Shunning/Blocking on IPS for ASA/PIX/Cisco IOS Router Configuration Example

Document ID: 111001

Contents

Introduction

This document describes how to configure shunning on a PIX/ASA/Cisco IOS Router with the help of Cisco IPS. ARC, the blocking application on the sensor, starts and stops blocks on routers, Cisco 5000 RSM and Catalyst 6500 series switches, PIX Firewalls, FWSM, and ASA. ARC issues a block or shun to the managed device for the malicious IP address. ARC sends the same block to all devices that the sensor manages. If a master blocking sensor is configured, the block is forwarded to and issued from this device. ARC monitors the time for the block and removes the block after the time has expired.

When you use IPS 5.1, special care must be taken when shunning to firewalls in multiple context mode as no VLAN information is sent with the shun request.

Note: Blocking is not supported in the admin context of a multiple context FWSM.

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 by security appliances. Security appliances only support host blocks with optional port and protocol 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.

For automatic blocks, you must choose Request Block Host or Request Block Connection as the event action for particular signatures, 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. Refer to Assigning Actions to Signatures, page 5−22 for more information on the procedure to add the Request Block Host or Request Block Connection event actions to the signature. Refer to Configuring Event Action Overrides, page 7−15 for more information on the procedure for the configuration of overrides that add the Request Block Host or Request Block Connection event actions to alarms of specific risk ratings.

On Cisco routers and Catalyst 6500 series switches, ARC creates blocks by applying ACLs or VACLs. ACLs and VACLs apply filters to interfaces, which includes direction, and VLANs, respectively in order to permit or deny traffic. . The PIX Firewall, FWSM, and ASA do not use ACLs or VACLs. The built−in **shun** and **no shun** command are used.

This information is required for the configuration of ARC:

- Login user ID, if the device is configured with AAA
- Login password
- Enable password, which is 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 is created. This does not apply to a PIX Firewall, FWSM, or ASA because they do not use ACLs or VACLs to block.
- Whether you use 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

Prerequisites

Requirements

Before you configure ARC for blocking or rate limiting, you must complete these tasks :

- 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).

Components Used

The information in this document is based on the Cisco Intrusion Prevention System 5.1 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Note: By default, ARC is configured for a limit of 250 block entries. Refer to Support Devices for more information on the list of blocking devices supported by ARC.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Use the Blocking Properties pane in order 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 in order to identify hosts and networks that should never be blocked. It is possible for the traffic of a trusted device to fire a signature. If this signature is configured to block the attacker, legitimate network traffic can be affected. The IP address of the device can be listed in the Never Block list in order to prevent this scenario.

A netmask specified in a Never Block entry is applied to the Never Block address. If no netmask is specified, a default /32 mask is applied.

Note: By default, the sensor is not permitted to issue a block for its own IP address as this interferes with the communication between the sensor and the blocking device. But, this option is configurable by the user.

Once ARC is configured to manage a blocking device, the blocking device's shuns and ACLs/VACLs that are used for blocking should not be altered manually. This can cause a disruption of the ARC service and can result in future blocks not being issued.

Note: By default, only blocking is supported on Cisco IOS devices. You can override the blocking default if you choose rate limiting or blocking plus rate limiting.

In order to issue or alter blocks, the IPS user must have the Administrator or Operator role.

Configure the Sensor to Manage Cisco Routers

This section describes how to configure the sensor to manage Cisco routers. It contains these topics:

- Configure User Profiles
- Routers and ACLs
- Configure Cisco Routers Using CLI

Configure User Profiles

The sensor manages the other devices with the **user−profiles** *profile_name* command in order to set up user profiles. The user profiles contain the userid, password, and enable password information. For example, routers that all share the same passwords and usernames can be under one user profile.

Note: You **must** create a user profile before you configure the blocking device.

Complete these steps in order to set up user profiles:

1. Log in to the CLI with an account that has Administrator privileges.
2. Enter network access mode.

```
sensor#configure terminal
```

```
sensor(config)#service network-access
sensor(config-net)#
```

3. Create the user profile name.

```
sensor(config-net)#user-profiles PROFILE1
```

4. Type the username for that user profile.

```
sensor(config-net-use)#username username
```

5. Specify the password for the user.

```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```

6. Specify the enable password for the user.

```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

7. Verify the settings.

```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   ----------------------------------------------
sensor(config-net-use)#
```

8. Exit network access submode.

```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```

9. Press **Enter** in order to apply the changes or enter no to discard them.

Routers and ACLs

When ARC is configured with a blocking device that uses ACLs, the ACLs are composed in this way:

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 pre−configured ACL and copies these lines to the start of the block ACL.
3. Any active blocks
4. Either: Post−Block ACL/ permit ip any any

   − **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)

Note: The ACLs that ARC makes should never be modified by you or any other system. These ACLs are temporary and new ACLs are constantly 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, complete these steps:

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.

Note: A single sensor can manage multiple devices, but multiple sensors cannot manage a single device. In the case that blocks issued from multiple sensors are meant for a single blocking device, a master blocking sensor must be incorporated into the design. A master blocking sensor receives blocking requests from multiple sensors and issues all of the blocking requests to the blocking device.

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 how to create ACLs.

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

ACLs are evaluated top−down and the first−match action is taken. The Pre−Block ACL may contain a permit which would take precedence over a deny that resulted from a block.

The Post−Block ACL is used to account for any conditions not handled by the Pre−Block ACL or blocks. If you have an existing ACL on the interface and in the direction which the blocks are issued, that ACL can be used as the 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 these 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 that are 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 block ACL is applied to an interface of the router, in a particular direction, it replaces any preexisting ACL on that interface in that direction.

Configure Cisco Routers Using CLI

Complete these steps in order to configure a sensor to manage a Cisco router to perform blocking and rate limiting:

1. Log in to the CLI with an account that has Administrator privileges.

2. Enter network access submode.

```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```

3. Specify the IP address for the router controlled by ARC.

```
sensor(config-net)#router-devices ip_address
```

4. Enter the logical device name that you created when you configured the user profile.

```
sensor(config-net-rou)#profile-name user_profile_name
```

ARC accepts anything you enter. It does not check to see if the user profile exists.

5. Specify the method used to access the sensor.

```
sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
```

If unspecified, SSH 3DES is used.

Note: If you use DES or 3DES, you must use the **ssh host-key ip_address** command in order to accept the SSH key from the device.

6. Specify the sensor NAT address.

```
sensor(config-net-rou)#nat-address nat_address
```

Note: This changes the IP address in the first line of the ACL from the address of the sensor to the NAT address. The NAT address is the sensor address, post-NAT, translated by an intermediary device, located between the sensor and blocking device.

7. Specify whether the router performs blocking, rate limiting, or both.

Note: The default is blocking. You do not have to configure response capabilities if you want the router to perform blocking only.

- Rate limiting only

```
sensor(config-net-rou)#response-capabilities rate-limit
```

- Both blocking and rate limiting

```
sensor(config-net-rou)#response-capabilities block|rate-limit
```

8. Specify the interface name and direction.

```
sensor(config-net-rou)#block-interfaces interface_name {in | out}
```

Note: The name of the interface must be an abbreviation that the router recognizes when used after the **interface** command.

9. (Optional) Add the pre-ACL name (blocking only).

```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```

10. (Optional) Add the post-ACL name (blocking only).

```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```

11. Verify the settings.

```
sensor(config-net-rou-blo)#exit

sensor(config-net-rou)#show settings
```

```
      ip-address: 10.89.127.97
      -------------------------------------------
         communication: ssh-3des default: ssh-3des
         nat-address: 19.89.149.219 default: 0.0.0.0
         profile-name: PROFILE1
         block-interfaces (min: 0, max: 100, current: 1)
         -----------------------------------------------
            interface-name: GigabitEthernet0/1
            direction: in
            ---------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ---------------------------------------------
         -----------------------------------------------
         response-capabilities: block|rate-limit default: block
      -------------------------------------------
   sensor(config-net-rou)#
```

12. Exit network access submode.

```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```

13. Press **Enter** in order to apply the changes or enter **no** to discard them.

Configure the Sensor to Manage Cisco Firewalls

Complete these steps in order to configure the sensor to manage Cisco firewalls:

1. Log in to the CLI with an account that has Administrator privileges.
2. Enter network access submode.

```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```

3. Specify the IP address for the firewall controlled by ARC.

```
sensor(config-net)#firewall-devices ip_address
```

4. Enter the user profile name that you created when you configured the user profile.

```
sensor(config-net-fir)#profile-name user_profile_name
```

   ARC accepts anything you type. It does not check to see if the logical device exists.

5. Specify the method used to access the sensor.

```
sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
```

   If unspecified, SSH 3DES is used.

   Note: If you use DES or 3DES, you must use the **ssh host-key ip_address** command in order to accept the key or ARC cannot connect to the device.

6. Specify the sensor NAT address.

```
sensor(config-net-fir)#nat-address nat_address
```

   Note: This changes the IP address in the first line of the ACL from the IP address of the sensor to the NAT address. The NAT address is the sensor address, post−NAT, translated by an intermediary device, located between the sensor and blocking device.

7. Exit network access submode.

```
sensor(config-net-fir)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```

8. Press **Enter** in order to apply the changes or enter **no** in order to discard them.

Block with SHUN in PIX/ASA

Issuing the **shun** command blocks connections from an attacking host. Packets that match the values in the command are dropped and logged until the blocking function is removed. The **shun** is applied regardless of whether a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, you narrow the shun to connections that match those parameters.

You can only have one **shun** command for each source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the security appliance configuration.

Whenever an interface is removed, all shuns that are attached to that interface are also removed.

This example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) to TCP. The connection in the security appliance connection table reads as follows:

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

In order to block connections from an attacking host, use the **shun** command in privileged EXEC mode. Apply the **shun** command with these options:

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The command deletes the connection from the security appliance connection table and also prevents packets from 10.1.1.27:555 to 10.2.2.89:666 (TCP) from going through the security appliance.

Related Information

- **Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers**
- **Configuring Attack Response Controller for Blocking and Rate Limiting using IDM 7.0**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 21, 2009 Document ID: 111001