6

Firewall

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

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

Configuring Firewall Rules to Control Inbound and Outbound Traffic

The zone-based firewall can permit or deny inbound or outbound traffic based on the zone, service, source and destination address, and schedule.

Refer to the following topics:

About Security Zones

A security zone is a group of interfaces to which a security policy can be applied to control traffic between zones. For ease of deployment, the Cisco ISA500 has several predefined zones with default security settings to protect your network. You can create additional zones as needed.

Each zone has an associated security level. The security level represents the level of trust, from low (0) to high (100). Default firewall rules are created for all predefined zones and your new zones, based on these security levels. For example, by default all traffic from the LAN zone (with a Trusted security level) to the WAN zone (with an Untrusted security level) is allowed but traffic from the WAN (Untrusted) zone to the LAN (Trusted) zone is blocked. You can create and modify firewall rules to specify the permit or block action for specified services, source and destination addresses, and schedules.

To learn more, see the **Security Levels and Predefined Zones** table.

Security Levels and Predefined Zones

Security Level	Description	Predefined Zones
Trusted (100)	Highest level of trust. By default, the DEFAULT VLAN is mapped to the predefined LAN zone. You can group one or more VLANs into a Trusted zone.	LAN
VPN (75)	Higher level of trust than a public zone, but a lower level of trust than a trusted zone. This security level is used exclusively for VPN connections. All traffic is encrypted.	VPN SSLVPN
Public (50)	Higher level of trust than a guest zone, but a lower level of trust than a VPN zone.	DMZ
Guest (25)	Higher level of trust than an untrusted zone, but a lower level of trust than a public zone.	GUEST
Untrusted (0)	Lowest level of trust. By default, the WAN1 interface is mapped to the WAN zone. If you are using the secondary WAN (WAN2), you can map it to the WAN zone or any other untrusted zone.	WAN
Voice	Designed exclusively for voice traffic. Incoming and outgoing traffic is optimized for voice operations. For example, assign Cisco IP Phones to the VOICE zone.	VOICE

Default Firewall Settings

By default, the firewall prevents all traffic from a lower security zone to a higher security zone (commonly known as Inbound) and allows all traffic from a higher security zone to a lower security zone (commonly known as Outbound).

For example, all traffic from the LAN (trusted zone) to the WAN (untrusted zone) is permitted, and traffic from the WAN (untrusted zone) to the DMZ (public zone) is blocked.

When you create a new zone, such as a Data zone, firewall rules are automatically generated to permit or block traffic between that zone and other zones, based on the security levels for the **From** and **To** zones.

The following table displays the default access control settings for traffic between the zones in the same or different security levels.

From/To	Trusted(100)	VPN(75)	Public(50)	Guest(25)	Untrusted(0)
Trusted(100)	Deny	Permit	Permit	Permit	Permit
VPN(75)	Deny	Deny	Permit	Permit	Permit
Public(50)	Deny	Deny	Deny	Permit	Permit
Guest(25)	Deny	Deny	Deny	Deny	Permit
Untrusted(0)	Deny	Deny	Deny	Deny	Deny

If you want to alter the default behaviors—for example, allowing some inbound access to your network (WAN to LAN) or blocking some outbound traffic from your network (LAN to WAN)—you must create firewall rules.

Use the Default Policies page to view the default firewall behaviors for all predefined zones and new zones.

STEP 1 Click **Firewall > Access Control > Default Policies**.

STEP 2 Click the triangle to expand or contract the default access control settings for a specific zone. The following behaviors are defined for all predefined zones.

From/To	LAN	VOICE	VPN	SSLVPN	DMZ	GUEST	WAN
LAN	N/A	Deny	Permit	Permit	Permit	Permit	Permit

VOICE	Deny	N/A	Permit	Permit	Permit	Permit	Permit
VPN	Deny	Deny	N/A	Deny	Permit	Permit	Permit
SSLVPN	Deny	Deny	Deny	N/A	Permit	Permit	Permit
DMZ	Deny	Deny	Deny	Deny	N/A	Permit	Permit
GUEST	Deny	Deny	Deny	Deny	Deny	N/A	Permit
WAN	Deny	Deny	Deny	Deny	Deny	Deny	N/A

NOTE ACL rules are applicable for inter-VLAN traffic, whether within a zone or between zones. You cannot set ACL rules for intra-VLAN traffic, such as LAN to LAN.

Priorities of Firewall Rules

The security appliance includes three types of firewall rules:

- **Default firewall rules:** The firewall rules that are defined on the security appliance for all predefined zones and new zones. The default firewall rules cannot be deleted nor edited.
- **Custom firewall rules:** The firewall rules that are configured by the users. The security appliance supports up to 100 custom firewall rules.
- **VPN firewall rules:** The firewall rules that are automatically generated by the zone access control settings in your VPN configurations. The VPN firewall rules cannot be edited in the Firewall > Access Control > ACL Rules page. To edit the zone access control settings in your VPN configurations, go to the VPN pages.

All firewall rules are sorted by the priority. The custom firewall rules have the highest priority. The VPN firewall rules have higher priorities than the default firewall rules, but lower than the custom firewall rules.

Preliminary Tasks for Configuring Firewall Rules

Depending on the firewall settings that you want to use, you may need to complete the following tasks before you configure firewall rules:

- To create a firewall rule that applies only to a specific zone except the predefined zones, first create the zone. See Configuring Zones, page 146.

- To create a firewall rule that applies to a specific service or service group, first create the service or service group. See Service Management, page 177.
- To create a firewall rule that applies only to a specific address or address group, first create the address or address group. See Address Management, page 175.
- To create a firewall rule that applies only at a specific day and time, first create the schedule. See Configuring Schedules, page 449.

General Firewall Settings

STEP 1 Click **Firewall > Access Control > ACL Rules**.

The ACL Rules window opens. The firewall rules appear in the ACL Control List (ACL) table. The table includes all firewall rules for controlling traffic from a particular zone to a particular destination.

STEP 2 The firewall rules are sorted by the priority. You can reorder the custom firewall rules by the priority. You can move a rule up, move a rule down, or move it to a specified location in the list.

- To move the rule up one position, click the **Move up** icon.
- To move the rule down one position, click the **Move down** icon.
- To move the rule to a specific location, click the **Move** icon and enter the target index number to move the selected rule to.

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

  NOTE: You cannot reorder the default firewall rules and VPN firewall rules. The custom firewall rules cannot be moved lower than the default firewall rules and VPN firewall rules.

STEP 3 To view the list of firewall rules that belong to the same group, choose the source and destination from the **From Zone** and **To Zone** drop-down lists and click **Apply**. Only the rules for the specified zones appear.

For example: If you choose WAN from the **From Zone** drop-down list and choose LAN from the **To Zone** drop-down list, only the firewall rules from WAN to LAN appear.

STEP 4 You can perform other tasks for firewall rules:

- Check **Enable** to enable a firewall rule, or uncheck this box to disable it. By default, all default firewall rules are enabled.
- To add a new entry, click the **Add** button.
- 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 the **Delete** button.
- Check **Log** to log the event when a firewall rule is hit. For information on configuring firewall logging settings, see **Configuring Firewall Logging Settings, page 260**.
- To permit traffic access, choose **Permit**. To deny traffic access, choose **Deny**. To increase the Hit Count number by one when the packet hits the firewall rule, choose **Accounting**.
- To view the type of a firewall rule, point your mouse cursor to the **Detail** icon.
- To set the values in the Hit Count column for all firewall rules to zero, click **Reset**.
- To manually refresh the data in the table, click **Refresh**.

NOTE: The default firewall rules cannot be disabled, deleted, edited, nor moved.

Configuring a Firewall Rule

This section describes how to configure a firewall rule to control inbound or outbound traffic.

NOTE For detailed firewall configuration examples, see **Firewall and NAT Rule Configuration Examples, page 274**.

STEP 1 Click **Firewall > Access Control > ACL Rules**.

The ACL Rules window opens.

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

The Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Enable:** Click **On** to enable the firewall rule, or click **Off** to create only the firewall rule.
- **From Zone:** Choose the source zone for traffic that is covered by this firewall rule. For example, choose **DMZ** if traffic is coming from a server on your DMZ.
- **To Zone:** Choose the destination zone for traffic that is covered by this firewall rule. For example, choose **WAN** if traffic is going to the Internet.

  NOTE: Only the existing zones are selectable. To create new zones, go to the **Networking > Zone** page. For information on configuring zones, see Configuring Zones, page 146.
- **Services:** Choose an existing service or service group that is covered by this firewall rule. If the service or service group that you want is not in the list, choose **Create a new service** to create a new service object or choose **Create a new service group** to create a new service group object. To maintain the service and service group objects, go to the **Networking > Service Management** page. See Service Management, page 177.
- **Source Address:** Choose an existing address or address group as the source address or network that is covered by this firewall rule.
- **Destination Address**: Choose an existing address or address group as the destination address or network that is covered by this firewall rule.

  If the address or address group that you want is not in the list, choose **Create a new address** to create a new address object, or choose **Create a new address group** to create a new address group object. To maintain the address and address group objects, go to the **Networking > Address Management** page. See Address Management, page 175.
- **Schedule:** By default, the firewall rule is always on. If you want to keep the firewall rule active at a specific day and time, choose the schedule for the firewall rule. If the schedule that you want is not in the list, choose **Create a new schedule** to create a new schedule. To maintain the schedules, go to the **Device Management > Schedules** page. See Configuring Schedules, page 449.
- **Log:** Click **On** to log the event when a firewall rule is hit. For information on configuring firewall logging settings, see Configuring Firewall Logging Settings, page 260.

- **Match Action:** Choose the action for traffic when the packet hits the firewall rule.
  - **Deny:** Deny access.
  - **Permit:** Permit access.
  - **Accounting:** Increase the Hit Count number by one when the packet hits the firewall rule.

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

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

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

- Prevent common types of attacks. See **Configuring Attack Protection, page 287**.
- Allow or block traffic from specified MAC addresses. See **Configuring MAC Address Filtering to Permit or Block Traffic, page 285**
- Associate the IP address with the MAC address to prevent spoofing. See **Configuring IP-MAC Binding to Prevent Spoofing, page 286**
- Allow or block the websites that contain specific domains or URL keywords. See **Configuring Content Filtering to Control Internet Access, page 281**.

Configuring a Firewall Rule to Allow Multicast Traffic

By default, multicast traffic from Any zone to Any zone is blocked by the firewall. To enable multicast traffic, you must first uncheck **Block Multicast Packets** in the **Firewall > Attack Protection** page, and then manually create firewall rules to allow multicast forwarding from a specific zone to other zones. The security appliance predefines a multicast address (**IPv4_Multicast**) for this purpose.

For example, IGMP Proxy can be active from WAN zone to LAN zone. When you enable IGMP Proxy and want to receive multicast packets from WAN zone to LAN zone, you must uncheck **Block Multicast Packets** in the **Firewall > Attack Protection** page, and then create a firewall rule to permit multicast traffic from WAN zone to LAN zone.

This section provides a configuration example about how to create a WAN-to-LAN firewall rule to permit multicast traffic by using the predefined multicast address object.

STEP 1 Click **Firewall > Access Control > ACL Rules**.

STEP 2 Click **Add** to add a new firewall rule.

The Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Enable:** Click **On** to enable the firewall rule.
- **From Zone:** Choose **WAN** as the source zone of traffic.
- **To Zone:** Choose **LAN** as the destination zone of traffic.
- **Services:** Choose **ANY** for this firewall rule.
- **Source Address:** Choose **ANY** as the source address.
- **Destination Address:** Choose the predefined multicast address called "**IPv4_Multicast**" as the destination address.
- **Schedule:** Choose **Always On** for this firewall rule.
- **Log:** Click **Off** for this firewall rule. We recommend that you disable the Log feature for a multicast firewall rule.
- **Match Action:** Choose **Permit** to allow access.

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

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

Configuring Firewall Logging Settings

Perform the following steps to log the firewall events and view firewall logs:

STEP 1 Enable the Log feature for firewall rules. See **Configuring a Firewall Rule, page 257**.

STEP 2 Go to the **Device Management > Logs > Log Settings** page to configure the log settings. You must enable the Log feature, set the log buffer size, and specify the Email Alert, Remote Logs, and Local Log settings if you want to send firewall logs to a specified email address, save firewall logs to your local syslog daemon, and save firewall logs to a specified remote syslog server. See Configuring Log Settings, page 444.

STEP 3 Go to the **Device Management > Logs > Log Facilities** page to enable Email Alert, Local Log, and/or Remote Log for the firewall facility.

- To send firewall logs to a specified email address, check the box of Email Alert for the **Firewall** facility.
- To save firewall logs to the local syslog daemon, check the box of Local Log for the **Firewall** facility.
- To save firewall logs to the remote syslog server, check the box of Remote Log for the **Firewall** facility.

STEP 4 After you configure the firewall logging settings, go to the **Device Management > Logs > View Logs** page to view firewall logs. Choose **Firewall** from the Log Facility drop-down list to view firewall logs. You can filter firewall logs by the severity level or by the source and destination IP addresses. See Viewing Logs, page 442.

Configuring NAT Rules to Securely Access a Remote Network

Network Address Translation (NAT) enables private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise only one public address for the entire network to the outside world.

NAT can also provide the following benefits:

- **Security:** Keeping internal IP addresses hidden discourages direct attacks.
- **IP routing solutions:** Overlapping IP addresses are not a problem when you use NAT.
- **Flexibility:** You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.

Refer to the following topics:

- **Viewing NAT Translation Status, page 262**
- **Priorities of NAT Rules, page 263**

- Configuring Dynamic PAT Rules, page 264
- Configuring Static NAT Rules, page 265
- Configuring Port Forwarding Rules, page 266
- Configuring Port Triggering Rules, page 268
- Configuring Advanced NAT Rules, page 269
- Configuring IP Alias for Advanced NAT rules, page 270
- Configuring an Advanced NAT Rule to Support NAT Hairpinning, page 272

NOTE For detailed NAT configuration examples, see **Firewall and NAT Rule Configuration Examples, page 274**.

Viewing NAT Translation Status

Use the NAT Status page to view information for all NAT rules. If one page cannot show all NAT entries, choose the page number from the drop-down list to view the NAT entries on another page.

Firewall > NAT > NAT Status

Field	Description
Original Source Address	Original source IP address in the packet.
Original Destination Address	Original destination IP address in the packet.
Source Port	Source interface that traffic comes from.
Destination Port	Destination interface that traffic goes to.
Translated Destination Address	IP address that the specified original destination address is translated to.
Translated Source Address	IP address that the specified original source address is translated to.
Translated Destination Port	Interface that the specified destination interface is translated to.

Field	Description
Translated Source Port	Interface that the specified source interface is translated to.
Tx Packets	Number of transmitted packets.
Rx Packets	Number of received packets.
Tx Bytes/Sec	Volume in bytes of transmitted traffic.
Rx Bytes/Sec	Volume in bytes of received traffic.

Priorities of NAT Rules

If there is a conflict between advanced NAT, static NAT, or port forwarding rules, the security appliance will process the rules as described below.

Inbound Traffic

For an inbound packet, the security appliance will perform NAT before a forwarding decision is made and will use the following order of precedence for the various types of rules:

1. Advanced NAT
2. Static NAT
3. Port Forwarding
4. Port Triggering

Outbound Traffic

For an outbound packet, the security appliance will perform NAT after a forwarding decision is made and will use the following order of precedence for various types of rules.

1. Advanced NAT
2. Static NAT
3. Dynamic PAT

For example, if an advanced NAT rule and a port forwarding rule conflict, then the advanced NAT rule will take precedence over the port forwarding rule and the port forwarding rule will not take effect.

Configuring Dynamic PAT Rules

Dynamic Port Address Translation (Dynamic PAT) can only be used to establish connections from private network to public network. Dynamic PAT translates multiple private addresses to one or more public IP address.

NOTE For the duration of the translation, a remote host can initiate a connection to the translated host if a firewall rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case, you can rely on the security of the firewall rules.

STEP 1 Click **Firewall > NAT > Dynamic PAT**.

STEP 2 Specify the PAT IP address for each WAN port.

- **Auto:** Automatically use the IP address of the WAN port as the translated IP address.
- **Manual:** Manually choose a single public IP address or a network address as the translated IP address from the **IP Address** drop-down list. 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.

STEP 3 Translate multiple private IP addresses of a VLAN to one or more mapped IP addresses.

- **Enable WAN1:** Check this box to translate all IP addresses of the selected VLAN into the public IP address specified on the WAN1 port.
- **Enable WAN2:** Check this box to translate all IP addresses of the selected VLAN into the public IP address specified on the WAN2 port.
- **VLAN IP Address:** The subnet IP address and netmask of the selected VLAN.

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

Configuring Static NAT Rules

Static NAT creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if a firewall rule allows it). With dynamic PAT, on the other hand, each host uses a different address or port for each subsequent translation, so bidirectional initiation is not supported.

Up to 64 static NAT rules can be configured on the security appliance. You must create firewall rules to allow access so that the static NAT rules can function properly.

NOTE Remote management will not work if you configure a static NAT rule that maps an internal server to the WAN IP address. For example, if you create a static NAT rule that maps 192.168.75.100 to the WAN IP address, 173.39.202.68, then remote users will not have access to the configuration utility via http://173.39.202.68:8080.

STEP 1 Click **Firewall > NAT > Static NAT**.

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

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 Static NAT Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **WAN:** Choose either WAN1 or WAN2 as the WAN port.
- **Public IP:** Choose an IP address object as the public IP address.
- **Private IP:** Choose an IP address object as the private IP address.

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

  NOTE: Firewall rules must be configured to allow access. You can go to the **Firewall > Access Control > ACL Rules** page or click the **Create Rule** link to do this, but save your settings on this page first.

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

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

Configuring Port Forwarding Rules

Port forwarding forwards a TCP/IP packet traversing a Network Address Translation (NAT) gateway to a pre-determined network port on a host within a NAT-masqueraded network, typically a private network based on the port number on which it was received at the gateway from the originating host.

Use the Port Forwarding page to assign a port number to a service that is associated with the application that you want to run, such as web servers, FTP servers, email servers, or other specialized Internet applications.

NOTE

- Up to 64 port forwarding rules can be configured on the security appliance. You must create firewall rules to allow access so that the port forwarding rules can function properly.
- To open an internal FTP server to the Internet, make sure that the FTP server is listening on TCP port 21 or both the FTP server and client must use the active mode when the FTP server is listening on some other TCP port. Otherwise the FTP client cannot access the FTP server.

STEP 1 Click **Firewall > NAT > Port Forwarding**.

STEP 2 To enable a port forwarding rule, check the box in the **Enable** column.

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

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 Port Forwarding Rule - Add/Edit window opens.

STEP 4 Enter the following information:

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

NOTE: One-to-one translation will be performed for port range forwarding. For example, if you want to translate an original TCP service with the port range of 50000 to 50002 to a TCP service with the port range of 60000 to 60002, then the port 50000 will be translated to the port 60000, the port 50001 will be translated to the port 60001, and the port 50002 will be translated to the port 60002.

- **Translated IP:** Choose the IP address of your local server that needs to be translated. If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the **Networking > Address Management** page. See Address Management, page 175.
- **WAN:** Choose either WAN1 or WAN2, or both as the incoming WAN port.
- **WAN IP:** Specify the public IP address of the server. You can use the IP address of the selected WAN port or a public IP address that is provided by your ISP. When you choose Both as the incoming WAN port, this option is grayed out.
- **Enable Port Forwarding:** Click **On** to enable the port forwarding rule, or click **Off** to create only the port forwarding rule.
- **Create Firewall Rule:** Check this box to automatically create a firewall rule to allow access so that the port forwarding rule can function properly. You must manually create a firewall rule if you uncheck this box.

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

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

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

Configuring Port Triggering Rules

Port triggering opens an incoming port for a specified type of traffic on a defined outgoing port. When a LAN device makes a connection on one of the defined outgoing ports, the security appliance opens the specified incoming port to support the exchange of data. The open ports will be closed again after 600 seconds when the data exchange is complete.

Port triggering is more flexible and secure than port forwarding, because the incoming ports are not open all the time. They are open only when a program is actively using the trigger port.

Some applications may require port triggering. Such applications require that, when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The security appliance must send all incoming data for that application only on the required port or range of ports. You can specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

NOTE Up to 15 port triggering rules can be configured on the security appliance. Port triggering is not appropriate for servers on the LAN, since the LAN device must make an outgoing connection before an incoming port is opened. In this case, you can create the port forwarding rules for this purpose.

STEP 1 Click **Firewall > NAT > Port Triggering**.

STEP 2 To enable a port triggering rule, check the box in the **Enable** column.

STEP 3 To add a new port triggering rule, click **Add**.

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 Port Triggering Rule - Add/Edit window opens.

STEP 4 Enter the following information:

- **Description:** Enter the name for the port triggering rule.
- **Triggered Service:** Choose an outgoing TCP or UDP service.
- **Opened Service:** Choose an incoming TCP or UDP service.

  If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the **Networking > Service Management** page. See Service Management, page 177.

- **Enable Port Triggering:** Click **On** to enable the port triggering rule, or click **Off** to create only the port triggering rule.

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

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

Configuring Advanced NAT Rules

Advanced NAT allows you to identify real addresses and real ports for address translation by specifying the source and destination addresses.

NOTE Up to 32 advanced NAT rules can be configured on the security appliance. You must create firewall rules to allow access so that advanced NAT rules can function properly.

STEP 1 Click **Firewall > NAT > Advanced NAT**.

STEP 2 To enable an advanced NAT rule, check the box in the **Enable** column.

STEP 3 To add a new advanced NAT rule, click **Add**.

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 Advanced NAT Rule - Add/Edit window opens.

STEP 4 Enter the following information:

- **Name:** Enter the name for the advanced NAT rule.
- **Enable:** Click **On** to enable the advanced NAT rule, or click **Off** to create only the advanced NAT rule.
- **From:** Choose **Any** or choose an interface (a WAN port or a VLAN) that traffic originates from.
- **To:** Choose **Any** or choose an interface (a VLAN or a WAN port) that traffic goes to.

  NOTE: When the original destination address is different with the translated destination address, you must choose **Any** for this option. When the original destination address is same with the translated destination address, you can choose a specific VLAN or WAN port for this option.

- **Original Source Address:** Choose the original source address for the packet.
- **Original Destination Address:** Choose the original destination address for the packet.
- **Original Services:** Choose the original TCP or UDP service.
- **Translated Source Address:** Choose the translated source address for the packet.
- **Translated Destination Address:** Choose the translated destination address for the packet.
- **Translated Services:** Choose the translated TCP or UDP service.

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

  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.

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

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

STEP 7 Firewall rules must be configured to allow access so that advanced NAT rules can function properly. After you save your settings, go to the **Firewall > Access Control > ACL Rules** page to do this. See **Configuring a Firewall Rule, page 257**.

Configuring IP Alias for Advanced NAT rules

A single WAN port can be accessible through multiple IP addresses by adding an IP alias to the port. When you configure an advanced NAT rule, the security appliance will automatically create an IP alias in the following cases:

Use Case: The inbound interface (**From**) is set to a WAN port but the original destination IP address (**Original Destination Address**) is different with the public IP address of the selected WAN port.

For example, you host a HTTP server (192.168.75.20) on your LAN. Your ISP has provided a static IP address (1.1.1.3) that you want to expose to the public as your HTTP server address. You want to allow Internet user to access the internal HTTP server by using the specified public IP address.

Solution: Assuming that the IP address of the WAN1 port is 1.1.1.2 and you are assigned another public IP address 1.1.1.3. You can first create a host address object with the IP 192.168.75.20 called “HTTPServer” and a host address object with the IP 1.1.1.3 called “PublicIP”, and then configure an advanced NAT rule as follows to open the HTTP server to the Internet.

From	WAN1 **NOTE:** It must be set as a WAN port and cannot be set as Any.
To	Any
Original Source Address	Any
Original Destination Address	PublicIP
Original Services	HTTP
Translated Source Address	Any
Translated Destination Address	HTTPServer
Translated Services	HTTP

Use Case: The outbound interface (**To**) is set to a WAN port but the translated source IP address (**Translated Source Address**) is different with the public IP address of the selected WAN port.

For example, you have provided a static IP address (1.1.1.3). The security appliance is set as a SSL VPN server. You want to translate the IP addresses of the SSL VPN clients to the specified public IP address when the SSL VPN clients access the Internet.

Solution: Assuming that the IP address of the WAN1 port is 1.1.1.2 and the SSL VPN client address pool is set as 192.168.200.0/24. You can first create a host address object with the IP 1.1.1.3 called "PublicIP," and then create an advanced NAT rule as follows to allow SSL VPN clients to access the Internet:

From	Any
To	WAN1 **NOTE:** It must be set as a WAN port and cannot be set as Any.
Original Source Address	SSLVPNPool
Original Destination Address	Any
Original Services	Any
Translated Source Address	PublicIP
Translated Destination Address	Any
Translated Services	Any

Configuring an Advanced NAT Rule to Support NAT Hairpinning

NAT hairpinning allows the hosts at LAN side to access internal servers by using their respective external IP addresses (public IP addresses). This section provides a configuration example about how to create an advanced NAT rule to support NAT hairpinning.

STEP 1 Go to the **Networking > Address Management** page to create a host address object with the IP 192.168.10.100 called "FTPServer." The FTP server locates in the LAN zone.

STEP 2 Go to the **Firewall > NAT > Port Forwarding** page to create a port forwarding rule as follows.

Original Service	FTP-CONTROL
Translated Service	FTP-CONTROL
Translated IP	FTPServer
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On
Create Firewall Rule	On

STEP 3 A firewall rule will be automatically created as follows to allow access.

From Zone	WAN
To Zone	LAN
Services	FTP-CONTROL
Source Address	ANY
Destination Address	FTPServer
Match Action	Permit

STEP 4 Then go to the **Firewall > NAT > Advanced NAT** page to create an advanced NAT rule as follows.

From	DEFAULT
To	Any
Original Source Address	DEFAULT_NETWORK
Original Destination Address	WAN1_IP
Original Services	FTP-CONTROL

Translated Source Address	WAN1_IP
Translated Destination Address	FTPServer
Translated Services	FTP-CONTROL

Firewall and NAT Rule Configuration Examples

This section provides some configuration examples on adding firewall and NAT rules.

- **Allowing Inbound Traffic Using the WAN IP Address, page 274**
- **Allowing Inbound Traffic Using a Public IP Address, page 276**
- **Allowing Inbound Traffic from Specified Range of Outside Hosts, page 279**
- **Blocking Outbound Traffic by Schedule and IP Address Range, page 280**
- **Blocking Outbound Traffic to an Offsite Mail Server, page 280**

Allowing Inbound Traffic Using the WAN IP Address

Use Case: You host a FTP server on your LAN. You want to open the FTP server to Internet by using the IP address of the WAN1 port. Inbound traffic is addressed to your WAN1 IP address but is directed to the FTP server.

Solution: Perform the following tasks to complete the configuration:

STEP 1 Go to the **Networking > Address Management** page to create a host address object with the IP 192.168.75.100 called “InternalFTP.”

STEP 2 Go to the **Firewall > NAT > Port Forwarding** page to create a port forwarding rule as follows.

Original Service	FTP-CONTROL
Translated Service	FTP-CONTROL
Translated IP	InternalFTP
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On

STEP 3 Or go to the **Firewall > NAT > Advanced NAT** page to create an advanced NAT rule as follows.

From	WAN1
To	DEFAULT
Original Source Address	ANY
Original Destination Address	WAN1_IP
Original Services	FTP-CONTROL
Translated Source Address	ANY
Translated Destination Address	InternalFTP
Translated Services	FTP-CONTROL

STEP 4 Then go to the **Firewall > Access Control > ACL Rules** page to create a firewall rule as follows to allow access:

From Zone	WAN
To Zone	LAN
Services	FTP-CONTROL

Source Address	ANY
Destination Address	InternalFTP
Match Action	Permit

NOTE When you create the port forwarding rule, you can check **Create Firewall Rule** to automatically generate the firewall rule.

Allowing Inbound Traffic Using a Public IP Address

Use Case: You host an RDP server on the DMZ. Your ISP has provided a static IP address that you want to expose to the public as your RDP server address. You want to allow Internet user to access the RDP server by using the specified public IP address.

Solution 1: Perform the following tasks to complete the configuration:

STEP 1 Go to the Networking > Address Management page to create a host address object with the IP 192.168.12.101 called “RDPServer” and a host address object with the IP 172.39.202.102 called “PublicIP.”

STEP 2 Go to the Networking > Service Management page to create a TCP service object with the port 3389 called “RDP.”

STEP 3 Go to the Firewall > NAT > Port Forwarding page to create a port forwarding rule as follows.

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

STEP 4 Or go to the Firewall > NAT > Advanced NAT page to create an advanced NAT rule as follows.

From	WAN1
To	DMZ
Original Source Address	ANY
Original Destination Address	PublicIP
Original Services	RDP
Translated Source Address	ANY
Translated Destination Address	RDPServer
Translated Services	RDP

STEP 5 Then go to the Firewall > Access Control > ACL Rules page to create a firewall rule as follows to allow access:

From Zone	WAN
To Zone	DMZ
Services	RDP
Source Address	ANY
Destination Address	RDPServer
Match Action	Permit

NOTE When you create the port forwarding rule, you can check **Create Firewall Rule** to automatically generate the firewall rule.

Solution 2: For this use case, you can use the DMZ Wizard to complete the configuration.

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

STEP 2 In the DMZ Configuration page, configure a DMZ network as follows:

Name	DMZ
IP	192.168.12.1
Netmask	255.255.255.0
Port	GE6
Zone	DMZ

STEP 3 In the DMZ Service page, create a DMZ service as follows:

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

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

STEP 5 A firewall rule will be automatically generated as follows to allow access.

From Zone	WAN
To Zone	DMZ
Services	RDP
Source Address	ANY
Destination Address	RDPServer

Match Action	Permit

Allowing Inbound Traffic from Specified Range of Outside Hosts

Use Case: You want to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses (132.177.88.2 to 132.177.88.254). In the example, connections for CU-SeeMe (an Internet video-conferencing client) are allowed only from a specified range of external IP addresses.

Solution: Perform the following tasks to complete the configuration:

STEP 1 Go to the Networking > Address Management page to create an address object with the range 132.177.88.2 to 132.177.88.254 called "OutsideNetwork" and a host address object with the IP 192.168.75.110 called "InternalIP."

STEP 2 Go to the Firewall > NAT > Port Forwarding page to create a port forwarding rule as follows.

Original Service	CU-SEEME
Translated Service	CU-SEEME
Translated IP	InternalIP
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On
Create Firewall Rule	Off

STEP 3 Go to the Firewall > Access Control > ACL Rules page and create the ACL rule as described below.

From Zone	WAN
To Zone	LAN

Services	CU-SEEME
Source Address	OutsideNetwork
Destination Address	InternalIP
Match Action	Permit

Blocking Outbound Traffic by Schedule and IP Address Range

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

Solution: Create an address object with the range 10.1.1.1 to 10.1.1.100 called "TempNetwork" and a schedule called "Weekend" to define the time period when the firewall rule is in effect. Then create a firewall rule as follows:

From Zone	LAN
To Zone	WAN
Services	HTTP
Source Address	TempNetwork
Destination Address	Any
Schedule	Weekend
Match Action	Deny

Blocking Outbound Traffic to an Offsite Mail Server

Use Case: Block access to the SMTP service to prevent a user from sending email through an offsite mail server.

Solution: Create a host address object with the IP address 10.64.173.20 called "OffsiteMail" and then create a firewall rule as follows:

From Zone	LAN
To Zone	WAN
Services	SMTP
Source Address	Any
Destination Address	OffsiteMail
Match Action	Deny

Configuring Content Filtering to Control Internet Access

Content Filtering blocks or allows HTTP access to websites containing specific keywords or domains. It controls access to certain Internet sites based on analysis of its content (domain or URL keyword), rather than its source or other criteria. It is most widely used on the Internet to filter web access.

Refer to the following topics:

- **Configuring Content Filtering Policy Profiles, page 281**
- **Configuring Website Access Control List, page 282**
- **Mapping Content Filtering Policy Profiles to Zones, page 283**
- **Configuring Advanced Content Filtering Settings, page 284**

NOTE Enabling Firewall Content Filtering will disable Web URL Filtering. Enabling Web URL Filtering will disable Firewall Content Filtering.

Configuring Content Filtering Policy Profiles

A content filtering policy profile is used to specify which websites are blocked or allowed.

NOTE Up to 16 content filtering policy profiles can be configured on the security appliance.

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

STEP 2 To add a content filtering 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 Content Filtering Policies - Add/Edit window opens.

STEP 3 Enter the following information:

- **Policy Profile:** Enter the name for the content filtering policy profile.
- **Description:** Enter a brief description for the content filtering policy profile.

STEP 4 In the **Website Access Control List** area, specify the list of websites that you want to allow or block. See **Configuring Website Access Control List, page 282**.

STEP 5 In the **For URLs not specified above** area, specify how to deal with the websites that are not specified in the list.

- **Permit them:** If you choose this option, all websites not specified in the list are allowed.
- **Deny them:** If you choose this option, all websites not specified in the list are blocked.

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

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

Configuring Website Access Control List

This section describes how to specify the website access control list to control access for specific websites.

NOTE Up to 32 website access rules can be configured for each content filtering policy profile.

STEP 1 In the **Website Access Control List** area, click **Add** to add a website access rule.

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

The Website Access Control List - Add/Edit window opens.

STEP 2 Enter the following information:

- **Enable Content Filter URL:** Click **On** to enable the website access rule, or click **Off** to create only the website access rule.
- **URL:** Enter the domain name or URL keyword of a website that you want to permit or block.
- **Match Type:** Specify how to match this rule:
  - **Web Site:** If you choose this option, permit or block the HTTP access of a website that fully matches the domain that you entered in the **URL** field.

    For example, if you enter yahoo.com in the URL field, then it can match the website http://yahoo.com/*, but cannot match the website http://*.yahoo.com.uk/*.
  - **URL Keyword:** If you choose this option, permit or block the HTTP access of a website that contains the keyword that you entered in the **URL** field.

    For example, if you enter yahoo in the URL field, then it can match the websites such as www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk, and www.yahoo.co.jp.
- **Action:** Choose **Permit** to permit access, or choose **Block** to block access.

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

Mapping Content Filtering Policy Profiles to Zones

Use the Policy to Zone Mapping page to apply the content filtering policy profile to each zone. The content filtering policy profile assigned to each zone determines whether to block or forward the HTTP requests from the hosts in the zone. The blocked requests will be logged.

STEP 1 Click **Firewall > Content Filtering > Policy to Zone Mapping**.

The Policy to Zone Mapping window opens.

STEP 2 Click **On** to enable the Content Filtering feature, or click **Off** to disable it.

STEP 3 Specify the policy profile for each zone. By default, the Default_Profile that permits all websites is selected for all predefined and new zones.

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

Configuring Advanced Content Filtering Settings

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

STEP 2 Enter the following information:

- **Filter Traffic on HTTP Port:** Enter the port number that is used for filtering HTTP traffic. Content Filtering only monitors and controls the website visits through this HTTP port. The default value is 80.
- **Filter Traffic on HTTPS port:** Enter the port number that is used for filtering HTTPS traffic. Web URL Filtering only monitors and controls the website visits through this HTTPS port. The default value is 443.
- **Blocked Web Components:** You can block web components like Proxy, Java, ActiveX, and Cookies. By default, all of them are permitted.
  - **Proxy:** Check this box to block proxy servers, which can be used to circumvent certain firewall rules and thus present a potential security gap.
  - **Java:** Check this box to block Java applets that can be downloaded from pages that contain them.
  - **ActiveX:** Check this box to prevent ActiveX applets from being downloaded through Internet Explorer.
  - **Cookies:** Check this box to block cookies, which typically contain sessions.
- **Action:** Choose one of the following actions when a web page is blocked:
  - **Display Default Blocked Page when the requested page is blocked:** Displays the default block page if a web page is blocked. If you choose this option, the message that you specify in the **Block Message** field will show on the default block page.
  - **Redirect URL:** Redirects to a specified web page if a web page is blocked. If you choose this option, enter a desired URL to be redirected. Make sure that specified URL is allowed by the Website Access Control List.

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

Configuring MAC Address Filtering to Permit or Block Traffic

MAC Address Filtering permits and blocks network access from specific devices through the use of MAC address list. The MAC Address Filtering settings apply for all traffic except Intra-VLAN and Intra-SSID.

STEP 1 Click **Firewall > MAC Filtering > MAC Address Filtering**.

The MAC Address Filtering window opens.

STEP 2 Click **On** to enable the MAC Address Filtering feature, or click **Off** to disable it.

STEP 3 If you enable MAC Address Filtering, choose one of the following options as the MAC Address Filtering policy:

- **Block MAC Addresses (and allow all others):** The MAC addresses in the list are blocked and all other MAC addresses not included in the list are permitted.
- **Allow MAC Addresses (and block all others):** Only the MAC addresses in the list are permitted and all other MAC addresses not included in the list are blocked.

STEP 4 In the **MAC Address Filtering Rules** area, specify the list of MAC addresses. To add a MAC address, click **Add**. 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**.

For example, if you click **Add**, the MAC Address Filtering Rule - Add/Edit window opens. Choose the MAC address object from the **MAC Address** drop-down list and click **OK**. If the MAC address object that you want is not in the list, choose **Create a new address** to create a new MAC address object. To maintain the MAC address objects, go to the Networking > Address Management page. See Address Management, page 175.

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

Configuring IP-MAC Binding to Prevent Spoofing

IP-MAC Binding allows you to bind an IP address to a MAC address and vice-versa. It only allows traffic when the host IP address matches a specified MAC address. By requiring the gateway to validate the source traffic's IP address with the unique MAC address of device, this ensures that traffic from the specified IP address is not spoofed. If a violation (the traffic's source IP address doesn't match the expected MAC address having the same IP address), the packets will be dropped and can be logged for diagnosis.

NOTE Up to 100 IP-MAC binding rules can be configured on the security appliance.

STEP 1 Click **Firewall > MAC Filtering > IP - MAC Binding Rules**.

The IP - MAC Binding Rules window opens.

STEP 2 To add an IP-MAC binding rule, click **Add**.

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 IP&MAC Binding Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the IP-MAC binding rule.
- **MAC Address:** Choose an existing MAC address object. If the MAC address object that you want is not in the list, choose **Create a new address** to add a new MAC address object. To maintain the MAC address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **IP Address:** Choose an existing IP address object that you want to bind with the selected MAC address. If the IP address object that you want is not in the list, choose **Create a new address** to add a new IP address object. To maintain the IP address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **Log Dropped Packets:** Choose **Enable** to log all packets that are dropped. Otherwise, choose **Disable**.

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

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

Configuring Attack Protection

Use the Attack Protection page to specify how to protect your network against common types of attacks including discovery, flooding, and echo storms.

STEP 1 Click **Firewall > Attack Protection**.

STEP 2 In the **WAN Security Checks** area, enter the following information:

- **Block Ping WAN Interface:** Check this box to prevent attackers from discovering your network through ICMP Echo (ping) requests. We recommend that you disable this feature only if you need to allow the security appliance to respond to pings for diagnostic purposes.
- **Stealth Mode:** Check this box to prevent the security appliance from responding to incoming connection requests from the WAN ports. In Stealth Mode, the security appliance does not respond to blocked inbound connection requests, and your network is less susceptible to discovery and attacks.
- **Block TCP Flood:** Check this box to drop all invalid TCP packets. This feature protects your network from a SYN flood attack, in which an attacker sends a succession of SYN (synchronize) requests to a target system. It blocks all TCP SYN flood attacks (more than 200 simultaneous TCP packets per second) from the WAN ports.

STEP 3 In the **LAN Security Checks** section, enter the following information:

- **Block UDP Flood:** Check this box to limit the number of simultaneous, active UDP connections from a single computer on the LAN. If you enable this feature, also enter the number of connections to allow per host per second. The default value is 500, and the valid range is from 100 to 10,000. When this limit is reached, the security appliance considers it a UDP flood attack and drops all connections from the host.

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

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

- **Block Multicast Packets:** Check this box to block multicast packets. By default, the firewall blocks all multicast packets. This feature has higher priority than the firewall rules, which indicates that the firewall rules that permit multicast traffic will be overridden if you enable this feature.

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

- **SYN Flood Detect Rate:** Enter the maximum number of SYN packets per second that will cause the security appliance to determine that a SYN Flood Intrusion is occurring. Enter a value from 0 to 65535 SYN packets per second. The default value is 128 SYN packets per seconds. A value of zero (0) indicates that the SYN Flood Detect feature is disabled.
- **Echo Storm:** Enter the number of pings per second that will cause the security appliance to determine that an echo storm intrusion event is occurring. Enter a value from 0 to 65535 ping packets per second. The default value is 15 ping packets per seconds. A value of zero (0) indicates that the Echo Storm feature is disabled.
- **ICMP Flood:** Enter the number of ICMP packets per second, including PING packets, that will cause the security appliance to determine that an ICMP flood intrusion event is occurring. Enter a value from 0 to 65535 ICMP packets per second. The default value is 100 ICMP packets per seconds. A value of zero (0) indicates that the ICMP Flood feature is disabled.

  NOTE: When one of DoS attack levels is exceeded, that kind of traffic will be dropped.

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

Configuring Session Limits

Use the Session Limits page to configure the maximum number of connection sessions. When the connection table is full, the new sessions that access the security appliance are dropped.

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

STEP 2 Enter the following information:

- **Current All Connections:** Displays the total number of current connections. Click **Disconnect All** to clean up all connected sessions.

- **Maximum Connections:** Limit the number for TCP and UDP connections. Enter a value in the range 1000 to 60000. The default value is 60000.
- **TCP Timeout:** Enter the timeout value in seconds for TCP session. Inactive TCP sessions are removed from the session table after this duration. The valid range is 5 to 3600 seconds. The default value is 1200 seconds.
- **UDP Timeout:** Enter the timeout value in seconds for UDP session. Inactive UDP sessions are removed from the session table after this duration. The valid range is 5 to 3600 seconds. The default value is 180 seconds.

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

Configuring Application Level Gateway

The security appliance can function as an Application Level Gateway (ALG) to allow certain NAT incompatible applications (such as SIP or H.323) to operate properly through the security appliance.

If Voice-over-IP (VoIP) is used in your organization, you should enable H.323 ALG or SIP ALG to open the ports necessary to allow the VoIP through your voice device. The ALGs are created to work in a NAT environment to maintain the security for privately addressed conferencing equipment protected by your voice device.

You can use both H.323 ALG and SIP ALG at the same time, if necessary. To determine which ALG to use, consult the documentation for your VoIP devices or applications.

STEP 1 Click **Firewall > Application Level Gateway**.

The Application Level Gateway window opens.

STEP 2 Enter the following information:

- **SIP Support:** SIP ALG can rewrite the information within the SIP messages (SIP headers and SDP body) to make signaling and audio traffic between the client behind NAT and the SIP endpoint possible. Check this box to enable SIP ALG support, or uncheck this box to disable this feature.

  NOTE: Enable SIP ALG when voice devices such as UC500, UC300, or SIP phones are connected to the network behind the security appliance.

- **H.323 Support:** H.323 is a standard teleconferencing protocol suite that provides audio, data, and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Check this box to enable H.323 ALG support, or uncheck this box to disable this feature.
- **FTP Support on TCP port:** Check the box to enable FTP support, or uncheck the box to disable the this feature. Then choose a listening port. The default port is FTP-CONTROL (21).

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