CounterACT Cisco PIX/ASA Firewall Integration Plugin

Configuration Guide

Version 2.0.1 and Above

Table of Contents

About the Cisco PIX/ASA Firewall Integration Plugin 3
Requirements 3

Configuring the Firewall..... 3

Install and Configure the Plugin..... 4

Apply Firewall Access Lists to a Host..... 5
Naming CounterACT Object Groups 5
Sample Firewall Commands.....6
Cisco PIX/ASA Access-list Action 6

About the Cisco PIX/ASA Firewall Integration Plugin

The Cisco PIX/ASA Firewall Integration Plugin forwards host blocking requests to an external Cisco PIX or ASA firewall.

Blocking is implemented using access lists that reference a set of object groups. CounterACT maintains the object groups, adding and removing hosts from the group as needed.

Requirements

- CounterACT version 6.3.4.0 and above.
- A firewall user account unique to CounterACT. See Configuring the Firewall for privileges and access requirements for this user.

Configuring the Firewall

Enter the following commands at each firewall while in configuration mode.

Record these values, and use them to configure CounterACT communication with the firewall as described in Install and Configure the Plugin.

1. Enable SSH Access from a CounterACT Device:

   Refer to Cisco documentation for general instructions on how to enable SSH access to the firewall. You will probably need to issue the following sequence of commands:

   ```
   ca gen rsa key 1024
   ca save all
   aaa authentication ssh console LOCAL
   write mem
   ```

   To enable SSH access from a CounterACT device, select INSIDE or OUTSIDE depending on the interface to which the CounterACT device connects.

2. Define a user name (the default is **forescout**), password and restrictive privilege level (**priv_level**) (the default is 4) for the CounterACT device user:

   ```
   username <user_name> password <user_password> privilege <priv_level>
   ```

3. Define the privilege level permissions:

   ```
   enable password <priv_password> level <priv_level>
   privilege configure level <priv_level> mode enable command configure
   privilege configure level <priv_level> command object-group
   privilege show level <priv_level> command object-group
   privilege configure level <priv_level> command network-object
   privilege configure level <priv_level> command port-object
   privilege configure level <priv_level> command pdm
   ```

Install and Configure the Plugin

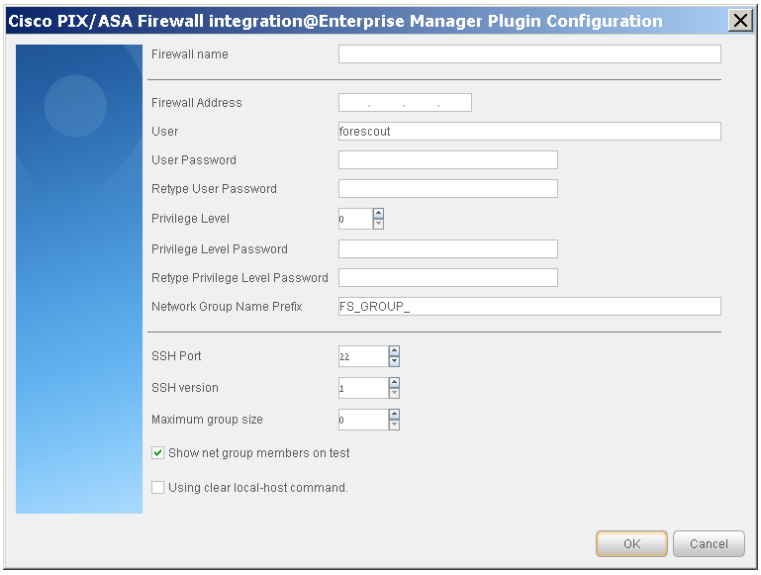
This section describes how to install and configure the Cisco PIX/ASA Firewall Integration Plugin.

To install and configure:

1. Download and save the plugin from the ForeScout website.
2. Select **Options** from the **Tools** menu at the Console.
3. Select the **Plugins** folder and then select **Install**.
4. Install the plugin from the location where you saved it.
5. Select **Cisco PIX/ASA Firewall Integration** and then select **Configure**.

   The Select Appliances dialog box opens.
6. Select the required CounterACT devices and then select **OK**.

   The Cisco PIX/ASA Firewall Integration Plugin Configuration dialog box opens.



The following table summarizes Cisco PIX/ASA Firewall Integration configuration options:

Field Name	Description
Firewall name	The name of the PIX or ASA firewall
Firewall Address	The IP address of the PIX or ASA firewall
User	The CounterACT device SSH user name
User Password	The CounterACT device SSH user password
Privilege Level	The CounterACT device user privilege level
Privilege Level Password	The password to obtain the privilege level

Field Name	Description
Network Group Name Prefix	A label that identifies network object groups used by CounterACT. This prefix is combined with a numerical value to specify an object group. Together, the prefix and suffix define a set of object groups. See Apply Firewall Access Lists to a Host for more information.
SSH Port	The port number for secure shell communication.
SSH version	The version of SSH used to access the PIX or ASA firewall
Maximum group size	The maximum size of a network object group
Show net group members on test	Specifies whether to list the members of the network object group when you test the plugin.
Using clear local-host command.	Specifies whether to run the **`clear local-host`** command at the firewall after a host is added to or removed from a network group. This command clears all existing connections and NAT sessions associated with the endpoint on its local network segment.

7. (Optional) Repeat Steps 5 and 6 to configure communication between remaining CounterACT devices and additional PIX/ASA firewalls.

Apply Firewall Access Lists to a Host

This plugin provides an action that adds a host to a network object group defined on PIX/ASA firewalls. These object groups are referenced by access list commands.

To add a host to an access list:

1. Define a network object group for use by CounterACT on the firewall.
2. Define an access-list statement that refers to the CounterACT network object group.

   Access list restrictions apply to all endpoints in the network object group.
3. Create a policy that uses the Cisco PIX/ASA Access-list Action to assign hosts to the CounterACT network object group.
   - Hosts that satisfy policy conditions are added to the object group on the target firewall(s). Access list restrictions apply to these hosts.
   - When hosts no longer satisfy policy conditions, they are removed from the object group. Access list restrictions no longer apply to these hosts.

Naming CounterACT Object Groups

Use this naming convention when you define network object groups for use by CounterACT.

The name of the network object groups used by CounterACT is constructed using the values of two string variables as follows:

`<Network_Group_Name><Netgroup_suffix>`

- The **Network Group Name** is a value you specified when you configured the firewall in the plugin. The default value for this string is FS_GROUP_.
- A numerical **Netgroup suffix** you specify in the *Cisco PIX/ASA Access-list* action.

This creates a series of object group names. For example, the default **Network Group Name** string **FS_GROUP_** can be combined with various **Netgroup suffix** values to yield the following series of object groups:

FS_GROUP_0 FS_GROUP_1 FS_GROUP_2 …

The **Netgroup suffix** value is policy-specific: you define the value when you use the *Cisco PIX/ASA Access-list* action.in a CounterACT policy. This means that each policy can use its own object group. At the firewall, you can apply different access list restrictions to each object group.

For example, you can configure the firewall to block internal network access for all members of *FS_GROUP_0*, and to block access to the finance server for all members of *FS_GROUP_1*. Different policies add hosts to each group.

Sample Firewall Commands

The following sample commands define a network object group that uses the CounterACT naming convention:

```
object-group network FS_GROUP_3
network-object host 0.0.0.1
```

You cannot define an empty group. A dummy host 0.0.0.1 is added to the group.

The following sample code applies access list restrictions to the CounterACT network object group defined in the previous command:

```
access-list 101 deny ip object-group FS_GROUP_3 any
access-group 101 in interface outside
```

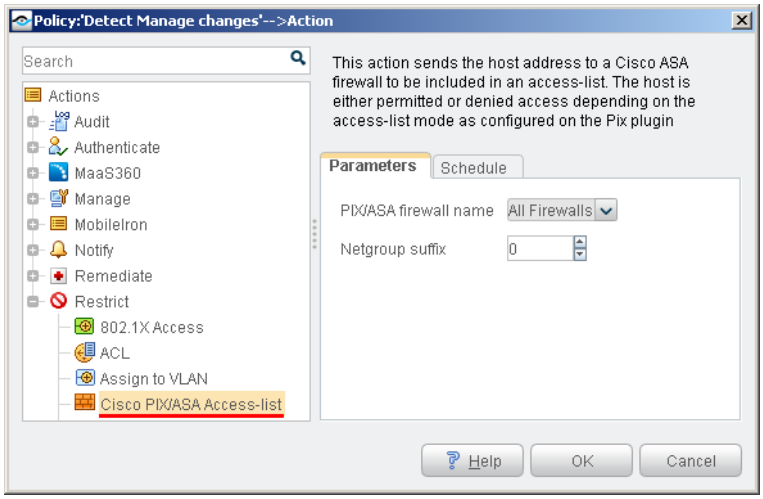
The access-list restrictions apply to the hosts in the FS_GROUP_3 network object group.

Remember to:

- Define all target firewalls in the plugin configuration pane.
- Copy these object group and access-list definitions to all the firewalls on which you want to implement the action.

Cisco PIX/ASA Access-list Action

This action adds hosts that satisfy the conditions of a policy to a network object group on PIX/ASA firewalls. This object group is referenced by a predefined access list.



The following options are available for this action:

- **PIX/ASA firewall name** – specifies the firewall on which the host is added to the network object group. Select **All Firewalls** to can add the host on all firewalls defined in CounterACT.
- **Netgroup suffix** – a numerical suffix that specifies the target network object group. This suffix is combined with the Network Group Name label configured for the plugin.

Select the **Schedule** tab to apply standard action scheduling options to this action.

Legal Notice