ForeScout

CounterACT NetScreen Firewall Plugin

Configuration Guide

Version 1.0

Table of Contents

About the NetScreen Firewall Plugin

The NetScreen Firewall plugin forwards block requests to an external NetScreen firewall. The plugin supports host blocking. Hosts blocked by the NetScreen firewall appear in the NetScreen column of the Detections pane at the Console.

After installing the plugin, you can select **Configure** from the Plugin pane to view and update default configuration values. After reviewing the configuration, select **Start** to run the plugin.

Firewall Configuration

The commands described in this section must be implemented from the NetScreen. firewall shell.

Enable SSH Access from the Appliance

1. To enable SSH access run the command: **`set ssh enable`**. (On older versions run: **`set scs enable`**)
2. Allow SSH access from the Appliance (if there is any policy which would prevent it).

Create a Blocked IP Group

1. Create a group to which blocked IPs are added.

   For example:

   `set group address Untrust ForeScout comment "ForeScout blocked IPs"`

2. Add a policy that uses the above group.

   For example:

   `set policy top from Untrust to Trust ForeScout any any deny`

   `set policy top from Untrust to DMZ ForeScout any any deny`

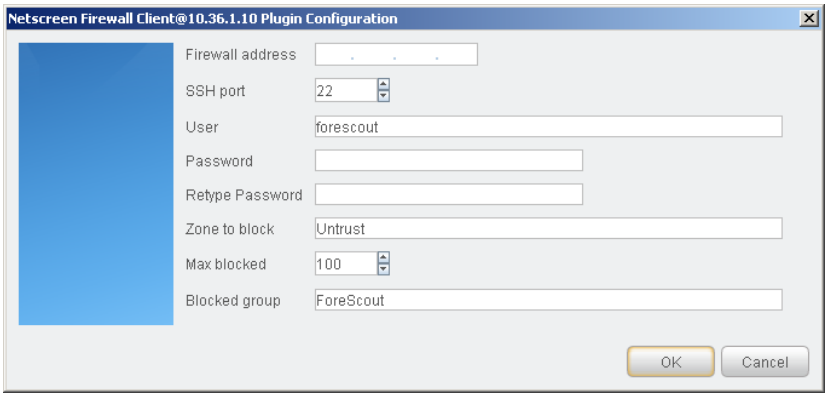
Plugin Configuration

This section describes how to install and configure the plugin.

To install and configure:

1. Download and save the plugin from the ForeScout web site.
2. Select **Options** from the **Tools** menu.
3. Select the **Plugin** folder and install the plugin from the Plugin pane.

4. Select **Configure**. The Select Appliances window opens.
5. Select the device to configure and select **OK**. The Configuration dialog box opens.



The table below summarizes NetScreen Firewall configuration options:

Field Name	Description
Firewall Address	Firewall IP address
SSH Port	SSH port number (default is 22)
User	Appliance SSH user name
Password	Appliance SSH user password
Zone to block	The zone to block.
Max blocked	Maximum number of concurrently blocked hosts. The firewall may become overloaded if it has to handle an extensive number of hosts. Default: 100
Blocked Group	Group of blocked IP addresses

Viewing NetScreen Hosts at the Control Center

Hosts blocked by the NetScreen firewall appear in the NetScreen column of the Detections pane on your main screen. One of the following indicators will appear in the column.

Blocked	The host was blocked by the NetScreen firewall.
Unblocked	The host was blocked and later released by the NetScreen firewall, but is still being monitored by CounterACT; or the host was blocked, but the plugin was stopped.
Failed to Block	The number of host blocks that the firewall platform supports has exceeded its limit. As a result, the host is not blocked.
Threshold exceeded	The host was not blocked because the threshold for the maximum blocked hosts configured at the plugin configuration dialog box has exceeded its limit.

Known Issues

- Port blocking and service blocking are not supported by the plugin.
- Blocking rules defined at the Virtual Firewall (CounterACT systems) are not supported by the plugin.

Legal Notice

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

May 2015