CHAPTER 1

Configuring Device Access Settings on Firewall Devices

The Device Access section, located under the Device Admin folder in the Policy selector, contains pages for defining access to firewall devices.

This chapter contains the following topics:

Configuring Console Timeout

Use the Console page to specify a timeout value for inactive console sessions. When the time limit you specify is reached, the console session is closed.

In the **Console Timeout** field, enter the number of minutes a console session can remain idle before the device closes it. Valid values are 0 to 60 minutes. To prevent a console session from timing out, enter 0.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Console** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Console** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Chapter 1, “Configuring Device Access Settings on Firewall Devices”

HTTP Page

Use the table on the HTTP page to manage the interfaces configured to access the HTTP server on a device, as well as HTTP redirect to HTTPS on those interfaces. You also can enable or disable the HTTP server on the device from this page. Administrative access by the specific device manager requires HTTPS access.

Note To redirect HTTP, the interface requires an access list that permits HTTP. Otherwise, the interface cannot listen to port 80, or to any other port that you configure for HTTP.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > HTTP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > HTTP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 1-1 HTTP Page

Element	Description
HTTP Interface table	Use the Add Row, Edit Row, and Delete Row buttons below this table to manage device interfaces on which HTTP-to-HTTPS redirect is configured. Add Row and Edit Row open the HTTP Configuration Dialog Box, page 1-2.
Enable HTTP Server	Enables or disables the HTTP server on the device. When enabled, you can specify a communications **Port** for the server. The Port range is 1 to 65535; the default is 443.

HTTP Configuration Dialog Box

Use the HTTP Configuration dialog box to add or edit a host or network that will be allowed to access the HTTP server on the device via a specific interface; you also can enable and disable HTTP redirect.

Navigation Path

You can access the HTTP Configuration dialog box from the HTTP Page, page 1-2.

Field Reference

Table 1-2 HTTP Configuration Dialog Box

Element	Description
Interface Name	Enter or Select the interface on which access to the HTTP server on the device is allowed.

Table 1-2 HTTP Configuration Dialog Box (Continued)

Element	Description
IP Address/Netmask	Enter the IP address and netmask, separated by a forward slash ("/") of the host or network that is permitted to establish an HTTP connection with the device. Alternately, you can click Select to select a Networks/Hosts object.
Enable Authentication Certificate	Select this option to require user certificate authentication in order to establish an HTTP connection. On ASA and PIX 8.0(2)+ devices, you can specify the authentication **Port**.
Redirect port	The port on which the security appliance listens for HTTP requests, which it then redirects to HTTPS. To disable HTTP redirect, ensure that this field is blank.

Configuring ICMP

Use the table on the ICMP page to manage Internet Control Message Protocol (ICMP) rules, which specify the addresses of all hosts or networks that are allowed or denied ICMP access to specific interfaces on the security device.

The ICMP rules control ICMP traffic that terminates on any device interface. If no ICMP control list is configured, the device accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the device does not respond to ICMP echo requests directed to a broadcast address.

It is recommended that permission is always granted for the ICMP Unreachable message (type 3). Denying ICMP Unreachable messages disables ICMP Path MTU discovery, which can halt IPsec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If an ICMP control list is configured, the device uses a first match to the ICMP traffic, followed by an implicit deny all. That is, if the first matched entry is a permit entry, the processing of the ICMP packet continues. If the first matched entry is a deny entry, or an entry is not matched, the device discards the ICMP packet and generates a syslog message. If an ICMP control list is not configured, a permit rule is assumed in all cases.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > ICMP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > ICMP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 1-3 ICMP Page

Element	Description
ICMP Rules Table	Use the Add Row, Edit Row, and Delete Row buttons below this table to manage ICMP rules. Add Row opens the Add ICMP dialog box, while Edit Row opens the Edit ICMP dialog box. See Add and Edit ICMP Dialog Boxes, page 1-4 for information about these dialog boxes.
ICMP Unreachable Parameters	
Rate Limit	For ICMP traffic that terminates at an interface on this device, the maximum number of ICMP Unreachable messages the device can transmit per second. This value can be between 1 and 100 messages per second; the default is 1 message per second.
Burst Size	The burst size for ICMP Unreachable messages; this can be a value between 1 and 10. **Note** This parameter is not currently used by the system, so you can choose any value.

Add and Edit ICMP Dialog Boxes

Use the Add ICMP dialog box to add an ICMP rule, which specifies a host/network that is allowed or denied the specified ICMP access on the specified device interface.

Note The Edit ICMP dialog box is virtually identical to the Add ICMP dialog box, and is used to modify existing ICMP rules. The following descriptions apply to both dialog boxes.

Navigation Path

You can access the Add or Edit ICMP dialog boxes from the Configuring ICMP, page 1-3.

Field Reference

Table 1-4 Add and ICMP Dialog Boxes

Element	Description
Action	Whether this rule permits or denies the selected ICMP Service message from the specified Network on the specified Interface. Choose: • **Permit** – ICMP messages from the specified networks/hosts are allowed to the specified interface. • **Deny** – ICMP messages from the specified networks/hosts to the specified interface are dropped.
ICMP Service	Enter or Select the specific ICMP service message to which the rule applies.
Interface	Enter or Select the device interface to which these ICMP messages are directed.

Table 1-4 Add and ICMP Dialog Boxes (Continued)

Element	Description
Network	Enter a host name or IP address, or Select a Networks/Hosts object, to define the specified ICMP message source.

Configuring Management Access

Use the Management Access page to enable or disable access on a high-security interface so you can perform management functions on the device. You can enable this feature on an internal interface to allow management functions to be performed on the interface over an IPsec VPN tunnel. You can enable the Management Access feature on only one interface at a time.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Management Access** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Management Access** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Enabling and Disabling Management Access

In the **Management Access Interface** field, enter the name of the device interface that is to permit management access connections. You can click Select to select the interface from a list of interface objects.

You can enable the Management Access feature on only one interface at a time.

Clear the Management Access Interface field to disable management access.

Configuring Secure Shell Access

Use the Secure Shell page to configure rules that permit administrative access to a security device using the SSH protocol. The rules restrict SSH access to a specific IP address and netmask. Any SSH connection attempts that comply with these rules must then be authenticated by an AAA server or Telnet password.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Secure Shell** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Secure Shell** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 1-5 Secure Shell Page

Element	Description
SSH Version	Specify the SSH version(s) accepted by the device: choose **1**, **2**, or **1 and 2**. By default, SSH Version 1 and SSH Version 2 connections are accepted.
Timeout	Enter the number of minutes, 1 to 60, the Secure Shell session can remain idle before the device closes it. The default value is 5 minutes.
Allowed Hosts table	Use the Add Row, Edit Row, and Delete Row buttons below this table to manage the hosts allowed to connect to the security device via SSH. Add Row opens the Add Host dialog box, while Edit Row opens the Edit Host dialog box. See Add and Edit SSH Host Dialog Boxes, page 1-6 for information about these dialog boxes.
Enable Secure Copy	Check this box to enable the secure copy (SCP) server on the security appliance. This allows the appliance to function as an SCP server for transferring files from/to the device. Only clients that are allowed to access the security appliance using SSH can establish a secure copy connection. This implementation of the secure copy server has the following limitations: • The server can accept and terminate connections for secure copy, but cannot initiate them. • The server does not have directory support. The lack of directory support limits remote client access to the security appliance internal files. • The server does not support banners. • The server does not support wildcards. • The security appliance license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Add and Edit SSH Host Dialog Boxes

Use the Add Host dialog box to add an SSH access rule.

Note The Edit Host dialog box is virtually identical to the Add Host dialog box, and is used to modify existing SSH access rules. The following descriptions apply to both dialog boxes.

Navigation Path

You can access the Add and Edit Host dialog boxes from the Configuring Secure Shell Access, page 1-5.

Field Reference

Table 1-6 Add and Edit Host Dialog Boxes

Element	Description
Interface	Enter or Select the name of the device interface on which SSH connections are permitted.
IP Addresses	Enter the name or IP address for each host or network that is permitted to establish an SSH connection with the security device on the specified interface; use commas to separate multiple entries. You also can click Select to select Networks/Hosts objects from a list.

Configuring SNMP

Simple Network Management Protocol (SNMP) defines a standard way for network management stations running on PCs or workstations to monitor the health and status of many types of devices, including switches, routers and security appliances. You can use the SNMP page to configure a firewall device for monitoring by SNMP management stations.

The Simple Network Management Protocol (SNMP) enables monitoring of network devices from a central location. Cisco security appliances support network monitoring using SNMP versions 1 and 2c, as well as traps and SNMP read access; SNMP write access is not supported.

You can configure a security appliance to send “traps” (event notifications) to a network management station (NMS), or you can use the NMS to browse the management information bases (MIBs) on the security appliance. Use CiscoWorks for Windows or any other SNMP MIB-II-compliant browser to receive SNMP traps and browse a MIB.

The security appliance has an SNMP agent that notifies designated management stations if specified events occur, for example, when a link in the network goes up or down. The notification includes an SNMP system object ID (OID), identifying the device to the management stations. The security appliance SNMP agent also replies when a management station asks for information.

SNMP MIBs and OIDs

An SNMP trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in Management Information Bases (MIBs), which can be either standard or enterprise-specific.

Standard traps and MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Standard traps are compiled into the security appliance software. If needed, you can also download RFCs, standard MIBS, and standard traps from the IETF website: http://www.ietf.org/.

For Cisco MIB files and OIDs, refer to: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. OIDs may be downloaded from this FTP site: ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz.

This section contains the following topics:

SNMP Terminology

Here are definitions for some common SNMP terms:

- **Agent** – The SNMP server running on the security appliance. The agent responds to requests for information and action from the management station. The agent also controls access to its management information base (MIB), the collection of data objects that can be viewed or changed by the SNMP manager.
- **Management stations** – The PCs or workstations set up to monitor SNMP events and manage devices such as the security appliance. Management stations can also receive messages about events which require attention, such as hardware failures.
- **MIBs** – The agent maintains standardized data structures called Management Information Bases (MIBs), used to collect information, such as packet, connection and error counters, and buffer usage and failover status. A number of MIBs are defined for specific products, and for the common protocols and hardware standards used by most network devices. SNMP management stations can browse MIBs, or request only specific fields. In some applications, MIB data can be modified for administrative purposes.
- **OID** – The SNMP standard assigns a system object ID (OID) so that a management station can uniquely identify network devices with SNMP agents, and indicate to users the source of information monitored and displayed.
- **Traps** – Specified events that generate a message from the SNMP agent to the management station. Events include alarm conditions such as linkup, linkdown, coldstart, authentication, or syslog events.

SNMP Page

Use the SNMP page to configure the security appliance for monitoring by Simple Network Management Protocol (SNMP) management stations.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > SNMP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Configuring SNMP, page 1-7

Field Reference

Table 1-7 SNMP Page

Element	Description
Enable SNMP Servers	When this option is selected, the security device provides SNMP information on the specified interface(s). You can deselect this option to disable SNMP monitoring while retaining the configuration information.

Table 1-7 SNMP Page (Continued)

Element	Description
Read Community String Confirm	Enter the password used by a SNMP management station when sending requests to this device. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The security device uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces are not permitted. Repeat the password in the **Confirm** field to ensure it was entered correctly.
System Administrator Name	Enter the name of the device administrator or other contact person. This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
Location	Describe the location of this security device (for example, ***Building 42, Sector 54***). This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
Port (PIX 7.x, ASA and FWSM 3.x only)	Specify the port on which incoming requests will be accepted. The default is 161.
Configure SNMP Traps	Click this button to configure SNMP traps in the SNMP Trap Configuration Dialog Box, page 1-9.
SNMP Hosts table	This table lists the SNMP management stations that can access the security appliance. This is a standard Security Manager table, with Add Row, Edit Row and Delete Row buttons, as described in Using Tables, page 1-36. The Add Row and Edit Row buttons open the Add SNMP Host Access Entry Dialog Box, page 1-12, used to add and edit management station host entries.

SNMP Trap Configuration Dialog Box

Use the SNMP Trap Configuration dialog box to configure SNMP traps (event notifications) for the selected security device.

Traps are different than browsing; they are unsolicited “comments” from the managed device to the management station for certain events, such as ***linkup***, ***linkdown***, and ***syslog event generated***.

An SNMP object ID (OID) for the device appears in SNMP event traps sent from the device. The SNMP service running on a security device performs two functions:

- Replies to SNMP requests from management stations.
- Sends traps to management stations or other devices that are registered to receive them from the security appliance.

Cisco security devices support three types of traps:

- firewall
- generic
- syslog

In the SNMP Trap Configuration dialog box, available traps are presented on four tabbed panels: Standard, Entity MIB, Resource, and Other.

Navigation Path

You can access the SNMP Trap Configuration dialog box from the SNMP Page, page 1-8.

Related Topics

- Configuring SNMP, page 1-7
- Add SNMP Host Access Entry Dialog Box, page 1-12

Field Reference

Table 1-8 SNMP Trap Configuration Dialog Box

Element	Description
Enable All SNMP Traps	Check this box to quickly select all traps on all four tabbed panels.
Enable Syslog Traps	Check this box to enable transmission of trap-related syslog messages. The severity level for syslog messages trapped is set on the Logging Filters Page, page 1-7.
Select the desired event-notification traps on the following four tabbed panels. Note that only the traps applicable to the selected device are displayed in the dialog box.	
Standard	• **Authentication** – Unauthorized SNMP access. This authentication failure occurs for packets with an incorrect community string. • **Link Up** – One of the device's communication links has become available (it has "come up"), as indicated in the notification. • **Link Down** – One of the device's communication links has failed, as indicated in the notification. • **Cold Start** – The device is reinitializing itself such that its configuration or the protocol entity implementation may be altered. • **Warm Start** – The device is reinitializing itself such that its configuration and the protocol entity implementation is unaltered.

Table 1-8 SNMP Trap Configuration Dialog Box (Continued)

Element	Description
Entity MIB	• **Field Replaceable Unit Insert** – A Field Replaceable Unit (FRU) has been inserted, as indicated. (FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc.) • **Field Replaceable Unit Remove** – A Field Replaceable Unit (FRU) has been removed, as indicated in the notification. • **Configuration Change** – There has been a hardware change, as indicated in the notification. • **Fan Failure** – A device cooling fan has failed, as indicated in the notification. • **CPU Temperature** – Temperature of the central processing unit has reached the configured limit. • **Power Supply Failure** – A device power supply has failed, as indicated in the notification. • **Redundancy Switchover** – Switchover occurred for redundant component, as indicated in the notification. • **Alarm Asserted** – The condition described by the alarm exists. • **Alarm Cleared** – The condition described by the alarm does not exist.
Resource	• **Connection Limit Reached** – This trap indicates that a connection attempt was rejected because the configured connections limit has been reached. • **Resource Limit Reached** – This notification is generated when the configured resource limit is reached, as described in the notification. • **Resource Rate Limit Reached** – This notification is generated when the configured resource rate limit is reached, as described in the notification

Table 1-8 SNMP Trap Configuration Dialog Box (Continued)

Element	Description
Other	• **IPSec Start** – IPsec has started, as indicated in the notification. • **IPSec Stop** – IPsec has stopped, as indicated in the notification. • **IKEv2 Start** – Internet Key Exchange version 2 (IKEv2) exchange initiated. • **IKEv2 Stop** – Internet Key Exchange version 2 (IKEv2) exchange terminated. • **Memory Threshold** – Available free memory has fallen below configured threshold, as indicated in the notification. • **Remote Access Session Threshold Exceeded** – The number of remote access sessions has reach the defined limit, as indicated in the notification. • **CPU Rising Threshold** – This notification is triggered when utilization of CPU resources exceeds the specified Percentage for a specified Period of time: **Percentage** – Enter the desired upper limit of CPU resource usage as a percentage of total available. Value values range from 10 to 94; default is 70%. **Period** – Specify the length of time, in minutes, that the specified Percentage can be exceeded before notification is triggered. Value values range from 1 to 60. • **Interface Threshold** – This notification is triggered when utilization of a physical interface exceeds the specified Percentage of total bandwidth: **Percentage** – Enter the desired upper limit on interface usage as a percentage of total available bandwidth. Value values range from 30 to 99; default is 70%. • **NAT Packet Discard** – This notification is generated when IP packets are discarded by the NAT function. Available Network Address Translation addresses or ports have fallen below configured threshold.

Add SNMP Host Access Entry Dialog Box

Use the Add SNMP Host Access Entry dialog box to add and edit entries in the SNMP Hosts table on the SNMP page. These entries represent SNMP management stations allowed to access the security device.

Navigation Path

You can access the Add SNMP Host Access Entry dialog box from the SNMP Page, page 1-8.

Related Topics

- Configuring SNMP, page 1-7
- SNMP Trap Configuration Dialog Box, page 1-9

Field Reference

Table 1-9 Add SNMP Host Access Entry Dialog Box

Element	Description
Interface Name	Enter or Select the interface on which this SNMP management station contacts the device.
IP Address	Enter the IP address, or Select a Networks/Hosts object, representing the SNMP management station.
UDP Port	(Optional) Enter a UDP port for requests from the SNMP host. You can use this field to override the global value specified on the SNMP page.
Community String Confirm	Enter the password used by the SNMP management station when sending requests to the security device. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. Thus, the password is used to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces are not permitted. Repeat the password in the **Confirm** field.
SNMP Version	Choose the version of SNMP used by this management station: **1** or **2c**.
Server Poll/Trap Specification	Specify the type(s) of communication with this management station: poll only, trap only, or both trap and poll. Check either or both: • Poll – The security device waits for periodic requests from the management station. • Trap – The device sends trap events when they occur.

Telnet Page

Use the Telnet page to configure rules that permit only specific hosts or networks to connect to the firewall device using the Telnet protocol.

The rules restrict administrative Telnet access through a firewall device interface to a specific IP address and netmask. Connection attempts that comply with the rules must then be authenticated by a preconfigured AAA server or the Telnet password. You can monitor Telnet sessions using Monitoring > Telnet Sessions.

Note Only five Telnet sessions can be active at the same time in single-context mode. In multiple-context mode on ASAs, there can be only five Telnet sessions active per context, 100 Telnet sessions active per blade. With resource class, the administrator can further tune this parameter.

Related Topics

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Telnet** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Telnet** from the Policy Type selector. Right-click **Telnet** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Telnet Configuration Dialog Box, page 1-14

Field Reference

Table 1-10 Telnet Page

Element	Description
Timeout	Number of minutes a Telnet session can remain idle before the firewall device closes it. Values can range from 1 to 1440 minutes.
Telnet Access Table	
Interface	Interface that receives Telnet packets from the client.
IP Addresses	The IP address and network mask of each host or network that can access the Telnet console through the specified interface.

Telnet Configuration Dialog Box

Use the Telnet Configuration dialog box to configure Telnet options for an interface.

Navigation Path

You can access the Telnet Configuration dialog box from the Telnet Page, page 1-13.

Field Reference

Table 1-11 Telnet Configuration Dialog Box

Element	Description
Interface Name	Enter or Select an interface that can receive Telnet packets from a client.
IP Addresses/Netmask	Enter or Select the IP address and netmask, separated by a "/", of each host or network permitted to access the firewall device's Telnet console through the specified interface. Use commas to separate multiple entries. **Note** To limit access to a single IP address, use 255.255.255.255 or 32 as the netmask. Do not use the subnetwork mask of the internal network.