ForeScout Extended Module for Palo Alto Networks Next-Generation Firewall
Configuration Guide

Version 1.1.0
Table of Contents

About the Palo Alto Networks Next-Generation Firewall Integration ........... 4
  Use Cases ........................................................................................................... 4
    Roll-out Dynamic Firewall Access Control Powered by CounterACT Policy Detections .......................................................... 4
    Leverage CounterACT as a Mission-critical Real-time Information Source ....... 4

About the Palo Alto Networks Next-Generation Firewall Extended Module .. 5
  How it Works ...................................................................................................... 5
    Central Firewall Management ......................................................................... 5
  What to Do ........................................................................................................ 7

Requirements ....................................................................................................... 7
  CounterACT Software Requirements ................................................................. 7
  ForeScout Module License Requirements .......................................................... 7
    Requesting a License ....................................................................................... 8
    More License Information ............................................................................... 9
  Palo Alto Networks Next-Generation Firewall Requirements ............................... 9

Install the Module ............................................................................................... 9

Palo Alto Networks Next-Generation Firewall Set Up ................................. 10
  Generate an API Key ....................................................................................... 10
  Prepare Your Security Policy - Create a Dynamic Address Group ...................... 10

Configure the Module ....................................................................................... 11
  Configure the Panorama Server ....................................................................... 12
  Configure Individual Firewalls ........................................................................ 15

Test the Module Configuration .......................................................................... 17

Run Palo Alto Networks Next-Generation Firewall Policy Templates .......... 17
  Send HIP Data Policy Template ....................................................................... 17

Create Custom Palo Alto Networks Next-Generation Firewall Policies....... 20
  Actions ............................................................................................................. 20
    Palo Alto Networks Next-Generation Firewall Policy Actions ....................... 21
    Map IP to User-ID .......................................................................................... 21
    Send HIP Data .............................................................................................. 22
    Tag Endpoints .............................................................................................. 24

Additional CounterACT Documentation .......................................................... 25
  Documentation Portal ...................................................................................... 25
  Customer Support Portal .................................................................................. 26
CounterACT Console Online Help Tools.................................................................26
About the Palo Alto Networks Next-Generation Firewall Integration

The CounterACT®/Palo Alto Networks® Next-Generation Firewall (NGFW) integration significantly magnifies firewall power by leveraging network visibility, inspection and enforcement capabilities provided by CounterACT.

The integration allows security teams to:

- Enrich the process of identifying, analyzing and controlling network threats.
- Enforce user-based and role-based access in real-time.
- Implement dynamic segmentation of endpoints based on endpoint classification.
- Enhance the firewall as an identity-savvy security solution.

To use the module, you should have a solid understanding of Palo Alto Networks Next-Generation Firewall concepts, functionality and terminology, and understand how CounterACT policies and other basic features work.

Use Cases

This module supports the following use case:

This module supports the following use cases:

- Roll-out Dynamic Firewall Access Control Powered by CounterACT Policy Detections
- Leverage CounterACT as a Mission-critical Real-time Information Source

Roll-out Dynamic Firewall Access Control Powered by CounterACT Policy Detections

Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, OS, location, risk status and more. This information is learned by CounterACT policies and delivered to the firewall to deal with rapid network changes.

Leverage CounterACT as a Mission-critical Real-time Information Source

Critical HIP Data without an Agent

Receive essential Host Information Profiles (HIP) from CounterACT, otherwise unavailable without the Palo Alto Networks GlobalProtect agent installed on network endpoints.

Relying on CounterACT for this information ensures that remote endpoints and guests accessing your critical resources are adequately maintained and comply with security standards before they access your network.
Real-time Identity Information

Receive real-time mapping of CounterACT detected IPs to user IDs to support granular filtering of users rather than IP addresses. CounterACT-based IP to User-ID capabilities provide vital support in environments where Active Directory is not available or limited.

About the Palo Alto Networks Next-Generation Firewall Extended Module

The Palo Alto Networks Next-Generation Firewall Module lets you integrate CounterACT with Palo Alto Networks Next-Generation Firewall so that you can:

- **Enhance firewall access control capabilities by tagging endpoints**
  
  You can leverage Palo Alto's use of tags as filtering criteria to determine the members of dynamic address groups. Using tags CounterACT can dynamically add endpoints to dynamic address groups based on endpoint assessment in policies. See Tag Endpoint.

- **Leverage CounterACT as a Mission-critical Real-time Information Source**
  
  - **Map endpoint IP addresses discovered by CounterACT to firewall User-IDs**. For example, the module can map the IP address of a user authenticating to a captive portal through a proxy. See Map IP to User-ID.
  
  - **Send HIP (Host Information Profiles) data**. Use endpoint properties such as domain name and operating system discovered by CounterACT for policy enforcement. See Send HIP Data.

How it Works

This section describes how the module communicates with Palo Alto Networks Panorama Server and firewalls.

Central Firewall Management

In addition to working directly with each firewall, the module integrates with the Palo Alto Network's central management system, Panorama, which manages a distributed network of virtual or physical firewalls.
CounterACT updates Panorama with endpoint tags so that firewalls can use these tags in real-time as matching criteria in the access rules.

The module communicates with Palo Alto Networks firewalls, supplying endpoint IP address information discovered by CounterACT using the CounterACT Map IP to User-ID, Send HIP Data and Tag Endpoint actions.

Each firewall is assigned to a connecting CounterACT device with which it communicates. Multiple firewalls can be assigned to a single CounterACT device. The connecting CounterACT device then sends the action-related information to the relevant firewall.
**What to Do**

You must perform the following to work with this module:

- Verify that requirements are met. See Requirements.
- Download and install the module. See Install the Module.
- Configure settings in Palo Alto Networks Next-Generation Firewall. See Palo Alto Networks Next-Generation Firewall.
- Define Panorama details and module settings. See Configure the Module.
- Configure the Map IP to User-ID, Send HIP Data and Tag Endpoint actions. See Palo Alto Networks Next-Generation Firewall Policy Actions.

**Requirements**

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Module License Requirements
- Palo Alto Networks Next-Generation Firewall Requirements

**CounterACT Software Requirements**

The module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 7.0.0.
- Service Pack 2.3.2 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- HPS Application Plugin 2.1.1 or higher
- HPS Inspection Engine Plugin 10.4.1 or higher
- For Mac and Linux endpoints the Macintosh/Linux Property Scanner Plugin 6.1.9 or higher is recommended for utilizing the Send HIP Data Action option.
- This module is a component of the Palo Alto Networks Next-Generation Firewall Extended Module and requires a module license. See ForeScout Module License Requirements for details.
- An active Maintenance Contract for the module.

**ForeScout Module License Requirements**

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin you are provided with a 90-day demo module license.
If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license.*

Demo license extension requests and permanent license requests are made from the CounterACT Console.

**Requesting a License**

When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.

![Example Module License Request - Step 3 of 4](image)

**To view the number of currently detected devices:**

1. Select the **Home** tab.

2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.
More License Information

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

Palo Alto Networks Next-Generation Firewall Requirements

The module requires Palo Alto Networks Firewall running one of the following versions of PAN-OS:

- 6.0.x
- 6.1.x
- 7.0.x
- 7.1.x
- 8.0.x

Install the Module

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:

1. Navigate to the Customer Support, ForeScout Modules page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select Options from the Tools menu.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. When the installation completes, select Close. The plugin is displayed in the Plugins pane. The Module Status column indicates the status of your license. See ForeScout Module License Requirements or the CounterACT Console User Manual for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select Start. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select OK. The plugin runs on the selected devices.

Palo Alto Networks Next-Generation Firewall Set Up

This section describes how to:

- Generate an API Key
- Prepare Your Security Policy - Create a Dynamic Address Group

Generate an API Key

To access the Server API, CounterACT requires an API key. To generate this key, refer to the section about generating an API key for information about API key management in the PAN-OS Administrator's Guide. Here you will also find information about API key management. This information is also available at https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/device-management/use-the-xml-api

Prepare Your Security Policy - Create a Dynamic Address Group

This section describes how to configure a Dynamic Address Group on the firewall.

Dynamic Address Groups allow you to create a CounterACT policy that automatically adapts to changes based on the filtering criteria of tags. These changes include additions, moves, or deletions of servers. It also provides flexibility for applying different rules to the same server based on its role on the network or the different kinds of traffic it processes.

To configure a Dynamic Address Group:
1. Log in to the web interface of the firewall.

- Dynamic Address Groups to be used in this integration need to be created locally on the Firewall. You cannot use Panorama shared objects.

2. Select the Objects tab and then select Address Groups.
3. Select **Add** and give the Dynamic Address Group a name. Under **Type**, select **Dynamic**.

![Address Group](image1)

4. Select **Add Match Criteria**. Since the tags are registered dynamically, add the Match Criteria to the Dynamic Group **Match** field.

The Match Criteria you define will be available for selection in the CounterACT Action.

5. Select **OK** and then **Commit**.

6. Use the group in the firewall policy based on your security requirements

![Firewall Policy](image2)

### Configure the Module

Configure the module for CounterACT to communicate with the Palo Alto Networks service.

- Define the Panorama server, including the name of the defined Panorama server and the CounterACT device it communicates with and import the firewalls and tags. See [Configure the Panorama Server](#).

- Define each firewall server and its login credentials and import the tags. See [Configure Individual Firewall](#). This is only required for standalone servers.
Once configured CounterACT devices synchronize with and provide information to these servers. Before you configure a firewall in CounterACT, you must ensure that the firewall has an administrator user with the required XML API permissions. See Generate an API Key.

When restarting the module, you need to start and stop the module on all CounterACT devices at the same time. Do not restart the module on individual CounterACT devices.

Before configuring the module, review the How it Works section.

## Configure the Panorama Server

Configure the Panorama server details and Connecting CounterACT device.

**To configure the Panorama Server:**

1. Select Options from the Tools menu and then select the Plugins folder.
2. In the Plugins pane, select the Palo Alto Networks Next-Generation Firewall Module.
3. In the right pane, ensure that the Panorama tab is selected.
5. In the **Panorama Server Definition** pane, configure the following connection parameters:

<table>
<thead>
<tr>
<th><strong>Panorama Server Name or IP Address</strong></th>
<th>Resolvable DNS name or IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Internal description of Panorama in CounterACT.</td>
</tr>
<tr>
<td><strong>Server API Access Key</strong></td>
<td>Acquired for API authentication.</td>
</tr>
<tr>
<td><strong>Verify Key</strong></td>
<td>Re-enter key.</td>
</tr>
</tbody>
</table>

6. Select **Next**. The **CounterACT Device** pane opens.
7. Set the configurations for the Connecting CounterACT device.

<table>
<thead>
<tr>
<th>Connecting CounterACT Device</th>
<th>The IP address of the CounterACT device that communicates with the firewall server. See <a href="https://www.paloaltonetworks.com/">Palo Alto Networks Next-Generation Firewall</a> for details.</th>
</tr>
</thead>
</table>
| SSL Version                  | • **SSL** - Select the preferred secured communication version to use.  
• **TLS v 1.2** - Select this option if you are using PAN OS 8.0.x.  
  
  - Make sure this selection in CounterACT is the same as what is configured on the Palo Alto Panorama server. |

8. Select **Finish**. The Palo Alto Networks Next-Generation Firewall pane displays with the new server listed.

9. If you have PAN firewalls that are managed by Panorama servers, select **Import**.

  - You need to perform Import every time a new server is added to the Panorama Server and you want to add it to the module.

10. Select **Apply**.
Configure Individual Firewalls

Configure individual firewall options to determine when API calls are sent from the module to the firewall.

To configure the firewall:

1. Select **Options** from the **Tools** menu and then select the **Plugins** folder.
2. In the **Plugins** pane, select the **Palo Alto Networks Next-Generation Firewall Module**.
3. Select the **Firewall** tab.
4. Select **Add**. The Add Firewall dialog box opens.
5. In the **Firewall Definition** pane, configure the following connection parameters:

<table>
<thead>
<tr>
<th>Firewall Name or IP Address</th>
<th>IP address or resolvable DNS name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the Firewall name.</td>
</tr>
<tr>
<td>Server API Access Key</td>
<td>Acquired for API authentication.</td>
</tr>
<tr>
<td>Verify Key</td>
<td>Re-enter key.</td>
</tr>
</tbody>
</table>

6. Select **Next**. The **CounterACT Device** pane opens.

![CounterACT Device pane](image)

7. Select the **Connecting CounterACT Device**.

<table>
<thead>
<tr>
<th>Connecting CounterACT Device</th>
<th>The IP address of the CounterACT device to communicate with the firewall server. See <a href="#">Palo Alto Networks Next-Generation Firewall Set Up</a> for details.</th>
</tr>
</thead>
</table>
| SSL Version                 | ▪ **SSL** - Select the preferred secured communication version to use.  
  ▪ **TLS v 1.2** - Select this option if you are using PAN OS 8.0.x.  
  
  "Make sure this selection in CounterACT is the same as what is configured on the Palo Alto Firewall." |

8. Select **Finish**. The Palo Alto Networks Next-Generation Firewall pane lists the new firewall.

9. Select **Apply**.
Test the Module Configuration

This section describes how to perform a configuration test. The test checks the API connectivity to the Panorama Server or Firewall Server.

To run a test:
1. In the Palo Alto Networks Next-Generation Firewall pane, select the Panorama tab or select an item in the Firewall tab.
2. Select Test.
   The Palo Alto Networks Next-Generation Firewall Module Configuration Test dialog box displays the test results.

3. Select Close.

Run Palo Alto Networks Next-Generation Firewall Policy Templates

CounterACT templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

The following template is available for detecting and managing endpoints:

- Send HIP Data Policy Template

Send HIP Data Policy Template

Use this template to create a CounterACT policy that lets you send Host Information Profile (HIP) data to the Palo Alto Networks Next-Generation Firewall.
To use the Palo Alto Networks Next-Generation Firewall Send HIP Data Policy Template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Palo Alto Networks Next-Generation Firewall folder and select Send HIP Data. The Send HIP Data pane opens.
4. Select Next. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.

Define Which Endpoints Will Be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

   Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The 32B32B added range appears in the Scope pane.

9. Select **Next**. The Main Rule pane opens.

**How Endpoints Are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. **Endpoints that do not match this rule are not inspected for this policy.** Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.
Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule of this policy applies a filter to Windows, Linux or Mac manageable devices.

10. Select **Next**. The Sub-Rules pane opens.

**Sub-Rules**

A policy sub-rule has been created for each Windows, Linux or Mac device. For example a Windows sub-rule not only checks whether the device is manageable but gets all the properties that can be sent as HIP data to the PAN firewall such as user, domain, OS, AV enable status, patch enable status, etc. The action then sends whatever property is available to the PAN firewall. The sub-rules for Linux and Mac are similarly setup.

By default, these actions are disabled.

11. Select **Finish** to create the policy.

12. On the Policy Manager, select **Apply** to save the policy.

---

**Create Custom Palo Alto Networks Next-Generation Firewall Policies**

Use CounterACT policies to:

- Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, OS, location, risk status and more. This information is learned by CounterACT policies and delivered to the firewall to deal with rapid network changes.

- Leverage CounterACT as a Mission-critical Real-time Information Source

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct CounterACT to apply a policy action to endpoints that match (or do not match) property values defined in policy conditions.

**Actions**

The CounterACT policy actions let you instruct CounterACT how to control detected devices. For example, assign detected device to an isolated VLAN or send the device user or IT team an email.

In addition to the bundled CounterACT actions available for detecting and handling endpoints, you can work with Palo Alto Networks Next-Generation Firewall module related actions to create custom policies. These items are available when you install the module.
For more information about working with policies, select Help from the policy wizard.

**To create a custom policy:**
1. Log in to the CounterACT Console.
2. Select the Policy icon from the Console toolbar.
3. Create or edit a policy.

**Palo Alto Networks Next-Generation Firewall Policy Actions**

This section describes the actions that are made available when the Palo Alto Networks Next-Generation Firewall module is installed.

**To access Palo Alto Networks Next-Generation Firewall Module actions:**
1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the Palo Alto Networks Next-Generation Firewall folder in the Actions tree. The following actions are available:
   - Map IP to User-ID
   - Send HIP Data
   - Tag Endpoint

**Map IP to User-ID**

This action lets you map an endpoint IP address detected by CounterACT to a Palo Alto Networks Next-Generation Firewall User-ID. CounterACT detects a fully qualified domain name (FQDN) to map an endpoint IP address.

Palo Alto Networks Next-Generation Firewall employs a User Identification (User-ID) feature to configure and enforce firewall policies based on users. User-ID identifies the user on the network and the IP addresses of the computers the user is logged into. In certain situations, however, firewalls cannot easily map between an IP address and a user identity. The module leverages CounterACT advanced endpoint detection capabilities to identify and contribute user information to firewalls.
The following parameters are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapping Timeout (Minutes)</td>
<td>The number of minutes that the action persists in the firewall. It is recommended to set a recurrence pattern to resend the User ID/mapping data at an interval shorter than the timeout set in the action.</td>
</tr>
<tr>
<td>Domain\User</td>
<td>By default, this parameter consists of the nbtdomain and user property tags representing the NetBIOS domain and the user name. You can select any CounterACT property tag by using the Tags option.</td>
</tr>
<tr>
<td>Specify one or more Firewall Servers</td>
<td>The target firewall(s) that the action is applied to. See Configure the Module.</td>
</tr>
</tbody>
</table>

**Send HIP Data**

This action lets you send the following endpoint host properties, if available, to the PAN firewall where the information can be used to further filter access and create a more restrictive policy. This allows better security control.

CounterACT can populate the following information in the first version of the module on the PAN firewall:

- User, OS, Domain, Hostname for Windows, Linux or Mac devices
- Running process list for Windows, Linux or Mac devices
- Disk Encryption for Windows devices only
- Anti-virus, Firewall and Patch Management enable/disable status for Windows and Mac devices

CounterACT can send HIP information to Panorama or to the firewall directly. Refer to the table below to see which PAN HIP object is mapped to a CounterACT host property and the plugin provides that host property.
The following parameters are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>OS</th>
<th>Data Sent</th>
<th>Default CounterACT Property</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Windows</td>
<td>Logged in User</td>
<td><code>{user}</code></td>
<td>HPS Inspection Engine</td>
</tr>
<tr>
<td></td>
<td>Mac</td>
<td>Logged in User</td>
<td><code>{mac_logged_users}</code></td>
<td>Mac / Linux Property Scanner</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>Logged in User</td>
<td><code>{linux_logged_users}</code></td>
<td>Mac / Linux Property Scanner</td>
</tr>
<tr>
<td>Domain</td>
<td>Windows / Mac / Linux</td>
<td>Domain</td>
<td><code>{nbtdomain}</code></td>
<td>Packet Engine</td>
</tr>
<tr>
<td>OS</td>
<td>Windows / Mac / Linux</td>
<td>OS</td>
<td><code>{user_def_fp}</code></td>
<td>Packet Engine</td>
</tr>
<tr>
<td>Host Name</td>
<td>Windows / Mac / Linux</td>
<td>Host Name</td>
<td><code>{nbthost}</code></td>
<td>Packet Engine</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Windows</td>
<td>Antivirus enabled or not</td>
<td><code>{av_install}</code></td>
<td>HPS Inspection Engine</td>
</tr>
<tr>
<td></td>
<td>Mac</td>
<td>Antivirus enabled or not</td>
<td><code>{mac_process_running}</code></td>
<td>Mac / Linux Property Scanner</td>
</tr>
<tr>
<td>Disk Encryption</td>
<td>Windows</td>
<td>List of disk encryption products/vendors installed on endpoint</td>
<td><code>{hd_installed_new}</code></td>
<td>HPS Inspection Engine</td>
</tr>
<tr>
<td>Parameter</td>
<td>OS</td>
<td>Data Sent</td>
<td>Default CounterACT Property</td>
<td>Dependency</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>----------------------------</td>
<td>------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Firewall</td>
<td>Windows</td>
<td>▪ Firewall enabled or not</td>
<td>{fw_active}</td>
<td>HPS Inspection Engine</td>
</tr>
<tr>
<td></td>
<td>Mac</td>
<td>▪ Firewall enabled or not</td>
<td>{mac_process_running}</td>
<td>Mac / Linux Property Scanner</td>
</tr>
<tr>
<td>Processes List</td>
<td>Windows</td>
<td>List of running processes</td>
<td>{process_no_ext}</td>
<td>HPS Inspection Engine</td>
</tr>
<tr>
<td></td>
<td>Mac</td>
<td>List of running processes</td>
<td>{mac_process_running}</td>
<td>Mac / Linux property scanner</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
<td>List of running processes</td>
<td>{linux_processes_running}</td>
<td>Mac / Linux property scanner</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Windows</td>
<td>List of missing patches</td>
<td>{vulns}</td>
<td>HPS Vulnerability DB / HPS Inspection Engine</td>
</tr>
<tr>
<td></td>
<td>Mac</td>
<td>List of missing patches</td>
<td>{mac_software_updates}</td>
<td>Mac/Linux property scanner / HPS Vulnerability DB</td>
</tr>
</tbody>
</table>

Specify one or more firewalls:

<table>
<thead>
<tr>
<th>Send to all firewalls</th>
<th>Send HIP data to all firewall servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send to specific firewalls</td>
<td>A list of target firewall servers. One or more can be selected.</td>
</tr>
</tbody>
</table>

**Tag Endpoints**

This action adds a tag to an endpoint. The tag is then matched to Firewall Dynamic Address Group by the PAN firewall.

A tag is a string or attribute that the firewall uses to match and determine the members of the group of endpoints that it will handle. The tag comprises logical and and or operators for defining the filtering criteria. CounterACT detects the endpoints to which these tag criteria are applied.

To ensure that you support the latest Dynamic Access Group configuration, ensure that you have imported the most recent tags set up on the server. Refer to [Prepare Your Security Policy - Create a Dynamic Address Group](#).
The following parameters are available for selection:

<table>
<thead>
<tr>
<th><strong>Tag</strong></th>
<th>Tag set up on the firewall server in the Palo Alto Networks Next-Generation Firewall Platform. Names are case sensitive.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Firewall Servers</strong></td>
<td>The action is applied to all firewall servers.</td>
</tr>
<tr>
<td><strong>Specify servers</strong></td>
<td>A list of target firewall servers. One or more can be selected.</td>
</tr>
</tbody>
</table>

### Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- [Documentation Portal](#)
- [Customer Support Portal](#)
- [CounterACT Console Online Help Tools](#)

### Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.
To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal
The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools
Access information directly from the CounterACT Console.

Console Help Buttons
Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

Console User Manual
Select CounterACT Help from the Help menu.

Plugin Help Files
1. After the plugin is installed, select Options from the Tools menu and then select Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
**Legal Notice**

Copyright © ForeScout Technologies, Inc. 2000-2017. 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 may be protected by one or more of the following 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/](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/](http://www.forescout.com/activecare-maintenance-and-support-policy/);
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at [http://www.forescout.com/professional-services-agreement/](http://www.forescout.com/professional-services-agreement/);
- 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/](http://www.forescout.com/evaluation-license/).
  - 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/](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/](http://www.forescout.com/nfr-license/).

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

2017-07-24 16:52