CounterACT Router Blocking Plugin

Configuration Guide

Version 1.0

Table of Contents

About the Router Blocking Plugin

The Router Blocking Plugin allows you to utilize the Cisco IOS C2600 v. 12.3, and C7606 v. 12.2 routers to better block remote computers via an Access Control List (ACL) or via NULL routing.

When working with policy detections in CounterACT, you can use the Router Block action to automatically block hosts that match your policy rules. This action is added to the Policy, Action screen when the router plugin is activated. After activating the plugin, the Router Block icon appears in the Detections pane.

Once a host is detected and blocked by the Router, the Router icon is assigned to the detected host. You can manually release the host by right-clicking it from the Control Center and selecting Release Router Blocking. Information about hosts blocked and released by the router appears in the Detections pane and Host Details dialog box.

Requirements

- CounterACT version 5.1.0 or above.
- This plugin runs with Cisco routers running IOS version 12.x.
- The Router Plugin supports Cisco IOS C2600v 12.3 and C7606 v. 12.2 routers, and works on top of either SSH or RCMD.

To work with the Router Plugin you must also:

1. Set up the router to allow connection to the Appliance.
2. Define Access Control List (ACL) or Null Routing definitions and management commands.
3. Configure the plugin.

Working with Malicious Hosts

Auto-blocking – Router blocking will be carried out automatically on malicious hosts when you have created a policy that utilizes the Malicious Host condition and the Router action. This means you cannot block malicious hosts with the router via the Malicious Host Policy.

Malicious scan events are however initially detected according to the Probe Count parameters you defined in the Malicious Host Policy - Customized dialog box.

Manual Blocking – You can manually block a malicious host with the router from the Control Center. To do this, right-click the host and select Router Block. Release the host by right-clicking it and selecting Release Router Block.

Refer to the CounterACT online Help for more information about these features.

Working with More than One Router

An option is also available to deploy more than one router plugin per Appliance. To work this way:

- Contact your ForeScout representative to acquire additional router plugins.
- Download, install and configure the plugin as required. New plugins are named numerically, i.e. Router Blocking 2, Router Blocking 3, etc. These names appear in the Plugin Management dialog box after installation.

Installation and Configuration

This section describes how to install and configure the plugin.

To install and configure the plugin:

1. Download and save the plugin from the ForeScout website.
2. Select **Options** from the **Tools** menu at the Console.
3. Select the **Plugin** folder and then select **Install**.
4. Install the plugin from the location you saved it.
5. Select the plugin and then select **Configure**. The Configuration dialog box opens. See Configuring the Plugin for more information.

Configuration also requires that you set up your router to work with the Appliance. See Appliance and Router Connection for more information. After performing the setup and configuration you must run the plugin in order to activate it.

Appliance and Router Connection

This section describes the procedures for connecting the Appliance and the router using SSH or RCMD. The default is SSH. It is recommended to choose SSH. Under certain circumstances when RCMD is chosen, blocking may require slightly more time.

RCMD Connection

1. Log in to the router and run the following commands:

```
configure terminal
ip rcmd rcp-enable
ip rcmd rsh-enable
ip rcmd remote-host <Router username> <Appliance IP address> root
enable
write memory
```

SSH Connection

1. Log in to the router and run the following command:

   `configure terminal`

2. If the domain name is not set, run the following command:

   `ip domain-name example.com`

3. To create encryption keys, run the following command:

   `crypto key generate rsa`

4. To allow SSH access on the vty0-vty4:

   `line vty 0 4`
   `transport input all` or **`transport input ssh`**
   `write memory`

Test the Connection

1. Verify the SSH connection by logging in to the Appliance and running the following command:

   `ssh -1x <router's IP address>`

Important: *If the connection fails, the plugin will cease to work if the rsa key is changed on the router. If this happens, you need to log in to the Appliance, and remove the offending entry from /root/.ssh/known_hosts.*

Create a Privilege Level and Privilege Password

You can configure an Appliance privilege level and password in order to limit access to blocking operations only. If you do not configure the privilege level, the Appliance will have administrator permissions at the router. If this is the case, you must use the administrator password in the router Configuration dialog box and choose the default privilege level, which is 0.

To create the privilege and password:

1. Log in to the router and run the following commands in the order shown below:

   – For Cisco IOS C2600v 12.3

   `configure terminal`
   `enable password level X <password>` (X being the privilege level)
   `privilege exec level X conf terminal`

   – For Cisco C7606 v. 12.2

   `login`
   `configure terminal`

enable password level X <password> (X being the privilege level)
privilege exec level X conf terminal

2. For ACL Blocking, enter the following commands:

   – For Cisco IOS C2600v 12.3

```
privilege configure level X ip access-list extended
privilege ipenacl all level X deny
privilege ipenacl all level X permit
write memory
```

   – For Cisco C7606 v. 12.2

```
privilege configure level X ip access-list extended
privilege ipenacl level 6 deny
privilege ipenacl level 6 permit
privilege ipenacl level 6 deny ip any any fragments
privilege ipenacl level 6 deny tcp any any eq
privilege ipenacl level 6 deny tcp host
privilege ipenacl level 6 deny udp any any eq
privilege ipenacl level 6 deny udp host
write memory
```

3. For Null Blocking, enter the following commands (for both 12.3 and 12.2):

   privilege exec level X show run (X being the level)
   privilege configure level X ip route (X being the level)
   write memory

Create an Access Control List (ACL)

If you want the router to block hosts via an Access Control List (ACL), you must configure the list at the router. Each time a host is blocked, a rule is added. If you are applying port blocking, a new rule is added for each port block. An additional rule is applied for each host if you choose to block non-initial fragments. (See Configuring the Plugin for more information about this kind of blocking.) You can configure the router to handle up to 500 rules. Once the threshold is passed, the router ceases to block hosts and the Appliance handles the blocking exclusively. You must also configure the interface to which the ACL is attached. See Interface Definition for more information.

To create an access list:

1. Log in to the router and run the following commands to create the list:

   qa-cisco>enableX (X being the privilege level, if you defined one.)
   Password:
   configure terminal

   A message appears.

2. Enter the following configuration commands, one per line. End with Ctrl-Z.

   ip access-list extended <Name> (Name being the unique Access Control List name)
   permit ip any any

```
exit
write memory
```

Interface Definition

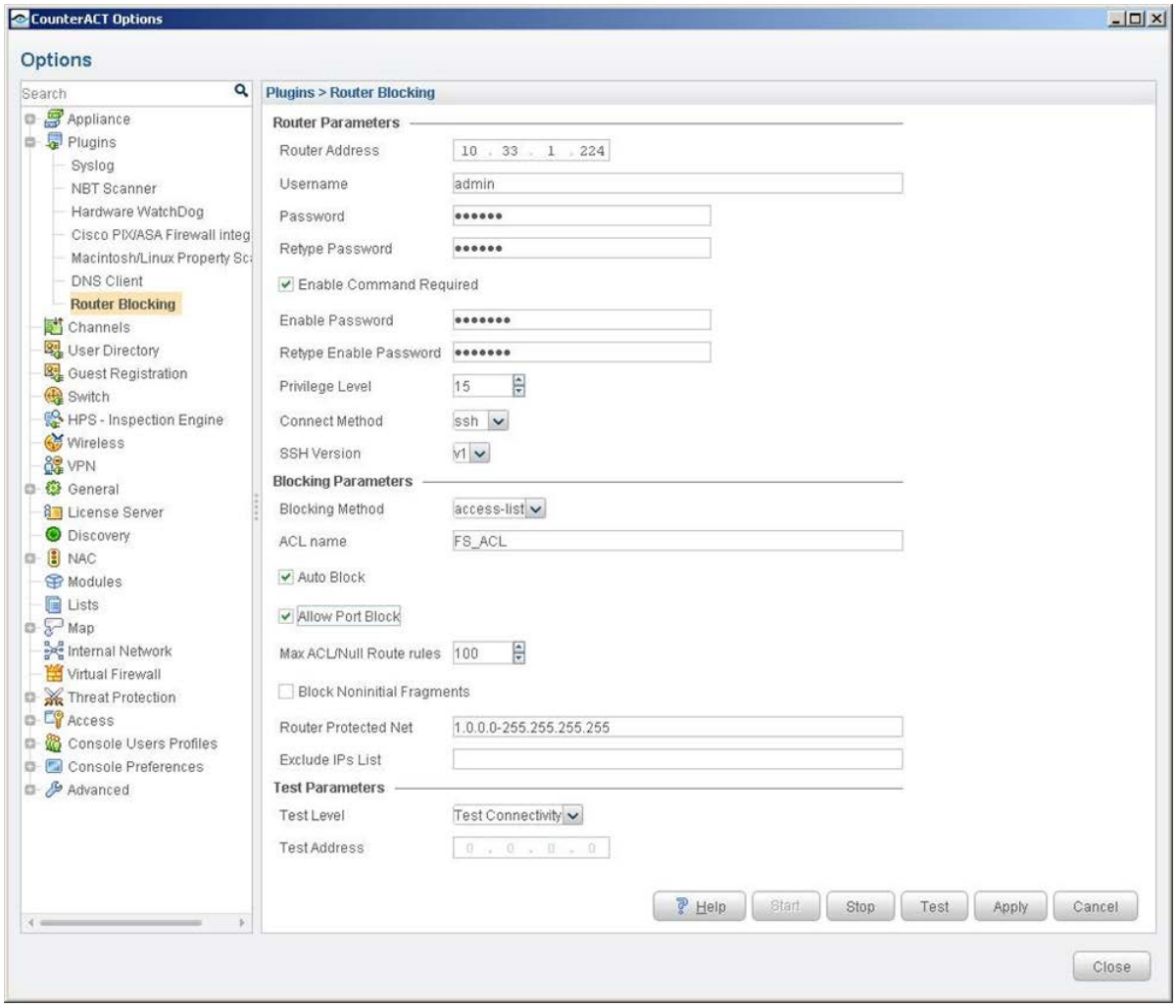
You must define instructions regarding the interface from which the router should block hosts.

1. Log in to the router and run the following commands to create the list:

   `interface fastEthernet X` (X being the interface number)
   `ip access-group <Name> Y` (Y being in or out - in is recommended; Name being the name of the ACL)
   `exit`
   `exit`
   `write memory`

Configuring the Plugin

This section describes how to configure the plugin.



Define the following information:

- Router Parameters
- Blocking Parameters
- Test Parameters

Router Parameters

Field	Description
Router Address	The IP address of the router.
Username	The username at the router.
Password	The password used to log in to the router.
Enable Command Required	Clear this checkbox to carry out blocking without providing ***Enable*** privileges to the Appliance.
Enable Password	The enable password used when defining a privilege level. See Create a Privilege Level and Privilege Password for more information.

Field	Description
Privilege Level	The privilege level defined when setting up the router.
Connect Method	The connection method. The default is ssh. You must have configured the router to connect using the selected method. See Appliance and Router Connection for more information.
SSH Version	Select an SSH version.

Blocking Parameters

Field	Description
Blocking Method	Choose between blocking using an Access List or implementing Null Routing. If you select the Access List option, you must configure the router to work with the list. See Create an Access Control List (ACL) for more information. Null Routing routes traffic to a non-existent interface. Both methods require the use of blocking rules. Specifically, each time a host is blocked a rule is added. If you are applying port blocking a new rule is added for each port block. An additional rule is applied for each host if you choose to block non-initial fragments. (See below for more information about this kind of blocking). You can configure the router to handle up to 500 rules. Once the threshold is passed, the router ceases to block hosts and the Appliance blocks exclusively. If you select the Access List option and have not configured an access list at the router, the router will not block any hosts.
ACL Name	Enter the name of the Access List you configured at the router.
Auto Block	Select the check box to instruct the router to automatically block all detected hosts. Clear the checkbox to use manual blocking. Manual blocking allows you to block and release hosts manually. If you update the configuration and move from Automatic block to Manual block, all hosts blocked by the router are released. If this option is selected and the Appliance policy is set to host block, the router will perform a host block and not a port block. When the port block policy is escalated to host block at the Appliance, the router will also perform a host block, regardless of the setting you define here.
Max ACL/Null Route rules	Define the maximum number of rules that you want the router to handle. The upper limit is 500 rules. After this threshold is passed, the router no longer blocks hosts, and the blocking is carried out by the Appliance exclusively. Port blocking and blocking non-initial fragments requires more rules per host than host blocking and only blocking initial fragments.
Block Noninitial Fragments	Select the check box to block both initial session packets and packets that follow. If you choose to block the entire session and are using the ACL blocking method, and additional rule will be added to the list
Router Protected Net	List of network ranges protected by the router. An infected computer outside this range is not subject to router blocking.
Exclude IPs List	A list of IP addresses that should be exempted from router blocking. Enter a space between each address.

Test Parameters

Field	Description
Test Level	▪ Select **Test Connectivity** to verify connection with test address and then select **Test** from the Plugin Management dialog box to run the test. ▪ Select **Test Block** to verify that the router blocks the test address and then select **Test** from the Plugin Management dialog box to run the test.
Test Address	Enter a host address for perform a blocking test or connectivity test.

Known Issues

Issues	Description
History view. Information incorrect with multiple plugin deployment.	The router blocking information displayed in the History view at your Appliance/Enterprise Manager will be incorrect if you have installed more than one Router plugin.
The right-click Router Block action is active from Control Center when router blocking is already carried out.	The right-click Router Block action is active from Console when router blocking is already carried out. This means that the option should be disabled because it was already selected, but the user can still select it. When this happens the Router icon appears with a red X, indicating that the action was already carried out. This information is also displayed in the Host Details dialog box, Network Integrity Logger.

Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2015. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

July 2015