Configuring Hostname, Resources, User Accounts, and SLAs

The following topics describe configuring the host name on a security appliance, defining and managing Resource classes on Firewall Services Modules (FWSMs) in multiple-context mode, managing user accounts in the Local user database, and monitoring service level agreements (SLAs) to perform route tracking.

This chapter contains the following topics:

Hostname Page

You can use the Hostname page to specify a host name for your security device, and to specify a default domain. After the configuration file is deployed, the device uses this domain name when you do not enter a fully-qualified domain name in other commands. It also uses this domain name in RSA key generation.

The device appends this domain name to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name “jupiter,” the security appliance completes the name to “jupiter.example.com.”

When you set a host name for the security appliance, that name appears in the command line prompt. If you establish sessions to multiple devices, the host name helps you keep track of where you enter commands. The default host name depends on your platform.

In multiple-context mode, you can specify a domain name for each context, as well as the system execution space. The host name you specify in the system execution space appears in the command line prompt for all contexts. The host name that you optionally set within a context does not appear in the command line, but can be used by the banner command $(hostname) token.

Navigation Path

In Device View, select a security device and then select **Platform > Device Admin > Hostname** from the Device Policy selector.

Field Reference

Table 1: Hostname Page

Element	Description
Host Name	Enter a unique device name to help you differentiate among devices; for example, *PIX-510-A* . **Note** We recommend that you use a unique host name for each device you manage. The device name can be up to 63 alphanumeric (U.S. English) characters and can include any of the following special characters: ` ( ) + - , . / : =.
Domain Name	Optionally, enter a valid Domain Name System (DNS) domain name for the device; for example, *cisco.com* .

Resource Management on Multi-context FWSMs

Note From version 4.17, though Cisco Security Manager continues to support FWSM features/functionality, it does not support any bug fixes or enhancements.

By default, all security contexts on a multiple-context Firewall Services Module (FWSM) have unlimited access to the resources of the FWSM, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.

Note The FWSM does not limit the bandwidth per context; however, the switch containing the FWSM can limit bandwidth per VLAN. See the switch documentation for more information.

The FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by its class. When you create a class, the FWSM does not set aside a portion of the resources for each context assigned to the class; rather, the FWSM sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can “use up” those resources, potentially affecting service to other contexts.

You can set the limit for all resources together as a percentage of the total available for the device. Also, you can set the limit for individual resources as a percentage or as an absolute value.

You can oversubscribe the FWSM by assigning more than 100 percent of the resources across all contexts. For example, you can set up a class to limit connections to 20 percent per context, and then assign 10 contexts to the class for a total of 200 percent. If contexts concurrently use more than the system limit, then each context gets less than the 20 percent you intended.

The FWSM also lets you assign unlimited access to one or more resources in a class, instead of a percentage or absolute number. When a resource is unlimited, contexts can use as much of the resource as the system has available. For example, contexts A, B, and C are assigned to class “Onepercent,” which limits each class member to one percent of the system inspections per second, for a total of three percent; but the three contexts are currently only using two percent combined. On the other hand, class “Nolimit” has unlimited access to inspections. The contexts in Nolimit can use more than the 97 percent of “unassigned” inspections; they can also use the one percent of inspections not currently in use by contexts A, B, and C, even if that means that contexts A, B, and C are unable to reach their three percent combined limit. Setting unlimited access is similar to oversubscribing the FWSM, except that you have less control over how much you oversubscribe the system.

Default Class

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a two percent limit for all concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with a two percent limit for all resources, the class uses no settings from the default class.

As initially configured, the default class provides unlimited access to resources for all contexts, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions – 5 sessions
- SSH sessions – 5 sessions
- IPSec sessions – 5 sessions
- MAC addresses – 65,535 entries

Note that you can edit the default class.

Related Topics

- Resources Page , on page 3
- Add/Edit Security Context Dialog Box (FWSM)

Resources Page

Use the Resources page to configure and manage resource-management classes.

The table on this page lists all currently defined resource classes. Use the buttons below the table to manage this list:

- Add Row – Opens the Add Resource dialog box, where you can define a new class, and assign it to security contexts. See Add and Edit Resource Dialog Boxes , on page 4 for more information.
- Edit Row – For the currently selected row, opens the Edit Resource dialog box, so you can edit that class and its context assignments. See Add and Edit Resource Dialog Boxes , on page 4 for more information.
- Delete Row – Deletes the currently selected row(s); confirmation may be required.

Navigation Path

In Device View, select the system context of an ASA or FWSM in multiple-context mode, and then select **Platform > Device Admin > Resources** from the Device Policy selector.

Related Topics

- Resource Management on Multi-context FWSMs , on page 2

Add and Edit Resource Dialog Boxes

Use the Add Resource and Edit Resource dialog boxes to add or edit resource classes and assignments for FWSM and ASA security contexts.

Except for their titles, both dialog boxes are identical; the following descriptions apply to both.

Navigation Path

You can access the Add Resource and Edit Resource dialog boxes from the Resources Page , on page 3.

Related Topics

- Resource Management on Multi-context FWSMs , on page 2

Field Reference

Table 2: Add and Edit Resource Dialog Boxes

Element	Description
Class Name	Enter a name for this class; can be a string of up to 20 alphanumeric characters, and may include any of the following special characters: ` ( ) + - , . / : =.
Limits Tab	
Note For the following Limits, if you do not specify a value for a particular limit, the limit is inherited from the default class. If the default class does not set that limit, the limit inherits the system limit. Also, any value you enter is considered to be that rate *per second* , unless you also check the related **percent** box, in which case the value is that percentage of the total resource.	
TCP or UDP Connections	Sets a Rate Limit for TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. You can set the limit as an absolute value by entering an integer between 0 (system limit) and 102400, or you can assign more than 100 percent if you want to oversubscribe the device.
Inspections (Fixups)	Sets a Rate Limit for application inspections. You can set the limit as an absolute value by entering an integer between 0 (system limit) and 10000 per second, or you can assign more than 100 percent if you want to oversubscribe the device.
Syslog Messages	Sets a Rate Limit for system log messages. You can set the limit as an absolute value, or you can assign more than 100 percent if you want to oversubscribe the device. The FWSM can support 30,000 messages per second for messages sent to the FWSM terminal or buffer. If you send messages to a syslog server, the FWSM supports 25,000 per second.

Element	Description
Connections	Sets the Absolute Limit for concurrent TCP or UDP connections. You can set the limit as an absolute value by entering an integer between 0 (system limit) and 999900, or you can assign more than 100 percent if you want to oversubscribe the device. **Note** For concurrent connections, the FWSM allocates half of the limit to each of two network processors (NPs) that accept connections. Typically, the connections are divided evenly between the NPs. However, in some circumstances, the connections are not evenly divided, and the maximum connection limit could be reached on one NP before reaching the maximum on the other. In this case, the maximum connections allowed is less than the limit you set. The NP distribution is controlled by the switch, based on a distribution algorithm. You can adjust this algorithm on the switch, or you can adjust the connection limit upward to account for the inequity.
Hosts	Sets the limit for concurrent hosts that can connect through the FWSM. You can set the limit as an absolute value by entering an integer between 0 (system limit) and 262144, or you can assign more than 100 percent if you want to oversubscribe the device.
IPsec Sessions	Sets the limit for IPsec sessions. You can set the limit as an absolute value by entering an integer between 1 and 5, or you can assign more than 100 percent if you want to oversubscribe the device. The system allows a maximum of 10 concurrent sessions divided between all contexts.
SSH Sessions	Sets the limit for SSH sessions. You can set the limit as an absolute value by entering an integer between 1 and 5, or you can assign more than 100 percent if you want to oversubscribe the device. The system allows a maximum of 100 concurrent sessions divided between all contexts.
Telnet Sessions	Sets the limit for concurrent Telnet sessions. You can set the limit as an absolute value by entering an integer between 1 and 5, or you can assign more than 100 percent if you want to oversubscribe the device. The system allows a maximum of 100 concurrent sessions divided between all contexts.
NAT Translations	Sets the limit for concurrent address translations. You can set the limit as an absolute value by entering an integer between 0 (system limit) and 266144, or you can assign more than 100 percent if you want to oversubscribe the device.
MAC Address	(Transparent mode only) Sets the limit for concurrent MAC address entries allowed in the MAC address table. You can set the limit as an absolute value by entering an integer between 0 (system limit) and 65535, or you can assign more than 100 percent if you want to oversubscribe the device.

Element	Description
ASDM	Sets the limit for ASDM management sessions (the default is 5). You can set the limit as an absolute value by entering an integer between 1 and 5, or you can enter a percentage between 3.0 and 15.0. The system allows a maximum of 80 concurrent sessions divided between all contexts. ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 80 ASDM sessions represents a limit of 160 HTTPS sessions, divided between all contexts.
Other VPN	Sets the limit for Site-to-site VPN sessions. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The sessions you assign for this resource are guaranteed to the context.
Other VPN Burst	Sets the limit for the number of site-to-site VPN sessions allowed beyond the amount assigned to a context with vpn other. For example, if your model supports 5000 sessions, and you assign 4000 sessions across all contexts with vpn other, then the remaining 1000 sessions are available for other vpn burst. Unlike other vpn, which guarantees the sessions to the context, other vpn burst can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis.
Note	The maximum value for Anyconnect VPN and Anyconnect VPN Burst depends on ASA licenses. Cisco Security Manager cannot validate the values entered for Anyconnect VPN and Anyconnect VPN Burst. Therefore, the user should make sure that the values for Anyconnect VPN and Anyconnect VPN Burst are within the maximum values; else it results in a deployment error. To find the maximum value, telnet into ASA and execute the show version command. The Total VPN Peers value corresponds to the maximum value.
Anyconnect VPN	Secure Client peers. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The peers you assign for this resource are guaranteed to the context.
Anyconnect VPN Burst	The number of Secure Client sessions allowed beyond the amount assigned to a context with Secure Client. For example, if your model supports 5000 peers, and you assign 4000 peers across all contexts with Secure Client, then the remaining 1000 sessions are available for AnyConnect Burst. Unlike Secure Client, which guarantees the sessions to the context, AnyConnect Burst can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis.
Storage	Beginning with version 4.12, Security Manager enables you to enter the storage size or select Default. This feature is available for ASA version 9.6(2) or later. The limit is set in MB. The default limit is 100% of the disk configured since this storage cannot span multiple disks.
All Resources Limit	Sets a limit for all resources. If you also set the limit for a specific resource, then that limit overrides the limit you set here for all resources. You can set the limit as a percentage, or as unlimited by setting the value to **0** (when **percent** is not checked). You cannot set any other absolute value. You can assign more than 100 percent if you want to oversubscribe the device.

Element	Description
Contexts Tab	
Available Contexts	Lists all contexts available for class assignments; contexts which already have class assignments are not displayed. Select one or more contexts and click the >> button to add the contexts to the Selected Contexts list.
Selected Contexts	Lists all contexts assigned to this class. Select one or more contexts and click the << button to return the contexts to the Available Contexts list.

Configuring User Accounts

The User Accounts page lets you manage the Local user database. User accounts in the Local database can be used in conjunction with the Authentication, Authorization, Accounting (AAA) functions to determine "who is allowed to do what" on a device. Refer to About AAA on Security Devices for more information.

The table on this page lists all currently defined Local user accounts, showing for each, the name of the user and the assigned privilege level. For a detailed explanation of these fields, see Add/Edit User Account Dialog Boxes , on page 8.

Important For a Cisco Security Manager-managed device, when you intend to change the password in the **Device Properties** page, make sure you update the same in the **User Accounts** page also. When you fail to do so, although the initial phase of communication between Security Manager and the device is successful and even the **Test Connectivity** gets verified successfully, the deployment still fails, because the password configured in the **User Accounts** page gets updated in the **Device Properties** page. It is therefore recommended to ensure that credential updates are made *parallelly* in **Device Properties** and the **User Accounts** pages.

- To add a user account, click the Add Row button.
- To edit the settings for an account, select it and click the Edit Row button.
- To delete a user account, select it and click the Delete Row button.

Navigation Path

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

Related Topics

- Local Database
- Preparing for AAA

Add/Edit User Account Dialog Boxes

Use the Add and Edit User Account dialog boxes to add a local user account or to modify an existing user account.

Navigation Path

You can access the Add and Edit User Account dialog boxes from the User Accounts page, as described in Configuring User Accounts , on page 7.

Field Reference

Table 3: Add/Edit User Account Dialog Boxes

Element	Description
Username	Enter a name for this user account: must be at least four characters; the maximum is 64 characters. Entries are case-sensitive.
Password	
Password as encrypted	Select Plain Text or Encrypted.
Password encrypt type	Select MD5 or PBKDF2.
Password	Enter a unique password for this user account. Entries are case-sensitive. **Note** To protect security, we recommend a password length of at least 8 characters. **Note** For Plain Text passwords: • The length of MD5 password should be three to 32 characters. • The length of PBKDF2 password should be 33 to 127 characters. Ensure PBKDF2 password has correct `sha` key values to avoid deployment failure.
Confirm	Re-enter the user password to confirm it.
Privilege Level	Choose a privilege level for this user; defines local command authorization. The range is 0 (lowest) to 15 (highest). The default privilege level is 2.

Monitoring Service Level Agreements (SLAs) To Maintain Connectivity

You can configure ASA or PIX devices that run version 7.2 or later to perform route tracking by monitoring service level agreements. By monitoring the connectivity to a device on another network, you can track the availability of a primary route and install a backup route if the primary route fails. For example, you can define a default route to an Internet service provider (ISP) gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable. This technique, called Dual ISP, provides security appliances with a form of high availability, which is a vital part of providing customers with the services to which they are entitled.

Without route tracking, there is no inherent mechanism for determining if the route is up or down. A static route remains in the routing table even if the next hop gateway becomes unavailable, and is removed only if the associated interface on the security appliance goes down.

The security appliance performs route tracking by associating a route with a monitoring target that you define in an SLA monitor policy object. It monitors the target using ICMP echo requests, according to the parameters configured in the object. If an echo reply is not received within a specified time period, the SLA monitor is considered down and the associated route is removed from the routing table. A previously configured backup route is used in place of the removed route.

SLA monitoring jobs start immediately after deployment and continue to run unless you remove the SLA monitor from the device configuration (that is, they do not age out).

Related Topics

- Configuring Static Routes
- Configuring Firewall Device Interfaces
- Creating Policy Objects

This section contains the following topics:

- Creating Service Level Agreements , on page 9

Creating Service Level Agreements

The following procedure explains how to configure SLA monitor objects and associate them with routes and interfaces in an ASA or PIX configuration.

Related Topics

- Monitoring Service Level Agreements (SLAs) To Maintain Connectivity , on page 8
- Configuring Static Routes
- Configuring Firewall Device Interfaces
- Creating Policy Objects

Step 1 Create the SLA monitor policy object:

a) Select **Manage** > **Policy Objects** to open the Policy Object Manager (see Policy Object Manager) and select **SLA Monitors** from the table of contents.

Tip You can also create SLA monitor objects when defining policies that use this object type. For more information, see Selecting Objects for Policies.

b) Right-click in the work area and select **New Object** to open the Add SLA Monitor dialog box. For more information, see Configuring SLA Monitor Objects , on page 10.

c) The monitoring options are appropriate for most connections, so you need only configure the following:

- Name—The name of the object.

- SLA Monitor ID—An identifying number for the monitoring process. The number must be unique within a device configuration.
- Monitored Address—The address that you are monitoring. When you select a monitoring target, make sure that it can respond to ICMP echo requests (pings). The target can be any network address that you choose, but consider the use of:
- The ISP gateway address.
- The next hop gateway address (if you are concerned about the availability of the ISP gateway).
- A server on the target network, such as an AAA server, with which the security appliance needs to communicate.
- A persistent network device on the destination network. (A desktop or notebook computer that gets shut down at night is not a good choice.)
- Interface—The interface name, or interface role that identifies an interface, that will be the source of the ICMP messages. The device pings the monitored address from this interface's IP address.

d) Click **OK** to save the object.

Step 2 Configure ASA/PIX policies to use the object to monitor routes. You can configure the following policies to monitor SLAs:

- **Platform** > **Routing** > **Static Route**—When you define a static route, you can select an SLA monitor object to do route tracking for the route. For more information, see Configuring Static Routes and Add/Edit Static Route Dialog Box.
- **Interfaces**—When you define an interface that uses DHCP or PPPoE, you can configure the DHCP or PPPoE learned default routes to be tracked. For more information, see Device Interface: IP Type (PIX/ASA 7.0+).

Configuring SLA Monitor Objects

Use the Add or Edit SLA (Service Level Agreement) Monitor dialog box to create, edit, and copy SLA monitor objects. Each SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The route is periodically checked for availability by sending ICMP echo requests and waiting for the response. If the requests time out, the route is removed from the routing table and replaced with a backup route.

You can configure SLA monitors only for security appliances running PIX/ASA version 7.2 or later. SLA monitoring jobs start immediately after deployment and continue to run unless you remove the SLA monitor from the device configuration (that is, they do not age out).

For more information about configuring and using SLA monitor objects, see Monitoring Service Level Agreements (SLAs) To Maintain Connectivity , on page 8.

Navigation Path

Select **Manage** > **Policy Objects**, then select **SLA Monitors** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Monitoring Service Level Agreements (SLAs) To Maintain Connectivity , on page 8

- Policy Object Manager

Field Reference

Table 4: SLA Monitor Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects.
Description	An optional description of the object.
SLA Monitor ID	The ID number of the SLA operation. Values range from 1 to 2147483647. You can create a maximum of 2000 SLA operations on a device. Each ID number must be unique to the policy and the device configuration.
Monitored Address	The IP address that is being monitored for availability by the SLA operation. For recommendations on selecting an address to monitor, see Monitoring Service Level Agreements (SLAs) To Maintain Connectivity , on page 8.
Interface	The source interface for all ICMP echo requests sent to the monitored address to test its availability. Enter the name of an interface or interface role, or click **Select** to select an it from a list or to create a new interface role.
Frequency	The frequency of ICMP echo request transmissions, in seconds. Values range from 1 to 604800 seconds (7 days). The default is 60 seconds. **Note** The frequency cannot be less than the timeout value; you must convert frequency to milliseconds to compare the values.
Threshold	The amount of time that must pass after an ICMP echo request before a rising threshold is declared, in milliseconds. Values range from 0 to 2147483647 milliseconds. The default is 5000 milliseconds. The threshold value is used only to indicate events that exceed the defined value. You can use these events to evaluate the proper timeout value. It is not a direct indicator of the reachability of the monitored address. **Note** The threshold value should not exceed the timeout value.
Time out	The amount of time that the SLA operation waits for a response to the ICMP echo requests, in milliseconds. Values range from 0 to 604800000 milliseconds (7 days). The default is 5000 milliseconds. If a response is not received from the monitored address within the amount of time defined in this field, the static route is removed from the routing table and replaced by the backup route. **Note** The timeout value cannot exceed the frequency value (adjust the frequency value to milliseconds to compare the numbers).

Element	Description
Request Data Size	The size of the ICMP request packet payload, in bytes. Values range from 0 to 16384 bytes. The default is 28 bytes, which creates a total ICMP packet of 64 bytes. Do not set this value higher than the maximum allowed by the protocol or the Path Maximum Transmission Unit (PMTU). For purposes of reachability, you might need to increase the default data size to detect PMTU changes between the source and the target. A low PMTU can affect session performance and, if detected, might indicate that the secondary path should be used.
ToS	The type of service (ToS) defined in the IP header of the ICMP request packet. Values range from 0 to 255. The default is 0. This field contains information such as delay, precedence, reliability, and so on. It can be used by other devices on the network for policy routing and features such as committed access rate.
Number of Packets	The number of packets that are sent. Values range from 1 to 100. The default is 1 packet. **Tip** Increase the default number of packets if you are concerned that packet loss might falsely cause the security appliance to believe that the monitored address cannot be reached.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects.