



CHAPTER 23

Configuring Application Layer Protocol Inspection

This chapter describes how to configure application layer protocol inspection. Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the FWSM to do a deep packet inspection instead of passing the packet through the fast path. As a result, inspection engines can affect overall throughput.

Several common inspection engines are enabled on the FWSM by default, but you might need to enable others depending on your network. This chapter includes the following sections:

- [Inspection Engine Overview, page 23-2](#)
 - [When to Use Application Protocol Inspection, page 23-2](#)
 - [Inspection Limitations, page 23-2](#)
 - [Default Inspection Policy, page 23-3](#)
- [Configuring Application Inspection, page 23-4](#)
- [CTIQBE Inspection, page 23-5](#)
- [DCERPC Inspection, page 23-6](#)
- [DNS Inspection, page 23-6](#)
- [ESMTP Inspection, page 23-8](#)
- [FTP Inspection, page 23-8](#)
- [GTP Inspection, page 23-10](#)
- [H.323 Inspection, page 23-11](#)
- [HTTP Inspection, page 23-13](#)
- [Instant Messaging Inspection, page 23-14](#)
- [ICMP Inspection, page 23-14](#)
- [ICMP Error Inspection, page 23-14](#)
- [ILS Inspection, page 23-14](#)
- [MGCP Inspection, page 23-15](#)
- [NetBIOS Inspection, page 23-17](#)
- [PPTP Inspection, page 23-17](#)
- [RSH Inspection, page 23-18](#)

- [RTSP Inspection, page 23-18](#)
- [SIP Inspection, page 23-19](#)
- [Skinny \(SCCP\) Inspection, page 23-21](#)
- [SMTP and Extended SMTP Inspection, page 23-22](#)
- [SNMP Inspection, page 23-23](#)
- [SQL*Net Inspection, page 23-23](#)
- [Sun RPC Inspection, page 23-24](#)
- [TFTP Inspection, page 23-26](#)
- [XDMCP Inspection, page 23-26](#)
- [Service Policy Field Descriptions, page 23-26](#)
- [Class Map Field Descriptions, page 23-36](#)
- [Inspect Map Field Descriptions, page 23-57](#)

Inspection Engine Overview

This section includes the following topics:

- [When to Use Application Protocol Inspection, page 23-2](#)
- [Inspection Limitations, page 23-2](#)
- [Default Inspection Policy, page 23-3](#)

When to Use Application Protocol Inspection

When a user establishes a connection, the FWSM checks the packet against access lists, creates an address translation, and creates an entry for the session in the fast path, so that further packets can bypass time-consuming checks. However, the fast path relies on predictable port numbers and does not perform address translations inside a packet.

Many protocols open secondary TCP or UDP ports. The initial session on a well-known port is used to negotiate dynamically assigned port numbers.

Other applications embed an IP address in the packet that needs to match the source address that is normally translated when it goes through the FWSM.

If you use applications like these, then you need to enable application inspection.

When you enable application inspection for a service that embeds IP addresses, the FWSM translates embedded addresses and updates any checksum or other fields that are affected by the translation.

When you enable application inspection for a service that uses dynamically assigned ports, the FWSM monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

Inspection Limitations

See the following limitations for application protocol inspection:

- State information for multimedia sessions that require inspection are not passed over the state link for stateful failover. The exception is GTP, which is replicated over the state link.
- Some inspection engines do not support PAT, NAT, outside NAT, or NAT between same security interfaces. See “[Default Inspection Policy](#)” for more information about NAT support.

Default Inspection Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy, so if you want to alter the global policy, for example, to apply inspection to non-standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one.

[Table 23-1](#) lists all inspections supported, the default ports used in the default class map, and the inspection engines that are on by default, shown in bold. This table also notes any NAT limitations.

Table 23-1 Supported Application Inspection Engines

Application ¹	Default Port	NAT Limitations	Standards ²	Comments
CTIQBE	TCP/2748	—	—	—
DNS over UDP	UDP/53	No NAT support is available for name resolution through WINS.	RFC 1123	No PTR records are changed.
FTP	TCP/21	—	RFC 959	—
GTP	UDP/3386 UDP/2123	—	—	Requires a special license.
H.323 H.225 and RAS	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	No NAT on same security interfaces. No static PAT.	ITU-T H.323, H.245, H225.0, Q.931, Q.932	—
HTTP	TCP/80	—	RFC 2616	Beware of MTU limitations stripping ActiveX and Java. If the MTU is too small to allow the Java or ActiveX tag to be included in one packet, stripping may not occur.
ICMP	—	—	—	All ICMP traffic is matched in the default class map.
ICMP ERROR	—	—	—	All ICMP traffic is matched in the default class map.
ILS (LDAP)	TCP/389	No PAT.	—	—
MGCP	UDP/2427, 2727	—	RFC 2705bis-05	—
NetBIOS Name Server over IP	UDP/137, 138 (Source ports)	—	—	NetBIOS is supported by performing NAT of the packets for NBNS UDP port 137 and NBDS UDP port 138.
PPTP	TCP/1723	—	RFC 2637	—

Table 23-1 Supported Application Inspection Engines (continued)

Application ¹	Default Port	NAT Limitations	Standards ²	Comments
RSN	TCP/514	No PAT	Berkeley UNIX	—
RTSP	TCP/554	No PAT. No outside NAT.	RFC 2326, 2327, 1889	No handling for HTTP cloaking.
SIP	TCP/5060 UDP/5060	No outside NAT. No NAT on same security interfaces.	RFC 2543	—
SKINNY (SCCP)	TCP/2000	No outside NAT. No NAT on same security interfaces.	—	Does not handle TFTP uploaded Cisco IP Phone configurations under certain circumstances.
SMTP and ESMTP	TCP/25	—	RFC 821, 1123	—
SNMP	UDP/161, 162	No NAT or PAT.	RFC 1155, 1157, 1212, 1213, 1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580.
SQL*Net	TCP/1521	—	—	v.1 and v.2.
Sun RPC over UDP and TCP	UDP/111	No NAT or PAT.	—	The default rule includes UDP port 111; if you want to enable Sun RPC inspection for TCP port 111, you need to create a new rule that matches TCP port 111 and performs Sun RPC inspection.
TFTP	UDP/69	—	RFC 1350	Payload IP addresses are not translated.
XDCMP	UDP/177	No NAT or PAT.	—	—

1. Inspection engines that are enabled by default for the default port are in bold.
2. The FWSM is in compliance with these standards, but it does not enforce compliance on packets being inspected. For example, FTP commands are supposed to be in a particular order, but the FWSM does not enforce the order.

Configuring Application Inspection

This feature uses Security Policy Rules. Service policies provide a consistent and flexible way to configure FWSM features. For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications. See [Chapter 22, “Configuring Service Policy Rules,”](#) for more information.

Inspection is enabled by default for some applications. See the [“Default Inspection Policy”](#) section for more information. Use this section to modify your inspection policy.

To configure application inspection, perform the following steps:

-
- Step 1** Click **Configuration > Firewall > Service Policy Rules**.
 - Step 2** Add or edit a service policy rule according to the [“Adding a Service Policy Rule”](#) section on page 22-5.

If you want to match non-standard ports, then create a new rule for the non-standard ports. See the [“Default Inspection Policy”](#) section on page 23-3 for the standard ports for each inspection engine. You can combine multiple rules in the same service policy if desired, so you can create one rule to match

certain traffic, and another to match different traffic. However, if traffic matches a rule that contains an inspection action, and then matches another rule that also has an inspection action, only the first matching rule is used.

- Step 3** On the Edit Service Policy Rule > Rule Actions dialog box, click the **Protocol Inspection** tab. For a new rule, the dialog box is called Add Service Policy Rule Wizard - Rule Actions.
- Step 4** Check each inspection type that you want to apply.
- Step 5** (Optional) Some inspection engines let you control additional parameters when you apply the inspection to the traffic. Click **Configure** for each inspection type to configure an inspect map. You can either choose an existing map, or create a new one. You can predefine inspect maps from the Configuration > Firewall > Objects > Inspect Maps pane. See the “[Inspect Map Field Descriptions](#)” section on page 23-57 for detailed information of each inspect map type.
- Step 6** You can configure other features for this rule if desired using the other Rule Actions tabs.
- Step 7** Click **OK** (or **Finish** from the wizard).
-

CTIQBE Inspection

This section describes CTIQBE application inspection. This section includes the following topics:

- [CTIQBE Inspection Overview, page 23-5](#)
- [Limitations and Restrictions, page 23-5](#)

CTIQBE Inspection Overview

CTIQBE protocol inspection supports NAT, PAT, and bidirectional NAT. This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to work successfully with Cisco CallManager for call setup across the FWSM.

TAPI and JTAPI are used by many Cisco VoIP applications. CTIQBE is used by Cisco TSP to communicate with Cisco CallManager.

Limitations and Restrictions

The following summarizes limitations that apply when using CTIQBE application inspection:

- CTIQBE application inspection does not support configurations with the **alias** command.
- Stateful failover of CTIQBE calls is not supported.
- Entering the **debug ctiqbe** command may delay message transmission, which may have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the FWSM, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.

The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the FWSM, calls between these two phones fails.

- When Cisco CallManager is located on the higher security interface compared to Cisco IP SoftPhones, if NAT or outside NAT is required for the Cisco CallManager IP address, the mapping must be static as Cisco IP SoftPhone requires the Cisco CallManager IP address to be specified explicitly in its Cisco TSP configuration on the PC.
- When using PAT or Outside PAT, if the Cisco CallManager IP address is to be translated, its TCP port 2748 must be statically mapped to the same port of the PAT (interface) address for Cisco IP SoftPhone registrations to succeed. The CTIQBE listening port (TCP 2748) is fixed and is not user-configurable on Cisco CallManager, Cisco IP SoftPhone, or Cisco TSP.

DCERPC Inspection

DCERPC is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

This typically involves a client querying a server called the Endpoint Mapper listening on a well known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. The FWSM allows the appropriate port number and network address and also applies NAT, if needed, for the secondary connection.

DCERPC inspect maps inspect for native TCP communication between the EPM and client on well known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and Port number are received from the applicable EPM response messages. Since a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have user configurable timeouts.

DNS Inspection

This section describes DNS application inspection. This section includes the following topics:

- [How DNS Application Inspection Works, page 23-6](#)
- [How DNS Rewrite Works, page 23-7](#)

How DNS Application Inspection Works

The FWSM tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the FWSM. The FWSM also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

When DNS inspection is enabled, which is the default, the FWSM performs the following additional tasks:

- Translates the DNS record based on the configuration completed using NAT rules. Translation only applies to the A-record in the DNS reply; therefore, DNS Rewrite does not affect reverse lookups, which request the PTR record.



Note DNS Rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record and the PAT rule to use is ambiguous.

- Enforces the maximum DNS message length (the default is 512 bytes and the maximum length is 65535 bytes). The FWSM performs reassembly as needed to verify that the packet length is less than the maximum length configured. The FWSM drops the packet if it exceeds the maximum length.
- Enforces a domain-name length of 255 bytes and a label length of 63 bytes.
- Verifies the integrity of the domain-name referred to by the pointer if compression pointers are encountered in the DNS message.
- Checks to see if a compression pointer loop exists.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each *app_id* runs independently.

Because the *app_id* expires independently, a legitimate DNS response can only pass through the FWSM within a limited period of time and there is no resource build-up. However, if you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

How DNS Rewrite Works

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

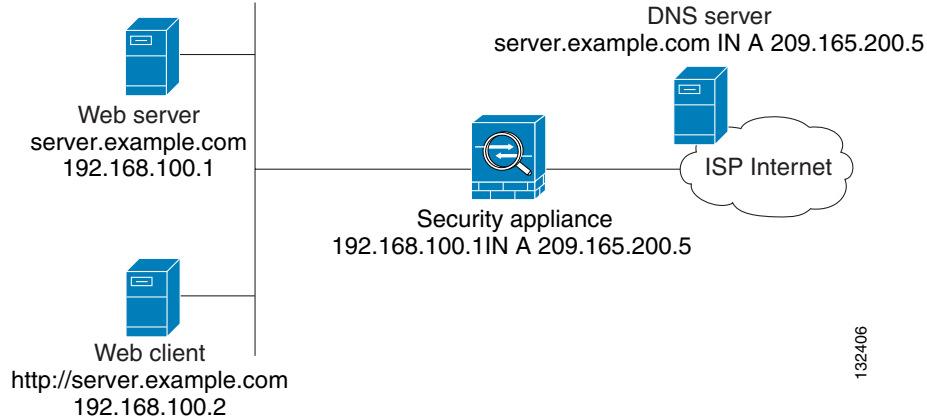
If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly. If the DNS inspection engine is disabled, the A-record is not translated.

As long as DNS inspection remains enabled, you can configure DNS rewrite using a NAT rule.

DNS Rewrite performs two functions:

- Translating a public address (the routable or “mapped” address) in a DNS reply to a private address (the “real” address) when the DNS client is on a private interface.
- Translating a private address to a public address when the DNS client is on the public interface.

In [Figure 23-1](#), the DNS server resides on the external (ISP) network. The real address of the server (192.168.100.1) has been mapped using a static NAT rule to the ISP-assigned address (209.165.200.5). When a web client on the inside interface attempts to access the web server with the URL `http://server.example.com`, the host running the web client sends a DNS request to the DNS server to resolve the IP address of the web server. The FWSM translates the non-routable source address in the IP header and forwards the request to the ISP network on its outside interface. When the DNS reply is returned, the FWSM applies address translation not only to the destination address, but also to the embedded IP address of the web server, which is contained in the A-record in the DNS reply. As a result, the web client on the inside network gets the correct address for connecting to the web server on the inside network.

Figure 23-1 Translating the Address in a DNS Reply (DNS Rewrite)

DNS rewrite also works if the client making the DNS request is on a DMZ network and the DNS server is on an inside interface.

ESMTP Inspection

ESMTP inspection detects attacks, including spam, phishing, malformed message attacks, buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detect several attacks, block senders/receivers, and block mail relay.

FTP Inspection

This section describes the FTP inspection engine. This section includes the following topics:

- [FTP Inspection Overview, page 23-8](#)
- [Using Strict FTP, page 23-9](#)
- [Verifying and Monitoring FTP Inspection, page 23-10](#)

FTP Inspection Overview

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address

FTP application inspection prepares secondary channels for FTP data transfer. Ports for these channels are negotiated through PORT or PASV commands. The channels are allocated in response to a file upload, a file download, or a directory listing event.

**Note**

If you disable FTP inspection engines, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

Using Strict FTP

Using strict FTP increases the security of protected networks by preventing web browsers from sending embedded commands in FTP requests. To enable strict FTP, click the **Configure** button next to FTP on the Configuration > Firewall > Service Policy Rules > Edit Service Policy Rule > Rule Actions > Protocol Inspection tab.

**Note**

To specify FTP commands that are not permitted to pass through the FWSM, create an FTP inspect map according to the “[FTP Class Map](#)” section on page 23-41.

After you enable the Strict option on an interface, FTP inspection enforces the following behavior:

- An FTP command must be acknowledged before the FWSM allows a new command.
- The FWSM drops connections that send embedded commands.
- The 227 and PORT commands are checked to ensure they do not appear in an error string.

**Caution**

Using the strict option may cause the failure of FTP clients that are not strictly compliant with FTP RFCs.

If the strict option is enabled, each FTP command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the PORT and PASV reply command is checked to see if it is five. If it is not five, then the PORT command is assumed to be truncated and the TCP connection is closed.
- Incorrect command—Checks the FTP command to see if it ends with <CR><LF> characters, as required by the RFC. If it does not, the connection is closed.
- Size of RETR and STOR commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.
- Command spoofing—The PORT command should always be sent from the client. The TCP connection is denied if a PORT command is sent from the server.
- Reply spoofing—PASV reply command (227) should always be sent from the server. The TCP connection is denied if a PASV reply command is sent from the client. This prevents the security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- TCP stream editing—The FWSM closes the connection if it detects TCP stream editing.
- Invalid port negotiation—The negotiated dynamic port value is checked to see if it is less than 1024. As port numbers in the range from 1 to 1024 are reserved for well-known connections, if the negotiated port falls in this range, then the TCP connection is freed.
- Command pipelining—The number of characters present after the port numbers in the PORT and PASV reply command is cross checked with a constant value of 8. If it is more than 8, then the TCP connection is closed.

- The FWSM replaces the FTP server response to the SYST command with a series of Xs. to prevent the server from revealing its system type to FTP clients. To override this default behavior, use the Low setting in the FTP map.

Verifying and Monitoring FTP Inspection

FTP application inspection generates the following log messages:

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

In conjunction with NAT, the FTP application inspection translates the IP address within the application payload. This is described in detail in RFC 959.

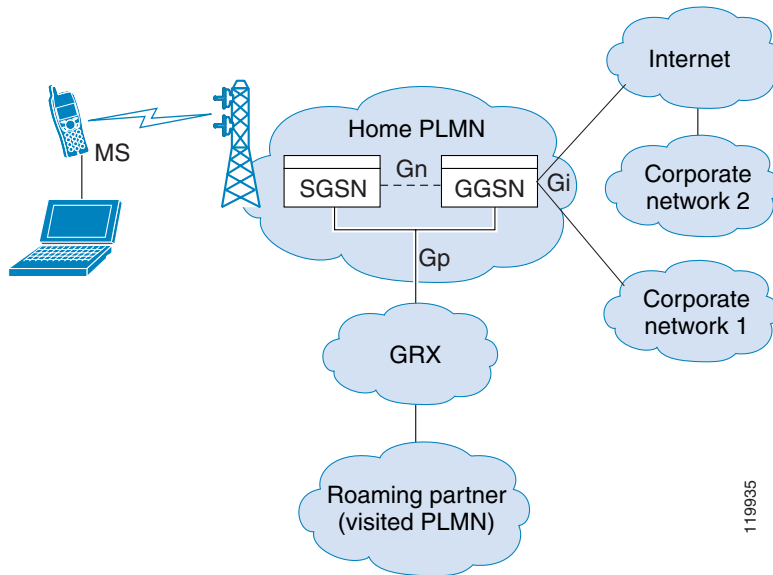
GTP Inspection

**Note**

GTP inspection requires a special license.

GPRS provides uninterrupted connectivity for mobile subscribers between GSM networks and corporate networks or the Internet. The GGSN is the interface between the GPRS wireless data network and other networks. The SGSN performs mobility, data session management, and data compression (See [Figure 23-2](#)).

Figure 23-2 GPRS Tunneling Protocol



The UMTS is the commercial convergence of fixed-line telephony, mobile, Internet and computer technology. UTRAN is the networking protocol used for implementing wireless networks in this system. GTP allows multi-protocol packets to be tunneled through a UMTS/GPRS backbone between a GGSN, an SGSN and the UTRAN.

GTP does not include any inherent security or encryption of user data, but using GTP with the FWSM helps protect your network against these risks.

The SGSN is logically connected to a GGSN using GTP. GTP allows multiprotocol packets to be tunneled through the GPRS backbone between GSNs. GTP provides a tunnel control and management protocol that allows the SGSN to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP uses a tunneling mechanism to provide a service for carrying user data packets.

**Note**

When using GTP with failover, if a GTP connection is established and the active unit fails before data is transmitted over the tunnel, the GTP data connection (with a “j” flag set) is not replicated to the standby unit. This occurs because the active unit does not replicate embryonic connections to the standby unit.

H.323 Inspection

This section describes the H.323 application inspection. This section includes the following topics:

- [H.323 Inspection Overview, page 23-12](#)
- [How H.323 Works, page 23-12](#)
- [Limitations and Restrictions, page 23-13](#)

H.323 Inspection Overview

H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The FWSM supports H.323 through Version 4, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H323 inspection enabled, the FWSM supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the FWSM.

The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the FWSM uses an ASN.1 decoder to decode the H.323 messages.
- Dynamically allocate the negotiated H.245 and RTP/RTCP connections.

How H.323 Works

The H.323 collection of protocols collectively may use up to two TCP connection and four to six UDP connections. FastConnect uses only one TCP connection, and RAS uses a single UDP connection for registration, admissions, and status.

An H.323 client may initially establish a TCP connection to an H.323 server using TCP port 1720 to request Q.931 call setup. As part of the call setup process, the H.323 terminal supplies a port number to the client to use for an H.245 TCP connection. In environments where H.323 gatekeeper is in use, the initial packet is transmitted using UDP.

H.323 inspection monitors the Q.931 TCP connection to determine the H.245 port number. If the H.323 terminals are not using FastConnect, the FWSM dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

Within each H.245 message, the H.323 endpoints exchange port numbers that are used for subsequent UDP data streams. H.323 inspection inspects the H.245 messages to identify these ports and dynamically creates connections for the media exchange. RTP uses the negotiated port number, while RTCP uses the next higher port number.

The H.323 control channel handles H.225 and H.245 and H.323 RAS. H.323 inspection uses the following ports.

- 1718—Gate Keeper Discovery UDP port
- 1719—RAS UDP port
- 1720—TCP Control Port

You must permit traffic for the well-known H.323 port 1720 for the H.225 call signaling; however, the H.245 signaling ports are negotiated between the endpoints in the H.225 signaling. When an H.323 gatekeeper is used, the FWSM opens an H.225 connection based on inspection of the ACF message.

After inspecting the H.225 messages, the FWSM opens the H.245 channel and then inspects traffic sent over the H.245 channel as well. All H.245 messages passing through the FWSM undergo H.245 application inspection, which translates embedded IP addresses and opens the media channels negotiated in H.245 messages.

The H.323 ITU standard requires that a TPKT header, defining the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPKT header does not necessarily need to be sent in the same TCP packet as H.225 and H.245 messages, the FWSM must remember the TPKT length to process and decode the messages properly. For each connection, the FWSM keeps a record that contains the TPKT length for the next expected message.

If the FWSM needs to perform NAT on IP addresses in messages, it changes the checksum, the UUIE length, and the TPKT, if it is included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, the FWSM proxy ACKs that TPKT and appends a new TPKT to the H.245 message with the new length.

**Note**

The FWSM does not support TCP options in the Proxy ACK for the TPKT.

Each UDP connection with a packet going through H.323 inspection is marked as an H.323 connection and times out with the H.323 timeout as configured on the Configuration > Firewall > Advanced > Global Timeouts pane.

Limitations and Restrictions

The following are some of the known issues and limitations when using H.323 application inspection:

- Static PAT may not properly translate IP addresses embedded in optional fields within H.323 messages. If you experience this kind of problem, do not use static PAT with H.323.
- H.323 application inspection is not supported with NAT between same-security-level interfaces.
- When a NetMeeting client registers with an H.323 gatekeeper and tries to call an H.323 gateway that is also registered with the H.323 gatekeeper, the connection is established but no voice is heard in either direction. This problem is unrelated to the FWSM.
- If you configure a network static address where the network static address is the same as a third-party netmask and address, then any outbound H.323 connection fails.

HTTP Inspection

Use the HTTP inspection engine to protect against specific attacks and other threats that may be associated with HTTP traffic. HTTP inspection performs several functions:

- Enhanced HTTP inspection
- URL screening through N2H2 or Websense
- Java and ActiveX filtering

The latter two features are configured in conjunction with Filter rules.

The enhanced HTTP inspection feature, which is also known as an application firewall and is available when you configure an HTTP inspect map (see the [“HTTP Class Map” section on page 23-46](#)), can help prevent attackers from using HTTP messages for circumventing network security policy. It verifies the following for all HTTP messages:

- Conformance to RFC 2616
- Use of RFC-defined methods only.
- Compliance with the additional criteria.

Instant Messaging Inspection

The IM inspect engine lets you apply fine grained controls on the IM application to control the network usage and stop leakage of confidential data, propagation of worms, and other threats to the corporate network.

ICMP Inspection

The ICMP inspection engine allows ICMP traffic to have a “session” so it can be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the FWSM in an access list. Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct.

ICMP Error Inspection

When this feature is enabled, the FWSM creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The FWSM overwrites the packet with the translated IP addresses.

When disabled, the FWSM does not create translation sessions for intermediate nodes that generate ICMP error messages. ICMP error messages generated by the intermediate nodes between the inside host and the FWSM reach the outside host without consuming any additional NAT resource. This is undesirable when an outside host uses the traceroute command to trace the hops to the destination on the inside of the FWSM. When the FWSM does not translate the intermediate hops, all the intermediate hops appear with the mapped destination IP address.

The ICMP payload is scanned to retrieve the five-tuple from the original packet. Using the retrieved five-tuple, a lookup is performed to determine the original address of the client. The ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the mapped IP is changed to the real IP (Destination Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
 - Original packet mapped IP is changed to the real IP
 - Original packet mapped port is changed to the real Port
 - Original packet IP checksum is recalculated

ILS Inspection

The ILS inspection engine provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

The FWSM supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the FWSM border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Because ILS traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the Configuration > Firewall > Advanced > Global Timeouts pane.

ILS/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions
- Parses the LDAP packet
- Extracts IP addresses
- Translates IP addresses as necessary
- Encodes the PDU with translated addresses using BER encode functions
- Copies the newly encoded PDU back to the TCP packet
- Performs incremental TCP checksum and sequence number adjustment

ILS inspection has the following limitations:

- Referral requests and responses are not supported
- Users in multiple directories are not unified
- Single users having multiple identities in multiple directories cannot be recognized by NAT

**Note**

Because H225 call signalling traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the interval specified by the TCP option on the Configuration > Firewall > Advanced > Global Timeouts pane. By default, this interval is set at 60 minutes.

MGCP Inspection

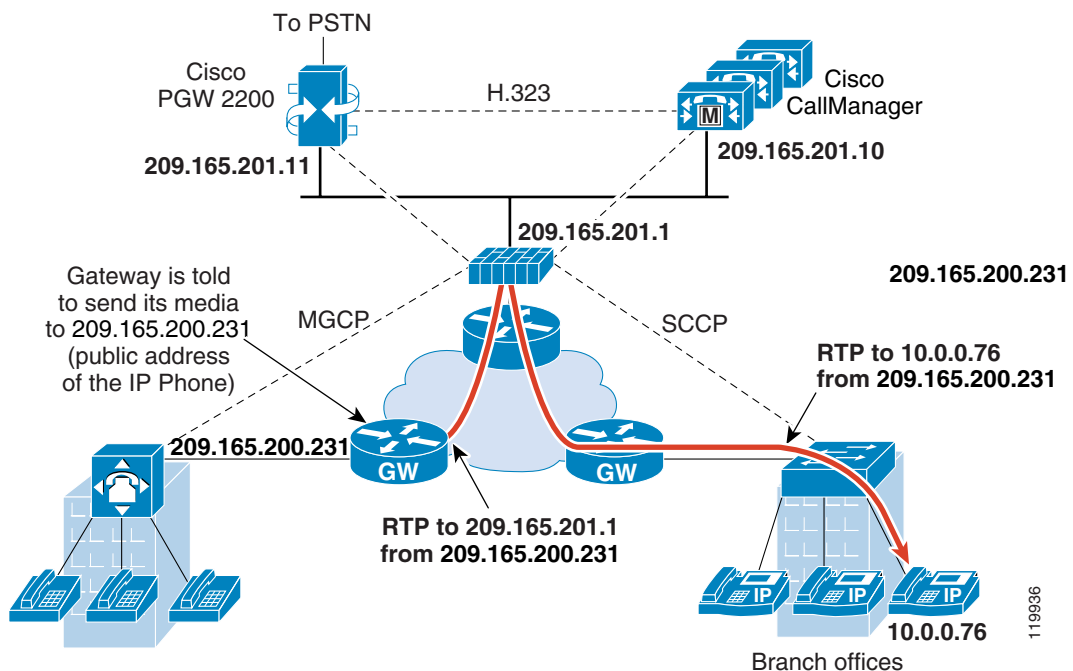
MGCP is a master/slave protocol used to control media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over

the Internet or over other packet networks. Using NAT and PAT with MGCP lets you support a large number of devices on an internal network with a limited set of external (global) addresses. Examples of media gateways are:

- Trunking gateways, that interface between the telephone network and a Voice over IP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways, that provide a traditional analog (RJ11) interface to a Voice over IP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, broad-band wireless devices.
- Business gateways, that provide a traditional digital PBX interface or an integrated soft PBX interface to a Voice over IP network.

MGCP messages are transmitted over UDP. A response is sent back to the source address (IP address and UDP port number) of the command, but the response may not arrive from the same address as the command was sent to. This can happen when multiple call agents are being used in a failover configuration and the call agent that received the command has passed control to a backup call agent, which then sends the response. [Figure 23-3](#) illustrates how NAT can be used with MGCP.

Figure 23-3 Using NAT with MGCP



MGCP endpoints are physical or virtual sources and destinations for data. Media gateways contain endpoints on which the call agent can create, modify and delete connections to establish and control media sessions with other multimedia endpoints. Also, the call agent can instruct the endpoints to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the call agent.

MGCP transactions are composed of a command and a mandatory response. There are eight types of commands:

- CreateConnection
- ModifyConnection

- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

The first four commands are sent by the call agent to the gateway. The Notify command is sent by the gateway to the call agent. The gateway may also send a DeleteConnection. The registration of the MGCP gateway with the call agent is achieved by the RestartInProgress command. The AuditEndpoint and the AuditConnection commands are sent by the call agent to the gateway.

All commands are composed of a Command header, optionally followed by a session description. All responses are composed of a Response header, optionally followed by a session description.

- The port on which the gateway receives commands from the call agent. Gateways usually listen to UDP port 2427.
- The port on which the call agent receives commands from the gateway. Call agents usually listen to UDP port 2727.

**Note**

MGCP inspection does not support the use of different IP addresses for MGCP signaling and RTP data. A common and recommended practice is to send RTP data from a resilient IP address, such as a loopback or virtual IP address; however, the FWSM requires the RTP data to come from the same address as MGCP signalling.

NetBIOS Inspection

NetBIOS inspection is enabled by default. The NetBios inspection engine translates IP addresses in the NetBios name service (NBNS) packets according to the FWSM NAT configuration.

PPTP Inspection

PPTP is a protocol for tunneling PPP traffic. A PPTP session is composed of one TCP channel and usually two PPTP GRE tunnels. The TCP channel is the control channel used for negotiating and managing the PPTP GRE tunnels. The GRE tunnels carries PPP sessions between the two hosts.

When enabled, PPTP application inspection inspects PPTP protocol packets and dynamically creates the GRE connections and xlates necessary to permit PPTP traffic. Only Version 1, as defined in RFC 2637, is supported.

PAT is only performed for the modified version of GRE [RFC 2637] when negotiated over the PPTP TCP control channel. Port Address Translation is *not* performed for the unmodified version of GRE [RFC 1701, RFC 1702].

Specifically, the FWSM inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing-call request and reply sequence are tracked. Connections and xlates are dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

As described in RFC 2637, the PPTP protocol is mainly used for the tunneling of PPP sessions initiated from a modem bank PAC (PPTP Access Concentrator) to the headend PNS (PPTP Network Server). When used this way, the PAC is the remote client and the PNS is the server.

However, when used for VPN by Windows, the interaction is inverted. The PNS is a remote single-user PC that initiates connection to the head-end PAC to gain access to a central network.

RSH Inspection

RSH inspection is enabled by default. The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

RTSP Inspection

This section describes RTSP application inspection. This section includes the following topics:

- [RTSP Inspection Overview, page 23-18](#)
- [Using RealPlayer, page 23-19](#)
- [Restrictions and Limitations, page 23-19](#)

RTSP Inspection Overview

The RTSP inspection engine lets the FWSM pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.



Note

For Cisco IP/TV, use RTSP TCP port 554 and TCP 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The FWSM only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that is used to transmit audio/video traffic, depending on the transport mode that is configured on the client.

The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

The FWSM parses Setup response messages with a status code of 200. If the response message is travelling inbound, the server is outside relative to the FWSM and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the FWSM does not need to open dynamic channels.

Because RFC 2326 does not require that the client and server ports must be in the SETUP response message, the FWSM keeps state and remembers the client ports in the SETUP message. QuickTime places the client ports in the SETUP message and then the server responds with only the server ports.

RTSP inspection does not support PAT or dual-NAT. Also, the FWSM cannot recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.

Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the FWSM, add an Access Rule from the server to the client or vice versa. For RealPlayer, change transport mode by clicking **Options>Preferences>Transport>RTSP Settings**.

If using TCP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the FWSM, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the FWSM, add an `inspect rtsp port` command.

Restrictions and Limitations

The following restrictions apply to RTSP inspection:

- The FWSM does not support multicast RTSP or RTSP messages over UDP.
- PAT is not supported.
- The FWSM does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The FWSM cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets could be fragmented and FWSM cannot perform NAT on fragmented packets.
- With Cisco IP/TV, the number of translates the FWSM performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.

SIP Inspection

This section describes SIP application inspection. This section includes the following topics:

- [SIP Inspection Overview, page 23-19](#)
- [SIP Instant Messaging, page 23-20](#)

SIP Inspection Overview

SIP, as defined by the IETF, enables call handling sessions, particularly two-party audio conferences, or “calls.” SIP works with SDP for call signalling. SDP specifies the ports for the media stream. Using SIP, the FWSM can support any SIP VoIP gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

To support SIP calls through the FWSM, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

The following limitations and restrictions apply when using PAT with SIP:

- If a remote endpoint tries to register with a SIP proxy on a network protected by the FWSM, the registration fails under very specific conditions, as follows:
 - PAT is configured for the remote endpoint.
 - The SIP registrar server is on the outside network.
 - The port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.
- If a SIP device transmits a packet in which the SDP portion has an IP address in the owner/creator field (o=) that is different than the IP address in the connection field (c=), the IP address in the o= field may not be properly translated. This is due to a limitation in the SIP protocol, which does not provide a port value in the o= field.

SIP Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. SIP supports the Chat feature on Windows XP using Windows Messenger RTC Client version 4.7.0105 only. The MESSAGE/INFO methods and 202 Accept response are used to support IM as defined in the following RFCs:

- Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO requests can come in at any time after registration/subscription. For example, two users can be online at any time, but not chat for hours. Therefore, the SIP inspection engine opens pinholes that time out according to the configured SIP timeout value. This value must be configured at least five minutes longer than the subscription duration. The subscription duration is defined in the Contact Expires value and is typically 30 minutes.

Because MESSAGE/INFO requests are typically sent using a dynamically allocated port other than port 5060, they are required to go through the SIP inspection engine.



Note

Only the Chat feature is currently supported. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

SIP inspection translates the SIP text-based messages, recalculates the content length for the SDP portion of the message, and recalculates the packet length and checksum. It dynamically opens media connections for ports specified in the SDP portion of the SIP message as address/ports on which the endpoint should listen.

SIP inspection has a database with indices CALL_ID/FROM/TO from the SIP payload. These indices identify the call, the source, and the destination. This database contains the media addresses and media ports found in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. The FWSM opens RTP/RTCP connections between the two endpoints using these media addresses/ports.

The well-known port 5060 must be used on the initial call setup (INVITE) message; however, subsequent messages may not have this port number. The SIP inspection engine opens signaling connection pinholes, and marks these connections as SIP connections. This is done for the messages to reach the SIP application and be translated.

As a call is set up, the SIP session is in the “transient” state until the media address and media port is received from the called endpoint in a Response message indicating the RTP port the called endpoint listens on. If there is a failure to receive the response messages within one minute, the signaling connection is torn down.

Once the final handshake is made, the call state is moved to active and the signaling connection remains until a BYE message is received.

If an inside endpoint initiates a call to an outside endpoint, a media hole is opened to the outside interface to allow RTP/RTCP UDP packets to flow to the inside endpoint media address and media port specified in the INVITE message from the inside endpoint. Unsolicited RTP/RTCP UDP packets to an inside interface does not traverse the FWSM, unless the FWSM configuration specifically allows it.

Skinny (SCCP) Inspection

This section describes SCCP application inspection. This section includes the following topics:

- [SCCP Inspection Overview, page 23-21](#)
- [Supporting Cisco IP Phones, page 23-22](#)
- [Restrictions and Limitations, page 23-22](#)

SCCP Inspection Overview

Skinny (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323 compliant terminals. Application layer functions in the FWSM recognize SCCP Version 3.3. There are 5 versions of the SCCP protocol: 2.4, 3.0.4, 3.1.1, 3.2, and 3.3.2. The FWSM supports all versions through Version 3.3.2.

The FWSM supports PAT and NAT for SCCP. PAT is necessary if you have more IP phones than global IP addresses for the IP phones to use. By supporting NAT and PAT of SCCP Signaling packets, Skinny application inspection ensures that all SCCP signalling and media packets can traverse the FWSM.

Normal traffic between Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration. The FWSM also supports DHCP options 150 and 66, which it accomplishes by sending the location of a TFTP server to Cisco IP Phones and other DHCP clients. Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route.

Supporting Cisco IP Phones

In topologies where Cisco CallManager is located on the higher security interface with respect to the Cisco IP Phones, if NAT is required for the Cisco CallManager IP address, the mapping must be **static** as a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An static identity entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an access list to connect to the protected TFTP server on UDP port 69. While you do need a static entry for the TFTP server, this does not have to be an identity static entry. When using NAT, an identity static entry maps to the same IP address. When using PAT, it maps to the same IP address and port.

When the Cisco IP Phones are on a *higher* security interface compared to the TFTP server and Cisco CallManager, no access list or static entry is required to allow the Cisco IP Phones to initiate the connection.

Restrictions and Limitations

The following are limitations that apply to the current version of PAT and NAT support for SCCP:

- PAT does not work with configurations containing the **alias** command.
- Outside NAT or PAT is *not* supported.

If the address of an internal Cisco CallManager is configured for NAT or PAT to a different IP address or port, registrations for external Cisco IP Phones fail because the FWSM currently does not support NAT or PAT for the file content transferred over TFTP. Although the FWSM supports NAT of TFTP messages and opens a pinhole for the TFTP file, the FWSM cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone configuration files that are transferred by TFTP during phone registration.



Note

The FWSM supports stateful failover of SCCP calls except for calls that are in the middle of call setup.

SMTP and Extended SMTP Inspection

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the FWSM and by adding monitoring capabilities.

ESMTP is an enhancement to the SMTP protocol and is similar in most respects to SMTP. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

Extended SMTP application inspection adds support for eight extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the FWSM supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, STARTLS, ONEX, VERB, CHUNKING, and private extensions are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as “500 Command unknown: 'XXX'.” Incomplete commands are discarded.

The ESMTP inspection engine changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “0” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

With SMTP inspection enabled, a Telnet session used for interactive SMTP may hang if the following rules are not observed: SMTP commands must be at least four characters in length; must be terminated with carriage return and line feed; and must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human-readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when invalid character embedded in the mail address is replaced. For more information, see RFC 821.

SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with <CR><LR>).
- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character (|) is deleted (changed to a blank space) and “<” ,”>” are only allowed if they are used to define a mail address (“>” must be preceded by “<”).
- Unexpected transition by the SMTP server.
- For unknown commands, the FWSM changes all the characters in the packet to X. In this case, the server generates an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

SNMP Inspection

SNMP application inspection lets you restrict SNMP traffic to a specific version of SNMP. Earlier versions of SNMP are less secure; therefore, denying certain SNMP versions may be required by your security policy. The FWSM can deny SNMP versions 1, 2, 2c, or 3. You control the versions permitted by creating an SNMP map.

SQL*Net Inspection

SQL*Net inspection is enabled by default.

The SQL*Net protocol consists of different packet types that the FWSM handles to make the data stream appear consistent to the Oracle applications on either side of the FWSM.

The default port assignment for SQL*Net is 1521. This is the value used by Oracle for SQL*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). Use the **class-map** command to apply SQL*Net inspection to a range of port numbers.

The FWSM translates all addresses and looks in the packets for all embedded ports to open for SQL*Net Version 1.

For SQL*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

```
(ADDRESS=(PROTOCOL=tcp) (DEV=6) (HOST=a.b.c.d) (PORT=a))
```

SQL*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the FWSM, a flag will be set in the connection data structure to expect the Data or Redirect message that follows to be translated and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be translated and port connections will be opened.

Sun RPC Inspection

This section describes Sun RPC application inspection. This section includes the following topics:

- [Sun RPC Inspection Overview, page 23-24](#)
- [SUNRPC Server, page 23-25](#)

Sun RPC Inspection Overview

The Sun RPC inspection engine enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access an Sun RPC service on a server, it must learn the port that service is running on. It does this by querying the port mapper process, usually rpcbind, on the well-known port of 111.

The client sends the Sun RPC program number of the service and the port mapper process responds with the port number of the service. The client sends its Sun RPC queries to the server, specifying the port identified by the port mapper process. When the server replies, the FWSM intercepts this packet and opens both embryonic TCP and UDP connections on that port.



Note

NAT or PAT of Sun RPC payload information is not supported.

SUNRPC Server

The Configuration > Firewall > Advanced > **SUNRPC Server** pane shows which SunRPC services can traverse the FWSM and their specific timeout, on a per server basis.

Fields

- **Interface**—Displays the interface on which the SunRPC server resides.
- **IP address**—Displays the IP address of the SunRPC server.
- **Mask**—Displays the subnet mask of the IP Address of the SunRPC server.
- **Service ID**—Displays the SunRPC program number, or service ID, allowed to traverse the FWSM.
- **Protocol**—Displays the SunRPC transport protocol (TCP or UDP).
- **Port**—Displays the SunRPC protocol port range.
- **Timeout**—Displays the idle time after which the access for the SunRPC service traffic is closed.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SUNRPC Service

The Configuration > Firewall > Advanced > **SUNRPC Server > Add/Edit SUNRPC Service** dialog box lets you specify what SunRPC services are allowed to traverse the FWSM and their specific timeout, on a per-server basis.

Fields

- **Interface Name**—Specifies the interface on which the SunRPC server resides.
- **Protocol**—Specifies the SunRPC transport protocol (TCP or UDP).
- **IP address**—Specifies the IP address of the SunRPC server.
- **Port**—Specifies the SunRPC protocol port range.
- **Mask**—Specifies the subnet mask of the IP Address of the SunRPC server.
- **Timeout**—Specifies the idle time after which the access for the SunRPC service traffic is closed. Format is HH:MM:SS.
- **Service ID**—Specifies the SunRPC program number, or service ID, allowed to traverse the FWSM.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

TFTP Inspection

TFTP inspection is enabled by default.

TFTP, described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The FWSM inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

XDMCP Inspection

XDMCP inspection is enabled by default; however, the XDMCP inspection engine is dependent upon proper configuration of the **established** command.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the FWSM must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the FWSM. Once XDMCP negotiates the port to send the display, The **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 n . Each display has a separate connection to the Xserver, as a result of the following terminal setting.

```
setenv DISPLAY Xserver:n
```

where n is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the FWSM can NAT if needed. XDMCP inspection does not support PAT.

Service Policy Field Descriptions

This section lists the field descriptions for each protocol inspection dialog box, and includes the following topics:

- [Rule Actions > Protocol Inspection Tab, page 23-27](#)
- [Select DCERPC Map, page 23-29](#)
- [Select DNS Map, page 23-29](#)
- [Select ESMTP Map, page 23-30](#)
- [Select FTP Map, page 23-30](#)
- [Select GTP Map, page 23-31](#)
- [Select H.323 Map, page 23-31](#)
- [Select HTTP Map, page 23-32](#)
- [Select IM Map, page 23-32](#)
- [Select IPSec-Pass-Thru Map, page 23-33](#)
- [Select MGCP Map, page 23-33](#)
- [Select NETBIOS Map, page 23-34](#)
- [Select RTSP Map, page 23-34](#)
- [Select SCCP \(Skinny\) Map, page 23-35](#)
- [Select SIP Map, page 23-35](#)
- [Select SNMP Map, page 23-36](#)

Rule Actions > Protocol Inspection Tab

Fields

- **CTIQBE**—Enables application inspection for the CTIQBE protocol.
- **DCERPC**—Enables application inspection for the DCERPC protocol.
 - **Configure**—Displays the **Select DCERPC Map** dialog box, which lets you select a map name to use for this protocol.
- **DNS**—Enables application inspection for the DNS protocol.
 - **Configure**—Displays the **Select DNS Map** dialog box, which lets you select a map name to use for this protocol.
- **ESMTP**—Enables application inspection for the ESMTP protocol.
 - **Configure**—Displays the **Select ESMTP Map** dialog box, which lets you select a map name to use for this protocol.
- **FTP**—Enables application inspection for the FTP protocol.
 - **Configure**—Displays the **Select FTP Map** dialog box, which lets you select a map name to use for this protocol.
- **GTP**—Enables application inspection for the GTP protocol.
 - **Configure**—Displays the **Select GTP Map** dialog box, which lets you select a map name to use for this protocol.



Note GTP inspection is not available without a special license.

- **H323 H225**—Enables application inspection for the H323 H225 protocol.

- Configure—Displays the **Select H323 H225 Map** dialog box, which lets you select a map name to use for this protocol.
- **H323 RAS**—Enables application inspection for the H323 RAS protocol.
 - Configure—Displays the **Select H323 RAS Map** dialog box, which lets you select a map name to use for this protocol.
- **HTTP**—Enables application inspection for the HTTP protocol.
 - Configure—Displays the **Select HTTP Map** dialog box, which lets you select a map name to use for this protocol.
- **ICMP**—Enables application inspection for the ICMP protocol.
- **ICMP Error**—Enables application inspection for the ICMP Error protocol.
- **ILS**—Enables application inspection for the ILS protocol.
- **IM**—Enables application inspection for the IM protocol.
 - Configure—Displays the **Select IM Map** dialog box, which lets you select a map name to use for this protocol.
- **IPSec-Pass-Thru**—Enables application inspection for the IPSec protocol.
 - Configure—Displays the **Select IPSec Map** dialog box, which lets you select a map name to use for this protocol.
- **MGCP**—Enables application inspection for the MGCP protocol.
 - Configure—Displays the **Select MGCP Map** dialog box, which lets you select a map name to use for this protocol.
- **NETBIOS**—Enables application inspection for the NetBIOS protocol.
 - Configure—Displays the **Select NETBIOS Map** dialog box, which lets you select a map name to use for this protocol.
- **PPTP**—Enables application inspection for the PPTP protocol.
- **RSH**—Enables application inspection for the RSH protocol.
- **RTSP**—Enables application inspection for the RTSP protocol.
- **SCCP SKINNY**—Enables application inspection for the Skinny protocol.
 - Configure—Displays the **Select SCCP (Skinny) Map** dialog box, which lets you select a map name to use for this protocol.
- **SIP**—Enables application inspection for the SIP protocol.
 - Configure—Displays the **Select SIP Map** dialog box, which lets you select a map name to use for this protocol.
- **SNMP**—Enables application inspection for the SNMP protocol.
 - Configure—Displays the **Select SNMP Map** dialog box, which lets you select a map name to use for this protocol.
- **SQLNET**—Enables application inspection for the SQLNET protocol.
- **SUNRPC**—Enables application inspection for the SunRPC protocol.
- **TFTP**—Enables application inspection for the TFTP protocol.
- **XDMCP**—Enables application inspection for the XDMCP protocol.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

[Inspect Map Field Descriptions, page 23-57](#)

Inspect command pages for each protocol in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

Select DCERPC Map

The **Select DCERPC Map** dialog box lets you select or create a new **DCERPC** map. A **DCERPC** map lets you change the configuration values used for **DCERPC** application inspection. The **Select DCERPC Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default DCERPC inspection map**—Specifies to use the default DCERPC map.
- **Select a DCERPC map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select DNS Map

The **Select DNS Map** dialog box lets you select or create a new **DNS** map. A **DNS** map lets you change the configuration values used for **DNS** application inspection. The **Select DNS Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default DNS inspection map**—Specifies to use the default DNS map.

- **Select a DNS map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select ESMTP Map

The **Select ESMTP Map** dialog box lets you select or create a new **ESMTP** map. An **ESMTP** map lets you change the configuration values used for **ESMTP** application inspection. The **Select ESMTP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default ESMTP inspection map**—Specifies to use the default **ESMTP** map.
- **Select an ESMTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select FTP Map

The **Select FTP Map** dialog box lets you enable strict FTP application inspection, select an FTP map, or create a new FTP map. An FTP map lets you change the configuration values used for FTP application inspection. The **Select FTP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **FTP Strict (prevent web browsers from sending embedded commands in FTP requests)**—Enables strict FTP application inspection, which causes the FWSM to drop the connection when an embedded command is included in an FTP request.
- **Use the default FTP inspection map**—Specifies to use the default FTP map.

- **Select an FTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select GTP Map

The **Select GTP Map** dialog box lets you select or create a new GTP map. A GTP map lets you change the configuration values used for GTP application inspection. The Select GTP Map table provides a list of previously configured maps that you can select for application inspection.



Note GTP inspection requires a special license. If you try to enable GTP application inspection on a FWSM without the required license, the FWSM displays an error message.

Fields

- **Use the default GTP inspection map**—Specifies to use the default GTP map.
- **Select an GTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select H.323 Map

The **Select H.323 Map** dialog box lets you select or create a new **H.323** map. An **H.323** map lets you change the configuration values used for **H.323** application inspection. The Select **H.323** Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default H.323 inspection map**—Specifies to use the default **H.323** map.

- **Select an H.323 map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select HTTP Map

The **Select HTTP Map** dialog box lets you select or create a new HTTP map. An HTTP map lets you change the configuration values used for HTTP application inspection. The Select HTTP Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default HTTP inspection map**—Specifies to use the default HTTP map.
- **Select an HTTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select IM Map

The **Select IM Map** dialog box lets you select or create a new IM map. An IM map lets you change the configuration values used for IM application inspection. The Select IM Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select IPSec-Pass-Thru Map

The **Select IPSec-Pass-Thru** dialog box lets you select or create a new **IPSec** map. An **IPSec** map lets you change the configuration values used for **IPSec** application inspection. The **Select IPSec Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default IPSec inspection map**—Specifies to use the default **IPSec** map.
- **Select an IPSec map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select MGCP Map

The **Select MGCP Map** dialog box lets you select or create a new **MGCP** map. An **MGCP** map lets you change the configuration values used for **MGCP** application inspection. The **Select MGCP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default MGCP inspection map**—Specifies to use the default **MGCP** map.
- **Select an MGCP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select NETBIOS Map

The **Select NETBIOS Map** dialog box lets you select or create a new **NetBIOS** map. A **NetBIOS** map lets you change the configuration values used for **NetBIOS** application inspection. The **Select NetBIOS Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default IM inspection map**—Specifies to use the default **NetBIOS** map.
- **Select a NetBIOS map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select RTSP Map

The **Select RTSP Map** dialog box lets you select or create a new **RTSP** map. An **RTSP** map lets you change the configuration values used for **RTSP** application inspection. The **Select RTSP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default RTSP inspection map**—Specifies to use the default **RTSP** inspection map.
- **Select a RTSP inspect map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select SCCP (Skinny) Map

The **Select SCCP (Skinny) Map** dialog box lets you select or create a new **SCCP (Skinny)** map. An **SCCP (Skinny)** map lets you change the configuration values used for **SCCP (Skinny)** application inspection. The **Select SCCP (Skinny) Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default SCCP (Skinny) inspection map**—Specifies to use the default **SCCP (Skinny)** map.
- **Select an SCCP (Skinny) map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.
- **TLS Proxy**—Lets you specify TLS proxy settings for the inspect map.
 - **Use TLS Proxy to enable inspection of encrypted traffic**—Specifies to use Transaction Layer Security Proxy to enable inspection of encrypted traffic.
 - TLS Proxy Name:**—Name of existing TLS Proxy.
 - New**—Opens the Add TLS Proxy dialog box to add a TLS Proxy.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select SIP Map

The **Select SIP Map** dialog box lets you select or create a new **SIP** map. A **SIP** map lets you change the configuration values used for **SIP** application inspection. The **Select SIP Map** table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default SIP inspection map**—Specifies to use the default **SIP** map.
- **Select a SIP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.

- Add—Opens the Add Policy Map dialog box for the inspection.
- TLS Proxy—Lets you specify TLS proxy settings for the inspect map.
 - Use TLS Proxy to enable inspection of encrypted traffic—Specifies to use Transaction Layer Security Proxy to enable inspection of encrypted traffic.

TLS Proxy Name:—Name of existing TLS Proxy.

New—Opens the Add TLS Proxy dialog box to add a TLS Proxy.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Select SNMP Map

The **Select SNMP Map** dialog box lets you select or create a new SNMP map. An SNMP map lets you change the configuration values used for SNMP application inspection. The Select SNMP Map table provides a list of previously configured maps that you can select for application inspection.

Fields

- **Use the default SNMP inspection map**—Specifies to use the default **SNMP** map.
- **Select an SNMP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- Add—Opens the Add Policy Map dialog box for the inspection.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Class Map Field Descriptions

An inspection class map matches application traffic with criteria specific to the application, such as a URL string. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

This section describes how to configure inspection class maps, and includes the following topics:

- [DNS Class Map, page 23-37](#)
- [FTP Class Map, page 23-41](#)
- [H.323 Class Map, page 23-44](#)
- [HTTP Class Map, page 23-46](#)
- [IM Class Map, page 23-51](#)
- [SIP Class Map, page 23-54](#)

DNS Class Map

The DNS Class Map panel lets you configure DNS class maps for DNS inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

Fields

- Name—Shows the DNS class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the DNS class map.
 - Value—Shows the value to match in the DNS class map.
- Description—Shows the description of the class map.
- Add—Adds match conditions for the DNS class map.
- Edit—Edits match conditions for the DNS class map.
- Delete—Deletes match conditions for the DNS class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DNS Traffic Class Map

The Add/Edit DNS Traffic Class Map dialog box lets you define a DNS class map.

Fields

- Name—Enter the name of the DNS class map, up to 40 characters in length.
- Description—Enter the description of the DNS class map.
- Add—Adds a DNS class map.
- Edit—Edits a DNS class map.
- Delete—Deletes a DNS class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DNS Match Criterion

The Add/Edit DNS Match Criterion dialog box lets you define the match criterion and value for the DNS class map.

Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- Criterion—Specifies which criterion of DNS traffic to match.
 - Header Flag—Match a DNS flag in the header.
 - Type—Match a DNS query or resource record type.
 - Class—Match a DNS query or resource record class.
 - Question—Match a DNS question.
 - Resource Record—Match a DNS resource record.
 - Domain Name—Match a domain name from a DNS query or resource record.
- Header Flag Criterion Values—Specifies the value details for the DNS header flag match.
 - Match Option—Specifies either an exact match or match all bits (bit mask match).
 - Match Value—Specifies to match either the header flag name or the header flag value.
 - Header Flag Name—Lets you select one or more header flag names to match, including AA (authoritative answer), QR (query), RA (recursion available), RD (recursion denied), TC (truncation) flag bits.
 - Header Flag Value—Lets you enter an arbitrary 16-bit value in hex to match.
- Type Criterion Values—Specifies the value details for the DNS type match.
 - DNS Type Field Name—Lists the DNS types to select.

- A—IPv4 address
- NS—Authoritative name server
- CNAME—Canonical name
- SOA—Start of a zone of authority
- TSIG—Transaction signature
- IXFR—Incremental (zone) transfer
- AXFR—Full (zone) transfer
- DNS Type Field Value—Specifies to match either a DNS type field value or a DNS type field range.
 - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
 - Range—Lets you enter a range match. Both values between 0 and 65535.
- Class Criterion Values—Specifies the value details for the DNS class match.
 - DNS Class Field Name—Specifies to match on internet, the DNS class field name.
 - DNS Class Field Value—Specifies to match either a DNS class field value or a DNS class field range.
 - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
 - Range—Lets you enter a range match. Both values between 0 and 65535.
- Question Criterion Values—Specifies to match on the DNS question section.
- Resource Record Criterion Values—Specifies to match on the DNS resource record section.
 - Resource Record— Lists the sections to match.
 - Additional—DNS additional resource record
 - Answer—DNS answer resource record
 - Authority—DNS authority resource record
- Domain Name Criterion Values—Specifies to match on the DNS domain name.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Manage Regular Expressions

The Manage Regular Expressions dialog box lets you configure [Regular Expressions](#) for use in pattern matching. Regular expressions that start with “_default” are default regular expressions and cannot be modified or deleted.

Fields

- Name—Shows the regular expression names.
- Value—Shows the regular expression definitions.
- Add—Adds a regular expression.
- Edit—Edits a regular expression.
- Delete—Deletes a regular expression.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Manage Regular Expression Class Maps

The Manage Regular Expression Class Maps dialog box lets you configure regular expression class maps. See [Regular Expressions](#) for more information.

Fields

- Name—Shows the regular expression class map name.
- Match Conditions—Shows the match type and regular expressions in the class map.
 - Match Type—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with “OR” next it, to indicate that this class map is a “match any” class map; traffic matches the class map if only one regular expression is matched.
 - Regular Expression—Lists the regular expressions included in each class map.
- Description—Shows the description of the class map.
- Add—Adds a regular expression class map.
- Edit—Edits a regular expression class map.
- Delete—Deletes a regular expression class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

FTP Class Map

The FTP Class Map panel lets you configure FTP class maps for FTP inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

Fields

- Name—Shows the FTP class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the FTP class map.
 - Value—Shows the value to match in the FTP class map.
- Description—Shows the description of the class map.
- Add—Adds an FTP class map.
- Edit—Edits an FTP class map.
- Delete—Deletes an FTP class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit FTP Traffic Class Map

The Add/Edit FTP Traffic Class Map dialog box lets you define a FTP class map.

Fields

- Name—Enter the name of the FTP class map, up to 40 characters in length.

- Description—Enter the description of the FTP class map.
- Add—Adds an FTP class map.
- Edit—Edits an FTP class map.
- Delete—Deletes an FTP class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit FTP Match Criterion

The Add/Edit FTP Match Criterion dialog box lets you define the match criterion and value for the FTP class map.

Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of FTP traffic to match.
 - Request-Command—Match an FTP request command.
 - File Name—Match a filename for FTP transfer.
 - File Type—Match a file type for FTP transfer.
 - Server—Match an FTP server.
 - User Name—Match an FTP user.
- Request-Command Criterion Values—Specifies the value details for the FTP request command match.
 - Request Command—Lets you select one or more request commands to match.
 - APPE—Append to a file.
 - CDUP—Change to the parent of the current directory.
 - DELE—Delete a file at the server site.
 - GET—FTP client command for the retr (retrieve a file) command.
 - HELP—Help information from the server.
 - MKD—Create a directory.
 - PUT—FTP client command for the stor (store a file) command.
 - RMD—Remove a directory.

RNFR—Rename from.

RNTO—Rename to.

SITE—Specify a server specific command.

STOU—Store a file with a unique name.

- File Name Criterion Values—Specifies to match on the FTP transfer filename.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- File Type Criterion Values—Specifies to match on the FTP transfer file type.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Server Criterion Values—Specifies to match on the FTP server.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- User Name Criterion Values—Specifies to match on the FTP user.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

H.323 Class Map

The H.323 Class Map panel lets you configure H.323 class maps for H.323 inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

Fields

- Name—Shows the H.323 class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the H.323 class map.
 - Value—Shows the value to match in the H.323 class map.
- Description—Shows the description of the class map.
- Add—Adds an H.323 class map.
- Edit—Edits an H.323 class map.
- Delete—Deletes an H.323 class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit H.323 Traffic Class Map

The Add/Edit H.323 Traffic Class Map dialog box lets you define a H.323 class map.

Fields

- Name—Enter the name of the H.323 class map, up to 40 characters in length.
- Description—Enter the description of the H.323 class map.
- Add—Adds an H.323 class map.
- Edit—Edits an H.323 class map.
- Delete—Deletes an H.323 class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit H.323 Match Criterion

The Add/Edit H.323 Match Criterion dialog box lets you define the match criterion and value for the H.323 class map.

Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of H.323 traffic to match.
 - Called Party—Match the called party.
 - Calling Party—Match the calling party.
 - Media Type—Match the media type.
- Called Party Criterion Values—Specifies to match on the H.323 called party.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Calling Party Criterion Values—Specifies to match on the H.323 calling party.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Media Type Criterion Values—Specifies which media type to match.
 - Audio—Match audio type.
 - Video—Match video type.
 - Data—Match data type.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

HTTP Class Map

The HTTP Class Map panel lets you configure HTTP class maps for HTTP inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

Fields

- Name—Shows the HTTP class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the HTTP class map.
 - Value—Shows the value to match in the HTTP class map.
- Description—Shows the description of the class map.
- Add—Adds an HTTP class map.
- Edit—Edits an HTTP class map.
- Delete—Deletes an HTTP class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit HTTP Traffic Class Map

The Add/Edit HTTP Traffic Class Map dialog box lets you define a HTTP class map.

Fields

- Name—Enter the name of the HTTP class map, up to 40 characters in length.
- Description—Enter the description of the HTTP class map.

- Add—Adds an HTTP class map.
- Edit—Edits an HTTP class map.
- Delete—Deletes an HTTP class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit HTTP Match Criterion

The Add/Edit HTTP Match Criterion dialog box lets you define the match criterion and value for the HTTP class map.

Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- Criterion—Specifies which criterion of HTTP traffic to match.
 - Request/Response Content Type Mismatch—Specifies that the content type in the response must match one of the MIME types in the accept field of the request.
 - Request Arguments—Applies the regular expression match to the arguments of the request.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Request Body Length—Applies the regular expression match to the body of the request with field length greater than the bytes specified.
 - Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.
 - Request Body—Applies the regular expression match to the body of the request.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Request Header Field Count—Applies the regular expression match to the header of the request with a maximum number of header fields.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Request Header Field Length—Applies the regular expression match to the header of the request with field length greater than the bytes specified.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.

- Request Header Field—Applies the regular expression match to the header of the request.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Request Header Count—Applies the regular expression match to the header of the request with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Request Header Length—Applies the regular expression match to the header of the request with length greater than the bytes specified.

- Greater Than Length—Enter a header length value in bytes.
- Request Header non-ASCII—Matches non-ASCII characters in the header of the request.
- Request Method—Applies the regular expression match to the method of the request.
 - Method—Specifies to match on a request method: bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.
 - Regular Expression—Specifies to match on a regular expression.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request URI Length—Applies the regular expression match to the URI of the request with length greater than the bytes specified.
 - Greater Than Length—Enter a URI length value in bytes.
- Request URI—Applies the regular expression match to the URI of the request.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Response Body—Applies the regex match to the body of the response.
 - ActiveX—Specifies to match on ActiveX.
 - Java Applet—Specifies to match on a Java Applet.
 - Regular Expression—Specifies to match on a regular expression.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Response Body Length—Applies the regular expression match to the body of the response with field length greater than the bytes specified.
 - Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.
- Response Header Field Count—Applies the regular expression match to the header of the response with a maximum number of header fields.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Response Header Field Length—Applies the regular expression match to the header of the response with field length greater than the bytes specified.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.

- Response Header Field—Applies the regular expression match to the header of the response.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Response Header Count—Applies the regular expression match to the header of the response with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Response Header Length—Applies the regular expression match to the header of the response with length greater than the bytes specified.

Greater Than Length—Enter a header length value in bytes.

- Response Header non-ASCII—Matches non-ASCII characters in the header of the response.
- Response Status Line—Applies the regular expression match to the status line.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

IM Class Map

The IM Class Map panel lets you configure IM class maps for IM inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

Fields

- Name—Shows the IM class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the IM class map.
 - Value—Shows the value to match in the IM class map.
- Description—Shows the description of the class map.
- Add—Adds an IM class map.
- Edit—Edits an IM class map.
- Delete—Deletes an IM class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit IM Traffic Class Map

The Add/Edit IM Traffic Class Map dialog box lets you define a IM class map.

Fields

- Name—Enter the name of the IM class map, up to 40 characters in length.
- Description—Enter the description of the IM class map.
- Add—Adds an IM class map.
- Edit—Edits an IM class map.
- Delete—Deletes an IM class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit IM Match Criterion

The Add/Edit IM Match Criterion dialog box lets you define the match criterion and value for the IM class map.

Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of IM traffic to match.
 - Protocol—Match IM protocols.
 - Service—Match IM services.
 - Version—Match IM file transfer service version.
 - Client Login Name—Match client login name from IM service.
 - Client Peer Login Name—Match client peer login name from IM service.
 - Source IP Address—Match source IP address.
 - Destination IP Address—Match destination IP address.
 - Filename—Match filename form IM file transfer service.
- Protocol Criterion Values—Specifies which IM protocols to match.
 - Yahoo! Messenger—Specifies to match Yahoo! Messenger instant messages.
 - MSN Messenger—Specifies to match MSN Messenger instant messages.

- Service Criterion Values—Specifies which IM services to match.
 - Chat—Specifies to match IM message chat service.
 - Conference—Specifies to match IM conference service.
 - File Transfer—Specifies to match IM file transfer service.
 - Games—Specifies to match IM gaming service.
 - Voice Chat—Specifies to match IM voice chat service (not available for Yahoo IM)
 - Web Cam—Specifies to match IM webcam service.
- Version Criterion Values—Specifies to match the version from the IM file transfer service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Login Name Criterion Values—Specifies to match the client login name from the IM service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Peer Login Name Criterion Values—Specifies to match the client peer login name from the IM service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Source IP Address Criterion Values—Specifies to match the source IP address of the IM service.
 - IP Address—Enter the source IP address of the IM service.
 - IP Mask—Mask of the source IP address.
- Destination IP Address Criterion Values—Specifies to match the destination IP address of the IM service.
 - IP Address—Enter the destination IP address of the IM service.
 - IP Mask—Mask of the destination IP address.
- Filename Criterion Values—Specifies to match the filename from the IM file transfer service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.

- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

SIP Class Map

The SIP Class Map panel lets you configure SIP class maps for SIP inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

Fields

- Name—Shows the SIP class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the SIP class map.
 - Value—Shows the value to match in the SIP class map.
- Description—Shows the description of the class map.
- Add—Adds a SIP class map.
- Edit—Edits a SIP class map.
- Delete—Deletes a SIP class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SIP Traffic Class Map

The Add/Edit SIP Traffic Class Map dialog box lets you define a SIP class map.

Fields

- Name—Enter the name of the SIP class map, up to 40 characters in length.
- Description—Enter the description of the SIP class map.
- Add—Adds a SIP class map.
- Edit—Edits a SIP class map.
- Delete—Deletes a SIP class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SIP Match Criterion

The Add/Edit SIP Match Criterion dialog box lets you define the match criterion and value for the SIP class map.

Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of SIP traffic to match.
 - Called Party—Match the called party as specified in the To header.
 - Calling Party—Match the calling party as specified in the From header.
 - Content Length—Match the Content Length header, between 0 and 65536.
 - Content Type—Match the Content Type header.
 - IM Subscriber—Match the SIP IM subscriber.
 - Message Path—Match the SIP Via header.
 - Request Method—Match the SIP request method.
 - Third-Party Registration—Match the requester of a third-party registration.
 - URI Length—Match a URI in the SIP headers, between 0 and 65536.
- Called Party Criterion Values—Specifies to match the called party. Applies the regular expression match.

- Regular Expression—Lists the defined regular expressions to match.
- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Calling Party Criterion Values—Specifies to match the calling party. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Content Length Criterion Values—Specifies to match a SIP content header of a length greater than specified.
 - Greater Than Length—Enter a header length value in bytes.
- Content Type Criterion Values—Specifies to match a SIP content header type.
 - SDP—Match an SDP SIP content header type.
 - Regular Expression—Match a regular expression.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- IM Subscriber Criterion Values—Specifies to match the IM subscriber. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Message Path Criterion Values—Specifies to match a SIP Via header. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Request Method Criterion Values—Specifies to match a SIP request method.
 - Request Method—Specifies a request method: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- Third-Party Registration Criterion Values—Specifies to match the requester of a third-party registration. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- URI Length Criterion Values—Specifies to match a URI of a selected type and greater than the specified length in the SIP headers.
 - URI type—Specifies to match either SIP URI or TEL URI.
 - Greater Than Length—Length in bytes.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Inspect Map Field Descriptions

This section describes how to configure inspect maps, and includes the following topics.

- [DCERPC Inspect Map, page 23-60](#)
- [DNS Inspect Map, page 23-62](#)
- [ESMTP Inspect Map, page 23-69](#)
- [FTP Inspect Map, page 23-76](#)
- [GTP Inspect Map, page 23-80](#)
- [H.225 Inspect Map, page 23-86](#)
- [HTTP Inspect Map, page 23-87](#)
- [Instant Messaging \(IM\) Inspect Map, page 23-95](#)
- [IPSec Pass Through Inspect Map, page 23-98](#)
- [MGCP Inspect Map, page 23-101](#)
- [NetBIOS Inspect Map, page 23-104](#)
- [RTSP Inspect Map, page 23-105](#)
- [SCCP \(Skinny\) Inspect Map, page 23-107](#)

- [SIP Inspect Map, page 23-112](#)
- [SNMP Inspect Map, page 23-118](#)

The algorithm the FWSM uses for stateful application inspection ensures the security of applications and services. Some applications require special handling, and specific application inspection engines are provided for this purpose. Applications that require special application inspection engines are those that embed IP addressing information in the user data packet or open secondary channels on dynamically assigned ports.

Application inspection engines work with NAT to help identify the location of embedded addressing information. This allows NAT to translate these embedded addresses and to update any checksum or other fields that are affected by the translation.

Each application inspection engine also monitors sessions to determine the port numbers for secondary channels. Many protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application inspection engine monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

In addition, stateful application inspection audits the validity of the commands and responses within the protocol being inspected. The FWSM helps to prevent attacks by verifying that traffic conforms to the RFC specifications for each protocol that is inspected.

The Inspect Maps feature lets you create inspect maps for specific protocol inspection engines. You use an inspect map to store the configuration for a protocol inspection engine. You then enable the configuration settings in the inspect map by associating the map with a specific type of traffic using a global security policy or a security policy for a specific interface.

Use the Service Policy Rules tab on the Security Policy pane to apply the inspect map to traffic matching the criteria specified in the service policy. A service policy can apply to a specific interface or to all the interfaces on the FWSM.

DCERPC	The DCERPC inspection lets you create, view, and manage DCERPC inspect maps. You can use a DCERPC map to inspect DCERPC messages between a client and endpoint mapper, and to apply NAT for the secondary connection, if needed. DCERPC is a specification for a remote procedure call mechanism.
DNS	The DNS inspection lets you create, view, and manage DNS inspect maps. You can use a DNS map to have more control over DNS messages and to protect against DNS spoofing and cache poisoning. DNS is used to resolve information about domain names, including IP addresses and mail servers.
ESMTP	The ESMTP inspection lets you create, view, and manage ESMTP inspect maps. You can use an ESMTP map for application security and protocol conformance to protect against attacks, to block senders and receivers, and to block mail relay. Extended SMTP defines protocol extensions to the SMTP standard.
FTP	The FTP inspection lets you create, view, and manage FTP inspect maps. FTP is a common protocol used for transferring files over a TCP/IP network, such as the Internet. You can use an FTP map to block specific FTP protocol methods, such as an FTP PUT, from passing through the FWSM and reaching your FTP server.

GTP	The GTP inspection lets you create, view, and manage GTP inspect maps. GTP is a relatively new protocol designed to provide security for wireless connections to TCP/IP networks, such as the Internet. You can use a GTP map to control timeout values, message sizes, tunnel counts, and GTP versions traversing the FWSM.
H.323	The H.323 inspection lets you create, view, and manage H.323 inspect maps. You can use an H.323 map to inspect RAS, H.225, and H.245 VoIP protocols, and for state tracking and filtering.
HTTP	The HTTP inspection lets you create, view, and manage HTTP inspect maps. HTTP is the protocol used for communication between Worldwide Web clients and servers. You can use an HTTP map to enforce RFC compliance and HTTP payload content type. You can also block specific HTTP methods and prevent the use of certain tunneled applications that use HTTP as the transport.
IM	The IM inspection lets you create, view, and manage IM inspect maps. You can use an IM map to control the network usage and stop leakage of confidential data and other network threats from IM applications.
IPSec Pass Through	The IPSec Pass Through inspection lets you create, view, and manage IPSec Pass Through inspect maps. You can use an IPSec Pass Through map to permit certain flows without using an access list.
MGCP	The MGCP inspection lets you create, view, and manage MGCP inspect maps. You can use an MGCP map to manage connections between VoIP devices and MGCP call agents.
NetBIOS	The NetBIOS inspection lets you create, view, and manage NetBIOS inspect maps. You can use a NetBIOS map to enforce NetBIOS protocol conformance including field count and length consistency, and message checks.
RADIUS Accounting	The RADIUS Accounting inspection lets you create, view, and manage RADIUS Accounting inspect maps. You can use a RADIUS map to protect against an overbilling attack.
RTSP	The RTSP inspection lets you create, view, and manage RTSP inspect maps. You can use an RTSP map to protect RTSP traffic, including RTSP PAT.
SCCP (Skinny)	The SCCP (Skinny) inspection lets you create, view, and manage SCCP (Skinny) inspect maps. You can use an SCCP map to perform protocol conformance checks and basic state tracking.
SIP	The SIP inspection lets you create, view, and manage SIP inspect maps. You can use a SIP map for application security and protocol conformance to protect against SIP-based attacks. SIP is a protocol widely used for internet conferencing, telephony, presence, events notification, and instant messaging.
SNMP	The SNMP inspection lets you create, view, and manage SNMP inspect maps. SNMP is a protocol used for communication between network management devices and network management stations. You can use an SNMP map to block a specific SNMP version, including SNMP v1, 2, 2c and 3.

DCERPC Inspect Map

The DCERPC pane lets you view previously configured DCERPC application inspection maps. A DCERPC map lets you change the default configuration values used for DCERPC application inspection.

DCERPC is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

This typically involves a client querying a server called the Endpoint Mapper (EPM) listening on a well known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. The FWSM allows the appropriate port number and network address and also applies NAT, if needed, for the secondary connection.

DCERPC inspect maps inspect for native TCP communication between the EPM and client on well known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and Port number are received from the applicable EPM response messages. Since a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have user configurable timeouts.

Fields

- DCERPC Inspect Maps—Table that lists the defined DCERPC inspect maps.
- Add—Configures a new DCERPC inspect map. To edit a DCERPC inspect map, select the DCERPC entry in the DCERPC Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the DCERPC Inspect Maps table.
- Security Level—Select the security level (high, medium, or low).
 - Low
 - Pinhole timeout: 00:02:00
 - Endpoint mapper service: not enforced
 - Endpoint mapper service lookup: enabled
 - Endpoint mapper service lookup timeout: 00:05:00
 - Medium—Default.
 - Pinhole timeout: 00:01:00
 - Endpoint mapper service: not enforced
 - Endpoint mapper service lookup: disabled.
 - High
 - Pinhole timeout: 00:01:00
 - Endpoint mapper service: enforced
 - Endpoint mapper service lookup: disabled
 - Customize—Opens the Add/Edit DCERPC Policy Map dialog box for additional settings.
 - Default Level—Sets the security level back to the default level of Medium.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DCERPC Policy Map

The Add/Edit DCERPC Policy Map pane lets you configure the security level and parameters for DCERPC application inspection maps.

Fields

- Name—When adding a DCERPC map, enter the name of the DCERPC map. When editing a DCERPC map, the name of the previously configured DCERPC map is shown.
- Description—Enter the description of the DCERPC map, up to 200 characters in length.
- Security Level—Select the security level (high, medium, or low).
 - Low
 - Pinhole timeout: 00:02:00
 - Endpoint mapper service: not enforced
 - Endpoint mapper service lookup: enabled
 - Endpoint mapper service lookup timeout: 00:05:00
 - Medium—Default.
 - Pinhole timeout: 00:01:00
 - Endpoint mapper service: not enforced
 - Endpoint mapper service lookup: disabled.
 - High
 - Pinhole timeout: 00:01:00
 - Endpoint mapper service: enforced
 - Endpoint mapper service lookup: disabled
 - Default Level—Sets the security level back to the default level of Medium.
- Details—Shows the Parameters to configure additional settings.
 - Pinhole Timeout—Sets the pinhole timeout. Since a client may use the server information returned by the endpoint mapper for multiple connections, the timeout value is configurable based on the client application environment. Range is from 0:0:1 to 1193:0:0. Default is 2 minutes.
 - Enforce endpoint-mapper service—Enforces endpoint mapper service during binding.
 - Enable endpoint-mapper service lookup—Enables the lookup operation of the endpoint mapper service. If disabled, the pinhole timeout is used.
 - Enforce Service Lookup Timeout—Enforces the service lookup timeout specified.
 - Service Lookup Timeout—Sets the timeout for pinholes from lookup operation.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DNS Inspect Map

The DNS pane lets you view previously configured DNS application inspection maps. A DNS map lets you change the default configuration values used for DNS application inspection.

DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. User configurable rules allow certain DNS types to be allowed, dropped, and/or logged, while others are blocked. Zone transfer can be restricted between servers with this function, for example.

The Recursion Desired and Recursion Available flags in the DNS header can be masked to protect a public server from attack if that server only supports a particular internal zone. In addition, DNS randomization can be enabled to avoid spoofing and cache poisoning of servers that either do not support randomization, or utilize a weak pseudo random number generator. Limiting the domain names that can be queried also restricts the domain names which can be queried, which protects the public server further.

A configurable DNS mismatch alert can be used as notification if an excessive number of mismatching DNS responses are received, which could indicate a cache poisoning attack. In addition, a configurable check to enforce a Transaction Signature be attached to all DNS messages is also supported.

Fields

- DNS Inspect Maps—Table that lists the defined DNS inspect maps.
- Add—Configures a new DNS inspect map. To edit a DNS inspect map, select the DNS entry in the DNS Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the DNS Inspect Maps table.
- Security Level—Select the security level (high, medium, or low).
 - Low—Default.
 - DNS Guard: enabled
 - NAT rewrite: enabled
 - Protocol enforcement: enabled
 - ID randomization: disabled
 - Message length check: enabled
 - Message length maximum: 512
 - Mismatch rate logging: disabled
 - TSIG resource record: not enforced
 - Medium

- DNS Guard: enabled
- NAT rewrite: enabled
- Protocol enforcement: enabled
- ID randomization: enabled
- Message length check: enabled
- Message length maximum: 512
- Mismatch rate logging: enabled
- TSIG resource record: not enforced
- High
 - DNS Guard: enabled
 - NAT rewrite: enabled
 - Protocol enforcement: enabled
 - ID randomization: enabled
 - Message length check: enabled
 - Message length maximum: 512
 - Mismatch rate logging: enabled
 - TSIG resource record: enforced
- Customize—Opens the Add/Edit DNS Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DNS Policy Map (Security Level)

The Add/Edit DNS Policy Map pane lets you configure the security level and additional settings for DNS application inspection maps.

Fields

- Name—When adding a DNS map, enter the name of the DNS map. When editing a DNS map, the name of the previously configured DNS map is shown.
- Description—Enter the description of the DNS map, up to 200 characters in length.
- Security Level—Select the security level (high, medium, or low).
 - Low—Default
 - DNS Guard: enabled

- NAT rewrite: enabled
- Protocol enforcement: enabled
- ID randomization: disabled
- Message length check: enabled
- Message length maximum: 512
- Mismatch rate logging: disabled
- TSIG resource record: not enforced
- Medium
 - DNS Guard: enabled
 - NAT rewrite: enabled
 - Protocol enforcement: enabled
 - ID randomization: enabled
 - Message length check: enabled
 - Message length maximum: 512
 - Mismatch rate logging: enabled
 - TSIG resource record: not enforced
- High
 - DNS Guard: enabled
 - NAT rewrite: enabled
 - Protocol enforcement: enabled
 - ID randomization: enabled
 - Message length check: enabled
 - Message length maximum: 512
 - Mismatch rate logging: enabled
 - TSIG resource record: enforced
- Default Level—Sets the security level back to the default level of Low.
- Details—Shows the Protocol Conformance, Filtering, Mismatch Rate, and Inspection tabs to configure additional settings.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DNS Policy Map (Details)

The Add/Edit DNS Policy Map pane lets you configure the security level and additional settings for DNS application inspection maps.

Fields

- **Name**—When adding a DNS map, enter the name of the DNS map. When editing a DNS map, the name of the previously configured DNS map is shown.
- **Description**—Enter the description of the DNS map, up to 200 characters in length.
- **Security Level**—Shows the security level to configure.
- **Protocol Conformance**—Tab that lets you configure the protocol conformance settings for DNS.
 - **Enable DNS guard function**—Performs a DNS query and response mismatch check using the identification field in the DNS header. One response per query is allowed to go through the FWSM.
 - **Enable NAT re-write function**—Enables IP address translation in the A record of the DNS response.
 - **Enable protocol enforcement**—Enables DNS message format check, including domain name, label length, compression, and looped pointer check.
 - **Randomize the DNS identifier for DNS query**—Randomizes the DNS identifier in the DNS query message.
 - **Enforce TSIG resource record to be present in DNS message**—Requires that a TSIG resource record be present in DNS transactions. Actions taken when TSIG is enforced:
 - Drop packet—Drops the packet (logging can be either enabled or disabled).
 - Log—Enables logging.
- **Filtering**—Tab that lets you configure the filtering settings for DNS.
 - **Global Settings**—Applies settings globally.
 - Drop packets that exceed specified maximum length (global)—Drops packets that exceed maximum length in bytes.
 - Maximum Packet Length—Enter maximum packet length in bytes.
 - **Server Settings**—Applies settings on the server only.
 - Drop packets that exceed specified maximum length—Drops packets that exceed maximum length in bytes.
 - Maximum Packet Length—Enter maximum packet length in bytes.
 - Drop packets sent to server that exceed length indicated by the RR—Drops packets sent to the server that exceed the length indicated by the Resource Record.
 - **Client Settings**—Applies settings on the client only.
 - Drop packets that exceed specified maximum length—Drops packets that exceed maximum length in bytes.
 - Maximum Packet Length—Enter maximum packet length in bytes.
 - Drop packets sent to client that exceed length indicated by the RR—Drops packets sent to the client that exceed the length indicated by the Resource Record.
- **Mismatch Rate**—Tab that lets you configure the ID mismatch rate for DNS.

- Enable Logging when DNS ID mismatch rate exceeds specified rate—Reports excessive instances of DNS identifier mismatches.
Mismatch Instance Threshold—Enter the maximum number of mismatch instances before a system message log is sent.
Time Interval—Enter the time period to monitor (in seconds).
- Inspections—Tab that shows you the DNS inspection configuration and lets you add or edit.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the DNS inspection.
 - Value—Shows the value to match in the DNS inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add DNS Inspect dialog box to add a DNS inspection.
 - Edit—Opens the Edit DNS Inspect dialog box to edit a DNS inspection.
 - Delete—Deletes a DNS inspection.
 - Move Up—Moves an inspection up in the list.
 - Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit DNS Inspect

The Add/Edit DNS Inspect dialog box lets you define the match criterion and value for the DNS inspect map.

Fields

- Single Match—Specifies that the DNS inspect has only one match statement.
- Match Type—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of DNS traffic to match.
 - Header Flag—Match a DNS flag in the header.
 - Type—Match a DNS query or resource record type.
 - Class—Match a DNS query or resource record class.
 - Question—Match a DNS question.

- Resource Record—Match a DNS resource record.
- Domain Name—Match a domain name from a DNS query or resource record.
- Header Flag Criterion Values—Specifies the value details for DNS header flag match.
 - Match Option—Specifies either an exact match or match all bits (bit mask match).
 - Match Value—Specifies to match either the header flag name or the header flag value.
 - Header Flag Name—Lets you select one or more header flag names to match, including AA (authoritative answer), QR (query), RA (recursion available), RD (recursion denied), TC (truncation) flag bits.
 - Header Flag Value—Lets you enter an arbitrary 16-bit value in hex to match.
- Type Criterion Values—Specifies the value details for DNS type match.
 - DNS Type Field Name—Lists the DNS types to select.
 - A—IPv4 address
 - NS—Authoritative name server
 - CNAME—Canonical name
 - SOA—Start of a zone of authority
 - TSIG—Transaction signature
 - IXFR—Incremental (zone) transfer
 - AXFR—Full (zone) transfer
 - DNS Type Field Value—Specifies to match either a DNS type field value or a DNS type field range.
 - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
 - Range—Lets you enter a range match. Both values between 0 and 65535.
- Class Criterion Values—Specifies the value details for DNS class match.
 - DNS Class Field Name—Specifies to match on internet, the DNS class field name.
 - DNS Class Field Value—Specifies to match either a DNS class field value or a DNS class field range.
 - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
 - Range—Lets you enter a range match. Both values between 0 and 65535.
- Question Criterion Values—Specifies to match on the DNS question section.
- Resource Record Criterion Values—Specifies to match on the DNS resource record section.
 - Resource Record— Lists the sections to match.
 - Additional—DNS additional resource record
 - Answer—DNS answer resource record
 - Authority—DNS authority resource record
- Domain Name Criterion Values—Specifies to match on DNS domain name.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.

- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Multiple Matches—Specifies multiple matches for the DNS inspection.
 - DNS Traffic Class—Specifies the DNS traffic class match.
 - Manage—Opens the Manage DNS Class Maps dialog box to add, edit, or delete DNS Class Maps.
- Actions—Primary action and log settings.
 - Primary Action—Mask, drop packet, drop connection, none.
 - Log—Enable or disable.
 - Enforce TSIG—Do not enforce, drop packet, log, drop packet and log.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Manage Class Maps

The Manage Class Map dialog box lets you configure class maps for inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, Instant Messaging (IM), and SIP.

Fields

- Name—Shows the class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the class map.
 - Value—Shows the value to match in the class map.
- Description—Shows the description of the class map.
- Add—Adds match conditions for the class map.
- Edit—Edits match conditions for the class map.
- Delete—Deletes match conditions for the class map.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

ESMTP Inspect Map

The ESMTP pane lets you view previously configured ESMTP application inspection maps. An ESMTP map lets you change the default configuration values used for ESMTP application inspection.

Since ESMTP traffic can be a main source of attack from spam, phishing, malformed messages, buffer overflows, and buffer underflows, detailed packet inspection and control of ESMTP traffic are supported. Application security and protocol conformance enforce the sanity of the ESMTP message as well as detect several attacks, block senders and receivers, and block mail relay.

Fields

- ESMTP Inspect Maps—Table that lists the defined ESMTP inspect maps.
- Add—Configures a new ESMTP inspect map. To edit an ESMTP inspect map, select the ESMTP entry in the ESMTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the ESMTP Inspect Maps table.
- Security Level—Select the security level (high, medium, or low).
 - Low—Default.
 - Log if command line length is greater than 512
 - Log if command recipient count is greater than 100
 - Log if body line length is greater than 1000
 - Log if sender address length is greater than 320
 - Log if MIME file name length is greater than 255
 - Medium
 - Obfuscate Server Banner
 - Drop Connections if command line length is greater than 512
 - Drop Connections if command recipient count is greater than 100
 - Drop Connections if body line length is greater than 1000
 - Drop Connections if sender address length is greater than 320
 - Drop Connections if MIME file name length is greater than 255
 - High
 - Obfuscate Server Banner
 - Drop Connections if command line length is greater than 512
 - Drop Connections if command recipient count is greater than 100
 - Drop Connections if body line length is greater than 1000
 - Drop Connections and log if sender address length is greater than 320

Drop Connections and log if MIME file name length is greater than 255

- MIME File Type Filtering—Opens the MIME Type Filtering dialog box to configure MIME file type filters.
- Customize—Opens the Add/Edit ESMTP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

MIME File Type Filtering

The MIME File Type Filtering dialog box lets you configure the settings for a MIME file type filter.

Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add MIME File Type Filter dialog box to add a MIME file type filter.
- Edit—Opens the Edit MIME File Type Filter dialog box to edit a MIME file type filter.
- Delete—Deletes a MIME file type filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit ESMTP Policy Map (Security Level)

The Add/Edit ESMTP Policy Map pane lets you configure the security level and additional settings for ESMTP application inspection maps.

Fields

- Name—When adding an ESMTP map, enter the name of the ESMTP map. When editing an ESMTP map, the name of the previously configured ESMTPS map is shown.
- Description—Enter the description of the ESMTP map, up to 200 characters in length.
- Security Level—Select the security level (high, medium, or low).
 - Low—Default.
 - Log if command line length is greater than 512
 - Log if command recipient count is greater than 100
 - Log if body line length is greater than 1000
 - Log if sender address length is greater than 320
 - Log if MIME file name length is greater than 255
 - Medium
 - Obfuscate Server Banner
 - Drop Connections if command line length is greater than 512
 - Drop Connections if command recipient count is greater than 100
 - Drop Connections if body line length is greater than 1000
 - Drop Connections if sender address length is greater than 320
 - Drop Connections if MIME file name length is greater than 255
 - High
 - Obfuscate Server Banner
 - Drop Connections if command line length is greater than 512
 - Drop Connections if command recipient count is greater than 100
 - Drop Connections if body line length is greater than 1000
 - Drop Connections and log if sender address length is greater than 320
 - Drop Connections and log if MIME file name length is greater than 255
 - MIME File Type Filtering—Opens the MIME Type Filtering dialog box to configure MIME file type filters.
 - Default Level—Sets the security level back to the default level of Low.
- Details—Shows the Parameters and Inspections tabs to configure additional settings.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit ESMTP Policy Map (Details)

The Add/Edit ESMTP Policy Map pane lets you configure the security level and additional settings for ESMTP application inspection maps.

Fields

- Name—When adding an ESMTP map, enter the name of the ESMTP map. When editing an ESMTP map, the name of the previously configured ESMTP map is shown.
- Description—Enter the description of the ESMTP map, up to 200 characters in length.
- Security Level—Shows the security level and mime file type filtering settings to configure.
- Parameters—Tab that lets you configure the parameters for the ESMTP inspect map.
 - Mask server banner—Enforces banner obfuscation.
 - Configure Mail Relay—Enables ESMTP mail relay.
 - Domain Name—Specifies a local domain.
 - Action—Drop connection or log.
 - Log—Enable or disable.
- Inspections—Tab that shows you the ESMTP inspection configuration and lets you add or edit.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the ESMTP inspection.
 - Value—Shows the value to match in the ESMTP inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add ESMTP Inspect dialog box to add an ESMTP inspection.
 - Edit—Opens the Edit ESMTP Inspect dialog box to edit an ESMTP inspection.
 - Delete—Deletes an ESMTP inspection.
 - Move Up—Moves an inspection up in the list.
 - Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit ESMTP Inspect

The Add/Edit ESMTP Inspect dialog box lets you define the match criterion and value for the ESMTP inspect map.

Fields

- Match Type—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of ESMTP traffic to match.
 - Body Length—Match body length at specified length in bytes.
 - Body Line Length—Match body line length matching at specified length in bytes.
 - Commands—Match commands exchanged in the ESMTP protocol.
 - Command Recipient Count—Match command recipient count greater than number specified.
 - Command Line Length—Match command line length greater than length specified in bytes.
 - EHLO Reply Parameters—Match an ESMTP ehlo reply parameter.
 - Header Length—Match header length at length specified in bytes.
 - Header To Fields Count—Match header To fields count greater than number specified.
 - Invalid Recipients Count—Match invalid recipients count greater than number specified.
 - MIME File Type—Match MIME file type.
 - MIME Filename Length—Match MIME filename.
 - MIME Encoding—Match MIME encoding.
 - Sender Address—Match sender email address.
 - Sender Address Length—Match sender email address length.
- Body Length Criterion Values—Specifies the value details for body length match.
 - Greater Than Length—Body length in bytes.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- Body Line Length Criterion Values—Specifies the value details for body line length match.
 - Greater Than Length—Body line length in bytes.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- Commands Criterion Values—Specifies the value details for command match.

- Available Commands Table:
 - AUTH
 - DATA
 - EHLO
 - ETRN
 - HELO
 - HELP
 - MAIL
 - NOOP
 - QUIT
 - RCPT
 - RSET
 - SAML
 - SOML
 - VERFY
- Add—Adds the selected command from the Available Commands table to the Selected Commands table.
- Remove—Removes the selected command from the Selected Commands table.
- Primary Action—Mask, Reset, Drop Connection, None, Limit Rate (pps).
- Log—Enable or disable.
- Rate Limit—Do not limit rate, Limit Rate (pps).
- Command Recipient Count Criterion Values—Specifies the value details for command recipient count match.
 - Greater Than Count—Specify command recipient count.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- Command Line Length Criterion Values—Specifies the value details for command line length.
 - Greater Than Length—Command line length in bytes.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- EHLO Reply Parameters Criterion Values—Specifies the value details for EHLO reply parameters match.
 - Available Parameters Table:
 - 8bitmime
 - auth
 - binarymime
 - checkpoint
 - dsn

- ecode
- etrn
- others
- pipelining
- size
- vrfy
- Add—Adds the selected parameter from the Available Parameters table to the Selected Parameters table.
- Remove—Removes the selected command from the Selected Commands table.
- Action—Reset, Drop Connection, Mask, Log.
- Log—Enable or disable.
- Header Length Criterion Values—Specifies the value details for header length match.
 - Greater Than Length—Header length in bytes.
 - Action—Reset, Drop Connection, Mask, Log.
 - Log—Enable or disable.
- Header To Fields Count Criterion Values—Specifies the value details for header To fields count match.
 - Greater Than Count—Specify command recipient count.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- Invalid Recipients Count Criterion Values—Specifies the value details for invalid recipients count match.
 - Greater Than Count—Specify command recipient count.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- MIME File Type Criterion Values—Specifies the value details for MIME file type match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Action—Reset, drop connection, log.
 - Log—Enable or disable.
- MIME Filename Length Criterion Values—Specifies the value details for MIME filename length match.
 - Greater Than Length—MIME filename length in bytes.
 - Action—Reset, Drop Connection, Log.
 - Log—Enable or disable.

- MIME Encoding Criterion Values—Specifies the value details for MIME encoding match.
 - Available Encodings table
 - 7bit
 - 8bit
 - base64
 - binary
 - others
 - quoted-printable
 - Add—Adds the selected parameter from the Available Encodings table to the Selected Encodings table.
 - Remove—Removes the selected command from the Selected Commands table.
 - Action—Reset, Drop Connection, Log.
 - Log—Enable or disable.
- Sender Address Criterion Values—Specifies the value details for sender address match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Action—Reset, Drop Connection, Log.
 - Log—Enable or disable.
- Sender Address Length Criterion Values—Specifies the value details for sender address length match.
 - Greater Than Length—Sender address length in bytes.
 - Action—Reset, Drop Connection, Log.
 - Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

FTP Inspect Map

The FTP pane lets you view previously configured FTP application inspection maps. An FTP map lets you change the default configuration values used for FTP application inspection.

FTP command filtering and security checks are provided using strict FTP inspection for improved security and control. Protocol conformance includes packet length checks, delimiters and packet format checks, command terminator checks, and command validation.

Blocking FTP based on user values is also supported so that it is possible for FTP sites to post files for download, but restrict access to certain users. You can block FTP connections based on file type, server name, and other attributes. System message logs are generated if an FTP connection is denied after inspection.

Fields

- FTP Inspect Maps—Table that lists the defined FTP inspect maps.
- Add—Configures a new FTP inspect map. To edit an FTP inspect map, select the FTP entry in the FTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the FTP Inspect Maps table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

File Type Filtering

The File Type Filtering dialog box lets you configure the settings for a file type filter.

Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add File Type Filter dialog box to add a file type filter.
- Edit—Opens the Edit File Type Filter dialog box to edit a file type filter.
- Delete—Deletes a file type filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit FTP Policy Map (Security Level)

The Add/Edit FTP Policy Map pane lets you configure the security level and additional settings for FTP application inspection maps.

Fields

- Name—When adding an FTP map, enter the name of the FTP map. When editing an FTP map, the name of the previously configured FTP map is shown.
- Description—Enter the description of the FTP map, up to 200 characters in length.
- Security Level—Select the security level (medium or low).
 - Low
 - Mask Banner Disabled
 - Mask Reply Disabled
 - Medium—Default.
 - Mask Banner Enabled
 - Mask Reply Enabled
 - File Type Filtering—Opens the Type Filtering dialog box to configure file type filters.
 - Default Level—Sets the security level back to the default level of Medium.
- Details—Shows the Parameters and Inspections tabs to configure additional settings.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit FTP Policy Map (Details)

The Add/Edit FTP Policy Map pane lets you configure the security level and additional settings for FTP application inspection maps.

Fields

- Name—When adding an FTP map, enter the name of the FTP map. When editing an FTP map, the name of the previously configured FTP map is shown.
- Description—Enter the description of the FTP map, up to 200 characters in length.
- Security Level—Shows the security level and file type filtering settings to configure.
- Parameters—Tab that lets you configure the parameters for the FTP inspect map.
 - Mask greeting banner from the server—Masks the greeting banner from the FTP server to prevent the client from discovering server information.
 - Mask reply to SYST command—Masks the reply to the syst command to prevent the client from discovering server information.
- Inspections—Tab that shows you the FTP inspection configuration and lets you add or edit.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the FTP inspection.
 - Value—Shows the value to match in the FTP inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add FTP Inspect dialog box to add an FTP inspection.
 - Edit—Opens the Edit FTP Inspect dialog box to edit an FTP inspection.
 - Delete—Deletes an FTP inspection.
 - Move Up—Moves an inspection up in the list.
 - Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit FTP Map

The Add/Edit FTP Inspect dialog box lets you define the match criterion and value for the FTP inspect map.

Fields

- Mask reply to system command—Masks reply to system command.
- Denied Request Commands—Specifies the request commands to be disallowed through the device. The connection will be closed and syslog generated when the traffic is found to have any disallowed commands.
 - APPE—Command that appends to a file.

- CDUP—Command that changes to the parent directory of the current working directory.
- DELE—Command that deletes a file.
- GET—Command that gets a file.
- HELP—Command that provides help information.
- MKD—Command that creates a directory.
- PUT—Command that sends a file.
- RMD—Command that deletes a directory.
- RNFR—Command that specifies rename-from filename.
- RNTO—Command that specifies rename-to filename.
- SITE—Commands that are specific to the server system. Usually used for remote administration.
- STOU—Command that stores a file using a unique filename.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

GTP Inspect Map

The GTP pane lets you view previously configured GTP application inspection maps. A GTP map lets you change the default configuration values used for GTP application inspection.

GTP is a relatively new protocol designed to provide security for wireless connections to TCP/IP networks, such as the Internet. You can use a GTP map to control timeout values, message sizes, tunnel counts, and GTP versions traversing the FWSM.



Note GTP inspection is not available without a special license.

Fields

- GTP Inspect Maps—Table that lists the defined GTP inspect maps.
- Add—Configures a new GTP inspect map. To edit a GTP inspect map, select the GTP entry in the GTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the GTP Inspect Maps table.
- Security Level—Security level low only.
 - Do not Permit Errors
 - Maximum Number of Tunnels: 500
 - GSN timeout: 00:30:00

- Pdp-Context timeout: 00:30:00
- Request timeout: 00:01:00
- Signaling timeout: 00:30:00.
- Tunnel timeout: 01:00:00.
- T3-response timeout: 00:00:20.
- Drop and log unknown message IDs.
- IMSI Prefix Filtering—Opens the IMSI Prefix Filtering dialog box to configure IMSI prefix filters.
- Customize—Opens the Add/Edit GTP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

IMSI Prefix Filtering

The IMSI Prefix tab lets you define the IMSI prefix to allow within GTP requests.

Fields

- Mobile Country Code—Defines the non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prepended by 0 to create a three-digit value.
- Mobile Network Code—Defines the two or three-digit value identifying the network code.
- Add—Add the specified country code and network code to the IMSI Prefix table.
- Delete—Deletes the specified country code and network code from the IMSI Prefix table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit GTP Policy Map (Security Level)

The Add/Edit GTP Policy Map pane lets you configure the security level and additional settings for GTP application inspection maps.

Fields

- Name—When adding a GTP map, enter the name of the GTP map. When editing a GTP map, the name of the previously configured GTP map is shown.
- Description—Enter the description of the GTP map, up to 200 characters in length.
- Security Level—Security level low only.
 - Do not Permit Errors
 - Maximum Number of Tunnels: 500
 - GSN timeout: 00:30:00
 - Pdp-Context timeout: 00:30:00
 - Request timeout: 00:01:00
 - Signaling timeout: 00:30:00.
 - Tunnel timeout: 01:00:00.
 - T3-response timeout: 00:00:20.
 - Drop and log unknown message IDs.
- IMSI Prefix Filtering—Opens the IMSI Prefix Filtering dialog box to configure IMSI prefix filters.
- Default Level—Sets the security level back to the default.
- Details—Shows the Parameters, IMSI Prefix Filtering, and Inspections tabs to configure additional settings.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit GTP Policy Map (Details)

The Add/Edit GTP Policy Map pane lets you configure the security level and additional settings for GTP application inspection maps.

Fields

- Name—When adding a GTP map, enter the name of the GTP map. When editing a GTP map, the name of the previously configured GTP map is shown.
- Description—Enter the description of the GTP map, up to 200 characters in length.
- Security Level—Shows the security level and IMSI prefix filtering settings to configure.
- Permit Parameters—Tab that lets you configure the permit parameters for the GTP inspect map.
 - Object Groups to Add

From object group—Specify an object group or use the browse button to open the Add Network Object Group dialog box.

To object group—Specify an object group or use the browse button to open the Add Network Object Group dialog box.

- Add—Add the specified country code and network code to the IMSI Prefix table.
- Delete—Deletes the specified country code and network code from the IMSI Prefix table.
- Permit Errors—Lets any packets that are invalid or that encountered an error during inspection to be sent through the FWSM instead of being dropped. By default, all invalid packets or packets that failed during parsing are dropped.
- General Parameters—Tab that lets you configure the general parameters for the GTP inspect map.
 - Maximum Number of Requests—Lets you change the default for the maximum request queue size allowed. The default for the maximum request queue size is 200. Specifies the maximum number of GTP requests that will be queued waiting for a response. The permitted range is from 1 to 9999999.
 - Maximum Number of Tunnels—Lets you change the default for the maximum number of tunnels allowed. The default tunnel limit is 500. Specifies the maximum number of tunnels allowed. The permitted range is from 1 to 9999999 for the global overall tunnel limit.
 - Timeouts
 - GSN timeout—Lets you change the default for the maximum period of inactivity before a GSN is removed. The default is 30 minutes. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.
 - PDP-Context timeout—Lets you change the default for the maximum period of inactivity before receiving the PDP Context for a GTP session. The default is 30 minutes. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.
 - Request Queue—Lets you change the default for the maximum period of inactivity before receiving the GTP message during a GTP session. The default is 1 minute. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.
 - Signaling—Lets you change the default for the maximum period of inactivity before a GTP signaling is removed. The default is 30 minutes. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.
 - Tunnel—Lets you change the default for the maximum period of inactivity for the GTP tunnel. The default is 1 hour. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down
 - Request timeout—Specifies the GTP Request idle timeout.
 - T3-Response timeout—Specifies the maximum wait time for a response before removing the connection.
- IMSI Prefix Filtering—Tab that lets you configure the IMSI prefix filtering for the GTP inspect map.
 - Mobile Country Code—Defines the non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prepended by 0 to create a three-digit value.
 - Mobile Network Code—Defines the two or three-digit value identifying the network code.
 - Add—Add the specified country code and network code to the IMSI Prefix table.

- Delete—Deletes the specified country code and network code from the IMSI Prefix table.
- Inspections—Tab that lets you configure the GTP inspect maps.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the GTP inspection.
 - Value—Shows the value to match in the GTP inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add GTP Inspect dialog box to add an GTP inspection.
 - Edit—Opens the Edit GTP Inspect dialog box to edit an GTP inspection.
 - Delete—Deletes an GTP inspection.
 - Move Up—Moves an inspection up in the list.
 - Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit GTP Map

The Add/Edit GTP Inspect dialog box lets you define the match criterion and value for the GTP inspect map.

Fields

- Match Type—Specifies whether traffic should match or not match the values.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of GTP traffic to match.
 - Access Point Name—Match on access point name.
 - Message ID—Match on the message ID.
 - Message Length—Match on the message length
 - Version—Match on the version.
- Access Point Name Criterion Values—Specifies an access point name to be matched. By default, all messages with valid APNs are inspected, and any APN is allowed.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Action—Drop.
- Log—Enable or disable.
- Message ID Criterion Values—Specifies the numeric identifier for the message that you want to match. The valid range is 1 to 255. By default, all valid message IDs are allowed.
 - Value—Specifies whether value is an exact match or a range.
 - Equals—Enter a value.
 - Range—Enter a range of values.
 - Action—Drop packet or limit rate (pps).
 - Log—Enable or disable.
- Message Length Criterion Values—Lets you change the default for the maximum message length for the UDP payload that is allowed.
 - Minimum value—Specifies the minimum number of bytes in the UDP payload. The range is from 1 to 65536.
 - Maximum value—Specifies the maximum number of bytes in the UDP payload. The range is from 1 to 65536.
 - Action—Drop packet.
 - Log—Enable or disable.
- Version Criterion Values—Specifies the GTP version for messages that you want to match. The valid range is 0-255. Use 0 to identify Version 0 and 1 to identify Version 1. Version 0 of GTP uses port 3386, while Version 1 uses port 2123. By default all GTP versions are allowed.
 - Value—Specifies whether value is an exact match or a range.
 - Equals—Enter a value.
 - Range—Enter a range of values.
 - Action—Drop packet.
 - Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

H.225 Inspect Map

The H.225 pane lets you view previously configured H.225 application inspection maps. An H.225 map lets you change the default configuration values used for H.225 application inspection.

Fields

- H.225 Inspect Maps—Table that lists the defined H.225 inspect maps.
- Add—Configures a new H.225 inspect map. To edit an H.225 inspect map, select the H.225 entry in the H.225 Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the H.323 Inspect Maps table.
- HSI groups associated with the selected H.225 map—Table that lists the defined HSI groups.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit HSI Group

The Add/Edit HSI Group dialog box lets you configure HSI Groups.

Fields

- Group ID—Enter the HSI group ID.
- IP Address—Enter the HSI IP address.
- Endpoints—Lets you configure the IP address and interface of the endpoints.
 - IP Address—Enter an endpoint IP address.
 - Interface—Specifies an endpoint interface.
- Add—Adds the HSI group defined.
- Delete—Deletes the selected HSI group.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit H.225 Map

The Add/Edit H.225 Inspect dialog box shows the HSI groups configured for the H.225 inspect map.

Fields

- Add—Adds an HSI group.
- Edit—Edits the selected HSI group.
- Delete—Deletes the selected HSI group.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

HTTP Inspect Map

The HTTP pane lets you view previously configured HTTP application inspection maps. An HTTP map lets you change the default configuration values used for HTTP application inspection.

HTTP application inspection scans HTTP headers and body, and performs various checks on the data. These checks prevent various HTTP constructs, content types, and tunneling and messaging protocols from traversing the FWSM.

HTTP application inspection can block tunneled applications and non-ASCII characters in HTTP requests and responses, preventing malicious content from reaching the web server. Size limiting of various elements in HTTP request and response headers, URL blocking, and HTTP server header type spoofing are also supported.

Fields

- HTTP Inspect Maps—Table that lists the defined HTTP inspect maps.
- Add—Configures a new HTTP inspect map. To edit an HTTP inspect map, select the HTTP entry in the HTTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the HTTP Inspect Maps table.
- Security Level—Select the security level (low, medium, or high).
 - Low—Default.
 - Protocol violation action: Drop connection
 - Drop connections for unsafe methods: Disabled
 - Drop connections for requests with non-ASCII headers: Disabled
 - URI filtering: Not configured
 - Advanced inspections: Not configured
 - Medium
 - Protocol violation action: Drop connection
 - Drop connections for unsafe methods: Allow only GET, HEAD, and POST
 - Drop connections for requests with non-ASCII headers: Disabled

URI filtering: Not configured

Advanced inspections: Not configured

– High

Protocol violation action: Drop connection and log

Drop connections for unsafe methods: Allow only GET and HEAD.

Drop connections for requests with non-ASCII headers: Enabled

URI filtering: Not configured

Advanced inspections: Not configured

- URI Filtering—Opens the URI Filtering dialog box to configure URI filters.
- Customize—Opens the Edit HTTP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Medium.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

URI Filtering

The URI Filtering dialog box lets you configure the settings for an URI filter.

Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add URI Filtering dialog box to add a URI filter.
- Edit—Opens the Edit URI Filtering dialog box to edit a URI filter.
- Delete—Deletes an URI filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit HTTP Policy Map (Security Level)

The Add/Edit HTTP Policy Map pane lets you configure the security level and additional settings for HTTP application inspection maps.

Fields

- Name—When adding an HTTP map, enter the name of the HTTP map. When editing an HTTP map, the name of the previously configured HTTP map is shown.
- Description—Enter the description of the HTTP map, up to 200 characters in length.
- Security Level—Select the security level (low, medium, or high).
 - Low—Default.
 - Protocol violation action: Drop connection
 - Drop connections for unsafe methods: Disabled
 - Drop connections for requests with non-ASCII headers: Disabled
 - URI filtering: Not configured
 - Advanced inspections: Not configured
 - Medium
 - Protocol violation action: Drop connection
 - Drop connections for unsafe methods: Allow only GET, HEAD, and POST
 - Drop connections for requests with non-ASCII headers: Disabled
 - URI filtering: Not configured
 - Advanced inspections: Not configured
 - High
 - Protocol violation action: Drop connection and log
 - Drop connections for unsafe methods: Allow only GET and HEAD.
 - Drop connections for requests with non-ASCII headers: Enabled
 - URI filtering: Not configured
 - Advanced inspections: Not configured
 - URI Filtering—Opens the URI Filtering dialog box which lets you configure the settings for an URI filter.
 - Default Level—Sets the security level back to the default.
- Details—Shows the Parameters and Inspections tabs to configure additional settings.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit HTTP Policy Map (Details)

The Add/Edit HTTP Policy Map pane lets you configure the security level and additional settings for HTTP application inspection maps.

Fields

- Name—When adding an HTTP map, enter the name of the HTTP map. When editing an HTTP map, the name of the previously configured HTTP map is shown.
- Description—Enter the description of the HTTP map, up to 200 characters in length.
- Security Level—Shows the security level and URI filtering settings to configure.
- Parameters—Tab that lets you configure the parameters for the HTTP inspect map.
 - Check for protocol violations—Checks for HTTP protocol violations.
Action—Drop Connection, Reset, Log.
Log—Enable or disable.
 - Spoof server string—Replaces the server HTTP header value with the specified string.
Spoof String—Enter a string to substitute for the server header field. Maximum is 82 characters.
 - Body Match Maximum—The maximum number of characters in the body of an HTTP message that should be searched in a body match. Default is 200 bytes. A large number will have a significant impact on performance.
- Inspections—Tab that shows you the HTTP inspection configuration and lets you add or edit.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the HTTP inspection.
 - Value—Shows the value to match in the HTTP inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add HTTP Inspect dialog box to add an HTTP inspection.
 - Edit—Opens the Edit HTTP Inspect dialog box to edit an HTTP inspection.
 - Delete—Deletes an HTTP inspection.
 - Move Up—Moves an inspection up in the list.
 - Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit HTTP Map

The Add/Edit HTTP Inspect dialog box lets you define the match criterion and value for the HTTP inspect map.

Fields

- Single Match—Specifies that the HTTP inspect has only one match statement.
- Match Type—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of HTTP traffic to match.
 - Request/Response Content Type Mismatch—Specifies that the content type in the response must match one of the MIME types in the accept field of the request.
 - Request Arguments—Applies the regular expression match to the arguments of the request.
Regular Expression—Lists the defined regular expressions to match.
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
Regular Expression Class—Lists the defined regular expression classes to match.
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Request Body Length—Applies the regular expression match to the body of the request with field length greater than the bytes specified.
Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.
 - Request Body—Applies the regular expression match to the body of the request.
Regular Expression—Lists the defined regular expressions to match.
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
Regular Expression Class—Lists the defined regular expression classes to match.
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Request Header Field Count—Applies the regular expression match to the header of the request with a maximum number of header fields.
Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type,

cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Request Header Field Length—Applies the regular expression match to the header of the request with field length greater than the bytes specified.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.

- Request Header Field—Applies the regular expression match to the header of the request.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Request Header Count—Applies the regular expression match to the header of the request with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Request Header Length—Applies the regular expression match to the header of the request with length greater than the bytes specified.

Greater Than Length—Enter a header length value in bytes.

- Request Header non-ASCII—Matches non-ASCII characters in the header of the request.
- Request Method—Applies the regular expression match to the method of the request.

- Method—Specifies to match on a request method: bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.
- Regular Expression—Specifies to match on a regular expression.
- Regular Expression—Lists the defined regular expressions to match.
- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request URI Length—Applies the regular expression match to the URI of the request with length greater than the bytes specified.

Greater Than Length—Enter a URI length value in bytes.
 - Request URI—Applies the regular expression match to the URI of the request.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Response Body—Applies the regex match to the body of the response.

ActiveX—Specifies to match on ActiveX.

Java Applet—Specifies to match on a Java Applet.

Regular Expression—Specifies to match on a regular expression.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
 - Response Body Length—Applies the regular expression match to the body of the response with field length greater than the bytes specified.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.
 - Response Header Field Count—Applies the regular expression match to the header of the response with a maximum number of header fields.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Response Header Field Length—Applies the regular expression match to the header of the response with field length greater than the bytes specified.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.

- Response Header Field—Applies the regular expression match to the header of the response.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Response Header Count—Applies the regular expression match to the header of the response with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Response Header Length—Applies the regular expression match to the header of the response with length greater than the bytes specified.

Greater Than Length—Enter a header length value in bytes.

- Response Header non-ASCII—Matches non-ASCII characters in the header of the response.
- Response Status Line—Applies the regular expression match to the status line.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Multiple Matches—Specifies multiple matches for the HTTP inspection.

- H323 Traffic Class—Specifies the HTTP traffic class match.
- Manage—Opens the Manage HTTP Class Maps dialog box to add, edit, or delete HTTP Class Maps.
- Action—Drop connection, reset, or log.
- Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Instant Messaging (IM) Inspect Map

The IM pane lets you view previously configured Instant Messaging (IM) application inspection maps. An Instant Messaging (IM) map lets you change the default configuration values used for Instant Messaging (IM) application inspection.

Instant Messaging (IM) application inspection provides detailed access control to control network usage. It also helps stop leakage of confidential data and propagations of network threats. A regular expression database search representing various patterns for Instant Messaging (IM) protocols to be filtered is applied. A syslog is generated if the flow is not recognized.

The scope can be limited by using an access list to specify any traffic streams to be inspected. For UDP messages, a corresponding UDP port number is also configurable. Inspection of Yahoo! Messenger and MSN Messenger instant messages are supported.

Fields

- Name—Enter the name of the inspect map, up to 40 characters in length.
- Description—Enter the description of the inspect map, up to 200 characters in length.
- IM Inspect Maps—Table that lists the defined IM inspect maps.
- Add—Configures a new IM inspect map.
- Edit—Edits the selected IM entry in the IM Inspect Maps table.
- Delete—Deletes the inspect map selected in the IM Inspect Maps table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Instant Messaging (IM) Policy Map

The Add/Edit Instant Messaging (IM) Policy Map pane lets you configure the security level and additional settings for IM application inspection maps.

Fields

- **Name**—When adding an IM map, enter the name of the IM map. When editing an IM map, the name of the previously configured IM map is shown.
- **Description**—Enter the description of the IM map, up to 200 characters in length.
- **Match Type**—Shows the match type, which can be a positive or negative match.
- **Criterion**—Shows the criterion of the IM inspection.
- **Value**—Shows the value to match in the IM inspection.
- **Action**—Shows the action if the match condition is met.
- **Log**—Shows the log state.
- **Add**—Opens the Add IM Inspect dialog box to add an IM inspection.
- **Edit**—Opens the Edit IM Inspect dialog box to edit an IM inspection.
- **Delete**—Deletes an IM inspection.
- **Move Up**—Moves an inspection up in the list.
- **Move Down**—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit IM Map

The Add/Edit IM Inspect dialog box lets you define the match criterion and value for the IM inspect map.

Fields

- **Single Match**—Specifies that the IM inspect has only one match statement.
- **Match Type**—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- **Criterion**—Specifies which criterion of IM traffic to match.
 - **Protocol**—Match IM protocols.
 - **Service**—Match IM services.
 - **Source IP Address**—Match source IP address.

- Destination IP Address—Match destination IP address.
 - Version—Match IM file transfer service version.
 - Client Login Name—Match client login name from IM service.
 - Client Peer Login Name—Match client peer login name from IM service.
 - Filename—Match filename form IM file transfer service.
- Protocol Criterion Values—Specifies which IM protocols to match.
 - Yahoo! Messenger—Specifies to match Yahoo! Messenger instant messages.
 - MSN Messenger—Specifies to match MSN Messenger instant messages.
- Service Criterion Values—Specifies which IM services to match.
 - Chat—Specifies to match IM message chat service.
 - Conference—Specifies to match IM conference service.
 - File Transfer—Specifies to match IM file transfer service.
 - Games—Specifies to match IM gaming service.
 - Voice Chat—Specifies to match IM voice chat service (not available for Yahoo IM)
 - Web Cam—Specifies to match IM webcam service.
- Source IP Address Criterion Values—Specifies to match the source IP address of the IM service.
 - IP Address—Enter the source IP address of the IM service.
 - IP Mask—Mask of the source IP address.
- Destination IP Address Criterion Values—Specifies to match the destination IP address of the IM service.
 - IP Address—Enter the destination IP address of the IM service.
 - IP Mask—Mask of the destination IP address.
- Version Criterion Values—Specifies to match the version from the IM file transfer service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Login Name Criterion Values—Specifies to match the client login name from the IM service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Peer Login Name Criterion Values—Specifies to match the client peer login name from the IM service. Applies the regular expression match.

- Regular Expression—Lists the defined regular expressions to match.
- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Filename Criterion Values—Specifies to match the filename from the IM file transfer service. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Multiple Matches—Specifies multiple matches for the IM inspection.
 - IM Traffic Class—Specifies the IM traffic class match.
 - Manage—Opens the Manage IM Class Maps dialog box to add, edit, or delete IM Class Maps.
- Action—Drop connection, reset, or log.
- Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

IPSec Pass Through Inspect Map

The IPSec Pass Through pane lets you view previously configured IPSec Pass Through application inspection maps. An IPSec Pass Through map lets you change the default configuration values used for IPSec Pass Through application inspection. You can use an IPSec Pass Through map to permit certain flows without using an access list.

Fields

- IPSec Pass Through Inspect Maps—Table that lists the defined IPSec Pass Through inspect maps.
- Add—Configures a new IPSec Pass Through inspect map. To edit an IPSec Pass Through inspect map, select the IPSec Pass Through entry in the IPSec Pass Through Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the IPSec Pass Through Inspect Maps table.
- Security Level—Select the security level (high or low).

- Low—Default.
Maximum ESP flows per client: Unlimited.
ESP idle timeout: 00:10:00.
Maximum AH flows per client: Unlimited.
AH idle timeout: 00:10:00.
- High
Maximum ESP flows per client: 10.
ESP idle timeout: 00:00:30.
Maximum AH flows per client: 10.
AH idle timeout: 00:00:30.
- Customize—Opens the Add/Edit IPSec Pass Thru Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit IPSec Pass Thru Policy Map (Security Level)

The Add/Edit IPSec Pass Thru Policy Map pane lets you configure the security level and additional settings for IPSec Pass Thru application inspection maps.

Fields

- Name—When adding an IPSec Pass Thru map, enter the name of the IPSec Pass Thru map. When editing an IPSec Pass Thru map, the name of the previously configured IPSec Pass Thru map is shown.
- Security Level—Select the security level (high or low).
 - Low—Default.
Maximum ESP flows per client: Unlimited.
ESP idle timeout: 00:10:00.
Maximum AH flows per client: Unlimited.
AH idle timeout: 00:10:00.
 - High
Maximum ESP flows per client: 10.
ESP idle timeout: 00:00:30.
Maximum AH flows per client: 10.

AH idle timeout: 00:00:30.

- Default Level—Sets the security level back to the default level of Low.
- Details—Shows additional parameter settings to configure.

Mode

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit IPSec Pass Thru Policy Map (Details)

The Add/Edit IPSec Pass Thru Policy Map pane lets you configure the security level and additional settings for IPSec Pass Thru application inspection maps.

Fields

- Name—When adding an IPSec Pass Thru map, enter the name of the IPSec Pass Thru map. When editing an IPSec Pass Thru map, the name of the previously configured IPSec Pass Thru map is shown.
- Description—Enter the description of the IPSec Pass Through map, up to 200 characters in length.
- Security Level—Shows the security level settings to configure.
- Parameters—Configures ESP and AH parameter settings.
 - Limit ESP flows per client—Limits ESP flows per client.
Maximum—Specify maximum limit.
 - Apply ESP idle timeout—Applies ESP idle timeout.
Timeout—Specify timeout.
 - Limit AH flows per client—Limits AH flows per client.
Maximum—Specify maximum limit.
 - Apply AH idle timeout—Applies AH idle timeout.
Timeout—Specify timeout.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

MGCP Inspect Map

The MGCP pane lets you view previously configured MGCP application inspection maps. An MGCP map lets you change the default configuration values used for MGCP application inspection. You can use an MGCP map to manage connections between VoIP devices and MGCP call agents.

Fields

- MGCP Inspect Maps—Table that lists the defined MGCP inspect maps.
- Add—Configures a new MGCP inspect map.
- Edit—Edits the selected MGCP entry in the MGCP Inspect Maps table.
- Delete—Deletes the inspect map selected in the MGCP Inspect Maps table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Gateways and Call Agents

The Gateways and Call Agents dialog box lets you configure groups of gateways and call agents for the map.

Fields

- Group ID—Identifies the ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The gateway IP address can only be associated with one group ID. You cannot use the same gateway with different group IDs. The valid range is from 0 to 2147483647.
- Criterion—Shows the criterion of the inspection.
- Gateways—Identifies the IP address of the media gateway that is controlled by the associated call agent. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, 2727.
- Call Agents—Identifies the IP address of a call agent that controls the MGCP media gateways in the call agent group. Normally, a call agent sends commands to the default MGCP port for gateways, 2427.
- Add—Displays the Add MGCP dialog box, which you can use to define a new application inspection map.
- Edit—Displays the Edit MGCP dialog box, which you can use to modify the application inspection map selected in the application inspection map table.
- Delete—Deletes the application inspection map selected in the application inspection map table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit MGCP Policy Map

The Add/Edit MGCP Policy Map pane lets you configure the command queue, gateway, and call agent settings for MGCP application inspection maps.

Fields

- Name—When adding an MGCP map, enter the name of the MGCP map. When editing an MGCP map, the name of the previously configured MGCP map is shown.
- Description—Enter the description of the MGCP map, up to 200 characters in length.
- Command Queue—Tab that lets you specify the permitted queue size for MGCP commands.
 - Command Queue Size—Specifies the maximum number of commands to queue. The valid range is from 1 to 2147483647.
- Gateways and Call Agents—Tab that lets you configure groups of gateways and call agents for this map.
 - Group ID—Identifies the ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The gateway IP address can only be associated with one group ID. You cannot use the same gateway with different group IDs. The valid range is from 0 to 2147483647.
 - Criterion—Shows the criterion of the inspection.
 - Gateways—Identifies the IP address of the media gateway that is controlled by the associated call agent. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, 2727.
 - Call Agents—Identifies the IP address of a call agent that controls the MGCP media gateways in the call agent group. Normally, a call agent sends commands to the default MGCP port for gateways, 2427.
 - Add—Displays the Add MGCP Group dialog box, which you can use to define a new MGCP group of gateways and call agents.
 - Edit—Displays the Edit MGCP dialog box, which you can use to modify the MGCP group selected in the Gateways and Call Agents table.
 - Delete—Deletes the MGCP group selected in the Gateways and Call Agents table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit MGCP Group

The Add/Edit MGCP Group dialog box lets you define the configuration of an MGCP group that will be used when MGCP application inspection is enabled.

Fields

- Group ID—Specifies the ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The valid range is from 0 to 2147483647.
- Gateways area
 - Gateway to Be Added—Specifies the IP address of the media gateway that is controlled by the associated call agent. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, 2727.
 - Add—Adds the specified IP address to the IP address table.
 - Delete—Deletes the selected IP address from the IP address table.
 - IP Address—Lists the IP addresses of the gateways in the call agent group.
- Call Agents
 - Call Agent to Be Added—Specifies the IP address of a call agent that controls the MGCP media gateways in the call agent group. Normally, a call agent sends commands to the default MGCP port for gateways, 2427.
 - Add—Adds the specified IP address to the IP address table.
 - Delete—Deletes the selected IP address from the IP address table.
 - IP Address—Lists the IP addresses of the call agents in the call agent group.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

NetBIOS Inspect Map

The NetBIOS pane lets you view previously configured NetBIOS application inspection maps. A NetBIOS map lets you change the default configuration values used for NetBIOS application inspection.

NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service packets and NetBIOS datagram services packets. It also enforces protocol conformance, checking the various count and length fields for consistency.

Fields

- NetBIOS Inspect Maps—Table that lists the defined NetBIOS inspect maps.
- Add—Configures a new NetBIOS inspect map.
- Edit—Edits the selected NetBIOS entry in the NetBIOS Inspect Maps table.
- Delete—Deletes the inspect map selected in the NetBIOS Inspect Maps table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit NetBIOS Policy Map

The Add/Edit NetBIOS Policy Map pane lets you configure the protocol violation settings for NetBIOS application inspection maps.

Fields

- Name—When adding a NetBIOS map, enter the name of the NetBIOS map. When editing an NetBIOS map, the name of the previously configured NetBIOS map is shown.
- Description—Enter the description of the NetBIOS map, up to 200 characters in length.
- Check for protocol violations—Checks for protocol violations and executes specified action.
 - Action—Drop packet or log.
 - Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

RTSP Inspect Map

The RTSP pane lets you view previously configured RTSP application inspection maps. An RTSP map lets you change the default configuration values used for RTSP application inspection. You can use an RTSP map to protect RTSP traffic.

Fields

- RTSP Inspect Maps—Table that lists the defined RTSP inspect maps.
- Add—Configures a new RTSP inspect map.
- Edit—Edits the selected RTSP entry in the RTSP Inspect Maps table.
- Delete—Deletes the inspect map selected in the RTSP Inspect Maps table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit RTSP Policy Map

The Add/Edit RTSP Policy Map pane lets you configure the parameters and inspections settings for RTSP application inspection maps.

Fields

- Name—When adding an RTSP map, enter the name of the RTSP map. When editing an RTSP map, the name of the previously configured RTSP map is shown.
- Description—Enter the description of the RTSP map, up to 200 characters in length.
- Parameters—Tab that lets you restrict usage on reserved ports during media port negotiation, and lets you set the URL length limit.
 - Enforce Reserve Port Protection—Lets you restrict the use of reserved ports during media port negotiation.
 - Maximum URL Length—Specifies the maximum length of the URL allowed in the message. Maximum value is 6000.
- Inspections—Tab that shows you the RTSP inspection configuration and lets you add or edit.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the RTSP inspection.
 - Value—Shows the value to match in the RTSP inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add RTSP Inspect dialog box to add a RTSP inspection.

- Edit—Opens the Edit RTSP Inspect dialog box to edit a RTSP inspection.
- Delete—Deletes a RTSP inspection.
- Move Up—Moves an inspection up in the list.
- Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit RTSP Inspect

The Add/Edit RTSP Inspect dialog box lets you define the match criterion, values, and actions for the RTSP inspect map.

Fields

- Match Type—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of RTSP traffic to match.
 - URL Filter—Match URL filtering.
 - Request Method—Match an RTSP request method.
- URL Filter Criterion Values—Specifies to match URL filtering. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- URL Filter Actions—Primary action and log settings.
 - Action—Drop connection or log.
 - Log—Enable or disable.
- Request Method Criterion Values—Specifies to match an RTSP request method.
 - Request Method—Specifies a request method: announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameters, teardown.
- Request Method Actions—Primary action settings.
 - Action—Limit rate (pps).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

SCCP (Skinny) Inspect Map

The SCCP (Skinny) pane lets you view previously configured SCCP (Skinny) application inspection maps. An SCCP (Skinny) map lets you change the default configuration values used for SCCP (Skinny) application inspection.

Skinny application inspection performs translation of embedded IP address and port numbers within the packet data, and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.

Fields

- SCCP (Skinny) Inspect Maps—Table that lists the defined SCCP (Skinny) inspect maps.
- Add—Configures a new SCCP (Skinny) inspect map. To edit an SCCP (Skinny) inspect map, select the SCCP (Skinny) entry in the SCCP (Skinny) Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the SCCP (Skinny) Inspect Maps table.
- Security Level—Select the security level (high or low).
 - Low—Default.
 - Registration: Not enforced.
 - Maximum message ID: 0x181.
 - Minimum prefix length: 4
 - Media timeout: 00:05:00
 - Signaling timeout: 01:00:00.
 - RTP conformance: Not enforced.
 - Medium
 - Registration: Not enforced.
 - Maximum message ID: 0x141.
 - Minimum prefix length: 4.
 - Media timeout: 00:01:00.
 - Signaling timeout: 00:05:00.
 - RTP conformance: Enforced.
 - Limit payload to audio or video, based on the signaling exchange: No.
 - High
 - Registration: Enforced.

Maximum message ID: 0x141.

Minimum prefix length: 4.

Maximum prefix length: 65536.

Media timeout: 00:01:00.

Signaling timeout: 00:05:00.

RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: Yes.

- Message ID Filtering—Opens the Messaging ID Filtering dialog box for configuring message ID filters.
- Customize—Opens the Add/Edit SCCP (Skinny) Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Message ID Filtering

The Message ID Filtering dialog box lets you configure the settings for a message ID filter.

Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add Message ID Filtering dialog box to add a message ID filter.
- Edit—Opens the Edit Message ID Filtering dialog box to edit a message ID filter.
- Delete—Deletes a message ID filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SCCP (Skinny) Policy Map (Security Level)

The Add/Edit SCCP (Skinny) Policy Map pane lets you configure the security level and additional settings for SCCP (Skinny) application inspection maps.

Fields

- Name—When adding an SCCP (Skinny) map, enter the name of the SCCP (Skinny) map. When editing an SCCP (Skinny) map, the name of the previously configured SCCP (Skinny) map is shown.
- Description—Enter the description of the SCCP (Skinny) map, up to 200 characters in length.
- Security Level—Select the security level (high or low).
 - Low—Default.
 - Registration: Not enforced.
 - Maximum message ID: 0x181.
 - Minimum prefix length: 4
 - Media timeout: 00:05:00
 - Signaling timeout: 01:00:00.
 - RTP conformance: Not enforced.
 - Medium
 - Registration: Not enforced.
 - Maximum message ID: 0x141.
 - Minimum prefix length: 4.
 - Media timeout: 00:01:00.
 - Signaling timeout: 00:05:00.
 - RTP conformance: Enforced.
 - Limit payload to audio or video, based on the signaling exchange: No.
 - High
 - Registration: Enforced.
 - Maximum message ID: 0x141.
 - Minimum prefix length: 4.
 - Maximum prefix length: 65536.
 - Media timeout: 00:01:00.
 - Signaling timeout: 00:05:00.
 - RTP conformance: Enforced.

- Limit payload to audio or video, based on the signaling exchange: Yes.
- Message ID Filtering—Opens the Messaging ID Filtering dialog box for configuring message ID filters.
- Default Level—Sets the security level back to the default.
- Details—Shows additional parameter, RTP conformance, and message ID filtering settings to configure.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SCCP (Skinny) Policy Map (Details)

The Add/Edit SCCP (Skinny) Policy Map pane lets you configure the security level and additional settings for SCCP (Skinny) application inspection maps.

Fields

- Name—When adding an SCCP (Skinny) map, enter the name of the SCCP (Skinny) map. When editing an SCCP (Skinny) map, the name of the previously configured SCCP (Skinny) map is shown.
- Description—Enter the description of the DNS map, up to 200 characters in length.
- Security Level—Shows the security level and message ID filtering settings to configure.
- Parameters—Tab that lets you configure the parameter settings for SCCP (Skinny).
 - Enforce endpoint registration—Enforce that Skinny endpoints are registered before placing or receiving calls.
 - Maximum Message ID—Specify value of maximum SCCP message ID allowed.
 - SCCP Prefix Length—Specifies prefix length value in Skinny messages.
 - Minimum Prefix Length—Specify minimum value of SCCP prefix length allowed.
 - Maximum Prefix Length—Specify maximum value of SCCP prefix length allowed.
 - Media Timeout—Specify timeout value for media connections.
 - Signaling Timeout—Specify timeout value for signaling connections.
- RTP Conformance—Tab that lets you configure the RTP conformance settings for SCCP (Skinny).
 - Check RTP packets for protocol conformance—Checks RTP/RTCP packets flowing on the pinholes for protocol conformance.
 - Limit payload to audio or video, based on the signaling exchange—Enforces the payload type to be audio/video based on the signaling exchange.
- Message ID Filtering—Tab that lets you configure the message ID filtering settings for SCCP (Skinny).
 - Match Type—Shows the match type, which can be a positive or negative match.

- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add Message ID Filtering dialog box to add a message ID filter.
- Edit—Opens the Edit Message ID Filtering dialog box to edit a message ID filter.
- Delete—Deletes a message ID filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—

Add/Edit Message ID Filter

The Add Message ID Filter dialog box lets you configure message ID filters.

Fields

- Match Type—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of SCCP (Skinny) traffic to match.
 - Message ID—Match specified message ID.
Message ID—Specify value of maximum SCCP message ID allowed.
 - Message ID Range—Match specified message ID range.
Lower Message ID—Specify lower value of SCCP message ID allowed.
Upper Message ID—Specify upper value of SCCP message ID allowed.
- Action—Drop packet.
- Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

SIP Inspect Map

The SIP pane lets you view previously configured SIP application inspection maps. A SIP map lets you change the default configuration values used for SIP application inspection.

SIP is a widely used protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats.

SIP application inspection provides address translation in message header and body, dynamic opening of ports and basic sanity checks. It also supports application security and protocol conformance, which enforce the sanity of the SIP messages, as well as detect SIP-based attacks.

Fields

- SIP Inspect Maps—Table that lists the defined SIP inspect maps.
- Add—Configures a new SIP inspect map. To edit a SIP inspect map, select the SIP entry in the SIP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the SIP Inspect Maps table.
- Security Level—Select the security level (high or low).
 - Low—Default.
 - SIP instant messaging (IM) extensions: Enabled.
 - Non-SIP traffic on SIP port: Permitted.
 - Hide server's and endpoint's IP addresses: Disabled.
 - Mask software version and non-SIP URIs: Disabled.
 - Ensure that the number of hops to destination is greater than 0: Enabled.
 - RTP conformance: Not enforced.
 - SIP conformance: Do not perform state checking and header validation.
 - Medium
 - SIP instant messaging (IM) extensions: Enabled.
 - Non-SIP traffic on SIP port: Permitted.
 - Hide server's and endpoint's IP addresses: Disabled.
 - Mask software version and non-SIP URIs: Disabled.
 - Ensure that the number of hops to destination is greater than 0: Enabled.
 - RTP conformance: Enforced.
 - Limit payload to audio or video, based on the signaling exchange: No
 - SIP conformance: Drop packets that fail state checking.

- High
 - SIP instant messaging (IM) extensions: Enabled.
 - Non-SIP traffic on SIP port: Denied.
 - Hide server's and endpoint's IP addresses: Disabled.
 - Mask software version and non-SIP URIs: Enabled.
 - Ensure that the number of hops to destination is greater than 0: Enabled.
 - RTP conformance: Enforced.
 - Limit payload to audio or video, based on the signaling exchange: Yes
 - SIP conformance: Drop packets that fail state checking and packets that fail header validation.
- Customize—Opens the Add/Edit SIP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SIP Policy Map (Security Level)

The Add/Edit SIP Policy Map pane lets you configure the security level and additional settings for SIP application inspection maps.

Fields

- Name—When adding a SIP, enter the name of the SIP map. When editing a SIP map, the name of the previously configured SIP map is shown.
- Description—Enter the description of the SIP map, up to 200 characters in length.
- Security Level—Select the security level (high or low).
 - Low—Default.
 - SIP instant messaging (IM) extensions: Enabled.
 - Non-SIP traffic on SIP port: Permitted.
 - Hide server's and endpoint's IP addresses: Disabled.
 - Mask software version and non-SIP URIs: Disabled.
 - Ensure that the number of hops to destination is greater than 0: Enabled.
 - RTP conformance: Not enforced.
 - SIP conformance: Do not perform state checking and header validation.
 - Medium
 - SIP instant messaging (IM) extensions: Enabled.

Non-SIP traffic on SIP port: Permitted.

Hide server's and endpoint's IP addresses: Disabled.

Mask software version and non-SIP URIs: Disabled.

Ensure that the number of hops to destination is greater than 0: Enabled.

RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: No

SIP conformance: Drop packets that fail state checking.

– High

SIP instant messaging (IM) extensions: Enabled.

Non-SIP traffic on SIP port: Denied.

Hide server's and endpoint's IP addresses: Disabled.

Mask software version and non-SIP URIs: Enabled.

Ensure that the number of hops to destination is greater than 0: Enabled.

RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: Yes

SIP conformance: Drop packets that fail state checking and packets that fail header validation.

– Default Level—Sets the security level back to the default.

- Details—Shows additional filtering, IP address privacy, hop count, RTP conformance, SIP conformance, field masking, and inspections settings to configure.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SIP Policy Map (Details)

The Add/Edit SIP Policy Map pane lets you configure the security level and additional settings for SIP application inspection maps.

Fields

- Name—When adding a SIP, enter the name of the SIP map. When editing a SIP map, the name of the previously configured SIP map is shown.
- Description—Enter the description of the SIP map, up to 200 characters in length.
- Security Level—Shows the security level settings to configure
- Filtering—Tab that lets you configure the filtering settings for SIP.

- Enable SIP instant messaging (IM) extensions—Enables Instant Messaging extensions. Default is enabled.
 - Permit non-SIP traffic on SIP port—Permits non-SIP traffic on SIP port. Permitted by default.
- IP Address Privacy—Tab that lets you configure the IP address privacy settings for SIP.
 - Hide server’s and endpoint’s IP addresses—Enables IP address privacy. Disabled by default.
- Hop Count—Tab that lets you configure the hop count settings for SIP.
 - Ensure that number of hops to destination is greater than 0—Enables check for the value of Max-Forwards header is zero.
Action—Drop packet, Drop Connection, Reset, Log.
Log—Enable or Disable.
- RTP Conformance—Tab that lets you configure the RTP conformance settings for SIP.
 - Check RTP packets for protocol conformance—Checks RTP/RTCP packets flowing on the pinholes for protocol conformance.
Limit payload to audio or video, based on the signaling exchange—Enforces payload type to be audio/video based on the signaling exchange.
- SIP Conformance—Tab that lets you configure the SIP conformance settings for SIP.
 - Enable state transition checking—Enables SIP state checking.
Action—Drop packet, Drop Connection, Reset, Log.
Log—Enable or Disable.
 - Enable strict validation of header fields—Enables validation of SIP header fields.
Action—Drop packet, Drop Connection, Reset, Log.
Log—Enable or Disable.
- Field Masking—Tab that lets you configure the field masking settings for SIP.
 - Inspect non-SIP URIs—Enables non-SIP URI inspection in Alert-Info and Call-Info headers.
Action—Mask or Log.
Log—Enable or Disable.
 - Inspect server’s and endpoint’s software version—Inspects SIP endpoint software version in User-Agent and Server headers.
Action—Mask or Log.
Log—Enable or Disable.
- Inspections—Tab that shows you the SIP inspection configuration and lets you add or edit.
 - Match Type—Shows the match type, which can be a positive or negative match.
 - Criterion—Shows the criterion of the SIP inspection.
 - Value—Shows the value to match in the SIP inspection.
 - Action—Shows the action if the match condition is met.
 - Log—Shows the log state.
 - Add—Opens the Add SIP Inspect dialog box to add a SIP inspection.
 - Edit—Opens the Edit SIP Inspect dialog box to edit a SIP inspection.
 - Delete—Deletes a SIP inspection.

- Move Up—Moves an inspection up in the list.
- Move Down—Moves an inspection down in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SIP Inspect

The Add/Edit SIP Inspect dialog box lets you define the match criterion and value for the SIP inspect map.

Fields

- Single Match—Specifies that the SIP inspect has only one match statement.
- Match Type—Specifies whether traffic should match or not match the values.
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of SIP traffic to match.
 - Called Party—Match a called party as specified in the To header.
 - Calling Party—Match a calling party as specified in the From header.
 - Content Length—Match a content length header.
 - Content Type—Match a content type header.
 - IM Subscriber—Match a SIP IM subscriber.
 - Message Path—Match a SIP Via header.
 - Request Method—Match a SIP request method.
 - Third-Party Registration—Match the requester of a third-party registration.
 - URI Length—Match a URI in the SIP headers.
- Called Party Criterion Values—Specifies to match the called party. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Calling Party Criterion Values—Specifies to match the calling party. Applies the regular expression match.

- Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Content Length Criterion Values—Specifies to match a SIP content header of a length greater than specified.
 - Greater Than Length—Enter a header length value in bytes.
- Content Type Criterion Values—Specifies to match a SIP content header type.
 - SDP—Match an SDP SIP content header type.
 - Regular Expression—Match a regular expression.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- IM Subscriber Criterion Values—Specifies to match the IM subscriber. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Message Path Criterion Values—Specifies to match a SIP Via header. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
 - Regular Expression Class—Lists the defined regular expression classes to match.
 - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request Method Criterion Values—Specifies to match a SIP request method.
 - Request Method—Specifies a request method: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- Third-Party Registration Criterion Values—Specifies to match the requester of a third-party registration. Applies the regular expression match.
 - Regular Expression—Lists the defined regular expressions to match.
 - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- URI Length Criterion Values—Specifies to match a URI in the SIP headers greater than specified length.
 - URI type—Specifies to match either SIP URI or TEL URI.
 - Greater Than Length—Length in bytes.
- Multiple Matches—Specifies multiple matches for the SIP inspection.
 - SIP Traffic Class—Specifies the SIP traffic class match.
 - Manage—Opens the Manage SIP Class Maps dialog box to add, edit, or delete SIP Class Maps.
- Actions—Primary action and log settings.
 - Action—Drop packet, drop connection, reset, log. Note: Limit rate (pps) action is available for request methods invite and register.
 - Log—Enable or disable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

SNMP Inspect Map

The SNMP pane lets you view previously configured SNMP application inspection maps. An SNMP map lets you change the default configuration values used for SNMP application inspection.

Fields

- Map Name—Lists previously configured application inspection maps. Check a map and click **Edit** to view or change an existing map.
- Add—Configures a new SNMP inspect map.
- Edit—Edits the selected SNMP entry in the SNMP Inspect Maps table.
- Delete—Deletes the inspect map selected in the SNMP Inspect Maps table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit SNMP Map

The Add/Edit SNMP Map dialog box lets you create a new SNMP map for controlling SNMP application inspection.

Fields

- SNMP Map Name—Defines the name of the application inspection map.
- SNMP version 1—Enables application inspection for SNMP version 1.
- SNMP version 2 (party based)—Enables application inspection for SNMP version 2.
- SNMP version 2c (community based)—Enables application inspection for SNMP version 2c.
- SNMP version 3—Enables application inspection for SNMP version 3.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

