

Application Note

Cisco Router and Security Device Manager for **Cisco IOS Firewall**

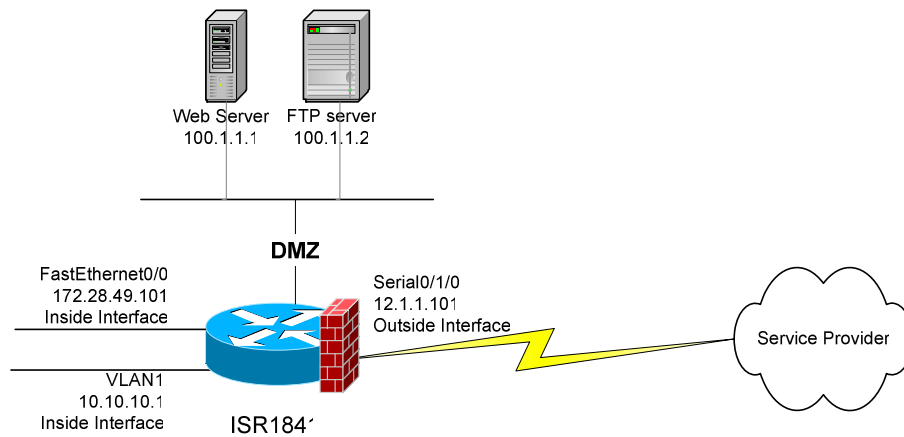
Introduction

Security administrators can easily and quickly configure and manage [Cisco IOS® Firewall](#) through a graphical and intuitive Firewall Wizard, Firewall Policy table and Application Security features available with Cisco® Router and Security Device Manager (SDM).

Deployment Scenario

Figure 1 shows the deployment of a branch-office Internet firewall. The Cisco IOS Firewall resides in a branch office, with the outside (Serial0/1/0) interface connected to the service provider via the serial connection, the inside (FastEthernet0/1) interface connected to the DMZ, and the inside (Fast Ethernet0/0 and VLAN1) interfaces connected to the branch-office private subnets.

Figure 1 Branch Office Internet Firewall Deployment Scenario



The deployment involves two steps: advanced firewall configuration including DMZ and Application Firewall configuration, and branch office-specific configuration.

Branch Office Internet Firewall Sample Configuration

Branch Office-Specific Firewall Configuration

The first step is to allow specific protocols that will be used in this deployment scenario. The protocols allowed on the branch office firewall are Telnet, and SMTP for both outside and inside traffic. Inspect the traffic from the branch-office subnets and the traffic from the Internet.

Cisco SDM Firewall Support

Cisco SDM allows users to easily configure Cisco IOS Firewall security features. The following steps are used to configure the same deployment scenario, using Cisco SDM as opposed to the Cisco IOS Software CLI.



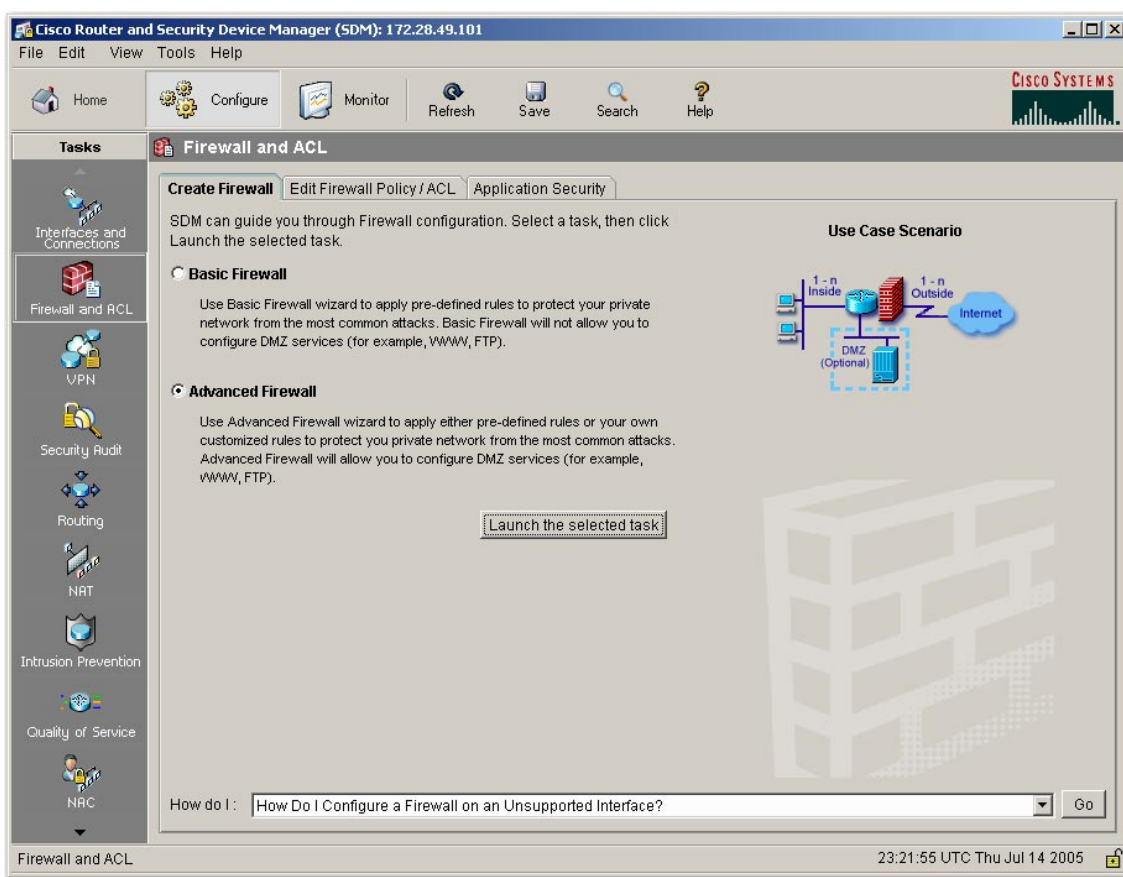
Advanced Firewall Configuration

The Cisco SDM Advanced Firewall Wizard can secure the branch office by using predefined rules or customized rules to protect the private networks and the DMZ zone from the most common attacks.

The Advanced Firewall Wizard allows you to secure your private network in the following ways: it allows private network users to access the Internet; it protects your router and private networks from outside attacks; it allows you to configure managed services in demilitarized zone (DMZ) that are accessible from the Internet. The Advanced Firewall Wizard applies access rules to the inside (trusted), outside (untrusted) and DMZ interfaces, applies inspection rules to the inside, and DMZ interfaces, and enables IP unicast reverse-path forwarding on the outside interfaces.

At **Configure Mode**, select the **Firewall and ACL** and then click **Create Firewall** tab to launch **Advanced Firewall** wizard (Figure 2).

Figure 2 Cisco SDM Firewall Wizard

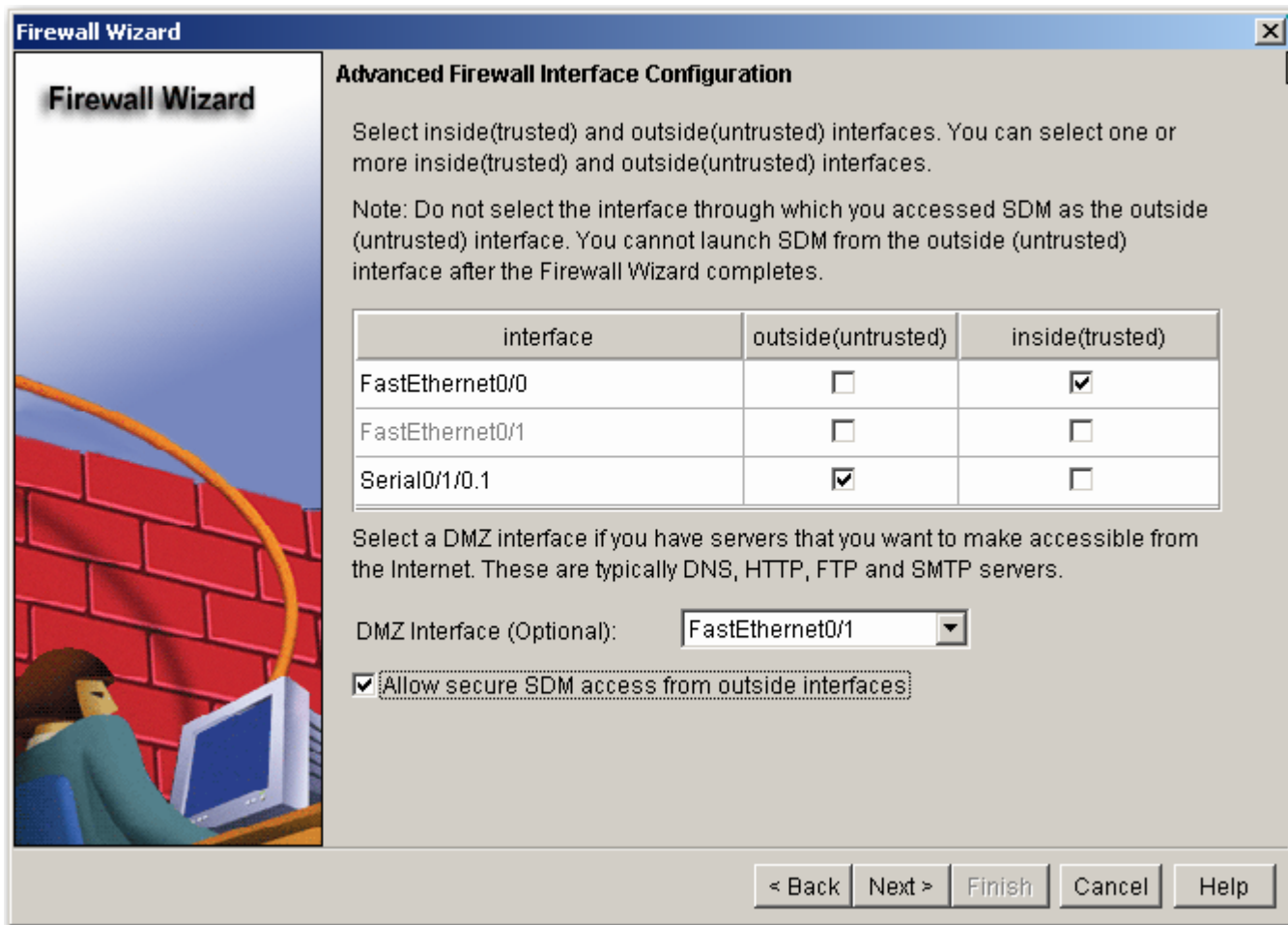




The Firewall Wizard (Figure 3) guides you through the advanced firewall configuration.

In this scenario, select **FastEthernet0/1** as the DMZ Interface, select **Serial0/1/0.1** as the outside interface, and select **FastEthernet0/0** as the inside interface, secure SDM access from outside interfaces is also allowed, click **Next**

Figure 3 Advanced Firewall Interface Configuration

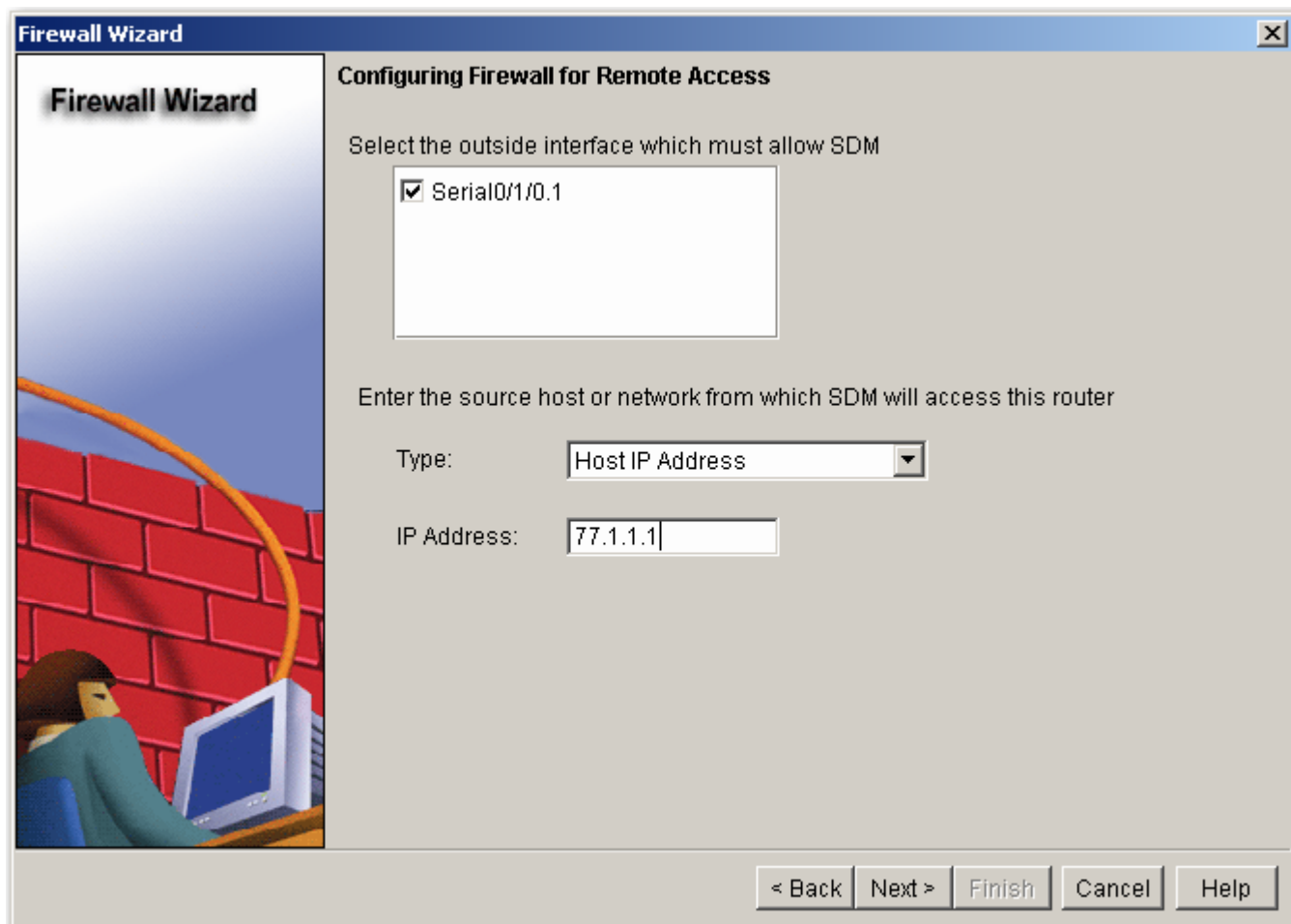


(Note: **Allow secure SDM access from outside interfaces** will be disabled if the following conditions are met: 1. When HTTPS or SSH secure communication is not enabled on the router, or 2. None of the outside interfaces is configured with a static IP address)

For SDM remote access, specify the outside interfaces to use for remote management access and the hosts from which administrators can log on to SDM to manage the router (Figure 4). In this scenario, SDM detects one outside interface, Serial0/1/0.1, select **Serial0/1/0.1** and select Type: **Host IP Address**, IP Address: **77.1.1.1**, click **Next**



Figure 4 Firewall Secure RSDM Access configuration



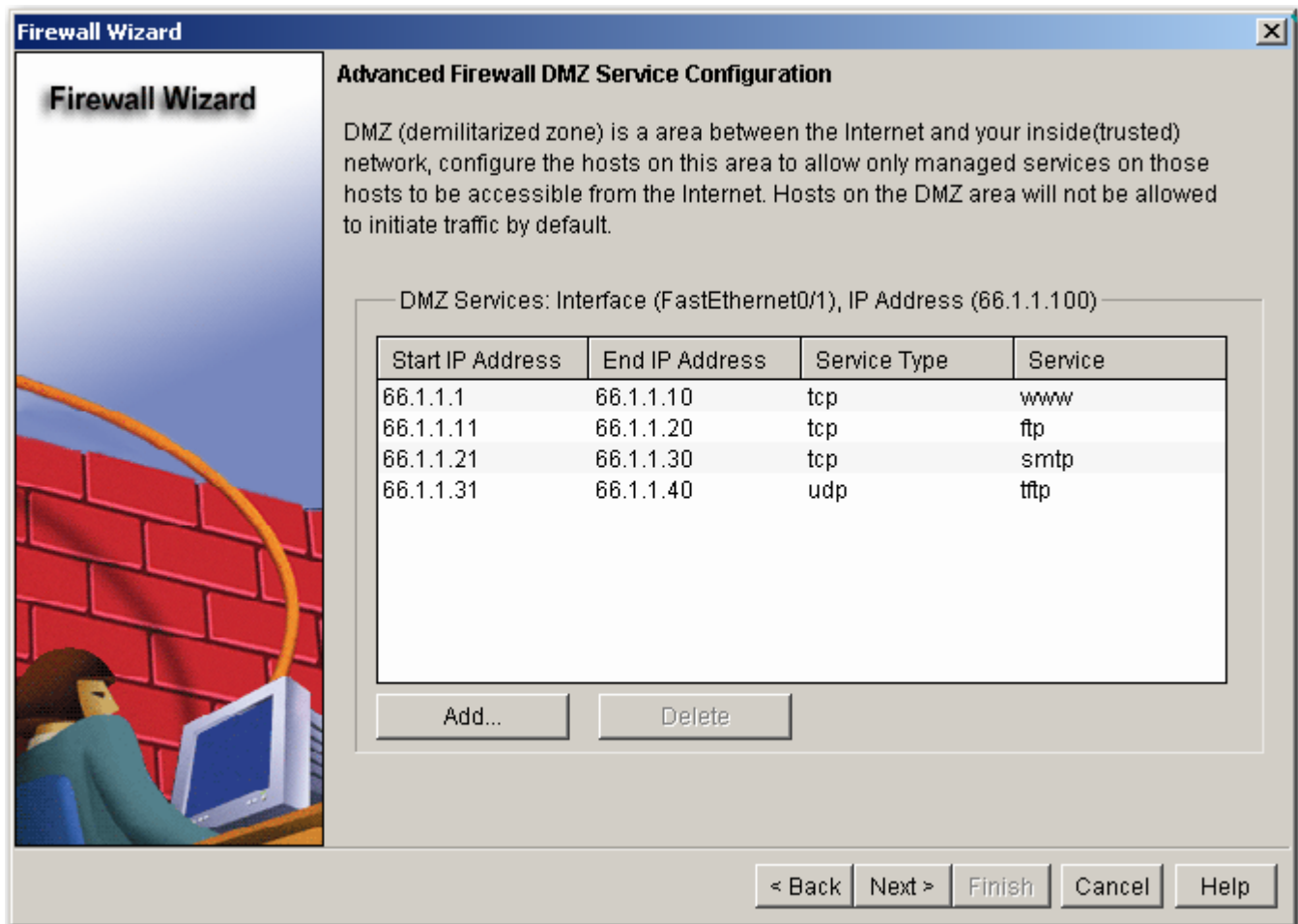
For DMZ Service Configuration (Figure 5), add the IP ranges and allowed protocols, in this scenario, we configured following IP ranges and protocols allowed in DMZ zone:

- o 66.1.1.1 – 66.1.1.10 for tcp/www
- o 66.1.1.11 – 66.1.1.20 for tcp/ftp
- o 66.1.1.21 – 66.1.1.30 for tcp/smtp
- o 66.1.1.31 – 66.1.1.40 for udp/ftp

click Next



Figure 5 DMZ Service Configuration

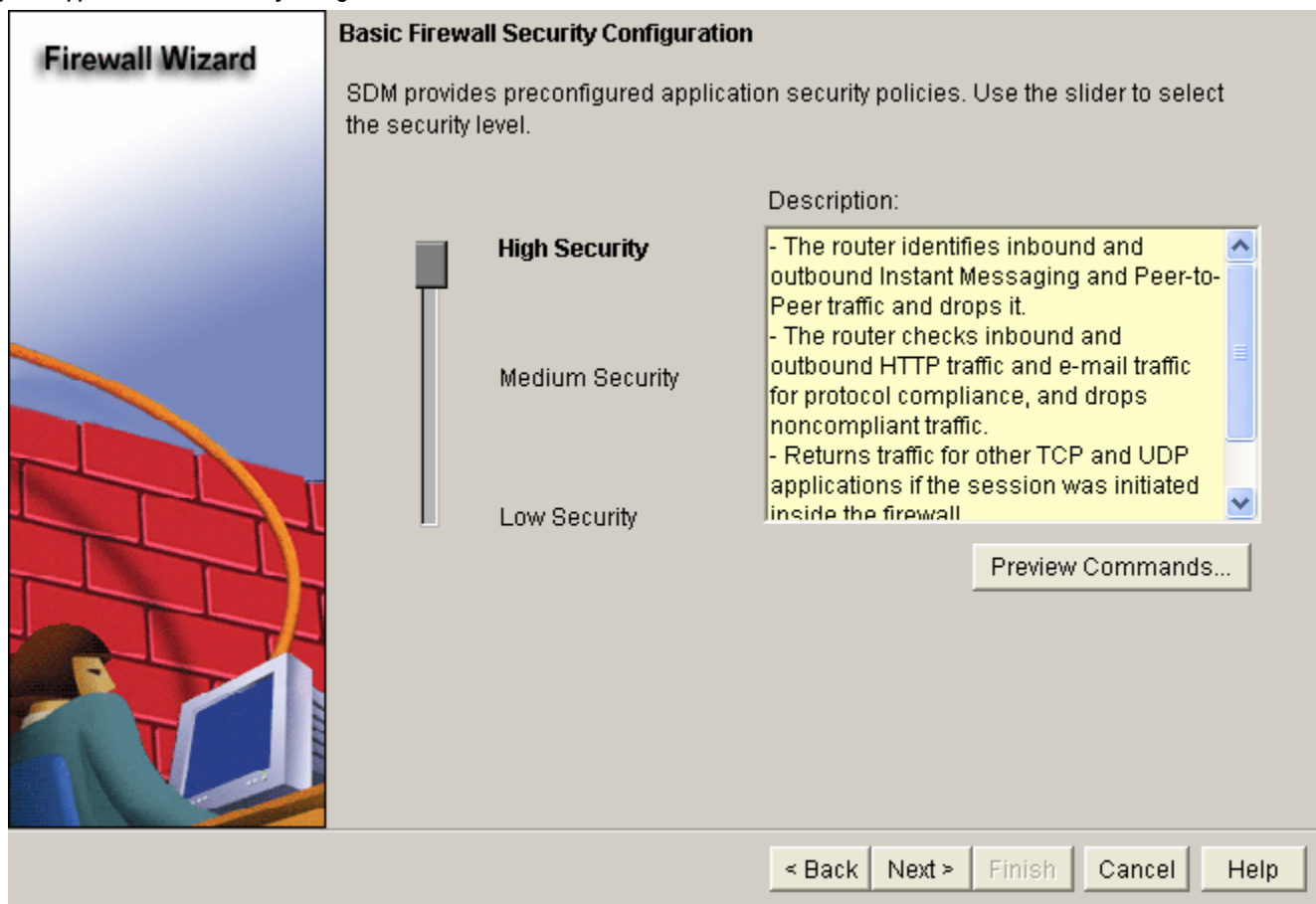


For Advanced Firewall Security Configuration (Figure 6), SDM provides preconfigured application security policies, High Security, Medium Security and Low Security, that you can use to protect the network, or you can create your own policies. In this scenario, select **Use a default SDM Application Security Policy with High Security**, and click **Preview Commands** to browse the details. Click **Next**

High Security	<ul style="list-style-type: none"> - The router identifies inbound and outbound Instant Messaging and Peer-to-Peer traffic and drops it. - The router checks inbound and outbound HTTP traffic and e-mail traffic for protocol compliance, and drops noncompliant traffic. - Return traffic for other TCP and UDP applications is routed if the session was initiated inside the firewall
Medium Security	<ul style="list-style-type: none"> - The router identifies inbound and outbound Instant Messaging and Peer-to-Peer traffic and checks inbound and outbound HTTP traffic and e-mail traffic for protocol compliance - Return TCP and UDP traffic on sessions initiated inside the firewall is routed
Low Security	<ul style="list-style-type: none"> - The router does not identify application-specific traffic. Return TCP and UDP traffic on sessions initiated inside the firewall is routed.



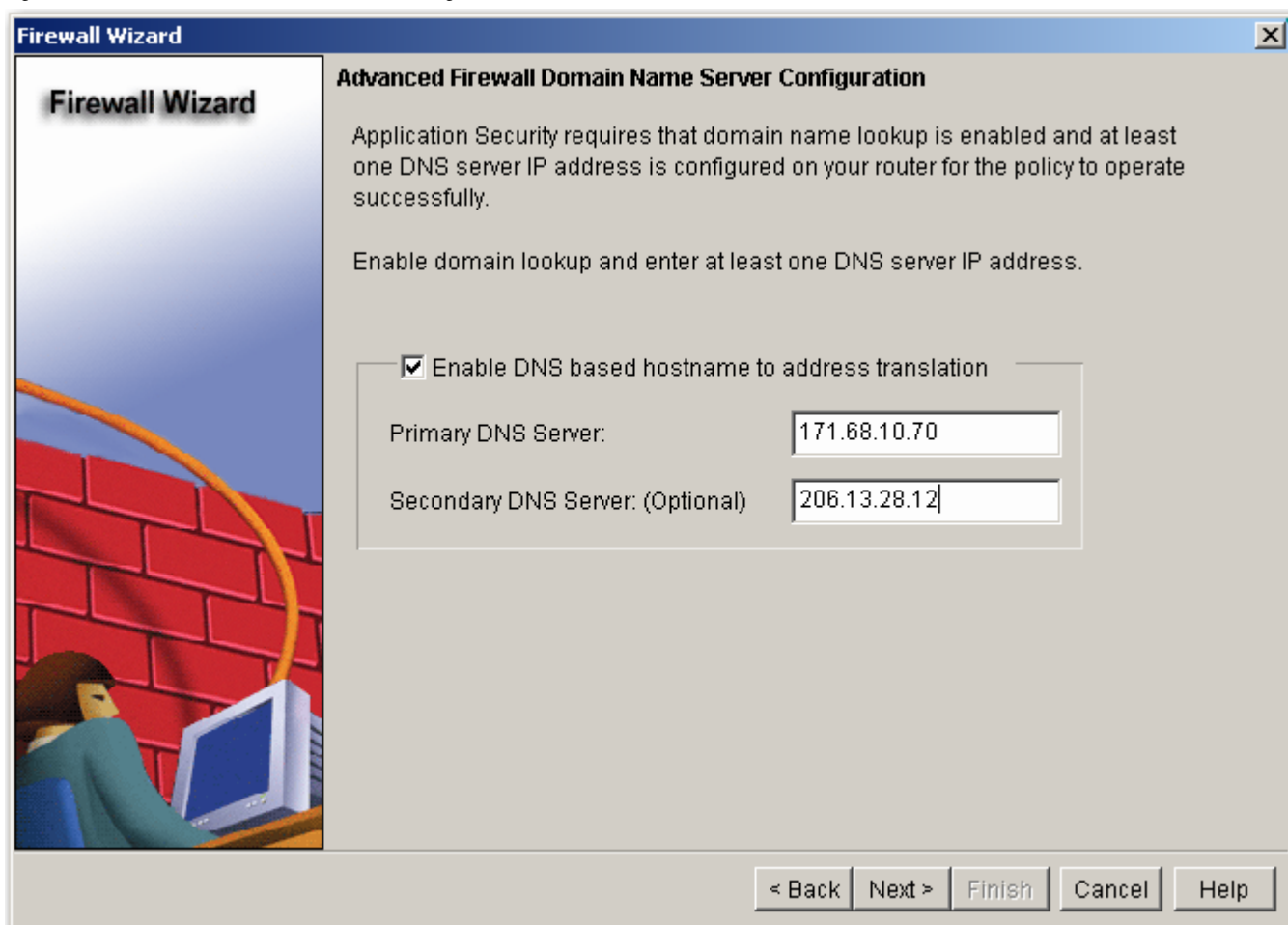
Figure 6 Application Firewall Policy Configuration



For Advanced Firewall Domain Name Server, Application Security requires that domain name lookup be enabled and at least one DNS server be configured (Figure 7). Primary DNS Server: **171.68.10.70**, Secondary DNS Server: (Optional) **206.13.28.12**, click **Next**.



Figure 7 Advanced Firewall Domain Name Server Configuration



When the summary window is displayed, view the configuration and click **Finish** to deliver the configuration, click **OK** to continue. You will be redirected to **Firewall Policy/ACL** page (Figure 8).

Figure 8 depicts the traffic originating from the branch-office inside network to DMZ zone are filtered by Access List 100 and inspected by the inspection rule SDM_HIGH.



Figure 8 Traffic from inside network (FastEthernet0/0) to DMZ zone (FastEthernet0/1)

The screenshot shows the Cisco SDM Firewall and ACL configuration page. The main configuration area is titled "Firewall and ACL" and includes a diagram of traffic flow between FastEthernet0/0 and FastEthernet0/1. The diagram shows originating traffic from FastEthernet0/0 to FastEthernet0/1 and returning traffic from FastEthernet0/1 to FastEthernet0/0. The configuration is for an IOS Firewall, Active (from FastEthernet0/0 to FastEthernet0/1).

Firewall Feature Availability: Available Access Rule: 100 Inspection Rule: SDM HIGH

Action	Source	Destination	Service	Log	Option	Description
Deny	11.1.1.0/0.0.0.255	any	IP ip			
Deny	66.1.1.0/0.0.0.255	any	IP ip			
Deny	255.255.255.255	any	IP ip			
Deny	127.0.0.0/0.255.2	any	IP ip			
Permit	any	any	IP ip			

Application Protocol	Description
Application Security	View/Edit Application Security
icmp	ICMP Protocol
dns	Domain Name Server

Apply Changes Discard Changes

Configuration delivered to router. 19:06:33 UTC Wed Sep 14 2005

Once the firewall is configured by the advanced firewall wizard, use the Cisco SDM/Firewall and ACL/Edit Firewall Policy/ACL page to display and alter the firewall configuration further if desired, and use the Cisco SDM/Firewall and ACL/Application Security page to view the details of inspection rules.



Cisco SDM Firewall Policy Table

The Cisco SDM Firewall Policy table displays the access rights for a particular traffic flow and the inspection rules on a particular interface.

Figure 9 depicts the traffic originating from the branch-office inside network to Internet filtered by Access List 100 and inspected by the inspection rule SDM_HIGH.

Figure 9 Traffic originated from inside network (FastEthernet0/0) to Internet (Serial0/1/0.1)

Firewall and ACL Configuration

From: FastEthernet0/0 To: Serial0/1/0.1

IOS Firewall : Active (from FastEthernet0/0 to Serial0/1/0.1)

Firewall Feature Availability: Available Access Rule: 100 Inspection Rule: SDM_HIGH

Action	Source	Destination	Service	Log	Option	Description
Deny	11.1.1.0/0.0.0.255	any	IP	ip		
Deny	66.1.1.0/0.0.0.255	any	IP	ip		
Deny	255.255.255.255	any	IP	ip		
Deny	127.0.0.0/0.255.2	any	IP	ip		
Permit	any	any	IP	ip		

Application Protocol	Description
Application Security	View/Edit Application Security
icmp	ICMP Protocol
dns	Domain Name Server

Apply Changes Discard Changes

19:17:58 UTC Wed Sep 14 2005



The Cisco SDM Firewall Policy table also displays the returning traffic via the **Returning traffic** radio button. Figure 10 shows the returned traffic from the Internet that enters the Cisco IOS Firewall outside (Serial0/1/0.1) interface. Inspection rule, SDM_HIGH, ensures the returned traffic is not blocked by Access Rule 102.

Figure 10 Returned Traffic

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface for configuring a Firewall Policy / ACL. The configuration is for traffic from FastEthernet0/0 to Serial0/1/0.1. The "Returning traffic" radio button is selected. The "IOS Firewall" is active from FastEthernet0/0 to Serial0/1/0.1. The "Access Rule" is 102 and the "Inspection Rule" is SDM_HIGH.

Services Table:

Action	Source	Destination	Service	Log	Option	Description
Deny	66.1.1.0/0.0.0.255	any	ip			ip
Deny	172.28.49.96/0.0.	any	ip			ip
Permit	any	11.1.1.100	echo-reply/icmp			echo-reply/icmp
Permit	any	11.1.1.100	time-exceeder/icmp			time-exceeder/icmp
Permit	any	11.1.1.100	unreachable/icmp			unreachable/icmp
Permit	77.1.1.1	11.1.1.100	dest:443/tcp			dest:443/tcp

Applications Table:

Application Protocol	Description
Application Security	View/Edit Application Security
icmp	ICMP Protocol
dns	Domain Name Server



Figure 11 shows the traffic originated from the Internet enter the Cisco IOS Firewall DMZ (FastEthernet0/1) interface. Access List 102 is used to filter the traffic, and the Inspection Rule dmzinspect inspects the traffic sent to the DMZ (FastEthernet0/1).

Figure 11 Traffic originated from Internet (Serial0/1/0.1) to DMZ zone (FastEthernet0/1)

Action	Source	Destination	Service	Log	Option	Description
Deny	66.1.1.0/0.0.0.255	any	ip			
Deny	172.28.49.96/0.0.0.0	any	ip			
Permit	any	11.1.1.100	echo-reply/icmp			
Permit	any	11.1.1.100	time-exceeded/icmp			
Permit	any	11.1.1.100	unreachable/icmp			
Permit	77.1.1.1	11.1.1.100	dest: 443/tcp			

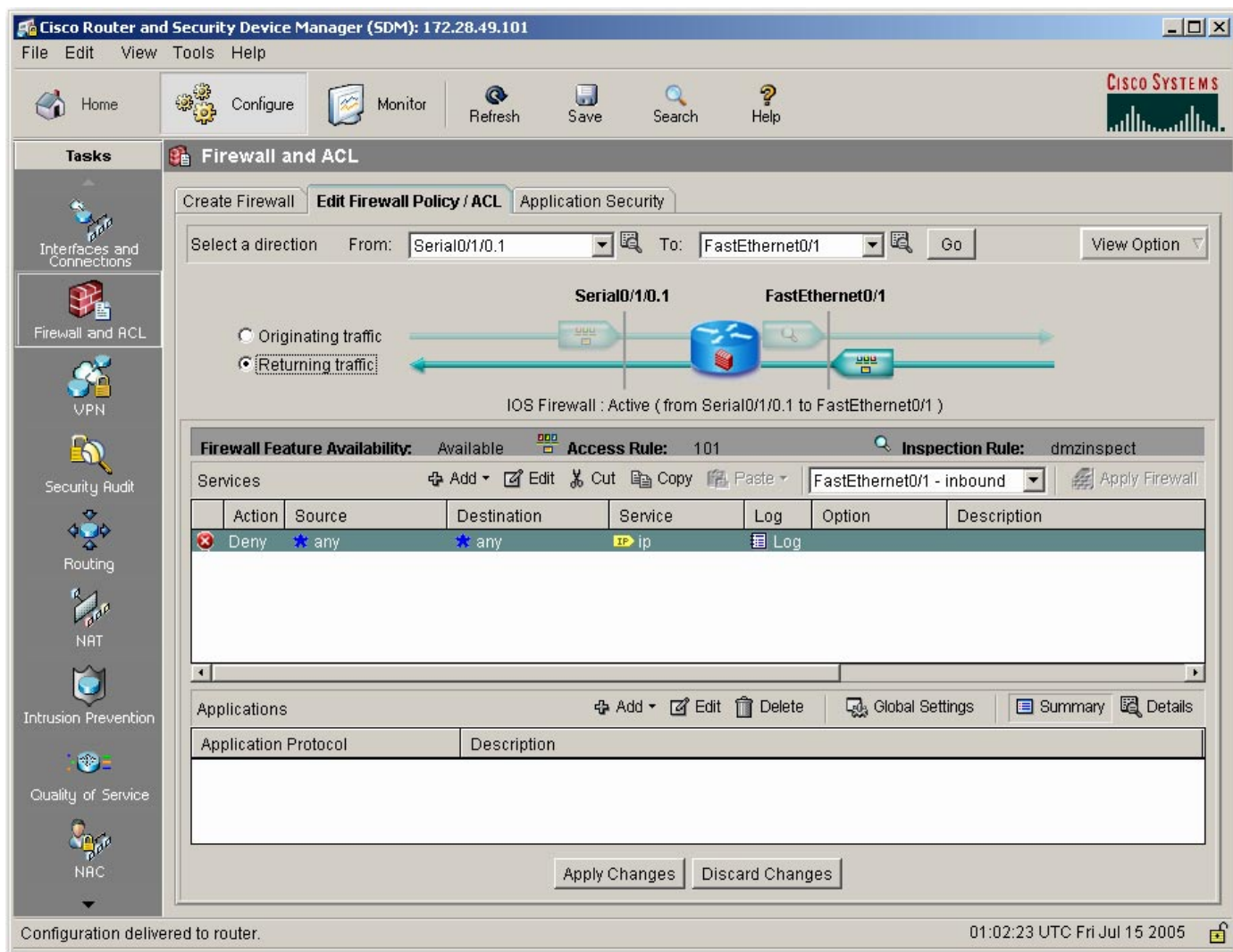
The Applications table is as follows:

Application Protocol	Description
tcp	Transmission Control Protocol
udp	User Datagram Protocol



Figure 12 shows that the returned traffic from the DMZ zone to Internet is filtered by Access list 101. The filter ensures no traffic can be originated from DMZ interface, which will prevent hackers from attacking inside hosts from the DMZ zone if the DMZ zone is compromised, and the Inspection rule, dmzinspect, ensures the returned traffic is not blocked by Access Rule 101.

Figure 12 Returned Traffic



(Note: If the servers in DMZ zone are required to access the inside hosts, users need to customize the Access list 101 to allow the traffic.)

Branch-Office Specific Firewall Configuration

The branch-office specific firewall policy allows the inside network to Telnet, FTP, and HTTP to the Internet. We have to configure the Inspection Rule to allow the return traffic. The user must merge the basic firewall configuration and the branch office-specific firewall together. Now, with the Cisco SDM Firewall Policy Table, it is simple and easy to add and merge the access entries. To use Cisco SDM Firewall Policy Table to merge access lists, take the following steps:

1. At **Configure**, select **Firewall and ACL**, click **Edit Firewall Policy/ACL**
2. Select a Direction from **FastEthernet0/1** to **Serial0/1/0.1**, then click **Go**



3. Go to Services panel
4. Click **Add**, select **Insert Before**
5. Add an Extended Rule Entry window appears
 - Action: **Permit**
 - Source Host/Network:
 - Type: **A Network**
 - IP Address: **172.28.49.100** (note: the inside network)
 - Wildcard Mask: **0.0.0.255**
 - Destination Host/Network:
 - Type: **Any IP Address**
 - Protocol and service:
 - **TCP**/Source Port Service = **telnet**
 - Destination Port Service = **telnet**
 - Uncheck Log matches against this entry
 - Click **OK** (Figure 13)

Figure 13 Add an Extended Rule Entry

The screenshot shows the 'Add an Extended Rule Entry' dialog box. The 'Action' dropdown is set to 'Deny'. The 'Description' field contains 'branch office-specific firewall policy - telnet'. The 'Source Host/Network' section has 'Type' set to 'A Network', 'IP Address' set to '172.28.49.100', and 'Wildcard Mask' set to '0.0.0.255'. The 'Destination Host/Network' section has 'Type' set to 'Any IP Address'. The 'Protocol and Service' section has 'TCP' selected, 'Source Port' set to 'any', and 'Destination Port' set to 'telnet'. The 'Log matches against this entry' checkbox is unchecked. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

6. Repeat step 4 and 5 to add FTP and HTTPS (443)
7. Click **Apply Changes** button on the center lower window to deliver the change when finish
8. Click **OK** to continue



Figure 14 shows merged Access List 100.

Figure 14 Merged Access List 100

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The main window is titled "Cisco Router and Security Device Manager (SDM): 172.28.49.100". The "Firewall and ACL" section is active, showing the configuration for Access List 100. The configuration is for an inbound policy on FastEthernet0/0, applying to traffic from 172.28.49.100/0.0 to any destination. The services table shows the following rules:

Action	Source	Destination	Service	Log	Option	Description
Permit	172.28.49.100/0.0	any	443/tcp, dest:			branch office-specific firewall policy - HTTP
Permit	172.28.49.100/0.0	any	ftp/tcp, dest: ft			branch office-specific firewall policy - FTP
Permit	172.28.49.100/0.0	any	telnet/tcp, des			branch office-specific firewall policy - telnet
Deny	11.1.1.0/0.0.0.255	any	ip			
Deny	66.1.1.0/0.0.0.255	any	ip			
Deny	255.255.255.255	any	ip			

The Applications table shows the following entries:

Application Protocol	Description
Application Security	View/Edit Application Security
icmp	ICMP Protocol
dns	Domain Name Server
esmtpt	Extended SMTP

The status bar at the bottom indicates "Configuration delivered to router." and the time is "20:05:13 UTC Wed Sep 14 2005".



Using the Firewall Policy Table to Create Inspection Rule

To create inspection rules, apply BranchFIRE inspection rule to the inbound traffic at the outside (Ethernet0) interface. Then take the following steps:

- Click **Configure**, select **Firewall and ACL**, and click **Edit firewall Policy/ACL** tab.
- Select the Direction from **Ethernet0** to **FastEthernet0**.
- Go to the **Application** panel.
- Click **Add**, select **Add...**
- Fill in the information and click **OK**.

In the Inspection Rule Editor (Figure 15), the Inspection Rule Name is **BranchFIRE**. Check Protocols **tcp** and **udp**.

Figure 15 Inspection Rule Editor

Protocol	Alert	Audit Trail	Timeout(sec):
<input type="checkbox"/> icmp	default(on)	default(off)	10
<input type="checkbox"/> netshow	default(on)	default(off)	3600
<input type="checkbox"/> rcmd	default(on)	default(off)	3600
<input type="checkbox"/> realaudio	default(on)	default(off)	3600
<input type="checkbox"/> rpc	default(on)	default(off)	30
<input type="checkbox"/> rtsp	default(on)	default(off)	3600
<input type="checkbox"/> sip	default(on)	default(off)	30
<input type="checkbox"/> skinny	default(on)	default(off)	3600
<input type="checkbox"/> smtp	default(on)	default(off)	3600
<input type="checkbox"/> sqlnet	default(on)	default(off)	3600
<input type="checkbox"/> streamworks	default(on)	default(off)	30
<input checked="" type="checkbox"/> tcp	default(on)	default(off)	3600
<input type="checkbox"/> tftp	default(on)	default(off)	30
<input checked="" type="checkbox"/> udp	default(on)	default(off)	30
<input type="checkbox"/> vdolive	default(on)	default(off)	3600

Option...

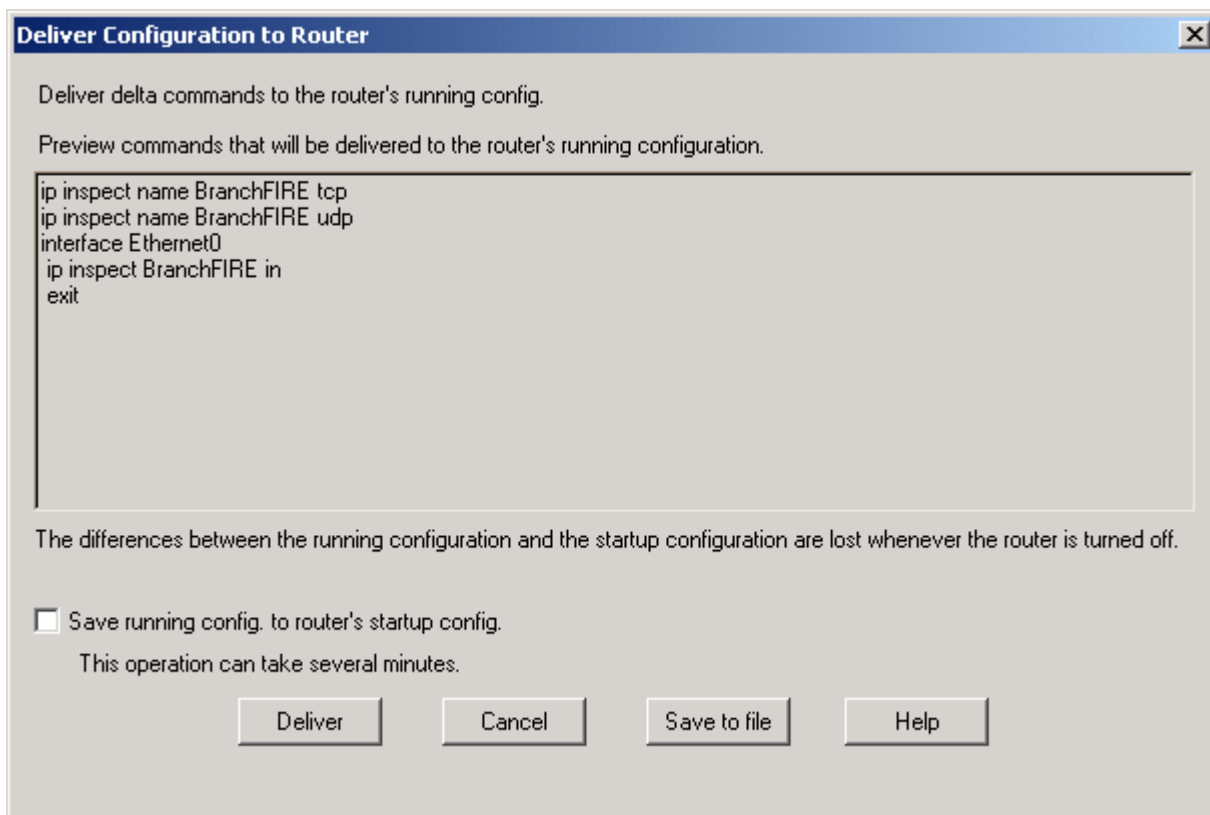
Insert additional RPC protocol entries

OK Cancel Help



Deliver the changes to the router (Figure 16). Click **Deliver**.

Figure 16 Cisco IOS Software CLI Commands Generated by Cisco SDM Firewall Policy Table



Application Security

Cisco SDM supports configuring following Cisco IOS Firewall features:

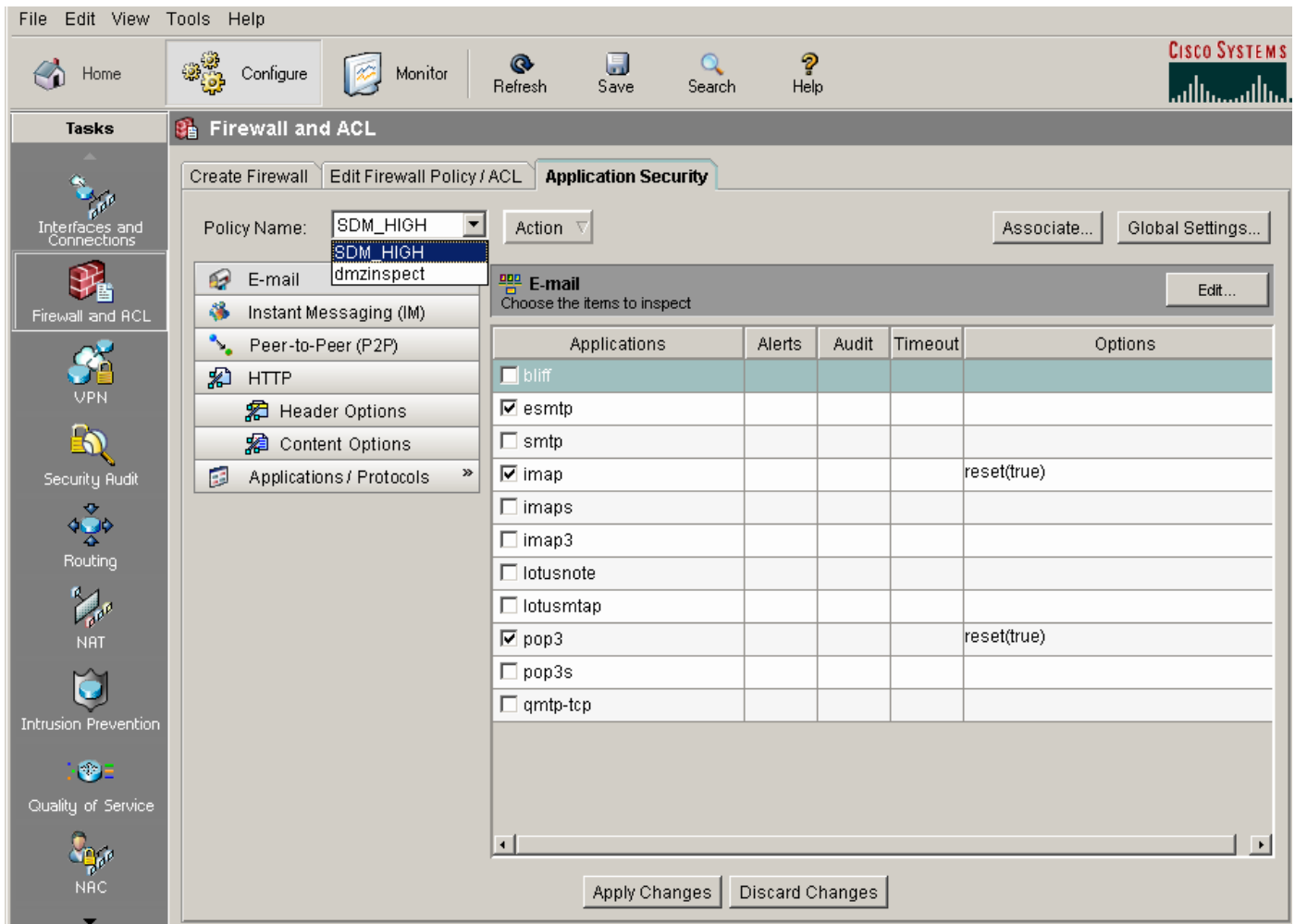
- Advanced Application Inspection and Control – This feature enforces protocol conformance for HTTP, Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), Internet Mail Access Protocol (IMAP), and point of presence 3 (POP3) with inspection engines. It helps enable detection and prevention of misuses of previously listed protocols by applications.
- Instant Messaging and Peer-to-Peer (P2P) File Sharing Application blocking – This feature allows Cisco IOS Firewall to control instant messaging and P2P applications on networks.
- Cisco IOS Firewall Engine (Context BAC) – This engine provides stateful packet inspection of TCP, User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) traffic for per-application-based access control to internal users. Also known as Context Based Access Control (CBAC).
- Voice traversal is provided by application-level intelligence of the protocol as to the call flow and associated channels that are opened.
- Granular Protocol Inspection – RFC 1700-compliant protocols and user-defined ports can be specified within TCP and UDP for more granular inspection of these protocols.
- Dynamic Port Mapping – This feature allows network administrators to run Cisco IOS Firewall-supported applications on nonstandard ports.

At **Configure Mode**, select the **Firewall and ACL** and then click **Application Security** tab, the Application Firewall page appears.



Example: To view or modify the policies created by the Advanced Firewall wizard earlier, click **Policy Name** . The dropdown menu on the upper left panel lists SDM_HIGH and dmzinspect (Figure 17). If there are no rules configured, this list is empty. To create a new policy click the **Action** button, and choose **Add**.

Figure 17 Application Security

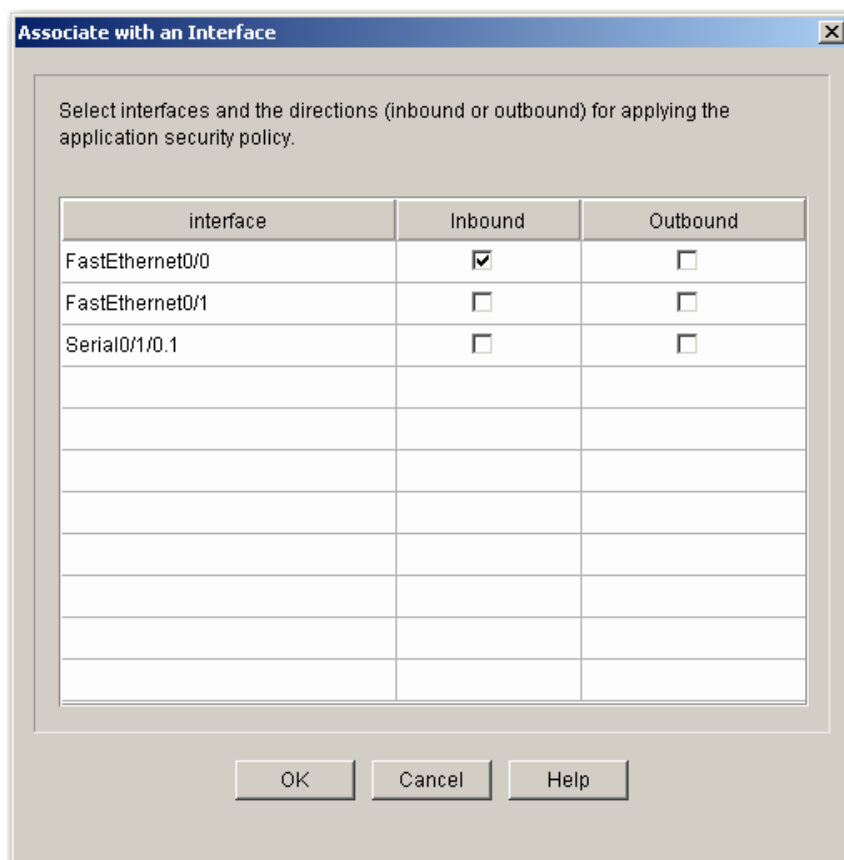


Select, click **Associated...** button on the right upper panel, the Associate with an Interface dialog appears (Figure 18).

Figure 18 shows the SDM_HIGH rule is applied to the incoming traffic on the interface FastEthernet0/0. The dialog allows to choose the interfaces, and to specify the traffic direction to which the policy is to apply.



Figure 18 Associate with an Interface – SDM_HIGH



Click the **Global Settings...** button on the right upper panel, the Global Timeouts and Thresholds dialog appears (Figure 19). It allows Context-Based Access Control (CBAC) global timeouts and thresholds. CBAC uses timeouts and thresholds to determine how long to manage state information for a session and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply to all sessions.

- TCP FIN Wait Timeout Value: The amount of time that a TCP session will still be managed after the firewall detects a FIN exchange.
- TCP Idle Timeout Value: The amount of time that a TCP session will still be managed after no activity has been detected.
- UDP Idle timeout Value: The amount of time that a UDP session will still be managed after no activity has been detected.
- DNS Timeout Value: The amount time that a Domain name System name lookup session will be managed after no activity has been detected.
- SYN Flood DoS Attack Thresholds: An unusually high number of half-open sessions may indicate that a Denial of Service (DoS) attack is under way. Dos attack thresholds allow the router to start deleting half-open sessions after the total number of them has reached a maximum threshold. By defining thresholds, you can specify when the router should start deleting half-open sessions and when it can stop deleting them.
 - One-minute session thresholds: These fields let you specify the threshold values for new connection attempts.
 - Low:** Stop delete new connections after the number of new connections drops below this value.
 - High:** Start deleting new connections when the number of new connections exceeds this value.



- Maximum incomplete session thresholds: These fields let you specify the threshold values for the total number of existing half-open sessions.

Low: Stop delete existing half-open sessions after the number of total half-open sessions drop below this value.

High: Start deleting existing half-open sessions when the number of total half-open sessions exceeds this value.

- TCP maximum incomplete session per host: The router starts deleting half-open sessions for the same host when the total number for that host exceeds this number.
- Enable audit globally: Check this box if you want to turn on CBAC audit trail message for all types of traffic.
- Enable alert globally: Check this box if you want to turn on CBAC alert messages for all types of traffic.

Figure 19 Global Timeouts and Thresholds

Global Timeouts and Thresholds

Global Timeout Values

TCP connection timeout value: 30 secs

TCP FIN-wait timeout value: 5 secs

TCP idle timeout value: 3600 secs

UDP idle timeout value: 30 secs

DNS timeout value: 5 secs

SYN Flooding DoS Attack Thresholds

The threshold values define the limits for triggering deletion of existing half-open sessions. An unusual number of half-open sessions may indicate a SYN Flooding DoS attack.

One Minute Session Threshold

Low: 400 High: 500

Maximum incomplete session threshold

Low: 400 High: 500

TCP maximum incomplete sessions per host: 50

Blocking Time: 0 mins

Other

Enable alert globally Enable audit globally

OK Cancel Help



Click the **E-mail** drawer. The default e-mail configuration for SDM_HIGH is displayed (Figure 20). You can make changes to e-email application security settings. Click **Apply Changes** button on the lower panel if any change needs to be made.

Figure 20 E-mail

The screenshot shows the Cisco SDM interface for configuring Application Security. The 'Firewall and ACL' section is active, and the 'Application Security' tab is selected. The policy name is 'SDM_HIGH'. The 'E-mail' drawer is expanded, showing a list of applications to inspect. The table below shows the configuration for these applications:

Applications	Alerts	Audit	Timeout	Options
<input type="checkbox"/> bliff				
<input checked="" type="checkbox"/> esmtp				
<input type="checkbox"/> smtp				
<input checked="" type="checkbox"/> imap				reset(true)
<input type="checkbox"/> imaps				
<input type="checkbox"/> imap3				
<input type="checkbox"/> lotusnote				
<input type="checkbox"/> lotusmtap				
<input checked="" type="checkbox"/> pop3				reset(true)
<input type="checkbox"/> pop3s				
<input type="checkbox"/> qmtp-tcp				

Click **Instant Messaging(IM)** drawer. The default IM configuration for SDM_HIGH is displayed (Figure 21). Use this page to control the traffic for Instant Messaging applications. SDM supports Yahoo Messenger, NMS Messenger and AIM.

Figure 21 Instant Messaging (IM)

The screenshot shows the Cisco SDM interface for configuring Application Security. The 'Instant Messaging (IM)' drawer is expanded, showing a table of IM applications to configure. The table below shows the configuration for these applications:

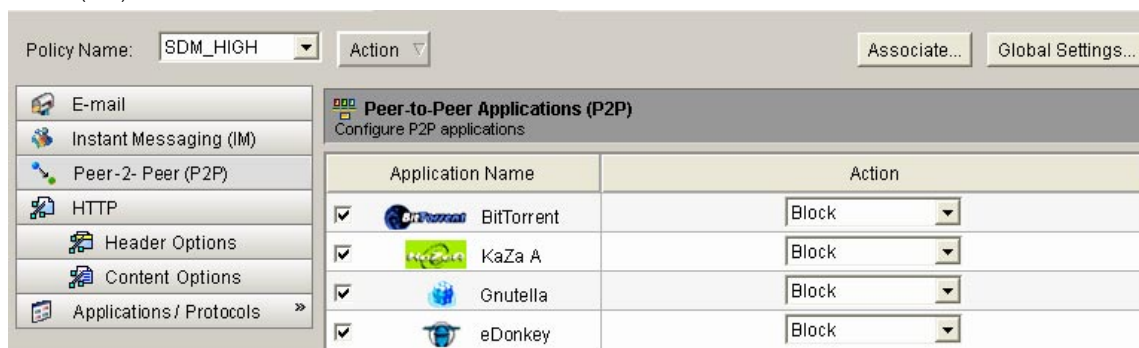
Application Name	Action	Send Alarm
<input checked="" type="checkbox"/> Yahoo Messenger	Block	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> MSN Messenger	Block	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> AIM	Block	<input checked="" type="checkbox"/>



In the Action column, choose **Permit** to allow traffic related to that option, or choose **Block** to deny traffic. If you want an alarm to be sent to the log when this type of traffic is encountered, check **Send Alarm**. Click **Apply Changes** button on the lower panel (not shown on Figure 21) if any change needs to be made (Note, Logging must be enabled for Application Security to send alarms to the log. Go to Additional Tasks > Router Properties > Logging)

Click **Point-2-Point (P2P)** drawer. The default P2P configuration for SDM_HIGH is displayed (Figure 22). This page allows you to make changes to security settings for P2P applications. SDM supports BitTorrent, KaZaA, Gnutella and eDonkey.

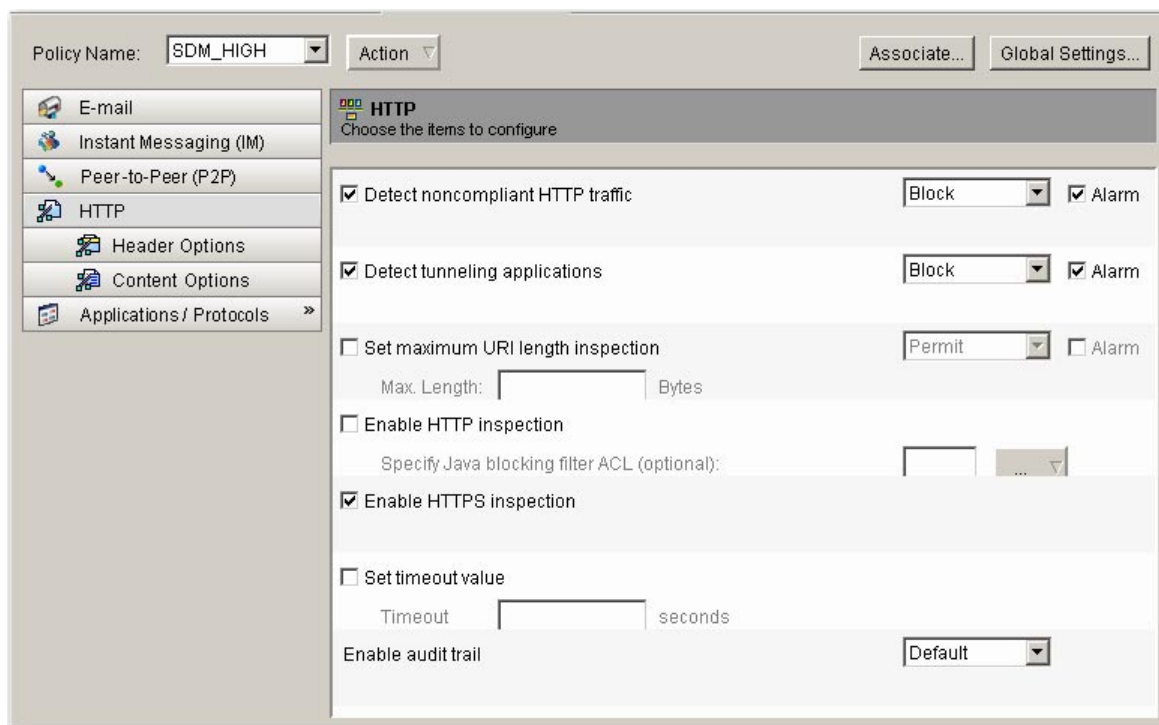
Figure 22 Point-2-Point (P2P)



In the Action column, choose **Permit** to allow traffic related to that option, or choose **Block** to deny traffic. Click **Apply Changes** button on the lower panel (note shown on Figure 22) if any change needs to be made.

Click **HTTP** drawer. The default HTTP configuration for SDM_HIGH is displayed (Figure 23). This page allows you to make changes to security settings for P2P applications. SDM supports BitTorrent, KaZaA, Gnutella and eDonkey.

Figure 23 HTTP

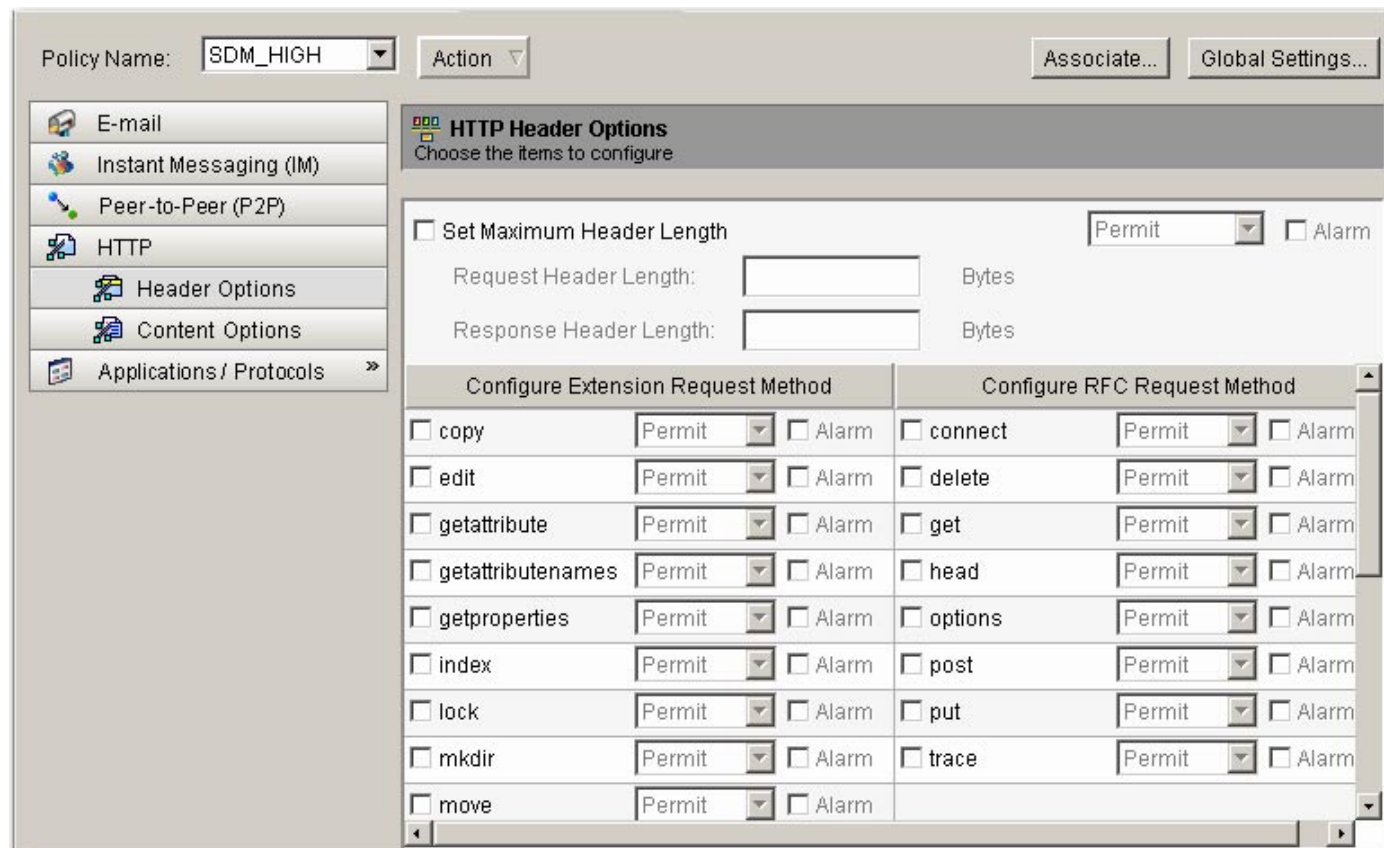




This page allows you to specify/change general settings for HTTP traffic inspection.

Click **HTTP/Header Options** drawer. The default HTTP/Header Option configuration for SDM_HIGH is displayed (Figure 24). At this page, you can configure the router to permit or deny traffic based on HTTP header length and the request method contained in the header.

Figure 24 HTTP – Header Options



Check the **Set Maximum Header Length** checkbox if you want the router to permit or deny traffic based on HTTP header length, and specify the maximum Request and maximum Response header length. Use the Permit, Block, and Alarm controls to specify the action the router is to take when header length exceeds these values.

If you want the router to permit or deny HTTP traffic based on an **Extension Request Method**, check the box next to that request method. Use the Permit, Block, and Alarm controls to specify the action the router is to take when it encounters traffic using that request method. If you want the router to permit or deny HTTP traffic based on one of the **RFC Request Methods** specified in RCP 2616, *Hypertext Transfer Protocol—HTTP/1.1*, check the box next to that request method.

Click **HTTP/Content Options** drawer. The default HTTP/Content Option configuration for SDM_HIGH is displayed (Figure 25). At this page, you can configure the router to examine the content of HTTP traffic and permit or block traffic, and generate alarms based on what packets that you make the router check.

Check the **Verify Content Type** box if you want the router to verify the content of HTTP packet by matching the response with the request, by enabling an alarm for unknown content types, or by using both of these methods. Use the Permit, Block, and Alarm controls to specify the action the router is to take when requests cannot be matched with responses, and when it encounters an unknown content type.

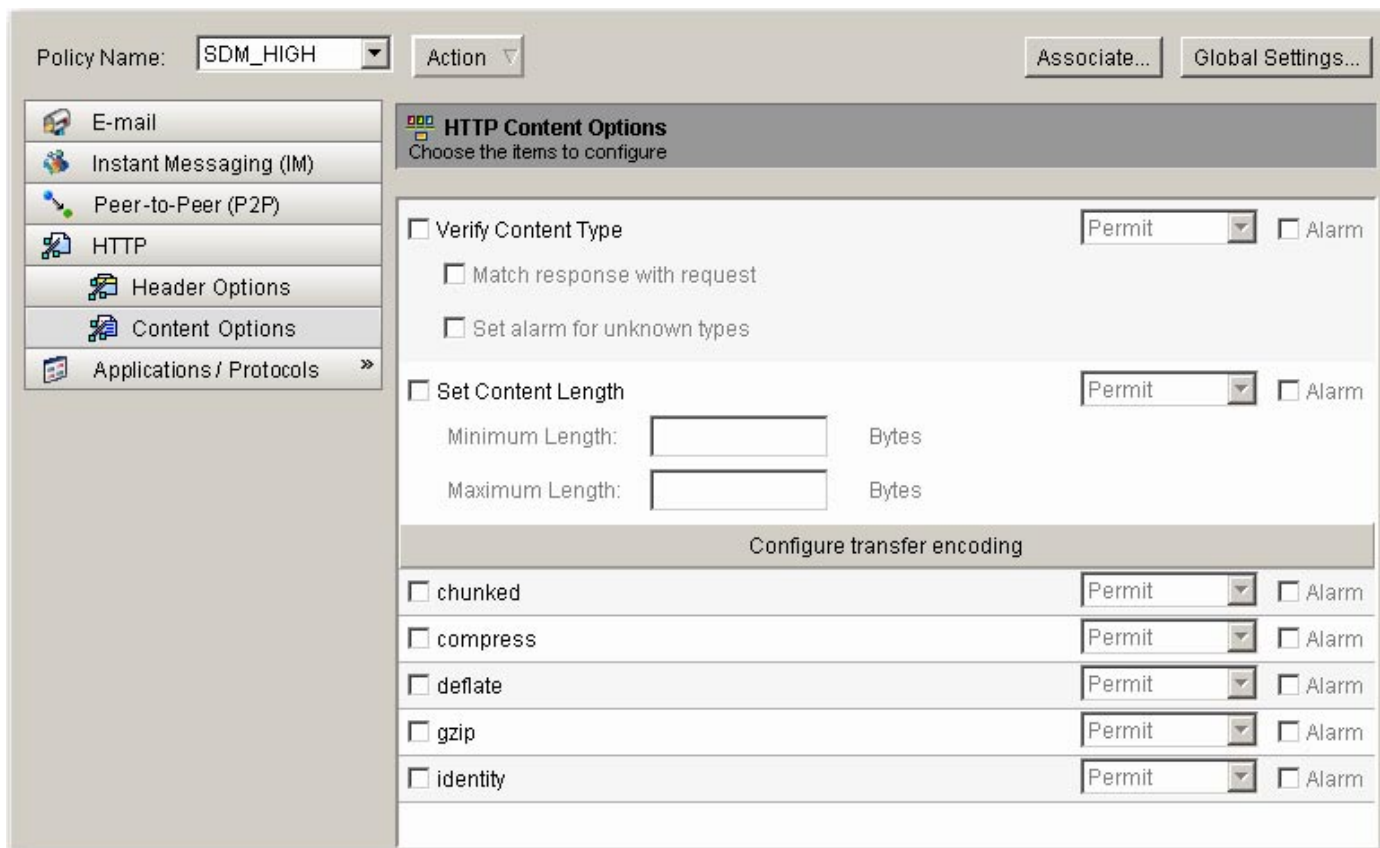


Check the **Set Content Length** box to set a minimum and maximum length for the data in an HTTP packet, and enter the values in the fields provided. Use the Permit, Block and Alarm controls to specify the action the router is to take when the amount of data falls below the minimum length or when it exceeds the maximum length.

For **Configure Transfer Encoding**, SDM supports following encoding list below, use the Permit, Block, and Alarm controls to specify the action the router is to take when it encounters the transfer encodings that you choose. The supported encoding:

- chunk: The encoding format specified in RFC 2616, *Hypertext Transfer Protocol—HTTP/1*. The body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
- compress: The encoding format produced by the UNIX “compress” utility.
- deflate: The “ZLIB” format defined in RFC 1950, ZLIB Compressed Data Format Specification version 3.3, combined with the “deflate” compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification version 1.3
- gzip: The encoding format produced by the GNU zip (“gzip”) program
- identity: Default encoding, which indicates that no encoding has been performed.

Figure 25 HTTP – Content Options



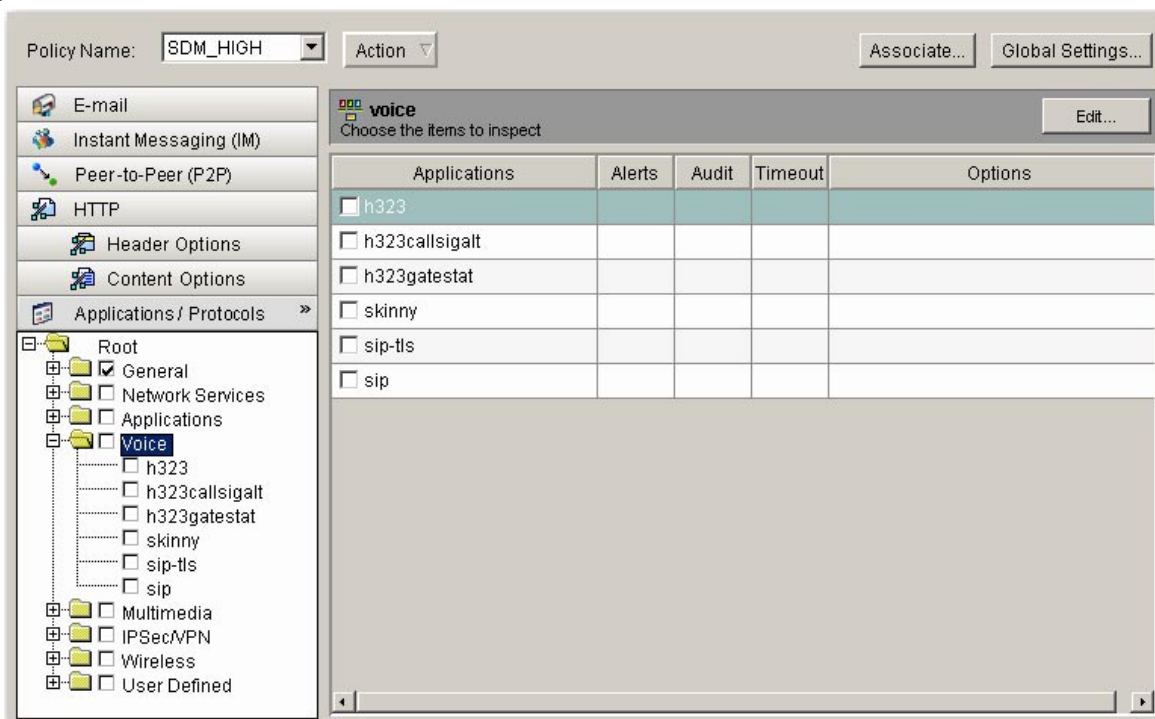
Click **Applications/Protocols** drawer. The default Applications/Protocols configuration for SDM_HIGH is displayed. SDM groups protocols based on technology to visualize the granular protocol inspection rules and make the configuration simple and easy.



The Application /Protocol tree enables you to filter the list on the right according to the type of applications and protocols that you want to view. First choose the branch for the general type that you want to display. The frame on the right displays the available items for the type that you choose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click on the + sign to expand the branch and then select the sub category that you want to display. If the list on the right is empty, there are no applications or protocols available for that type. To choose an application, check the box next to it in the tree, or you can check the box next to it in the list.

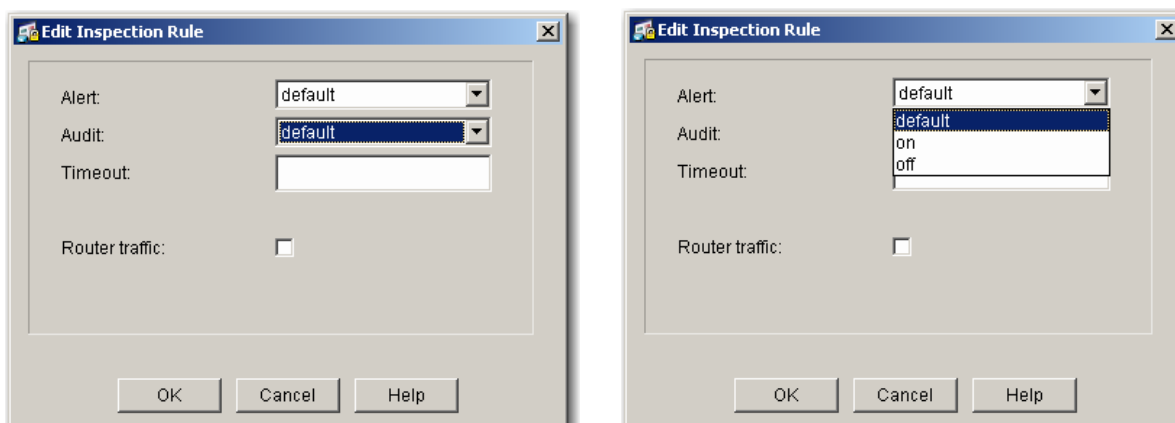
Example: If you want to display and choose a Voice related applications, expand **Root**, expand **Voice**, the tree displays the supported applications. The list appears on the page when you click on Voice (Figure 26).

Figure 26 Applications/Protocols -> Root/Voice



Use the **Edit...** button on the right upper panel to edit the settings for the chose application. Settings that you make override the global settings configured on the router. Click the **Edit...** button., The Edit Inspection Rule dialog appears (Figure 27).

Figure 27 Edit Inspection Rule

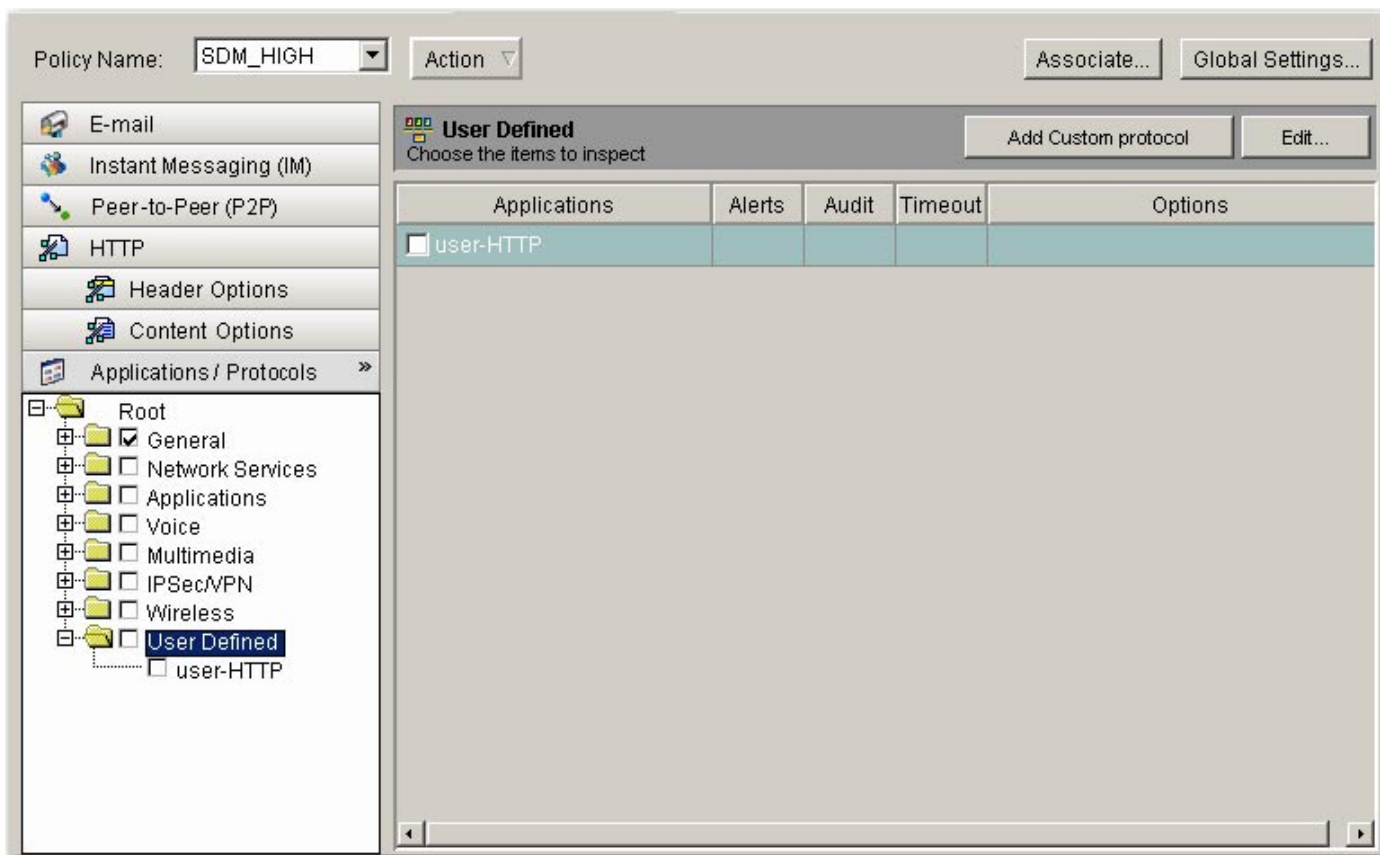




- Alert/Audit:
 - default: User the global setting for alerts
 - on: Generate an alert when traffic of this type is encountered
 - off: Do not generate an alert when traffic of this type is encountered.
- Timeout: Enter the number of seconds that a session for this application should be managed after no activity has been detected. The timeout value that you enter sets the TCP Idle Timeout value if this is a TCP application, or the UDP timeout value if this is a UDP application.
- Router Traffic: Enable inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Port to Application Mapping (PAM) allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application. To establish PAM, at the **Application /Protocol** tree, expand **Root**, and select **User Defined** (Figure 28). Click **Add Custom protocol** button on the right upper panel, the **Add Port Map Entry** dialog appears.

Figure 28 User Defined



Example: If you want to establish a web-based application using TCP port 3001 (Figure 29):

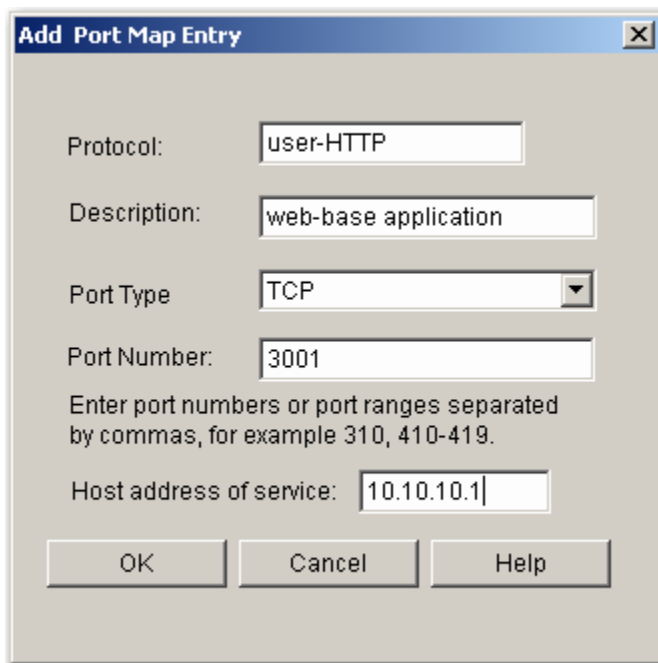
- Protocol: **user-HTTP**
- Description: **web-based application**
- Port Type: **TCP**
- Port Number: **3001**



- Host address of service: **10.10.10.1**

Use **Edit** button next to the **Add Custom protocol** button to specify the inspection rule on the user-defined application.

Figure 29 Add Port Map Entry



Monitoring

Activity on your firewall is monitored through the creation of log entries. If logging is enabled on the router, whenever a rule (access rule or inspection rule) that is configured to generate log entries is invoked – for example, if a connection was attempted from a denied IP address, or an application is blocked by the firewall, then a log entry is generated and can be viewed in Monitor mode.

Make sure logging is enabled on the router, at **Configure Mode**, select the **Additional Tasks**, expand the **Router Properties**, and then select **Logging**. In order for Application Security log entries to be collected, you must configure logging level of informational (6) or higher. If you have already configured logging for debugging(7), the log will contain application security log messages. In this example (Figure 30), the Property **Syslog** is **Enabled**, the Property **Logging Level** is configured with **debugging (7)**

Figure 30 Logging



Additional Tasks

- Router Properties
 - Date/Time
 - NTP/SNTP
 - Logging**
 - SNMP
- Router Access
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor

Logging

Property	Value
Syslog	Enabled
Syslog Server1	10.10.10.5
Logging to Buffer	Enabled
Buffer Size	51200
Logging Level	debugging (7)

To view the Firewall log, at **Monitor Mode**, select the **Firewall Status**, click **Firewall Log** tab (Figure 31). This sample Firewall Status page displays the following statistics about the firewall:

- Firewall Log: whether or not the router is configured to maintain a log of connection attempts allowed and denied by the firewall
- Number of attempts denied by firewall: shows the number of connections attempts rejected by the firewall



Figure 31 Firewall Log

The screenshot shows the Cisco Firewall Status page. The top navigation bar includes Home, Configure, Monitor, Refresh, Save, Search, and Help. The left sidebar contains navigation icons for Overview, Interface Status, Firewall Status, VPN Status, QoS Status, NAC Status, and Logging. The main content area is titled "Firewall Status" and has two tabs: "Firewall Log" (selected) and "Application Security Log".

Firewall Log: Configured
Number of attempts denied by firewall: 208

The table below shows the log of attempts denied by firewall

Time	Description
Sep 28 23:23:00.	list 101 denied tcp 207.46.2.47(1863) -> 128.107.252.131(2309), 1 packet
Sep 28 23:27:27.	list 101 denied tcp 128.107.253.42(8999) -> 128.107.252.131(2275), 1 packet
Sep 28 23:27:32.	list 101 denied tcp 128.107.253.40(8999) -> 128.107.252.131(2277), 1 packet
Sep 28 23:28:12.	list 101 denied tcp 207.46.2.47(1863) -> 128.107.252.131(2309), 10 packets
Sep 28 23:33:12.	list 101 denied tcp 128.107.253.42(8999) -> 128.107.252.131(2275), 8 packets
Sep 28 23:33:12.	list 101 denied tcp 128.107.253.40(8999) -> 128.107.252.131(2277), 8 packets
Sep 28 23:33:37.	list 101 denied tcp 128.107.253.44(8999) -> 128.107.252.131(2384), 1 packet
Sep 28 23:33:50.	list 101 denied tcp 128.107.253.39(8999) -> 128.107.252.131(2390), 1 packet
Sep 28 23:39:12.	list 101 denied tcp 128.107.253.44(8999) -> 128.107.252.131(2384), 8 packets
Sep 28 23:39:12.	list 101 denied tcp 128.107.253.39(8999) -> 128.107.252.131(2390), 8 packets
Sep 28 23:53:32.	list 101 denied icmp 128.107.145.16 -> 128.107.252.131 (8/0), 1 packet
Sep 28 23:55:17.	list 101 denied icmp 128.107.174.113 -> 128.107.252.131 (8/0), 1 packet
Sep 28 23:56:56.	list 101 denied icmp 128.107.142.133 -> 128.107.252.131 (8/0), 1 packet
Sep 29 00:00:40.	list 101 denied tcp 65.214.44.160(45854) -> 128.107.252.131(80), 1 packet
Sep 29 00:06:12.	list 101 denied tcp 65.214.44.160(45854) -> 128.107.252.131(80), 5 packets
Sep 29 00:09:04.	list 101 denied tcp 128.107.253.43(8999) -> 128.107.252.131(2595), 1 packet
Sep 29 00:09:15.	list 101 denied icmp 128.107.142.133 -> 128.107.252.131 (8/0), 1 packet
Sep 29 00:14:12.	list 101 denied tcp 128.107.253.43(8999) -> 128.107.252.131(2595), 8 packets
Sep 29 00:27:42.	list 101 denied tcp 128.107.253.37(8999) -> 128.107.252.131(2682), 1 packet
Sep 29 00:33:12.	list 101 denied tcp 128.107.253.37(8999) -> 128.107.252.131(2682), 8 packets
Sep 29 00:45:37.	list 101 denied tcp 198.133.219.101(80) -> 128.107.252.131(3076), 1 packet
Sep 29 00:48:16.	list 101 denied tcp 198.133.219.107(80) -> 128.107.252.131(3152), 1 packet
Sep 29 00:51:12.	list 101 denied tcp 198.133.219.101(80) -> 128.107.252.131(3076), 3 packets
Sep 29 00:54:12.	list 101 denied tcp 198.133.219.107(80) -> 128.107.252.131(3152), 7 packets
Sep 29 00:55:40.	list 101 denied tcp 128.107.253.42(8999) -> 128.107.252.131(3075), 1 packet
Sep 29 00:56:12.	list 101 denied icmp 128.107.174.113 -> 128.107.252.131 (8/0), 1 packet
Sep 29 00:56:28.	list 101 denied tcp 198.133.219.107(80) -> 128.107.252.131(3334), 1 packet
Sep 29 00:56:41.	list 101 denied tcp 198.133.219.107(80) -> 128.107.252.131(3337), 1 packet

User the **Update** button on the right upper window to poll the router and update the information shown on the screen with current information.

Click **Application Security Log** tab (Figure 32). The Application Security Log shows the alarms generated when the router encounters traffic from applications or protocols. In the sample Application Security Log page, im-msn traffic from private network 10.10.10.11 is blocked, packets are dropped.



Figure 32 Application Security Log

Time	Log Type	Details
Sep 28 23:29:20.731	HTTP MAX REQ EXCEED	Maximum of 10 unanswered HTTP requests exceeded from 10.10.10.11:2432 to 1
Sep 28 23:23:30.739	SESS AUDIT TRAIL START	Start im-msn session: initiator (10.10.10.11:2379) -- responder (65.54.239.80:1863)
Sep 28 23:23:30.855	DROP PKT	Dropping tcp pkt 65.54.239.80:1863 => 10.10.10.11:2379
Sep 28 23:23:33.115	SESS AUDIT TRAIL START	Start im-msn session: initiator (10.10.10.11:2380) -- responder (207.46.2.29:1863)
Sep 28 23:23:38.111	SESS AUDIT TRAIL	Stop im-msn session: initiator (10.10.10.11:2379) sent 144 bytes -- responder (65.54.239.80:1863)
Sep 28 23:24:01.303	DROP PKT	Dropping tcp pkt 207.46.2.29:1863 => 10.10.10.11:2380
Sep 28 23:24:32.839	DROP PKT	Dropping tcp pkt 207.46.2.29:1863 => 10.10.10.11:2380
Sep 28 23:24:57.451	SESS AUDIT TRAIL	Stop im-msn session: initiator (10.10.10.11:2380) sent 910 bytes -- responder (207.46.2.29:1863)
Sep 28 23:29:20.735	DROP PKT	Dropping tcp pkt 128.107.252.131:2432 => 198.133.219.25:80
Sep 29 00:17:31.947	DROP PKT	Dropping tcp pkt 128.107.252.131:2680 => 207.126.111.223:443
Sep 29 00:45:37.275	DROP PKT	Dropping tcp pkt 128.107.252.131:3076 => 198.133.219.25:80
Sep 29 00:48:12.055	DROP PKT	Dropping tcp pkt 128.107.252.131:3152 => 198.133.219.25:80
Sep 29 00:51:21.447	DROP PKT	Dropping tcp pkt 128.107.252.131:3168 => 198.133.219.25:80
Sep 29 00:56:11.463	DROP PKT	Dropping tcp pkt 128.107.252.131:3330 => 198.133.219.25:80
Sep 29 00:56:41.979	DROP PKT	Dropping tcp pkt 128.107.252.131:3341 => 198.133.219.25:80

User the **Update** button on the right upper window to poll the router and update the information show on the screen with current information

In summary, by using Cisco SDM Firewall Wizard, the Firewall Policy Table and Application Security tool, users can generate complex firewall configuration easily and quickly with minimum knowledge of Cisco IOS Software commands and minimal security knowledge. In addition, the Policy View provides users with a graphical interface to view the details of the firewall policies with access rights, traffic flows, and interfaces.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)