30 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet with the DMZ IP address.
- **Lease Time:** Enter the maximum connection time that a dynamic IP address is “leased” to a network user. When the time elapses, the user is automatically renewed the dynamic IP address.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.
- **WINS2:** Optionally, enter the IP address of the secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the DMZ.
- **Default Gateway:** Enter the IP address of default gateway.

STEP 31 After you are finished, click **Next**.

Configuring DMZ Services

STEP 32 Use the DMZ Service page to configure the DMZ services.

STEP 33 Click **Add** to create a DMZ service.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete.**

STEP 34 In the DMZ Service - Add/Edit window, enter the following information:

- **Original Service:** Choose a service as the incoming service.
- **Translated Service:** Choose a service as the translated service or choose **Original** if the translated service is same as the incoming service. If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the Networking > Service Management page. See Service Management, page 177.

  NOTE: One-to-one translation will be performed for port range forwarding. For example, if you want to translate an original TCP service with the port range of 50000 to 50002 to a TCP service with the port range of 60000 to 60002, then the port 50000 will be translated to the port 60000, the port 50001 will be translated to the port 60001, and the port 50002 will be translated to the port 60002.
- **Translated IP:** Choose the IP address of your local server that needs to be translated. If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **WAN:** Choose either WAN1 or WAN2, or both as the incoming WAN port.
- **WAN IP:** Specify the public IP address for the server. You can use the IP address of the selected WAN port or a public IP address that is provided by your ISP. When you choose **Both** as the incoming WAN port, this option is grayed out.
- **Enable DMZ Service:** Click **On** to enable the DMZ service, or click **Off** to create only the DMZ service.
- **Create Firewall Rule:** Check this box to automatically create a firewall rule to allow access for this DMZ service. You must manually create a firewall rule if you uncheck this box.

  NOTE: If you choose Both as the incoming WAN port, a firewall rule from Any zone to Any zone will be created accordingly.
- **Description:** Enter the name for the DMZ service.

For example, you host an RDP server (192.168.12.101) on the DMZ. Your ISP has provided a static IP address (172.39.202.102) that you want to expose to the public as your RDP server address. You can create a DMZ service as follows to allow Internet user to access the RDP server by using the specified public IP address.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

NOTE: In this example, you must manually create two address objects (RDPServer and PublicIP) and a TCP service object with the port 3389 called “RDP.”

STEP 35 Click **OK** to save your settings.

STEP 36 After you are finished, click **Next**.

Configuring Wireless Radio Settings

STEP 37 If you are using the ISA550 or ISA570, proceed to **Viewing Configuration Summary, page 50**. If you are using the ISA550W or ISA570W, use the Wireless Radio Setting page to configure the wireless radio settings.

- **Wireless Radio:** Click **On** to turn wireless radio on and hence enable the SSID called “cisco-data,” or click **Off** to turn wireless radio off.
- **Wireless Network Mode:** Choose the 802.11 modulation technique.
  - **802.11b/g mixed:** Choose this mode if some devices in the wireless network use 802.11b and others use 802.11g. Both 802.11b and 802.11g clients can connect to the access point.
  - **802.11g/n mixed:** Choose this mode if some devices in the wireless network use 802.11g and others use 802.11n Both 802.11g and 802.11n clients can connect to the access point.

- **802.11b/g/n mixed:** Choose this mode to allow 802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency to connect to the access point.
- **802.11n only:** Choose this mode if all devices in the wireless network can support 802.11n. Only 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.

- **Wireless Channel:** Choose a channel from a list of channels or choose **Auto** to let the system determine the optimal channel to use based on the environmental noise levels for the available channels.

STEP 38 After you are finished, click **Next**.

Configuring Intranet WLAN Access

STEP 39 If you turned the wireless radio off, proceed to **Viewing Configuration Summary, page 50**. If you turned the wireless radio on, use the Intranet WLAN Access page to configure the wireless connectivity settings for the SSID called “cisco-data.”

- **SSID Name:** The name of the SSID.
- **Security Mode:** Choose the encryption algorithm for data encryption for this SSID and configure the corresponding settings. For complete details, see Configuring Wireless Security, page 211.
- **VLAN Name:** Choose the VLAN to which this SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. For Intranet VLAN access, you must choose a VLAN that is mapped to a trusted zone.

  NOTE: ISA550W and ISA570W support four SSIDs. To configure the wireless connectivity settings for other SSIDs, go to the Wireless > Basic Settings page (see Configuring SSID Profiles, page 210), or use the Wireless Wizard (see Using the Wireless Wizard (for ISA550W and ISA570W only), page 76).

STEP 40 After you are finished, click **Next**.

Configure Security Services

STEP 41 Use the Security Services page to enable security services and to specify how to handle the affected traffic when the reputation-based security services are unavailable.

NOTE:

- Enabling a security service will apply its default settings on the security appliance to provide a moderate level of protection. We strongly recommend that you customize the settings for each enabled security service after the Setup Wizard is complete. For complete details, see **Chapter 7, "Security Services."**

- Application Control and Web URL Filtering need additional configuration on the Security Services pages.

- A valid security license is required to activate security services. If the security license is not yet installed, go back the License Installation page to enter the Product Authorization Key (PAK) and email address. After the Setup Wizard is complete, the security appliance first validates the security license through the Internet and then activates security services.

The following features are available:

- **Anti-Virus:** Anti-Virus blocks viruses and malware from entering your network through email, web, FTP, CIFS, and NetBIOS applications. Check this box to enable the Anti-Virus feature on the security appliance, or uncheck this box to disable it.

- **Intrusion Prevention (IPS):** IPS monitors network protocols and prevents attacks to client devices by analyzing and responding to certain types of network traffic. Check this box to enable the IPS feature on the security appliance, or uncheck this box to disable it.

- **Network Reputation:** Network Reputation blocks incoming traffic from IP addresses that are known to initiate attacks throughout the Internet. Check this box to enable the Network Reputation feature on the security appliance, or uncheck this box to disable it. By default, Network Reputation is enabled.

- **Spam Filter:** Spam Filter detects and blocks email spam. Check this box to enable the Spam Filter feature on the security appliance, or uncheck this box to disable it. If you enable Spam Filter, enter the IP address or domain name of your internal SMTP server in the **Local SMTP Server IP Address** field. The SMTP server must have its Internet traffic routed through the security appliance. The SMTP server or the clients that use this SMTP server can be configured to respond to the spam and suspected spam tags that the security appliance applies to the emails.

- **Web Reputation Filtering:** Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware, or phishing links. Check this box to enable the Web Reputation Filtering feature on the security appliance, uncheck this box to disable it.

  NOTE: Clicking the **Details** link for a security service can open the help page that provides complete details for the security service.

STEP 42 Spam Filter, Network Reputation, Web Reputation Filtering, and Web URL Filtering are reputation-based security services. You can specify how to deal with the affected traffic when these reputation services are unavailable. Choose one of the following options:

- **Prevent affected network traffic:** All affected traffic is blocked until the reputation-based security services are available.
- **Allow affected network traffic:** All affected traffic is allowed until the reputation-based security services are available.

STEP 43 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 44 Use the Summary page to view information about the configuration.

STEP 45 To modify any settings, click **Back**. If the configuration is correct, click **Apply** to apply the settings.

After your configuration is successfully applied, the Setup Wizard immediately checks for firmware updates.

STEP 46 If the Firmware Upgrade window appears, follow the on-screen prompts to download and install the firmware. See Upgrading your Firmware After your First Login, page 33. If you are using the latest firmware, click **Finish**.

Using the Dual WAN Wizard to Configure WAN Redundancy Settings

If you have two ISP links, a backup WAN is required so that you can provide backup connectivity or load balancing. Use the Dual WAN Wizard to configure the WAN redundancy settings. Refer to the following steps:

- **Starting the Dual WAN Wizard, page 51**
- **Configuring a Configurable Port as a Secondary WAN Port, page 51**
- **Configuring the Primary WAN, page 52**
- **Configuring the Secondary WAN, page 52**
- **Configuring WAN Redundancy, page 52**
- **Configuring Network Failure Detection, page 53**
- **Viewing Configuration Summary, page 54**

Starting the Dual WAN Wizard

STEP 1 Click **Configuration Wizards > Dual WAN Wizard**.

STEP 2 Click **Next**.

Configuring a Configurable Port as a Secondary WAN Port

STEP 3 On the Port Configuration page, specify a configurable port (from GE6 to GE10) as the secondary WAN port. The physical port GE1 is reserved for the primary WAN port.

STEP 4 After you are finished, click **Next**.

Configuring the Primary WAN

STEP 5 Use the Primary WAN Connection page to configure the primary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the primary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the primary WAN port. The security appliance supports DHCP Client, Static IP, PPPoE, PPTP, and L2TP. For complete details, see Network Addressing Mode, page 125.

STEP 6 After you are finished, click **Next**.

Configuring the Secondary WAN

STEP 7 Use the Secondary WAN Connection page to configure the secondary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the secondary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the secondary WAN port. For complete details, see Network Addressing Mode, page 125.

STEP 8 After you are finished, click **Next**.

Configuring WAN Redundancy

STEP 9 Use the WAN Redundancy page to determine how the two ISP links are used.

- **Weighted Load Balancing:** Choose this option if you want to use both ISP links simultaneously. Load Balancing distributes the bandwidth to two WAN ports by the weighted percentage or by the weighted link bandwidth. The two links will carry data for the protocols that are bound to them.
  - **Weighted by percentage:** If you choose this option, specify the percentage for each WAN, such as 80% percentage bandwidth for WAN1 and least 20% percentage bandwidth for WAN2.

  - **Weighted by Link Bandwidth:** If you choose this option, specify the amount of bandwidth for each WAN, such as 80 Mbps for WAN1 and 20 Mbps for WAN2, which indicates that 80% bandwidth is distributed to WAN1 and at least 20% bandwidth is distributed to WAN2.

  NOTE: The Weighted by Link Bandwidth option has the same effect with the Weighted by Percentage option. It just provides more percentage options than Weighted by Percentage that only provides three percentage options.

- **Failover:** Choose this option if you want to use one ISP link as a backup. The Failover mode directs all Internet traffic to the secondary link if the primary link is down. When the primary link regains connectivity, all Internet traffic is directed to the primary link and the secondary link becomes idle.

  - **Select WAN Precedence:** Choose one of the following options:

    Primary: WAN1; Secondary: WAN2: If you choose this option, WAN1 is set as the primary link and WAN2 is set as the backup link.

    Primary: WAN2; Secondary: WAN1: If you choose this option, WAN2 is set as the primary link and WAN1 is set as the backup link.

  - **Preempt Delay Timer:** Enter the time in seconds that the security appliance will preempt the primary link from the backup link after the primary link is up again. The default is 5 seconds.

STEP 10 After you are finished, click **Next**.

Configuring Network Failure Detection

STEP 11 Use the Network Detection page to configure network failure detection.

- **Retry Count:** Enter the number of retries. The security appliance repeatedly tries to connect to the ISP after the network failure is detected.

- **Retry Timeout:** Enter the interval value between two detection packets (Ping or DNS detection).

- **Ping Detection-Ping using WAN Default Gateway:** If you choose this option, ping the IP address of the default WAN gateway. If the default WAN gateway can be detected, the network connection is active.

- **DNS Detection-DNS lookup using WAN DNS Servers:** If you choose this option, the security appliance sends the DNS query for www.cisco.com to the default WAN DNS server. If the DNS server can be detected, the network connection is active.

STEP 12 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 13 Use the Summary page to view information about the configuration.

STEP 14 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

Using the Remote Access VPN Wizard

Use the Remote Access VPN Wizard to configure the security appliance as an IPsec VPN server or as a SSL VPN gateway so that remote users can securely access the corporate network resources over the VPN tunnels. The Remote Access VPN Wizard supports the following VPN types:

- **IPsec Remote Access:** Enable the IPsec Remote Access feature and hence set the security appliance as an IPsec VPN server. If you choose this option, follow the on-screen prompts to configure an IPsec Remote Access group policy and specify the users and user groups for IPsec remote access. For complete details, see **Using the Remote Access VPN Wizard for IPsec Remote Access, page 54**.
- **SSL Remote Access:** Enable the SSL Remote Access feature and hence set the security appliance as a SSL VPN server. If you choose this option, follow the on-screen prompts to configure the SSL VPN group policies and specify the users and user groups for SSL remote access. For complete details, see **Using Remote Access VPN Wizard for SSL Remote Access, page 60**.

Using the Remote Access VPN Wizard for IPsec Remote Access

This section describes how to use the Remote Access VPN Wizard to configure an IPsec Remote Access group policy and specify the users and user groups for IPsec remote access. Refer to the following steps:

- **Starting the Remote Access VPN Wizard, page 55**
- **Configuring IPsec Remote Access Group Policy, page 55**

Starting the Remote Access VPN Wizard

STEP 1 Click **Configuration Wizards > Remote Access VPN Wizard**.

STEP 2 On the Getting Started page, choose **IPsec Remote Access** from the **VPN Tunnel Type** drop-down list.

STEP 3 Click **Next**.

Configuring IPsec Remote Access Group Policy

STEP 4 Use the IPsec Group Policy page to configure the following parameters of the IPsec Remote Access group policy:

- **Group Name:** Enter the name for the group policy.
- **IKE Authentication Method:** Specify the authentication method.
  - **Pre-shared Key:** Uses a simple, password-based key to authenticate. If you choose this option, enter the desired value that remote VPN clients must provide to establish the VPN connections. The pre-shared key must be entered exactly the same here and on remote VPN clients.
  - **Certificate:** Uses the digital certificate from a third party Certificate Authority (CA) to authenticate. If you choose this option, select a CA certificate as the local certificate from the **Local Certificate** drop-down list and select a CA certificate as the remote certificate from the **Peer Certificate** drop-down list for authentication. The selected remote certificate on the IPsec VPN server must be set as the local certificate on remote VPN clients.

NOTE: You must have valid CA certificates imported on your security appliance before you use the digital certificates to authenticate. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.

STEP 5 After you are finished, click **Next**.

Configuring WAN Settings

STEP 6 Use the WAN page to choose the WAN port that traffic passes through over the VPN tunnel. If you have two links, you can enable WAN Failover to redirect traffic to the secondary link when the primary link is down.

- **WAN Failover:** Click **On** to enable WAN Failover, or click **Off** to disable it.

  NOTE: To enable WAN Failover for IPsec Remote Access, make sure that the secondary WAN port was configured and the WAN redundancy was set as the Load Balancing or Failover mode. The security appliance will automatically update the local WAN gateway for the VPN tunnel based on the configurations of the backup WAN link. For this purpose, Dynamic DNS has to be configured because the IP address will change due to failover. In this case, remote VPN clients must use the domain name of the IPsec VPN server to establish the VPN connections.

- **WAN Interface:** Choose the WAN port that traffic passes through over the VPN tunnel.

STEP 7 After you are finished, click **Next**.

Configuring Operation Mode

STEP 8 Use the Network page to configure the mode of operation. The Cisco VPN hardware client supports Network Extension Mode (NEM) and Client Mode. The IPsec Remote Access group policy must be configured with the corresponding mode to allow only the Cisco VPN hardware clients in the same operation mode to be connected.

For example, if you choose the Client mode for the IPsec Remote Access group policy, only the Cisco VPN hardware clients in Client mode can be connected by using this group policy. For more information about the operation mode, see Modes of Operation, page 365.

- **Mode:** Choose one of the following modes:
  - **Client:** Choose this mode for the group policy that is used for both the PC running the Cisco VPN Client software and the Cisco device that supports the Cisco VPN hardware client in Client mode. In Client mode,

the IPsec VPN server can assign the IP addresses to the outside interfaces of remote VPN clients. To define the pool range for remote VPN clients, enter the starting and ending IP addresses in the **Start IP** and **End IP** fields.

- **NEM:** Choose this mode for the group policy that is only used for the Cisco device that supports the Cisco VPN hardware client in NEM mode.

- **Client Internet Access:** Check this box to automatically create advanced NAT rules to allow remote VPN clients to access the Internet over the VPN tunnels. If you uncheck this box, you can manually create advanced NAT rules. For complete details, see Allowing IPsec Remote VPN Clients to Access the Internet, page 360.

STEP 9 After you are finished, click **Next**.

Configuring Access Control Settings

STEP 10 Use the Access Control page to control access from the PC running the Cisco VPN Client software or the private network of the Cisco VPN hardware client to the zones over the VPN tunnel. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone access control settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 11 After you are finished, click **Next**.

Configuring DNS and WINS Settings

STEP 12 Optionally, use the DNS/WINS page to specify the DNS and domain settings.

- **Primary DNS Server:** Enter the IP address of the primary DNS server.
- **Secondary DNS Server:** Enter the IP address of the secondary DNS server.
- **Primary WINS Server:** Enter the IP address of the primary WINS server.
- **Secondary WINS Server:** Enter the IP address of the secondary WINS server.
- **Default Domain:** Enter the default domain name that should be pushed to remote VPN clients.

STEP 13 After you are finished, click **Next**.

Configuring Backup Servers

STEP 14 Use the Backup Server page to optionally specify up to three IPsec VPN servers as backup. When the connection to the primary server fails, remote VPN clients can attempt to connect to the backup servers.

Backup Server 1/2/3: Enter the IP address or domain name for the backup server. The backup server 1 has the highest priority and the backup server 3 has the lowest priority.

NOTE: The backup servers that you specified on the IPsec VPN server will be sent to remote VPN clients when initiating the VPN connections. The remote VPN clients will cache them.

STEP 15 After you are finished, click **Next**.

Configuring Split Tunneling

STEP 16 Use the Split Tunnel page to specify the split tunneling settings:

- **Split Tunnel:** Click **On** to enable the split tunneling feature, or click **Off** to disable it. Split tunneling allows only traffic that is specified by the VPN client routes to corporate resources through the VPN tunnel. If you enable the split tunneling feature, you need to define the split subnets. To add a subnet, enter the IP address and netmask in the **IP Address** and **Netmask** fields and click **Add**. To delete a subnet, select it from the list and click **Delete**.
- **Split DNS:** Split DNS directs DNS packets in clear text through the VPN tunnel for domains served by the corporate DNS. To add a domain, enter domain name that should be resolved by your network's DNS server in the **Domain Name** field and click **Add**. To delete a domain, select it from the list and click **Delete**.

  To use Split DNS, you must also enable the split tunneling feature and specify the domains. The Split DNS feature supports up to 10 domains.

STEP 17 After you are finished, click **Next**.

Viewing Group Policy Summary

STEP 18 Use the Group Policy Summary page to view information for the group policy settings.

STEP 19 Click **Next**.

Configuring IPsec Remote Access User Groups

STEP 20 Use the IPsec Remote Access - User Group page to configure the users and user groups for IPsec remote access. The IPsec Remote Access service must be enabled for each user group. All members of the user groups can use the specified group policy to establish the VPN connections.

STEP 21 Click **Add** to add a user group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 22 In the **Group Settings** tab, enter the following information:

- **Name:** Enter the name for the user group.
- **Services:** Specify the service policy for the user group. The **IPsec Remote Access** service must be enabled for this user group so that all members of the group can establish the VPN tunnel to securely access your network resources.

STEP 23 In the **Membership** tab, specify the members of the user group. You must add at least one user in the user group before proceeding.

- To add a member, select an existing user from the **User** list and click the right arrow. The members of the group appear in the **Membership** list.
- To delete a member from the group, select the member from the **Membership** list and then click the left arrow.
- To create a new user, enter the username in the **User Name** field and the password in the **Password** field, enter the same password in the **Password Confirm** field for confirmation, and then click **Create**.

STEP 24 Click **OK** to save your settings.

STEP 25 After you are finished, click **Next**.

Viewing IPsec Remote Access Summary

STEP 26 Use the IPsec Remote Access - Summary page to view information for the specified IPsec Remote Access group policy and user groups.

STEP 27 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

After the settings are saved, the security appliance is set as an IPsec VPN server. Remote users that belong to the specified user groups can use the specified group policy to establish the VPN connections. If you check **Client Internet Access**, the corresponding advanced NAT rules are automatically created to allow remote VPN clients to access the Internet over the VPN tunnels.

Using Remote Access VPN Wizard for SSL Remote Access

This section describes how to use the Remote Access VPN Wizard to configure the SSL VPN group policies and specify the users and user groups for SSL remote access. Refer to the following steps:

- **Starting the Remote Access VPN Wizard with SSL Remote Access, page 60**
- **Configuring SSL VPN Gateway, page 60**
- **Configuring SSL VPN Group Policy, page 62**
- **Configuring SSL VPN User Groups, page 65**
- **Viewing SSL VPN Summary, page 66**

Starting the Remote Access VPN Wizard with SSL Remote Access

STEP 1 Click **Configuration Wizards > Remote Access VPN Wizard**.

STEP 2 Choose **SSL Remote Access** from the **VPN Tunnel Type** drop-down list.

STEP 3 Click **Next**.

Configuring SSL VPN Gateway

STEP 4 Use the SSL VPN - Configuration page to configure the SSL VPN gateway settings.

STEP 5 In the **Gateway (Basic)** area, enter the following information:

- **Gateway Interface:** Choose the WAN port that traffic passes through the SSL VPN tunnel.
- **Gateway Port:** Enter the port number used for the SSL VPN gateway. By default, SSL operates on port 443. However, the SSL VPN gateway should be flexible enough to operate on a user defined port. The firewall should

permit the port to ensure delivery of packets destined for the SSL VPN gateway. The SSL VPN clients need to enter the entire address pair “Gateway IP address: Gateway port number” for connecting purposes.

- **Certificate File:** Choose the default certificate or an imported certificate to authenticate users who try to access your network resource through the SSL VPN tunnels. For information on importing the certificates, see **Managing Certificates for Authentication, page 418**.
- **Client Address Pool:** The SSL VPN gateway has a configurable address pool with maximum size of 255 which is used to allocate IP addresses to the remote clients. Enter the IP address pool for all remote clients. The client is assigned an IP address by the SSL VPN gateway.

  NOTE: Configure an IP address range that does not directly overlap with any other addresses on your local network.
- **Client Netmask:** Enter the IP address of the netmask used for SSL VPN clients. The client netmask can only be one of 255.255.255.0, 255.255.255.128, and 255.255.255.192.

  The Client Address Pool is used with the Client Netmask. The following table displays the valid settings for entering the client address pool and the client netmask.

Client Netmask	Client Address Pool
255.255.255.0	x.x.x.0
255.255.255.128	x.x.x.0, or x.x.x.128
255.255.255.192	x.x.x.0, x.x.x.64, x.x.x.128, or x.x.x.192

For example, if they are set as follows, then the SSL VPN client will get a VPN address whose range is from 10.10.10.1 to 10.10.10.254.

- Client Address Pool = 10.10.10.0
- Client Netmask = 255.255.255.0

- **Client Internet Access:** Check this box to automatically create advanced NAT rules to allow SSL VPN clients to access the Internet over SSL VPN tunnels. If you uncheck this box, you can manually create advanced NAT rules. For complete details, see Allowing SSL VPN Clients to Access the Internet, page 382.

- **Client Domain:** Enter the domain name that should be pushed to the SSL VPN clients.
- **Login Banner:** After the SSL VPN user logged in, a configurable login banner is displayed. Enter the message text to display along with the banner.

STEP 6 In the **Gateway (Advanced)** area, enter the following information:

- **Idle Timeout:** Enter the timeout value in seconds that the SSL VPN session can remain idle. The default value is 2100 seconds.
- **Session Timeout:** Enter the timeout value in seconds that a SSL VPN session can remain active. The default value is 0 seconds, which indicates that the SSL VPN session can always be active.
- **Client DPD Timeout:** Dead Peer Detection (DPD) allows detection of dead peers. Enter the DPD timeout that a session will be maintained with a nonresponsive remote client. The default value is 300 seconds.
- **Gateway DPD Timeout:** Enter the DPD timeout that a session will be maintained with a nonresponsive SSL VPN gateway. The default value is 300 seconds.

  NOTE: If the SSL VPN gateway has no response over two or three times of the DPD timeout, the SSL VPN session will be terminated.
- **Keep Alive:** Enter the interval, in seconds, at which the SSL VPN client will send keepalive messages. These messages ensure that the SSL VPN connection remains open, even if the client's maximum idle time is limited by an intermediate device, such as a proxy, firewall or NAT device.
- **Lease Duration:** Enter the amount of time after which the SSL VPN client must send an IP address lease renewal request to the server. The default value is 43200 seconds.
- **Max MTU:** Enter the maximum transmission unit for the session. The default value is 1406 bytes.
- **Rekey Interval:** Enter the frequency of the rekey in this field. The default value is 3600 seconds.

STEP 7 After you are finished, click **Next**.

Configuring SSL VPN Group Policy

STEP 8 Use the Group Policy page to configure the SSL VPN group policies.

NOTE: Up to 32 SSL VPN group policies can be configured on the security appliance.

STEP 9 Click **Add** to add a new SSL VPN group policy.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 10 In the **Basic Settings** tab, enter the following information:

- **Policy Name:** Enter the name for the SSL VPN group policy.
- **Primary DNS:** Optionally, enter the IP address of the primary DNS server.
- **Secondary DNS:** Optionally, enter the IP address of the secondary DNS server.
- **Primary WINS:** Optionally, enter the IP address of the primary WINS server.
- **Secondary WINS:** Optionally, enter the IP address of the secondary WINS server.

STEP 11 In the **IE Proxy Settings** tab, enter the following information:

The SSL VPN gateway can specify several Microsoft Internet Explorer (MSIE) proxies for client PCs. If these settings are enabled, IE on the client PC is automatically configured with these settings.

- **IE Proxy Policy:** Choose one of the following options:
  - **None:** Allows the browser to use no proxy settings.
  - **Auto:** Allows the browser to automatically detect the proxy settings.
  - **Bypass-Local:** Allows the browser to bypass the proxy settings that are configured on the remote user.
  - **Disable:** Disables the MSIE proxy settings.
- **Address:** If you choose Bypass-Local or Auto, enter the IP address or domain name of the MSIE proxy server.
- **Port:** Enter the port number of the MSIE proxy server.
- **IE Proxy Exception:** You can specify the exception hosts for IE proxy settings. This option allows the browser to not send traffic for the given hostname or IP address through the proxy. To add an entry, enter the IP address or domain name of an exception host and click **Add**.

STEP 12 In the **Split Tunneling Settings** area, enter the following information:

Split tunneling permits specific traffic to be carried outside of the SSL VPN tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the ISP or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time.

- **Enable Split Tunneling:** By default, all of traffic from the host is directed through the tunnel. Check this box to enable the split tunneling feature so that the tunnel is used only for traffic that is specified by the client routes.
- **Split Selection:** If you enable split tunneling, choose one of the following options:
  - **Include Traffic:** Allows you to add the client routes on the SSL VPN client so that only traffic to the destination networks can be redirected through the SSL VPN tunnels. To add a client route, enter the destination subnet to which a route is added on the SSL VPN client in the **Address** field and the subnet mask for the destination network in the **Netmask** field, and then click **Add**.
  - **Exclude Traffic:** Allows you to exclude the destination networks on the SSL VPN client. Traffic to the destination networks is redirected using the SSL VPN client's native network interface (resolved through the ISP or WAN connection). To add a destination subnet, enter the destination subnet to which a route is excluded on the SSL VPN client in the **Address** field and the subnet mask for the excluded destination in the **Netmask** field, and then click **Add**.

    NOTE: To exclude the destination networks, make sure that the Exclude Local LANs feature is enabled on the Cisco AnyConnect Secure Mobility clients.
  - **Exclude Local LANs:** If you choose Exclude Traffic, check the box to permit remote users to access their local LANs without passing through VPN tunnel, or uncheck the box to deny remote users to access their local LANs without passing through VPN tunnel.

    NOTE: To exclude local LANs, make sure that the Exclude Local LANs feature is enabled on both the SSL VPN server and the Cisco AnyConnect Secure Mobility clients.
- **Split DNS:** Split DNS can direct DNS packets in clear text over the Internet for domains served through an external DNS (serving your ISP) or through a SSL VPN tunnel to domains served by the corporate DNS. To add a domain

for tunneling DNS requests to destinations in the private network, enter the IP address or domain name in the field and click **Add**. To delete a domain, select it from the list and click **Delete**.

STEP 13 In the **Zone-based Firewall Settings** area, you can control access from the SSL VPN clients to the zones over the SSL VPN tunnels. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone-based firewall settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 14 Click **OK** to save your settings.

STEP 15 After you are finished, click **Next**.

Configuring SSL VPN User Groups

STEP 16 Use the User Group page to configure the users and user groups for SSL remote access. The SSL VPN service must be enabled for the user groups. All members of a user group can use the selected SSL VPN group policy to establish the SSL VPN connections.

STEP 17 Click **Add** to add a user group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 18 In the **Group Settings** tab, enter the following information:

- **Name:** Enter the name for the user group.
- **Services:** Specify the service policy for the user group. The **SSL VPN** service must be enabled for this user group so that all members of the user group can establish the SSL VPN tunnels based on the selected SSL VPN group policy to access your network resources.

STEP 19 In the **Membership** tab, specify the members of the user group. You must add at least one user in the user group before proceeding.

- To add a member, select an existing user from the **User** list and then click the right arrow. The members of the group appear in the **Membership** list.
- To delete a member from the group, select the member from the **Membership** list and then click the left arrow.

- To create a new member, enter the username in the **User Name** field and the password in the **Password** field, enter the same password in the **Password Confirm** field for confirmation, and then click **Create**.

STEP 20 Click **OK** to save your settings.

STEP 21 After you are finished, click **Next**.

Viewing SSL VPN Summary

STEP 22 Use the SSL VPN Summary page to view information for all configured SSL VPN group policies and user groups.

STEP 23 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

After the settings are saved, the security appliance is set as a SSL VPN server. The SSL VPN users that belong to the specified user groups can use the selected group policies to establish the SSL VPN connections. If you check **Client Internet Access**, the advanced NAT rules will be automatically created to allow SSL VPN clients to access the Internet over SSL VPN tunnels.

Using the Site-to-Site VPN Wizard to Configure Site-to-Site VPN

Use the Site-to-Site VPN Wizard to configure a site-to-site VPN policy to provide a secure connection between two routers that are physically separated. Refer to the following steps:

- **Starting the Site-to-Site VPN Wizard, page 67**
- **Configuring VPN Peer Settings, page 67**
- **Configuring IKE Policies, page 68**
- **Configuring Transform Policies, page 69**
- **Configuring Local and Remote Networks, page 70**
- **Viewing Configuration Summary, page 70**

Starting the Site-to-Site VPN Wizard

STEP 1 Click **Configuration Wizards > Site-to-Site VPN Wizard**.

STEP 2 Click **Next**.

Configuring VPN Peer Settings

STEP 3 Use the VPN Peer Settings page to configure an IPsec VPN policy for establishing the VPN connection with a remote router.

- **Profile Name:** Enter the name for the IPsec VPN policy.
- **WAN Interface:** Choose the WAN port that traffic passes through over the VPN tunnel.
- **Remote Type:** Specify the type of the remote peer:
  - **Static IP:** Choose this option if the remote peer uses a static IP address. Enter the IP address of the remote device in the **Remote Address** field.
  - **Dynamic IP:** Choose this option if the remote peer uses a dynamic IP address.
  - **FQDN (Fully Qualified Domain Name):** Choose this option if you want to use the domain name of the remote network such as vpn.company.com. Enter the domain name of the remote device in the **Remote Address** field.
- **Authentication Method:** Specify the authentication method.
  - **Pre-Shared Key:** Uses a simple, password-based key to authenticate. If you choose this option, enter the desired value that the peer device must provide to establish a connection in the **Key** field. The pre-shared key must be entered exactly the same here and on the remote peer.
  - **Certificate:** Uses the digital certificate from a third party Certificate Authority (CA) to authenticate. If you choose this option, select a CA certificate as the local certificate from the **Local Certificate** drop-down list and select a CA certificate as the remote certificate from the **Remote Certificate** drop-down list. The selected remote certificate on the local gateway must be set as the local certificate on the remote peer.

    NOTE: You must have valid CA certificates imported on your security appliance before you use the digital certificates to authenticate. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.

STEP 4 After you are finished, click **Next**.

Configuring IKE Policies

STEP 5 Use the IKE Policies page to configure the IKE policies and to specify an IKE policy for the IPsec VPN policy. You can choose the default or a custom IKE policy.

STEP 6 Click **Add** to add an IKE policy.

Other options: To edit an entry, click **Edit**. To delete an entry, select it and click **Delete**. The default IKE policy (**DefaultIke**) cannot be edited or deleted.

STEP 7 Enter the following information:

- **Name:** Enter the name for the IKE policy.
- **Encryption:** Choose the algorithm used to negotiate the security association. There are four algorithms supported by the security appliance: ESP_3DES, ESP_AES_128, ESP_AES_192, and ESP_AES_256.
- **HASH:** Specify the authentication algorithm for the VPN header. There are two HASH algorithms supported by the security appliance: SHA1 and MD5. Ensure that the authentication algorithm is configured identically on both sides.
- **Authentication:** Specify the authentication method that the security appliance uses to establish the identity of each IPsec peer.
  - **PRE_SHARE:** Use a simple, password-based key to authenticate. The alpha-numeric key is shared with IKE peer. Pre-shared keys do not scale well with a growing network but are easier to set up in a small network.
  - **RSA_SIG:** Use a digital certificate to authenticate. RSA_SIG is a digital certificate with keys generated by the RSA signatures algorithm. In this case, a certificate must be configured in order for the RSA-Signature to work.
- **D-H Group:** Choose the Diffie-Hellman group identifier. The identifier is used by two IPsec peers to derive a shared secret without transmitting it to each other. The D-H Group sets the strength of the algorithm in bits. The default is Group 5. The lower the Diffie-Hellman group number, the less CPU time it requires to be executed. The higher the D-H group number, the greater the security level.
  - Group 2 (1024-bit)
  - Group 5 (1536-bit)

- Group 14 (2048-bit)

- **Lifetime:** Enter the number of seconds for the IKE Security Association (SA) to remain valid. As a general rule, a shorter lifetime provides more secure ISAKMP negotiations. However, with shorter lifetimes, the security appliance sets up future IKE SAs more quickly.

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

STEP 9 After you are finished, click **Next**.

Configuring Transform Policies

STEP 10 Use the Transform Policies page to configure the transform policies and to specify a transform set for the IPsec VPN policy. You can choose the default or a custom transform set.

STEP 11 Click **Add** to add a transform set.

Other options: To edit an entry, click **Edit**. To delete an entry, select it and click **Delete**. The default transform set (**DefaultTrans**) cannot be edited or deleted.

STEP 12 Enter the following information:

- **Name:** Enter the name for the transform set.
- **Integrity:** Choose the hash algorithm used to ensure data integrity. The hash algorithm ensures that a packet comes from where it says it comes from, and that it has not been modified in transit.
  - **ESP_SHA1_HMAC:** Authentication with SHA1 (160-bit).
  - **ESP_MD5_HMAC:** Authentication with MD5 (128-bit). MD5 has a smaller digest and is considered to be slightly faster than SHA1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant that IKE uses prevents this attack.
- **Encryption:** Choose the symmetric encryption algorithm that protects data transmission between two IPsec peers. The default is ESP_3DES. The Advanced Encryption Standard supports key lengths of 128, 192, 256 bits.
  - **ESP_3DES:** Encryption with 3DES (168-bit).
  - **ESP_AES_128:** Encryption with AES (128-bit).
  - **ESP_AES_192:** Encryption with AES (192-bit).
  - **ESP_AES_256:** Encryption with AES (256-bit).

STEP 13 Click **OK** to save your settings.

STEP 14 After you are finished, click **Next**.

Configuring Local and Remote Networks

STEP 15 Use the Local and Remote VPN Networks page to configure the local and remote networks.

- **Local Subnet:** Choose the IP address for your local network. Choose **Any** if you want to enable the zone access control settings so that you can control incoming traffic from remote VPN network to the zones over the VPN tunnels.
- **Remote Subnet:** Choose the IP address for the remote network. You must know the IP address of the remote network before connecting the VPN tunnel.

  If the IP address object that you want is not in the list, choose **Create a new address** to add a new address object or choose **Create a new address group** to add a new address group object. To maintain the address and address group objects, go to the Networking > Address Management page. See Address Management, page 175.

  NOTE: The security appliance can support multiple subnets for establishing the VPN tunnels. You should select an address group object including multiple subnets for local and remote networks.

STEP 16 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 17 Use the Summary page to view information for the IPsec VPN policy.

STEP 18 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

STEP 19 After you click Finish, a warning message appears saying “Do you want to make this connection active when the settings are saved? (Only one connection can be active at a time.)”

- If you want to immediately activate the connection after the settings are saved, click **Activate Connection**. After you save your settings, the security appliance will immediately try to initiate the VPN connection.

- If you only want to create the IPsec VPN policy and do not want to immediately activate the connection after the settings are saved, click **Do Not Activate**. The connection will be triggered by any traffic that matches this IPsec VPN policy and the VPN tunnel will be set up automatically. You can also go to the VPN > Site-to-Site > IPsec Policies page to manually establish the VPN connection by clicking the **Connect** icon.

Using the DMZ Wizard to Configure DMZ Settings

Use the DMZ Wizard to configure DMZ and DMZ services if you need to host public services. Refer to the following steps:

- **Starting the DMZ Wizard, page 71**
- **Configuring DDNS Profiles, page 71**
- **Configuring DMZ Network, page 72**
- **Configuring DMZ Services, page 74**
- **Viewing Configuration Summary, page 76**

Starting the DMZ Wizard

STEP 1 Click **Configuration Wizards > DMZ Wizard**.

STEP 2 Click **Next**.

Configuring DDNS Profiles

STEP 3 Optionally, use the DDNS Setup page to configure the DDNS profiles for remote management of the DMZ network.

NOTE: Up to 16 DDNS profiles can be configured on the security appliance.

STEP 4 Click **Add** to create a DDNS profile.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 5 Enter the following information:

- **Service:** Choose either DynDNS or No-IP service.

  NOTE: You must sign up for an account with either one of these providers before you can use this service.

- **Active On Startup:** Click **On** to activate the DDNS setting when the security appliance starts up.

- **WAN Interface:** Choose the WAN port for the DDNS service. Traffic for DDNS services will pass through the specified WAN port.

  NOTE: If the WAN redundancy is set as the Failover mode, this option is grayed out. When WAN failover occurs, DDNS will switch traffic to the active WAN port.

- **User Name:** Enter the username of the account that you registered in the DDNS provider.

- **Password:** Enter the password of the account that you registered in the DDNS provider.

- **Host and Domain Name:** Specify the complete host name and domain name for the DDNS service.

- **Use wildcards:** Check this box to allow all sub-domains of your DDNS host name to share the same public IP address as the host name.

- **Update every week:** Check this box to update the host information every week.

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

STEP 7 After you are finished, click **Next**.

Configuring DMZ Network

STEP 8 Use the DMZ Configuration page to configure the DMZ networks.

NOTE: Up to 4 DMZ networks can be configured on the security appliance. You must configure at least one DMZ network to finish the DMZ wizard.

STEP 9 Click **Add** to create a DMZ network.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 10 In the **Basic Setting** tab, enter the following information:

- **Name:** Enter the name for the DMZ.
- **IP:** Enter the subnet IP address for the DMZ.
- **Netmask:** Enter the subnet mask for the DMZ.
- **Spanning Tree:** Check this box to enable the Spanning Tree feature to determine if there are loops in the network topology.
- **Port:** Choose a configurable port from the **Port** list and add it to the **Member** list. The selected configurable port is set as a DMZ port in the Access mode.
- **Zone:** Choose the default DMZ zone or a custom DMZ zone to which the DMZ is mapped.

STEP 11 In the **DHCP Pool Settings** tab, choose the DHCP mode from the **DHCP Mode** drop-down list.

- **Disable:** Choose this option if the computers on the DMZ are configured with static IP addresses or are configured to use another DHCP server.
- **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the DMZ. Any new DHCP client joining the DMZ is assigned an IP address of the DHCP pool.
- **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 12 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet with the DMZ IP address.
- **Lease Time:** Enter the maximum connection time 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.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of a secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.

- **WINS2:** Optionally, enter the IP address of a secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the DMZ.
- **Default Gateway:** Enter the IP address of default gateway.

STEP 13 Click **OK** to save your settings.

STEP 14 After you are finished, click **Next**.

Configuring DMZ Services

STEP 15 Use the DMZ Service page to configure the DMZ services.

STEP 16 Click **Add** to create a DMZ service.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 17 Enter the following information:

- **Original Service:** Choose a service as the incoming service.
- **Translated Service:** Choose a service as the translated service or choose **Original** if the translated service is same as the incoming service. If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the Networking > Service Management page. See Service Management, page 177.

  NOTE: One-to-one translation will be performed for port range forwarding. For example, if you want to translate an original TCP service with the port range of 50000 to 50002 to a TCP service with the port range of 60000 to 60002, then the port 50000 will be translated to the port 60000, the port 50001 will be translated to the port 60001, and the port 50002 will be translated to the port 60002.
- **Translated IP:** Choose the IP address of your local server that needs to be translated. If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **WAN:** Choose either WAN1 or WAN2, or both as the incoming WAN port.

- **WAN IP:** Specify the public IP address for the server. You can use the IP address of the selected WAN port or a public IP address that is provided by your ISP. When you choose **Both** as the incoming WAN port, this option is grayed out.
- **Enable DMZ Service:** Click **On** to enable the DMZ service, or click **Off** to create only the DMZ service.
- **Create Firewall Rule:** Check this box to automatically create a firewall rule to allow access for this DMZ service. You must manually create a firewall rule if you uncheck this box.

  NOTE: If you choose Both as the incoming WAN port, a firewall rule from Any zone to Any zone will be created accordingly.
- **Description:** Enter the name for the DMZ service.

  For example, you host an RDP server (192.168.12.101) on the DMZ. Your ISP has provided a static IP address (172.39.202.102) that you want to expose to the public as your RDP server address. You can create a DMZ service as follows to allow Internet user to access the RDP server by using the specified public IP address.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

NOTE: In the above example, you must manually create two address objects (RDPServer and PublicIP) and a TCP service object with the port 3389 called “RDP.”

STEP 18 Click **OK** to save your settings.

STEP 19 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 20 Use the Summary page to view information for the configuration.

STEP 21 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

Using the Wireless Wizard (for ISA550W and ISA570W only)

If you are using the ISA550W or ISA570W, you can use the Wireless Wizard to configure your wireless network. Refer to the following steps:

- **Starting the Wireless Wizard, page 76**
- **Configuring Wireless Radio Settings, page 76**
- **Configuring Wireless Connectivity Types, page 77**
- **Specify Wireless Connectivity Settings for All Enabled SSIDs, page 78**
- **Viewing Configuration Summary, page 78**

Starting the Wireless Wizard

STEP 1 Click **Configuration Wizards > Wireless Wizard**.

STEP 2 Click **Next**.

Configuring Wireless Radio Settings

STEP 3 Use the Wireless Radio page to configure the wireless radio settings.

- **Wireless Mode:** Choose the 802.11 modulation technique.
  - **802.11b/g mixed:** Choose this mode if some devices in the wireless network use 802.11b and others use 802.11g. Both 802.11b and 802.11g clients can connect to the access point.
  - **802.11g/n mixed:** Choose this mode if some devices in the wireless network use 802.11g and others use 802.11n Both 802.11g and 802.11n clients can connect to the access point.

  - **802.11b/g/n mixed:** Choose this mode to allow 802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency to connect to the access point.
  - **802.11n only:** Choose this mode if all devices in the wireless network can support 802.11n. Only 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.
- **Wireless Channel:** Choose a channel from a list of channels or choose **Auto** to let the system determine the optimal channel to use based on the environmental noise levels for the available channels.

STEP 4 After you are finished, click **Next**.

Configuring Wireless Connectivity Types

STEP 5 Use the Choose SSIDs page to enable and configure the SSIDs that you want to use.

- **Enable:** Check this box to enable the SSID.
- **Mode:** Choose the wireless connectivity type for each enabled SSID.
  - **Intranet WLAN Access:** Allows the wireless users to access the corporate network via the wireless network. By default, the WLAN is mapped to the DEFAULT VLAN.
  - **Guest WLAN Access:** Only allows the wireless users who connect to the guest SSID to access the corporate network via the wireless network. By default, the WLAN is mapped to the GUEST VLAN.
  - **Captive Portal Access:** Only allows the users who have authenticated successfully to access the corporate network via the wireless network. The wireless users will be directed to a specific HotSpot Login page to authenticate, and then will be directed to a specified web portal after login before they can access the Internet.

NOTE: Only one SSID can be set for Captive Portal access at a time.

STEP 6 After you are finished, click **Next**.

Specify Wireless Connectivity Settings for All Enabled SSIDs

STEP 7 Specify the wireless connectivity settings for all enabled SSIDs.

- For complete details to configure the connectivity settings for Intranet WLAN access, see **Configuring the SSID for Intranet WLAN Access, page 78**.
- For complete details to configure the connectivity settings for Guest WLAN access, see **Configuring the SSID for Guest WLAN Access, page 80**.

STEP 8 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 9 Use the Summary page to view information for the configuration.

STEP 10 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to save your settings.

Configuring the SSID for Intranet WLAN Access

Follow these steps to configure the connectivity settings for Intranet WLAN access.

STEP 1 Enter the following information:

- **SSID:** Enter the name of the SSID.
- **Broadcast SSID:** Check this box to broadcast the SSID in its beacon frames. 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 SSID.
- **Station Isolation:** Check so that the wireless clients on the same SSID will be unable to see each other.

STEP 2 In the **Security Settings** area, specify the wireless security settings.

- **Security Mode:** Choose the security mode and configure the corresponding security settings. For security purposes, we strongly recommend that you use WPA2 for wireless security. For example, if you choose WPA2-Personal, enter the following information:
  - **Encryption:** WPA2-Personal always uses AES for data encryption.
  - **Shared Secret:** The Pre-shared Key (PSK) is the shared secret key for WPA. Enter a string of at least 8 characters to a maximum of 63 characters.
  - **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. A value of zero (0) indicates that the key is not refreshed. The default is 3600 seconds.

  NOTE: For information on configuring other security modes, see **Configuring Wireless Security, page 211**.

STEP 3 In the **Advanced Settings** area, enter the following information:

- **VLAN Mapping:** Choose the VLAN to which the SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. For Intranet VLAN access, you must choose a VLAN that is mapped to a trusted zone.
- **User Limit:** Specify the maximum number of users that can simultaneously connect to this SSID. Enter a value in the range of 0 to 200. The default value is zero (0), which indicates that there is no limit for this SSID.

  NOTE: The maximum number of users that can simultaneously connect to all enabled SSIDs is 200.

Configuring the SSID for Guest WLAN Access

Follow these steps to configure the connectivity settings for Guest WLAN access.

STEP 1 Enter the following information:

- **SSID:** Enter the name of the SSID.
- **Broadcast SSID:** Check this box to broadcast the SSID in its beacon frames. 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 SSID.
- **Station Isolation:** Check so that the wireless clients on the same SSID will be unable to see each other.

STEP 2 In the **Security Settings** area, specify the wireless security settings.

- **Security Mode:** Choose the security mode and configure the corresponding security settings. For complete details on configuring the security mode, see Configuring Wireless Security, page 211.

STEP 3 In the **Advanced Settings** area, enter the following information:

- **VLAN Mapping:** Choose the VLAN to which the SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. For Guest VLAN access, you must choose a VLAN that is mapped to a guest zone.
- **User Limit:** Specify the maximum number of users that can simultaneously connect to this SSID. Enter a value in the range of 0 to 200. The default value is zero (0), which indicates that there is no limit for this SSID.

  NOTE: The maximum number of users that can simultaneously connect to all enabled SSIDs is 200.