C H A P T E R 8

Configuring Attack Response Controller for Blocking and Rate Limiting

This chapter provides information for setting up Attack Response Controller (ARC) to perform blocking and rate limiting on the sensor.

Note ARC was formerly known as Network Access Controller. The name has been changed for IPS 5.1, although IDM still contains the term Network Access Controller.

This chapter contains the following sections:

Understanding Blocking

ARC, the blocking application on the sensor, starts and stops blocks on routers, switches, PIX. Firewalls, FWSM, and ASA. 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 master blocking sensors. ARC monitors the time for the block and removes the block after the time has expired.

Caution   If FWSM is configured in multi-mode, blocking is not supported for the admin context. Blocking is only supported in single mode and in multi-mode customer context.

Note   ARC was designed to complete the action response for a new block in no more than 4 to 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 firewall, ASA, or FWSM 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 may not apply blocks in a timely manner or may not be able to apply blocks at all.

For firewalls, such as ASA, PIX Firewall 7.0, and FWSM 2.1 or greater, configured in multi-mode, IPS 5.1 does not include VLAN information in the block request. Therefore you must make sure the IP addresses being blocked are correct for each firewall. For example, the sensor is monitoring packets on a firewall customer context that is configured for VLAN A, but is blocking on a different firewall customer context that is configured for VLAN B. Addresses that trigger blocks on VLAN A may refer to a different host on VLAN B.

There are three types of blocks:

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

- 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.

  Note   Connection blocks are not supported on firewalls. Firewalls only support host blocks with additional connection information.

- 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.

Caution   Do not confuse blocking with the sensor's ability 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.

For automatic blocks, you must choose Request Block Host or Request Block Connection as the event action for particular signatures, and add them to any event action overrides you have configured, so that SensorApp sends a block request to ARC when the signature is triggered. Once ARC receives the block request from SensorApp, it updates the device configurations to block the host or connection. For the procedure to add the Request Block Host or Request Block Connection event actions to the signature, see Assigning Actions to Signatures, page 5-23. Or for the procedure for configuring overrides that add the Request Block Host or Request Block Connection event actions to alarms of specific risk ratings, see Configuring Event Action Overrides, page 7-15.

On Cisco routers and Catalyst 6500 series switches, ARC creates blocks by applying ACLs or 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 PIX Firewall, FWSM, and ASA do not use ACLs or VACLs. The built-in **shun** and **no shun** command is used.

⚠️

Caution   The ACLs that ARC makes should never be modified by you or any other system. These ACLs are temporary and new ACLs are constantly being created by the sensor. The only modifications that you can make are to the Pre- and Post-Block ACLs. For more information, see How the Sensor Manages Devices, page 8-22.

You need the following information for ARC to manage a device:

- Login user ID (if the device is configured with AAA)
- Login password
- Enable password (not needed if the user has enable privileges)
- Interfaces to be managed (for example, ethernet0, vlan100)
- Any existing ACL or VACL information you want applied at the beginning (Pre-Block ACL or VACL) or end (Post-Block ACL or VACL) of the ACL or VACL that will be created

  This does not apply to a PIX Firewall, FWSM, or ASA because they do not use ACLs to block.
- Whether you are using Telnet or SSH to communicate with the device
- IP addresses (host or range of hosts) you never want blocked
- How long you want the blocks to last

🔍

Tip   To check the status of ARC, enter **show statistics network-access** at the `sensor#`. The output shows the devices you are managing, any active blocks and rate limits, and the status of all devices. Or in IDM, choose **Monitoring > Statistics** to see the status of ARC.

✎

Note   ARC is formerly known as Network Access Controller. Although the name has been changed, IDM and the CLI contain references to Network Access Controller, **nac**, and **network-access**.

Understanding Rate Limiting

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 version 12.3 or later. For configuring rate limiting on routers, see Configuring Blocking and Rate Limiting Devices, page 8-18. Master blocking sensors can also forward rate limit requests to blocking forwarding sensors. See Configuring the Master Blocking Sensor for more information.

🔍

Tip   To check the status of ARC, enter **show statistics network-access** at the `sensor#`. The output shows the devices you are managing, any active blocks and rate limits, and the status of all devices. Or in IDM, choose **Monitoring > Statistics** to see the status of ARC.

To add a rate limit, you specify a combination of protocol, destination IP address, and data value to match one of the signatures that are allowed to generate rate limit events. For the procedure, see Managing Active Rate Limits, page 8-11. You must also set the action to Request Rate Limit and set the percentage for these signatures.

Table 8-1 lists the supported signatures and parameters.

Table 8-1   Rate Limit Signatures

Signature ID	Signature Name	Protocol	Destination IP Address Allowed	Data
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	none
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	None
6910	Net Flood UDP	UDP	No	None
6920	Net Flood TCP	TCP	No	None
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

Before Configuring ARC

Before you configure ARC for blocking or rate limiting, make sure you do the following:

- Analyze your network topology to understand which devices should be blocked by which sensor, and which addresses should never be blocked.

⚠

Caution   Two sensors cannot control blocking or rate limiting on the same device. If this situation is needed, configure one sensor as the master blocking sensor to manage the devices and the other sensors can forward their requests to the master blocking sensor. For the procedure, see Configuring the Master Blocking Sensor, page 8-31.

✎

Note   When you add a master 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 master blocking sensor.

- Gather the usernames, device passwords, enable passwords, and connections types (Telnet or SSH) needed to log in to each device.

- Know the interface names on the devices.

- Know the names of the Pre-Block ACL or VACL and the Post-Block ACL or VACL if needed.

- Understand which interfaces should and should not be blocked and in which direction (in or out). You do not want to accidentally shut down an entire network.

Supported Devices

By default, ARC supports up to 250 devices in any combination. The following devices are supported for blocking by ARC:

Note ARC was designed to complete the action response for a new block in no more than 4 to 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 firewall, ASA, or FWSM 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.

Caution If the recommended limits are exceeded, ARC may not apply blocks in a timely manner or may not be able to apply blocks at all.

- Cisco series routers using Cisco IOS 11.2 or later (ACLs):
    - Cisco 1600 series router
    - Cisco 1700 series router
    - Cisco 2500 series router
    - Cisco 2600 series router
    - Cisco 2800 series router
    - Cisco 3600 series router
    - Cisco 3800 series router
    - Cisco 7200 series router
    - Cisco 7500 series router
- Catalyst 5000 switches with RSM with IOS 11.2(9)P or later (ACLs)
- Catalyst 6500 switches and 7600 routers with IOS 12.1(13)E or later (ACLs)
- Catalyst 6500 switches 7600 routers with Catalyst software version 7.5(1) or later (VACLs)
    - Supervisor Engine 1A with PFC
    - Supervisor Engine 1A with MSFC1
    - Supervisor Engine 1A with MFSC2
    - Supervisor Engine 2 with MSFC2
    - Supervisor Engine 720 with MSFC3

Note We support VACL blocking on the Supervisor Engine and ACL blocking on the MSFC.

- PIX Firewall with version 6.0 or later (**shun** command)

– 501

– 506E

– 515E

– 525

– 535

- ASA with version 7.0 or later (**shun** command)

    – ASA-5510

    – ASA-5520

    – ASA-5540

- FWSM 1.1 or later (**shun** command)

You configure blocking using either ACLs, VACLS, or the **shun** command. All firewall and ASA models support the **shun** command.

The following devices are supported for rate limiting by ARC:

- Cisco series routers using Cisco IOS 12.3 or later:

    – Cisco 1700 series router

    – Cisco 2500 series router

    – Cisco 2600 series router

    – Cisco 2800 series router

    – Cisco 3600 series router

    – Cisco 3800 series router

    – Cisco 7200 series router

    – Cisco 7500 series router

Configuring Blocking Properties

This section describes how to configure blocking properties, and contains the following topics:

-
-
-
-

Overview

Use the Blocking Properties pane to configure the basic settings required to enable blocking and rate limiting.

ARC controls blocking and rate limiting actions on managed devices.

You must tune your sensor to identify hosts and networks that should never be blocked, not even manually. You may have a trusted network device whose normal, expected behavior appears to be an attack. Such a device should never be blocked, and trusted, internal networks should never be blocked.

Properly tuning signatures reduces the number of false positives and helps ensure proper network operations. Tuning and filtering signatures prevents alarms from being generated. If an alarm is not generated, the associated block does not occur.

> **Note** Never Block Address does not apply to rate limiting. This option applies only to the Request Block Host and Request Block Connection event actions. It does not apply to the Deny Attacker Inline, Deny Connection Inline, or Deny Packet Inline event actions. Use event action rules to filter out the hosts that you do not want blocked, denied, or dropped. For more information, see Configuring Event Action Filters, page 7-20.

If you specify a netmask, this is the netmask of the network that should never be blocked. If no netmask is specified, only the IP address you specify will never be blocked.

> **Caution** We recommend that you do not permit the sensor to block itself, because it may stop communicating with the blocking device. You can configure this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

By default, blocking is enabled on the sensor. If ARC is managing a device and you need to manually configure something 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.

> **Note** By default, only blocking is supported on Cisco IOS devices. You can override the blocking default by selecting rate limiting or blocking plus rate limiting.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to add or edit blocking properties.

Field Definitions

This section lists the field definitions for blocking properties, and contains the following topics:

- Blocking Properties Pane, page 8-8
- Add and Edit Never Block Address Dialog Boxes, page 8-9

Blocking Properties Pane

The following fields and buttons are found in the Blocking Properties pane.

Field Descriptions:

- Enable blocking— Whether or not to enable blocking of hosts.

    The default is enabled. You receive an error message if Enable blocking is disabled and nondefault values exist in the other fields.

    > **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.

    > **Note**   Even if you do not enable blocking, you can configure all other blocking settings.

- Allow the sensor IP address to be blocked—Whether or not the sensor IP address can be blocked.

    The default is disabled.

- Log all block events and errors—Configures the sensor 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—Configures the sensor to have the router write to NVRAM when 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—Causes ARC to append the log parameter to block entries in the ACL or VACL.

    This causes the device to generate syslog events when packets are filtered. This option only applies to routers and switches. The default is disabled.

- Maximum Block Entries—Maximum number of entries to block.

    The value is 1 to 65535. The default is 250.

- Maximum Interfaces—Configures the maximum number of interfaces for performing blocks.

    For example, a PIX Firewall 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.

> **Note**   You use Maximum 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 master blocking sensors) cannot exceed this value. The total number of blocking items also cannot exceed this value, where a blocking item is one firewall 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: 250 interfaces per device, 250 firewalls, 250 routers, 250 Catalyst Software switches, and 100 master blocking sensors.

- Maximum Rate Limit Entries—Maximum number of rate limit entries.

  The maximum rate limit should be equal or less then the maximum blocking entries. If you configure more rate limit entries than block entries, you receive an error. The value is 1 to 32767. The default is 250.

- Never Block Addresses—Lets you configure IP addresses that you want the sensor to avoid blocking:

> **Note**   Never Block Address does not apply to rate limiting. This option applies only to the Request Block Host and Request Block Connection event actions. It does not apply to the Deny Attacker Inline, Deny Connection Inline, or Deny Packet Inline event actions. Use event action rules to filter out the hosts that you do not want blocked, denied, or dropped. For more information, see Configuring Event Action Filters, page 7-25.

  - IP Address—IP address to never block.
  - Mask—Mask corresponding to the IP address never to block.

Button Functions:

- Add—Opens the Add Never Block Address dialog box. From this dialog box, you can add a host or network to the list of hosts and networks never to be blocked.
- Edit—Opens the Edit Never Block dialog box. From this dialog box, you can change the host or network that is never to be blocked.
- Delete—Removes this host or network from the list of hosts and networks never to be blocked.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Never Block Address Dialog Boxes

The following fields and buttons are found in the Add and Edit Never Block Address dialog boxes.

Field Descriptions:

- IP Address—IP address to never block.
- Mask—Mask corresponding to the IP address never to block.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Blocking Properties

To configure blocking properties, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Blocking Properties**.

The Blocking Properties pane appears.

Step 3 Check the Enable blocking check box to enable blocking and rate limiting.

> **Note** For blocking or rate limiting to operate, you must set up devices to do the blocking or rate limiting. For the procedures, see Configuring Router Blocking or Rate Limiting Device Interfaces, page 8-22, and Configuring Cat 6K Blocking Device Interfaces, page 8-27.

Step 4 Do not check the Allow the sensor IP address to be blocked check box unless necessary.

> **Caution** We recommend that you do not allow the sensor to block itself, because it may stop communicating with the blocking device. You can choose this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

Step 5 Check the Log all block events and errors check box if you want the blocking events and errors logged.

Step 6 Check the Enable NVRAM write check box if you want the sensor to have the router write to NVRAM when ARC first connects.

Step 7 Check the Enable ACL logging check box if you want ARC to append the log parameter to block entries in the ACL or VACL.

Step 8 Enter how many blocks are to be maintained simultaneously (1 to 65535) in the Maximum Block Entries field.

> **Note** We do not recommend setting the maximum block entries higher than 250.

> **Note** The number of blocks will not exceed the maximum block entries. If the maximum is reached, new blocks will not occur until existing blocks time out and are removed.

Step 9 Enter the number of interfaces you want to have performing blocks in the Maximum Interfaces field.

Step 10 Enter the number of rate limit entries (1 to 32767) you want in the Maximum Rate Limit Entries field.

⚠

Caution   The maximum rate limit should be equal or less then the maximum blocking entries. If you configure more rate limit entries than block entries, you receive an error.

Step 11   Click **Add** to add a host or network to the list of addresses never to be blocked.

The Add Never Block Address dialog box appears.

Step 12   Enter the IP address of the host or network in the IP Address field.

Step 13   Enter the network mask of the host or network in the Network Mask field or choose a network mask from the list.

🔎

Tip   To discard your changes and close the Add Never Block Address dialog box, click **Cancel**.

Step 14   Click **OK**.

You receive an error message if the entries are identical.

The new host or network appears in the Never Block Addresses list in the Blocking Properties pane.

Step 15   To edit an existing entry in the never block addresses list, select it, and click **Edit**.

The Edit Never Block Address dialog box appears.

Step 16   Edit the IP address of the host or network in the IP Address field.

Step 17   Edit the network mask of the host or network in the Network Mask field.

🔎

Tip   To discard your changes and close the Edit Never Block Address dialog box, click **Cancel**.

Step 18   Click **OK**.

The edited host or network appears in the Never Block Addresses list in the Allowed Hosts pane.

Step 19   To delete a host or network from the list, select it, and click **Delete**.

The host no longer appears in the Never Block Addresses list in the Blocking Properties pane.

🔎

Tip   To discard your changes, click **Reset**.

Step 20   Click **Apply** to apply your changes and save the revised configuration.

Managing Active Rate Limits

This section describes how to manage active rate limits, and contains the following sections:

Overview

Use the Rate Limits pane to configure and manage rate limiting.

A rate limit restricts the amount of a specified type of traffic that is allowed on a network device interface to a percentage of maximum bandwidth capacity. Traffic that exceeds this percentage is dropped by the network device. A rate limit can restrict traffic to a specified target host, or to all traffic that crosses the configured interface/directions. You can use rate limits permanently or for a specified amount of time. A rate limit is identified by a protocol, an optional destination address, and an optional data value.

⚠

Caution   Although the pane displays source address, source port, and destination port, those fields are not supported in this version.

Because the rate limit is specified as a percent, it may translate to different actual limits on interfaces with different bandwidth capacities. A rate limit percent value must be an integer between 1 and 100 inclusive.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure rate limits.

Field Definitions

This section lists the field definitions for rate limits, and contains the following topics:

Rate Limits Pane

The following fields and buttons are found in the Rate Limits pane.

Field Descriptions:

- Protocol—Protocol of the traffic that is rate limited.
- Rate—Percent of maximum bandwidth that is allowed for the rate-limited traffic.

    Matching traffic that exceeds this rate will be dropped.

- Source IP—(Optional) Source host IP address of the rate-limited traffic.
- Source Port—(Optional) Source host port of the rate-limited traffic.
- Destination IP—Destination Host IP address of the rate-limited traffic.
- Destination Port—(Optional) Destination host port of the rate-limited traffic.

- Data—(Optional) Additional identifying information needed to more precisely qualify traffic for a given protocol.

    For example, echo-request narrows the ICMP protocol traffic to rate-limit pings.

- Minutes Remaining—Remaining minutes that this rate limit is in effect.

- Timeout (minutes)—Total number of minutes for this rate limit.

Button Functions:

- Add—Opens the Add Rate Limit dialog box. From this dialog box, you can configure the options for rate limiting.

- Delete—Deletes this entry from the table.

- Refresh—Refreshes the contents of the table.

Add Rate Limit Dialog Box

The following fields and buttons are found in the Add Rate Limit dialog box.

Field Descriptions:

- Protocol—Protocol of the traffic that is rate-limited (ICMP, TCP, or UDP).

- Rate—Percentage of the maximum bandwidth allowed for the rate-limited traffic.

- Source IP—(Optional) Source host IP address of the rate-limited traffic.

- Source Port—(Optional) Source host port of the rate-limited traffic.

- Destination IP—(Optional) Destination host IP address of the rate-limited traffic.

- Destination Port—(Optional) Destination host port of the rate-limited traffic.

- Use Additional Data—(Optional) Lets you choose whether to specify more data, such as echo-reply, echo-request, or halfOpenSyn.

- Timeout—Lets you choose whether to enable timeout:

    – No Timeout—Timeout not enabled.

    – Enable Timeout—Lets you specify the timeout in minutes (1 to 70560).

Button Functions:

- Apply—Applies your changes and closes the dialog box.

- Cancel—Discards your changes and closes the dialog box.

- Help—Displays the help topic for this feature.

Configuring and Managing Rate Limits

For more information on rate limiting, see Understanding Rate Limiting, page 8-3.

To configure and manage rate limiting, follow these steps:

Step 1   Log in to IDM using an account with administrator or operator privileges.

Step 2   Choose **Monitoring > Rate Limits**.

The Rate Limits pane appears.

Step 3   Click **Add** to add a rate limit.

The Add Rate Limit dialog box appears.

Step 4   Choose the protocol (ICMP, TCP, or UDP) of the traffic you want rate limited from the Protocol list.

Step 5   Enter the rate limit (1 to 100) in the Rate field.

Step 6   (Optional) Enter the destination IP address in the Destination IP field.

Step 7   Check the Use Additional Data check box if you want to configure the rate limit to use additional data.

Step 8   Choose the additional data (echo-reply, echo-request, or halfOpenSyn) from the Select Data list.

Step 9   Check the Enable Timeout check box if you want to configure a timeout in minutes.

Step 10   Enter the amount of time in minutes (1 to 70560) in the Timeout field.

> **Tip**   To discard your changes and close the Add Rate Limit dialog box, click **Cancel**.

Step 11   Check the No Timeout check box if you do not want to configure the rate limit for a specified amount of time.

Step 12   Click **Apply**.

The new rate limit appears in the list in the Rate Limits pane.

Step 13   Click **Refresh** to refresh the contents of the Rate Limits list.

Step 14   To delete a rate limit, choose a rate limit from the list, and click **Delete**.

The Delete Rate Limit dialog box asks if you are sure you want to delete this rate limit.

> **Tip**   To close the Delete Rate Limit dialog box, click **No**.

Step 15   Click **Yes** to delete the rate limit.

The rate limit no longer appears in the rate limits list.

Configuring Device Login Profiles

This section describes how to configure device login profiles, and contains the following topics:

- Overview, page 8-15
- Supported User Role, page 8-15
- Field Definitions, page 8-15
- Configuring Device Login Profiles, page 8-17

Overview

Use the Device Login Profiles pane to configure the profiles that the sensor uses when logging in to blocking devices.

You must set up device login profiles for the other hardware that the sensor manages. The device login profiles contain username, login password, and enable password information under a name that you create. For example, routers that all share the same passwords and usernames can be under one device login profile name.

> **Note** You must have a device login profile created before configuring the blocking devices.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to add or edit device login profiles.

Field Definitions

This section lists the field definitions for device login profiles, and contains the following topics:

- Device Login Profile Pane, page 8-15
- Add and Edit Device Login Profile Dialog Boxes, page 8-16

Device Login Profile Pane

The following fields and buttons are found in the Device Login Profile pane.

Field Descriptions:

- Profile Name—Name of the profile.
- Username—Username used to log in to the blocking device (optional).
- Login Password—Login password used to log in to the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  > **Note** If a password exists, it is displayed with a fixed number of asterisks.

- Enable Password—Enable password used on the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  > **Note** If a password exists, it is displayed with a fixed number of asterisks.

Button Functions:

- Add—Opens the Add Device Login Profile dialog box. From this dialog box, you can add a device login profile.
- Edit—Opens the Edit Device Login Profile box. From this dialog box, you can change the values associated with this device login profile.
- Delete—Removes this device login profile from the list of device login profiles. You receive an error message if you try to delete a profile that is being used.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Device Login Profile Dialog Boxes

The following fields and buttons are found in the Add and Edit Device Login Profile dialog boxes.

Field Descriptions:

- Profile Name—Name of the profile.
- Username—Username used to log in to the blocking device (optional).
- Login Password—Login password used to log in to the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  > **Note** If a password exists, it is displayed with a fixed number of asterisks.

- Enable Password—Enable password used on the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  > **Note** If a password exists, it is displayed with a fixed number of asterisks.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Device Login Profiles

To configure device login profiles, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Device Login Profiles**.

The Device Login Profiles pane appears.

Step 3 Click **Add** to add a profile.

The Add Device Login Profile dialog box appears.

Step 4 Enter the profile name in the Profile Name field.

Step 5 Enter the username used to log in to the blocking device in the Username field.

Step 6 Enter the login password in the New Password field and retype it in the Confirm New Password field.

Step 7 Enter the enable password in the New Password field and retype it in the Confirm New Password field.

> **Tip**   To discard your changes and close the Add Device Login Profile dialog box, click **Cancel**.

Step 8 Click **OK**.

You receive an error message if the profile name already exists.

The new device login profile appears in the list in the Device Login Profile pane.

Step 9 To edit an existing entry in the device login profile list, select it, and click **Edit**.

The Edit Device Login Profile dialog box appears.

Step 10 Edit the username used to log in to the blocking device in the Username field.

Step 11 Check the Change the login password check box to change the login password.

Step 12 Enter the new login password in the New Password field and reenter it in the Confirm New Password field.

Step 13 Check the Change the enable password check box to change the enable password.

Step 14 Enter the new enable password in the New Password field and reenter it in the Confirm New Password field.

> **Tip**   To discard your changes and close the Edit Device Login Profile dialog box, click **Cancel**.

Step 15 Click **OK**.

The edited device login profile appears in the list in the Device Login Profile pane.

Step 16   To delete a device login profile from the list, select it, and click **Delete**.

The device login profile no longer appears in the list in the Device Login Profile pane.

Tip   To discard your changes, click **Reset**.

Step 17   Click **Apply** to apply your changes and save the revised configuration.

Configuring Blocking and Rate Limiting Devices

This section describes how to configure blocking and rate limiting devices, and contains the following topics:

Overview

Use the Blocking Devices pane to configure the devices that the sensor uses to implement blocking and rate limiting.

You can configure your sensor to block an attack by generating ACL rules for deployment to a Cisco IOS router, or a Catalyst 6500 switch, or by generating shun rules on a PIX Firewall or ASA. The router, switch, or firewall is called a blocking device.

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.

Caution   A single sensor can manage multiple devices but multiple senors cannot manage a single device. For that you must use a master blocking sensor. For the procedure for setting up a master blocking sensor, see Configuring the Master Blocking Sensor, page 8-31.

You must specify a device login profile for each device that the sensor manages before you can configure the devices in the Blocking Devices pane.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure blocking devices.

Field Definitions

This section lists the field definitions for blocking devices, and contains the following topics:

Blocking Devices Pane

The following fields and buttons are found in the Blocking Devices pane.

Field Descriptions:

- IP Address—IP address of the blocking device.
- Sensor's NAT Address—(Optional) NAT address of the sensor.
- Device Login Profile—Device login profile used to log in to the blocking device.
- Device Type—Type of device (Cisco Router, Cat 6K, PIX/ASA).

  The default is Cisco Router.
- Response Capabilities—Indicates whether the device uses blocking or rate limiting or both.
- Communication—Indicates the communication mechanism used to log in to the blocking device (SSH 3DES, SSH DES, Telnet).

  The default is SSH 3DES.

Button Functions:

- Add—Opens the Add Blocking Device dialog box. From this dialog box, you can add a blocking device.

  You receive an error message if the IP address already exists.
- Edit—Opens the Edit Blocking Device box. From this dialog box, you can change the values associated with this blocking device.
- Delete—Removes this blocking device from the list of blocking devices. You receive an error message if you try to delete a blocking device that is being used.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Blocking Devices Dialog Boxes

The following fields and buttons are found in the Add and Edit Blocking Device dialog boxes.

Field Descriptions:

- IP Address—IP address of the blocking device.
- Sensor's NAT Address—(Optional) NAT address of the sensor.
- Device Login Profile—Device login profile used to log in to the blocking device.

- Device Type—Type of device (Cisco Router, Cat 6K, PIX/ASA).

  The default is Cisco Router.

- Response Capabilities—Indicates whether the device uses blocking or rate limiting or both.

- Communication—Indicates the communication mechanism used to log in to the blocking device (SSH 3DES, SSH DES, Telnet).

  The default is SSH 3DES.

Button Functions:

- OK—Accepts your changes and closes the dialog box.

- Cancel—Discards your changes and closes the dialog box.

- Help—Displays the help topic for this feature.

Configuring Blocking and Rate Limiting Devices

To configure blocking and rate limiting devices, follow these steps:

Step 1   Log in to IDM using an account with administrator or operator privileges.

Step 2   Choose **Configuration > Blocking > Blocking Devices**.

The Blocking Devices pane appears.

Step 3   Click **Add** to add a blocking device.

You receive an error message if you have not configured the device login profile. For the procedure, see Configuring Device Login Profiles, page 8-14.

The Add Blocking Device dialog box appears.

Step 4   Enter the IP address of the blocking device in the IP Address field.

Step 5   (Optional) Enter the sensor's NAT address in the Sensor's NAT Address field.

Step 6   Choose the device login profile from the Device Login Profile drop-down list.

Step 7   Choose the device type from the Device Type drop-down list.

Step 8   Choose whether the device will perform blocking, rate limiting, or both by checking the Block and/or Rate Limit check boxes.

> **Note**   You must choose the blocking and rate limiting actions for particular signatures so that SensorApp sends a block or rate limit request to ARC when the signature is triggered. For more information, see Assigning Actions to Signatures, page 5-23.

Step 9   Choose the communication type from the Communication drop-down list.

If you choose SSH 3DES or SSH DES, go to Step11.

> **Tip**   To discard your changes and close the Add Blocking Device dialog box, click **Cancel**.

Step 10 Click **OK**.

You receive an error message if the IP address has already been added.

The new device appears in the list in the Blocking Devices pane.

Step 11 If you choose SSH 3DES or SSH DES, you must add the device to the known hosts list:

> ✎
> **Note**   If you choose SSH 3DES or SSH DES, the blocking device must have a feature set or license that supports the desired 3DES/DES encryption.

> ✎
> **Note**   You can also add the device to the known hosts list in the Configuration > SSH > Known Host Keys > Add Known Host Key dialog box. For the procedure, see Defining Known Host Keys, page 2-10.

    a. Telnet to your sensor and log in to the CLI.

    b. Enter global configuration mode:

```
sensor# configure terminal
```

    c. Obtain the public key:

```
sensor(config)# ssh host-key blocking_device_ip_address
```

    d. You are prompted to confirm adding the public key to the known hosts list:

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

    e. Enter **yes**.

    f. Exit global configuration mode and the CLI:

```
sensor(config)# exit
sensor# exit
```

Step 12 To edit an existing entry in the blocking devices list, select it, and click **Edit**.

The Edit Blocking Device dialog box appears.

Step 13 Edit the sensor's NAT address if desired.

Step 14 Change the device login profile if desired.

Step 15 Change the device type if desired.

Step 16 Change whether the device will perform blocking or rate limiting if desired.

Step 17 Change the communication type if desired.

> 🔍
> **Tip**   To discard your changes and close the Edit Blocking Device dialog box, click **Cancel**.

Step 18 Click **OK**.

The edited blocking device appears in the list in the Blocking Device pane.

Step 19 To delete a blocking device from the list, select it, and click **Delete**.

The blocking device no longer appears in the list in the Blocking Device pane.

Tip   To discard your changes, click **Reset**.

Step 20   Click **Apply** to apply your changes and save the revised configuration.

Configuring Router Blocking or Rate Limiting Device Interfaces

This section describes how to configure the router blocking or rate limiting interfaces, and contains the following topics:

- How the Sensor Manages Devices, page 8-22
- Overview, page 8-23
- Supported User Role, page 8-24
- Field Definitions, page 8-24
- Configuring the Router Blocking and Rate Limiting Device Interfaces, page 8-26

How the Sensor Manages Devices

ARC uses ACLs on Cisco routers and switches to manage those devices. These ACLs are built as follows:

Note   ACLs do not apply to rate limiting devices.

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

    Note   If you permit the sensor to be blocked, this line does not appear in the ACL.

2. Pre-Block ACL (if specified)

    This ACL must already exist on the device.

    Note   ARC reads the lines in the ACL and copies these lines to the beginning of the ACL.

3. Any active blocks

4. Either:

    – Post-Block ACL (if specified)

       This ACL must already exist on the device.

       Note   ARC reads the lines in the ACL and copies these lines to the end of the ACL.

> **Note** Make sure the last line in the ACL is **permit ip any any** if you want all unmatched
> packets to be permitted.

   – **permit ip any any** (not used if a Post-Block ACL is specified)

ARC uses two ACLs to manage devices. Only one is active at any one time. It uses the offline ACL name
to build the new ACL, then applies it to the interface. ARC then reverses the process on the next cycle.

> **Caution** The ACLs that ARC makes should never be modified by you or any other system. These ACLs are
> temporary and new ACLs are constantly being created by the sensor. The only modifications that you
> can make are to the Pre- and Post-Block ACLs.

> **Note** The ACLs that ARC creates are not removed from the managed device after you configure ARC to no
> longer manage that device. You must remove the ACLs manually on any device that ARC formerly
> managed.

If you need to modify the Pre-Block or Post-Block ACL, do the following:

1. Disable blocking on the sensor.

2. Make the changes to the device configuration.

3. Reenable blocking on the sensor.

When blocking is reenabled, the sensor reads the new device configuration. For the procedure, see
Configuring Blocking Properties, page 8-6.

> **Caution** A single sensor can manage multiple devices, but you cannot use multiple sensors to control a single
> device. In this case, use a master blocking sensor. For the procedure, see Configuring the Master
> Blocking Sensor, page 8-31.

Understanding Service Policies for Rate Limiting

IPS 5.1 does not support service policies that you define and apply in connection with rate limiting. They
are not compatible with sensor rate limits. 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.

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.

Overview

You must configure the blocking or rate limiting interfaces on the router and specify the direction of
traffic you want blocked or rate-limited in the Router Blocking Device Interfaces pane.

You create and save Pre-Block and Post-Block ACLs in your router configuration. These ACLs must be extended IP ACLs, either named or numbered. See your router documentation for more information on creating ACLs.

Note   Pre-Block and Post-Block ACLS do not apply to rate limiting.

Enter the names of these ACLs that are already configured on your router in the Pre-Block ACL and Post-Block ACL fields.

The Pre-Block ACL is mainly used for permitting what you do not want the sensor to ever block. When a packet is checked against the ACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block ACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the ACL. The Pre-Block ACL can override the deny lines resulting from the blocks.

The Post-Block ACL 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. If you do not have a Post-Block ACL, the sensor inserts **permit ip any any** at the end of the new ACL.

When the sensor starts up, it reads the contents of the two ACLs. It creates a third ACL with the following entries:

- A **permit** line for the sensor IP address
- Copies of all configuration lines of the Pre-Block ACL
- A **deny** line for each address being blocked by the sensor
- Copies of all configuration lines of the Post-Block ACL

The sensor applies the new ACL to the interface and direction that you designate.

Note   When the new ACL is applied to an interface or direction of the router, it removes the application of any other ACL to that interface or direction.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the router blocking device interfaces.

Field Definitions

This section lists the field definitions for router interfaces, and contains the following topics:

Router Blocking Device Interfaces Pane

The following fields and buttons are found in the Router Blocking Device Interfaces pane.

Field Descriptions:

- Router Blocking Device—IP address of the router blocking or rate limiting device.
- Blocking Interface—Interface to be used on the router blocking or rate limiting device.

  A valid value is 1 to 64 characters in the format a-z, A-Z, 0-9 and the special characters "." and "/."
- Direction—Direction to apply the blocking ACL.

  A valid value is In or Out.
- Pre-Block ACL—ACL to apply before the blocking ACL.

  A valid value is 0 to 64 characters. This field does not apply to rate limiting.
- Post-Block ACL—ACL to apply after the blocking ACL.

  A valid value is 0 to 64 characters. This field does not apply to rate limiting

> ✎
>
> **Note**   The Post-Block ACL cannot be the same as the Pre-Block ACL.

Button Functions:

- Add—Opens the Add Router Blocking Device Interface dialog box. From this dialog box, you can add a router blocking or rate limiting device interface.

  You receive an error message if there are no router blocking devices.
- Edit—Opens the Edit Router Blocking Device Interface box. From this dialog box, you can change the values associated with this router blocking or rate limiting device interface.
- Delete—Removes this router blocking device interface from the list of router blocking device interfaces.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Router Blocking Device Interface Dialog Boxes

The following fields and buttons are found in the Add and Edit Router Blocking Device Interface dialog boxes.

Field Descriptions:

- Router Blocking Device—IP address of the router blocking or rate limiting device.
- Blocking Interface—Interface to be used on the router blocking or rate limiting device.

  A valid value is 1 to 64 characters in the format a-z, A-Z, 0-9 and the special characters "." and "/."
- Direction—Direction to apply the blocking ACL.

  A valid value is In or Out.
- Pre-Block ACL—ACL to apply before the blocking ACL.

  A valid value is 0 to 64 characters. This field does not apply to rate limiting.

- Post-Block ACL—ACL to apply after the blocking ACL.

   A valid value is 0 to 64 characters. This field does not apply to rate limiting

   ✎
   Note   The Post-Block ACL cannot be the same as the Pre-Block ACL.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring the Router Blocking and Rate Limiting Device Interfaces

To configure router blocking and rate limiting device interfaces, follow these steps:

Step 1   Log in to IDM using an account with administrator or operator privileges.

Step 2   Choose **Configuration > Blocking > Router Blocking Device Interfaces**.

The Router Blocking Device Interfaces pane appears.

Step 3   Click **Add** to add a router blocking or rate limiting device interface.

The Add Router Blocking Device Interface dialog box appears.

Step 4   Choose the IP address of the router blocking or rate limiting device from the drop-down list.

Step 5   Enter the blocking or rate limiting interface name in the Blocking Interface field.

Step 6   Choose the direction (in or out) from the Direction drop-down list.

Step 7   (Optional) Enter the name of the Pre-Block ACL in the Pre-Block ACL field.

   ✎
   Note   This step does not apply to rate limiting devices.

Step 8   (Optional) Enter the name of the Post-Block ACL in the Post-Block ACL field.

   ✎
   Note   This step does not apply to rate limiting devices.

   🔎
   Tip   To discard your changes and close the Add Router Blocking Device Interface dialog box, click **Cancel**.

Step 9   Click **OK**.

You receive an error message if the IP address/interface/direction combination already exists.

The new interface appears in the list in the Router Blocking Device Interfaces pane.

Step 10   To edit an existing entry in the router blocking device interfaces list, select it, and click **Edit**.

The Edit Router Blocking Device dialog box appears.

Step 11   Edit the blocking or rate limiting interface name.

Step 12   Change the direction.

Step 13   (Optional) Edit the Pre-Block ACL name.

Step 14   (Optional) Edit the Post-Block ACL name.

> **Tip**   To discard your changes and close the Edit Router Blocking Device Interface dialog box, click **Cancel**.

Step 15   Click **OK**.

The edited router blocking or rate limiting device interface appears in the list in the Router Blocking Device Interfaces pane.

Step 16   To delete a router blocking or rate limiting device interface from the list, select it, and click **Delete**.

The router blocking or rate limiting device interface no longer appears in the list in the Router Blocking Device Interfaces pane.

> **Tip**   To discard your changes, click **Reset**.

Step 17   Click **Apply** to apply your changes and save the revised configuration.

Configuring Cat 6K Blocking Device Interfaces

This section describes how to configure Catalyst 6500 series switch interfaces, and contains the following topics:

- Overview, page 8-27
- Supported User Role, page 8-28
- Field Definitions, page 8-28
- Configuring Cat 6K Blocking Device Interfaces, page 8-30

Overview

You specify the VLAN ID and VACLs on the blocking Catalyst 6500 series switch on the Cat 6K Blocking Device Interfaces pane.

You can configure ARC to block using VACLs on the switch itself when running Cisco Catalyst software, or to block using router ACLs on the MSFC or on the switch itself when running Cisco IOS software. This section describes blocking using VACLs. You cannot configure switches that use VACLs to perform rate limiting.

You must configure the blocking interfaces on the Catalyst 6500 series switch and specify the VLAN of traffic you want blocked.

You create and save Pre-Block and Post-Block VACLs in your switch configuration. These VACLs must be extended IP VACLs, either named or numbered. See your switch documentation for more information on creating VACLs.

Enter the names of these VACLs that are already configured on your switch in the Pre-Block VACL and Post-Block VACL fields.

The Pre-Block VACL is used mainly for permitting what you do not want the sensor to ever block. When a packet is checked against the VACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block VACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the VACL. The Pre-Block VACL can override the deny lines resulting from the blocks.

The Post-Block VACL is best used for additional blocking or permitting that you want to occur on the same VLAN. If you have an existing VACL on the VLAN that the sensor will manage, the existing VACL can be used as a Post-Block VACL. If you do not have a Post-Block V ACL, the sensor inserts **permit ip any any** at the end of the new VACL.

Note   IDSM-2 inserts **permit ip any any capture** at the end of the new VACL.

When the sensor starts up, it reads the contents of the two VACLs. It creates a third VACL with the following entries:

- A **permit** line for the sensor's IP address
- Copies of all configuration lines of the Pre-Block VACL
- A **deny** line for each address being blocked by the sensor
- Copies of all configuration lines of the Post-Block VACL

The sensor applies the new VACL to the VLAN that you designate.

Note   When the new VACL is applied to a VLAN of the switch, it removes the application of any other VACL to that VLAN.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the Catalyst 6500 series switches blocking device interfaces.

Field Definitions

This section lists the field definitions for the Catalyst 6500 series switch interfaces, and contains the following topics:

Cat 6K Blocking Device Interfaces Pane

The following fields and buttons are found in the Cat 6K Blocking Device Interfaces pane.

Field Descriptions:

- Cat 6K Blocking Device—IP address of the Catalyst 6500 series switch blocking device.
- VLAN ID—VLAN ID to be used on the Catalyst 6500 series switch blocking device.

  The value is 1 to 4094.
- Pre-Block VACL—VACL to apply before the blocking VACL.

  The value is 0 to 64 characters.
- Post-Block VACL—VACL to apply after the blocking VACL.

  The value is 0 to 64 characters.

> **Note**   The Post-Block VACL cannot be the same as the Pre-Block VACL.

Button Functions:

- Add—Opens the Add Cat 6K Blocking Device Interface dialog box. From this dialog box, you can add a Catalyst 6500 series switch blocking device interface.

  You receive an error if there are no Catalyst 6500 series switches.
- Edit—Opens the Edit Cat 6K Blocking Device Interface box. From this dialog box, you can change the values associated with this Catalyst 6500 series switch blocking device interface.
- Delete—Removes this switch interface from the list of switch blocking device interfaces.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Cat 6K Blocking Device Interface Dialog Boxes

The following fields and buttons are found in the Add and Edit Cat 6K Blocking Device Interface dialog boxes.

Field Descriptions:

- Cat 6K Blocking Device—IP address of the Catalyst 6500 series switch blocking device.
- VLAN ID—VLAN ID to be used on the Catalyst 6500 series switch blocking device.

  The value is 1 to 4094.
- Pre-Block VACL—VACL to apply before the blocking VACL.

  The value is 0 to 64 characters.
- Post-Block VACL—VACL to apply after the blocking VACL.

  The value is 0 to 64 characters.

> **Note**   The Post-Block VACL cannot be the same as the Pre-Block VACL.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Cat 6K Blocking Device Interfaces

To configure Catalyst 6500 series switch blocking device interfaces, follow these steps:

Step 1   Log in to IDM using an account with administrator or operator privileges.

Step 2   Choose **Configuration > Blocking > Cat 6K Blocking Device Interfaces**.

The Cat 6K Blocking Device Interfaces pane appears.

Step 3   Click **Add** to add a Catalyst 6500 series switch blocking device interface.

The Add Cat 6K Blocking Device Interface dialog box appears.

Step 4   Choose the IP address of the Catalyst 6500 series switch from the drop-down list.

Step 5   Enter the VLAN ID in the VLAN ID field.

Step 6   (Optional) Enter the name of the Pre-Block VACL in the Pre-Block VACL field.

Step 7   (Optional) Enter the name of the Post-Block VACL in the Post-Block VACL field.

Tip   To discard your changes and close the Add Cat 6K Blocking Device Interface dialog box, click **Cancel**.

Step 8   Click **OK**.

You receive an error message if issued if the IP address/VLAN combination already exists.

The new interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 9   To edit an existing entry in the Catalyst 6500 series switch blocking device interfaces list, select it, and click **Edit**.

The Edit Cat 6K Blocking Device Interface dialog box appears.

Step 10   Edit the VLAN ID.

Step 11   Edit the Pre-Block VACL name.

Step 12   Edit the Post-Block VACL name.

Tip   To discard your changes and close the Edit Cat 6K Blocking Device Interface dialog box, click **Cancel**.

Step 13   Click **OK**.

The edited Catalyst 6500 series switch blocking device interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 14   To delete a Catalyst 6500 series switch blocking device interface from the list, select it, and click **Delete**.

The Catalyst 6500 series switch blocking device interface no longer appears in the list in the Cat 6K Blocking Device Interfaces pane.

Tip   To discard your changes, click **Reset**.

Step 15   Click **Apply** to apply your changes and save the revised configuration.

Configuring the Master Blocking Sensor

This section describes how to configure the sensor to be a master blocking sensor, and contains the following topics:

Note   A master blocking sensor can also operate as a master rate limiting sensor.

- Overview
- Supported User Role, page 8-32
- Field Definitions, page 8-32
- Configuring the Master Blocking Sensor, page 8-34

Overview

You specify the master blocking sensor that is used to control the blocking devices in the Master Blocking Sensor pane.

Multiple sensors (blocking forwarding sensors) can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The master 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. The ARC on a master blocking sensor controls blocking on devices at the request of the ARCs running on other sensors.

Caution   Two sensors cannot control blocking or rate limiting on the same device. If this situation is needed, configure one sensor as the master blocking sensor to manage the devices and the other sensors can forward their requests to the master blocking sensor.

Note   When you add a master 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 master blocking sensor.

Master blocking sensors can also forward rate limits.

On the blocking forwarding sensor, identify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its access list.

If the master 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 master blocking sensor remote host. Sensors by default have TLS enabled, but you can change this option.

> **Note** Typically the master 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.

Even if you have no devices configured for blocking or rate limiting, a sensor that is configured for blocking or rate limiting can forward blocking and rate limiting requests to a master blocking sensor. 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 master blocking sensor, which then performs the block or rate limit.

> **Caution** Only one sensor should control all blocking interfaces on a device.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the master blocking sensor.

Field Definitions

This section lists the field definitions for the master blocking sensor, and contains the following topics:

- Master Blocking Sensor Pane, page 8-32
- Add and Edit Master Blocking Sensor Dialog Boxes, page 8-33

Master Blocking Sensor Pane

The following fields and buttons are found in the Master Blocking Sensor pane.

Field Descriptions:

- IP Address—IP address of the master blocking sensor.
- Port—Port on which to connect to the master blocking sensor.

  The default is 443.

- Username—Username used to log in to the master blocking sensor.

  The username follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.

- TLS Used—Whether or not TLS is being used.

Button Functions:

- Add—Opens the Add Master Blocking Sensor dialog box. From this dialog box, you can add an master blocking sensor.

- Edit—Opens the Edit Master Blocking Sensor box. From this dialog box, you can change the values associated with this master blocking sensor.

- Delete—Removes this master blocking sensor from the list of master blocking sensors.

- Apply—Applies your changes and saves the revised configuration.

- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Master Blocking Sensor Dialog Boxes

The following fields and buttons are found in the Add and Edit Master Blocking Sensor dialog boxes.

Field Descriptions:

- IP Address—IP address of the master blocking sensor.

  You receive a warning if the IP address already exists.

- Port—(Optional) Port on which to connect on the master blocking sensor.

  The default is 443.

- Username—Username used to log in to the master blocking sensor.

  The username follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.

- Change the password—Whether or not to change the password.

- New Password—Login password used to log in to the master blocking sensor.

- Confirm Password—Confirm the login password.

- Use TLS—Whether or not to use TLS.

Button Functions:

- OK—Accepts your changes and closes the dialog box.

- Cancel—Discards your changes and closes the dialog box.

- Help—Displays the help topic for this feature.

Configuring the Master Blocking Sensor

To configure the master blocking sensor, follow these steps:

Step 1   Log in to IDM using an account with administrator or operator privileges.

Step 2   Choose **Configuration > Blocking > Master Blocking Sensor**.

The Master Blocking Sensor pane appears.

Step 3   Click **Add** to add an master blocking sensor.

The Add Master Blocking Sensor dialog box appears.

Step 4   Enter the IP address of the master blocking sensor in the IP Address field.

Step 5   (Optional) Enter the port number in the Port field.

The default is 443.

Step 6   Enter the username in the Username field.

Step 7   Enter the password for the user in the Password field.

Step 8   Retype the password in the Confirm New Password field.

Step 9   Check the TLS check box.

> **Tip**   To discard your changes and close the Add Master Blocking Sensor dialog box, click **Cancel**.

Step 10   Click **OK**.

You receive an error message if the IP address has already been added.

The new master blocking sensor appears in the list in the Master Blocking Sensor pane.

Step 11   If you selected TLS, configure the ARC of the blocking forwarding sensor to accept the TLS/SSL X.509 certificate of the master blocking sensor remote host:

> **Note**   You can also configure the blocking forwarding sensor to accept the X.509 certificate by choosing Configuration > Certificates > Trusted Hosts > Add Trusted Host. For the procedure, see Adding Trusted Hosts, page 2-15.

a.   Log in to the CLI of the blocking forwarding sensor using an account with administrator privileges.

b.   Enter global configuration mode:

```
sensor# configure terminal
```

c.   Add the trusted host:

```
sensor(config)# tls trusted-host ip-address master_blocking_sensor_ip_address
```

You are prompted to confirm adding the trusted host:

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

d.   Enter **yes** to add the host.

e.   Exit global configuration mode and the CLI:

```
sensor(config)# exit
sensor# exit
```

> **Note**   You are prompted to accept the certificate based on the certificate's fingerprint. Sensors provide only self-signed certificates (instead of certificates signed by a recognized certificate authority). You can verify the master blocking sensor host sensor's certificate by logging in to the host sensor and entering the **show tls fingerprint** command to see that the host certificate's fingerprints match.

Step 12   To edit an existing entry in the master blocking sensor list, select it, and click **Edit**.

The Edit Master Blocking Sensor dialog box appears.

Step 13   (Optional) Edit the port.

Step 14   Edit the username.

Step 15   Check the Change the password check box if you want to change the password for this user.

    a.   Enter the new password in the New Password field.

    b.   Confirm the new password in the Confirm New Password field.

Step 16   Check or uncheck the TLS check box.

> **Tip**   To discard your changes and close the Edit Master Blocking Sensor dialog box, click **Cancel**.

Step 17   Click **OK**.

The edited master blocking sensor appears in the list in the Master Blocking Sensor pane.

Step 18   To delete a master blocking sensor from the list, select it, and click **Delete**.

The master blocking sensor no longer appears in the list in the Master Blocking Sensor pane.

> **Tip**   To discard your changes, click **Reset**.

Step 19   Click **Apply** to apply your changes and save the revised configuration.

Managing Active Host Blocks

This section describes how to manage active host blocks, and contains the following topics:

- Overview, page 8-36
- Supported User Role, page 8-36
- Field Definitions, page 8-36
- Configuring and Managing Active Host Blocks, page 8-37

Overview

Use the Active Host Blocks pane to configure and manage blocking of hosts.

An active host block denies traffic from a specific host permanently (until you remove the block) or for a specified amount of time. You can base the block on a connection by specifying the destination IP address and the destination protocol and port.

An active host block is defined by its source IP address. If you add a block with the same source IP address as an existing block, the new block overwrites the old block.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the host block remains in effect until the sensor is rebooted or the block is deleted.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure active host blocks.

Field Definitions

This section lists the field definitions for active host blocks, and contains the following topics:

- Active Host Blocks Pane, page 8-36
- Add Active Host Block Dialog Box, page 8-37

Active Host Blocks Pane

The following fields and buttons are found in the Active Host Blocks pane.

Field Descriptions:

- Source IP—Source IP address for the block.
- Destination IP—Destination IP address for the block.
- Destination Port—Destination port for the block.
- Protocol—Type of protocol (TCP, UDP, or ANY).
  The default is ANY.
- Minutes Remaining—Time remaining for the blocks in minutes.
- Timeout (minutes)—Original timeout value for the block in minutes.
  A valid value is between 1 to 70560 minutes (49 days).
- VLAN— Indicates the VLAN that carried the data that fired the signature.

⚠ **Caution** Even though the VLAN ID is included in the block request, it is not passed to the firewall. Sensors cannot block on FWSM 2.1 or greater when logged in to the admin context.

- Connection Block Enabled—Whether or not to block the connection for the host.

Button Functions:

- Add—Opens the Add Active Host Block dialog box. From this dialog box, you can add a manual block for a host.
- Delete—Removes this manual block from the list of active host blocks.
- Refresh—Refreshes the contents of the table.

Add Active Host Block Dialog Box

The following fields and buttons are found in the Add Active Host Block dialog box.

Field Descriptions:

- Source IP—Source IP address for the block.
- Enable connection blocking—Whether or not to block the connection for the host.
- Connection Blocking—Lets you configure parameters for connection blocking:
  - Destination IP—Destination IP address for the block.
  - Destination Port—(Optional) Destination port for the block.
  - Protocol—(Optional) Type of protocol (TCP, UDP, or ANY).
    The default is ANY.
- VLAN—(Optional) Indicates the VLAN that carried the data that fired the signature.

⚠ **Caution** Even though the VLAN ID is included in the block request, it is not passed to the firewall. Sensors cannot block on FWSM 2.1 or later when logged in to the admin context.

- Enable Timeout—Lets you set a timeout value for the block in minutes.
- Timeout—Number of minutes for the block to last.
  A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Active Host Blocks

To configure and manage active host blocks, follow these steps:

Step 1   Log in to IDM using an account with administrator or operator privileges.

Step 2   Choose **Monitoring > Active Host Blocks**.

The Active Host Blocks pane appears.

Step 3   Click **Add** to add an active host block.

The Add Active Host Block dialog box appears.

Step 4   Enter the source IP address of the host you want blocked.

Step 5   Check the Enable Connection Blocking check box if you want the block to be connection-based.

✎

Note   A connection block blocks traffic from a given source IP address to a given destination IP address and destination port.

   a.   Enter the destination IP address in the Destination IP field.

   b.   (Optional) Enter the destination port in the Destination Port field.

   c.   Choose the protocol from the Protocol drop-down list.

Step 6   (Optional) Enter the VLAN for the connection block in the VLAN field.

Step 7   Check the Enable Timeout check box if you want to configure the block for a specified amount of time.

Step 8   Enter the amount of time in minutes in the Timeout field.

🔎

Tip   To discard your changes and close the Add Active Host Block dialog box, click **Cancel**.

Step 9   Check the No Timeout check box if you do not want to configure the block for a specified amount of time.

Step 10   Click **Apply**.

You receive an error message if a block is configured for that IP address.

The new active host block appears in the list in the Active Host Blocks pane.

Step 11   Click **Refresh** to refresh the contents of the active host blocks list.

Step 12   To delete a block, choose an active host block in the list, and click **Delete**.

The Delete Active Host Block dialog box asks if you are sure you want to delete this block.

🔎

Tip   To discard your changes and close the Delete Active Host Block dialog box, click **Cancel**.

Step 13   Click **Yes** to delete the block.

Managing Network Blocks

This section describes how to manage network blocks, and contains the following topics:

Overview

Use the Network Blocks pane to configure and managing blocking of networks.

A network block denies traffic from a specific network permanently (until you remove the block) or for a specified amount of time.

A network block is defined by its source IP address and netmask. The netmask defines the blocked subnet. A host subnet mask is accepted also.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the block remains in effect until the sensor is rebooted or the block is deleted.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure network blocks.

Field Definitions

This section lists the field definitions for network blocks, and contains the following topics:

Network Blocks Pane

The following fields and buttons are found in the Network Blocks pane.

Field Descriptions:

- IP Address—IP address for the block.
- Mask—Network mask for the block.
- Minutes Remaining—Time remaining for the blocks in minutes.

- Timeout (minutes)—Original timeout value for the block in minutes.

  A valid value is between 1 and 70560 minutes (49 days).

Button Functions:

- Add—Opens the Add Network Block dialog box. From this dialog box, you can add a block for a network.

- Delete—Removes this network block from the list of blocks.

- Refresh—Refreshes the contents of the table.

Add Network Block Dialog Box

The following fields and buttons are found in the Add Network Block dialog box.

Field Descriptions:

- Source IP—IP address for the block.

- Netmask—Network mask for the block.

- Enable Timeout—Indicates a timeout value for the block in minutes.

- Timeout—Indicates the duration of the block in minutes.

  A valid value is between 1 and 70560 minutes (49 days).

- No Timeout—Lets you choose to have no timeout for the block.

Button Functions:

- Apply—Sends this block to the sensor immediately.

- Cancel—Discards your changes and closes the dialog box.

- Help—Displays the help topic for this feature.

Configuring and Managing Network Blocks

To configure and manage network blocks, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Features > IPS >Network Blocks**.

The Network Blocks pane appears.

Step 3 Click **Add** to add a network block.

The Add Network Block dialog box appears.

Step 4 Enter the source IP address of the network you want blocked.

Step 5 Choose the netmask from the Netmask drop-down list.

Step 6 Check the Enable Timeout check box if you want to configure the block for a specified amount of time.

Step 7 Enter the amount of time in minutes in the Timeout field.

Tip To discard your changes and close the Add Network Block dialog box, click **Cancel**.

Step 8   Click **Apply**.

You receive an error message if a block has already been added.

The new network block appears in the list in the Network Blocks pane.

Step 9   Click **Refresh** to refresh the contents of the network blocks list.

Step 10   Choose a network block in the list and click **Delete** to delete that block.

The Delete Network Block dialog box asks if you are sure you want to delete this block.

Step 11   Click **Yes** to delete the block.