Configuring a Zone-Based Firewall on the Cisco ISA500 Security Appliance

This application note describes how to configure a zone-based firewall on the Cisco ISA500 security appliance. This document includes the following sections:

A zone-based firewall can permit or deny inbound or outbound traffic to the Internet based on the zone, service, source and destination address, and time of day. Zone-based security is a powerful and flexible method of managing both internal and external network segments that allows you to separate and protect critical internal network resources from unapproved access or attacks.

Understanding Zones

A zone is a group of interfaces to which a security policy can be applied. The interfaces (such as VLAN, DMZ, WAN, and VPN) in a zone share common functions or features. For example, two interfaces that belong to the internal network might be placed in one security zone and the interfaces connected to the Internet might be placed in another zone. Security policies are used to control the transit traffic between the different zones that protects the different services.

Zone Security Levels

The zone security level is the level of trust given to that zone. Table 1 lists the security levels that the ISA500 supports.The greater the value, the higher the permission level.

Table 1. Supported Security Levels

Trusted (100)	Highest level of trust. By default, the LAN zone is trusted.
VPN (75)	Higher level of trust than a public zone, but a lower level of trust than a trusted zone. This security level is only used by the predefined VPN and SSLVPN zones. All traffic to and from a VPN zone is encrypted.
Public (50)	Higher level of trust than a guest zone, but a lower level of trust than a VPN zone. The Demilitarized (DMZ) zone is a public zone.
Guest (25)	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)	Lowest level of trust used by both the WAN and the virtual multicast zones. The WAN port can only be mapped to an untrusted zone.

Predefined Zones

The default behaviors for all predefined zones and new zones are determined by their security levels. Table 2 lists the predefined zones that the ISA500 supports. The default behavior is as follows:

- Traffic from a higher security zone to a lower security zone is permitted.
- Traffic from a lower security zone to higher security zone is blocked.
- Traffic between zones with the same security level is blocked.

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.

If you create a new trusted zone such as a data zone, firewall rules are automatically generated to permit or block traffic from the data zone to other zones or vice-versa. This permit or block action is determined by the security levels.

Table 2. Predefined Zones

WAN	**Untrusted zone**. By default, the WAN port is mapped to the WAN zone and can only be mapped to an untrusted zone.
LAN	**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	**Public zone**. Zone used for the public servers that you host in the DMZ networks.
SSLVPN	**Virtual zone**. Zone used for simplifying secure and remote SSL VPN connections. The SSLVPN zone does not have an assigned physical port.
VPN	**Virtual zone**. Zone used for simplifying secure IPsec VPN connections. The VPN zone does not have an assigned physical port.
GUEST	**Guest zone**. Only used for guest access. By default, the GUEST VLAN is mapped to this zone.
VOICE	**Trusted zone**. Security zone designed for voice traffic. Incoming and outgoing traffic from this zone is optimized for voice operations. If you have voice devices, such as a Cisco IP Phone, we recommend that you place devices into the VOICE zone.

Default Firewall Settings

By default, the firewall prevents all traffic from a lower security zone to a higher security zone, and allows all traffic from a higher security zone to a lower security zone. These rules are also referred to as access control lists or ACLs.

After you create a new zone, the default firewall rules are automatically generated to permit or block traffic from the new zone to another zone or vice-versa. Table 3 shows the default access control settings for traffic between zones with the same or different security levels.

Table 3. Default ACL Settings

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

The default behaviors for all predefined zones and new zones are determined by their security levels. For example, by default, all traffic from the LAN (trusted zone) to the WAN (untrusted zone) is permitted. All traffic from the WAN (untrusted zone) to the DMZ (public zone) is blocked.

Table 4 lists the default ACL settings for the predefined zones.

Table 4. Predefined ACL Settings

From/To	LAN	Voice	VPN	SSLVPN	DMZ	GUEST	WAN
LAN	**Permit**	Deny	**Permit**	**Permit**	**Permit**	**Permit**	**Permit**
Voice	Deny	**Permit**	**Permit**	**Permit**	**Permit**	**Permit**	**Permit**
VPN	Deny	Deny	**Permit**	Deny	**Permit**	**Permit**	**Permit**
SSLVPN	Deny	Deny	Deny	**Permit**	**Permit**	**Permit**	**Permit**
DMZ	Deny	Deny	Deny	Deny	**Permit**	Deny	Deny
GUEST	Deny	Deny	Deny	Deny	**Permit**	**Permit**	**Permit**
WAN	Deny	Deny	Deny	Deny	**Permit**	Deny	**Permit**

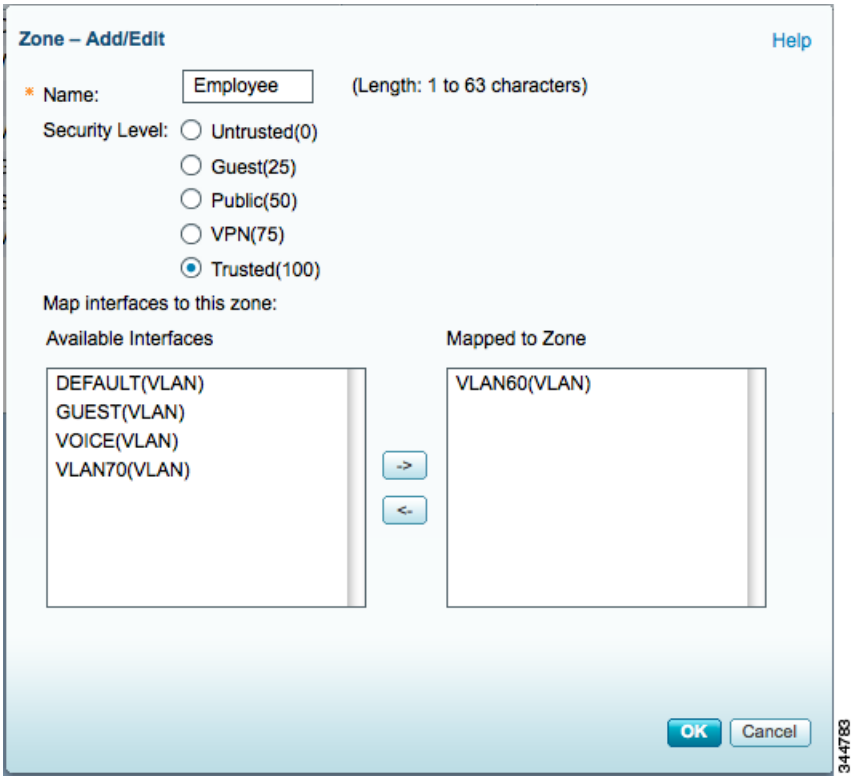
NOTE All predefined zones (except for the VOICE zone) cannot be deleted. Only the associated ports and VLANs for the predefined zones (except for the VPN and SSLVPN zones) can be edited.

Configuring Zones

Follow these steps to add a new zone, specify its security level, and map the interface to the zone:

Step 1. From the ISA500 Configuration Utility main page, choose **Networking > Zones**.

Step 2. To add a new zone, click **Add**.



Step 3. Enter a name for the new zone. For example: **Employee**.

Step 4. Specify the zone security level.

- For VLANs, all security levels are supported. In this example, the security level is set to **Trusted (100)**.
- For DMZs, choose **Public (50)**.
- For WAN ports, choose **Untrusted (0)**.

Step 5. Map interfaces to this zone.

Choose the existing VLANs or WAN ports from the **Available Interfaces** list and then click the right arrow to add them to the **Mapped to Zone** list. Up to 16 VLANs can be mapped to a zone.

Step 6. Click **OK** to apply your settings.

After you create a new zone, the firewall rules are automatically generated between zones. To customize your own rules, see Configuring Firewall Rules, page 5.

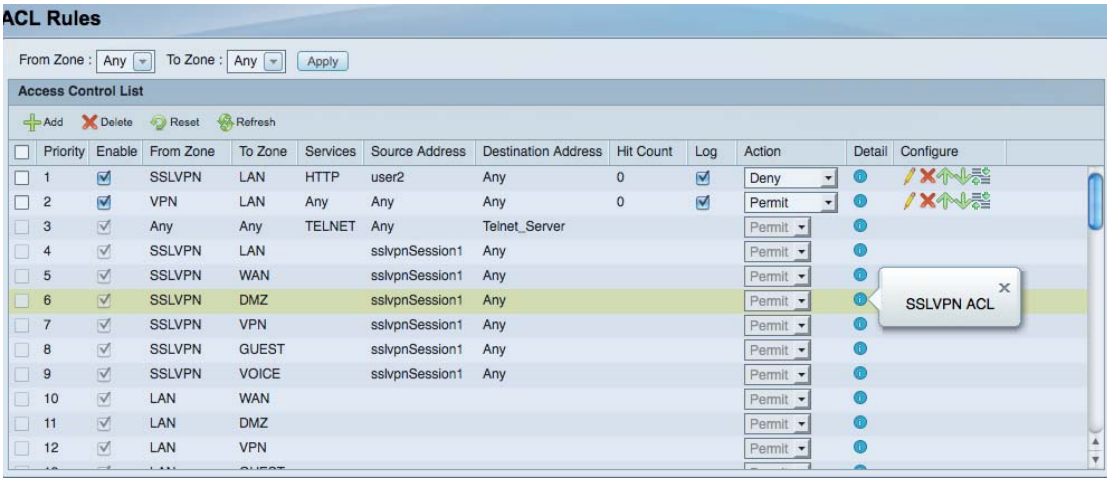
NOTE if you enabled services such as Intrusion Prevention (IPS), Anti-Virus, and Application Control on the ISA500, you will need to apply the security services on these zones. For more information, see the *Cisco ISA500 Series Integrated Security Appliances Administration Guide* at: www.cisco.com/go/isa500resources.

Configuring Firewall Rules

The ISA500 supports three types of firewall rules:

- Default Firewall Rules
- Custom Firewall Rules
- Automatically Generated Firewall Rules

This page shows the different types of firewall rules.



Default Firewall Rules

These are rules that are defined on the ISA500 for all predefined zones and new zones based on their security levels. You cannot edit, delete, or move these rules up or down. For more information, see Default Firewall Settings, page 3.

Custom Firewall Rules

There may be situations when you need to create your own custom firewall rules. Custom rules override the default and autogenerated firewall rules. For example, you can set a rule to allow or deny traffic, and apply it to a specific zone, service, group, IP address, or time of day. You can also log traffic for each rule that you define.

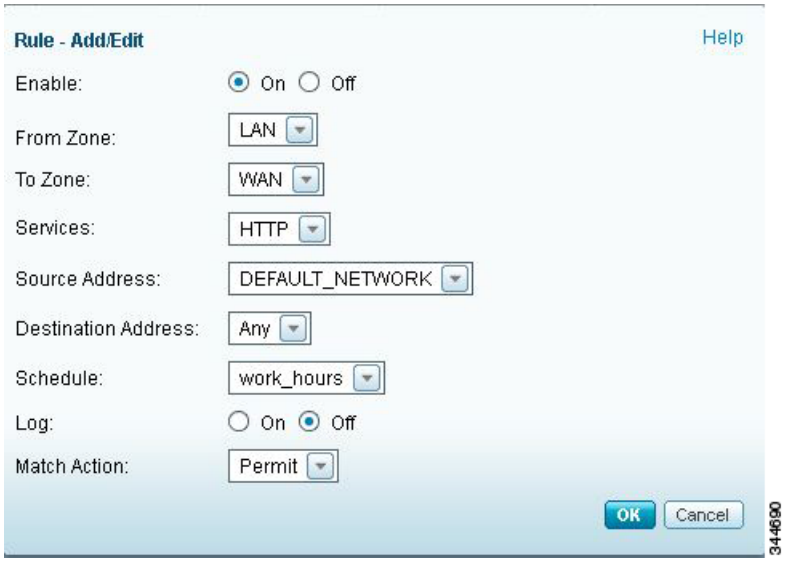
NOTE The ISA500 supports up to 100 custom firewall rules.

Scenario. You want to restrict user Internet access during work hours. By default, the DEFAULT VLAN is mapped to the LAN zone and the LAN to WAN ACL rule is set to Permit. This means that all users in the default VLAN can access the Internet at any time.

Solution. Create an ACL rule to deny access at a specific time of day as follows:

Step 1. Choose **Firewall > Access Control > ACL Rules**.

Step 2. Click **Add**.



Step 3. Click **On** to enable the firewall rule.

Step 4. Enter the following information:

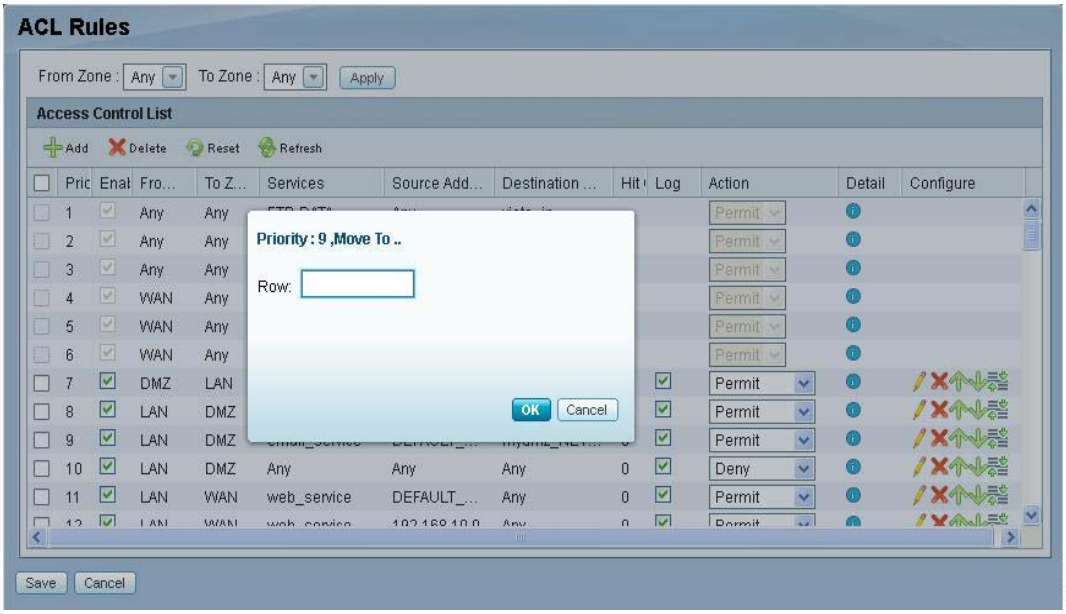
- **From Zone**: Choose **LAN**.
- **To Zone**: Choose **WAN**.
- **Services**: Choose **HTTP**.
- **Source Address**: Choose **DEFAULT_NETWORK**.
- **Destination Address**: Choose **Any**.
- **Schedule**: **Create a New Schedule**. When selected, the Schedule - Add/Edit window opens that allows you to specify when the firewall rule is active. In this example, a schedule was created called “work_hours” so that the user can only access the Internet during working hours.
- **Log**: To log the event when the firewall rule is hit, select **On**. In this example, event logging is set to off.
- **Match Action**: Choose **Permit**.

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

The new work_hours rule is added to the ACL Rules list.

Prioritizing Rules

If a firewall policy contains more than one rule that permits traffic, you can reorder them by priority. The rules are sorted in this order: Custom rules (highest priority), system automatically generated rules, and the default rules (lowest priority). You can move a rule up, move a rule down, or move it to another location in the Access Control List.



Automatically Generated Firewall Rules

You can configure the ISA500 so that the firewall rules are automatically generated for features such as port forwarding and VPN. For example, firewall rules can be automatically generated for port forwarding to allow access from the Internet to an internal server, or to allow an SSL VPN user to access all trusted zones automatically.

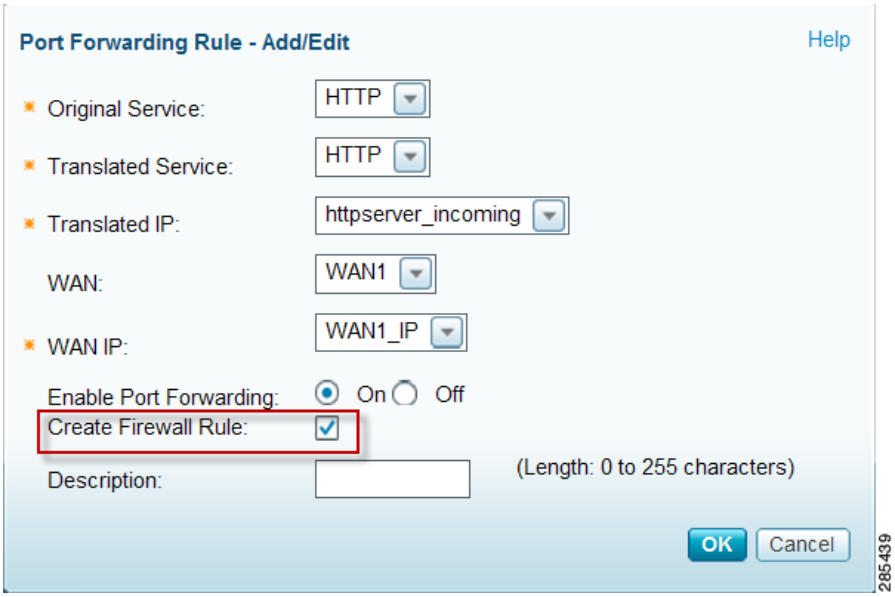
The following examples show different configurations of autogenerated rules. In each configuration, a rule is automatically generated by clicking the **Create Firewall Rule** box.

- ACL Generated by Using Port Forwarding
- ACL Generated by a Site-to-Site IPsec VPN
- ACL Generated by Remote Access IPsec VPN

NOTE You cannot edit or delete an autogenerated rule. You can only override it by creating a custom firewall rule. See Custom Firewall Rules, page 5.

ACL Generated by Using Port Forwarding

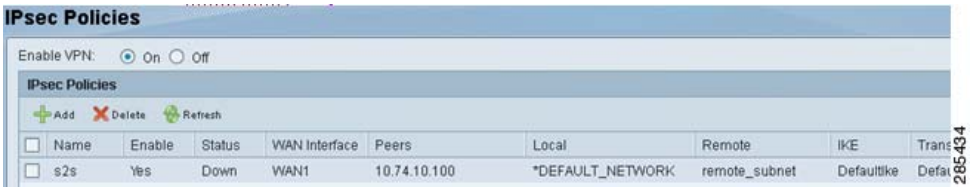
In this example, a new port forwarding rule was added from the **Firewall > NAT > Port Forwarding** page.



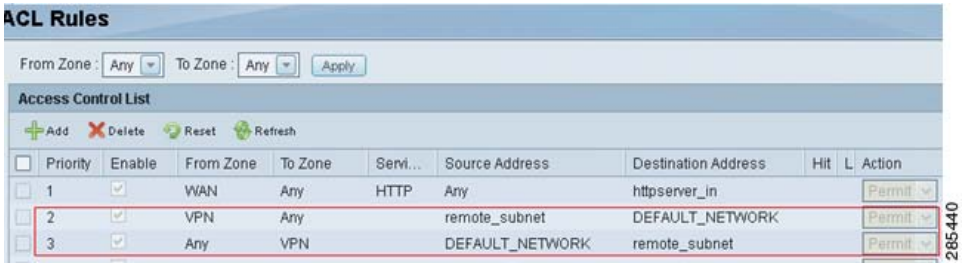
By clicking the Create Firewall Rule box, the ACL rule was automatically created to allow access from the Internet to the internal server.

ACL Generated by a Site-to-Site IPsec VPN

In this example, a site-to-site VPN was enabled for an existing IPsec Policy (**VPN > Site-to-Site > IPsec Policies**).

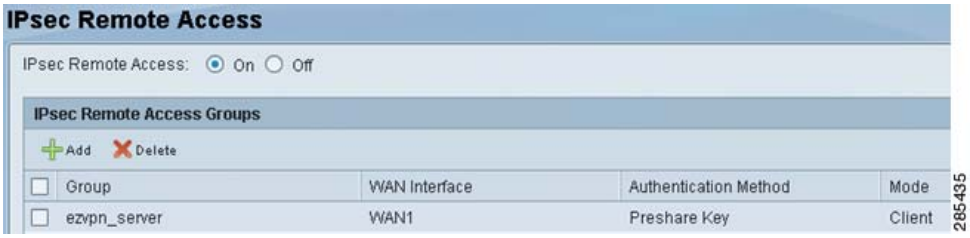


ACL rules were automatically generated to allow site-to-site VPN access.

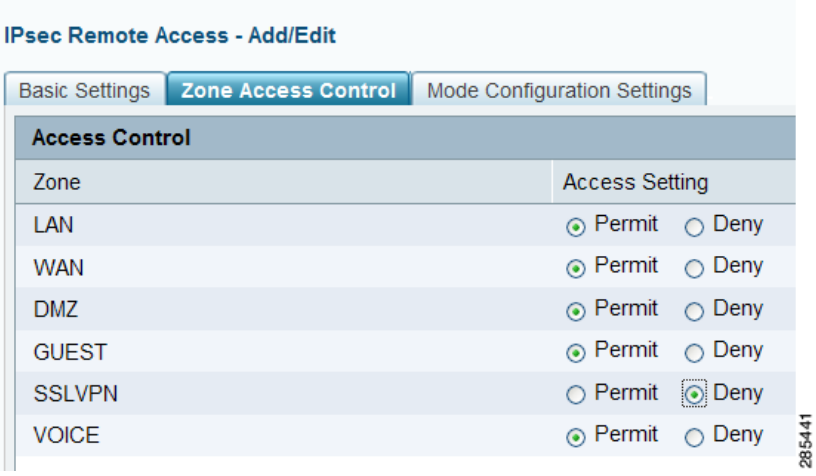


ACL Generated by Remote Access IPsec VPN

In this example, IPsec remote access was enabled to allow remote VPN clients to establish the VPN connections.



The access control settings were specified on the Basic Settings page.



The VPN ACLs for remote client access were automatically generated and added to the Access Control List.

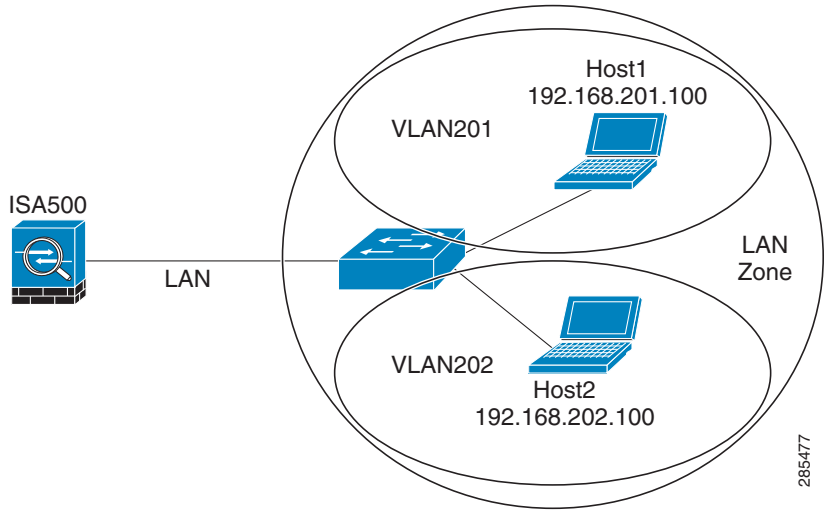
Intrazone ACL Rules

Intrazone ACL rules (ACLs between VLANs in a zone) are supported by the ISA500. These are two examples:

- Two different VLANs in the same zone. See Figure 1.
- SSLVPN-to-SSLVPN: You can create a VPN to VPN ACL rule to deny access between two ezVPN clients (the default is permit) or two SSL VPN/L2TP clients.

NOTE IntraVLAN ACLs or ACLs within a VLAN are not supported.

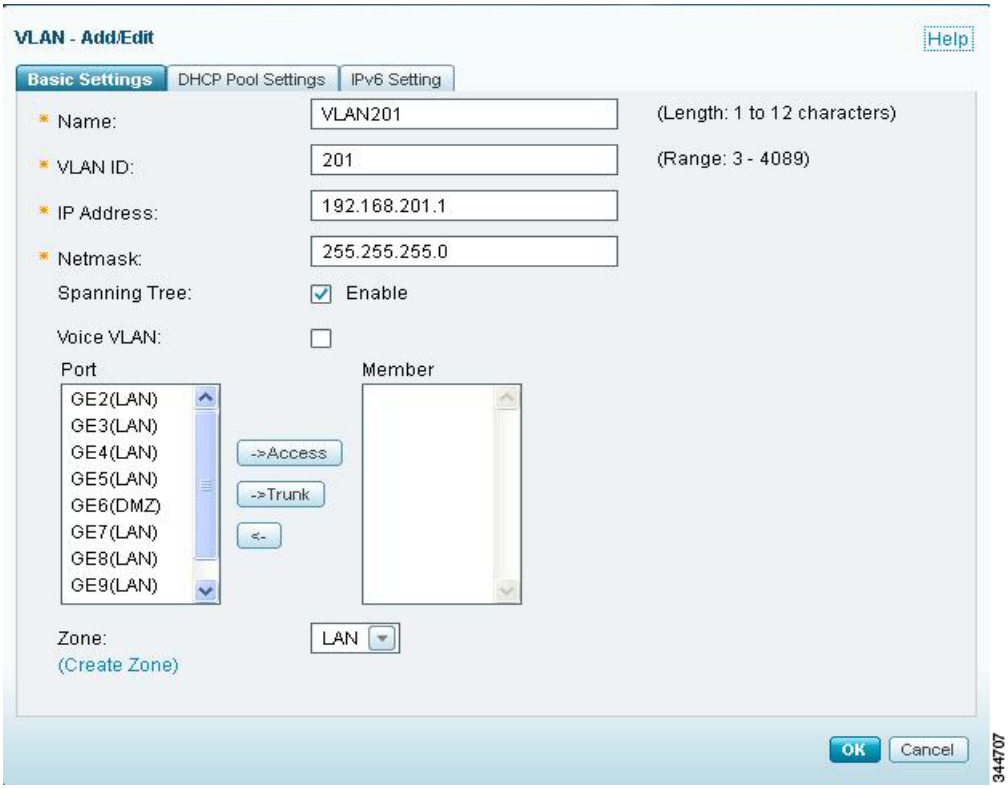
Figure 1 Example of an IntrazoneTopology

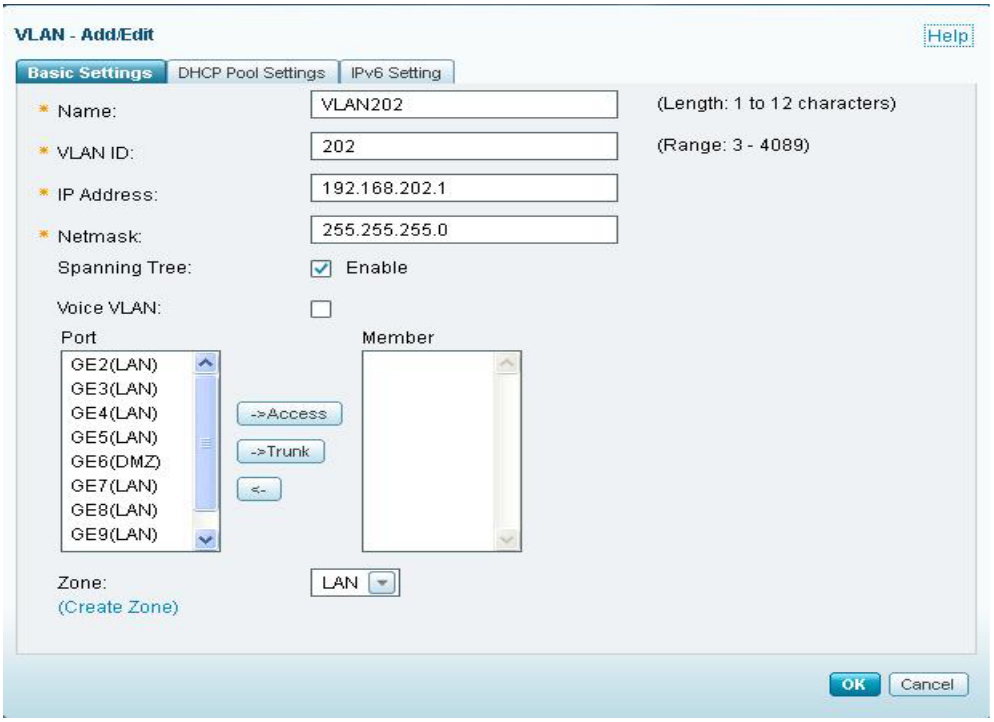


Scenario. The switch has two VLANs: VLAN201 and VLAN202. You want to deny traffic from VLAN202 to VLAN201 but allow traffic from VLAN201 to VLAN202.

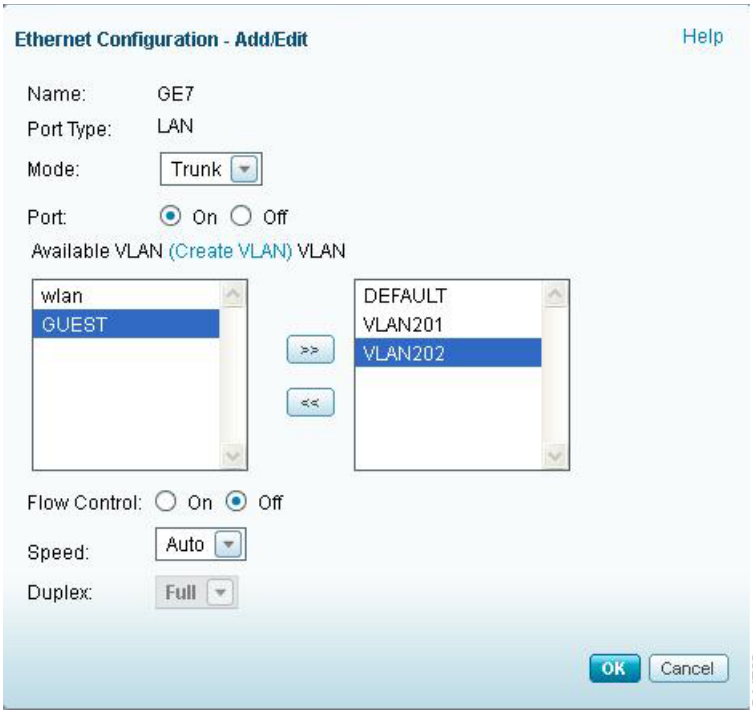
Solution.

Step 1. From the **Firewall > NAT > VLAN** page, add two new VLANs (VLAN201 and VLAN202) and assign them both to the LAN zone.

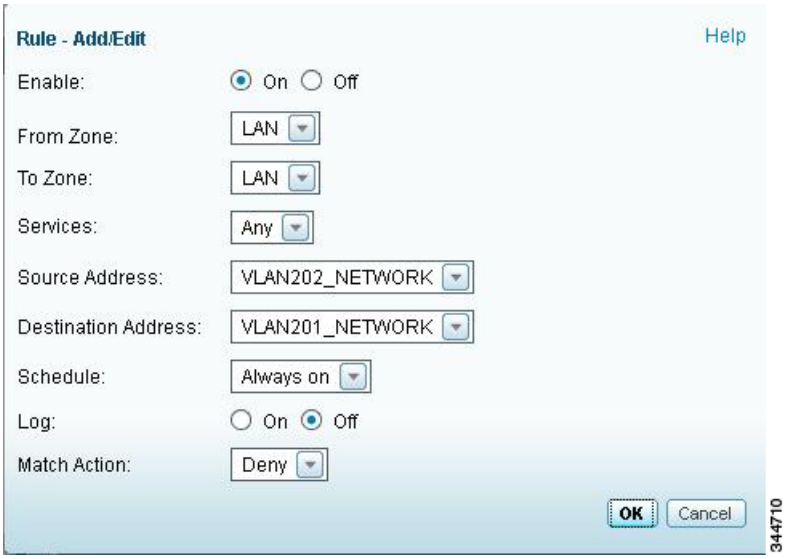




Step 2. Choose **Networking > Ports > Physical Interface** and set the LAN port to **Trunk** mode (for example: GE7). Then assign the VLAN to the port.



Step 3. Choose **Firewall > Access Control > ACL Rules**. Add a rule to block (Deny) traffic from VLAN202 to VLAN201.



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

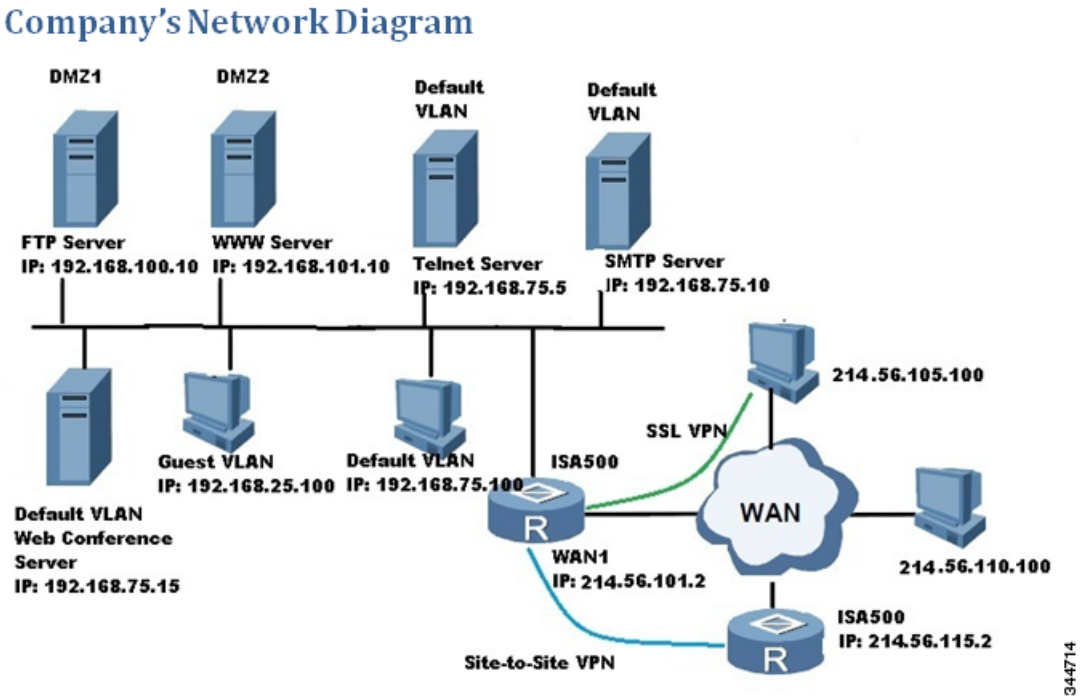
NOTE You do not need to create a rule to permit traffic. Intrazone traffic is permitted by default.

ACL Rules Case Study

The following case study describes how ACLs might be used in a company network to permit or deny access to their network. Figure 2 shows the company network diagram with following details:

- The company accesses the Internet through the WAN1 interface.
- Employees are connected to the Default VLAN network, which is a highly secured Intranet.
- The Telnet server (192.168.75.5), SMTP server (192.168.75.10), and Web Conference server (192.168.75.15) are all hosted on the Default VLAN network, whose access is only restricted to the company employees in the Default VLAN.
- The FTP server (192.168.100.10) and Web server (192.168.101.10) are hosted on the DMZ network that can be accessed by any user on the less secured networks, such as the Internet.
- The FTP and Web servers are hosted on the DMZ network. Non-employees can connect to the Guest VLAN (192.168.25.0). Any non-employees visiting the company can be added to the Guest network who have access to the Internet and DMZ network, but not to the company Intranet (Default VLAN).
- A site-to-site tunnel exists between an ISA500 with WAN IP address (214.56.101.2) and another ISA500 with WAN IP address (214.56.115.2) so that the remote office can securely connect to the main office.
- The company has a branch office physically away from the main office. Employees in the branch office can connect to the company's network on a secured site-to-site VPN connection.
- Employees (such as 214.56.105.100) can connect to the company from their home or from any hot-spots by using AnyConnect (SSL VPN) or the Cisco VPN (IPsec VPN) client.

Figure 2 Company's Network Diagram



How Default ACL Rules are Applied to the Company Network

The following sections describe the behavior of the default ACL rules. These rules are created by default.

Default VLAN Network ACL Policies

- Access to network resources such as Telnet, SMTP, and Web Conference Servers from any other network is denied.
- The host (192.168.75.100) on the Default VLAN can access the network resources on other networks such as the Internet, DMZ, Guest VLAN, and so forth.

Guest VLAN Network ACL Policies

- The host (192.168.25.100) on the Guest VLAN can access network resources on the less secured networks such as the WAN and DMZ.
- The host (192.168.25.100) on the Guest VLAN is unable to access the network resources on the more secured networks, such as the Default VLAN.

DMZ Network Access Policies

- The host on the WAN (214.56.110.100) cannot access the services hosted on the DMZ network. In this case, you must change the default ACL rules to allow the hosts on the less secured networks to access the DMZ network services.
- The FTP server and Web server cannot initiate connections to the high security Default VLAN network.

WAN Network Access Policies

- The hosts on the company networks (192.168.75.100, 192.168.25.100, Web, FTP, SMTP, Web Conference and Telnet servers) are allowed access to the Internet.
- The hosts on the Internet (214.56.110.100 and 238.56.105.100) are denied access to the company networks.

Configuring ACL Policies

The company's network administrator needs to change some of default ACL rules to allow access to certain network hosts or services from the less secure networks, and to deny access to certain network hosts or services from the more secure networks to the less secure services.

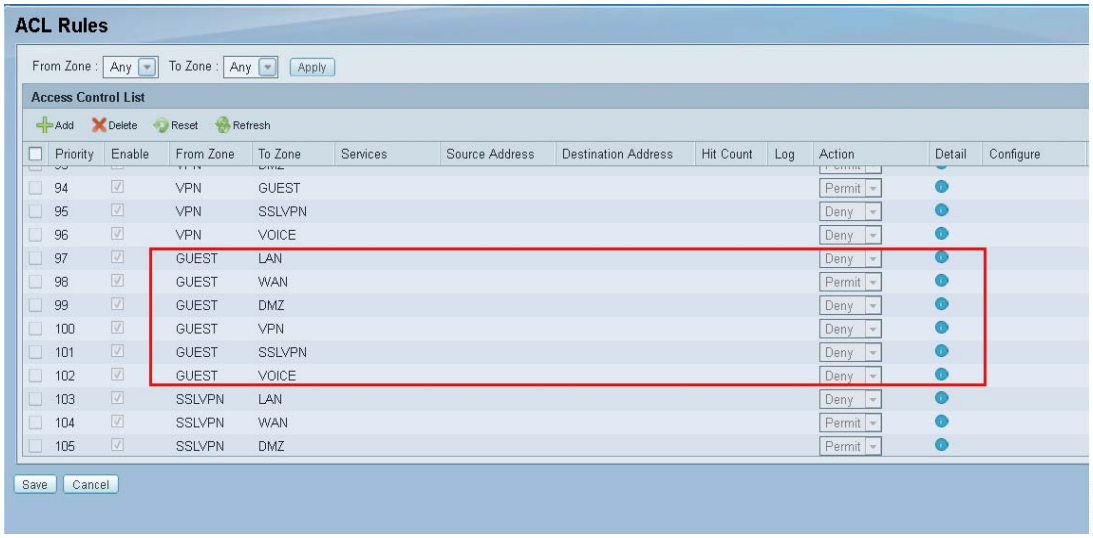
In this example, the network administrator must configure the following ACL policies to override the default policies to make the company network fully functional.

Default VLAN ACL Settings

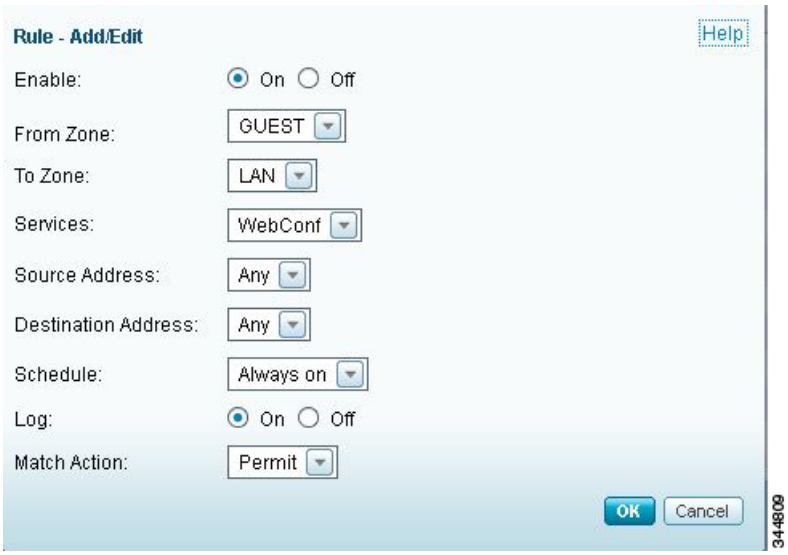
The company wants to allow the hosts on the Default VLAN to access the Internet, DMZ, Guest VLAN, and VPN endpoints, but wants to deny access to the DMZ and Guest and Internet access to the default VLAN. In this case, the default ACL rules will remain as-is.

Guest VLAN ACL Settings

Hosts in the Guest VLAN (192.168.25.100) can only access the WAN network as shown here. However, the company wants the Guest VLAN host to access the Web Conference services hosted on the server in Default VLAN network.



To allow the Guest VLAN host access, a new rule was created from the **Firewall > Access Control > ACL Rules > Rule- Add/Edit** page.



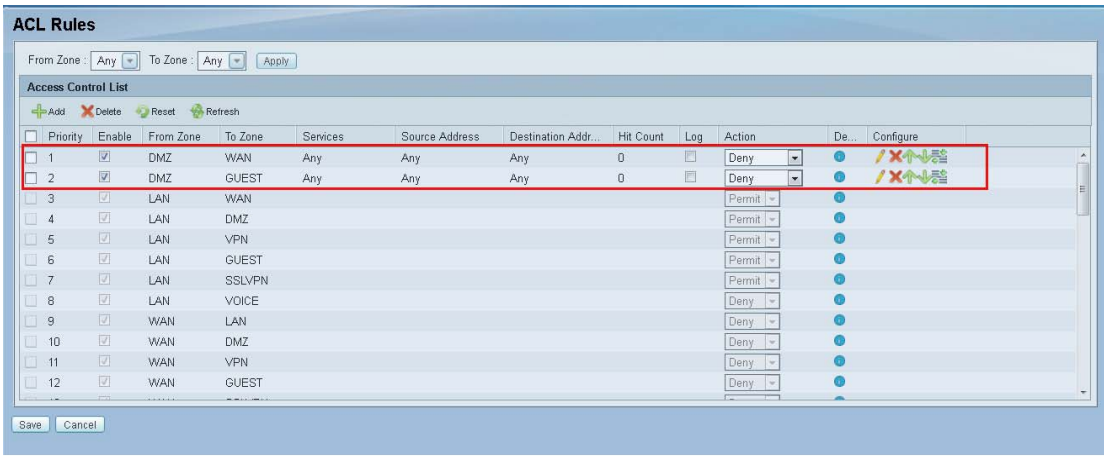
The new rule was successfully added and appears on the ACL Rules page.

DMZ ACL Settings

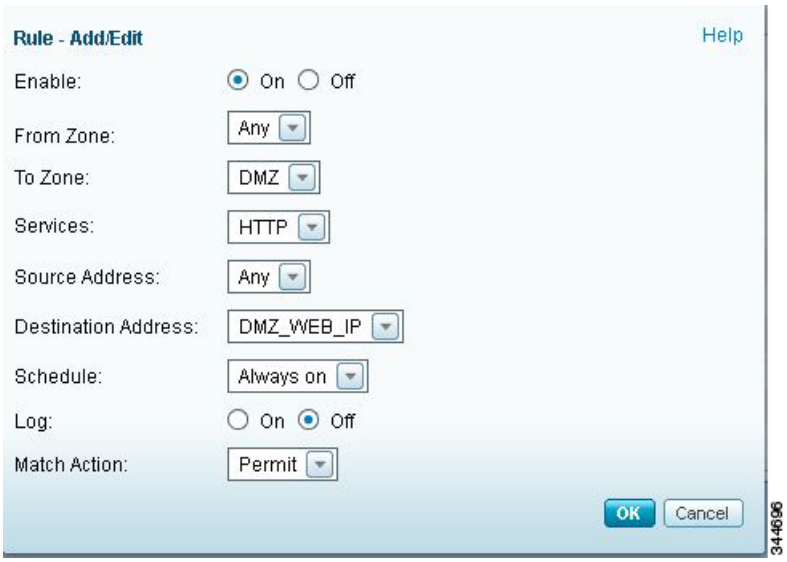
The company wants to host the FTP and Web servers on the DMZ network. It does not want any host on the DMZ network to access to any other networks for network resources.

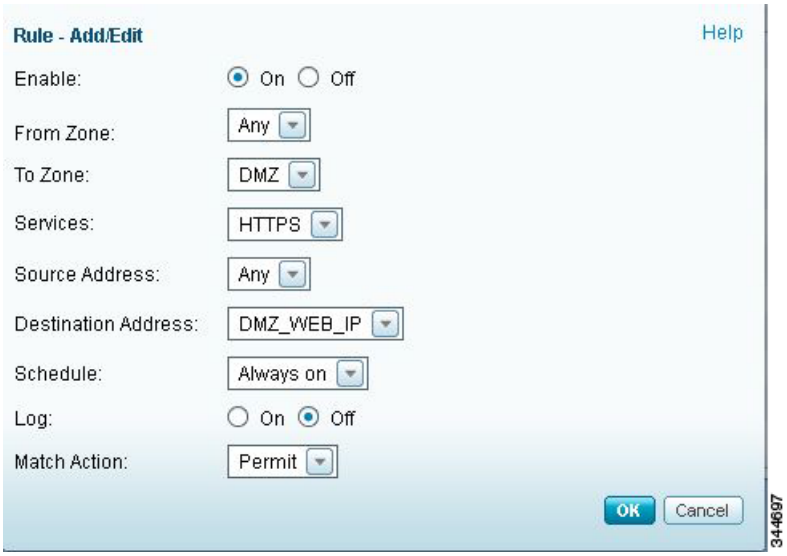
The default DMZ ACL rules are shown here.

In this example, the Administrator changed the DMZ ALC rules to deny access to all the networks from DMZ.

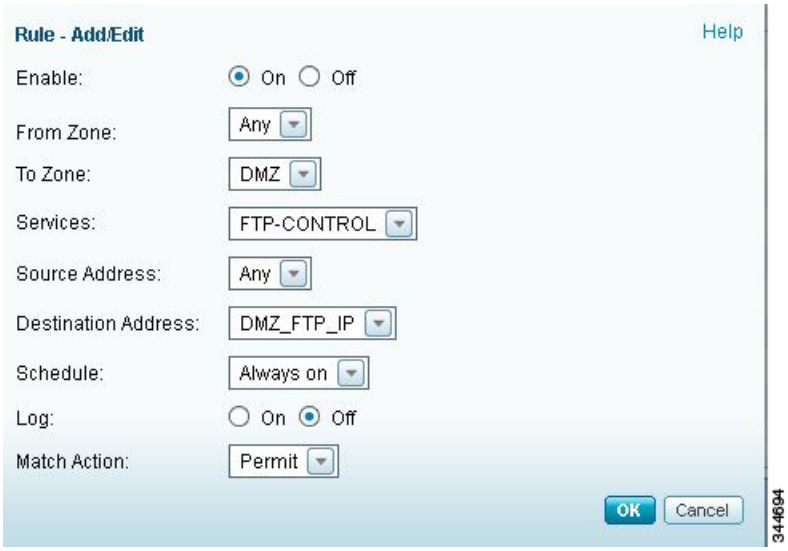


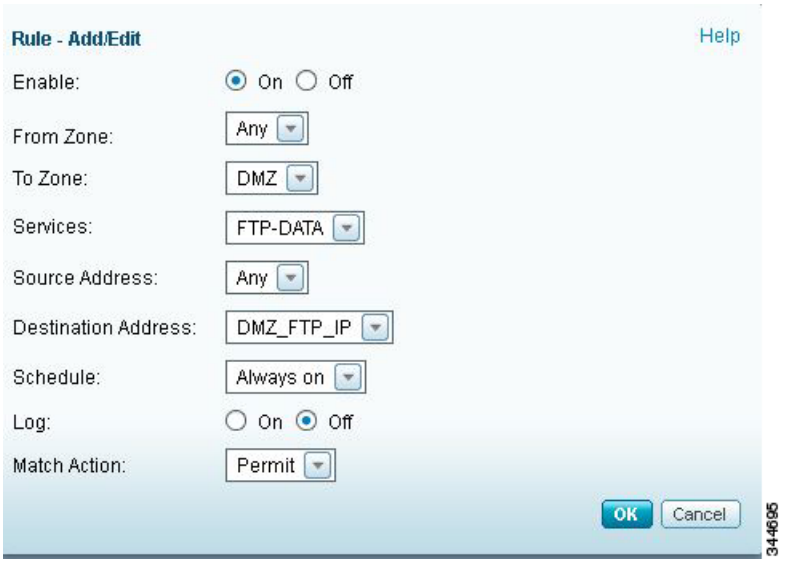
Two ACL rules were added to permit the host on any network to access the HTTP and HTTPS services on the Web server (192.168.101.10). In this example, the Destination Address **DMZ_WEB_IP** is the address object for the Web server address (192.168.101.10).



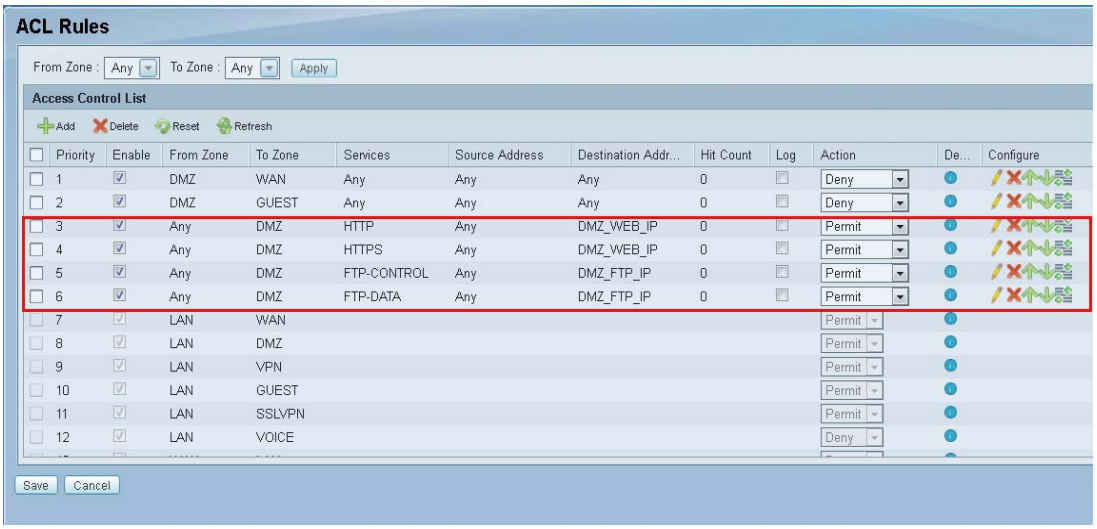


Two more rules were added to permit hosts on any network to access the FTP server (192.168.100.10) and to permit FTP control and FTP data ports on the FTP server.





The newly configured DMZ ACL rules are shown here.

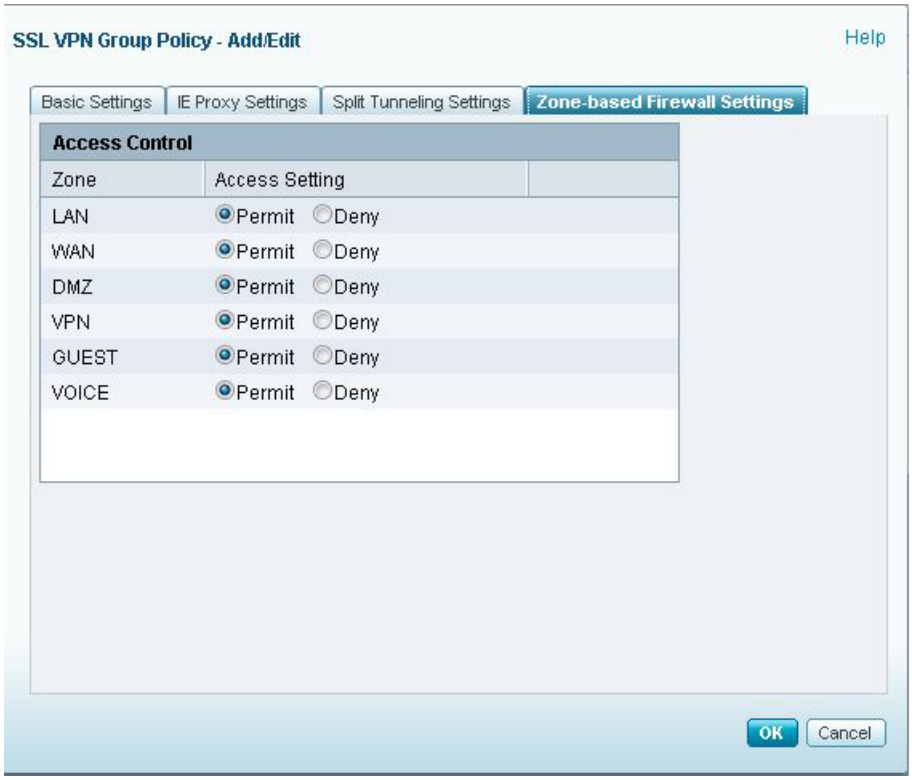


WAN ACL Settings

By default, access from the hosts on the WAN to any subnet in the company network is denied, however the company allows the host on the Internet to access the FTP and Web servers on the DMZ. These rules were already configured in the previous section (see DMZ ACL Settings, page 17), so no changes to the WAN ACL settings are required.

SSL VPN ACL Settings

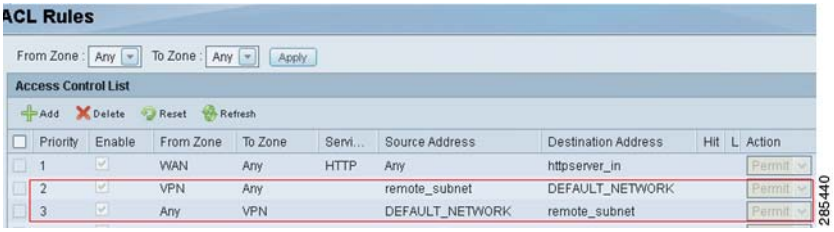
By default, remote access users are permitted to access all the available networks. If needed, you can change the permissions from the Zone-based Firewall Settings tab on the SSL VPN Group Policy page as shown here.



The ACL rules for each SSL VPN session are automatically generated when the session is established.

Site-to-Site ACL Settings

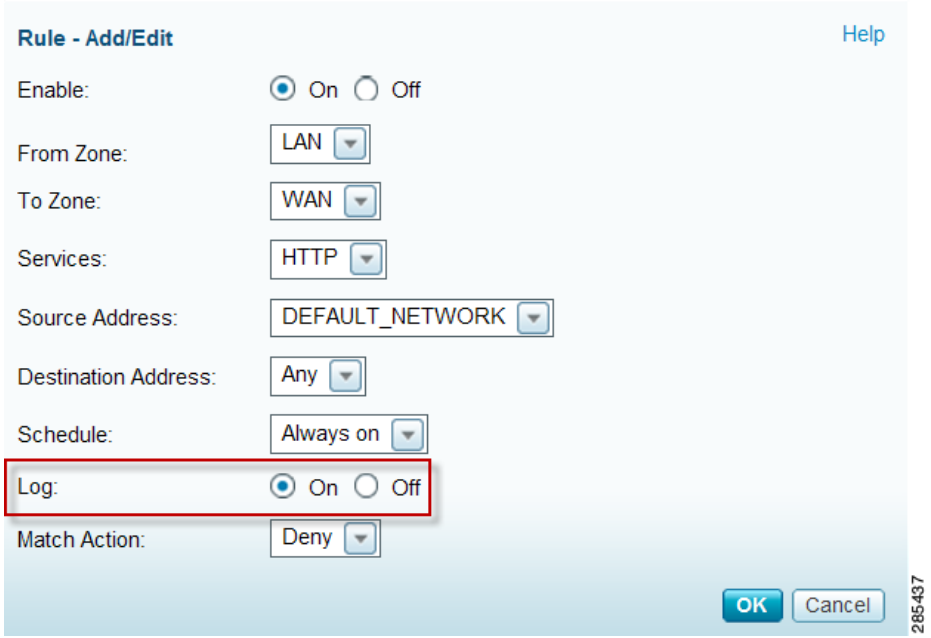
ACL rules for site-to-site VPN are automatically generated when the IPSec tunnel is established between the ISA500 in the main office (214.56.101.2) and the ISA500 in the branch office (214.56.115.2).



ACL rules permit any host on the Default VLAN (192.168.75.0) in the main office to access hosts on the subnet in the branch office and vice versa (The local network and remote network settings are configured on the **VPN > Site-to-Site > IPsec Policies** page). After the IPSec tunnel is established, any host on the chosen DEFAULT_VLAN (192.168.75.0 in the example) can access any host in remote_network on the other side of tunnel.

Troubleshooting

When you create a rule, you can log the firewall events by enabling logging (**Firewall > Access Control > ACL Rules**). These logs can be used for troubleshooting and for tracking potential security threats. A variety of events can be captured and logged for review.



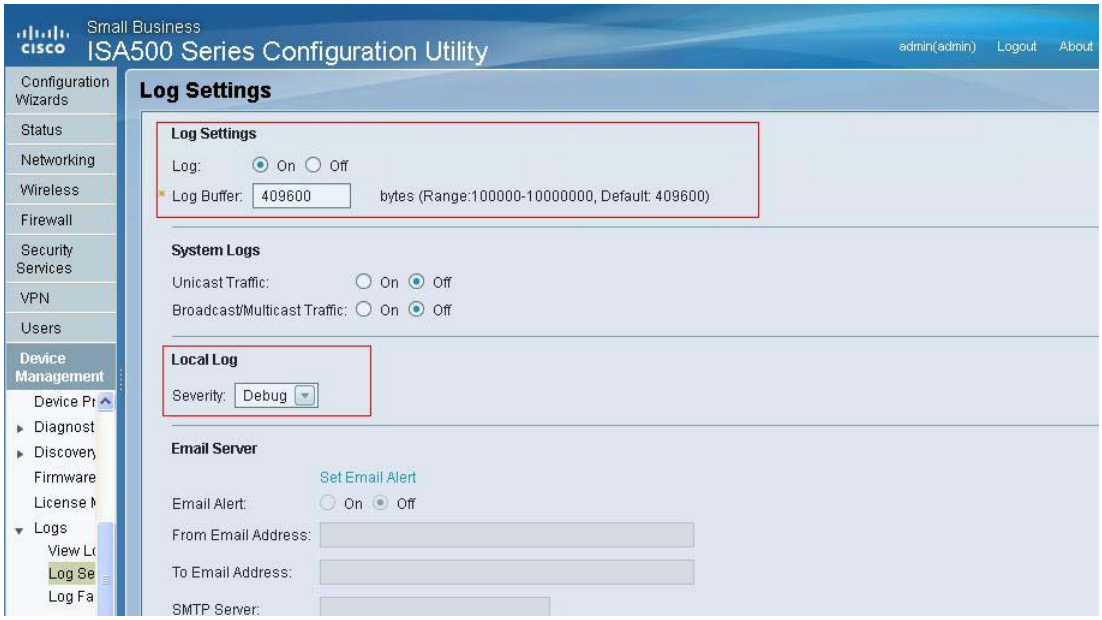
To view the log information, select **Device Management > Logs > View Logs**. This example shows the log information for the firewall rule we just created.

Troubleshooting Example

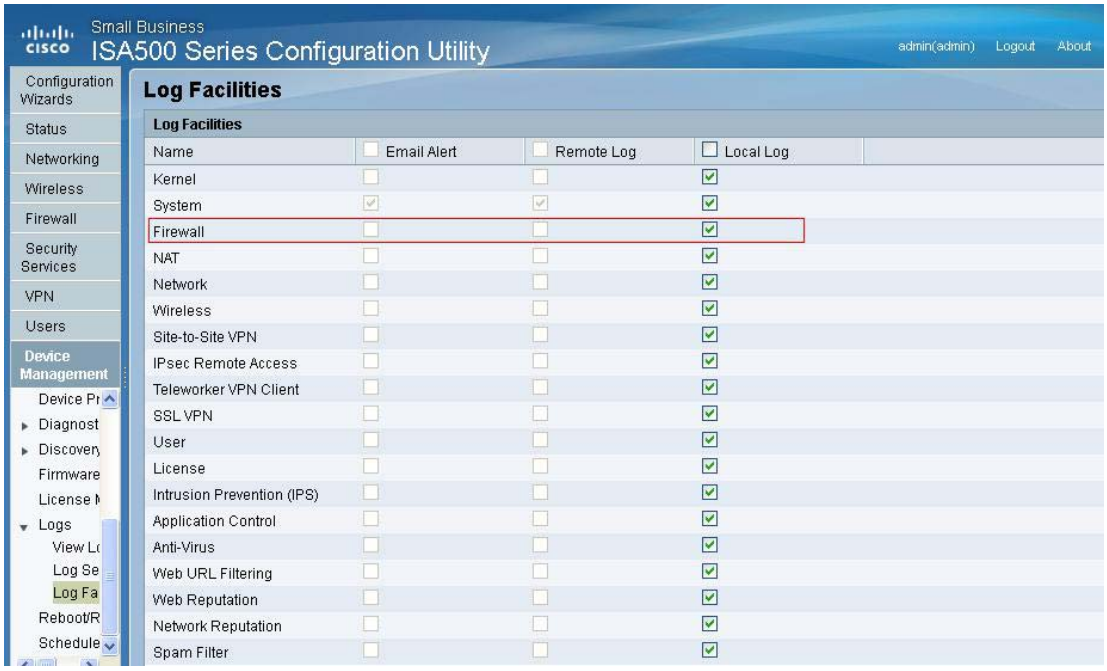
A user on the network (identified as 192.168.75.101 in the default VLAN) is unable to access an external FTP server (10.74.10.194). To isolate the problem, enable firewall logging on the ISA500 as follows:

Step 1. Choose **Device Management > Logs > Log Settings**.

Step 2. Under Log Settings, click **On** to enable logging.



Step 3. Choose **Device Management > Logs > Log Facilities**.

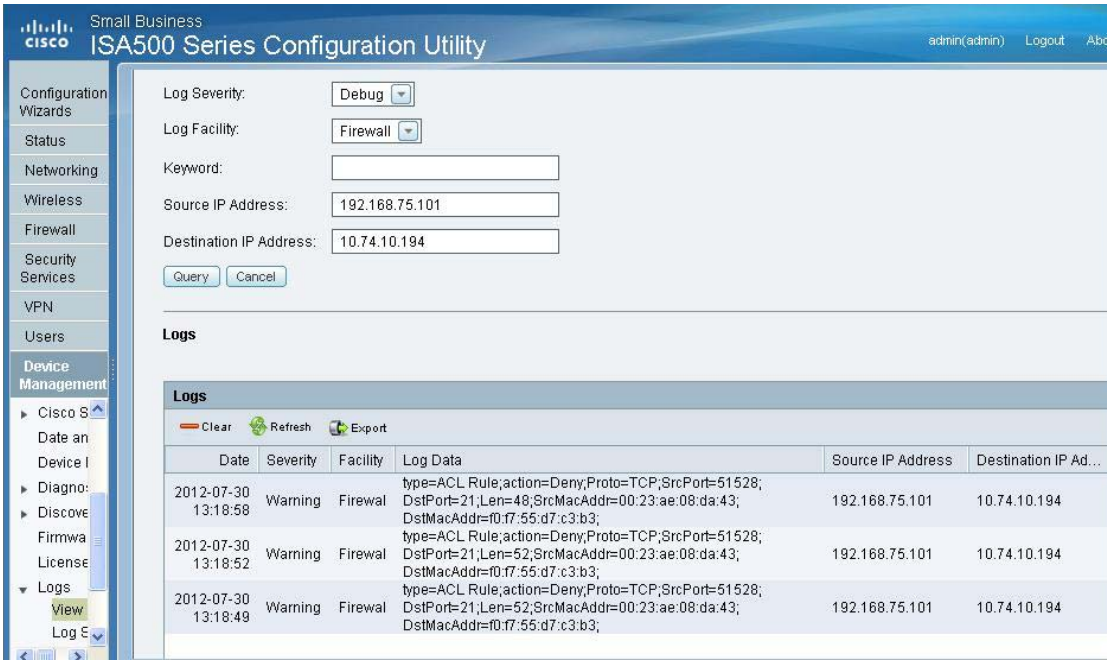


Step 4. Check **Local Log** next to the Firewall Log Facility.

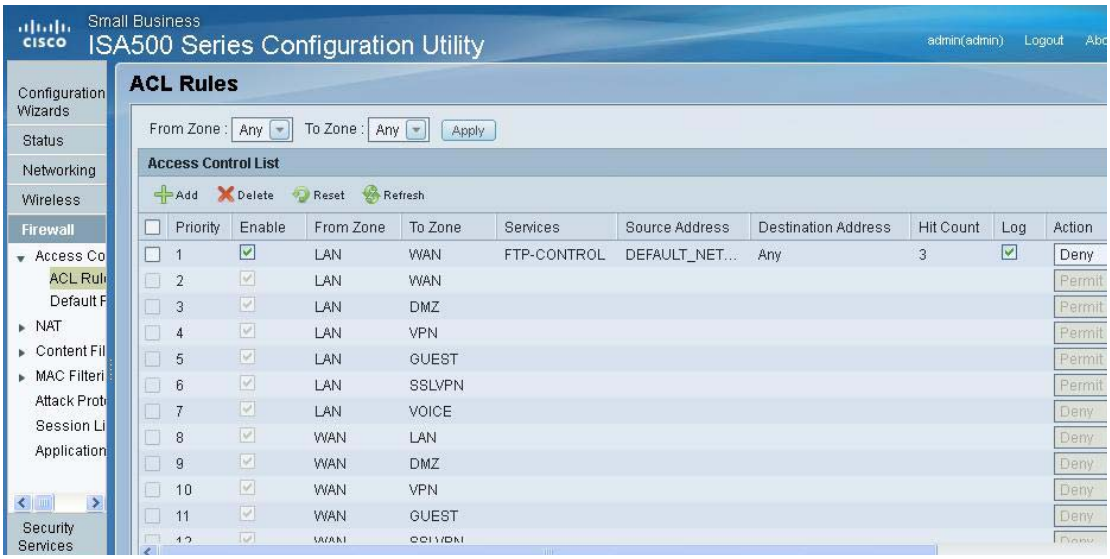
Step 5. Click **Save**.

Step 6. Initiate the FTP connection again. If the connection fails, view the firewall log from the from the **Device Management > Logs > View Logs** page.

Step 7. Specify the source IP address and destination IP address and click the **Query** button. In this example, the log indicates that the FTP connection (DstPort=21) is blocked by an ACL rule.



Step 8. To isolate the problem, choose **Firewall > Access Control > ACL Rules** to view the list of rules. As shown here, the FTP ACL is set to Deny.

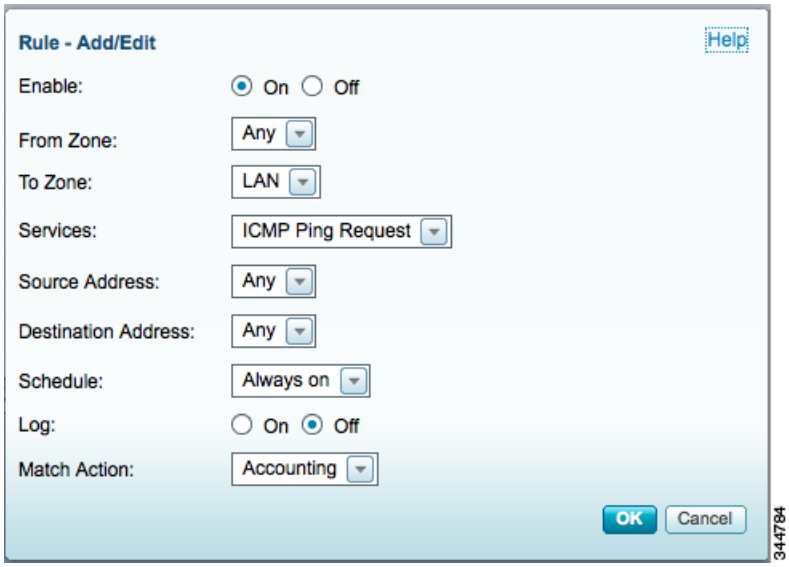


Step 9. Change Deny to Permit and click **Save**.

Firewall Accounting

You can check if a certain packet matches the ACL rule by creating an ACL Rule (**Firewall > Access Control > ACL Rules**) with **Match Action** set to **Accounting**. This option increases the hit count number by one when it hits the firewall rule. Accounting does not deny or permit traffic. It only checks the number of times that a rule is matched.

This example shows an ACL rule configured to check traffic originating from Any zone to the LAN interface.



After you configure the rule, you can view its hit count on the ACL page. This page shows the log data for the rule that you just created.

For More Information

Product Resources	Location
Product Documentation	www.cisco.com/go/isa500resources
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
Firmware Downloads	www.cisco.com/go/isa500software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb