Configuring Security Contexts on Firewall Devices

You can define multiple security "contexts" on a single security appliance. Each context operates as an independent virtual device, with its own security policy, interfaces and administrators. Multiple contexts are similar to having multiple stand-alone devices. Many features are supported in multiple-context mode, including routing tables, firewall features, IPS, and management. Some features are not supported; for example, VPN, multicast, and dynamic routing protocols; security contexts support only static routes; and you cannot enable OSPF or RIP in multiple-context mode. Also, some features are not directly managed by Cisco Security Manager, such as the IPS feature set for ASA and PIX devices.

In multiple-context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and most of the options you can configure on a stand-alone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single-mode configuration, is the start-up configuration. The system configuration identifies basic settings for the security appliance, but it does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses the context that is designated as the Admin context. The system configuration is used to add, delete and edit basic context settings, including allocating network interfaces to the various contexts.

The Admin context is just like any other context, except that when a user logs in to the Admin context, that user has system administrator rights and can access the system configuration and all other contexts.

This chapter contains the following topics:

Enabling and Disabling Multiple-Context Mode

Cisco Security Manager does not support switching to multiple-context mode on an existing device. To perform this task, you must delete the device from Security Manager, enable multiple-context mode using a device manager or CLI input, and then add the device again to Security Manager. After the device is added in multiple-context mode, you can add, edit and delete security contexts.

Note When manually defining a multiple-context device, choose **Multi** from the Contexts list in the Operating System section of the New Device - Device Information dialog box.

Similarly, Cisco Security Manager does not support restoring an existing device to single-context mode. To perform this task, you must delete the device and any of its child contexts from Security Manager, restore single-context operation using a device manager or CLI input, and then add the device again to Security Manager.

Note When manually defining a single-context device, choose **Single** from the Contexts list in the Operating System section of the New Device - Device Information dialog box.

Related Topics

- Checklist for Configuring Multiple Security Contexts, page 59-3
- Managing Security Contexts, page 59-7
  - Add/Edit Security Context Dialog Box (PIX/ASA), page 59-9
  - Add/Edit Security Context Dialog Box (FWSM), page 59-8

Checklist for Configuring Multiple Security Contexts

Security contexts allow a single physical device to act as multiple independent firewalls. Each security context defines a single virtual firewall, complete with its own configuration—and just as with physical devices, each security context must be correctly configured, or overall security can be compromised. Thus, defining and configuring multiple firewalls on the same physical appliance requires special care.

The following checklist outlines the basic steps necessary to configure a firewall device with multiple security contexts. Each of these steps may involve multiple substeps; all steps should be performed in the order presented. For example, you must define interfaces before configuring the various contexts.

Step	Task
Step 1	**Define interfaces and subinterfaces, or VLANs, on the physical appliance.** In this task, you define the interfaces and subinterfaces, or VLANs on FWSMs, that will be allocated to the various security contexts when you create them later. Provide physical interface parameters, such as connection type (Ethernet, GigabitEthernet, etc.), hardware Port ID, speed, and duplex mode, as well as VLAN ID if defining a subinterface. **Result**: All interfaces and subinterfaces are defined. For more information, see Configuring Firewall Device Interfaces, page 46-3.

Step	Task
Step 2	**Define an Admin context for administering the base security appliance.** This task is called out separately to ensure you define a context and IP address specifically for administration of the security appliance. The process is the same as defining a security context; however, during the process, be sure to check **Admin Context** to designate this as the administration context. In addition to being used to administer the appliance, the Admin context is used to publish syslog and SNMP messages to monitoring devices, such as the Cisco Security Monitoring, Analysis and Response System (CS-MARS), for further processing. Until you associate a specific management IP address with the Admin context, the IP address used to manage the security appliance is the one you specified when defining the device. When you specify a Management IP Address with the Admin context, it takes precedence over the one on the Device Properties page. **Result**: The Admin context is defined and associated with a physical interface. For more information, see: • Add/Edit Security Context Dialog Box (PIX/ASA), page 59-9 • Add/Edit Security Context Dialog Box (FWSM), page 59-8

Step	Task
Step 3	**Define each security context, or virtual firewall, on the base appliance.** In this task, you define individual security contexts, naming each, assigning a location for its configuration files, and allocating interfaces. Each security context represents a virtual firewall, and its definition includes the interfaces and range of associated VLAN IDs that are under its control. **Note** While the Admin context can operate as a firewall device, it is typically used as such only in single-context mode. Therefore, security contexts are treated as separate entities in this checklist. You cannot add new interfaces or modify the hardware Port value when defining a security context—you simply select previously defined interfaces for allocation to the context. **Result**: Each security context is defined and associated with a physical interface; the VLANs on which the security context will inspect traffic are also specified. For more information, see: • Add/Edit Security Context Dialog Box (PIX/ASA), page 59-9 • Add/Edit Security Context Dialog Box (FWSM), page 59-8
Step 4	**Submit/deploy to generate the virtual firewalls as children of the base appliance.** You must create the desired contexts on the security appliance before you can begin defining the individual settings of each context. To create contexts on the appliance, you must define them, and then either submit changes in Workflow mode, or deploy the changes to the security appliance in non-Workflow mode. When you create a security context, a “virtual firewall device” appears beneath the original security appliance in the Device View. Each virtual device is indicated by a related device icon with a dotted outline, and its name is the base security appliance name, underscore (_), context name. For example, the virtual device *asaMultiRouted_admin* would represent the Admin context (named “admin”) on the security appliance named “asaMultiRouted.” Similarly, *asaMultiRouted_security1* would represent the security context “security1” on the same base appliance. **Result**: Your changes are submitted or deployed (depending on the Workflow mode), which in turn creates the Admin and security contexts as children of the base security appliance. For more information, see: • Workflow and Activities Overview, page 1-20 • Submitting an Activity for Approval (Workflow Mode with Activity Approver), page 4-20 • Working with Deployment and the Configuration Archive, page 8-25
Step 5	**Define additional settings for each security context.** You can now complete the definition of each security context by selecting a virtual firewall device in the Device Selector and editing available policies, such as access rules, translation options and so on. **Result**: Each security context is fully defined, ready to operate as a virtual firewall.

Managing Security Contexts

The Security Contexts page lists security contexts configured for the selected device. You can add, edit and delete security contexts for an ASA, PIX 7.0+, or FWSM device running in multiple-context mode from this page.

Tip Deleting a security context from an FWSM device removes the security context from the running configuration of the device, but it does not delete the associated configuration file. This can cause problems if you later add another security context with the same name as the one previously deleted. This is a known issue for FWSM and is not connected to the behavior of Security Manager. A work-around is to use the CLI to delete the configuration file from the device.

Remember, the security appliance must be in multiple-context mode in order for you to configure contexts using Security Manager. See Enabling and Disabling Multiple-Context Mode, page 59-1 for more information.

Follow these steps to manage security contexts:

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

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 5-30).

Step 2 Select the appliance you want to configure.

Step 3 Select **Security Contexts** in the Device Policy selector to display the Security Contexts page.

Note The child contexts of a multiple-mode device are represented using a different icon than firewall devices in single mode.

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

- To define a new context, click the **Add Row** button at the bottom of the page to open the Add Security Context box.
- To edit an existing context, select the desired entry in the Security Contexts list and then click the **Edit Row** button at the bottom of the page to open the Edit Security Context dialog box.
- To delete an existing context, select the desired entry in the list and then click the **Delete Row** button.

  Note Deleting a security context here will also cause the security context device to be removed from device inventory.

  Confirm the deletion of the security context and corresponding security context device.

Note Except for the titles, the Add Security Context dialog box and the Edit Security Context dialog box are identical. For PIX/ASA devices, see Add/Edit Security Context Dialog Box (PIX/ASA), page 59-9 for more information; for FWSMs, see Add/Edit Security Context Dialog Box (FWSM), page 59-8 for more information.

Add/Edit Security Context Dialog Box (FWSM)

The Add Security Context and Edit Security Context dialog boxes let you define and maintain contexts for the currently selected Firewall Service Module. (Except for their titles, the two dialog boxes are identical.)

Note that at least one security context must be designated as the Admin context.

Caution Security Manager does not support mapped (that is, "named" or "aliased") interfaces for FWSMs. If you discover an FWSM with named interfaces and then change the related configuration, redeployment will fail. Replace any interface aliases with the appropriate VLAN IDs.

Navigation Path

You can access the Add Security Context and Edit Security Context dialog boxes from the Security Contexts page, as described in Managing Security Contexts, page 59-7.

Field Reference

Table 59-1 Add/Edit Security Context Dialog Box (FWSM)

Element	Description
Name	Enter a name of up to 32 characters for the context. The names `System` and `Null` (in any combination of upper- and lower-case letters) are reserved, and cannot be used. **Note** While context names are case-sensitive on the device, they are not in Security Manager. That is, you cannot have two contexts with the same name but different capitalization in Security Manager.
Mode (FWSM 3.1+)	Choose the mode, Router or Transparent, for this security context. **Note** You cannot change the chosen mode in the Edit Security Context dialog box.
Admin Context	Check this box if this context is to be the Admin context for this device. **Note** The name of the Admin context for the device is displayed below the Security Contexts table.
VLAN IDs	Enter the VLANs assigned to this context. Use commas to separate multiple VLAN entries.

Table 59-1 Add/Edit Security Context Dialog Box (FWSM) (continued)

Element	Description
Config URL	Specify the context configuration location, as a URL-type address, by choosing a file-system protocol and then entering the path and name of the file to access for the context configuration. That is, choose a protocol type from the drop-down list, and then type the server name (for remote file systems), path, and file name in the related text field. For example, the combined URL for FTP has the following format: `ftp://server.example.com/configs/admin.cfg`. Available protocols are: • `disk:/` • `ftp://` • `http://` • `https://` • `tftp://`
Failover Group	If this context is part of an active/active failover configuration, choose the failover group to which this context belongs.
Description	Enter an optional description for the context.

Add/Edit Security Context Dialog Box (PIX/ASA)

The Add Security Context and Edit Security Context dialog boxes let you define and maintain contexts for the currently selected PIX/ASA security appliance. (Except for their titles, the two dialog boxes are identical.)

Note that at least one security context must be designated as the Admin context.

Navigation Path

You can access the Add Security Context and Edit Security Context dialog boxes from the Security Contexts page, as described in Managing Security Contexts, page 59-7.

Field Reference

Table 59-2 Add/Edit Security Context Dialog Box (PIX/ASA)

Element	Description
Name	Enter a name of up to 32 characters for the context. The names `System` and `Null` (in any combination of upper- and lower-case letters) are reserved, and cannot be used. **Note** While context names are case-sensitive on the device, they are not in Security Manager. That is, you cannot have two contexts with the same name but different capitalization in Security Manager.
Description	Enter an optional description for the context.

Table 59-2 Add/Edit Security Context Dialog Box (PIX/ASA) (continued)

Element	Description
Mode (ASA 9.0+)	Choose the mode, Router or Transparent, for this security context. **Note** You cannot change the chosen mode in the Edit Security Context dialog box.
Admin Context	Check this box if this context is to be the Admin context for this device. **Note** The name of the Admin context for the device is displayed below the Security Contexts table. **Note** If this box is checked, the IPv4 Address Pool field is disabled.
Config URL	Specify the context configuration location, as a URL-type address, by choosing a file-system protocol and then entering the path and name of the file to access for the context configuration. That is, choose a protocol type from the drop-down list, and then type the server name (for remote file systems), path, and file name in the related text field. For example, the combined URL for FTP has the following format: `ftp://server.example.com/configs/admin.cfg`. Available protocols are: • `disk0:/` • `disk1:/` • `flash:/` • `ftp://` • `http://` • `https://` • `tftp://`
VPN in multiple context mode—Beginning with Security Manager version 4.12 for ASA version 9.6(2) devices, remote access VPN on multi-context supports flash virtualization. Within a multi-context structure, each created user context can have a private storage space and a shared storage place based on the total flash that is available.	
Storage URL - Private	Click the Private check box to store files associated only with that user and specific to the content that you want for that user. From the drop-down menu, choose the private directory that you created and map it to what you designated in Config URL. Select one of the following options for Private Storage URL for multi-context ASA 9.6(2) or later devices. • `disk0:/` • `flash:/` The default value of Storage URL - Private is **disk0:/**. You can modify this value. This context label name is used as a directory while performing any file deploy activity for ASA 9.6(2) Multi Context devices.

Table 59-2 Add/Edit Security Context Dialog Box (PIX/ASA) (continued)

Element	Description
Storage URL - Shared	Click the Shared check box to upload files to the shared storage space and have it accessible to any user context for read/write access. From the drop-down menu. choose the shared directory that you created and map it to what you designated in Config URL. Select one of the following options for Shared Storage URL for multi-context ASA 9.6(2) or later devices. • `disk0:/` • `flash:/` The default value of Storage URL - Shared is **shared**. You can modify this value. This context label name is used as a directory while performing any file deploy activity for ASA 9.6(2) Multi Context devices.
ScanSafe Settings	To enable ScanSafe inspection in this context, select Enable ScanSafe Web Security. To override the license specified in the system configuration, enter a license ID in the License field; must be 32 hexadecimal characters. See Chapter 20, "Working with ScanSafe Web Security" for more information.
Interfaces	This table lists the interfaces and subinterfaces allocated to this context, and their associated settings. These are the interfaces and subinterfaces for which the security context will inspect traffic. To add interfaces and subinterfaces to this context, click the Add Row button below the table to open the Allocate Interfaces Dialog Box (PIX/ASA only), page 59-11. You can allocate one or more interfaces, and optionally with each interface, one or a range of subinterfaces. To edit an allocation entry, select it and then click the Edit Row button below the table to open the Edit Interface dialog box. Note that you can edit only the Alias Name and the Show hardware properties option; you cannot change the interface/subinterface assignments. Refer to Allocate Interfaces Dialog Box (PIX/ASA only), page 59-11 for more information about these options. To remove an interface/subinterface allocation, select the appropriate row in this table and then click the Delete Row button below the table.
Failover Group	If this context is part of an active/active failover configuration, choose the failover group to which this context belongs.

Allocate Interfaces Dialog Box (PIX/ASA only)

The Allocate Interfaces dialog box lets you assign an interface, and optionally one or a range of related subinterfaces, to a context, and set name-aliasing options.

Navigation Path

You access the Allocate Interfaces dialog box from the Add Security Context and Edit Security Context dialog boxes. See Add/Edit Security Context Dialog Box (PIX/ASA), page 59-9 for more information.

Related Topics

- Managing Security Contexts, page 59-7

Field Reference

Table 59-3 Allocate Interfaces Dialog Box

Element	Description
Physical Interface	Choose a physical interface to assign to this context. In transparent firewall mode, you can assign only an interface that has not been allocated to another context. If you choose an interface already assigned to another context, you must also specify an subinterface.
Sub Interface ID From/To	Use these drop-down lists to specify a subinterface, or a range of subinterfaces; both lists present the subinterface IDs associated with the chosen Physical Interface. To specify a single subinterface, choose the desired ID from the first list. To specify a range, if available, choose the ending ID from the second list. (In transparent firewall mode, only subinterfaces that have not been allocated to other contexts are shown.)
View Allocation button	Click this button to open the View Interface Allocation dialog box, which presents a read-only list of all physical interfaces defined on this device and the security contexts and failover groups associated with each. You can use this to quickly determine current allocations without closing the Allocate Interfaces dialog box.
Use aliased name in context	To enable name aliasing for this interface/subinterface, check **Use aliased names in the security context** and then enter an alias in the Alias Name field. The specified alias replaces the name of this physical interface or subinterface anywhere it would be displayed for this context—for example, the Hardware Port column on the Interfaces Page.
Alias Name	Enter the desired alias. An alias must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and underscores.
Suffix Range From/To	If you specified a range of subinterfaces, these fields are available to let you specify numeric suffixes for their aliased name. The aliased name for each subinterface consists of its sequence number from this range appended to the Alias Name you provided in the previous field. These values default to the beginning and ending subinterface ID numbers, but you can enter any valid range of numbers.
Show hardware properties in context	Select this option to allow the **show interface** CLI command to display of physical interface properties for the context even if you defined an alias. If not selected, the show interface output includes the aliased name.