4

Networking

Using the Networking module to configure your Internet connection, VLAN, DMZ, zones, routing, Quality of Service (QoS), and related features. It includes the following sections:

- **Viewing Network Status, page 116**
- **Configuring IPv4 or IPv6 Routing, page 116**
- **Managing Ports, page 116**
- **Configuring the WAN, page 122**
- **Configuring a VLAN, page 137**
- **Configuring DMZ, page 141**
- **Configuring Zones, page 146**
- **Configuring DHCP Reserved IPs, page 149**
- **Configuring Routing, page 149**
- **Configuring Quality of Service, page 155**
- **Configuring IGMP, page 172**
- **Configuring VRRP, page 173**
- **Address Management, page 175**
- **Service Management, page 177**

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

Viewing Network Status

Use the Networking > Network Status pages to view the traffic statistics, the usage reports, the WAN bandwidth reports, all ARP (Address Resolution Protocol) entries, and DHCP address assignment. For descriptions of these status reports, see Network Status, page 88.

Configuring IPv4 or IPv6 Routing

Use the Networking > IPv4 or IPv6 Routing page to choose the IP routing mode for your network. 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 WAN, LAN, and DMZ.

⚠ **CAUTION** In the current firmware, IPv6 functionalities are limited. ISA500 does not support firewall, VPN, and other security services for IPv6 in this firmware. We recommend enabling IPv6 for lab testing only with this firmware. Please check future firmware and release notes for information about any IPv6 updates.

STEP 1 Click **IPv4 or IPv6** to enable both IPv4 and IPv6 addressing, or click **IPv4 only** to enable only IPv4 addressing. By default, only IPv4 addressing is supported.

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

Managing Ports

Use the Networking > Ports pages to configure the physical ports, port mirroring, and port-based access control settings. Refer to the following topics:

- **Viewing Status of Physical Interfaces, page 117**
- **Configuring Physical Ports, page 118**

- Configuring Port Mirroring, page 119
- Configuring Port-Based (802.1x) Access Control, page 120

Viewing Status of Physical Interfaces

Use the Networking > Ports > Physical Interface page to view information about all physical ports on the security appliance.

For all models, the following information appears:

- **Name:** The name of the physical port.
- **Enable:** Shows if the physical port is enabled or disabled.
- **Port Type:** The type of the physical port, such as WAN, LAN, or DMZ.
- **Mode:** The access mode of the physical port. A WAN or DMZ port is always set to the Access mode. A LAN port can be set to the Access or Trunk mode.
- **VLAN:** The VLANs to which the physical port is mapped.
- **PVID:** The Port VLAN ID (PVID) is used to forward or filter the untagged packets coming into port. The PVID of a trunk port is fixed to the DEFAULT VLAN (1).
- **Speed/Duplex:** The duplex mode (speed and duplex setting) of the physical port.
- **Link Status:** Shows if the physical port is connected or disconnected.

For the ISA550W and the ISA570W, the Wireless Interfaces area displays the following information for all SSIDs:

- **SSID Name:** The name of the SSID.
- **VLAN:** The VLAN to which the SSID is mapped.
- **Client Associated:** The number of client stations that are connected to the SSID.

  NOTE: To configure your wireless network, go to the Wireless pages. See Wireless (for ISA550W and ISA570W only), page 206.

STEP 1 Proceed as needed:

- Check the box in the **Enable** column to enable a physical port, or uncheck this box to disable the physical port.
- To edit the settings of a physical port, click the **Edit** (pencil) icon. See **Configuring Physical Ports, page 118**.

STEP 2 Click **Save** to apply your settings.

Configuring Physical Ports

After you click the Edit (pencil) icon on the Networking > Ports > Physical Interface page, use the Ethernet Configuration - Add/Edit page to enable or disable the selected physical port, assign it to one or more VLANs, and configure the duplex mode.

STEP 1 Enter the following information:

- **Name:** The name of the physical port.
- **Port Type:** The type of the physical port, such as WAN, LAN, or DMZ.
- **Mode:** Choose either **Access** or **Trunk** mode for a LAN port, or choose **Access** for a WAN or DMZ port. By default, all ports are set to the Access mode.
  - **Access:** All data going into and out of the Access port is untagged. Access mode is recommended if the port is connected to a single end-user device which is VLAN unaware.
  - **Trunk:** All data going into and out of the Trunk port is tagged. Untagged data coming into the port is not forwarded, except for the DEFAULT VLAN, which is untagged. Trunk mode is recommended if the port is connected to a VLAN-aware switch or router.
- **Port:** Click **On** to enable the port, or click **Off** to disable it. By default, all ports are enabled.
- **VLAN:** You can assign the physical port to VLANs.
  - To assign the port to a VLAN, choose an existing VLAN from the Available VLAN list and click the right arrows. The associated VLANs appear in the list of VLAN.

- To release the port from a VLAN, choose a VLAN from the VLAN list and click the left arrows.

NOTE: A LAN port can be assigned to multiple VLANs, but an Access LAN port can only be assigned to one VLAN. A DMZ port must be assigned to a DMZ network.

NOTE: You can click the **Create VLAN** link to create new VLANs. For information on configuring VLAN, see **Configuring a VLAN, page 137**.

- **Flow Control:** Click **On** to control the flow on the port, or click **Off** to disable it.

  NOTE: Gigabit Ethernet flow control is provided by a PAUSE frame mechanism. A congested port sends an XON PAUSE frame, which causes the source port to stop sending data until an XOFF PAUSE frame is received. For this mechanism to work, flow control must be enabled on the source port and the destination port. Even with flow control enabled, the packet drops may occur if the receiving port runs out of buffers.

- **Speed:** Choose one of these options: AUTO, 10M, 100M, and 1000M. The default is AUTO for all ports. The AUTO option lets the system and network determine the optimal port speed.

- **Duplex:** Choose either Half or Full based on the port speed setting. The default is Full Duplex for all ports.

  - **Full:** The port supports transmissions between the device and the client in both directions simultaneously.

  - **Half:** The port supports transmissions between the device and the client in only one direction at a time.

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

STEP 3 On the Networking > Ports > Physical Interface page, click **Save** to apply your settings.

Configuring Port Mirroring

Use the Networking > Ports > Port Mirroring page to allow traffic on one port to be visible on other ports. This feature is useful for debugging or traffic monitoring.

NOTE The dedicated WAN port (GE1) cannot be set as a destination or monitored port.

STEP 1 Click **On** to enable port mirroring, or click **Off** to disable this feature.

STEP 2 If you enable port mirroring, enter the following information:

- **TX Destination:** Choose the port that monitors the transmitted traffic for other ports.
- **TX Monitored Ports:** Check the ports that are monitored. The port that you set as a TX Destination port cannot be selected as a monitored port.
- **RX Destination:** Choose the port that monitors the received traffic for other ports.
- **RX Monitored Ports:** Check the ports that are monitored. The port that you set as a RX Destination port cannot be selected as a monitored port.

STEP 3 Click **Save** to apply your settings.

Configuring Port-Based (802.1x) Access Control

Use the Networking > Ports > Port-Based Access Control page to configure IEEE 802.1x port-based authentication, which prevents unauthorized devices (802.1x-capable clients) from gaining access to the network.

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a VLAN through publicly accessible ports. The authentication server authenticates each client (supplicant in Windows 2000, XP, Vista, Windows 7, and Mac OS) connected to a port before making available any service offered by the security appliance or the VLAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This feature simplifies the security management by allowing you to control access from a master database in a single server (although you can use up to three RADIUS servers to provide backups in case access to the primary server fails). It also means that user can enter the same authorized RADIUS username and password pair for authentication, regardless of which switch is the access point into the VLAN.

STEP 1 In the **RADIUS Settings** area, specify the RADIUS servers for authentication.

The security appliance predefines three RADIUS groups. Choose a predefined RADIUS group from the **RADIUS Index** drop-down list to authenticate users on 802.1x-capable clients. The RADIUS server settings of the selected group are displayed. You can edit the RADIUS server settings here but the settings that you specify will replace the default settings of the selected group. For information on configuring RADIUS servers, see Configuring RADIUS Servers, page 401.

STEP 2 In the **Port-Based Access Control Settings** area, perform the following actions:

- **Access Control:** Check this box to enable the 802.1x access control feature, or uncheck this box to disable it. This feature is not available for trunk ports.
- **Guest Authentication:** After you enable the 802.1x access control feature, check this box to enable the Guest Authentication feature, or uncheck this box to disable it.
- **Authorization Mode:** Specify the authorization mode for each physical port by clicking one of the following icons:
  - **Forced Authorized:** Disable the 802.1x access control feature and cause the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client.
  - **Forced Unauthorized:** Cause the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The security appliance cannot provide authentication services to the client through the port.
  - **Auto:** Enable the 802.1x access control feature and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The security appliance requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the security appliance by using the client's MAC address.

STEP 3 To specify the authenticated VLANs on a physical port, click the **Edit** (pencil) icon.

STEP 4 Enter the following information in the Port-Base Access Control - Edit page:

- **Access Control:** Check this box to enable the 802.1x access control feature.

- **Authenticated VLAN:** If you enable the 802.1x access control feature, choose the authenticated VLAN to which this port is assigned. The users who authenticated successfully can access the authenticated VLAN through the port. If the authentication fails, block access through the port.
- **Guest Authenticated:** If you enable the 802.1x access control feature, check this box to enable the Guest Authentication feature.
- **Authenticated VLAN:** If you enable the Guest Authentication feature, choose the guest VLAN to be associated with the port. If the authentication fails, the port is assigned to the selected guest VLAN instead of shutting down. For 802.1x-incapable clients, the port is also assigned to the selected guest VLAN when Guest Authentication is enabled.

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

STEP 6 Click **Save** to apply your settings.

Configuring the WAN

By default, the 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 use the Networking > WAN pages modify the WAN settings to ensure Internet connectivity. Refer to the following topics:

- **Configuring WAN Settings for Your Internet Connection, page 122**
- **Configuring WAN Redundancy, page 130**
- **Configuring Link Failover Detection, page 132**
- **Configuring Dynamic DNS, page 134**

Configuring WAN Settings for Your Internet Connection

Use the Networking > WAN > WAN Settings to configure WAN settings by using the account information provided by your ISP. If you have two ISP links, you can configure one for WAN1 and another for WAN2.

Proceed as needed:

- **Release or renew a DHCP WAN connection, page 123**

- Configure the primary WAN, page 123
- Configure a secondary WAN, page 125

Release or renew a DHCP WAN connection

If a WAN interface is configured to obtain an IP address from the ISP by using Dynamic Host Configuration Protocol (DHCP), you can click the **Release** icon to release its IP address, or click the **Renew** icon to obtain a new IP address.

Configure the primary WAN

To configure the settings for the primary WAN (WAN1), click the **Edit** (pencil) icon. Then use the WAN - Add/Edit page to configure the connection. If you enabled IPv4/IPv6 routing mode, complete both tabbed pages. Click **OK** to save your settings. Click **Save** to apply your settings to the security appliance.

For IPv4 routing mode, enter the following information on the **IPv4** tab:

- **Physical Port:** The physical port associated with the primary WAN.
- **WAN Name:** The name of the primary WAN (WAN1).
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and complete the corresponding settings. The security appliance supports DHCP Client, Static IP, PPPoE, PPTP, and L2TP. For information on configuring network addressing mode, see Network Addressing Mode, page 125.
- **DNS Server Source:** DNS servers map Internet domain names 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 you have assigned a static DNS IP address. Also enter the addresses in the **DNS1** and **DNS2** fields.
- **MAC Address Source:** Specify the MAC address for the primary WAN. Typically, you can use the unique 48-bit local Ethernet address of the security appliance as your MAC address source.
  - **Use Default MAC Address:** Choose this option to use the default MAC address.

  - **Use the following MAC address:** If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, choose this option and enter the MAC address that your ISP requires for this connection.

- **MAC Address:** Enter the MAC address, for example 01:23:45:67:89:ab.

- **Zone:** Choose the default WAN zone or an untrusted zone for the primary WAN. You can click the **Create Zone** link to view, edit, or add the zones on the security appliance.

For IPv4/IPv6 routing mode, enter the following information on the **IPv6** tab:

- **IP Address Assignment:** Choose **Static IP** if your ISP assigned a fixed (static or permanent) IP address, or choose **SLAAC** if you were not assigned a static IP address. By default, your security appliance is configured to be a DHCPv6 client of the ISP, with stateless address auto-configuration (SLAAC).

  - **SLAAC:** SLAAC provides a convenient method to assign IP addresses to IPv6 nodes. This method does not require any human intervention from an IPv6 user. If you choose SLAAC, the security appliance can generate its own addresses using a combination of locally available information and information advertised by routers.

  - **Static IP:** If your ISP assigned a static IPv6 address, configure the IPv6 WAN connection in the following fields:

    IPv6 Address: Enter the static IP address that was provided by your ISP.

    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: Enter a valid IP address of the primary DNS server.

    Secondary DNS Server (Optional): Optionally, enter a valid IP address of the secondary DNS server.

Configure a secondary WAN

To configure a secondary WAN (WAN2), click **Add**. Then use the WAN - Add/Edit page to configure the connection. If you enabled IPv4/IPv6 routing mode, complete both tabbed pages, as described for the primary WAN interface. Click **OK** to save your settings in the pop-up window. Click **Save** to apply your settings to the security appliance. To determine how the two ISP links are used, configure the WAN redundancy settings. See **Configuring WAN Redundancy, page 130**.

- If you are having problems with your WAN connection, see Internet Connection, page 453.

Network Addressing Mode

The security appliance supports five types of network addressing modes. You need to specify the network addressing mode for the primary WAN and the secondary WAN depending on your ISP requirements.

NOTE Confirm that you have proper network information from your ISP or a peer router to configure the security appliance to access the Internet.

Network Addressing Mode	Configuration
DHCP Client	Connection type often used with cable modems. Choose this option if your ISP dynamically assigns an IP address on connection. **NOTE:** Unless a change is required by your ISP, it is recommended that the MTU values be left as is. ▪ **MTU:** The Maximum Transmission Unit is the size, in bytes, of the largest packet that can be passed on. Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Network Addressing Mode	Configuration
Static IP	Choose this option if the ISP provides you with a static (permanent) IP address and does not assign it dynamically. Use the corresponding information from your ISP to complete the following fields: ▪ **IP Address:** Enter the IP address of the WAN port that can be accessible from the Internet. ▪ **Subnet Mask:** Enter the IP address of the subnet mask. ▪ **Gateway:** Enter the IP address of default gateway. ▪ **MTU:** The Maximum Transmission Unit is the size, in bytes, of the largest packet that can be passed on. Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Network Addressing Mode	Configuration
PPPoE	PPPoE uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. Choose this option if your ISP provides you with client software, username, and password. Use the necessary PPPoE information from your ISP to complete the PPPoE configuration. ▪ **User Name:** Enter the username that is required to log into the ISP. ▪ **Password:** Enter the password that is required to log into the ISP. ▪ **Authentication Type:** Choose the authentication type specified by your ISP. ▪ **Connect Idle Time:** Choose this option to let the security appliance disconnect from the Internet after a specified period of inactivity (Idle Time). This choice is recommended if your ISP fees are based on the time that you spend online. ▪ **Keep alive:** Choose this option to keep the connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service. ▪ **MTU:** Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes. ▪ **Add VLAN Tag:** Click **Yes** to support VLAN Tagging (802.1q) over the WAN port, or click **No** to disable it. ▪ **VLAN Tag ID:** Specify the VLAN tag (ID) to the WAN port. ▪ **Reset Timer:** You can reset the PPPoE connection at a given time of a day and day of a week. The reset events are logged if you enable this feature. Choose one of the following options from the **Frequency** drop-down list and specify the corresponding settings: - **Never:** Choose this option to disable this feature. - **Daily:** Choose this option to reset the PPPoE connection at a given time of a day. Specify the time of a day in the **Time** fields. - **Weekly:** Choose this option to reset the PPPoE connection at a given day of a week. Then specify the day of a week and the time of a day.

Network Addressing Mode	Configuration
PPTP	The PPTP protocol is typically used for VPN connection. Use the necessary information from your ISP to complete the PPTP configuration: ▪ **IP Address:** Enter the IP address of the WAN port that can be accessible from the Internet. ▪ **Subnet Mask:** Enter the subnet mask. ▪ **Gateway:** Enter the IP address of default gateway. ▪ **User Name:** Enter the username that is required to log into the PPTP server. ▪ **Password:** Enter the password that is required to log into the PPTP server. ▪ **PPTP Server IP Address:** Enter the IP address of the PPTP server. ▪ **MPPE Encryption:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in PPP-based dial-up connections or PPTP VPN connections. Check this box to enable the MPPE encryption to provide data security for the PPTP connection that is between the VPN client and the VPN server. ▪ **Connect Idle Time:** Choose this option to let the security appliance disconnect from the Internet after a specified period of inactivity (Idle Time). This choice is recommended if your ISP fees are based on the time that you spend online. ▪ **Keep alive:** Choose this option to keep the connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service. ▪ **MTU:** Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Network Addressing Mode	Configuration
L2TP	Choose this option if you want to use IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypt all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations. Use the necessary information from your ISP to complete the L2TP configuration: ▪ **IP Address:** Enter the IP address of the WAN port that can be accessible from the Internet. ▪ **Subnet Mask:** Enter the subnet mask. ▪ **Gateway:** Enter the IP address of default gateway. ▪ **User Name:** Enter the username that is required to log into the L2TP server. ▪ **Password:** Enter the password that is required to log into the L2TP server. ▪ **L2TP Server IP Address:** Enter the IP address of the L2TP server. ▪ **Secret (Optional):** L2TP incorporates a simple, optional, CHAP-like tunnel authentication system during control connection establishment. Enter the secret for tunnel authentication if necessary. ▪ **Connect Idle Time:** Choose this option to let the security appliance disconnect from the Internet after a specified period of inactivity (Idle Time). This choice is recommended if your ISP fees are based on the time that you spend online. ▪ **Keep alive:** Choose this option to keep the connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service. ▪ **MTU:** Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Configuring WAN Redundancy

If you have two ISP links, one for WAN1 and another for WAN2, use the Networking > WAN Redundancy pages to configure the WAN redundancy to determine how the two ISP links are used. Refer to the following topics:

- **Dual WAN Settings, page 130**
- **Load Balancing with Policy-Based Routing Configuration Example, page 133**

NOTE Before you configure the WAN redundancy settings, you must first configure the secondary WAN connection. See **Configure a secondary WAN, page 125**.

NOTE When the security appliance is working in the Dual WAN Settings or Failover mode, if one WAN link is down such as the cable is disconnected, the WAN redundancy and Policy-Based Routing settings are ignored and all traffic is handled by the active WAN port.

Dual WAN Settings

Use the Networking > WAN Redundancy > Dual WAN Settings page to segregate traffic between links that are not of the same speed. For example, you can bind the high-volume services through the port that is connected to a high speed link, and bind the 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 address public and keeping the other one private.

NOTE To configure load balancing, make sure that you configure both WAN ports to keep alive. If the WAN port is configured to time out after a specified period of inactivity, then load balancing is not applicable.

STEP 1 Choose an option in the Dual WAN Settings section to specify how the two ISP links are used. The two links will carry data for the protocols that are bound to them.

- **Weighted Dual WAN Settings:** Distributes the bandwidth to two WAN ports by the weighted percentage or by the weighted link bandwidth. If you choose this mode, choose one of the following options and finish the settings:
  - **Weighted by Percentage:** If you choose this option, specify the percentage for each WAN, such as 80% bandwidth for WAN1 and at least 20% 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. For example, you can set 60 Mbps for WAN1 and 40 Mbps for WAN2, which indicates that 60% bandwidth is distributed to WAN1 and the remaining 40% bandwidth is distributed to WAN2.

- **Based on Real-time Bandwidth:** Sends traffic to the link that has the highest real-time bandwidth. Use information from your service provider to specify the base bandwidth for each link in the **WAN1** and **WAN2** fields.

- **Failover:** If a failure is detected on the primary link, then the security appliance diverts 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. By default, WAN1 is set as the primary link and the WAN2 is set as the backup link.

  NOTE: When the security appliance is working in the Failover mode, the Policy-Based Routing settings will be ignored.

  - **Select WAN Precedence:** Choose which link to use as the primary link and the secondary link. The default option is Primary: WAN1; Secondary: WAN2.

  - **Preempt Delay Timer:** Enter the time in seconds that the security appliance will wait before sending traffic to the primary link from the backup link after the primary link is up again. The default value is 5 seconds.

- **Routing Table:** Uses the static routing policies to determine the types of traffic that pass through the two WAN links. For information on configuring static routing, see **Configuring Static Routing, page 151**.

STEP 2 Enable **Policy Based Routing** if you want to use policies to specify the internal IP and/or service going through each WAN port to provide more flexible and granular traffic handling capabilities. Click **On** to enable this feature, or click **Off** to disable it. After enabling this feature, click **Configure** to set the policies. See **Configuring Policy-Based Routing, page 153**.

NOTE: If you enable Policy-Based Routing, the policy-based routing settings will take precedence over the load balancing settings. Traffic matching the policy-based routing policies will be routed based on these settings. Traffic not matching the policy-based routing policies will be routed based on the load balancing settings.

STEP 3 Click **Save** to apply your settings.

Configuring Link Failover Detection

Use the Networking > WAN > WAN Redundancy > Link Failover Detection page to detect the link failure. If a failure occurs, traffic for the unavailable link is diverted to the active link.

STEP 1 Enter the following information:

- **Failover Detection:** Click **On** to enable the Link Failover Detection feature, or click **Off** to disable it.
- **Retry Count:** Enter the number of retries. The security appliance repeatedly tries to connect to the ISP after the link failure is detected. The default value is 5.
- **Retry Timeout:** If the connection to the ISP is down, the security appliance tries to connect to the ISP after a specified timeout. Enter the timeout, in seconds, to re-connect to the ISP. The default value is 5 seconds.
- **Ping Detection:** Choose this option to detect the WAN failure by pinging the IP address that you specify in the following fields:
  - **Default IP Gateways:** Ping the IP address of default WAN gateway. If the default WAN gateway can be detected, the network connection is active.
  - **Specify the IP Gateways:** Ping the specified remote hosts. Enter the IP addresses in the **Primary IP Gateway** and **Secondary IP Gateway** fields. In Failover mode, if the primary WAN remote host can be detected, the network connection is active. When using Dual WAN Settings, if the remote hosts for both WAN ports can be detected, the WAN connection is active.

- **DNS Detection:** Choose this option to detect the WAN failure by looking up the DNS servers that you specify in the following fields:
  - **Default DNS Servers:** Send 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.
  - **Specify DNS Servers:** Send the DNS query for www.cisco.com to the specified DNS servers. Enter the IP addresses in the **Primary WAN DNS Server** and **Secondary WAN DNS Server** fields. If the primary or secondary DNS server can be detected, the network connection is active.

STEP 2 Click **Save** to apply your settings.

Load Balancing with Policy-Based Routing Configuration Example

Use Case: A customer has two lines, one is a cable link and another is a DSL link. The majority of traffic goes through the cable link since it has larger bandwidth, and the rest traffic goes through the DSL link. As lots of secure websites (such as bank, or online shopping) are sensitive to flip flop the source IP address, let traffic for https, ftp, video, and game go through the cable link.

Solution: Complete the following configuration tasks:

- Configure a configurable port as the secondary WAN (WAN2). See **Configure a secondary WAN, page 125**.
- Connect the cable modem to the primary WAN port (WAN1) and connect the DSL modem to the secondary WAN port (WAN2).
- Enable the Weighted Dual WAN Settings and set the weighted value of WAN1 to 80% and the weighted value of WAN2 to 20%. See **Dual WAN Settings, page 130**.
- Enable the Policy-Based Routing feature and configure the Policy-Based Routing rules so that traffic for HTTPS, FTP, video, and game is directed to WAN1. See **Configuring Policy-Based Routing, page 153**.
- (Optional) Enable the Usage reports and the WAN Bandwidth reports so that you can view the network bandwidth usage. See **Usage Reports, page 92** and WAN Bandwidth Reports, page 94.

Configuring Dynamic DNS

Use the Networking > WAN > DDNS page to configure Dynamic DNS (DDNS). 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 obtain an IP address dynamically, then DDNS provides the domain name to map the dynamic IP address for your website. To use DDNS, you must set up an account with a DDNS provider such as DynDNS.com.

DDNS Services Table

The **Status** column displays the status of DDNS service. Click **Active** to manually update the IP address of the WAN interface to the user-specified domain name.

- **Non-active:** The DDNS service is not active (DDNS daemon does not start).
- **Active (initial):** The DDNS daemon starts but the DDNS updating process is not complete yet.
- **Active (updated WAN**x**):** The DDNS updating process is complete and the address of the WAN interface is updated to the user-specified domain name.

Adding or modifying a DDNS service

Click **Add** to add a new DDNS service. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 1 Enter the following information:

- **Service:** Specify the provider for your DDNS service. You can 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:** Check this box to activate the DDNS service when the security appliance starts up.
- **WAN Interface:** Choose the WAN port for the DDNS service. Traffic for the 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:** Enter the complete host name and domain name for the DDNS service, for example: name.dyndns.org.

- **Wildcards:** Check this box to allow all subdomains of your DDNS host name to share the same public IP address as the host name.

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

STEP 2 Click **OK** to save your settings and close the pop-up window.

STEP 3 Click **Save** to apply your settings.

Measuring and Limiting Traffic with the Traffic Meter

Use the Networking > WAN > Traffic Metering pages to measure and limit traffic routed by the security appliance. If you enabled a secondary WAN link, use the navigation tree to choose either Primary WAN Metering or Secondary WAN Metering.

STEP 1 In the **Traffic Meter** area, enter the following information:

- **Enable:** Click **On** to enable traffic metering on the port, or click **Off** to disable it. Enabling this feature on the port will keep a record of the volume of traffic going from this port.

- **Traffic Limit:** Specify the restriction on the volume of data being transferred through the port.

  - **No Limit:** The default option, where no limits on data transfer are imposed.

  - **Download Only:** Limit the amount of download traffic. Enter the maximum allowed data in Megabytes that can be downloaded for a given month in the **Monthly Limit** field. After the limit is reached, no traffic is allowed from the WAN side.

  - **Both Directions:** Calculate traffic for both upload and download directions. The traffic limit entered into the **Monthly Limit** field is shared by both upload and download traffic. For example, for a 1 GB 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 that is applicable for this month. This limit will apply to the type of direction (Download Only or Both Direction) selected above. The value of zero (0) indicates that all traffic through this port will be blocked.

STEP 2 In the **Traffic Counter** area, enter the following information:

- **Traffic Counter:** Specify the action to be taken on the traffic counter.
  - **Restart Now:** Choose this option and then click **Save** to reset the counter immediately.
  - **Specific Time:** Choose this option if you want the counter to restart at a specified day and time. Then enter the time in hours (hh) and minutes (mm) and select the day of the month in the **Reset Time** area.
- **Send Email Report:** Click **On** to send an alert email to the specified email address before the traffic counter is reset, or click **Off** to disable it. This feature requires that you enable the Traffic Meter Alert feature and configure the email server settings on the Email Alert Settings page. See Configuring Email Alert Settings, page 408.

STEP 3 In the **When Limit is Reached** area, specify the action when the traffic limit is reached.

- **Traffic Block:** Choose one of the following options:
  - **All Traffic:** Block all traffic through the WAN port when the traffic limit is reached.
  - **All Traffic Except Email:** Block all traffic except email through the WAN port when the traffic limit is reached.
- **Email Alert:** Click **On** to send an alert email to the specified email address when the traffic limit is reached, or click **Off** to disable it. This feature requires that you enable the Traffic Meter Alert feature and configure the email server settings on the Email Alert Settings page. See Configuring Email Alert Settings, page 408.

STEP 4 In the **Internet Traffic** area, the following information is displayed after you enable Traffic Metering:

Start Date/Time	Date on which the traffic meter was started or the last time that the traffic counter was reset.
Outgoing Traffic Volume	Volume of traffic, in Megabytes, that was uploaded through this port.
Incoming Traffic Volume	Volume of traffic, in Megabytes, that was downloaded through this port.
Average per day	Average volume of traffic that passed through this port.
Traffic Utilized	Amount of traffic, in percent, that passed through this port against the monthly limit.

STEP 5 Click **Save** to apply your settings.

Configuring a VLAN

Use the Networking > WAN > VLAN page to configure a Virtual LAN (VLAN). VLANs allow you to segregate and isolate traffic. A PC on one VLAN cannot access the network resources on other VLANs.

The security appliance predefines three VLANs:

- A native VLAN (DEFAULT), with VLAN ID 1 and IP address 192.168.75.1. By default, this VLAN is in the LAN zone.
- A guest VLAN (GUEST), with VLAN ID 2 and IP address 192.168.25.1. By default, this VLAN is in the GUEST zone.
- A voice VLAN (VOICE) with VLAN ID 100 and IP address 10.1.1.2. By default, this VLAN is in the VOICE zone.

You can change the settings for predefined VLANs or add new VLANs to meet your business needs.

NOTE Up to 16 VLANs can be configured on the security appliance.

STEP 1 To add a new VLAN, click **Add**. To modify the settings for a VLAN, click the **Edit** (pencil) icon.

Other options: To delete a VLAN, click the **Delete** (x) icon. The default VLANs cannot be deleted.

STEP 2 In the **Basic Settings** tab, enter the following information:

- **Name:** Enter the name for the VLAN.
- **VLAN ID:** Enter a unique identification number for the VLAN, which can be any number from 3 to 4089. The VLAN ID 1 is reserved for the DEFAULT VLAN and the VLAN ID 2 is reserved for the GUEST VLAN.
- **IP Address:** Enter the subnet IP address for the VLAN.
- **Netmask:** Enter the subnet mask for the VLAN.
- **Spanning Tree:** Check this box to enable the Spanning Tree feature to determine if there are loops in the network topology. The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. The STP is used to prevent bridge loops and to ensure broadcast radiation.
- **Voice VLAN:** Check the box if you want voice applications to use this VLAN.
- **Port:** Assign the LAN ports to the VLAN. Traffic through the selected LAN ports is directed to the VLAN. All available ports including the dedicated LAN ports and the configurable ports appear in the **Port** list.

  Choose the ports from the **Port** list and click **Access** to add them to the **Member** list and set the selected ports as the Access mode. Alternatively, you can choose the ports from the **Port** list and click **Trunk** to add them to the **Member** list and set the selected ports as the Trunk mode.

  NOTE: This setting will change the port type and access mode of the selected physical ports. For example, choose a port that was set as a DMZ port and add it to the Member list. The DMZ port will be configured as a LAN port. Changing the port type will wipe out all configuration relative to the physical port.
- **Zone:** Choose the zone to which the VLAN is mapped. By default, the DEFAULT VLAN is mapped to the LAN zone, the GUEST VLAN is mapped to the GUEST zone, and the VOICE VLAN is mapped to the VOICE zone. You can click the **Create Zone** link to view, edit, or add the zones on the security appliance.

STEP 3 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 VLAN 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 VLAN. Any new DHCP client joining the VLAN 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 4 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 VLAN 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 will be 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 VLAN.
- **Default Gateway:** Enter the IP address for default gateway.
- **Option 66:** Provides provisioning server address information to hosts requesting this option. Only supports the IP address or host name of a single TFTP server. Enter the IP address of the single TFTP server for the VLAN.
- **Option 67:** Provides a configuration/bootstrap file name to the hosts requesting this option. This is used in conjunction with the option 66 to allow the client to form an appropriate TFTP request for the file. Enter the configuration/bootstrap file name on the specified TFTP server.

- **Option 150:** Supports a list of TFTP servers (2 TFTP servers). Enter the IP addresses of TFTP servers. Separate multiple entries with commas (,).

  NOTE: Enterprises with small branch offices that implement a Cisco IP Telephony Voice over IP solution typically implement Cisco CallManager at a central office to control Cisco IP Phones at small branch offices. This implementation allows centralized call processing, reduces the equipment required, and eliminates the administration of additional Cisco CallManager and other servers at branch offices. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address pre-configured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

STEP 5 In the **IPv6 Setting** tab, specify IPv6 addressing for the VLAN if you enable the IIPv4 or Pv6 mode.

- **IPv6 Address:** Enter the IPv6 address based on your network requirements.
- **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 6 Click **OK** to save your settings and close the pop-up window.

STEP 7 Click **Save** to apply your settings.

STEP 8 If you want to reserve certain IP addresses for specified devices, go to the Networking > DHCP Reservations page. See **Configuring DHCP Reserved IPs, page 149**. You must enable the DHCP Server or DHCP Relay mode for this purpose.

Configuring DMZ

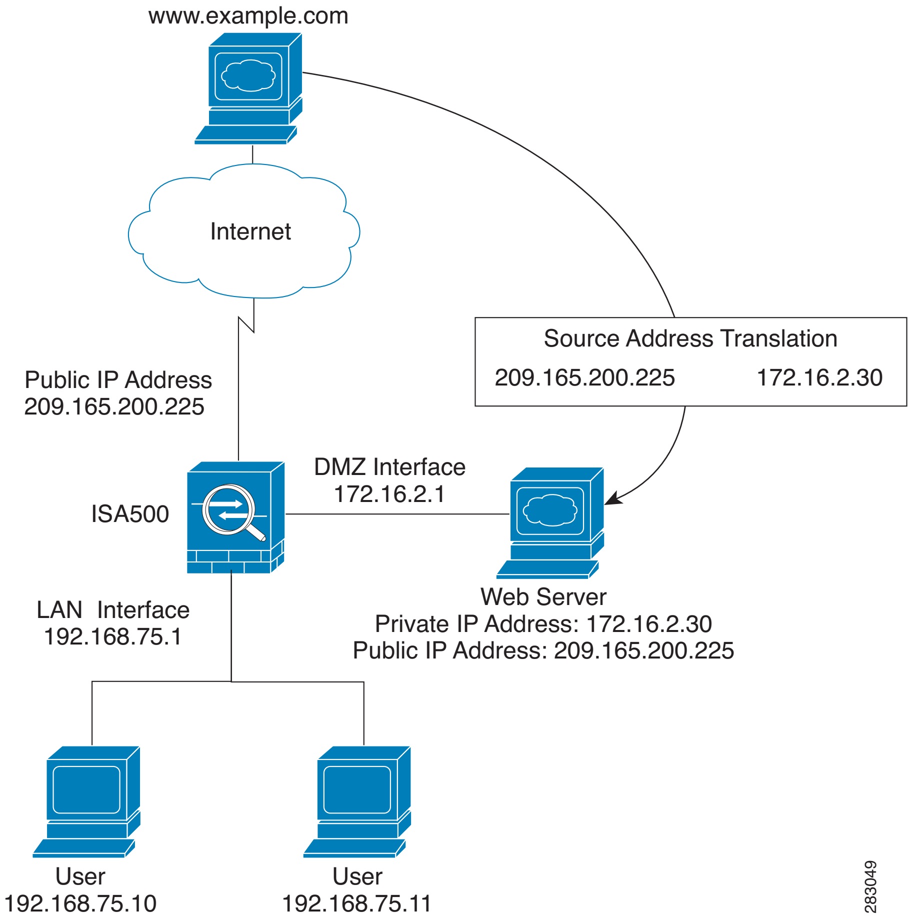
Use the Networking > DMZ page to configure a Demarcation Zone or Demilitarized Zone (DMZ). A DMZ is a sub-network that is behind the firewall but that is open to the public. By placing your public services on a DMZ, you can add an additional layer of security to the LAN. The public can connect to the 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).

About DMZ networks

This section describes how to configure the DMZ networks. The DMZ configuration is identical to the VLAN configuration. There are no restrictions on the IP address or subnet assigned to the DMZ port, except it cannot be identical to the IP address given to the predefined VLANs.

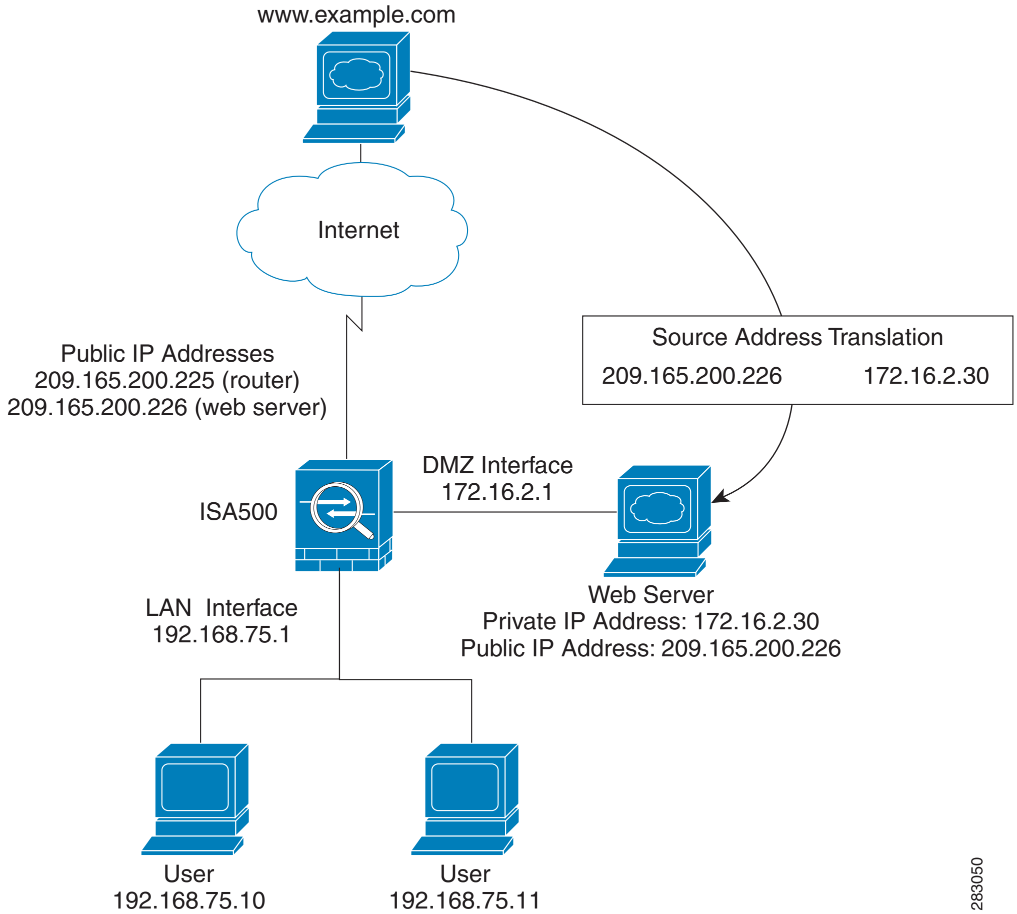
NOTE Up to 4 DMZs can be configured on the security appliance.

Figure 1 Example DMZ with One Public IP Address for WAN and DMZ



In this scenario, the business has one public IP address, 209.165.200.225, which is used for both the security appliance's public IP address and the web server's public IP address. The administrator configures the configurable 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 enter the domain name that is associated with the IP address 209.165.200.225 and can then connect to the web server. The same IP address is used for the WAN interface.

Figure 2 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 security appliance's public IP address. The administrator configures the configurable 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 enter the domain name that is associated with the IP address 209.165.200.226 and can then connect to the web server.

Configuring a DMZ

STEP 1 To add a new DMZ, click **Add**. To modify the settings for a DMZ, click the **Edit** (pencil) icon.

Other options: To delete a DMZ, click the **Delete** (x) icon.

STEP 2 In the **Basic Settings** tab, enter the following information:

- **Name:** Enter the name for the DMZ.
- **IP Address:** 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:** Specify a configurable port as a DMZ port. Traffic through the DMZ port is directed to the DMZ. All available configurable ports appear in the **Port** list. Choose a port from the **Port** list and add it to the **Member** list. The selected configurable port will be set as a DMZ port.

  NOTE: This setting will change the port type and access mode of the selected configurable port. Changing the port type will wipe out all configuration relative to the physical port.
- **Zone:** Choose the default DMZ zone or a custom DMZ zone to which the DMZ is mapped. You can click the **Create Zone** link to view, edit, or add the zones on the security appliance.

STEP 3 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 4 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address in the DHCP range.
- **End IP:** Enter the ending IP address in the DHCP range.

  NOTE: The Start and End IP addresses must 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 will be automatically renewed the dynamic IP address.
- **DNS 1:** Enter the IP address of the primary DNS server.
- **DNS 2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS 1:** Optionally, enter the IP address of the primary WINS server.
- **WINS 2:** 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.
- **Option 66:** Provides provisioning server address information to hosts requesting this option. Only supports the IP address or host name of a single TFTP server. Enter the IP address of the single TFTP server for the DMZ.
- **Option 67:** Provides a configuration/bootstrap file name to the hosts requesting this option. This is used in conjunction with the option 66 to allow the client to form an appropriate TFTP request for the file. Enter the configuration/bootstrap file name on the specified TFTP server.
- **Option 150:** Supports a list of TFTP servers (2 TFTP servers). Enter the IP addresses of TFTP servers. Separate multiple entries with commas (,).

STEP 5 In the **IPv6 Setting** tab, specify IPv6 addressing for the DMZ if you enable the IPv4/IPv6 mode.

- **IPv6 Address:** Enter the IPv6 address based on your network requirements.
- **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 6 Click **OK** to save your settings.

STEP 7 Click **Save** to apply your settings.

STEP 8 If you want to reserve certain IP addresses for specified devices, go to the Networking > DHCP Reservations page. See **Configuring DHCP Reserved IPs, page 149**. You must enable DHCP Server or DHCP Relay mode for this purpose.

Configuring Zones

Use the Networking > Zones page to configure a security zone, which is a group of interfaces to which a security policy can be applied. The interfaces in a zone share common functions or features. For example, two interfaces that are connected to the local LAN might be placed in one security zone, and the interfaces connected to the Internet might be placed in another security zone.

The interfaces are IP-based interfaces (VLANs, WAN1, WAN2, and so forth). Each interface can only join one zone, but each zone with specific security level can have multiple interfaces.

Refer to the following topics:

- **Security Levels for Zones, page 146**
- **Predefined Zones, page 147**
- **Configuring Zones, page 147**

NOTE We recommend that you configure the zones before you configure WAN, VLAN, DMZ, zone-based firewall, and security services.

Security Levels for Zones

The security level for the zone defines the level of trust given to that zone. The security appliance supports five security levels for the zones as described below. The greater value, the higher the permission level. The predefined VPN and SSLVPN zones have the same security level.

- **Trusted(100):** Offers the highest level of trust. The LAN zone is always trusted.
- **VPN(75):** Offers a higher level of trust than a public zone, but a lower level of trust than a trusted zone, which is used exclusively by the predefined VPN and SSLVPN zones. All traffic to and from a VPN zone is encrypted.
- **Public(50):** Offers a higher level of trust than a guest zone, but a lower level of trust than a VPN zone. The DMZ zone is a public zone.
- **Guest(25):** Offers a higher level of trust than an untrusted zone, but a lower level of trust than a public zone. Guest zones can only be used for guest access.

- **Untrusted(0):** Offers the lowest level of trust. It is used by both the WAN and the virtual multicast zones. You can map the WAN port to an untrusted zone.

Predefined Zones

The security appliance predefines the following zones with different security levels:

- **WAN:** The WAN zone is an untrusted zone. By default, the WAN1 port is mapped to the WAN zone. If the secondary WAN (WAN2) is applicable, it can be mapped to the WAN zone or any other untrusted zone.
- **LAN:** The LAN zone is a trusted zone. You can map one or multiple VLANs to a trusted zone. By default, the DEFAULT VLAN is mapped to the LAN zone.
- **DMZ:** The DMZ zone is a public zone used for the public servers that you host in the DMZ networks.
- **SSLVPN:** The SSLVPN zone is a virtual zone used for simplifying secure and remote SSL VPN connections. This zone does not have an assigned physical port.
- **VPN:** The VPN zone is a virtual zone used for simplifying secure IPsec VPN connections. This zone does not have an assigned physical port.
- **GUEST:** The GUEST zone can only be used for guest access. By default, the GUEST VLAN is mapped to this zone.
- **VOICE:** The VOICE zone is a security zone designed for voice traffic. Traffic coming and outgoing from this zone will be optimized for voice operations. If you have voice devices, such as Cisco IP Phone, it is desirable to place the devices into the VOICE zone.

Configuring Zones

This section describes how to configure the zones on the security appliance. You can restore the zone configuration to the factory default settings, edit the settings of the predefined zones (except for the VPN and SSLVPN zones), or customize new zones for your specific business needs.

NOTE You can click **Reset** to restore your zone configuration to the factory default settings. All custom zones will be removed and the settings relevant to these custom zones will be cleaned up after you perform this operation.

STEP 1 To add a new zone, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

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

NOTE: All predefined zones (except for the VOICE zone) cannot be deleted. Only the associated ports and VLANs for the predefined zones (except for the VPN and SSLVPN zones) can be edited.

STEP 2 Enter the following information:

- **Name:** Enter the name for the zone.
- **Security Level:** Specify the security level for the zone.
  - For VLANs, all security levels are selectable.
  - For DMZs, choose Public(50).
  - For WAN ports, choose Untrusted(0).
- **Map interfaces to this zone:** Choose the existing VLANs or WAN ports from the **Available Interfaces** list and click the right arrow to add them to the **Mapped to Zone** list. Up to 16 VLANs can be mapped to a zone.

STEP 3 Click **OK** to save your settings and close the pop-up window.

STEP 4 Click **Save** to apply your settings.

NOTE Next steps:

- After you create a new zone, a certain amount of firewall rules will be automatically generated to permit or block traffic from the new zone to other zones or from other zones to the new zone. The permit or block action is determined by the security level of the new zone. By default, the firewall prevents all inbound traffic and allows all outbound traffic. To customize firewall rules for the new zone, go to the Firewall > Access Control > ACL Rules page. For information on configuring firewall rules, see Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 252.
- Apply the security services on the zones if you enable the security services such as Intrusion Prevention (IPS), Anti-Virus, and Application Control on the security appliance. For complete details, see **Chapter 7, "Security Services."**

Configuring DHCP Reserved IPs

Use the Networking > DHCP Reservations page to reserve certain IP addresses for specified devices, identified by their MAC addresses. Whenever the 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.

STEP 1 To add a DHCP Reservation rule, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

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

The DHCP IP Reservation- Add/Edit window opens.

STEP 2 Enter the following information:

- **Name:** Enter the name for the DHCP Reservation rule.
- **MAC Address:** Enter the MAC address of the host under a VLAN.
- **IP Address:** Enter the IP address that is assigned to the host. The address must be within the DHCP pool of the VLAN.

STEP 3 Click **OK** to save your settings and close the pop-up window.

STEP 4 Click **Save** to apply your settings.

Configuring Routing

This section provides information on configuring the routing mode between WAN and LAN, viewing the routing table, and configuring the static routing, dynamic routing, and Policy-Based Routing settings. Refer to the following topics:

- **Viewing the Routing Table, page 150**
- **Configuring Routing Mode, page 150**
- **Configuring Static Routing, page 151**
- **Configuring Dynamic Routing - RIP, page 152**
- **Configuring Policy-Based Routing, page 153**

Viewing the Routing Table

Use the **Networking > Routing > Routing Table** page to view the following information:

- **Destination Address:** The IP address of the host or the network that the route leads to.
- **Subnetwork Mask:** The subnet mask of the destination network.
- **Gateway:** The IP address of the gateway through which the destination host or network can be reached.
- **Flags:** The status flag of the route.
- **Metric:** The cost of a route. Routing metrics are assigned to routes by routing protocols to provide measurable values that can be used to judge how useful (or how low cost) a route will be.
- **Interface:** The physical port through which this route is accessible.

This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the routing table.

Configuring Routing Mode

Use the **Networking > Routing > Routing Mode** page to enable or disable routing mode, based on the requirements of your ISP. By default, routing mode is disabled.

STEP 1 Enable or disable routing mode:

- If your ISP assigns an IP address for each of the computers that you use, click **On** to enable the Routing mode.
- If you are sharing IP addresses across several devices such as your LAN and using other dedicated devices for the DMZ, click **Off** to disable the Routing mode.

STEP 2 Click **Save** to apply your settings.

Configuring Static Routing

Use the Networking > Routing > Static Routing page to configure static routes. You can optionally assign a priority, which determines the route is selected when there are multiple routes travelling to the same destination.

NOTE Up to 150 static routing rules can be configured on the security appliance.

STEP 1 To add a static route, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

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

STEP 2 Enter the following information:

- **Destination Address:** Choose an existing address object for the host or for the network that the route leads to. If the address object that you want is not in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to the Networking > Address Management page. See **Address Management, page 175**.
- **Setting as default route:** Check this box to set this static route as the default route.
- **Next Hop:** Choose a port or an IP address as the next hop for this static route.
  - **Interface:** Choose either WAN1 or WAN2 as the next hop.
  - **IP Address:** Choose an IP address of the gateway through which the destination host or network can be reached.
- **Metric:** Optionally, enter a number to manage the route priority. If multiple routes to the same destination exist, the route with the lowest metric is selected.

STEP 3 Click **OK** to save your settings and close the pop-up window.

STEP 4 Click **Save** to apply your settings.

Configuring Dynamic Routing - RIP

Use the Networking > Routing > Dynamic - RIP page to configure Dynamic Routing or RIP. 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.

STEP 1 At the top of the page, enter the following information:

- **RIP Enable:** Click **On** to enable RIP, or click **Off** to disable it. By default, RIP is disabled.
- **RIP Version:** If you enable RIP, specify the RIP version. The security appliance supports RIP Version 1 and RIP Version 2.
  - **RIP Version 1** is a class-based routing version that does not include subnet information. This is the most commonly supported version.
  - **RIP Version 2** includes all the functionality of RIPv1 plus it supports subnet information.
  - **Default:** The data is sent in RIP Version 1 format and received in RIP Version 1 and 2 format. This is the default setting.

STEP 2 In the table, specify the RIP settings for each available interface:

- **RIP Enable:** Check this box to enable the RIP settings on the port or VLAN.
- **Authentication:** If you are using RIP Version 2, click the **Edit** (pencil) icon to specify the authentication method for the port or VLAN.
  - **None:** Choose this option to invalidate the authentication.
  - **Simple Password Authentication:** Choose this option to validate the simple password authentication. Enter the password in the field.
  - **MD5 Authentication:** Choose this option to validate the MD5 authentication. Enter the unique key ID in the **MD5 Key ID** field and the Key in the **MD5 Auth Key** field.
- **Port Passive:** Determines how the security appliance receives RIP packets. Check this box to enable this feature on the port or VLAN.

STEP 3 Click **Save** to apply your settings.

Configuring Policy-Based Routing

Use the Networking > Routing > Policy Based Routing page to configure Policy-Based Routing (PBR). PBR specifies the internal IP and/or service going through a WAN port to provide more flexible and granular traffic handling capabilities. Up to 100 Policy-Based Routing rules can be configured on the security appliance.

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, although HTTP traffic is typically routed through WAN1, by using PBR you can bind the HTTP protocol to WAN1 and bind the FTP protocol to WAN2. In this case, the security appliance automatically channels FTP data through WAN2.

If multiple routing features operate simultaneously, the security appliance first matches the Policy-Based Routing rules, and then matches the Static Routing and default routing rules. For example, if the WAN redundancy is set as the Weighted Dual WAN Settings and the Policy-Based Routing and Static Routing rules are configured, the routing priority works as follows:

1. If traffic cannot match the Policy-Based Routing or Static Routing rules, traffic follows the Weighted Dual WAN Settings.
2. If traffic A matches the Policy-Based Routing or Static Routing rules, it will first be handled by the Policy-Based Routing or Static Routing rules, while other traffic follows the Weighted Dual WAN Settings.

NOTE Make sure that you configure a secondary WAN connection and that the WAN redundancy is set to Dual WAN Settings or Routing Table mode before you configure the Policy-Based Routing settings.

STEP 1 Click **On** to enable PBR, or click **Off** to disable it.

STEP 2 To add a new PBR rule, click **Add.** To edit an entry, click the **Edit** (pencil) icon.

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

STEP 3 Enter the following information:

- **From:** Choose the VLAN that traffic originates from.
- **Service:** For service binding only, choose an existing service. For IP binding only, choose **All Traffic**. 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**.
- **Source IP:** For service binding only, choose **Any**. For IP binding only, choose the source IP address for outbound traffic. If the address object that you want is not in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to the Networking > Address Management page. See **Address Management, page 175**.
- **Destination IP:** For service binding only, choose **Any**. For IP binding only, choose the destination IP address for outbound traffic.
- **DSCP:** Choose the DSCP value to assign the traffic priority.
- **Route to:** Choose the WAN port that outbound traffic routes to.
- **Failover:** Click **On** to enable WAN Failover, or click **Off** to disable it. When the selected WAN port for routing is down, enabling Failover will forward traffic to the backup WAN.

  NOTE: When one WAN connection is down (a connection failure is detected by ping or DNS query) and the Failover feature of PBR is disabled, traffic will be dropped.

STEP 4 Click **OK** to save your settings and close the pop-up window.

STEP 5 Click **Save** to apply your settings.

NOTE: After you apply your settings, the modified PBR settings will take effect immediately for any new sessions, but not for the existing sessions. You can manually clear the existing sessions on the Firewall > Session Limits page to apply the PBR settings immediately for all new sessions.

Configuring Quality of Service

The Quality of Service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and that the desired traffic receives preferential treatment.

QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games, and IPTV, since these applications are delay sensitive and often require a fixed bit rate.

Refer to the following topics:

- **General QoS Settings, page 155**
- **Configuring WAN QoS, page 156**
- **Configuring LAN QoS, page 166**
- **Configuring Wireless QoS, page 169**
- **Understanding DSCP Values**

General QoS Settings

Use the General Settings page to enable or disable the WAN QoS, LAN QoS, and WLAN QoS features.

STEP 1 Click **Networking** > **QoS** > **General Settings**.

STEP 2 Enter the following information:

- **WAN QoS:** Check this box to enable WAN QoS. By default, WAN QoS is disabled.
- **LAN QoS:** Check this box to enable LAN QoS. LAN QoS specifies priority values that can be used to differentiate traffic and give preference to higher-priority traffic, such as telephone calls. By default, LAN QoS is disabled.
- **Wireless QoS:** Check this box to enable Wireless QoS. Wireless QoS controls priority differentiation for data packets in wireless egress direction. By default, Wireless QoS is disabled. The wireless QoS only applies to the ISA550W and ISA570W.

STEP 3 Click **Save** to apply your settings.

Configuring WAN QoS

This section describes how to configure WAN QoS. Refer to the following topics:

- **Managing WAN Bandwidth for Upstream Traffic, page 156**
- **Configuring WAN Queue Settings, page 157**
- **Configuring Traffic Selectors, page 158**
- **Configuring WAN QoS Policy Profiles, page 160**
- **Configuring WAN QoS Class Rules, page 160**
- **Mapping WAN QoS Policy Profiles to WAN Interfaces, page 161**
- **WAN QoS Configuration Example, page 162**
- **Configure WAN QoS for Voice Traffic from LAN to WAN, page 164**
- **Configuring WAN QoS for Voice Traffic from WAN to LAN, page 165**

Managing WAN Bandwidth for Upstream Traffic

Use the Bandwidth page to specify the maximum bandwidth for upstream traffic allowed on each WAN interface.

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

STEP 2 Enter the amount of maximum bandwidth for upstream traffic allowed on each WAN interface. The default value is 6000 Kbps, which indicates that there is no limit for upstream traffic.

STEP 3 Click **Save** to apply your settings.

Configuring WAN Queue Settings

Use the Queue Settings page to determine how traffic in queues is handled for each WAN port. The security appliance supports six queues for the WAN ports, Q1 to Q6. There are three ways of determining how traffic in queues is handled:

Strict Priority (SP)	Egress traffic from the highest-priority queue (Q1) is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the highest numbered queue.
Weighted Round Robin (WRR)	Distributes the bandwidth between the classes using the weighted round robin scheme. The weights decide how fast each queue can send packets. In WRR mode the number of packets sent from the queue is proportional to the weight of the queue. The higher the weight, the more frames are sent.
Low Latency Queuing (LLQ)	The default setting, Low Latency Queuing (LLQ) allows delay-sensitive data (such as voice) to be given preferential treatment over other traffic by sending it first. You can enter the PQ for Q1 and a description for each queue. By default the PQ is 1200 Kbps. The Queue Descriptions are: Q1—Voice traffic Q2—Signaling Q3—Routing/VPN control Q4—Management Q5—Video Q6—Best Effort

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

STEP 2 Specify the way of determining how traffic in queues is handled for each WAN port.

- **Strict Priority (SP):** Set the order in which queues are serviced, traffic scheduling for the selected queue and all higher queues is based strictly on the queue priority, starting with Q1 (the highest priority queue) and going to the next lower queue when each queue is complete.
- **Weighted Round Robin (WRR):** Enter the WRR weight, in percentage, assigned to the queues that you want to use. Traffic scheduling for the selected queue is based on WRR.
- **Low Latency Queuing (LLQ):** Apply SP mode to Q1 and WRR mode to other queues (Q2 to Q6). Q1 has the highest priority and is always processed to completion before the lower priority queues. If you choose LLQ, enter the amount of bandwidth assigned to Q1, and enter the WRR weights for other queues that you want to use.

STEP 3 If needed, enter a brief description for each queue in the field in the **Queue Description** column.

STEP 4 In the **Random Early Detection** area, click **On** to enable the Random Early Detection (RED) mechanism, or click **Off** to disable RED. RED is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

STEP 5 Click **Save** to apply your settings.

Configuring Traffic Selectors

Traffic Selector (or Traffic Classification) is used to classify traffic through WAN interfaces to a given traffic class so that traffic in need of management can be identified.

NOTE Up to 256 traffic selectors can be configured on the security appliance.

STEP 1 Click **Networking > QoS > WAN QoS > Traffic Selector (Classification)**.

The Traffic Selector (Classification) window opens.

STEP 2 To add a new traffic selector, click **Add**.

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

The Traffic Selector - Add/Edit window opens.

STEP 3 Enter the following information:

- **Class Name:** Enter a descriptive name for the traffic class.
- **Source Address:** Choose **Any** or choose an existing address or address group (network) that traffic comes from.
- **Destination Address:** Choose **Any** or choose an existing address or address group (network) that traffic goes to.

  If the address objects that you want are not in the list, choose **Create a new address group** to create a new address group object or choose **Create a new address** to create a new address object. To maintain the address or address group objects, go to the Networking > Address Management page. See **Address Management, page 175**.
- **Source Service:** Choose **Any** or choose an existing service from the drop-down list.
- **Destination Service:** Choose **Any** or choose an existing service from the drop-down list.

  If the service objects that you want are 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**.
- **DSCP:** DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Select the DSCP values for the traffic class and click the right arrow. For more information, see **Understanding DSCP Values, page 171**.
- **CoS:** QoS-based IEEE 802.1p Class of Service (CoS) specifies a priority value of between 0 and 7 that can be used to differentiate traffic and give preference to higher-priority traffic. Choose the CoS value for the traffic class.
- **VLAN:** Choose the VLAN for identifying the host to which the traffic selector will apply.

NOTE: Traffic that matches the above settings will be classified to a class for management purposes.

STEP 4 Click **Save** to apply your settings.

Configuring WAN QoS Policy Profiles

Use the QoS Policy Profile page to configure class-based policy profiles for managing traffic through the WAN interfaces.

NOTE Up to 32 WAN QoS policy profiles can be configured on the security appliance.

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

STEP 2 To add a new WAN QoS policy profile, click **Add**.

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

The QoS Policy - Add/Edit window opens.

STEP 3 Enter the following information:

- **Policy Name:** Enter the name for the WAN QoS policy profile.
- **Apply this policy to:** Click **Inbound Traffic** to apply this policy profile for inbound traffic, or click **Outbound Traffic** to apply this policy profile for outbound traffic.

STEP 4 Specify the QoS settings for the traffic classes that you want to associate with the policy profile. For complete details, see **Configuring WAN QoS Class Rules, page 160**.

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

STEP 6 Click **Save** to apply your settings.

Configuring WAN QoS Class Rules

This section describes how to configure the QoS class rules that you want to associate with the WAN QoS policy profile.

NOTE Up to 64 traffic classes can be associated with one WAN QoS policy profile.

STEP 1 In the **QoS Class Rules** area, click **Add** to add a WAN QoS class rule.

The QoS Class Rule - Add/Edit window opens.

STEP 2 Enter the following information:

- **Class:** Choose an existing traffic selector (traffic class) to associate with the policy profile.
- **Queue:** For an outbound traffic policy profile, choose the queue for sending the packets that belongs to the selected traffic class. This option will be disabled for an inbound traffic policy profile.
- **DSCP Marking:** Choose the DSCP remarking value to assign the priority for traffic. For more information, see **Understanding DSCP Values, page 171**.
- **CoS Marking:** For an inbound traffic policy profile, choose the CoS remarking value to assign the priority for inbound traffic. This option will be disabled for an outbound traffic policy profile.
- **Rate-limiting:** Enter the amount of bandwidth limitation in Kbps for the selected traffic class. For example, if the policy profile is applied to inbound traffic, the rate-limiting setting only applies to incoming traffic that belongs to the selected class. The default value is 0 Kbps, which indicates that there is no limit.

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

Mapping WAN QoS Policy Profiles to WAN Interfaces

Use the Policy Profile to Interface Mapping page to apply the WAN QoS policy profiles on the WAN interfaces.

STEP 1 Click **Networking > QoS > WAN QoS > Policy Profile to Interface Mapping**.

The Policy Profile to Interface Mapping window opens.

STEP 2 To edit the policy profile settings associated with a WAN interface, click the **Edit** (pencil) icon.

The Policy Profile to Interface Mapping - Edit window opens.

STEP 3 Enter the following information:

- **Interface:** The name of the WAN interface with which the policy profiles are associated.
- **Inbound Policy Name:** Choose an inbound policy profile for managing inbound traffic through the selected WAN interface.
- **Outbound Policy Name:** Choose an outbound policy profile for managing outbound traffic through the selected WAN interface.

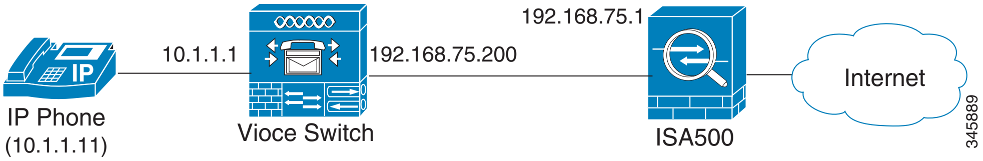
STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

WAN QoS Configuration Example

This section provides a configuration example on setting up WAN QoS to give the voice traffic a higher priority for a phone system or the SPA phones through the security appliance.

Use Case: An IP phone is connected directly to the voice switch behind the security appliance or the LAN port the security appliance. Both voice and data traffic is sent out through the WAN port of the security appliance.



Solution: For the voice traffic from LAN to WAN (outbound voice traffic), make sure that the outbound voice traffic is handled by the highest priority queue (Q1) and other outbound traffic such as data traffic is handled by the lower priority queues (Q2 to Q6). For the voice traffic from WAN to LAN (inbound voice traffic), CoS and DSCP will be remarked so that the voice switch can prioritize the inbound voice traffic by incoming CoS or DSCP.

Perform the following configuration tasks to give the voice traffic a higher priority:

- Go to the Networking > Routing > Static Routing page to add a static routing rule as follows:

Destination Address	voice_phone_ip **NOTE:** In this case, you can manually create an IP address object called "voice_phone_ip" with the IP address 10.1.1.11 by selecting the **Create a new address** option.
IP Address	voice_switch_ip **NOTE:** In this case, you can manually create an IP address object called "voice_switch_ip" with the IP address 192.168.75.200 by selecting the **Create a new address** option.
Metric	1

- Go to the Firewall > NAT > Advanced NAT page to add an advanced NAT rule as follows to permit the voice and data traffic through the WAN port (WAN1) of the security appliance:

Name	voice_traffic_nat
Enable	On
From	Any
To	WAN1
Original Source Address	voice_phone_ip
Translated Source Address	WAN1_IP

- Go to the Networking > QoS > General Settings page to enable WAN QoS on the security appliance.
- Go to the Networking > QoS > WAN QoS > Bandwidth page to specify the upstream bandwidth for the WAN port.
- Configure WAN QoS for the outbound voice traffic. For complete details, see **Configure WAN QoS for Voice Traffic from LAN to WAN, page 164**.

- Configure WAN QoS for the inbound voice traffic. For complete details, see **Configuring WAN QoS for Voice Traffic from WAN to LAN, page 165**.

Configure WAN QoS for Voice Traffic from LAN to WAN

Follow these steps to configure WAN QoS to manage the outbound voice traffic from LAN to WAN:

STEP 1 Go to the Networking > QoS > WAN QoS > Queue Settings page to determine how traffic in queues is handled for the WAN port.

a. Select the **Low Latency Queuing (LLQ)** radio button. LLQ allows delay-sensitive data (such as voice traffic) to be given preferential treatment over other traffic by letting the data to be de-queued and sent first.

a. Enter the amount of bandwidth assigned to Q1. Q1 has the highest priority and is always processed to completion before the lower priority queues.

b. Enter the percentage assigned to other queues (Q2 to Q6) that you want to use.

STEP 2 Go to the Networking > QoS > WAN QoS > Traffic Selector (Classification) page to add two traffic selectors used to classify the outbound voice and data traffic.

a. Add a traffic selector as follows to classify the outbound data traffic:

Class Name	data-outbound-class
VLAN	Default VLAN

b. Add a traffic selector as follows to classify the outbound voice traffic:

Class Name	voice-outbound-class
Source Address	voice_phone_ip

STEP 3 Go to the Networking > QoS > WAN QoS > QoS Policy Profile page to add a class-based QoS policy profile to manage the outbound voice and data traffic through the WAN port.

a. Add a WAN QoS policy profile as follows:

Policy Name	voice-outbound-profile
Apply this policy to	Outbound Traffic

b. Add two QoS class rules to associate the specified traffic classes with the QoS policy profile as follows:

QoS Class Rule 1	
Class	Choose the traffic class called “voice-outbound-class.”
Queue	Choose the highest queue Q1 for the outbound voice traffic.
QoS Class Rules 2	
Class	Choose the traffic class called “data-outbound-class.”
Queue	Choose one queue from Q2 to Q6 for the outbound data traffic.

STEP 4 Go to the Networking > QoS > WAN QoS > Policy Profile to Interface Mapping page to apply this QoS policy profile on the WAN port. In this case, choose the QoS policy profile called “voice-outbound-profile” from the **Outbound Policy Name** drop-down list.

Configuring WAN QoS for Voice Traffic from WAN to LAN

Follow these steps to configure WAN QoS to manage the inbound voice traffic from WAN to LAN:

STEP 1 Go to the Networking > QoS > WAN QoS > Traffic Selector (Classification) page to add a traffic selector as follows to classify the inbound voice traffic:

Class Name	voice-inbound-class
Destination Address	voice_phone_ip

STEP 2 Go to the Networking > QoS > WAN QoS > QoS Policy Profile page to add a class-based QoS policy profile as follows to manage the inbound voice traffic through the WAN port:

Policy Name	voice-inbound-profile
Apply this policy to	Inbound Traffic

QoS Class Rule	Add a QoS class rule with the following settings: ▪ **Class:** Choose the traffic class called "voice-inbound-class." ▪ **DSCP Marking:** Choose the DSCP tag value (such as 46) for the inbound voice traffic depending on the QoS settings on your voice switch. For more information, see **Understanding DSCP Values, page 171**. ▪ **CoS Marking:** Choose the CoS tag value (such as 6) for the inbound voice traffic depending on the QoS settings on your voice switch.

STEP 3 Go to the Networking > QoS > WAN QoS > Policy Profile to Interface Mapping page to apply the inbound QoS policy profile on the WAN port. In this case, choose the QoS policy profile called "voice-inbound-profile" from the **Inbound Policy Name** drop-down list.

Configuring LAN QoS

LAN QoS specifies priority values that can be used to differentiate traffic and give preference to higher-priority traffic, such as telephone calls. Refer to the following topics:

- **Configuring LAN Queue Settings, page 167**
- **Configuring LAN QoS Classification Methods, page 167**
- **Mapping CoS to LAN Queue, page 168**
- **Mapping DSCP to LAN Queue, page 168**
- **Configuring Default CoS, page 169**

Configuring LAN Queue Settings

Use the Queue Settings page to configure whether traffic scheduling on Ethernet interfaces is based on either SP or WRR, or the combination of the two. The security appliance supports four queues for LAN traffic, Q1 to Q4.

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

STEP 2 Specify how to determine LAN traffic in queues.

- **Strict Priority (SP):** Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
- **Weighted Round Robin (WRR):** Indicates that traffic scheduling for the selected queue is based strictly on the WRR weights. If WRR is selected, the predefined weights 8, 4, 2 and 1 are assigned to queues 1, 2, 3 and 4 respectively.
- **SP and WRR:** Integrates the SP and WRR queues. It applies SP to Q1 and WRR to other queues (Q2 to Q4). If you choose SP+WRR, the PQ is assigned to Q1 and the predefined weights 4, 2 and 1 are assigned to Q2, Q3, and Q4 respectively. There is no limit for PQ, indicating that WRR queues may be starved if PQ is always sending traffic greater than the maximum bandwidth of the LAN ports.

STEP 3 If needed, enter the description for each queue in the field in the **Queue Description** column.

STEP 4 Click **Save** to apply your settings.

Configuring LAN QoS Classification Methods

Traffic Classification is used to classify traffic through the LAN interfaces to a given traffic class so that traffic in need of management can be identified.

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

STEP 2 Depending on your networking design, choose either Differentiated Services Code Point (DSCP) or Class of Service (CoS) remarking method for traffic through all LAN interfaces. When you choose DSCP as the classification method, the Mapping CoS to LAN Queue feature will be grayed out. In this case, the mapping relationship between LAN queues and CoS is defined as follows:

LAN Queue	CoS Value
1	6
2	4
3	2
4	0

STEP 3 Click **Save** to apply your settings.

Mapping CoS to LAN Queue

STEP 1 Click **Networking** > **QoS** > **LAN QoS** > **Mapping CoS to Queue**.

STEP 2 Choose the traffic forwarding queue to which the CoS priority tag value is mapped. Four traffic priority queues are supported, where Q4 is the lowest and Q1 is the highest.

STEP 3 Click **Save** to apply your settings.

Mapping DSCP to LAN Queue

STEP 1 Click **Networking** > **QoS** > **LAN QoS** > **Mapping DSCP to Queue**.

STEP 2 Choose the traffic forwarding queue to which the DSCP priority tag value is mapped. Four traffic priority queues are supported, where Q4 is the lowest and Q1 is the highest. For more information, see **Understanding DSCP Values, page 171**.

STEP 3 Click **Save** to apply your settings.

Configuring Default CoS

Use the Default CoS page to configure the default CoS values for incoming packets through each LAN interface. The possible field values are 0 to 7. The default value is 0.

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

STEP 2 Enter the following information:

- **Default CoS:** Choose the default CoS priority tag value for the LAN interfaces, where 0 is the lowest and 7 is the highest.
- **Trust:** Choose **Yes** to keep the CoS tag value for packets through the LAN interfaces, or choose **No** to change the CoS tag value for packets through the LAN interfaces.

STEP 3 Click **Save** to apply your settings.

Configuring Wireless QoS

Wireless QoS controls priority differentiation for data packets in wireless egress direction. Refer to the following topics:

- **Default Wireless QoS Settings, page 169**
- **Configuring Wireless QoS Classification Methods, page 170**
- **Mapping CoS to Wireless Queue, page 171**
- **Mapping DSCP to Wireless Queue, page 171**

Default Wireless QoS Settings

Wireless QoS uses the default queuing method for wireless traffic. Wireless traffic is always trusted. The following tables display the default mapping settings between 802.1p and 802.1e.

802.1p to IEEE 802.11e Mapping

802.1p Priority	802.11e Priority
0	0 (Best Effort Priority)

802.1p Priority	802.11e Priority
1	1 (Background Priority)
2	2 (Background Priority)
3	4 (Video Priority)
4	5 (Video Priority)
5	6 (Voice Priority)
6	7 (Voice Priority)
7	7 (Voice Priority)

IEEE 802.11e to 802.1p Mapping

802.11e Priority	802.1p Priority
0 (Best Effort Priority)	0
1 (Background Priority)	1
2 (Background Priority)	2
3 (Best Effort Priority)	0
4 (Video Priority)	3
5 (Video Priority)	4
6 (Voice Priority)	5
7 (Voice Priority)	6

Configuring Wireless QoS Classification Methods

Traffic Classification is used to classify traffic through the SSIDs to a given traffic class so that traffic in need of management can be identified.

STEP 1 Click **Networking > QoS > Wireless QoS > Classification Methods**.

STEP 2 Depending on your networking design, choose either DSCP or CoS remarking method for traffic through each SSID.

STEP 3 Click **Save** to apply your settings.

Mapping CoS to Wireless Queue

STEP 1 Click **Networking > QoS > Wireless QoS > Mapping CoS to Queue**.

STEP 2 Choose the traffic forwarding queue to which the CoS priority tag value is mapped.

STEP 3 Click **Save** to apply your settings.

Mapping DSCP to Wireless Queue

STEP 1 Click **Networking > QoS > Wireless QoS > Mapping DSCP to Queue**.

STEP 2 Choose the traffic forwarding queue to which the DSCP priority tag value is mapped. For more information, see **Understanding DSCP Values, page 171**.

STEP 3 Click **Save** to apply your settings.

Understanding DSCP Values

DSCP Value	Decimal Value	Meaning
101 110	46	High Priority, Expedited Forwarding (EF)
000 000	0	Best Effort
001 010	10	AF11
001 100	12	AF12
001 110	14	AF13
010 010	18	AF21

DSCP Value	Decimal Value	Meaning
010 100	20	AF22
010 110	22	AF23
011 010	26	AF31
011 100	28	AF32
011 110	30	AF33
100 010	34	AF41
100 100	36	AF42
100 110	38	AF43

Configuring IGMP

Internet Group Management Protocol (IGMP) is a communication protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP can be used for online streaming video and gaming, and can allow more efficient use of resources when supporting these types of applications.

IGMP Proxy enables hosts that are not directly connected to a downstream router to join a multicast group sourced from an upstream network. IGMP Snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it. IGMP Snooping runs on IGMP Version 3 that is backward compatible with the previous versions.

NOTE By default, multicast traffic from Any zone to Any zone is blocked by the firewall. When you enable IGMP Proxy and want to receive multicast packets from WAN to LAN, you must first uncheck **Block Multicast Packets** in the Firewall > Attack Protection page, and then create a firewall rule to permit multicast traffic from WAN to LAN. For information on configuring firewall rules to allow or deny multicast traffic, see Configuring a Firewall Rule to Allow Multicast Traffic, page 259.

STEP 1 Click **Networking > IGMP**.

The IGMP window opens.

STEP 2 Enter the following information:

- **IGMP Proxy:** Click **On** to enable IGMP Proxy so that the security appliance can act as a proxy for all IGMP requests and communicate with the IGMP servers of the ISP, or click **Off** to disable it.
- **IGMP Version:** Choose either IGMP Version 1 and 2 or IGMP Version 3.
  - **IGMP Version 1:** Hosts can join multicast groups. There are no leave messages. Routers use a time-out based mechanism to discover the groups that are of no interest to the members.
  - **IGMP Version 2:** Leave messages are added to the protocol. This allows group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.
  - **IGMP Version 3:** Major revision of the protocol. It allows hosts to specify the lists of hosts from which they want to receive traffic. Traffic from other hosts is blocked inside the network. It also allows hosts to block packets inside the network that come from sources sending unwanted traffic.
- **IGMP Snooping:** Snooping streamlines multicast traffic handling for VLANs. By examining (snooping) IGMP membership report messages from interested hosts, multicast traffic is limited to the subset of VLAN interfaces on which the hosts reside. IGMP snooping can reduce bandwidth consumption to avoid flooding the entire VLAN. Click **On** to enable IGMP snooping, or click **Off** to disable it.

STEP 3 Click **Save** to apply your settings.

Configuring VRRP

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol for LAN access device. VRRP configures a groups of routers (include a master router and several backup routers) as a virtual router.

STEP 1 Click **Networking > VRRP**.

The VRRP window opens.

STEP 2 Check the box next to **Enable Virtual Router Redundancy Protocol (VRRP)** to enable VRRP, or uncheck this box to disable it.

STEP 3 If you enable VRRP, enter the following information:

- **Interface:** The default port of the master virtual router (your security appliance).
- **Source IP:** The source IP address of the master virtual router.

  NOTE: If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a master virtual router.
- **VRID:** The ID of the master virtual router. A virtual router has a unique ID that will be represented as the unique virtual MAC address. Enter a value from 1 to 255.
- **Priority:** The priority of the master virtual router. Priority determines the role that each VRRP router plays and what happens if the master virtual router fails. Enter a value from 1 to 254.
- **Advertisement Interval:** Specify the interval in seconds between successive advertisements by the master virtual router in a VRRP group. By default, the advertisements are sent every one second. The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

  NOTE: All routers in a VRRP group must use the same advertisement interval value. If the interval values are not same, the routers in the VRRP group will not communicate with each other and any mis-configured router will change its state to master.
- **Verify:** Click **On** to enable the authentication, or click **Off** to disable it. The security appliance will ignore incoming VRRP packets from routers that do not have the same authentication configuration for a VRRP group. VRRP supports the plaintext and IPsec-AH authentication schemes. Choose either Pass or AH as the authentication scheme and specify the settings.
- **Virtual IP Address:** Enter the virtual IP address used for all backup virtual routers in the same group.
- **Status:** Displays the status of VRRP verification.

STEP 4 Click **Save** to apply your settings.

Address Management

Use the Address Management page to manage the address and address group objects. The security appliance is configured with a long list of common address objects so that you can use to configure firewall rules, port forwarding rules, or other features. See Default Address Objects, page 478.

Refer to the following topics:

- **Configuring Addresses, page 175**
- **Configuring Address Groups, page 176**

Configuring Addresses

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

STEP 2 In the **Address Objects** area, click **Add Address** to add a new address object.

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**. The default address objects cannot be edited and deleted.

The Address Object - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the address object.
- **Type:** Specify the address type and enter the corresponding information.
  - **Host:** Defines a single host by its IP address. The netmask for a Host address object will automatically be set to 32-bit (255.255.255.255) to identify it as a single host. If you choose Host, enter the IP address of the host in the **IP Address** field.
  - **Range:** Defines a range of contiguous IP addresses. No netmask is associated with the Range address object, but internal logic generally treats each member of the specified range as a 32-bit masked host object. If you choose Range, enter the starting IP address in the **Starting IP Address** field and the ending IP address in the **Ending IP Address** field.

- **Network:** Network address object like the Range object comprises multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network address objects must be defined by the network's address and a corresponding netmask. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable. If you choose Network, enter the subnet IP address in the **IP Address** field and the broadcast address in the **Netmask** field.
- **MAC:** Identifies a host by its hardware address or MAC (Media Access Control) address. MAC addresses are uniquely assigned to wired or wireless networking devices by their hardware manufacturers. MAC addresses are 48-bit values that are expressed in 6 byte hex-notation. If you choose MAC, enter the MAC address in the **MAC** field.

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

STEP 5 Click **Save** to apply your settings.

Configuring Address Groups

An address group object combines with multiple address objects. The security appliance supports up to 64 address group objects. An address group can include up to 100 address members.

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

STEP 2 In the **Address Groups** area, click **Add Group** to add a new address group object.

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**.

The Address Group - Add/Edit window opens.

STEP 3 Enter the name for the address group object in the **Group Name** field.

STEP 4 To add the address objects to the group, select the address objects from the left list and click the right arrow.

STEP 5 To remove the address objects from the group, select the address objects from the right list and click the left arrow.

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

STEP 7 Click **Save** to apply your settings.

Service Management

Use the Service Management page to maintain the service or service group objects. The security appliance is configured with a long list of standard services so that you can use to configure the firewall rules, port forwarding rules, or other features. See Default Service Objects, page 474.

Refer to the following topics:

- **Configuring Services, page 177**
- **Configuring Service Groups, page 178**

Configuring Services

If you need to configure a feature for a custom service that is not in the standard list, you must first define the service object.

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

STEP 2 In the **Services** area, click **Add Service** to add a new 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**. The default services cannot be deleted. Only the port range for the default services can be modified.

The Service Object - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the service.
- **Protocol:** Specify the protocol and port range for the service:
  - **IP:** Uses the predefined IP type. If you choose this option, enter the protocol number in the **IP Type** field.

- **ICMP:** Internet Control Message Protocol (ICMP) is a TCP/IP protocol used to send error and control messages. If you choose this option, enter the ICMP type in the **ICMP Type** field.
- **TCP:** Transmission Control Protocol (TCP) is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety. If you choose this option, enter the starting port number in the **Port Range Start** field and the ending port number in the **Port Range End** field.
- **UDP:** User Datagram Protocol (UDP) is a protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required. If you choose this option, enter the starting port number in the **Port Range Start** field and the ending port number in the **Port Range End** field.
- **Both (TCP/UDP):** If you choose this option, enter the starting port number in the **Port Range Start** field and the ending port number in the **Port Range End** field.

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

STEP 5 Click **Save** to apply your settings.

Configuring Service Groups

Services that apply to common applications are grouped as a service group object. The service group is treated as a single service. The security appliance supports up to 64 service groups. A service group can include up to 64 service members.

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

STEP 2 In the **Service Groups** area, click **Add Group** to add a new service 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**.

The Service Group - Add/Edit window opens.

STEP 3 Enter the name for the service group in the **Group Name** field.

STEP 4 To add the services to the group, select the services from the left list and click the right arrow.

STEP 5 To remove the services from the group, select the services from the right list and click the left arrow.

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

STEP 7 Click **Save** to apply your settings.

Configuring Captive Portal

You may want to direct users to a web portal before they can access the Internet through the security appliance. To achieve this goal, you can enable Captive Portal on a wireless network, a VLAN, or a DMZ.

When a user in a Captive Portal user group attempts to access the Internet via a web browser, a portal page appears. You can require a log in or the entry of payment information, for example, and you can set up the portal page to display information, usage guidelines, warning messages, and so on. After successfully logging in, paying, or acknowledging your messages, the user can use other applications on the PC to communicate with the network.

In addition to the portal options mentioned above, additional options make it easy to adapt the Captive Portal feature to your needs:

- You can specify certain domains that users can access without going through the portal.
- The portal page can be stored locally on the ISA500 device or on an external web server that you specify.

Requirements

This feature is compatible with these browsers:

- Internet Explorer (v 8.0 or above)
- Firefox (v 9.0 or above)
- Google Chrome
- Safari

A computer accessing the Captive Portal must have one of these operating systems:

- Windows 7
- Windows XP
- Mac OS

Captive Portal also can be used from a mobile device with one of these operating systems:

- iOS (iPhone, iPad)
- Android

Before You Begin

Before you configure your portal, you may need to configure VLANs, SSIDs, and users. Read the following information to determine what steps may be needed to achieve your goals.

VLAN Setup

No special VLAN configuration is required for a Captive Portal, but you may want to consider the points below before proceeding. To configure VLANs, use the Networking > VLAN page..

- Each SSID is associated with a VLAN. You can use the pre-configured VLANs (DEFAULT, GUEST, and VOICE) or add a custom VLAN.
- You may want to associate a VLAN, such as the GUEST VLAN, with a security zone so that you can configure appropriate security policies. For example, you can apply URL filtering policies to the zone to prevent access to certain types of websites.
- A Captive Portal must be associated either with a single SSID or with a VLAN. If you want to enable a portal for users of multiple SSIDs, you will need to assign them all to the same VLAN. You can use a pre-configured VLAN or can create a VLAN for this purpose.

Wireless Setup

For a Captive Portal on the wireless network, you must enable the wireless radio and at least one SSID before you can enable a Captive Portal. To configure these settings, use the Wireless > Basic Settings page. .

- Enable the wireless radio.
- Enable the SSID(s) that you want to use for the portal.
- If you created a special VLAN for use with your Captive Portal, assign it to the SSID(s) that you want to use for the portal.

User Authentication

If you want to require user authentication for your portal, the security appliance can authenticate the users by using the local database and an external AAA server (such as RADIUS, AD, and LDAP). The authentication method is derived from the user authentication settings that you specified in the Users > User Authentication page. See Configuring User Authentication Settings, page 393.

For the local database option, you need to set up a User Group with the Captive Portal service enabled, and add the users' names and passwords. .

Configuring a Captive Portal

You configure this feature separately for the wireless network (**Wireless > Captive Portal**) and for the wired network (**Networking > Captive Portal**).

STEP 1 **Enable Captive Portal:** Click **On** to enable the Captive Portal feature.

STEP 2 **Apply On:** Choose the SSID, VLAN, or DMZ interface on which to apply the Captive Portal settings.

STEP 3 **Web Authentication Type:** Choose one of the following methods for web authentication. The security appliance can authenticate the users by using the local database and external AAA server (such as RADIUS, AD, and LDAP). The authentication method is derived from the user authentication settings that you specified in the Users > User Authentication page.

- **Internal:** Uses the default HotSpot Login page and requires a login.

- **Internal, no auth with accept button:** Uses the default HotSpot Login page and does not require a login. A user simply clicks the **Accept** button to access the Internet.
- **External:** Uses a custom HotSpot Login page on the specified external web server and requires a login.
- **External, no auth with accept button:** Uses a custom HotSpot Login page on the specified external web server and does not require a login. A user simply clicks the **Accept** button to access the Internet.

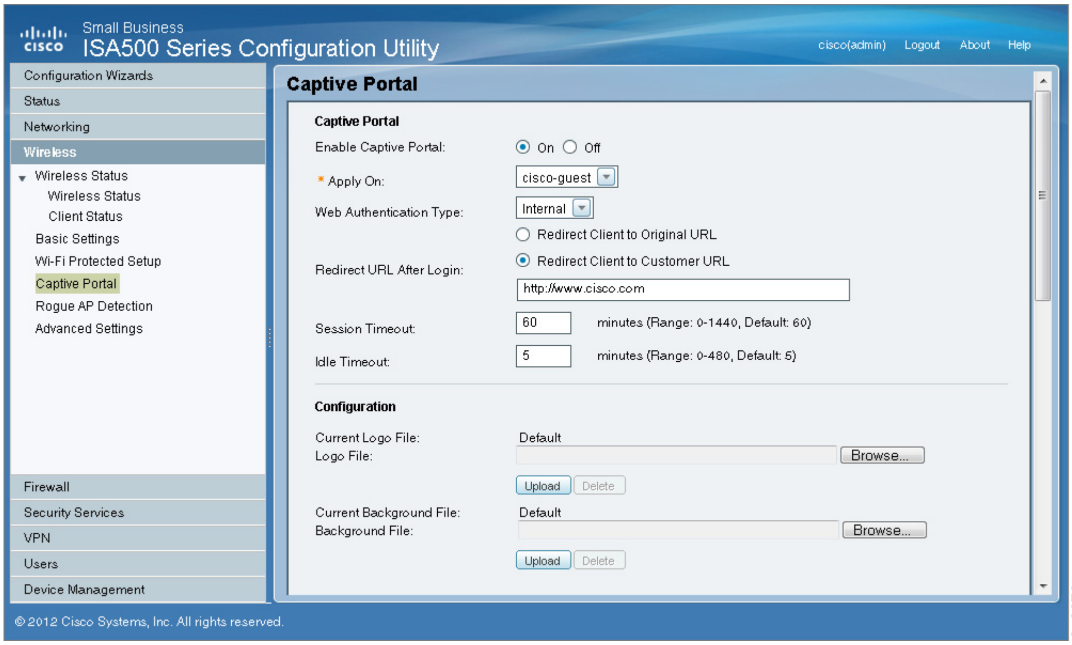
Note: If you chose Internal or External, you will need to use the Users > Users and Groups page to create a User Group with Captive Portal service enabled, and to add users to the group.

STEP 4 **Redirected URL After Login:** Choose one of the following options to determine what happens after a user leaves the portal page:

- **Redirect Client to Customer URL:** Directs the users to a particular URL (such as the URL for your company). If you choose this option, enter the desired URL in the field, including http:// or https://.
- **Redirect Client to Original URL:** Directs the users to the URL that they were trying to access originally.

STEP 5 Configure the timeout settings, or keep the default values.

- **Session Timeout:** Enter the maximum number of minutes that a wireless session can remain connected. After the timeout period elapses, the session will be terminated. Enter 0 to allow a user to remain connected without any limit. The default value is 60 minutes.
- **Idle Timeout:** Enter the maximum number of minutes that a wireless session can be idle. After the timeout period elapses, an idle session will be terminated. The default value is 5 minutes.



Captive Portal

Captive Portal

Enable Captive Portal: ● On ○ Off

* Apply On: cisco-guest

Web Authentication Type: Internal

Redirect URL After Login: ○ Redirect Client to Original URL ● Redirect Client to Customer URL http://www.cisco.com

Session Timeout: 60 minutes (Range: 0-1440, Default: 60)

Idle Timeout: 5 minutes (Range: 0-480, Default: 5)

Configuration

Current Logo File: Default

Logo File:

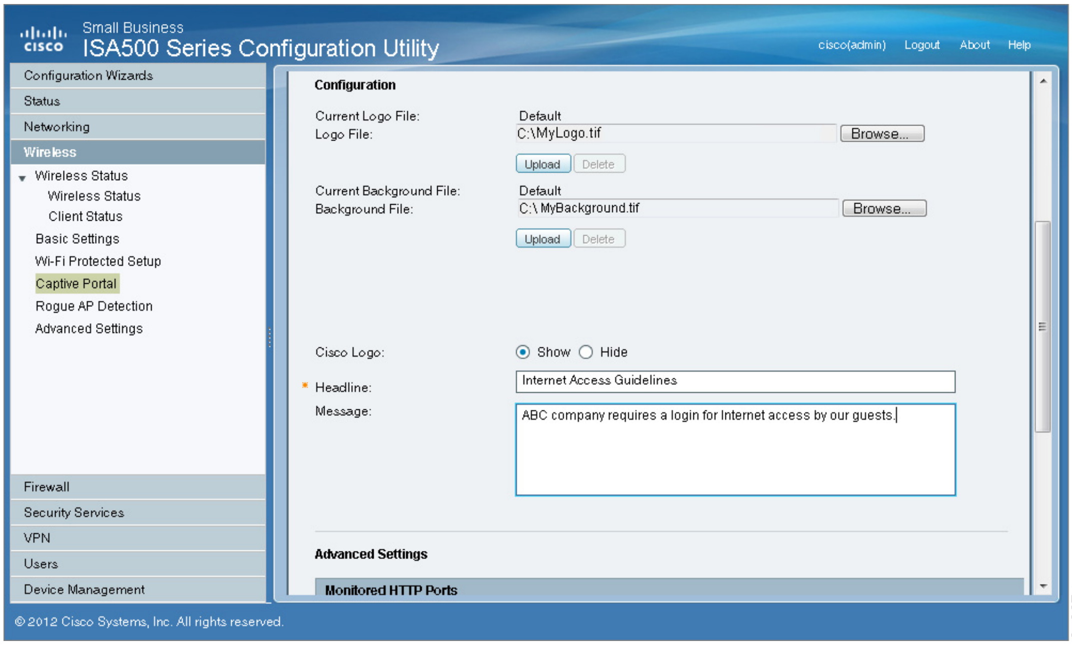
Current Background File: Default

Background File:

STEP 6 If you chose **Internal** or **Internal, no auth with accept button**, set up the default HotSpot Login page:

- **Logo File:** You can import an image, such as your corporate logo, to display on the login page. Click **Browse** to locate and select an image file from your local PC and then click **Upload**. To delete the loaded file, click **Delete**.
- **Background File:** You can import an image to display as the background for the login page. Click **Browse** to locate and select an image file (jpg, gif, or png) from your local PC and then click **Upload**. To delete the loaded file, click **Delete**.

  NOTE: When uploading a file, select a bmp, jpg, gif, or png file of 200KB or less. The Current Logo File field displays the filename of the file that is in use, or *Default* if no file has been uploaded for this purpose.
- **Cisco Logo:** If you want to hide the Cisco logo that appears on the login page, choose **Hide**. Otherwise, choose **Show**.
- **Headline:** If you want to create your own headline on the login page, enter the desired text in this field.
- **Message:** If you want to create your own message on the login page, enter the desired text in this field.



Configuration

Current Logo File: Default
Logo File: C:\MyLogo.tif

Current Background File: Default
Background File: C:\ MyBackground.tif

Cisco Logo: ● Show ○ Hide

* Headline: Internet Access Guidelines

Message: ABC company requires a login for Internet access by our guests.

Advanced Settings

Monitored HTTP Ports

STEP 7 If you chose **External** or **External, no auth with accept button**, specify these settings for your external portal page:

- **Authentication Web Server:** Enter the full URL of the external web server (including https://), for example https://172.24.10.10/cgi-bin/PortalLogin.cgi.
- **Authentication Web Key:** Enter the key used to protect the username and password that the external web server sends to the security appliance for authentication.

STEP 8 If you want to use the portal for HTTP requests through other ports besides the default 80 and 443, add the ports in the **Advanced Settings > Monitored HTTP Ports** area.

NOTE: Captive Portal only monitors HTTPS requests through the port 443.

a. Click **Add**.

b. Enter the port number in the **Port** field.

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

STEP 9 If you want to bypass the portal for certain IP addresses, add them in the **Advanced Settings > Open Domains** area.

a. Click **Add**.

b. Enter the IP address or domain name in the **Domain** field.

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

STEP 10 Click **Save** to apply your settings.

Troubleshooting

Problem 1: User is not redirected to portal page when internal web authentication type is chosen.

Solution: Either of the following could resolve the problem:

- Check the device is connected to Captive Portals wireless network and the IP address is assigned to the device.
- Check Web Authentication Type is selected as Internal or Internal, no auth with accept button.
- Check the TCP ports on which HTTP requests are sent are added under Monitored HTTP Ports under Advanced Settings on Captive Portal page.

Problem 2: User is not redirected to portal page when internal web authentication type is chosen.

Solution: Either of the following could resolve the problem:

- Check the device is connected to Captive Portals wireless network and the IP address is assigned to the device. .
- Check Web Authentication Type is selected as External or External, no auth with accept button.
- Check the TCP ports on which HTTP requests are sent are added under Monitored HTTP Ports under Advanced Settings on Captive Portal page.
- Check the connectivity of Web-server from ISA500.
- Web-server should be able to accessed by the devices on the Captive Portal wireless network. In other words, the firewall rules associated with

the VLAN to which Captive Portal users join should be able to access the web-server.

- Check if the web-server has any issues.

Using External Web-Hosted CGI Scripts

Following is a CGI script which asks for the authentication information of a user.

The secret string programmed in the **uamsecret** variable should be configured as Authentication Web Key on the Captive portal page. Replace the **MySMB** string in the following section with your company name.

```
# !/usr/bin/perl
# chilli - ChilliSpot.org. A Wireless LAN Access Point Controller
# Copyright (C) 2003, 2004 Mondru AB.
#
# The contents of this file may be used under the terms of the GNU
# General Public License Version 2, provided that the above copyright
# notice and this permission notice is included in all copies or
# substantial portions of the software.

# Redirects from ChilliSpot daemon:
#
# Redirection when not yet or already authenticated
#   notyet:  ChilliSpot daemon redirects to login page.
#   already: ChilliSpot daemon redirects to success status page.
#
# Response to login:
#   already: Attempt to login when already logged in.
#   failed:  Login failed
#   success: Login succeded
#
# logoff:  Response to a logout


# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
$uamsecret = "ht2eb8ej6s4et3rg1ulp";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1; [1]

# Our own path
$loginpath = $ENV{'SCRIPT_URL'};

use Digest::MD5  qw(md5 md5_hex md5_base64);

# Make sure that the form parameters are clean
```

```
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$| = 1;
if ($ENV{'CONTENT_LENGTH'}) {
    read (STDIN, $_, $ENV{'CONTENT_LENGTH'});
}
s/[^$OK_CHARS]/_/go;
$input = $_;


# Make sure that the get query parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$_ = $query=$ENV{QUERY_STRING};
s/[^$OK_CHARS]/_/go;
$query = $_;


# If she did not use https tell her that it was wrong.
if (!($ENV{HTTPS} =~ /^on$/)) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>[7.1]
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>[7.2]
  <center>
    Login must use encrypted connection.
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>102</ResponseCode>
<ReplyMessage>Login must use encrypted connection</ReplyMessage>[7.3]
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


#Read form parameters which we care about
@array = split('&',$input);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^UserName$/) { $username = $array2[1]; }
    if ($array2[0] =~ /^Password$/) { $password = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^button$/) { $button = $array2[1]; }
    if ($array2[0] =~ /^logout$/) { $logout = $array2[1]; }
    if ($array2[0] =~ /^prelogin$/) { $prelogin = $array2[1]; }
    if ($array2[0] =~ /^res$/) { $res = $array2[1]; }
    if ($array2[0] =~ /^uamip$/) { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/) { $uamport = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}

#Read query parameters which we care about
@array = split('&',$query);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^res$/)       { $res = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^uamip$/)     { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/)   { $uamport = $array2[1]; }
    if ($array2[0] =~ /^reply$/)     { $reply = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}


$reply =~ s/\+/ /g;
$reply =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$userurldecode = $userurl;
$userurldecode =~ s/\+/ /g;
$userurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$redirurldecode = $redirurl;
$redirurldecode =~ s/\+/ /g;
$redirurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$password =~ s/\+/ /g;
$password =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

# If attempt to login
if ($button =~ /^Login$/) {
    $hexchal  = pack "H32", $challenge;
    if (defined $uamsecret) {
   $newchal  = md5($hexchal, $uamsecret);
    }
    else {
   $newchal  = $hexchal;
    }
    $response = md5_hex("\0", $password, $newchal);
    $pappassword = unpack "H32", ($password ^ $newchal);
#sleep 5;
print "Content-type: text/html\n\n";
print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&password=
$pappassword&userurl=$userurl\">";
    } else {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&response=$response&userurl=
$userurl\">";
    }
print "</head>
<body bgColor = '#c0d8f4'>";
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&password=$pappassword</LoginResultsURL>";
    } else {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&response=$response&userurl=$userurl</LoginResultsURL>";
    }
print "</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


# Default: It was not a form request
$result = 0;
```

```
# If login successful
if ($res =~ /^success$/) {
    $result = 1;
}

# If login failed
if ($res =~ /^failed$/) {
    $result = 2;
}

# If logout successful
if ($res =~ /^logoff$/) {
    $result = 3;
}

# If tried to login while already logged in
if ($res =~ /^already$/) {
    $result = 4;
}

# If not logged in yet
if ($res =~ /^notyet$/) {
    $result = 5;
}

# If login from smart client
if ($res =~ /^smartclient$/) {
    $result = 6;
}

# If requested a logging in pop up window
if ($res =~ /^popup1$/) {
    $result = 11;
}

# If requested a success pop up window
if ($res =~ /^popup2$/) {
    $result = 12;
}

# If requested a logout pop up window
if ($res =~ /^popup3$/) {
    $result = 13;
}


# Otherwise it was not a form request
# Send out an error message
if ($result == 0) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must be performed through MySMB daemon.
  </center>
</body>
</html>
";
    exit(0);
}

#Generate the output
print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>[2.1]
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
  <SCRIPT LANGUAGE=\"JavaScript\">
    var blur = 0;
    var starttime = new Date();
    var startclock = starttime.getTime();
    var mytimeleft = 0;

    function doTime() {
      window.setTimeout( \"doTime()\", 1000 );
      t = new Date();
      time = Math.round((t.getTime() - starttime.getTime())/1000);
      if (mytimeleft) {
        time = mytimeleft - time;
        if (time <= 0) {
          window.location = \"$loginpath?res=popup3&uamip=$uamip&uamport=
$uamport\";
        }
      }
      if (time < 0) time = 0;
      hours = (time - (time % 3600)) / 3600;
      time = time - (hours * 3600);
      mins = (time - (time % 60)) / 60;
      secs = time - (mins * 60);
      if (hours < 10) hours = \"0\" + hours;
      if (mins < 10) mins = \"0\" + mins;
      if (secs < 10) secs = \"0\" + secs;
      title = \"Online time: \" + hours + \":\" + mins + \":\" + secs;
      if (mytimeleft) {
        title = \"Remaining time: \" + hours + \":\" + mins + \":\" + secs;
      }
      if(document.all || document.getElementById){
         document.title = title;
      }
      else {
        self.status = title;
      }
    }

    function popUp(URL) {
      if (self.name != \"chillispot_popup\") {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
    }

    function doOnLoad(result, URL, userurl, redirurl, timeleft) {
      if (timeleft) {
        mytimeleft = timeleft;
      }
      if ((result == 1) && (self.name == \"chillispot_popup\")) {
        doTime();
      }
      if ((result == 1) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
      if ((result == 2) || result == 5) {
        document.form1.UserName.focus()
      }
      if ((result == 2) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open('', 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
400,height=200');
        chillispot_popup.close();
      }
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        doTime();
        if (redirurl) {
          opener.location = redirurl;
        }
        else if (userurl) {
          opener.location = userurl;
        }
        else if (opener.home) {
          opener.home();
        }
        else {
          opener.location = \"about:home\";
        }
        self.focus();
        blur = 0;
      }
      if ((result == 13) && (self.name == \"chillispot_popup\")) {
        self.focus();
        blur = 1;
      }
    }
    function doOnBlur(result) {
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        if (blur == 0) {
          blur = 1;
          self.focus();
        }
      }
    }
  </script>
</head>
<body onLoad=\"javascript:doOnLoad($result, '$loginpath?res=popup2&uamip=
$uamip&uamport=$uamport&userurl=$userurl&redirurl=$redirurl&timeleft=
$timeleft','$userurldecode', '$redirurldecode', '$timeleft')\" onBlur =
\"javascript:doOnBlur($result)\" bgColor = '#c0d8f4'>";


#      if (!window.opener) {
#        document.bgColor = '#c0d8f4';
#      }

#print "THE INPUT: $input";
#foreach $key (sort (keys %ENV)) {
#  print $key, ' = ', $ENV{$key}, "<br>\n";
#}

if ($result == 2) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>";[6.1]
    if ($reply) {
   print "<center> $reply </BR></BR></center>";
    }
}

if ($result == 5) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login</h1>";[2.2]
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurldecode\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\" style=\"width:
217px;\">
    <tbody>
      <tr>
        <td align=\"right\">Username:</td>[2.3]
        <td><input STYLE=\"font-family: Arial\" type=\"text\" name=
\"UserName\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
```

```
        <td align=\"right\">Password:</td>[2.4]
        <td><input STYLE=\"font-family: Arial\" type=\"password\" name=
\"Password\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input type=
\"submit\" name=\"button\" value=\"Login\"[2.5] onClick=
\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}

if ($result == 1) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>";[8.1]

  if ($reply) {
      print "<center> $reply </BR></BR></center>";
  }

  print "
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>[8.2]
  </center>
</body>
</html>";
}

if (($result == 4) || ($result == 12)) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>[4.1]
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>[4.2]
  </center>
</body>
</html>";
}


if ($result == 11) {
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>[3.1]";
  print "
  <center>
    Please wait...... [3.2]
  </center>
</body>
</html>";
}
```

```
if (($result == 3) || ($result == 13)) {
    print "
  <h1 style=\"text-align: center;\">Logged out from MySMB</h1>[5.1]
  <center>
    <a href=\"http://$uamip:$uamport/prelogin\">Login</a>[5.2]
  </center>
</body>
</html>";
}


exit(0);
```

CGI Source Code Example: No Authentication and Accept Button

Following is a CGI script which presents a Accept button on the portal page.

The secret string programmed in **`uamsecret`** variable should be configured as Authentication Web Key on the Captive portal page. Replace the **MySMB** string in the following section with your company name.

```
#!/usr/bin/perl

# chilli - ChilliSpot.org. A Wireless LAN Access Point Controller
# Copyright (C) 2003, 2004 Mondru AB.
#
# The contents of this file may be used under the terms of the GNU
# General Public License Version 2, provided that the above copyright
# notice and this permission notice is included in all copies or
# substantial portions of the software.

# Redirects from ChilliSpot daemon:
#
# Redirection when not yet or already authenticated
#   notyet:  ChilliSpot daemon redirects to login page.
#   already: ChilliSpot daemon redirects to success status page.
#
# Response to login:
#   already: Attempt to login when already logged in.
#   failed:  Login failed
#   success: Login succeded
#
# logoff:  Response to a logout


# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
#$uamsecret = "ht2eb8ej6s4et3rg1ulp";
```

```
$uamsecret = "gemteksmb";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;

# Our own path
$loginpath = $ENV{'SCRIPT_URL'};

use Digest::MD5  qw(md5 md5_hex md5_base64);

# Make sure that the form parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$| = 1;
if ($ENV{'CONTENT_LENGTH'}) {
    read (STDIN, $_, $ENV{'CONTENT_LENGTH'});
}
s/[^$OK_CHARS]/_/go;
$input = $_;


# Make sure that the get query parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$_ = $query=$ENV{QUERY_STRING};
s/[^$OK_CHARS]/_/go;
$query = $_;


# If she did not use https tell her that it was wrong.
if (!($ENV{HTTPS} =~ /^on$/)) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must use encrypted connection.
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>102</ResponseCode>
<ReplyMessage>Login must use encrypted connection</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


#Read form parameters which we care about
@array = split('&',$input);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^UserName$/) { $username = $array2[1]; }
    if ($array2[0] =~ /^Password$/) { $password = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^button$/) { $button = $array2[1]; }
    if ($array2[0] =~ /^logout$/) { $logout = $array2[1]; }
    if ($array2[0] =~ /^prelogin$/) { $prelogin = $array2[1]; }
    if ($array2[0] =~ /^res$/) { $res = $array2[1]; }
    if ($array2[0] =~ /^uamip$/) { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/) { $uamport = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}

#Read query parameters which we care about
@array = split('&',$query);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^res$/)       { $res = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^uamip$/)     { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/)   { $uamport = $array2[1]; }
    if ($array2[0] =~ /^reply$/)     { $reply = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}


$reply =~ s/\+/ /g;
$reply =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$userurldecode = $userurl;
$userurldecode =~ s/\+/ /g;
$userurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$redirurldecode = $redirurl;
$redirurldecode =~ s/\+/ /g;
$redirurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$password =~ s/\+/ /g;
```

```
$password =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

# If attempt to login
if ($button =~ /^Accept$/) {
    $hexchal  = pack "H32", $challenge;
    if (defined $uamsecret) {
   $newchal  = md5($hexchal, $uamsecret);
    }
    else {
   $newchal  = $hexchal;
    }
    $response = md5_hex("\0", $password, $newchal);
    $pappassword = unpack "H32", ($password ^ $newchal);
#sleep 5;
print "Content-type: text/html\n\n";
print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&password=
$pappassword&userurl=$userurl\">";
    } else {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&response=$response&userurl=
$userurl\">";
    }
print "</head>
<body bgColor = '#c0d8f4'>";
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&password=$pappassword</LoginResultsURL>";
    } else {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&response=$response&userurl=$userurl</LoginResultsURL>";
    }
```

```
print "</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


# Default: It was not a form request
$result = 0;

# If login successful
if ($res =~ /^success$/) {
    $result = 1;
}

# If login failed
if ($res =~ /^failed$/) {
    $result = 2;
}

# If logout successful
if ($res =~ /^logoff$/) {
    $result = 3;
}

# If tried to login while already logged in
if ($res =~ /^already$/) {
    $result = 4;
}

# If not logged in yet
if ($res =~ /^notyet$/) {
    $result = 5;
}

# If login from smart client
if ($res =~ /^smartclient$/) {
    $result = 6;
}

# If requested a logging in pop up window
if ($res =~ /^popup1$/) {
    $result = 11;
}

# If requested a success pop up window
if ($res =~ /^popup2$/) {
    $result = 12;
}

# If requested a logout pop up window
if ($res =~ /^popup3$/) {
    $result = 13;
```

```
}


# Otherwise it was not a form request
# Send out an error message
if ($result == 0) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must be performed through MySMB daemon.
  </center>
</body>
</html>
";
    exit(0);
}

#Generate the output
print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
  <SCRIPT LANGUAGE=\"JavaScript\">
    var blur = 0;
    var starttime = new Date();
    var startclock = starttime.getTime();
    var mytimeleft = 0;

    function doTime() {
      window.setTimeout( \"doTime()\", 1000 );
      t = new Date();
      time = Math.round((t.getTime() - starttime.getTime())/1000);
      if (mytimeleft) {
        time = mytimeleft - time;
        if (time <= 0) {
          window.location = \"$loginpath?res=popup3&uamip=$uamip&uamport=
$uamport\";
        }
      }
      if (time < 0) time = 0;
      hours = (time - (time % 3600)) / 3600;
      time = time - (hours * 3600);
      mins = (time - (time % 60)) / 60;
      secs = time - (mins * 60);
      if (hours < 10) hours = \"0\" + hours;
      if (mins < 10) mins = \"0\" + mins;
      if (secs < 10) secs = \"0\" + secs;
      title = \"Online time: \" + hours + \":\" + mins + \":\" + secs;
      if (mytimeleft) {
        title = \"Remaining time: \" + hours + \":\" + mins + \":\" + secs;
      }
      if(document.all || document.getElementById){
         document.title = title;
      }
      else {
        self.status = title;
      }
    }

    function popUp(URL) {
      if (self.name != \"chillispot_popup\") {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
    }

    function doOnLoad(result, URL, userurl, redirurl, timeleft) {
   if (timeleft) {
        mytimeleft = timeleft;
      }
      if ((result == 1) && (self.name == \"chillispot_popup\")) {
        doTime();
      }
      if ((result == 1) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
      if ((result == 2) || result == 5) {
        //document.form1.UserName.focus()
      }
      if ((result == 2) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open('', 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
400,height=200');
        chillispot_popup.close();
      }
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        doTime();
        if (redirurl) {
          opener.location = redirurl;
        }
        else if (userurl) {
          opener.location = userurl;
        }
        else if (opener.home) {
          opener.home();
        }
        else {
          opener.location = \"about:home\";
        }
        self.focus();
        blur = 0;
      }
      if ((result == 13) && (self.name == \"chillispot_popup\")) {
        self.focus();
        blur = 1;
      }
    }

    function doOnBlur(result) {
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        if (blur == 0) {
          blur = 1;
          self.focus();
        }
      }
    }
  </script>
</head>
<body onLoad=\"javascript:doOnLoad($result, '$loginpath?res=popup2&uamip=
$uamip&uamport=$uamport&userurl=$userurl&redirurl=$redirurl&timeleft=
$timeleft','$userurldecode', '$redirurldecode', '$timeleft')\" onBlur =
\"javascript:doOnBlur($result)\" bgColor = '#c0d8f4'>";


#      if (!window.opener) {
#        document.bgColor = '#c0d8f4';
#      }

#print "THE INPUT: $input";
#foreach $key (sort (keys %ENV)) {
#  print $key, ' = ', $ENV{$key}, "<br>\n";
#}

if ($result == 2) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>";
    if ($reply) {
   print "<center> $reply </BR></BR></center>";
    }
}

if ($result == 5) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login</h1>";
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurldecode\">
  <INPUT TYPE=\"hidden\" NAME=\"UserName\" VALUE=\"\">
  <INPUT TYPE=\"hidden\" NAME=\"Password\" VALUE=\"\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\" style=\"width:
217px;\">
    <tbody>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input type=
\"submit\" name=\"button\" value=\"Accept\" onClick=
\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}

if ($result == 1) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>";

  if ($reply) {
      print "<center> $reply </BR></BR></center>";
  }

  print "
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>
  </center>
</body>
</html>";
}

if (($result == 4) || ($result == 12)) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>
  </center>
</body>
</html>";
}


if ($result == 11) {
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
```

```
</body>
</html>";
}


if (($result == 3) || ($result == 13)) {
    print "
  <h1 style=\"text-align: center;\">Logged out from MySMB</h1>
  <center>
    <a href=\"http://$uamip:$uamport/prelogin\">Login</a>
  </center>
</body>
</html>";
}


exit(0);
```

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/isa500software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Documentation	
Product Documentation	www.cisco.com/go/isa500resources
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

78-21182-01