Configuring Attack Response Controller for Blocking and Rate Limiting

Note From 4.17, though Cisco Security Manager continues to support IPS features/functionality, it does not support any enhancements as IPS is now End of Life. For more information, see EOL notice.

You can configure an IPS device to implement blocks or rate limits to control attacks. Blocking and rate limiting are primarily of use when operating in promiscuous mode. When operating in inline mode, it is much more efficient to have the IPS drop traffic itself. Blocking and rate limiting are actions that other devices implement at the request of the IPS; thus, configuring blocking and rate limiting is a more complex configuration than simple inline denies.

To configure blocking or rate limiting, you must identify the network device that performs the blocking. A network device that performs blocking is called a blocking device. Many network devices can be used to support blocking: Cisco IOS routers and Catalyst 6500 switches, Cisco security appliances (ASA, PIX, and FWSM), and Catalyst 6500/7600 devices running the Catalyst operating system. You can also configure another IPS device to act as a main blocking sensor.

Note IPS blocking and rate limiting works only for IPS appliances and service modules. You cannot configure it for Cisco IOS IPS.

This chapter contains the following topics:

Understanding IPS Blocking

The Attack Response Controller (ARC) component of the IPS is responsible for managing network devices in response to suspicious events by blocking access from attacking hosts and networks. ARC blocks the IP address on the devices it is managing. It sends the same block to all the devices it is managing, including any other main blocking sensors. ARC monitors the time for the block and removes the block after the time has expired.

Note ARC is formerly known as Network Access Controller. Although the name has been changed, the IPS documentation and configuration interfaces contain references to Network Access Controller, nac, and network-access.

ARC completes the action response for a new block in no more than 7 seconds. In most cases, it completes the action response in less time. To meet this performance goal, you should not configure the sensor to perform blocks at too high a rate or to manage too many blocking devices and interfaces. We recommend that the maximum number of blocks not exceed 250 and the maximum number of blocking items not exceed 10. To calculate the maximum number of blocking items, a security appliance counts as one blocking item per blocking context. A router counts as one blocking item per blocking interface/direction. A switch running Catalyst software counts as one blocking item per blocking VLAN. If the recommended limits are exceeded, ARC might not apply blocks in a timely manner or might not be able to apply blocks at all.

For security appliances configured in multiple-context mode, Cisco IPS does not include VLAN information in the block request. Therefore you must make sure the IP addresses being blocked are correct for each security appliance. For example, the sensor is monitoring packets on a security appliance customer context that is configured for VLAN A, but is blocking on a different security appliance customer context that is configured for VLAN B. Addresses that trigger blocks on VLAN A might refer to a different host on VLAN B.

Note Blocking is not supported on the FWSM on the admin context in multiple-context mode.

There are three types of blocks:

- Host block—Blocks all traffic from a given IP address.

  To configure the IPS to initiate automatic host blocks when a signature is triggered, add the **Request Block Host** event action to a signature, or add it to events based on risk rating using the event action override policy. See Configuring Event Action Overrides, page 40-13 and Configuring Signatures, page 39-4.

- Connection block—Blocks traffic from a given source IP address to a given destination IP address and destination port. Multiple connection blocks from the same source IP address to either a different destination IP address or destination port automatically switch the block from a connection block to a host block.

  To configure the IPS to initiate automatic connection blocks when a signature is triggered, add the **Request Block Connection** event action to a signature, or add it to events based on risk rating using the event action override policy.

- Network block—Blocks all traffic from a given network.

  You can initiate host and connection blocks manually or automatically when a signature is triggered. You can only initiate network blocks manually. You cannot initiate network blocks from within Security Manager; use the IPS Device Manager instead.

Tip Connection blocks and network blocks are not supported on security appliances (firewalls). Security appliances only support host blocks with additional connection information.

Note Do not confuse blocking with the ability of the sensor to drop packets. The sensor can drop packets when the following actions are configured for a sensor in inline mode: deny packet inline, deny connection inline, and deny attacker inline.

On Cisco IOS Software devices (routers and Catalyst 6500 series switches), ARC creates blocks by applying ACLs; on Catalyst 6500/7600 devices that run the Catalyst operating system, ARC creates blocks by applying VACLs. ACLs and VACLs permit or deny passage of data packets through interface directions or VLANs. Each ACL or VACL contains permit and deny conditions that apply to IP addresses. The security appliances use the **shun** command instead of ACLs.

Tip For a list of the specific devices and operating system versions that you can configure as blocking devices, see the supported device information in the chapter "Configuring Attack Response Controller for Blocking and Rate Limiting" in the *Installing and Using Cisco Intrusion Prevention System Device Manager* publication for your IPS software version. These publications are available on Cisco.com at http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html.

The following topics explain more about IPS blocking:

Strategies for Applying Blocks

Blocking is performed only when an event occurs and the event includes the Request Block Connection or Request Block Host event actions. These event actions are not typically needed when you operate the IPS in inline mode, where you use Deny actions to drop undesired traffic.

The following are situations in which you might want to implement blocking actions:

- Promiscuous mode—When running in promiscuous mode, the IPS cannot implement Deny actions. Thus, if you want to prevent traffic from a host, you must implement blocking.
- Inline mode—In inline mode, you can implement Deny actions to immediately drop undesired traffic. However, you might want to add blocking actions to protect other segments of your network.

  For example, suppose that your network consists of five subnets, A, B, C, D, and E, and that each of these segments has an inline IPS device monitoring it. If the IPS for subnet A identifies an attack, the IPS can use Deny actions to protect subnet A, but also use Request Block actions to configure the firewalls that protect B, C, D, and E to shun the attacker before the attack can target those other subnets. In this example, you would want to designate a single IPS as the main blocking sensor and have the other four IPS sensors perform blocking through the main blocking sensor.

Use the following techniques to add the request block actions to an event:

- Event Action Override policy—Configure an event action override rule to add the action to all events based on the event's risk rating. This is a simple approach. You could add the request block action for the same risk ratings used for adding Deny actions. For more information, see Configuring Event Action Overrides, page 40-13.
- Signatures policy—You can add the request block actions to individual signatures. This requires editing each signature to add the action. This can be a time-consuming approach, but it allows you to configure blocking for just the types of events that concern you most. For more information, see Configuring Signatures, page 39-4.

Related Topics

- Understanding IPS Blocking, page 43-1
- Understanding the Master Blocking Sensor, page 43-6
- Understanding Interface Modes, page 37-2
- Configuring IPS Blocking and Rate Limiting, page 43-7
- Blocking Page, page 43-8

Understanding Rate Limiting

Attack Response Controller (ARC) is responsible for rate limiting traffic in protected networks. Rate limiting lets sensors restrict the rate of specified traffic classes on network devices. Rate limit responses are supported for the Host Flood and Net Flood engines, and the TCP half-open SYN signature. ARC can configure rate limits on network devices running Cisco IOS 12.3 or later. Main blocking sensors can also forward rate limit requests to blocking forwarding sensors.

To add a rate limit to a signature, you must add the Request Rate Limit action. You can then edit the signature parameters to set the percentage for these signatures in the Event Actions Settings folder.

Tip You can also manually implement rate limits, but you cannot do so using Security Manager; use the IPS Device Manager instead.

On the blocking device, you must not apply a service policy to an interface/direction that is configured for rate limiting. If you do so, the rate limit action will fail. Before configuring rate limits, confirm that there is no service policy on the interface/direction, and remove it if one exists. ARC does not remove the existing rate limit unless it is one that ARC had previously added.

Rate limits use ACLs, but not in the same way as blocks. Rate limits use ACLs and class-map entries to identify traffic, and policy-map and service-policy entries to police the traffic.

Understanding Router and Switch Blocking Devices

You can use routers or Catalyst 6500/7600 devices running Cisco IOS Software, or Catalyst 6500/7600 devices running the Catalyst operating system, to implement IPS blocking in your network. When you use routers or switches, Attack Response Controller (ARC) configures extended ACLs (on IOS devices) or VLAN ACLs (on Catalyst OS devices) to implement the blocks. These ACLs and VACLs are created and managed in the same way.

Rate limits also use ACLs, but not in the same way as blocks. Rate limits use ACLs and class-map entries to identify traffic, and policy-map and service-policy entries to police the traffic.

Tip IPS considers Catalyst 6500/7600 devices that run Cisco IOS Software to be equivalent to routers. When you add these devices as blocking devices, add them as routers.

When you configure a router interface or switch VLAN as a blocking interface, you can optionally specify the names of pre- and post-ACLs or VACLs. Although specifying ACL or VACL names is optional, if you have configured ACLs or VACLs on the interface or VLAN, you must identify them to the IPS or ARC will remove them from your device configuration.

The pre- and post-ACL/VACL have the following uses:

- The Pre-Block ACL/VACL is mainly used for permitting what you do not want the sensor to ever block. When a packet is checked against the ACL/VACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block ACL/VACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the ACL/VACL. The Pre-Block ACL/VACL can override the deny lines resulting from the blocks.
- The Post-Block ACL/VACL is best used for additional blocking or permitting that you want to occur on the same interface or direction. If you have an existing ACL on the interface or direction that the sensor will manage, that existing ACL can be used as a Post-Block ACL/VACL. If you do not have a Post-Block ACL/VACL, the sensor inserts permit ip any any at the end of the new ACL/VACL.

  If you are managing the IOS Software blocking device in Security Manager, you can identify the ACL name by selecting the blocking device, then selecting **Tools > Preview Config**. Look for the **ip access-group** command in the interface configuration, and check the direction. For example, the following lines show that there is an ACL named CSM_FW_ACL_GigabitEthernet0/1 in the In direction attached to the GigabitEthernet0/1 interface.

  ```
  interface GigabitEthernet0/1
    ip access-group CSM_FW_ACL_GigabitEthernet0/1 in
  ```

  In this example, if you configure GigabitEthernet0/1 in the In direction as a blocking interface, ensure that you specify CSM_FW_ACL_GigabitEthernet0/1 as a pre- or post-ACL. In most cases, you should specify the ACL as the post-ACL, so that the relatively short IPS blocking ACL first filters out undesirable traffic before the blocking device implements your other access rules.

  Because Security Manager does not manage Catalyst OS devices, you must examine a Catalyst OS device configuration outside of Security Manager to determine VACL names. Keep in mind that a Catalyst 6500/7600 device that runs IOS Software can also have VACLs, but the IPS does not do VLAN blocking on Catalyst 6500/7600 VLANs when the device is running IOS Software.

When the sensor starts up, it reads the contents of the two ACL/VACLs. It creates a third ACL/VACL with the following entries in this order, and this combined ACL/VACL is applied to the interface or VLAN:

1. A **permit** line with the sensor IP address or, if specified, the NAT address of the sensor.

   If you select the Allow Sensor IP address to be Blocked option on the General tab of the Blocking policy, this permit entry is not added. For more information, see General Tab, IPS Blocking Policy, page 43-10.
2. Pre-Block ACL/VACL, if specified.
3. Any active blocks generated by the IPS (deny statements).
4. The Post-Block ACL/VACL, if specified.

   If you do not specify a Post-Block ACL/VACL, a **permit ip any any** entry is added to allow all unfiltered traffic. Note that this negates the normal implicit deny any that ends interface ACLs.

   When using Catalyst OS, IDSM-2 inserts **permit ip any any capture** at the end of the new VACL.

If ARC is managing a device and you need to configure the ACL/VACLs on that device, you should disable blocking first. You want to avoid a situation in which both you and ARC could be making a change at the same time on the same device. This could cause the device or ARC to fail. If you need to modify the Pre-Block or Post-Block ACL/VACL, do the following:

1. Disable blocking on the sensor.

   Because you are making a temporary change, you can disable and then reenable blocking by using the IPS Device Manager (IDM) on the device. Alternatively, you can deselect the Enable Blocking option on the General tab of the Blocking policy in Security Manager, then deploy the configuration to the IPS sensor. To reenable blocking, select the Enable Blocking option again and deploy the configuration to the IPS sensor.
2. Make the changes to the configuration of the device. For example, if you manage the blocking device in Security Manager, deploy the updated configuration and wait for the device to reload.
3. Reenable blocking on the sensor.

Understanding the Master Blocking Sensor

Multiple sensors (blocking forwarding sensors) can forward blocking requests to a specified main blocking sensor, which controls one or more devices. The main blocking sensor is the ARC running on a sensor that controls blocking on one or more devices on behalf of one or more other sensors. When a signature fires that has blocking or rate limit requests configured as event actions, the sensor forwards the block or rate limit request to the main blocking sensor, which then performs the block or rate limit.

When you add a main blocking sensor, you reduce the number of blocking devices per sensor. For example, if you want to block on 10 firewalls and 10 routers with one blocking interface/direction each, you can assign 10 to the sensor and assign the other 10 to a main blocking sensor.

You configure main blocking sensors on the Master Blocking Sensors tab of the Blocking policy, as described in Blocking Page, page 43-8.

When configuring main blocking sensors, keep the following tips in mind:

- Two sensors cannot control blocking or rate limiting on the same device. If this situation is needed, configure one sensor as the main blocking sensor to manage the devices and the other sensors can forward their requests to the main blocking sensor.
- On the blocking forwarding sensor, identify which remote host serves as the main blocking sensor; on the main blocking sensor you must add the blocking forwarding sensors to its access list using the Allowed Hosts policy. See Identifying Allowed Hosts, page 36-7.
- If the main blocking sensor requires TLS for web connections, you must configure the ARC of the blocking forwarding sensor to accept the X.509 certificate of the main blocking sensor remote host. Sensors by default have TLS enabled, but you can change this option. For more information, see Master Blocking Sensor Dialog Box, page 43-13.
- Typically the main blocking sensor is configured to manage the network devices. Blocking forwarding sensors are not normally configured to manage other network devices, although doing so is permissible.
- Only one sensor should control all blocking interfaces on a device.

Configuring IPS Blocking and Rate Limiting

If you use the Request Block Host, Request Block Connection, or Request Rate Limit actions on any signatures, or add them to events using the event action override policy, you must configure blocking devices. If you do not use these actions, there is no need to configure blocking devices.

Before you configure blocking, read the following topics:

- Understanding IPS Blocking, page 43-1
- Strategies for Applying Blocks, page 43-3
- Understanding Rate Limiting, page 43-4
- Understanding Router and Switch Blocking Devices, page 43-4
- Understanding the Master Blocking Sensor, page 43-6

Step 1 Do one of the following:

- (Device view) Select **Platform > Security > Blocking** from the Policy selector.
- (Policy view) Select **IPS > Platform > Security > Blocking**, then select an existing policy or create a new one.

For an overview of the blocking policy, see Blocking Page, page 43-8.

Step 2 On the General tab, change any settings where you want non-default values. However, the default values are appropriate for most networks. For detailed information about the settings, see General Tab, IPS Blocking Policy, page 43-10.

Step 3 Click the **User Profiles** tab and create the user profiles that are required to log into the blocking devices.

- To add a profile, click the **Add Row** button and fill in the Add User Profile dialog box (see User Profile Dialog Box, page 43-12).
- To edit a profile, select it and click the **Edit Row** button.
- To delete a profile, select it and click the **Delete Row** button. Before you delete a profile, ensure that it is not currently being used by a blocking device.

Step 4 If you need to use a main blocking sensor, as described in Understanding the Master Blocking Sensor, page 43-6, click the **Master Blocking Sensors** tab and do the following:

- To add a main blocking sensor, click the **Add Row** button and fill in the Add Master Blocking Sensor dialog box (see Master Blocking Sensor Dialog Box, page 43-13).
- To edit a main blocking sensor, select it and click the **Edit Row** button.
- To delete a main blocking sensor, select it and click the **Delete Row** button.

Step 5 Identify the blocking devices (unless you will use main blocking sensors only). You must add the devices to the correct tab:

- **Routers** tab—For all Cisco IOS Software devices, including Catalyst 6500 switches that are running IOS Software.
- **Firewalls** tab—For ASA, PIX, and FWSM.
- **Catalyst 6K** tab—For Catalyst 6500/7600 devices that are running the Catalyst operating system.

On each tab, the configuration steps are the same:

- To add a device, click the **Add Row** button and fill in the Add Router, Firewall, or Cat6K Device dialog box (see Router, Firewall, Cat6K Device Dialog Box, page 43-14).

- To edit a device, select it and click the **Edit Row** button.
- To delete a device, select it and click the **Delete Row** button.

Step 6 Click the **Never Block Hosts and Networks** tab and identify the hosts and networks that should never be blocked. These lists affect blocking actions, but they do not affect limiting actions. Identify your trusted networks and hosts:

- To add a host or network, click the **Add Row** button beneath the appropriate table and fill in the Add Never Block Host or Network dialog box (see Never Block Host or Network Dialog Boxes, page 43-17).
- To edit a host or network, select it and click the **Edit Row** button.
- To delete a host or network, select it and click the **Delete Row** button.

Blocking Page

Use the Blocking page to configure IPS sensor blocking properties. Configure the blocking policy only if you use the Request Block Connection, Request Block Host, or Request Rate Limit event actions in your signatures or event actions policies. Blocking hosts are used only for events to which these actions are assigned.

Tip The list of hosts and networks to never block applies only to the Request Block Connection and Request Block Host event actions. The list does not affect rate limiting, nor does it affect any of the Deny actions such as Deny Packet Inline. To exempt hosts and networks from Deny or rate limiting actions, use event action filter rules, specify the hosts and networks as Attackers, and remove the actions from events. For more information, see Configuring Event Action Filters, page 40-4.

Navigation Path

- (Device view) Select **Platform > Security > Blocking** from the Policy selector.
- (Policy view) Select **IPS > Platform > Security > Blocking**, then select an existing policy or create a new one.

Related Topic

- Configuring IPS Blocking and Rate Limiting, page 43-7
- Understanding IPS Blocking, page 43-1
- Strategies for Applying Blocks, page 43-3
- Understanding Rate Limiting, page 43-4
- Understanding Router and Switch Blocking Devices, page 43-4
- Understanding the Master Blocking Sensor, page 43-6
- Understanding IPS Event Actions, page 40-2

Field Reference

Table 43-1 IPS Blocking Policy

Element	Description
General tab	The basic settings required to enable blocking and rate limiting. For information about the options on the General tab, see General Tab, IPS Blocking Policy, page 43-10.
User Profiles tab	The connection credential information profiles for logging into the blocking devices. Before you define a blocking device, create the user profile required to log into the device. The table shows the profile name, username, and the passwords, which are masked with a fixed number of asterisks. • To add a profile, click the **Add Row** button and fill in the Add User Profile dialog box (see User Profile Dialog Box, page 43-12). • To edit a profile, select it and click the **Edit Row** button. • To delete a profile, select it and click the **Delete Row** button. Before you delete a profile, ensure that it is not currently being used by a blocking device.
Master Blocking Sensors tab	The main blocking IPS sensors (see Understanding the Master Blocking Sensor, page 43-6). A main blocking sensor manages blocks for other IPS devices. The table shows the IP address (or network/host object) of the main blocking sensor, the username and password for logging into it, the port used for connections, and whether TLS is used for login. • To add a main blocking sensor, click the **Add Row** button and fill in the Add Master Blocking Sensor dialog box (see Master Blocking Sensor Dialog Box, page 43-13). • To edit a main blocking sensor, select it and click the **Edit Row** button. • To delete a main blocking sensor, select it and click the **Delete Row** button.
Router tab	The IOS routers and Catalyst 6500/7600 devices (that are running IOS Software) to be used as blocking or rate limiting devices. The table shows the IP address (or network/host object) of the device, the communication method used to log into it, the NAT address of the sensor (0.0.0.0 if NAT is not used), the name of the profile that is used for logging into the device, and the device's response capabilities (blocking, rate limiting, or both). • To add a router, click the **Add Row** button and fill in the Add Router Device dialog box (see Router, Firewall, Cat6K Device Dialog Box, page 43-14). • To edit a router, select it and click the **Edit Row** button. • To delete a router, select it and click the **Delete Row** button.

Table 43-1 IPS Blocking Policy (continued)

Element	Description
Firewall tab	The ASA, PIX, and FWSM devices to be used as blocking devices. The table shows the IP address (or network/host object) of the device, the communication method used to log into it, the NAT address of the sensor (0.0.0.0 if NAT is not used), and the name of the profile that is used for logging into the device. • To add a firewall, click the **Add Row** button and fill in the Add Firewall Device dialog box (see Router, Firewall, Cat6K Device Dialog Box, page 43-14). • To edit a firewall, select it and click the **Edit Row** button. • To delete a firewall, select it and click the **Delete Row** button.
Catalyst 6K tab	The Catalyst 6500/7600 devices that are using Catalyst software to be used as blocking devices. The table shows the IP address (or network/host object) of the device, the communication method used to log into it, the NAT address of the sensor (0.0.0.0 if NAT is not used), and the name of the profile that is used for logging into the device. **Tip** Do not use this tab for Catalyst 6500/7600 devices that run Cisco IOS Software. Instead, use the Router tab. • To add a Catalyst OS device, click the **Add Row** button and fill in the Add Cat6K Device dialog box (see Router, Firewall, Cat6K Device Dialog Box, page 43-14). • To edit a Catalyst OS device, select it and click the **Edit Row** button. • To delete a Catalyst OS device, select it and click the **Delete Row** button.
Never Block Hosts and Networks	The hosts and networks that should never be blocked. Hosts and networks are shown in separate tables. The tables show the IP address or network/host object for the host or network. These lists do not affect rate limiting actions, nor do they apply to Deny actions. • To add a host or network, click the **Add Row** button beneath the appropriate table and fill in the Add Never Block Host or Network dialog box (see Never Block Host or Network Dialog Boxes, page 43-17). • To edit a host or network, select it and click the **Edit Row** button. • To delete a host or network, select it and click the **Delete Row** button.

General Tab, IPS Blocking Policy

Use the General tab of the Blocking policy to configure the basic settings required to enable blocking and rate limiting.

Navigation Path

- (Device view) Select **Platform > Security > Blocking** from the Policy selector. If necessary, select the **General** tab.
- (Policy view) Select **IPS > Platform > Security > Blocking**, then select an existing policy or create a new one. If necessary, select the **General** tab.

Related Topic

- Understanding IPS Blocking, page 43-1
- Configuring IPS Blocking and Rate Limiting, page 43-7
- Blocking Page, page 43-8

Field Reference

Table 43-2 General Tab, IPS Blocking Policy

Element	Description
Log All Block Events and Errors	Whether to log events that follow blocks from start to finish and any error messages that occur. When a block is added to or removed from a device, an event is logged. You may not want all these events and errors to be logged. Disabling this option suppresses new events and errors. The default is enabled. **Note** Log all block events and errors also applies to rate limiting.
Enable NVRAM Write	Whether to have the router write to non-volatile RAM (NVRAM) when Attack Response Controller (ARC) first connects. If enabled, NVRAM is written each time the ACLs are updated. The default is disabled. Enabling NVRAM writing ensures that all changes for blocking and rate limiting are written to NVRAM. If the router is rebooted, the correct blocks and rate limits will still be active. If NVRAM writing is disabled, a short time without blocking or rate limiting occurs after a router reboot. Not enabling NVRAM writing increases the life of the NVRAM and decreases the time for new blocks and rate limits to be configured.
Enable ACL Logging	Whether to have ARC append the log parameter to block entries in the access control list (ACL) or VLAN ACL (VACL). This causes the device to generate syslog events when packets are filtered. This option applies to routers and switches only. The default is disabled.
Allow Sensor IP address to be Blocked	Whether the sensor IP address can be blocked. The default is disabled. **Tip** If you allow the sensor address to be blocked, the IPS does not add an explicit permit entry to the interface ACL to allow the IPS address. You must ensure that the IPS address is permitted by the device ACL or the IPS cannot implement blocking on the device.
Enable Blocking	Whether to enable the blocking and rate limiting of hosts. The default is enabled. **Note** When you enable blocking, you also enable rate limiting. When you disable blocking, you also disable rate limiting. This means that ARC cannot add new or remove existing blocks or rate limits.

Table 43-2 General Tab, IPS Blocking Policy (continued)

Element	Description
Max Blocks	The maximum number of entries to block. The range is 1 to 65535. The default is 250.
Max Interfaces	The maximum number of interfaces for performing blocks. For example, a PIX 500 series security appliance counts as one interface. A router with one interface counts as one, but a router with two interfaces counts as two. The maximum number of interfaces is 250 per device. The default is 250. You use Max Interfaces to set an upper limit on the number of devices and interfaces that ARC can manage. The total number of blocking devices (not including main blocking sensors) cannot exceed this value. The total number of blocking items also cannot exceed this value, where a blocking item is one security appliance context, one router blocking interface/direction, or one Catalyst Software switch blocking VLAN. **Note** In addition, the following maximum limits are fixed and you cannot change them: 100 interfaces per device, 250 security appliances, 250 routers, 250 Catalyst Software switches, and 100 main blocking sensors.
Max Rate Limits	The maximum number of rate limit entries. The maximum rate limit must be equal to or less than the maximum blocking entries. The range is 1 to 32767. The default value is 250.

User Profile Dialog Box

Use the Add or Modify User Profile dialog box to add or modify a user profile for an IPS blocking device. The profile defines a username and passwords that the IPS device can use to log into and configure the router, switch, or firewall that will implement IPS blocking.

Although you can save a profile that has a profile name only, the requirements for username, password, and enable password are determined by the device. You must specify the items required by the device to enter configuration mode, or the IPS cannot configure blocking on the device.

Navigation Path

From the IPS Blocking policy, select the User Profiles tab and click the **Add Row** button or select an existing sensor and click the **Edit Row** button. For information on opening the Blocking policy, see Blocking Page, page 43-8.

Field Reference

Table 43-3 User Profile Dialog Box

Element	Description
Profile Name	The name of the profile, up to 64 alphanumeric characters.
Username	The username to use when logging into the blocking device.
Password	The login password for the username, if required.

Table 43-3 User Profile Dialog Box (continued)

Element	Description
Enable Password	The enable password for entering Privileged EXEC Mode (enable mode), if required.

Master Blocking Sensor Dialog Box

Use the Add or Modify Master Blocking Sensor dialog box to configure a main blocking sensor. For more information about main blocking sensors, see Understanding the Master Blocking Sensor, page 43-6.

Navigation Path

From the IPS Blocking policy, select the Master Blocking Sensors tab and click the **Add Row** button or select an existing sensor and click the **Edit Row** button. For information on opening the Blocking policy, see Blocking Page, page 43-8.

Field Reference

Table 43-4 Master Blocking Sensor Dialog Box

Element	Description
IP Address	The IP address of the main blocking sensor. Enter the IP address or the name of a network/host policy object that contains a single host address, or click **Select** to select an object from a list or to create a new one.
Username	The username to use to log in to the main blocking sensor. The user account must be an active account configured on the main blocking sensor.
Password	The login password for the username.
Port	The port on which to connect on the main blocking sensor. The default is 443.
TLS	Whether to use TLS. If you select the TLS option, you must configure the ARC of the blocking forwarding sensor to accept the TLS/SSL X.509 certificate of the main blocking sensor remote host. (The blocking forwarding sensor is any device to which you are assigning this blocking policy.) The easiest way to configure the blocking forwarding sensor to accept the X.509 certificate is to use the IPS Device Manager (IDM) to log into the sensor, choose **Configuration > Sensor Management > Certificates > Trusted Hosts > Add Trusted Host**, and add the main blocking sensor as a trusted host. Alternatively, you can log into the sensor CLI, enter configuration mode, and use the **tls trusted-host ip-address** command.

Router, Firewall, Cat6K Device Dialog Box

Use the Add or Modify Router, Firewall, or Cat6K Device dialog box to configure a device as a blocking device for an IPS sensor. The name of the dialog box indicates the type of device you are adding:

- Router—IOS Software routers and Catalyst 6500/7600 devices. These devices can do rate limiting as well as blocking. See Understanding Router and Switch Blocking Devices, page 43-4.
- Firewall—ASA and PIX appliances.
- Cat6K—Catalyst 6500/7600 devices that are running Catalyst OS software.

Tip If the Catalyst 6500/7600 runs Cisco IOS Software, add the device as a router on the Router tab. Do not add the device to the Cat6K tab.

Navigation Path

From the IPS Blocking policy, select the Router, Firewall, or Catalyst 6K tab and click the **Add Row** button or select an existing row and click the **Edit Row** button. For information on opening the Blocking policy, see Blocking Page, page 43-8.

Field Reference

Table 43-5 Router, Firewall, Cat6K Device Dialog Boxes

Element	Description
IP Address	The IP address of the device. Enter the IP address or the name of a network/host policy object that contains a single host address, or click **Select** to select an object from a list or to create a new one.
Communication Type	The communication mechanism used to log in to the blocking device (SSH 3DES, SSH DES, Telnet). The default is SSH 3DES. If you choose SSH 3DES or SSH DES, you must add the device to the known hosts list. The easiest way to add the device to the known hosts list is to use the IPS Device Manager (IDM) to log into the sensor, choose **Configuration > Sensor Management > SSH > Known Host Keys > Add Known Host Key**, and add the device address. Alternatively, you can log into the sensor CLI, enter configuration mode, and use the **ssh host-key** command.
NAT Address	The NAT address of the sensor, if any is used between the sensor and the blocking device. Enter the NAT address or the name of a network/host policy object that contains a single host address, or click **Select** to select an object from a list or to create a new one. Leave the default 0.0.0.0 if NAT is not used.
Profile Name	The login profile used to log in to the blocking device. You must create this profile on the User Profiles tab of the blocking policy or the IPS cannot successfully use this blocking device.

Table 43-5 Router, Firewall, Cat6K Device Dialog Boxes (continued)

Element	Description
Interfaces and directions where blocks will be applied (table) (Routers only.)	The interfaces on the device that should be used for blocking or rate limiting. The table shows the interface name, direction, and the names of existing ACLs that the IPS device should incorporate into the blocking ACL. If the interface already has an ACL configured for the specified direction, you must specify that ACL name as a pre- or post-ACL or the IPS removes the ACL. These ACLs are used for blocking only, not for rate limiting. • To add an interface, click the **Add Row** button and fill in the Add Router Block Interface dialog box (see Router Block Interface Dialog Box, page 43-15). • To edit an interface, select it and click the **Edit Row** button. • To delete an interface, select it and click the **Delete Row** button.
Response Capabilities (Routers only.)	The actions that this router can implement. Use Ctrl+click to select multiple actions (highlighted actions are selected). Options are: • **Block**—The router can implement blocks in response to Request Block Connection and Request Block Host actions. • **Rate Limit**—The router can implement rate limits in response to Request Rate Limit actions.
VLANs where blocks will be applied (table) (Catalyst 6500/7600 devices running the Catalyst operating system only.)	The VLANs on the device that should be used for blocking. The table shows the VLAN name and the names of existing VLAN ACLs (VACL) that the IPS device should incorporate into the blocking VACL. If the VLAN already has a VACL configured, you must specify that VACL name as a pre- or post-VACL or the IPS removes the VACL. • To add a VLAN, click the **Add Row** button and fill in the Add Cat6K Block VLAN dialog box (see Cat6k Block VLAN Dialog Box, page 43-16). • To edit a VLAN, select it and click the **Edit Row** button. • To delete a VLAN, select it and click the **Delete Row** button.

Router Block Interface Dialog Box

Use the Add or Modify Router Block Interface dialog box to configure a blocking interface on a router or IOS Software Catalyst 6500/7600 device that is configured as an IPS blocking device. The IPS sensor uses the interface for blocking actions.

Navigation Path

From the Add or Modify Router Device dialog box, click the **Add Row** button beneath the interfaces table, or select a row in the table and click the **Edit Row** button. For information on opening the Router Device dialog box, see Router, Firewall, Cat6K Device Dialog Box, page 43-14.

Field Reference

Table 43-6 Router Block Interface Dialog Box

Element	Description
Interface Name	The name of the interface on the router that the IPS should use for blocking. Enter the name exactly as it is configured on the router (for example, GigabitEthernet0/1).
Direction	The direction to apply the blocking ACL, In or Out.

Pre ACL Name
Post ACL Name
	The ACLs to combine with the blocking entries that the IPS creates to implement blocking actions. The Pre ACL is added before the blocking ACL, and the Post ACL is added after the blocking ACL. For more information, see Understanding Router and Switch Blocking Devices, page 43-4.
	Tip If you have configured an ACL on the interface in the specified direction, you must specify the name of the ACL in the Pre or Post ACL Name field or the ACL will be removed from the interface. When you identify an interface and direction as a blocking interface, the IPS takes control of the ACL on that interface/direction.
	If you are managing the blocking device in Security Manager, you can identify the ACL name by selecting the blocking device, then selecting **Tools > Preview Config**. Look for the **ip access-group** command in the interface configuration, and check the direction. For example, the following lines show that there is an ACL named CSM_FW_ACL_GigabitEthernet0/1 in the In direction attached to the GigabitEthernet0/1 interface.
	`interface GigabitEthernet0/1`
	`  ip access-group CSM_FW_ACL_GigabitEthernet0/1 in`
	In this example, if you configure GigabitEthernet0/1 in the In direction as a blocking interface, ensure that you specify CSM_FW_ACL_GigabitEthernet0/1 as a pre- or post-ACL. In most cases, you should specify the ACL as the post-ACL, so that the relatively short IPS blocking ACL first filters out undesirable traffic before the blocking device implements your other access rules.

Cat6k Block VLAN Dialog Box

Use the Add or Modify Cat6k Block VLAN dialog box to configure a blocking VLAN on a Catalyst 6500/7600 device that runs the Catalyst operating system and that is configured as an IPS blocking device. The IPS sensor uses the VLAN for blocking actions.

Tip If the Catalyst 6500/7600 runs Cisco IOS Software, add the device as a router, not a Cat6K.

Navigation Path

From the Add or Modify Cat6K Device dialog box, click the **Add Row** button beneath the VLANs table, or select a row in the table and click the **Edit Row** button. For information on opening the Cat6K Device dialog box, see Router, Firewall, Cat6K Device Dialog Box, page 43-14.

Field Reference

Table 43-7 Cat6k Block VLAN Dialog Box

Element	Description
VLAN	The number of the VLAN on the Catalyst 6500/7600 device that the IPS should use for blocking. The number can be 1 to 4094 and must be defined on the device.
Pre VACL Name Post VACL Name	The VLAN ACLs to combine with the blocking entries that the IPS creates to implement blocking actions. The Pre VACL is added before the blocking VACL, and the Post VACL is added after the blocking VACL. For more information, see Understanding Router and Switch Blocking Devices, page 43-4. **Tip** If you have configured a VACL on the VLAN, you must specify the name of the VACL in the Pre or Post VACL Name field or the VACL will be removed from the VLAN. When you identify a VLAN as a blocking interface, the IPS takes control of the VACL on that VLAN. Typically, you would specify the VACL name as the post-VACL.

Never Block Host or Network Dialog Boxes

Use the Add or Modify Never Block Host or Network dialog boxes to specify a host or network that should never be subject to blocking. The name of the dialog box indicates whether you are adding a host or network address.

Enter the IP address or the name of a network/host policy object that specifies the address. You can also click **Select** to select an object from a list or to create a new object. When selecting objects, the object can contain a single entry of the appropriate type. Host addresses do not have subnet masks (for example, 10.100.10.1), whereas network addresses have masks (for example, 10.100.10.0/24).

Navigation Path

From the IPS Blocking policy, select the Never Block Hosts or Networks tab and click the **Add Row** button or select an existing row and click the **Edit Row** button. Hosts and networks are listed in separate tables, so ensure that you click the buttons associated with the desired table. For information on opening the Blocking policy, see Blocking Page, page 43-8.