ForeScout

Prevent Network Attacks

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Preventing Network Attacks

CounterACT provides powerful tools that let you continuously track and control four common categories of threats to your organizational network:

- ***Malicious Hosts***: Harmful network activity, such as a worm infection or malware propagation attempts.
- ***ARP Spoofing***: Attempts to illegally gain access to your organizational network, modify the traffic, or stop the traffic altogether using the Address Resolution Protocol.
- ***Impersonation***: Attempts to masquerade as a legitimate corporate device in order to gain access to your network.
- ***Dual Homed***: De facto bridge connection to your organizational network, created by a host such as a rogue wireless access point.

Follow the step-by-step procedures in this guide to:

- Use a wizard-based CounterACT template to create a Threat Protection policy that detects threats to your network. Optional notification actions, disabled by default, can be used to inform users at the malicious endpoint, as well as the CounterACT administrator, that the endpoint is threatened.
- Review an extensive range of information about threats at hosts and about the users connected to them.
- Generate real-time and trend reports on threatening activity across your network.

This How-to guide provides basic configuration instructions designed for a quick setup. For more information on the extended configuration options, refer to the Console User Manual or the Console Online Help.

Prerequisites

- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.

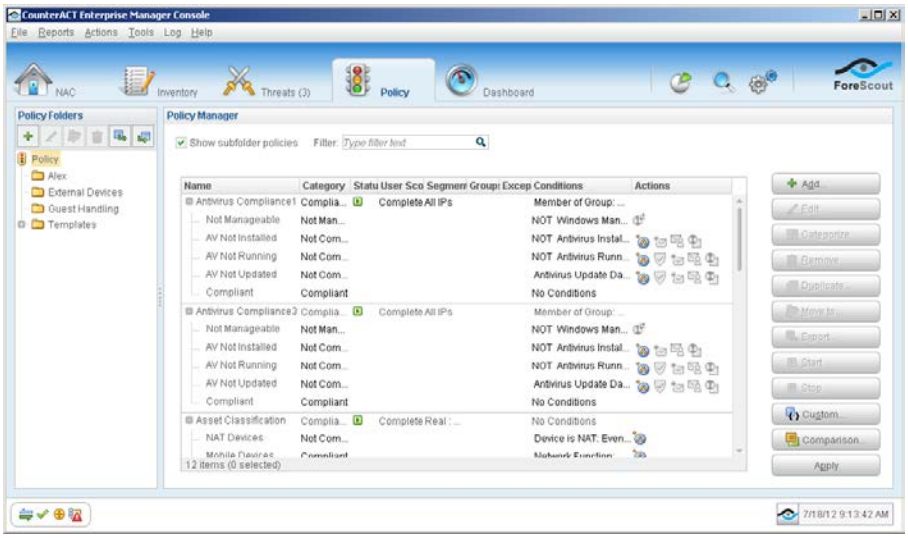
Create and Apply a Threat Protection Policy

Follow these steps to detect threats to your network using a policy template.

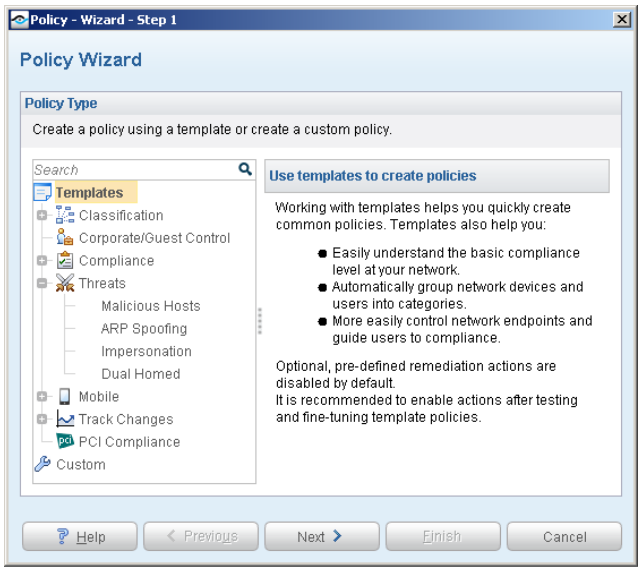
This guide discusses malicious hosts, but it also applies to ARP spoofing, impersonation and dual-homed hosts.

Select the Malicious Hosts Template

1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.



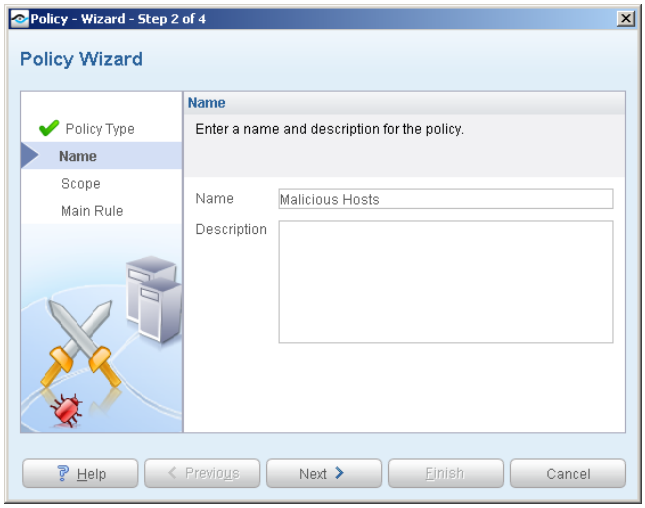
3. In the Policy Manager pane select **Add**. The Policy Wizard opens, guiding you through policy creation.



4. Under **Templates**, expand the **Threats** folder and select **Malicious Hosts**.
5. Select **Next**. The Policy Name pane opens.

2 Name the Policy

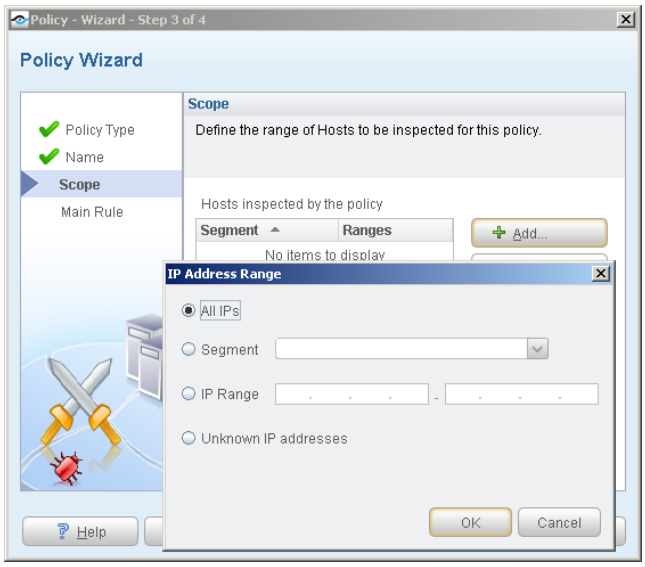
1. In the Name pane, a default policy name appears in the **Name** field.



2. Accept the default name or create a new name, and add a description.
3. Select **Next**. The Scope pane and the IP Address Range dialog box opens.

3 Choose the Hosts to Inspect

1. Use the IP Address Range dialog box to define the IP addresses you want to inspect.



The following options are available:

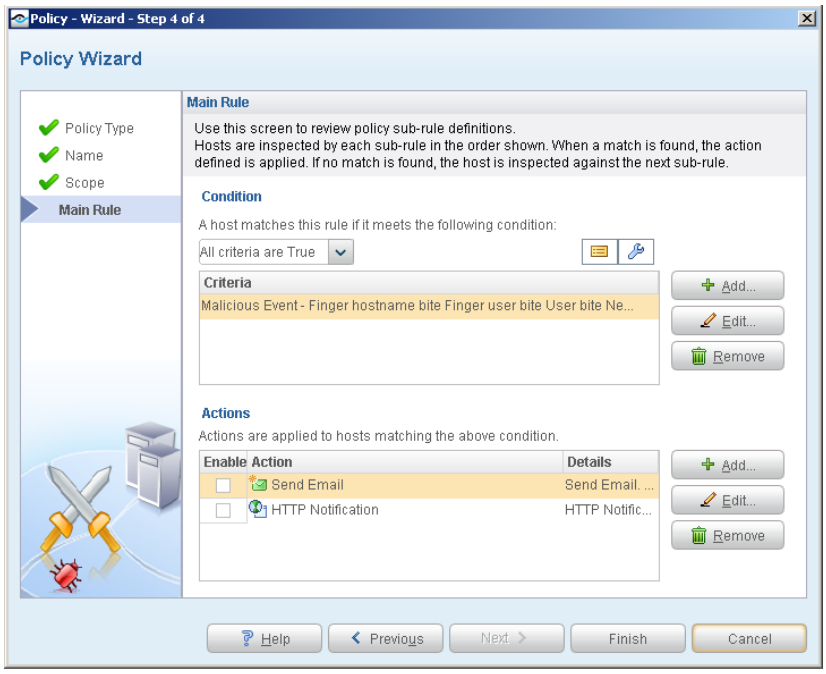
- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments**  from the Scope pane.
- **IP Range** lets you define a range of IP addresses. These addresses must be within the Internal Network.
- **Unknown IP addresses** applies the policy to hosts whose IP addresses are not known. Not applicable for this policy template.

Viewing or modifying the Internal Network is performed separately. Select Tools>Options>Internal Network.

2. Select **OK**. The added range appears in the Scope list.
3. Select **Next**. The Main Rule pane opens.

Finish Policy Creation

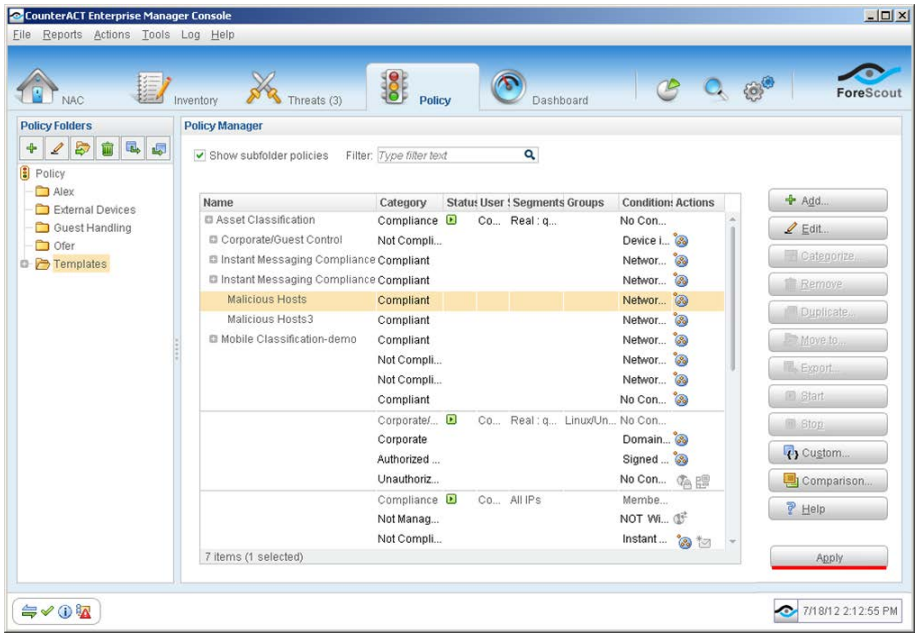
The policy main rules are displayed in the Main Rule pane. Rules instruct CounterACT how to detect hosts (Condition) and handle hosts (Actions). Optional notification actions, disabled by default, can be used to notify endpoint users or the CounterACT administrator that the endpoint is threatened. After you have run the policy and verified that results accurately reflect your network, you can remediate by enabling these actions.



1. Select **Finish**. The policy automatically appears highlighted in the Policy Manager, where it can be activated.

5 Activate the Policy

1. On the Console toolbar, select the Policy tab.
2. In the Policy Manager, select the policy you created.



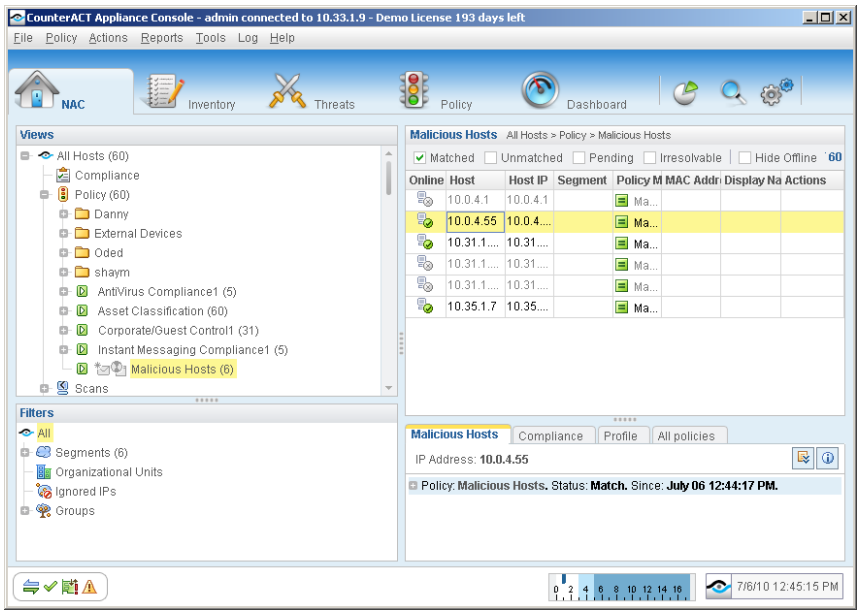
3. Select **Apply**. The policy is activated.

Evaluate Threats

After activating the policy, you can view an extensive range of details about endpoints under threat of network attacks.

To view details about endpoints and end users under threat of network attacks:

1. On the Console toolbar select the NAC tab.
2. In the Views pane, expand the **Policy** folder and scroll to the policy containing your Malicious Hosts policy.
3. In the Detections pane, select a host. Host information is displayed in the Details pane.



4. To customize the information displayed about hosts and users connected to endpoints, right-click a column heading, select **Add/Remove Columns**, and select the information of interest to you. You can also reorder the columns.

Generate Reports

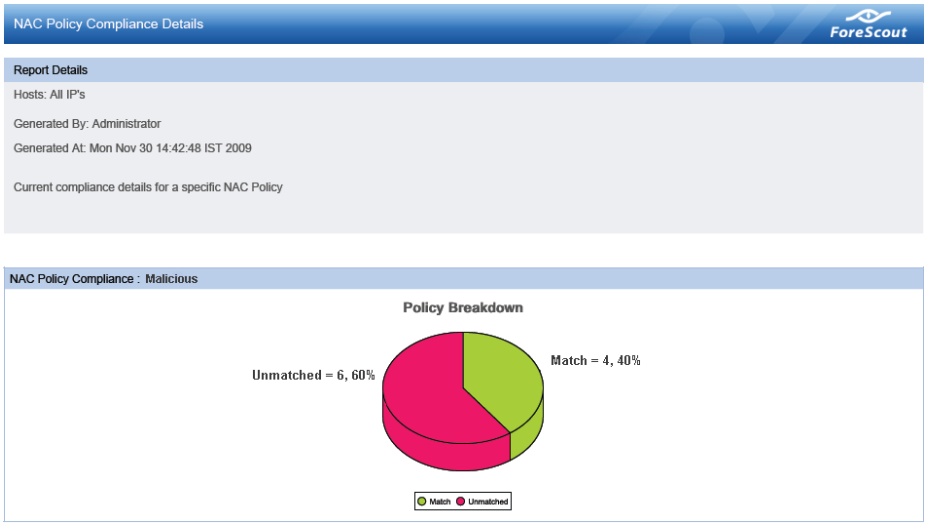
After the policy runs, you can generate reports with real-time and trend information about hosts that are under threat of attacks. You can generate and view the reports immediately, or generate schedules to ensure that changes are automatically and consistently reported.

The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the CounterACT Console User Guide.

To generate a report:

1. Select **Web Reports** from the Console **Reports** menu. The Reports portal opens.
2. Select **Add**. The Add Report Template dialog box opens.
3. Select a report template, and select **Next**. A report configuration page opens.
4. Define the report specifications in each field.
5. Schedule report generation (optional).
6. Select **Save** (optional) to save the report settings and assign them a name. The report name appears in the **Reports** list for future use.
7. Select **Run** to generate and display the report.

In the following example, the Policy Compliance Details report was selected. This report gives you a pie chart breakdown of network assets. It also provides details about each asset, depending on the information fields you selected to view.



Legal Notice

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

January 2015