FORESCOUT

Forescout

Core Extensions Module: Packet Engine

Configuration Guide

Version 8.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-03-25 10:21

Table of Contents

About the Packet Engine

The Packet Engine is a component of the Forescout® Core Extensions Module. See Core Extensions Module Information for details about the module.

The Packet Engine provides unprecedented network visibility using real-time port mirroring in the network. Port mirroring – known in Cisco networks as Switched Port Analyzer (SPAN) configuration and in 3COM networks as Roving Analysis Port (RAP) configuration – allows Forescout 8.1 to directly monitor traffic in the network. This supplements other methods and sources – such as the Flow Collector, the Switch Plugin, the DHCP Classifier Plugin, and the DNS Plugin – that Forescout 8.1 uses to learn information from the network.

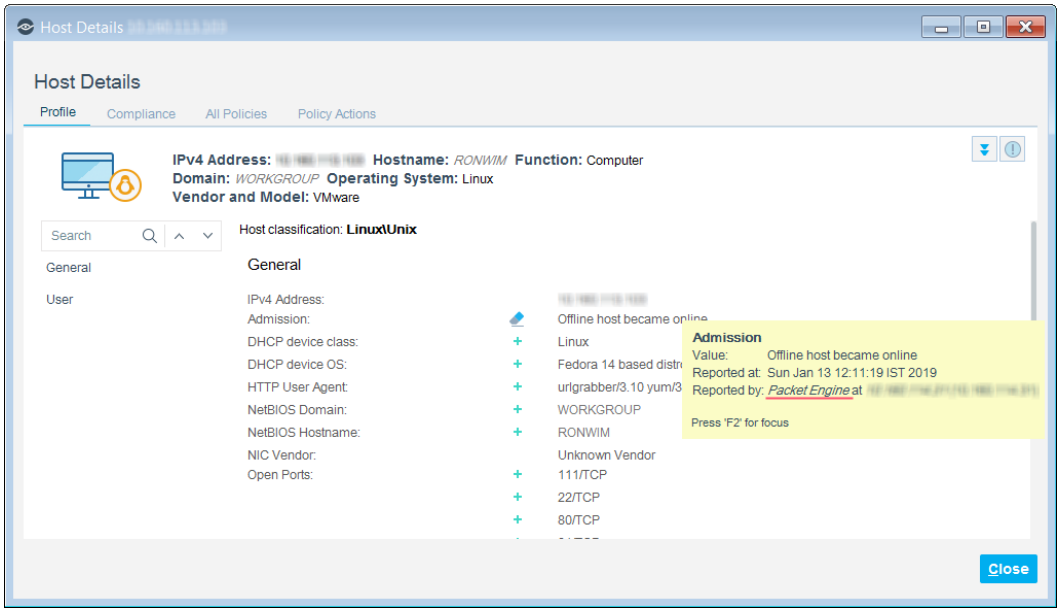
The Packet Engine does not support RSPAN (Remote SPAN) or ERSPAN (Encapsulated Remote SPAN).

The synergistic use of port mirroring and other real time/low latency data sources provides the following advantages:

- Endpoint discovery from first communication on the network
- Detection of authentication and client/server sessions from the first query
- Passive learning of configuration settings and other endpoint properties
- Detection of NAT behavior, spoofing, port scanning, and other suspicious or malicious behavior patterns
- Network management using messages injected into the data stream via the mirror port, such as for virtual firewall enforcement and HTTP session redirection (for IPv4 addresses only)

The Packet Engine parses and analyzes mirrored traffic data packets for:

- Network traffic monitoring
- Endpoint discovery
- Endpoint property evaluation
- Traffic data accumulation for the Segmentation Manager connectivity matrix (if the eyeSegment Module is installed)



How It Works

Information reported to Forescout 8.1 based on parsed traffic is stored as *host properties*. Host property values are displayed in Console views, and can be evaluated and examined by policies to trigger *actions* that restrict network access or manage/remediate endpoints.

To parse traffic in the different layers, the Packet Engine contains different parsers for common network protocols. Among these are:

- ARP
- DCE/RPC
- DHCP - the Packet Engine detects hosts that act as DHCP servers and DHCP relays
- DICOM
- HTTP
- NetBIOS/SMB

The Packet Engine parses most session-based protocol messaging to detect sessions as they are established, and to determine which entity acts as client and which acts as server.

For NAT detection, the Packet Engine leverages both passive traffic monitoring and the ability to send responses. Typical methods implemented by the Packet Engine include detection of behavior patterns such as port scanning, and injection of test messages similar to Nmap diagnostics.

The Packet Engine listens to HTTP traffic and notes the user agent header in HTTP requests. Based on defined translation rules, the user agent is used to resolve the value of the Network Function property.

The Packet Engine passively listens to SMB traffic. It determines the value of the Network Function property based on unique signatures in the traffic. This is useful for determining Windows Machine devices.

The Packet Engine performs passive fingerprinting of the SYN and SYN-ACK packets.

The Packet Engine resolves several endpoint properties, including:

- Traffic seen
- Host is Online
- HTTP User Agent (for IPv4 addresses only)
- Open Ports (for IPv4 addresses only)
- Network Function
- Admission (Authentication Login and Authentication Server for IPv4 addresses only)
- Mac Address
- ARP Spoofing
- Sessions as Client (for IPv4 addresses only, and only resolved when used in a policy)
- Sessions as Server (for IPv4 addresses only, and only resolved when used in a policy)

Requirements

This version of the Packet Engine requires the following Forescout release:

- Forescout version 8.1

Packet Engine Commands

You can customize certain Packet Engine features, including default parser ports.

To see the commands available for retrieving conf_params:

- Log in to the CounterACT device through the command-line interface (CLI) and run the following command:

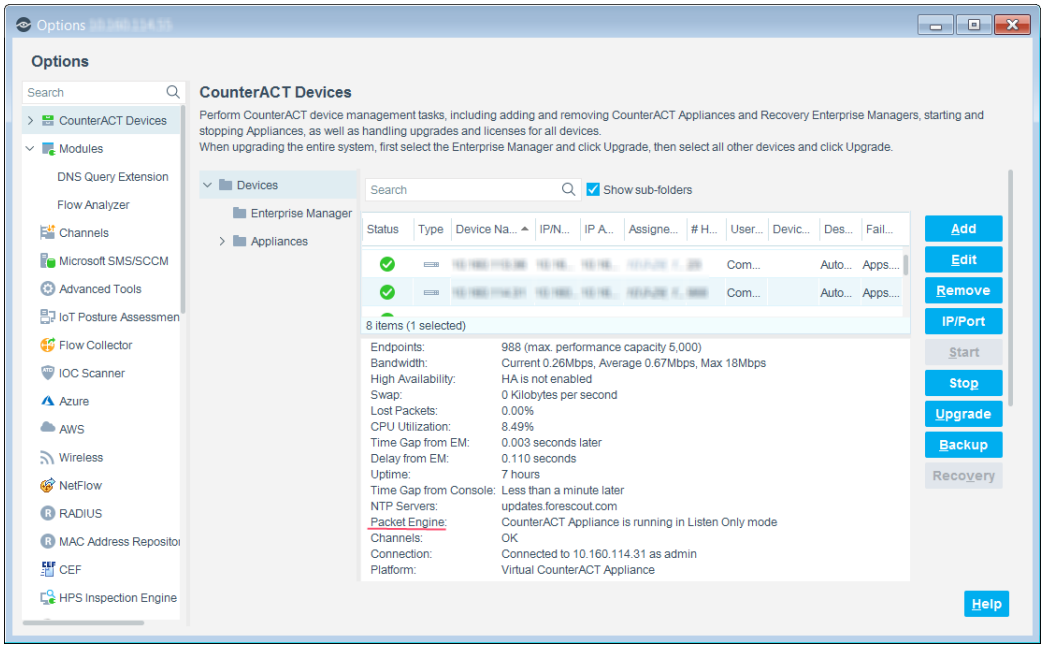
  `help pe`

Packet Engine Status

To view the Packet Engine status on an Appliance:

1. Select **Tools > Options > CounterACT Devices**.

2. Select the Appliance. The Packet Engine status is included in the Appliance health information.



For information about the Packet Engine detailed status (ctDeviceEngine) in the SNMP MIB table, refer to the Forescout Administration Guide.

Configuration

Refer to the *Forescout Administration Guide* for information about Packet Engine features, including:

- Appliance channel assignments
- Threat protection
- Legitimate scan
- Internal network vs. active response range
- Virtual Firewall action blocking rules
- HTTP actions:
  - HTTP Login
  - HTTP Sign Out
  - HTTP Localhost Login
  - HTTP Notification
  - HTTP Redirection to URL

Performance Optimization

For improved Packet Engine speed, follow these recommendations.

Physical Appliances

Configure one or two 10G monitor ports in each physical Appliance that monitors traffic.

When an Appliance uses more than two monitor ports:

- Ensure that an even number of monitor ports is used.
- Do not mix interface types, such as a 1Gb network adapter together with a 10Gb network adapter.

Virtual Appliances

When using Virtual Appliances:

- On VMWare, the VMXNET3 adapter type is preferred over the E1000 adapter type.
- Hyper-V Windows 2016 is preferable to Windows 2012.

Endpoint Discovery

The host MAC address is not learned from ARP reply packets, but rather from ARP requests only. Use the following command to enable learning the MAC address from ARP reply packets:

```
fstool pe set_conf_param LearnEventMacReplyChangesOnly 0
```

> *All **`fstool pe set_conf_param`** commands must be followed by a restart for the Packet Engine daemon: **`fstool engine kill`***

Host Properties

By default, the Packet Engine learns Open Ports from a connection's packets, including reset packets. Use the following command to disable learning from reset packets:

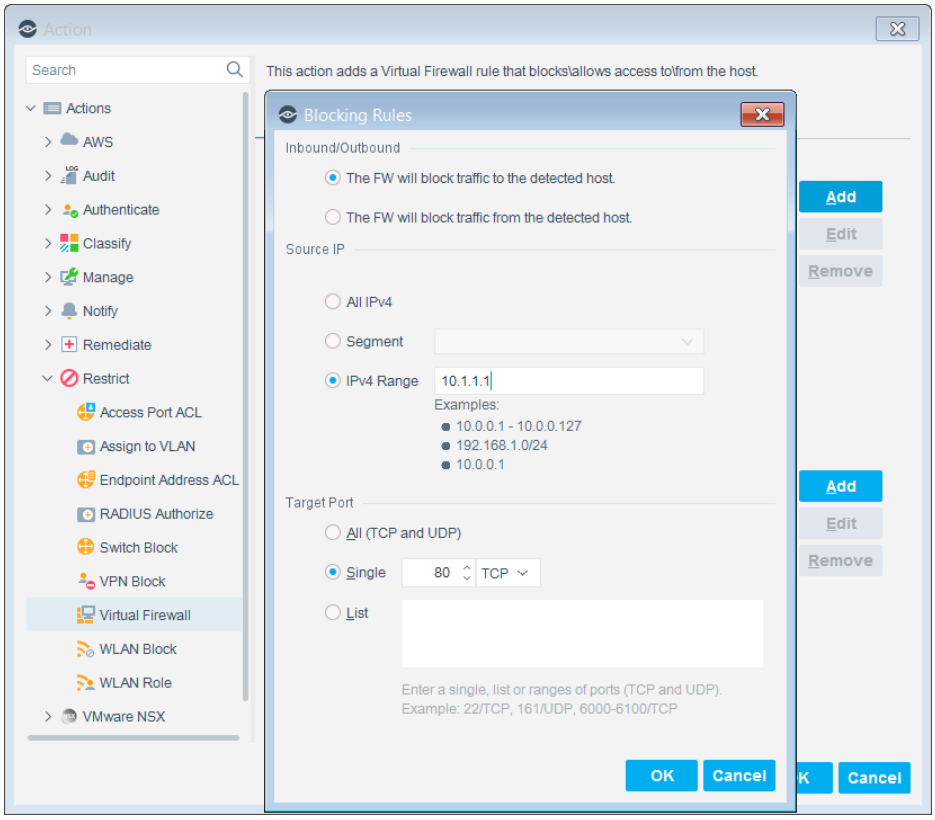
```
fstool set_conf_param DontLearnFromReset 1
```

> *All **`fstool pe set_conf_param`** commands must be followed by a restart for the Packet Engine daemon: **`fstool engine kill`***

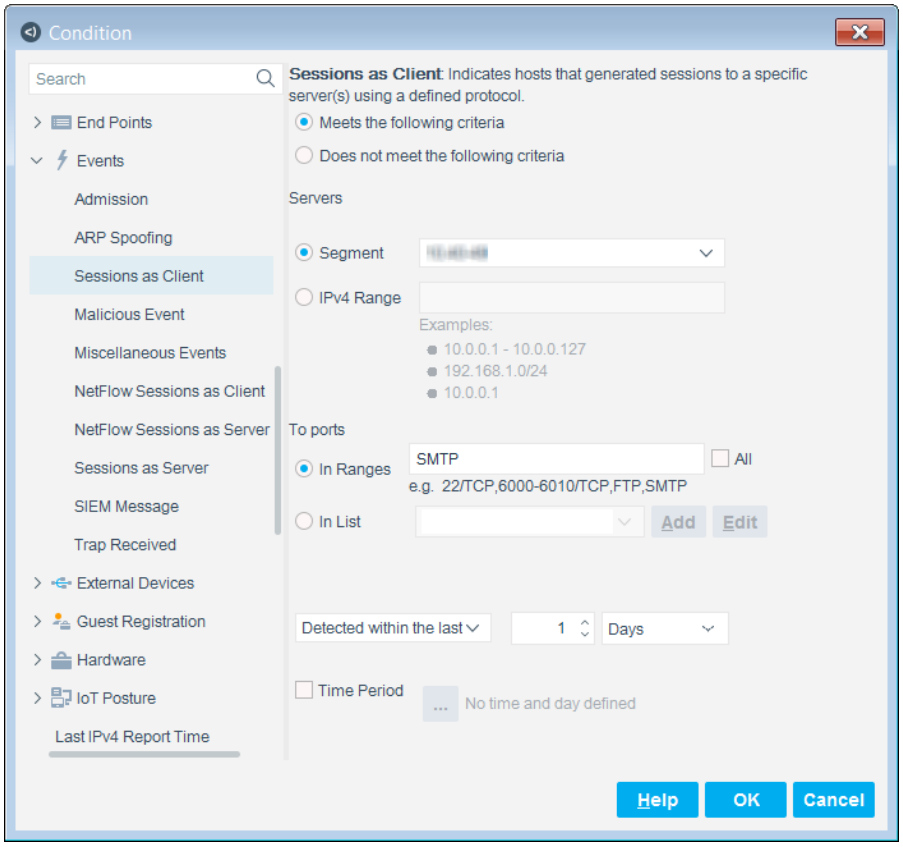
Packet Engine Rule Optimization

Packet Engine rules are *Virtual Firewall* policy actions and *Session as Client/Server* policy conditions. Examples of Packet Engine rules:

- A Virtual Firewall action to block all HTTP traffic to a specific server



- A Session as Client policy condition to identify all SMTP clients in a segment



Consider the following Packet Engine rule performance guidelines.

- Network Traffic Rule Limitation
- Number of Ranges in Each Packet Engine Rule

Network Traffic Rule Limitation

Packet Engine rules require the Packet Engine to hold in memory a set of Network Traffic rules. The number of Network Traffic rules enforced dynamically via policy evaluation can dramatically impact performance. ***It is recommended to run no more than 100,000 Network Traffic rules per Appliance for each of the following:***

- 'Virtual Firewall' actions. See Network Traffic Rules Generated by 'Virtual Firewall' Actions.
- 'Sessions as Server/Client' conditions. See Network Traffic Rules Generated by 'Sessions as Server/Client' Conditions.
- 'Legitimate Scan' rules. Follow the same performance guidelines as for Packet Engine rules.
- Exceptions to HTTP redirection actions.

Network Traffic Rules Generated by 'Virtual Firewall' Actions

When using the Virtual Firewall action in a policy, each matched endpoint generates a separate Network Traffic rule. To minimize the number of Network Traffic rules generated:

- Narrow the policy scope as much as possible.
- Define precise policy conditions for Virtual Firewall actions.

Network Traffic Rules Generated by 'Sessions as Server/Client' Conditions

Each time a Sessions as Server/Client condition is used in a policy, the number of Network Traffic rules generated depends on the complexity of the ranges or segments specified in the condition.

Number of Ranges in Each Packet Engine Rule

Each Virtual Firewall action or Sessions as Server/Client condition in a Packet Engine rule includes the following rule parameters:

- IP addresses in the policy scope
- Source or target ranges
- Port ranges

Minimal Items in One of the Rule Parameters

Ensure that at least one rule parameter in each Packet Engine rule includes *less than 10* items. The following examples are acceptable because one of the parameters includes only one or two items:

- Policy Scope: 10.1.1.1,40.1.1.4 To: segment-HQ Port Range: 1-1024
- Policy Scope: segment-HR To: segment-HQ Port Range: 80

If it is not feasible to limit any of the rule parameters to less than 10, contact Forescout support for additional solutions.

Number of Total Ranges in a Rule

It is recommended to minimize the number of effective ranges within all rule parameters. For example, it is preferable for a parameter to have 8 different ranges than for it to have 40 different ranges.

Perform the following best practices:

- Combine different ranges into a single continuous range.
- If a rule parameter must include many more than 10 different ranges, divide it into two or more different rules.

Packet Engine Considerations

Consider the following Packet Engine behaviors.

Network Configuration

Whenever channel definition interfaces are reconfigured, an Appliance reboot is required.

Virtual Appliances

Hyper-V affinity configuration is not supported.

Policy Actions

- Each Appliance can support up to 200 hijack actions per minute.
- Virtual Firewall is not an inline router. As a result:
  - The effectiveness of restrict actions depends on the proximity of the Appliance to the client or server being restricted.
  - UDP traffic blocking is not guaranteed per packet.
- By default, the Virtual Firewall restrict action is session-based. Use the following command to configure it as packet-based:

  `fstool pe set_conf_param packetBaseBlocking 1`

  *All **`fstool pe set_conf_param`** commands must be followed by a restart for the Packet Engine daemon: **`fstool engine kill`***

- *Partial Enforcement* mode is recommended for evaluation purposes only. This mode lets you monitor network traffic, but it limits your ability to respond to it. Specifically, the Threat Protection, HTTP Actions, and Virtual Firewall options are disabled in this mode.

  Host profiles in the Console do not indicate that these actions are not run.

IPv6 Endpoints

The following features are not supported for IPv6 endpoints:

- Virtual Firewall and HTTP actions
- Threat protection

Deep Packet Inspection (DPI)

Ports for DICOM Parsing

DICOM protocol inspection is supported on TCP only. By default, the DICOM parser works on TCP ports 4100, 104 and 11112. Use the following commands to configure DICOM parsing to apply to additional TCP ports:

- Get value command:

fstool pe get_conf_param Plugin_Extra_Ports_dicom

- Set value command:

  fstool pe set_conf_param Plugin_Extra_Ports_dicom <comma-separated list of ports>

  For example: **fstool pe set_conf_param Plugin_Extra_Ports_dicom 4100,104,11112,4242,4444**

*All **fstool pe set_conf_param** commands must be followed by a restart for the Packet Engine daemon: **fstool engine kill***

Resources Required for DICOM Parsing

When heavy DICOM traffic consumes almost all of an Appliance's maximum traffic monitoring rate, other features, such as endpoint and switch management, might slow.

Core Extensions Module Information

The Forescout Core Extensions Module provides an extensive range of capabilities that enhance the core Forescout solution. These capabilities enhance detection, classification, reporting, troubleshooting and more. The following components are installed with the Core Extensions Module:

Advanced Tools Plugin	Dashboard Plugin	NBT Scanner Plugin
CEF Plugin	Device Classification Engine	Packet Engine
DHCP Classifier Plugin	External Classifier Plugin	Reports Plugin
DNS Client Plugin	Flow Analyzer Plugin	Syslog Plugin
DNS Enforce Plugin	Flow Collector	Technical Support Plugin
DNS Query Extension Plugin	IOC Scanner Plugin	Web Client Plugin
	IoT Posture Assessment Engine	

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).