CHAPTER 35

Managing Firewall Devices

The following topics describe configuration and management of security services and policies on Cisco security devices: Adaptive Security Appliances (ASAs), PIX Firewalls, and Firewall Services Modules (FWSMs) on Catalyst 6500 series switches:

This chapter contains the following topics:

Default Firewall Configurations

Firewall devices are shipped with certain settings already configured. When you manually add a newly installed firewall device to Cisco Security Manager, you should discover (import) the pre-set or default policies for that device. Importing these policies into Security Manager prevents them being unintentionally removed the first time you deploy a configuration to that device. For more information about importing policies, see Discovering Policies, page 5-12.

Cisco Security Manager provides a set of configuration files that contain default policies for a number of device types and versions. These configuration files are located in the directory: *<install_dir>*\CSCOpx\MDC\fwtools\pixplatform\ (for example, `C:\Program Files\CSCOpx\MDC\fwtools\pixplatform\`).

The file name indicates device type, operating system version, context support, and operation type. For example, “FactoryDefault_FWSM2_2_MR.cfg” is the configuration file for an FWSM, version 2.2, with support for Multiple contexts, operating in Routed mode. Similarly, “FactoryDefault_ASA7_0_1_ST.cfg” is the configuration file for an ASA, version 7.0.1, in Single-context, Transparent mode.

Refer to Interfaces in Single and Multiple Contexts, page 35-4 for more about security contexts, and Interfaces in Routed and Transparent Modes, page 35-4 for more about routed and transparent operation.

See Adding Devices from Configuration Files, page 3-17 for information about adding new devices from the supplied configuration files.

Configuring Firewall Device Interfaces

The Interfaces page displays configured interfaces, subinterfaces and redundant interfaces for the selected device. From this page, you can add, edit and delete interfaces, subinterfaces and redundant interfaces; enable communication between interfaces on the same security level; and manage VPDN groups and PPPoE users, as described in the following sections.

Understanding Device Interfaces

An interface is a point of connection between a security device and some other network device. Interfaces are initially disabled; thus, as an essential part of firewall configuration, interfaces must be enabled and configured to allow appropriate packet inspection and forwarding.

There are two types of interface: physical and logical, where a physical interface is the actual slot on the device into which a network cable is plugged, and a logical interface is a virtual port assigned to a specific physical port. Generally, physical ports are referred to as “interfaces,” while logical ports are referred to as “subinterfaces.” The number and type of interfaces you can define varies with appliance model and type of license purchased.

Note On devices running version 6.3 of the PIX operating system, the labels “physical” and “logical” are used, rather than “interface” and “subinterface.” Also, transparent mode and multiple contexts are not supported on these devices.

Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. Because VLANs keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. This feature is particularly useful in multiple-context mode, allowing you to assign unique interfaces to each context.

As a general rule, interfaces attach to router-based networks, and subinterfaces attach to switch-based networks. All subinterfaces must be associated with a physical interface that is responsible for routing allowed traffic correctly.

Note If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. The physical interface must be enabled for the subinterface to pass traffic, but do not name the physical interface to ensure it does not pass traffic. However, if you do want to let the physical interface pass untagged packets, you can name the interface as usual. (See Using the Add/Edit Interface Dialog Box, page 35-6 for information about naming an interface.)

The FWSM does not include any external physical interfaces—instead, it uses internal VLAN interfaces. For example, assume you assign VLAN 201 to the FWSM inside interface, and VLAN 200 to the outside interface. You assign these VLANs to physical switch ports, and hosts connect to those ports. When communication occurs between VLANs 201 and 200, the FWSM is the only available path between the VLANs, forcing traffic to be statefully inspected.

See the following sections for additional information about device interfaces:

- About Redundant Interfaces, page 35-3
- Interfaces in Routed and Transparent Modes, page 35-4
- Interfaces in Single and Multiple Contexts, page 35-4

Note The ASA 5505, combining switch and security appliance features, is a special case in that you configure both physical switch ports and logical VLAN interfaces. See Understanding ASA 5505 Ports and Interfaces, page 35-5 for more information.

Firewall devices come in a variety of configurations, and the configuration determines how to define the interfaces associated with a specific device. The following table outlines the various configurations.

Table 35-1 Security Appliance Configurations

Device Type	Operational Mode (Router or Transparent)	Context Support (Single or Multiple)
PIX 6.3.x	N/A	N/A
PIX 7.0/ASA	Router or Transparent	Single
PIX 7.0/ASA, or security context of unmanaged PIX 7.0/ASA	Router or Transparent	Multiple (see Checklist for Configuring Multiple Security Contexts, page 47-2)
FWSM, or security context of unmanaged switch (multiple mode)	Router or Transparent	Single or Multiple

About Redundant Interfaces

Beginning with Security Manager 3.2.2, you can define logical “redundant” interfaces to increase security appliance reliability. A redundant interface is a specific pair of physical interfaces, with one designated as active (or primary) and the other as standby (or secondary). When the active interface fails, the standby interface becomes active and starts passing traffic. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover, if desired. You can configure up to eight redundant interface pairs.

A redundant interface functions as a single interface (inside, outside, etc.), with only one of the member pair active at any one time. This redundant interface is configured normally, with a unique interface name, security level and IP address. Note that each member interface must be of the same type (e.g., GigabitEthernet), and cannot have a name, security level, or IP address assigned. In fact, do not configure any options other than Duplex and Speed on the member interfaces.

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can explicitly assign a MAC address to the redundant interface; this address is then used regardless of the member interface MAC addresses. In either case, when the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Interfaces in Routed and Transparent Modes

Beginning with ASA/PIX 7.0 and FWSM 2.2.1, you can configure a security device to operate in one of two modes: *routed* or *transparent*. (The PIX 6.3 operates only in routed mode.)

In routed mode, the security appliance acts as a gateway or router for connected networks: it maintains IP addresses for its interfaces, and inspects and filters traffic traversing these interfaces based on IP address (Layer 3) information. In this mode, each device interface is connected to a different IP subnet, and has its own IP address on that subnet. Routed mode supports up to 256 interfaces in single mode or per context, with a maximum of 1000 interfaces divided between all contexts.

In transparent mode, the security appliance operates as a Layer 2 (data link) device, or transparent bridge, and is often referred to as a “bump in the wire,” or a “stealth firewall.” In this mode, you can define only two interfaces: inside and outside. The interfaces do not require IP addresses; they use VLAN IDs to forward inspected traffic. However, if the device includes a dedicated management interface, you can use it—either the physical interface or a subinterface—as a third interface for device-management traffic.

Note Cisco Security Manager does not populate the interface information for FWSM 2.x devices during discovery.

Related Topics

- Configuring Bridging Policies on Firewall Devices, page 35-17
- Bridging, page 48-31

Interfaces in Single and Multiple Contexts

Security “contexts” allow a single physical device to operate as multiple, independent firewalls. In multiple-context mode, each context defines a single virtual firewall, complete with its own configuration. Each context acts as a unique virtual firewall that inspects and filters traffic traversing the interfaces allocated to that context. Each context is “unaware” of other contexts defined on the same security appliance.

As with a single-context, routed-mode device, interfaces on a multiple-context device connect to router-based networks, subinterfaces connect to switch-based networks, and each subinterface must be associated with an interface that routes allowed traffic correctly.

However, you cannot define IP addresses, the routed-mode portion of the configuration, or identify the management interface until you have defined and deployed the contexts. But you cannot define a security context until you have defined the necessary interfaces and subinterfaces.

In other words, you must enable and configure the interfaces and subinterfaces on a device that will provide multiple security contexts (in either routed or transparent mode) before you can define and configure the security contexts themselves.

Refer to Chapter 47, "Configuring Security Contexts on Firewall Devices" for more information.

Understanding ASA 5505 Ports and Interfaces

The ASA 5505 is unique in that it includes a built-in switch, and there are two kinds of ports and interfaces that you need to configure:

- Physical switch ports—The ASA 5505 has eight Fast Ethernet switch ports that forward traffic at Layer 2, using the switching function in hardware. Two of these ports are power-over-Ethernet (PoE) ports. You can connect these ports directly to user equipment such as PCs, IP phones, or DSL modems. Or you can connect to another switch.
- Logical VLAN interfaces—In routed mode, these interfaces forward traffic between VLAN networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces forward traffic between the VLANs on the same network at Layer 2, using the configured security policy to apply firewall services.

To segregate the switch ports into separate VLANs, you assign each switch port to a VLAN interface. Switch ports on the same VLAN can communicate with each other using hardware switching. But when a switch port on one VLAN attempts to communicate with a switch port on another VLAN, the ASA 5505 applies the security policy to the traffic, and routes or bridges between the two VLANs.

Note Subinterfaces are not available on the ASA 5505.

For more information, see ASA 5505 Ports and Interfaces Page, page 48-26.

Managing Device Interfaces

The Interfaces page displays configured interfaces, subinterfaces and redundant interfaces for the selected device. Each security device must be configured, and each active interface must be enabled. Inactive interfaces can be disabled. When disabled, the interface does not transmit or receive data, but its configuration information is retained.

If you bootstrapped a new firewall device, the set-up feature configures only the addresses and names associated with the inside interface. You must define the remaining interfaces on that device before you can specify access and translation rules for traffic traversing that security device.

Follow these steps to manage security-device interfaces. You can add, edit and delete configured interfaces, subinterfaces and redundant interfaces, and also enable communication between interfaces with the same security level.

Step 1 Ensure Device View is your present application view; if necessary, click the **Device View** button on the toolbar.

Note For more information on using the Device View to configure device policies, see Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-27).

Step 2 Select the appliance you want to configure.

Step 3 Select **Interfaces** in the Device Policy selector.

The Interfaces page is displayed. For a description of the fields on this page, see Interfaces Page: PIX and ASA, page 48-2.

Step 4 Add, edit and delete interfaces, as necessary:

- To define a new interface, click the **Add Row** button at the bottom of the Interfaces page to open the Add/Edit Interface dialog box (see Using the Add/Edit Interface Dialog Box, page 35-6).
- To edit an existing interface, select the desired entry in the Interfaces list and then click the **Edit Row** button at the bottom of the Interfaces page to open the Add/Edit Interface dialog box (see Using the Add/Edit Interface Dialog Box, page 35-6).
- To delete an existing interface, select the desired entry in the list and then click the **Delete Row** button. A confirmation dialog box may appear; click OK to delete the interface.

Step 5 Click **Save** at the bottom of the window to save your interface definitions to the Cisco Security Manager server.

Using the Add/Edit Interface Dialog Box

This section describes using the Add/Edit Interface dialog box to configure security-device interfaces. Some of the parameters presented in this dialog box vary according to device type and version, operational mode (routed versus transparent), and whether the device hosts a single or multiple contexts. Thus, some of the following descriptions might not exactly mirror the device you are configuring. However, the basic configuration steps are the same, and links to additional information for specific devices are provided. In addition, you can refer to the reference page, Add/Edit Interface Dialog Box, page 48-4, for descriptions of all parameters found in the various versions of the Add/Edit Interface dialog box.

The ASA 5505, combining switch and security appliance features, is a special case in that you configure both physical switch ports and logical VLAN interfaces. See Understanding ASA 5505 Ports and Interfaces, page 35-5 for more information.

Note If you intend to use a physical interface for failover, you can define that interface in this dialog box but do not configure it; instead, use the Failover page (see Chapter 37, “Configuring Failover”). In particular, do not specify an interface Name, as this parameter disqualifies the interface from being used as the failover link.

To define and configure an interface, subinterface, or redundant interface, follow these steps:

Step 1 Open the Add/Edit Interface dialog box, as described in Managing Device Interfaces, page 35-5.

Step 2 Select **Enable Interface** to enable the interface. Deselect this option to disable the interface but preserve its definition.

Traffic cannot traverse an interface, a related subinterface, or a redundant interface if the interface is not enabled. If you are defining a subinterface, enable the interface it will be associated with before defining the subinterface. If you are defining a redundant interface, enable the member interfaces before defining the redundant interface.

Step 3 Select **Management Only** to reserve this interface for device administration. Only traffic for management of this device is accepted; pass-through traffic for other interfaces and devices is rejected.

Step 4 Select **Redundant Interface** to configure two physical interfaces as a single logical "redundant" interface. (See About Redundant Interfaces, page 35-3 for more information.)

When Redundant Interface is checked, the Type option is disabled, the Hardware Port, Duplex and Speed options disappear, and the **Redundant ID**, **Primary Interface** and **Secondary Interface** options appear.

Provide an identifier for this redundant interface; valid IDs are the integers from 1 to 8. Choose the Primary Interface from the list of available interfaces. Similarly, choose the Secondary Interface from the related list.

Step 5 Choose the type of interface you are defining from the Type list:

Interface represents a physical interface, whereas **Subinterface** represents a logical interface (or VLAN connection) associated with a previously defined physical interface.

Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. Because VLANs keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. This feature is particularly useful in multiple-context mode, letting you assign unique interfaces to each context.

Note If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterface to pass traffic, do not name the physical interface to ensure it does not pass traffic. However, if you want to let the physical interface pass untagged packets, you can name the interface as usual.

Step 6 (Optional) Provide an identifier of up to 48 characters for this interface in the **Name** field.

Certain names are reserved for specific interfaces, in accordance with the interface naming conventions of the security appliance. As such, these reserved names enforce default, reserved security levels. Specifically, *inside* and *outside* are used to represent the internal, highest-security connection, and the external, lowest-security network connection respectively.

Also, a subinterface name typically identifies its associated interface, in addition to its own unique identifier. For example, *DMZoobmgmt* could represent an out-of-band management network attached to the DMZ interface.

Again, **do not name the interface if you intend to use it for failover or as a member of a redundant interface**. See Chapter 37, "Configuring Failover" and About Redundant Interfaces, page 35-3 for more information.

Step 7 Specify the **Hardware Port** used by this interface.

If you are defining an interface, enter a physical port ID, which includes network type, slot and port number, in the form: *type[slot/]port*. If you are defining a subinterface, you can simply choose the desired Hardware Port from a list of previously defined ports (you must also supply a VLAN ID).

The network type specified for the physical interface can be either Ethernet or GigabitEthernet; on the ASA 5580, TenGigabitEthernet is also available. Note that this field provides automatic pattern matching: if you begin typing with the letter e, "Ethernet" is inserted into the field. Similarly, typing the letter g produces "GigabitEthernet."

For a **PIX 500 series** security appliance, enter the type and port number; for example, *ethernet0*. For details about the interface numbering for a specific PIX Firewall model, refer to the *Cisco PIX Firewall Hardware Installation Guide, Version 6.3*.

For an **ASA 5500 series** appliance, enter the type and a slot/port pair; for example, *gigabitethernet0/1*. Ports that are built into the chassis are assigned to slot 0, while ports on the 4GE SSM are assigned to slot 1.

The ASA 5500 series appliances also include a **management** interface type. The management interface is a Fast Ethernet interface designed for device-management traffic only, and is specified as *management0/0*. You can, however, use this physical interface for through traffic if desired (be sure the Management Only option is not selected). Thus, in transparent firewall mode, you can use the management interface in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context in multiple-context mode.

Step 8 (Subinterfaces only) Provide an identifier for this subinterface: enter an integer between 1 and 4294967295 in the **Subinterface ID** field.

For subinterface port identification, this ID is appended to the chosen Hardware Port. For example, *GigabitEthernet0.4* represents the subinterface assigned an ID of 4, operating on the port GigabitEthernet0.

Step 9 (ASA slot/port interfaces only) Select the **Media Type**: RJ45 (copper) or SFP (fiber); SFP is required for 10-Gigabit Ethernet cards.

Step 10 (Interfaces only) Choose the appropriate options for **Duplex** and **Speed**. Note that the Speed and Duplex options are intended primarily for copper-based interfaces.

Duplex	Speed
auto – Automatically detects the duplex setting; required for copper-based Gigabit Ethernet.	**auto** – Automatically detects the speed setting.
full – Communication can be in both directions simultaneously.	**10** – Sets the speed to 10 Mbps.
half – Communication can be in one direction at a time.	**100** – Sets the speed to 100 Mbps.
N/A – The duplex setting is not applicable to fiber-based interfaces.	**1000** – Sets the speed to 1000 Mbps; for use with copper-based Gigabit Ethernet only.
	10000 – Set automatically for TenGigabitEthernet (10000BASE-SX) interfaces; available on ASA 5580 only.
	nonegotiate – Sets the speed to 1000 Mbps and does not negotiate link parameters; for fiber-based interfaces only.

On a PIX 6.3 device, Speed and Duplex settings are combined; the options are **auto**, **10baset**, **10full**, **100basetx**, **100full**, **aui**, and **bnc**.

Note We strongly recommend you use the **auto** setting for both parameters, letting the security appliance automatically select the correct speed and duplex settings. If you specify a fixed setting for either and then change it later, the interface will shut down.

Also, to avoid duplex mismatch, be sure the remote interface linked to this interface is configured with the same settings.

Step 11 Specify the maximum packet size in bytes in the **MTU** (Maximum Transmission Unit) field.

Valid values are 300 to 65535. The default is 1500 for all IP types except PPPoE, for which the default is 1492. See Device Interface: IP Type (PIX/ASA), page 35-9 and Device Interface: IP Type (PIX 6.3), page 35-11 for information about IP types.

Step 12 (Subinterfaces only) Specify a VLAN ID for this subinterface: enter a value between 1 and 4094 (4096 for FWSM) in the **VLAN ID** field. The specified VLAN ID must not be in use on any connected device.

Step 13 (PIX only) Specify the interface security level: enter a number between 0 (least secure) and 100 (most secure) in the **Security Level** field.

- The *outside* interface is always 0.
- The *inside* interface is always 100.
- DMZ interfaces are between 1 and 99.

Step 14 (Optional) You can enter a **Description** for this interface of up to 240 characters (on one line; i.e., no carriage returns).

Step 15 Other Add/Edit Interface dialog box sections are:

- Device Interface: IP Type (PIX/ASA), page 35-9 or Device Interface: IP Type (PIX 6.3), page 35-11
- Device Interface: MAC Address, page 35-12
- Device Interface: Media Type, page 35-13
- Bridge Groups – A bridge group is a pair of VLAN interfaces, along with a management IP address, connecting the same network on an FWSM (3.1 or later) operating in transparent mode. The Add/Edit Interface dialog box opened for such an FWSM contains a read-only **Bridge Group** field that lists the group to which the interface is assigned. See Add/Edit Bridge Group Dialog Box, page 48-25 for information about defining Bridge groups.
- Roles – All interface roles assigned to this interface are listed in this field. Role assignments are based on pattern matching between the Name given to this interface and all currently defined Interface Role objects in Cisco Security Manager. Refer to Understanding Interface Role Objects, page 6-55 for more information.

Step 16 Click OK to close the Add/Edit Interface dialog box and enable the interface.

Device Interface: IP Type (PIX/ASA)

A security device operating in single-context, routed mode requires IP addressing for its interfaces; firewall interfaces do not have IP addresses until you assign them. (In multiple-context mode, interface IP addresses are set in the context configuration.) Note that in transparent mode, the device acts as an access-control bridge (a “bump in the wire”)—you assign different VLANs to each interface, but IP addressing is not necessary.

The Add/Edit Interface dialog box presented for a security device in single-context, routed mode includes the section IP Type, where you specify the type of IP addressing for the interface and provide related parameters, as described here. See Using the Add/Edit Interface Dialog Box, page 35-6 for information about the other sections of the dialog box.

Caution Do not specify IP Type information for an interface you intend to use in a redundant interface.

Note The IP Type section of the Add/Edit Interface dialog box for PIX 6.3 devices is described in Device Interface: IP Type (PIX 6.3), page 35-11.

Step 1 In the Add/Edit Interface dialog box, choose a method for address assignment from the **IP Type** list, and then provide related parameters:

- **Static IP** – Provide a static **IP Address** and **Subnet Mask** that represents the security device on this interface's connected network. If you omit the Subnet Mask value, a "classful" network is assumed, as follows:
  - The Class A netmask (255.0.0.0) is assumed if the first octet of the IP Address is 1 through 126 (i.e., addresses 1.0.0.0 through 126.255.255.255).
  - The Class B netmask (255.255.0.0) is assumed if the first octet of the IP Address is 128 through 191 (i.e., addresses 128.0.0.0 through 191.255.255.255).
  - The Class C netmask (255.255.255.0) is assumed if the first octet of the IP Address is 192 through 223 (i.e., addresses 192.0.0.0 through 223.255.255.255).
- **Use DHCP** – Enables Dynamic Host Configuration Protocol (DHCP) for automatic assignment of an IP address from a DHCP server on the connected network. The following options become available:
  - **DHCP Learned Route Metric** (required) – Assign an administrative distance to the learned route. Valid values are 1 to 255. If this field is blank, the administrative distance for learned routes defaults to 1.
  - **Obtain Default Route using DHCP** – Check this box to obtain a default route from the DHCP server so that you do not need to configure a default static route.
  - **Enable Tracking for DHCP Learned Route** – If Obtain Default Route using DHCP is checked, you can check this box to enable route tracking via a specific Service Level Agreement (SLA) monitor. The following options become available:
  - **Tracked SLA Monitor** – Required if Enable Tracking for DHCP Learned Route is selected. Provide the name of the SLA Monitor object to be used for route tracking. You can use the Select button to select from a list of available SLA monitors. (Refer to Chapter 44, "Monitoring Service Level Agreements (SLAs) To Maintain Connectivity" for more information.)
- **PPPoE (PIX and ASA 7.2+)** – Enables PPPoE for automatic assignment of an IP address of an IP address from a PPPoE server on the connected network; not supported with failover.
  - **VPDN Group Name** (required) – Virtual Private Dialup Network (VPDN) group that contains the authentication method and user name/password to use for network connection, negotiation and authentication. See Managing VPDN Groups, page 35-16 for more information.
  - **IP Address** – If provided, this static IP address is used for connection and authentication, instead of a negotiated address.
  - **Subnet Mask** – The subnet mask to be used in conjunction with the provided IP Address.
  - **PPPoE Learned Route Metric** (required) – Assign an administrative distance to the learned route. Valid values are 1 to 255. If this field is blank, the administrative distance for learned routes defaults to 1.
  - **Obtain Default Route using PPPoE** – Check this box to obtain a default route from the PPPoE server; sets the default routes when the PPPoE client has not yet established a connection. When using this option, you cannot have a statically defined route in the configuration.

- **Enable Tracking for PPPoE Learned Route** – If Obtain Default Route using PPPoE is selected, you can select this option to enable route tracking for PPPoE-learned routes. The following options become available:
- **Dual ISP Interface** – If you are defining interfaces for dual ISP support, choose Primary or Secondary to indicate which connection you are configuring.
- **Tracked SLA Monitor** – Required if Enable Tracking for DHCP Learned Route is selected. Provide the name of the SLA Monitor object to be used for route tracking. You can use the Select button to select from a list of available SLA monitors. (Refer to Chapter 44, "Monitoring Service Level Agreements (SLAs) To Maintain Connectivity" for more information.)

Note You can configure DHCP and PPPoE only on the outside interface of a firewall device. If you have already configured PPPoE on the outside interface, it is no longer available as an option.

Device Interface: IP Type (PIX 6.3)

A PIX version 6.3 security device requires IP addressing for its interfaces; firewall interfaces do not have IP addresses until you assign them.

Note The IP Type options presented for other security appliances are described in Device Interface: IP Type (PIX/ASA), page 35-9.

The Add/Edit Interface dialog box presented for a PIX 6.3 security device includes the section IP Type, where you specify the type of IP addressing for the interface and provide related parameters, as described here. See Using the Add/Edit Interface Dialog Box, page 35-6 for information about the other sections of the dialog box.

Step 1 In the Add/Edit Interface dialog box, choose a method for address assignment from the **IP Type** list, and then provide related parameters:

- **Static IP** – Provide a static **IP Address** and **Subnet Mask** that represents the security device on this interface's connected network. If you omit the Subnet Mask value, a "classful" network is assumed, as follows:
  - The Class A netmask (255.0.0.0) is assumed if the first octet of the IP Address is 1 through 126 (i.e., addresses 1.0.0.0 through 126.255.255.255).
  - The Class B netmask (255.255.0.0) is assumed if the first octet of the IP Address is 128 through 191 (i.e., addresses 128.0.0.0 through 191.255.255.255).
  - The Class C netmask (255.255.255.0) is assumed if the first octet of the IP Address is 192 through 223 (i.e., addresses 192.0.0.0 through 223.255.255.255).
- **Use DHCP** – Enables Dynamic Host Configuration Protocol (DHCP) for automatic assignment of an IP address from a DHCP server on the connected network. The following options become available:
  - **Obtain Default Route using DHCP** – Check this box to obtain a default route from the DHCP server so that you do not need to configure a default static route.
  - **Retry Count** – The number of times the PIX will resend the DHCP request. Valid values are 4 to 16; the default is four.

- **PPPoE (PIX and ASA 7.2+)** – Enables PPPoE for automatic assignment of an IP address of an IP address from a PPPoE server on the connected network; not supported with failover.
  - **IP Address** – If provided, this static IP address is used for connection and authentication, instead of a negotiated address.
  - **Subnet Mask** – The subnet mask to be used in conjunction with the provided IP Address.
  - **Obtain Default Route using PPPoE** – Check this box to obtain a default route from the PPPoE server; sets the default routes when the PPPoE client has not yet established a connection. When using this option, you cannot have a statically defined route in the configuration.
  - **Retry Count** – The number of times the PIX will resend the PPPoE request. Valid values are 4 to 16; the default is four.

Note You can configure DHCP and PPPoE only on the outside interface of a firewall device. If you have already configured PPPoE on the outside interface, it is no longer available as an option.

Device Interface: MAC Address

By default, a physical interface uses its burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address. A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then its MAC address changes to match the MAC address of the interface that is now listed first. If you manually assign a MAC address to the redundant interface, that is used regardless of the physical-interface MAC addresses.

You also might want to assign unique MAC addresses to subinterfaces. For example, your service provider might control access based on MAC addresses.

Further, if you use failover, you can provide a standby MAC address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

(Optional) To manually assign a private MAC address to the current interface:

Step 1 In the Add/Edit Interface dialog box, provide the desired MAC address in the **Active MAC Address** field.

MAC addresses are provided in *H.H.H* format, where *H* is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

Step 2 Press the Tab key on your keyboard, or click elsewhere in the dialog box (e.g., in the Description field), to trigger a dialog-box update, which includes activating the **Standby MAC Address** field.

Step 3 If desired, provide a **Standby MAC Address** for use with device-level failover.

If the active unit fails over and the standby unit becomes active, the new active unit begins using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 4 Continue configuring the device interface in the Using the Add/Edit Interface Dialog Box, page 35-6.

Device Interface: Media Type

For ASA 5500 series appliances, ports that are built into the chassis are assigned to slot 0, while ports on the 4GE SSM are assigned to slot 1. By default, all connectors used on an ASA are RJ-45 connectors. However, the ports on the 4GE SSM can include fiber SFP connectors.

As part of the interface configuration for one of these fiber-based connections, you must change the Media Type setting from the default (RJ45) to the fiber-connector setting (SFP). Therefore, in the Add/Edit Interface dialog box, when you enter a hardware port ID with slot/port numbers in the Hardware Port field, the Media Type options are enabled.

Note The fiber interface does not support duplexing and has a fixed speed, so the Duplex option is disabled, and the Speed options are limited to auto and nonegotiate. See Using the Add/Edit Interface Dialog Box, page 35-6 for more information about the Speed and Duplex options.

Follow these steps to change the Media Type for an ASA interface to fiber:

Step 1 In the Add/Edit Interface dialog box, provide a physical port ID with a slot number of 1 in the **Hardware Port** field; for example, *gigabitethernet1/2*.

Step 2 Press the Tab key on your keyboard, or click elsewhere in the dialog box (e.g., in the Description field), to trigger a dialog-box update, which includes enabling the **Media Type** options.

If this is the first time you have followed this procedure, you may receive a message warning you to ensure a fiber connection is being used. Click OK to close the message box.

Step 3 Click the **SFP** button to change the connection type for this interface to fiber.

Step 4 Continue configuring the device interface in the Using the Add/Edit Interface Dialog Box, page 35-6.

Advanced Device Interface Configuration

Advanced configuration options are available for interfaces on devices operating in single-context mode. Note that these are general device-related settings; that is, they are not applied to individual interfaces. These options include:

- Enabling traffic between interfaces with the same security level
- Defining and editing PPPoE users (does not apply to FWSMs)
- Creating and editing VPDN groups (does not apply to FWSMs)

Note The information in this section does not apply to PIX 6.3 devices, nor to security devices in multiple-context mode.

Follow these steps to configure advanced interface settings:

Step 1 Ensure Device View is your present application view; if necessary, click the **Device View** button on the toolbar.

Note For more information on using the Device View to configure device policies, see Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-27.

Step 2 Select the appliance you want to configure.

Step 3 Select **Interfaces** in the Device Policy selector.

The Interfaces page is displayed. For a description of the fields on this page, see Managing Device Interfaces, page 35-5.

Step 4 Click the **Advanced** button at the bottom of the Interfaces page to open the Advanced Interface Settings dialog box.

Step 5 (optional) Choose the desired setting for **Traffic between interfaces with the same security levels**, as described in Enabling Traffic between Interfaces with the Same Security Level, page 35-14.

Step 6 (optional; PIX/ASA only) To create and manage a list of PPPoE users, click the **PPPoE Users** button to open the PPPoE Users dialog box.

You can add, edit and delete PPPoE users in this dialog box, as described in Managing the PPPoE Users List, page 35-15.

Step 7 (optional; PIX/ASA only) Follow these steps to manage VPDN groups:

- To add a VPDN group, click the Add Row button in the Advanced Interface Settings dialog box; the Add VPDN Group dialog box appears.
- To edit a VPDN group, select the desired group from the list in the dialog box and then click the Edit Row button; the Edit VPDN Group dialog box appears.
- To delete a VPDN group, select the desired group from the list in the dialog box and then click the Delete Row button. A confirmation dialog box may appear; click OK to delete the group.

The Add VPDN Group dialog box and the Edit VPDN Group dialog box are virtually identical; they are described in Managing VPDN Groups, page 35-16.

Step 8 Click **OK** to close the Advanced Interface Settings dialog box.

Enabling Traffic between Interfaces with the Same Security Level

The Advanced Interface Settings dialog box presented for a single-context security device includes the “Traffic between interfaces with the same security level” drop-down list, as described in this section. (See Advanced Device Interface Configuration, page 35-13 for information about the Advanced Interface Settings dialog box.)

By default, interfaces or subinterfaces on the same security level cannot communicate with each other. Allowing communication between same-security interfaces provides the following benefits:

- You can configure more than 101 communicating interfaces.

  If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).

- You can allow traffic to flow freely between all same-security interfaces without access lists.

Note If you enable NAT control, you do not need to configure NAT between same-security-level interfaces.

Step 1 In the Advanced Interface Settings dialog box, choose the option that identifies how you want this device to handle **Traffic between interfaces with the same security levels**:

- **Disabled**—Communication between interfaces on the same security level is not allowed.
- **Inter-interface**—Enables traffic flows between interfaces with the same security level setting. When this option is enabled, you are not required to define translation rules to enable traffic flow between interfaces in the firewall device.
- **Intra-interface**—Enables traffic flows between subinterfaces with the same security level setting. When this option is enabled, you are not required to define translation rules to enable traffic flow between subinterfaces assigned to an interface.
- **Both**—Allows both intra- and inter-interface communications among interfaces and subinterfaces with the same security level.

Step 2 Continue with Advanced Device Interface Configuration, page 35-13, or click OK to close the Advanced Interface Settings dialog box.

Managing the PPPoE Users List

Point-to-Point Protocol over Ethernet (PPPoE) allows standard PPP communication between a security device and an external ISP, via an Ethernet interface on the device. To establish a communication link, the device must provide authentication credentials and obtain network parameters. This is accomplished using a Virtual Private Dialup Network (VPDN) group, which basically consists of an established PPPoE user (i.e., a user name and password) and an authentication protocol. See Managing VPDN Groups, page 35-16 for more information about VPDN groups.

The PPPoE user credentials available for use with VPDN groups are maintained in the PPPoE Users dialog box, which opens when you click the PPPoE Users button in the Advanced Interface Settings dialog box (see Advanced Device Interface Configuration, page 35-13).

The PPPoE Users dialog box presents a table of currently defined PPPoE users, along with standard Add Row, Edit Row, and Delete Row buttons:

- To add a new PPPoE user to the list, click the Add Row button; the Add PPPoE User dialog box appears.
- To edit a PPPoE user, select the desired user in the list and then click the Edit Row button; the Edit PPPoE User dialog box appears.
- To delete a PPPoE user, select the desired user in the list and then click the Delete Row button. A confirmation dialog box may appear; click OK to delete the user.

Except for the title, the Add PPPoE User dialog box and the Edit PPPoE User dialog box are identical; use of both to manage PPPoE user credentials is described in the following steps.

Step 1 Enter or edit the following PPPoE user-credential parameters:

- **Username**—The name assigned to this user account; generally provided by the external ISP.
- **Password**—The password assigned to this user account; generally provided by the external ISP.

- **Confirm**—Re-enter the password.
- **Store Username and Password in Local Flash**—If selected, this PPPoE user information will be stored in the device's local Flash memory, ensuring it cannot be inadvertently overwritten.

Step 2 Click OK to close the Add (Edit) PPPoE User dialog box and return to the PPPoE Users dialog box.

Managing VPDN Groups

A Virtual Private Dialup Network (VPDN) group—basically an established PPPoE user and an authentication protocol—is used by a security device to contact an external ISP and authenticate itself, in order to establish a PPPoE communications link and obtain network parameters. (See Managing the PPPoE Users List, page 35-15 for information about establishing PPPoE users.)

Available VPDN groups are maintained in the Advanced Interface Settings dialog box, which opens when you click the Advanced button at the bottom of the Interfaces page, as described in Advanced Device Interface Configuration, page 35-13.

The dialog box includes a table of currently defined VPDN groups, and standard Add Row, Edit Row, and Delete Row buttons. The Add Row button opens the Add VPDN Group dialog box; the Edit Row button opens the virtually identical Edit VPDN Group dialog box. Use of both is described in the following steps.

Step 1 Enter or edit the following VPDN group parameters:

- **Group Name**—A name to identify this group in Security Manager; up to 63 characters.
- **PPPoE Username**—The name identifying the PPPoE credentials to be used by this group for authentication with an ISP.

  Choose from the list of available PPPoE users. Refer to Managing the PPPoE Users List, page 35-15 for information about creating and editing users.
- **PPP Authentication**—Choose the authentication method expected by the ISP:
  - **PAP**—Password Authentication Protocol, with exchange of credentials in clear text.
  - **CHAP**—Challenge Handshake Authentication Protocol, with encrypted credential exchange.
  - **MSCHAP**—Microsoft's CHAP, version 1 only.

Step 2 Click OK to close the Add (Edit) VPDN Group dialog box and return to the Advanced Interface Settings dialog box.

Troubleshooting Interfaces

Use the following information to help troubleshoot problems encountered while configuring interfaces.

Error: Interface IP addresses defined for this device have overlap.

Conditions: Attempting to save changes made to the Interfaces page, such as manually adding an interface to a firewall device.

Description: Indicates that two or more interfaces defined on this device share an IP address on the same subnet. Each interface in the device must be attached to a different network or subnet.

Resolution: Verify that you have entered the correct IP address and subnet mask values required to identify a unique subnet for each interface.

Configuring Bridging Policies on Firewall Devices

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 device that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. The security appliance connects the same network on its inside and outside ports, acting as an access-control bridge; you assign different VLANs to each interface, and IP addressing is not used.

Thus, you can easily introduce a transparent firewall into an existing network—IP re-addressing is unnecessary—and maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.

Although the transparent-mode device acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the security appliance unless you explicitly permit it with specific access rules. The only traffic allowed through the transparent firewall without an access list is ARP traffic, which you can control using ARP inspection.

When the security appliance runs in transparent mode, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup. Route statements can still be configured, but they apply only to security appliance-originated traffic. For example, if your syslog server is located on a remote network, you must use a static route so the security appliance can reach that subnet.

To configure a transparent firewall, use the following policies. When configuring an ASA/PIX/FWSM device in multiple-context mode, configure these policies on each transparent security context.

- **Firewall > Access Rules**—Access rules control layer 3 and higher traffic using extended access control lists. In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on access rules. Likewise, protocols like HSRP or VRRP can pass through the security appliance. However, the transparent-mode security appliance does not pass CDP packets.

  For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can provide those functions. For example, by using access rules, you can allow DHCP traffic to pass (instead of the unsupported DHCP relay feature), or multicast traffic such as that created by IP/TV.

  For more information, see Understanding Access Rules, page 14-1 and Configuring Access Rules, page 14-6.

- **Firewall > Transparent Rules**—Transparent rules control non-IP layer 2 traffic using Ethertype access control lists. For example, you can configure rules to allow AppleTalk, IPX, BPDUs, and MPLS to pass through the device. For more information, see Configuring Transparent Firewall Rules, page 19-1.

- **Platform > Bridging > ARP Table** and **ARP Inspection**—Use these policies to control the types of ARP traffic allowed through the bridge. If desired, you can configure static ARP entries and drop any traffic not defined by those static rules. Enable ARP inspection so that if a mismatch between the MAC address, the IP address, or the interface occurs, the security appliance drops the packet. This helps prevent ARP spoofing. For more information, see ARP Table Page, page 48-31 and ARP Inspection Page, page 48-33.

Note The ARP table is the only bridging policy available for non-transparent ASA/PIX/FWSM devices.

- **Platform > Bridging > MAC Address Table** and **MAC Learning**—Use these policies to configure static MAC-IP address mappings and to enable or disable MAC learning. MAC learning is enabled by default, which allows the appliance to add MAC-IP address mappings as traffic passes through the interface. If you want to prevent all traffic except from static entries, you can disable MAC learning. For more information, see MAC Address Table Page, page 48-34 and MAC Learning Page, page 48-35.
- **Platform > Bridging > Management IP**—Use this policy to configure a management IP address that Security Manager can use to communicate with the device. If you change this address, you also need to update the device properties for the device or security context. Follow these steps:
  - Change the management IP address, save and submit your changes.
  - Deploy your changes to the device.
  - In Device view, select the device or security context, then select **Tools > Device Properties**. On the General page, enter the new management IP address in the IP Address field. On the Credentials tab, update the username and password fields with account credentials that can log into the management interface. Security Manager will now use this address and user account for subsequent deployments and device communication.

  For more information, see Management IP Page, page 48-37.

Related Topics

- Bridging, page 48-31
- Bridging Support for FWSM 3.1, page 35-18
- Interfaces in Routed and Transparent Modes, page 35-4
- Transparent Rules Page, page 19-3

Bridging Support for FWSM 3.1

Although FWSM 3.1 can support multiple L2 interface pairs, Security Manager lets you specify no more than two L2 interfaces (a single interface pair), and one associated management IP address. That means only one bridge group with two named interfaces associated is provisioned with a management IP address. If the device configuration contains a maximum of one bridge group and two named interfaces, it is valid for discovery. All other scenarios result in an error message and the commands are ignored during discovery. Furthermore, discovery will not show any bridge-group information in Security Manager, although the bridge-group commands will be generated during deployment. Bridge group 1 will be deployed and used in transparent rule policies if no bridge group exists in the device configuration.

Related Topics

- Configuring Bridging Policies on Firewall Devices, page 35-17

Configuring Device Administration Policies on Firewall Devices

The Device Admin section contains pages for configuring device administration policies for firewall devices. For more information, see the following topics:

- Configuring AAA, page 35-19
- Configuring Banners, page 35-23
- Configuring Boot Image and Configuration Settings, page 35-24
- Configuring Clock Settings, page 35-25
- Configuring Contact Credentials, page 35-26

Configuring AAA

Authentication-Authorization-Accounting (AAA) enables the security appliance to determine who a user is (authentication), what the user can do (authorization), and what the user did (accounting). You can use authentication alone, or with authorization and accounting. Authorization always requires a user to be authenticated first. You also can use accounting alone, or with authentication and authorization.

Authentication-Authorization-Accounting provides an extra level of protection and control for user access beyond access lists alone. For example, you can create an ACL that allows all outside users to access Telnet on a server on the DMZ network. If you want to limit user access to the server when you may not always know the IP addresses of these users, you can enable AAA to allow only authenticated and/or authorized users to make it through the security appliance. (The Telnet server enforces authentication, too; the security appliance prevents unauthorized users from attempting to access the server.)

- **Authentication**—Authentication grants access based on user identity. Authentication establishes user identity by requiring valid user credentials, which are typically a user name and password. You can configure the security appliance to authenticate the following items:
  - Administrative connections to the security appliance using Telnet, SSH, HTTPS/ASDM, or serial console.
  - The **enable** command.
- **Authorization**—Authorization controls user capabilities after users are authenticated. Authorization controls the services and commands available to each authenticated user. If you do not enable authorization, authentication alone would provide the same access to services for all authenticated users.

  If you need the control that authorization provides, you can configure a broad authentication rule, and then have a detailed authorization configuration. For example, you might authenticate inside users who attempt to access any server on the outside network, and then use authorization to limit the outside servers that a particular user can access.

  The security appliance caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the security appliance does not resend the request to the authorization server.
- **Accounting**—Accounting tracks traffic that passes through the security appliance, providing a record of user activity. If you enable authentication for that traffic, you can account for traffic per user. If you do not authenticate the traffic, you can account for traffic per IP address. Accounting information includes when sessions start and stop, user name, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

Preparing for AAA

AAA services depend upon the use of the Local database or at least one AAA server. You can also use the Local database as a fallback for most services provided by an AAA server. Before you implement AAA, you should configure the Local database and configure AAA server groups and servers.

Configuration of the Local database and AAA servers depends upon the AAA services you want the security appliance to support. Regardless of whether you use AAA servers, you should configure the Local database with user accounts that support administrative access, to prevent accidental lock-outs and, if so desired, to provide a fallback method when AAA servers are unreachable. For more information, see Chapter 40, "Configuring User Accounts".

The following table provides a summary of AAA service support by each AAA server type and by the Local database. You manage the Local database by configuring user accounts on the **Platform > Device Admin > User Accounts** page (see Chapter 40, "Configuring User Accounts"). You establish AAA server groups and add individual AAA servers to the server groups using the **Platform > Device Admin > AAA** page.

Table 35-2 Summary of AAA Support

	Database Type							
AAA Service	**Local**	**RADIUS**	**TACACS+**	**SDI**	**NT**	**Kerberos**	**LDAP**	**HTTP Form**
Authentication of...								
VPN users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
Firewall sessions	Yes	Yes	Yes	No	No	No	No	No
Administrators	Yes	Yes	Yes	No	No	No	No	No
Authorization of...								
VPN users	Yes	Yes	No	No	No	No	Yes	No
Firewall sessions	No	Yes[2]	Yes	No	No	No	No	No
Administrators	Yes[3]	No	Yes	No	No	No	No	No
Accounting of...								
VPN connections	No	Yes	Yes	No	No	No	No	No
Firewall sessions	No	Yes	Yes	No	No	No	No	No
Administrators	No	Yes	Yes	No	No	No	No	No

[1] HTTP Form protocol supports single sign-on authentication for WebVPN users only.

[2] For firewall sessions, RADIUS authorization is supported with user-specific ACLs only, which are received or specified in a RADIUS authentication response.

[3] Local command authorization is supported by privilege level only.

Local Database

The security appliance maintains a Local database that you can populate with user accounts, which contain, at a minimum, a user name. Typically, you assign a password and a privilege level to each user name, although passwords are optional. You can manage Local user accounts on the **Platform > Device Admin > User Accounts** page (see Chapter 40, "Configuring User Accounts").

If you enable command authorization using the Local database, the security appliance refers to the assigned user privilege level to determine what commands are available. By default, all commands are assigned either privilege level 0 or level 15.

Note If you add users to the Local database with access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. Without command authorization, users can access privileged mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication for console access so the user will not be able to use the login command, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged mode.

You cannot use the local database for network access authorization.

The user accounts in the Local database can provide fallback support for console and enable-password authentication, for command authorization, and for VPN authentication and authorization. This behavior is designed to help you prevent accidental lock-out from the security appliance.

For users who need fallback support, we recommend that their user names and passwords in the Local database match their user names and passwords on the AAA servers. This provides transparent fallback support. Because the user cannot determine whether a AAA server or the local database is providing the service, using user names and passwords on AAA servers that are different than the user names and passwords in the Local database means that the user cannot be certain which user name and password should be given.

For multiple-context mode, you can configure user names in the system execution space to provide individual logins at the CLI using the **login** command; however, you cannot configure any **aaa** commands that use the local database in the system execution space.

Note VPN functions are not supported in multiple mode.

AAA for Device Administration

You can authenticate all administrative connections to the security appliance, including:

- Telnet
- SSH
- Serial console
- ASDM
- VPN management access

You can also authenticate administrators who attempt to enter enable mode. You can authorize administrative commands. You can have accounting data for administrative sessions and for commands issued during a session sent to an accounting server.

You can configure AAA for device administration using the **Platform > Device Admin > AAA** page (see Defining AAA Policies, page 35-22).

AAA for Network Access

You can configure rules for authenticating, authorizing, and accounting for traffic passing through the firewall by using the **Firewall > AAA Rules** page (see Chapter 13, "Managing Firewall AAA Rules"). The rules you create are similar to access rules, except that they specify whether to authenticate, authorize, or perform accounting for the traffic defined; and which AAA server group the security appliance is to use to process the AAA service request.

AAA for VPN Access

AAA services for VPN access include the following:

- User account settings for assigning users to VPN groups, configured on the **Platform > Device Admin > User Accounts** page (see Chapter 40, "Configuring User Accounts").
- VPN group policies that can be referenced by many user accounts or tunnel groups, configured on the **Remote Access VPN > RA VPN Policies > User Group Policy** or **Site to Site VPN > User Group Policy** page.
- Tunnel group policies, configured on the **Remote Access VPN > RA VPN Policies > PIX7.0/ASA Tunnel Group Policy** or **Site to Site VPN > PIX7.0/ASA Tunnel Group Policy** page.

Defining AAA Policies

Use the following procedure to define the AAA settings for a device or shared policy.

Related Topics

- AAA Page, page 48-37
- Chapter 40, "Configuring User Accounts"

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > AAA** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > AAA** from the Policy Types selector. Right-click **AAA** and choose **New AAA Policy** to create a policy, or select an existing policy from the Policies selector.

The AAA page is displayed. For a description of the fields on this page, see AAA Page, page 48-37.

Step 2 Click the **Authentication** tab.

Step 3 To require AAA authentication for privileged commands:

a. Check the **Enable** box under Require AAA Authentication to allow use of privileged commands.

b. Enter the name of the AAA server group to use for authentication, or click **Select** to select from a list.

c. To use the local database as a fallback method for privileged command authentication, check the **Use LOCAL when server group fails** box.

Step 4 To require AAA authentication for HTTP, serial-console, SSH, or Telnet access to the security appliance:

a. Check the box next to the type of device access you want to authenticate (HTTP, Serial, SSH, or Telnet).

b. Enter the name of the AAA server group to use for authentication, or click **Select** to select from a list.

c. To use the local database as a fallback method for authentication of this device access, check the **Use LOCAL when server group fails** box.

Step 5 In the Login Prompt field, enter the prompt you want users to see when authentication takes place.

Step 6 Enter the messages you want users to see when accepted or rejected in the corresponding boxes.

Step 7 Click the **Authorization** tab.

Step 8 To require AAA authorization for command access:

a. Check the **Enable Authorization for Command Access** box.

b. Enter the name of the AAA server group to use for authorization, or click **Select** to select from a list.

c. To use the local database as a fallback method for command authorization, check the **Use LOCAL when server group fails** box.

Step 9 Click the **Accounting** tab.

Step 10 To require AAA accounting for privileged commands:

a. Check **Enable** under Require AAA Accounting for privileged commands.

b. Enter the name of the AAA server group to use for accounting, or click **Select** to select from a list.

Step 11 To require AAA accounting for HTTP, serial-console, SSH, or Telnet access to the security appliance:

a. Check the box next to the type of device access for which you want accounting enabled (HTTP, Serial, SSH, or Telnet).

b. Enter the name of the AAA server group to use for accounting, or click **Select** to select from a list.

Step 12 To require AAA accounting for command access:

a. Check **Enable** under Require Accounting for command access.

b. Enter the name of the AAA server group to use for accounting, or click **Select** to select from a list.

c. Select the minimum privilege level that must be associated with a command for an accounting record to be generated.

Configuring Banners

You can use the Banner page to specify the Session (exec), Login and Message-of-the-Day (motd) banners for a firewall device or shared policy.

If you use the tokens `$(hostname)` or `$(domain)`, they are replaced with the host name and domain name of the security appliance. When you enter the `$(system)` token in a context configuration, the context uses the banner configured in the system configuration.

Spaces in the text are preserved; however, tabs cannot be entered. Multiple lines in a banner are handled by entering a line of text for each line you wish to add. Each line is then appended to the end of the existing banner. If the text is empty, then a carriage return (CR) will be added to the banner.

There is no limit on the length of a banner other than RAM and Flash memory limits. You can only use ASCII characters, including new line (the Enter key, which counts as two characters). When accessing the security appliance through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages, or if a TCP write error occurs when attempting to display the banner messages.

Related Topics

- Banner Page, page 48-41

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Banner** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Banner** from the Policy Types selector. Right-click **Banner** and choose **New Banner Policy** to create a policy, or select an existing policy from the Policies selector.

The Banner page is displayed. For a description of the fields on this page, see Table 48-26 on page 48-42.

Step 2 In the Session (exec) Banner box, enter the text that you want the system to display as a banner before displaying the enable prompt.

Step 3 In the Login Banner box, enter the text that you want the system to display as a banner before the password login prompt when accessing the security appliance using Telnet.

Step 4 In the Message-of-the-Day (motd) Banner box, enter the text that you want the system to display as a message-of-the-day banner.

Step 5 To replace a banner, change the contents of the appropriate box.

Step 6 To remove a banner, clear the contents of the appropriate box.

Configuring Boot Image and Configuration Settings

Boot Image/Configuration lets you choose which image file a security appliance running PIX 7.x or later will boot from, as well as which configuration file it will use at start-up.

You can specify up to four local binary image files for use as the start-up image, and one image located on a TFTP server for the device to boot from. If you specify an image located on a TFTP server, it must be first in the list. In the event the device cannot reach the TFTP server to load the image from, it will attempt to load the next image file in the list located in Flash memory.

If you do not specify any boot variable, the first valid image on internal flash will be chosen to boot the system.

Related Topics

- Boot Image/Configuration Page, page 48-42

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Boot Image/Configuration** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Boot Image/Configuration** from the Policy Types selector. Select an existing policy from the Policies selector, or create a new one.

The Boot Image/Configuration page is displayed. For a description of the fields on this page, see Table 48-27 on page 48-43.

Step 2 Enter the URL of the configuration file to use when the system is loaded. For syntax information, see Table 48-27 on page 48-43.

Step 3 Enter the path to the ASA image file on the security appliance, for example, `flash:/asa`. For syntax information, see Table 48-27 on page 48-43.

Step 4 For each system image file that you want to add, edit, or delete, do one of the following:

- To add a system image file to the Boot Images table, click **Add Row** to open the Images dialog box.
- To edit a system image file, select the entry and click **Edit Row** to open the Images dialog box.
- To delete a system image file from the Boot Images table, select the entry and click **Delete Row**.

Step 5 Enter the URL of the system image file to use when the system is loaded, and then click **OK**. For syntax information, see Images Dialog Box, page 48-43.

Step 6 To move a system image file up or down in the table, select the row for that image file and then click the **Up Arrow** or **Down Arrow** buttons as necessary.

Configuring Clock Settings

The Clock page lets you manually set the date and time for the security appliance.

Note In multiple-context mode, set the time in the system configuration only.

To dynamically set the time using an NTP server, see NTP Page, page 39-16; time derived from an NTP server overrides any time set manually on the Clock page.

Related Topics

- Clock Page, page 48-44

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Clock** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Clock** from the Policy Types selector. Right-click **Clock** and choose **New Clock Policy** to create a policy, or select an existing policy from the Policies selector.

The Clock page is displayed. For a description of the fields on this page, see Table 48-29 on page 48-45.

Step 2 Select the time zone for this device in the **Device Time Zone** list box.

Step 3 If daylight savings time does not apply to this device, select **None**.

Step 4 Otherwise, to specify daylight savings time using a start and end date:

a. Select **Set by Date**.

b. Click the Calendar button under Start to pick the date on which daylight savings time begins.

c. Select the hour and minute that daylight savings time begins using the drop-down list boxes.

d. Click the Calendar button under End to pick the date on which daylight savings time ends.

e. Select the hour and minute that daylight savings time ends using the drop-down list boxes.

Step 5 To specify daylight savings time using a specific day of the year (for example, the first Sunday in August):

a. To specify that daylight savings time occurs on the same days every year, select the **Specify Recurring Time** check box.

b. Select the month in which daylight savings time begins in the **Month** drop-down list box under Start.

c. Select the number that corresponds to the week in which daylight savings time begins in the **Week** drop-down list box under Start.

d. Select the day of the week on which daylight savings time begins in the **Weekday** drop-down list box under Start.

e. Select the hour at which daylight savings time begins in the **Hour** drop-down list box under Start.

f. Select the minute at which daylight savings time begins in the **Minute** drop-down list box under Start.

g. Select the month in which daylight savings time ends in the **Month** drop-down list box under End.

h. Select the number that corresponds to the week in which daylight savings time ends in the **Week** drop-down list box under End.

i. Select the day of the week on which daylight savings time ends in the **Weekday** drop-down list box under End.

j. Select the hour at which daylight savings time ends in the **Hour** drop-down list box under End.

k. Select the minute at which daylight savings time ends in the **Minute** drop-down list box under End.

Configuring Contact Credentials

You can use the Contact Credentials page to specify the future contact settings that Cisco Security Manager should use when contacting a device. You can also use the Contact Credentials page to change the login password and the enable password on a device.

The login password lets you access EXEC mode if you connect to the security appliance using a Telnet or SSH session. (If you configure user authentication for Telnet or SSH access, then each user has their own password, and this login password is not used.)

The enable password lets you access privileged EXEC mode after you log in. (If you configure user authentication for enable access, then each user has their own password, and this enable password is not used.)

Related Topics

- Credentials Page, page 48-46

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Contact Credentials** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Contact Credentials** from the Policy Types selector. Right-click **Contact Credentials** and choose **New Contact Credentials Policy** to create a policy, or select an existing policy from the Policies selector.

The Contact Credentials page is displayed. For a description of the fields on this page, see Table 48-30 on page 48-46.

Step 2 To change the contact user name and password:

a. Check the **Change the contact username and password** box.

The Username and Password fields are enabled.

b. Enter a user name for logging in to the device.

c. Enter the password for logging in to the device.

d. Re-enter the password for logging in to the device.

e. Select the privilege level of the user logging in to the device.

Step 3 To change the enable password:

a. Check the **Change the enable password** box.

The Enable Password fields are enabled.

b. Enter the enable password.

c. Re-enter the enable password.

Step 4 To change the Telnet/SSH password:

a. Check the **Change the TELNET/SSH password** box.

The Telnet Password fields are enabled.

b. Enter the enable password.

c. Re-enter the enable password.