



CHAPTER 12

Configuring Attack Response Controller for Blocking and Rate Limiting



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**.

This chapter describes how to configure blocking on your sensor. It contains the following sections:

- [ARC Components, page 12-1](#)
- [Configuring Blocking Properties, page 12-7](#)
- [Configuring Device Login Profiles, page 12-11](#)
- [Configuring Blocking Devices, page 12-14](#)
- [Configuring Router Blocking Device Interfaces, page 12-17](#)
- [Configuring Cat 6K Blocking Device Interfaces, page 12-21](#)
- [Configuring the Master Blocking Sensor, page 12-24](#)

ARC Components

This section describes the various components of ARC, and contains the following topics:

- [Understanding Blocking, page 12-1](#)
- [Understanding Rate Limiting, page 12-4](#)
- [Understanding Service Policies for Rate Limiting, page 12-5](#)
- [Before Configuring ARC, page 12-5](#)
- [Supported Devices, page 12-5](#)

Understanding Blocking

ARC 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 master blocking sensors. ARC monitors the time for the block and removes the block after the time has expired.

**Caution**

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

**Note**

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 may not apply blocks in a timely manner or may not be able to apply blocks at all.

For security appliances configured in multi-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 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.

- 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.

**Note**

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

**Caution**

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.

For automatic blocks, you must check the Request Block Host or Request Block Connection check boxes 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. When ARC receives the block request from SensorApp, it updates the device configurations to block the host or connection.

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 security appliances 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.

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 the security appliances 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.

**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**.

**Tip**

To see the status of ARC, in IDM choose **Monitoring > Sensor Monitoring > Support Information > Statistics**.

**Note**

Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

For More Information

- For the procedure to add Request Block Host or Request Block Connection event actions to a signatures, see [Assigning Actions to Signatures, page 7-17](#).
- For the procedure for configuring overrides that add the Request Block Host or Request Block Connection event actions to alerts of specific risk rating, see [Adding, Editing, Deleting, Enabling, and Disabling Event Action Overrides, page 9-14](#).
- For more information on Pre- and Post-Block ACLs, see [How the Sensor Manages Devices, page 12-18](#).

Understanding Rate Limiting

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. Master blocking sensors can also forward rate limit requests to blocking forwarding sensors.



Tip

To see the status of ARC, in IDM choose **Monitoring > Sensor Monitoring > Support Information > Statistics**.

To add a rate limit, you specify the following:

- Source address and/or destination address for any rate limit
- Source port and/or destination port for rate limits with TCP or UDP protocol

You can also tune rate limiting signatures. You must also set the action to Request Rate Limit and set the percentage for these signatures.



Note

Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

Table 12-1 lists the supported rate limiting signatures and parameters.

Table 12-1 Rate Limiting 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 |

For More Information

- For the procedure for configuring rate limiting on a router, see [Configuring the Router Blocking and Rate Limiting Device Interfaces, page 12-20](#).
- For the procedure for configuring a sensor to be a master blocking sensor, see [Configuring the Master Blocking Sensor, page 12-26](#).

Understanding Service Policies for Rate Limiting

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.

Before Configuring ARC



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 security appliances 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.

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.
- 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



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.

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

- 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

**Caution**

ARC cannot perform rate limits on 7500 routers with VIP. ARC reports the error but cannot rate limit.

Configuring Blocking Properties

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

- [Blocking Properties Pane, page 12-7](#)
- [Understanding Blocking Properties, page 12-7](#)
- [Blocking Properties Pane Field Definitions, page 12-8](#)
- [Configuring Blocking Properties, page 12-9](#)
- [Add and Edit Never Block Address Dialog Boxes Field Definitions, page 12-10](#)
- [Adding, Editing, and Deleting IP Addresses Never to be Blocked, page 12-11](#)

Blocking Properties Pane

**Note**

You must be administrator or operator to add, edit, or delete IP addresses never to be blocked.

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

Understanding Blocking Properties

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.

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.

Blocking Properties Pane Field Definitions

The following fields are found in the Blocking Properties pane:

- 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.

**Note**

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 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.



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 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: 250 interfaces per device, 250 security appliances, 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 to or less than 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.

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

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 > Sensor Management > Blocking > Blocking Properties**.

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.

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 select 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 In the Maximum Block Entries field, enter how many blocks are to be maintained simultaneously (1 to 65535).



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 to or less than the maximum blocking entries. If you configure more rate limit entries than block entries, you receive an error.



Tip

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.




Add and Edit Never Block Address Dialog Boxes Field Definitions

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

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

Adding, Editing, and Deleting IP Addresses Never to be Blocked

To add, edit, and delete an IP address never to be blocked, follow these steps:

-
- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Sensor Management > Blocking > Blocking Properties**, and click **Add** to add a host or network to the list of addresses never to be blocked.
- Step 3** In the IP Address field, enter the IP address of the host or network.
- Step 4** In the Network Mask field, enter the network mask of the host or network, or select a network mask from the list.
-  **Tip** To discard your changes and close the Add Never Block Address dialog box, click **Cancel**.
-
- Step 5** 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 6** To edit an existing entry in the never block addresses list, select it, and click **Edit**.
- Step 7** In the IP Address field, edit the IP address of the host or network.
- Step 8** In the Network Mask field, edit the network mask of the host or network.
-  **Tip** To discard your changes and close the Edit Never Block Address dialog box, click **Cancel**.
-
- Step 9** Click **OK**. The edited host or network appears in the Never Block Addresses list in the Allowed Hosts pane.
- Step 10** 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 11** Click **Apply** to apply your changes and save the revised configuration.
-

Configuring Device Login Profiles

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

- [Device Login Profiles Pane, page 12-12](#)
- [Device Login Profiles Pane Field Definitions, page 12-12](#)
- [Add and Edit Device Login Profile Dialog Boxes Field Definitions, page 12-12](#)
- [Configuring Device Login Profiles, page 12-13](#)

Device Login Profiles Pane


Note

You must be administrator or operator to add or edit device login profiles.

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.

Device Login Profiles Pane Field Definitions

The following fields are found on the Device Login Profiles pane:

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


Note

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

- Enable Password—Enable password used on the blocking device.


Note

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

Add and Edit Device Login Profile Dialog Boxes Field Definitions

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

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


Note

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

- Enable Password—Enable password used on the blocking device.


Note

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

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 > Sensor Management > Blocking > Device Login Profiles**, and click **Add** to add a profile.
 - Step 3** In the Profile Name field, enter the profile name.
 - Step 4** (Optional) In the Username field, enter the username used to log in to the blocking device.
 - Step 5** (Optional) In the New Password field, enter the login password.
 - Step 6** (Optional) In the Confirm New Password field, enter the login password again to confirm it.
 - Step 7** (Optional) In the New Password field, enter the enable password.
 - Step 8** (Optional) In the Confirm New Password field, enter the enable password again to confirm it.



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

- Step 9** 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 10** To edit an existing entry in the device login profile list, select it, and click **Edit**.
- Step 11** In the Username field, edit the username used to log in to the blocking device.
- Step 12** Check the **Change the login password check box** to change the login password.
- Step 13** In the New Password field, enter the new login password.
- Step 14** In the Confirm New Password field, enter the new login password to confirm it.
- Step 15** Check the **Change the enable password** check box to change the enable password.
- Step 16** In the New Password field, enter the new enable password.
- Step 17** In the Confirm New Password field, enter the enable password to confirm it.



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

- Step 18** Click **OK**. The edited device login profile appears in the list in the Device Login Profile pane.
- Step 19** 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 20** Click **Apply** to apply your changes and save the revised configuration.
-

Configuring Blocking Devices

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

- [Blocking Device Pane, page 12-14](#)
- [Blocking Devices Pane Field Definitions, page 12-14](#)
- [Add and Edit Blocking Device Dialog Boxes Field Definitions, page 12-15](#)
- [Adding, Editing, and Deleting Blocking and Rate Limiting Devices, page 12-15](#)

Blocking Device Pane

**Note**

You must be administrator or operator to configure blocking devices.

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 security appliance. The router, switch, or security appliance 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 sensors cannot manage a single device. For that you must use a master blocking sensor.

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.

Blocking Devices Pane Field Definitions

The following fields are found in the Blocking Devices pane:

- IP Address—IP address of the blocking device.
- Sensor's NAT Address—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.

Add and Edit Blocking Device Dialog Boxes Field Definitions

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

- IP Address—IP address of the blocking device.
- Sensor's NAT Address—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.

Adding, Editing, and Deleting Blocking and Rate Limiting Devices

To add, edit, or delete 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**, and click **Add** to add a blocking device. You receive an error message if you have not configured the device login profile.
- Step 3** In the IP Address field, enter the IP address of the blocking device.
- Step 4** (Optional) In the Sensor's NAT Address field, enter the NAT address of the sensor.
- Step 5** From the Device Login Profile drop-down list, choose the device login profile.
- Step 6** From the Device Type drop-down list, choose the device type.
- Step 7** In the Response Capabilities field, check the **Block** and/or **Rate Limit** check boxes to specify whether the device will perform blocking, rate limiting, or both.



Note You must select 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.

- Step 8** From the Communication drop-down list, choose the communication type. If you choose SSH 3DES or SSH DES, go to Step 11.



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

- Step 9** 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 10** If you choose SSH 3DES or SSH DES, you must add the device to the known hosts list:



Note If you select 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 choose **Configuration > Sensor Management > SSH > Known Host Keys > Add Known Host Key** to add the device to the known hosts list.

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

Step 12 Edit the NAT address of the sensor if desired.

Step 13 Change the device login profile if desired.

Step 14 Change the device type if desired.

Step 15 Change whether the device will perform blocking or rate limiting if desired.

Step 16 Change the communication type if desired.



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

Step 17 Click **OK**. The edited blocking device appears in the list in the Blocking Device pane.

Step 18 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 19 Click **Apply** to apply your changes and save the revised configuration.

Configuring Router Blocking Device Interfaces

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

- [Router Blocking Device Interfaces Pane, page 12-17](#)
- [Understanding Router Blocking Device Interfaces, page 12-17](#)
- [How the Sensor Manages Devices, page 12-18](#)
- [Router Blocking Device Interfaces Pane Field Definitions, page 12-19](#)
- [Add and Edit Router Blocking Device Interface Dialog Boxes Field Definitions, page 12-19](#)
- [Configuring the Router Blocking and Rate Limiting Device Interfaces, page 12-20](#)

Router Blocking Device Interfaces Pane

**Note**

You must be administrator or operator to configure the router blocking device interfaces.

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.

Understanding Router Blocking Device Interfaces

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.

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 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.

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 configuration of the device.
3. Reenable blocking on the sensor.

When blocking is reenabled, the sensor reads the new device configuration.

**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 More Information

- For the procedure for enabling blocking, see [Configuring Blocking Properties, page 12-9](#).
- For the procedure for configuring the sensor to be a master blocking sensor, see [Configuring the Master Blocking Sensor, page 12-26](#).

Router Blocking Device Interfaces Pane Field Definitions

The following fields are found in the Router Blocking Device Interfaces pane:

- 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.

Add and Edit Router Blocking Device Interface Dialog Boxes Field Definitions

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

- 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.

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 > Sensor Management > Blocking > Router Blocking Device Interfaces**, and click **Add** to add a router blocking or rate limiting device interface.
- Step 3** In the Router Blocking Device drop-down list, choose the IP address of the router blocking or rate limiting device.
- Step 4** In the Blocking Interface field, enter the blocking or rate limiting interface name.
- Step 5** From the Direction drop-down list, choose the direction (in or out).
- Step 6** (Optional) In the Pre-Block ACL field, enter the name of the Pre-Block ACL.



Note This step does not apply to rate limiting devices.

- Step 7** (Optional) In the Post-Block ACL field, enter the name of the Post-Block ACL.



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 8** 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 9** To edit an existing entry in the router blocking device interfaces list, select it, and click **Edit**.
- Step 10** Edit the blocking or rate limiting interface name, if needed.
- Step 11** Change the direction, if needed.
- Step 12** Edit the Pre-Block ACL name, if needed.
- Step 13** Edit the Post-Block ACL name, if needed.



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

- Step 14** Click **OK**. The edited router blocking or rate limiting device interface appears in the list in the Router Blocking Device Interfaces pane.
- Step 15** 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 16** 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 interfaces, and contains the following topics:

- [Cat 6K Blocking Device Interfaces Pane, page 12-21](#)
- [Understanding Cat 6K Blocking Device Interfaces, page 12-21](#)
- [Cat 6K Blocking Device Interfaces Pane Field Definitions, page 12-22](#)
- [Configuring Cat 6K Blocking Device Interfaces, page 12-23](#)

Cat 6K Blocking Device Interfaces Pane



Note You must be administrator or operator to configure the Catalyst 6500 series switches blocking device interfaces.

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

Understanding Cat 6K Blocking Device Interfaces

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 VACL, the sensor inserts **permit ip any any** at the end of the new VACL.

**Note**

The IDSM2 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 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.

For More Information

For blocking using router ACLs, see [Configuring the Router Blocking and Rate Limiting Device Interfaces](#), page 12-20.

Cat 6K Blocking Device Interfaces Pane Field Definitions

The following fields are found in the Cat 6K Blocking Device Interfaces pane:

- 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.

Add and Edit Cat 6K Blocking Device Interface Dialog Boxes Field Definitions

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

- 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.

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 > Sensor Management > Blocking > Cat 6K Blocking Device Interfaces**, and click **Add** to add a Catalyst 6500 series switch blocking device interface.
 - Step 3** From the Cat 6K Blocking Device drop-down list, choose the IP address of the Catalyst 6500 series switch.
 - Step 4** In the VLAN ID field, enter the VLAN ID.
 - Step 5** (Optional) In the Pre-Block VACL field, enter the name of the Pre-Block VACL.
 - Step 6** (Optional) In the Post-Block VACL field, enter the name of the Post-Block VACL.

**Tip**

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

- Step 7** Click **OK**. You receive an error message if the IP address/VLAN combination already exists. The new interface appears in the list in the Cat 6K Blocking Device Interfaces pane.
- Step 8** To edit an existing entry in the Catalyst 6500 series switch blocking device interfaces list, select it, and click **Edit**.
- Step 9** Edit the VLAN ID, if needed.
- Step 10** Edit the Pre-Block VACL name, if needed.
- Step 11** Edit the Post-Block VACL name, if needed.

**Tip**

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

Step 12 Click **OK**. The edited Catalyst 6500 series switch blocking device interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 13 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 14 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Master Blocking Sensor

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

- [Master Blocking Sensor Pane, page 12-24](#)
- [Understanding the Master Blocking Sensor, page 12-24](#)
- [Master Blocking Sensor Pane Field Definitions, page 12-25](#)
- [Add and Edit Master Blocking Sensor Dialog Boxes Field Definitions, page 12-25](#)
- [Configuring the Master Blocking Sensor, page 12-26](#)

Master Blocking Sensor Pane



Note You must be administrator or operator to configure the master blocking sensor.

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

Understanding the Master Blocking Sensor

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.

Master Blocking Sensor Pane Field Definitions

The following fields are found in the Master Blocking Sensor pane:

- 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.

Add and Edit Master Blocking Sensor Dialog Boxes Field Definitions

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

- 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—Confirms the login password.
- Use TLS—Whether or not to use TLS.

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 > Sensor Management > Blocking > Master Blocking Sensor**, and click **Add** to add an master blocking sensor.
- Step 3** In the IP Address field, enter the IP address of the master blocking sensor.
- Step 4** (Optional) In the Port field, enter the port number. The default is 443.
- Step 5** In the Username field, enter the username.
- Step 6** In the New Password field, enter the password for the user.
- Step 7** In the Confirm New Password field, enter the password to confirm it.
- Step 8** Check the **TLS** check box.



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

- Step 9** 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 10** 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 choose **Configuration > Sensor Management > Certificates > Trusted Hosts > Add Trusted Host** to configure the blocking forwarding sensor to accept the X.509 certificate.

- Log in to the CLI of the blocking forwarding sensor using an account with administrator privileges.
- Enter global configuration mode:

```
sensor# configure terminal
```

- 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]:
```

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

Step 11 To edit an existing entry in the master blocking sensor list, select it, and click **Edit**.

Step 12 (Optional) Edit the port.

Step 13 Edit the username, if needed.

Step 14 To change the password for this user, check the **Change the password** check box.

a. In the New Password field, enter the new password.

b. In the Confirm New Password field, enter the new password to confirm it.

Step 15 Check or uncheck the **TLS** check box, if needed.



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

Step 16 Click **OK**. The edited master blocking sensor appears in the list in the Master Blocking Sensor pane.

Step 17 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 18 Click **Apply** to apply your changes and save the revised configuration.

