Forescout

Port Mirroring

Technical Note

ForeScout 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 10:19

Table of Contents

About Port Mirroring and the Packet Engine

The Forescout solution is distinguished from other network access, security, and management tools by its unprecedented network visibility.

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.

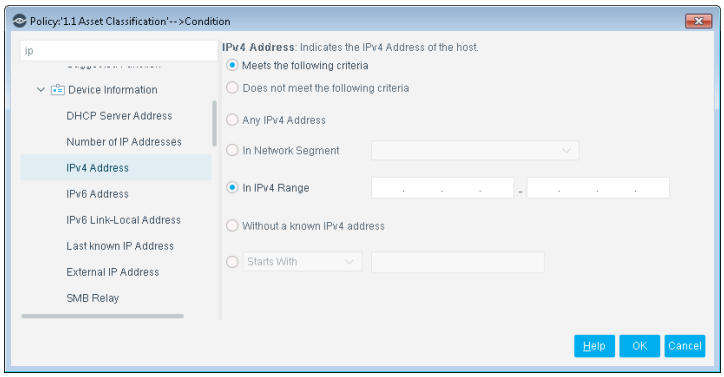
The Packet Engine does not support RSPAN (Remote SPAN) or ERSPAN (Encapsulated Remote SPAN).

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)



This document provides an overview of the messages that the Packet Engine selects from the mirrored traffic and then parses to discover endpoints and to track network interactions.

Information Based on Specific Protocols

This section describes in detail how the Packet Engine parses messages in the most common network protocols, and how the information learned is used to evaluate Forescout 8.1 host properties. Protocols analyzed by the Packet Engine include:

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

ARP

Benefits

- Quickly learn and map IP/MAC addresses to endpoints.
- Learning endpoint IP addresses is a prerequisite for further inspection.
- Identify spoofing and Man-in-the-Middle attacks.

Endpoint Detection: ARP fields are parsed to passively learn MAC addresses of endpoints.

- Information is reported in the **MAC Address** host property.
- This information is also reported to Forescout 8.1 by other processes, such as the HPS Inspection Engine.

> *ARP tables on switches are queried extensively by the Switch Plugin, a core plugin of the system. Refer to the Forescout Administration Guide and the Switch Plugin Configuration Guide for more information.*

The Forescout solution also injects targeted ARP requests, and maps IP/MAC addresses based on the response. This allows detection of many spoofing and Man-in-the-Middle threats.

- Reported information is used to evaluate the **ARP Spoofing** host property.
- It is recommended to configure your environment using the following guidelines when detecting ARP spoofing:

  - To allow ARP packet injection, do *not* configure the response interface as the IP Layer. Refer to the section on working with Appliance channel assignments in the Forescout Administration Guide for more information.
  - Set up your network to hear ARP traffic on VLANs.
  - Configure the CounterACT device with one IP address per monitored VLAN.

ActiveResponse™ Threat Protection

The Forescout solution injects targeted ARP replies that are structured to detect malicious scanning in the broadcast domain.

- This feature is enabled when the Appliance operates in Full Enforcement mode. Refer to the Forescout Administration Guide for more information about the Enforcement mode.

DHCP

Benefits

- Detect endpoints from their first communication on the network.
- Map DHCP servers and relays in the network.

Endpoint Detection: DHCP requests are parsed to detect endpoints from their first communication on the network. This information is also used to generate internal *admission events* that initiate further learning of the new endpoint by the HPS Inspection Engine and other Forescout processes.

- Information is reported in the following host properties:
  - Admission
  - DHCP Request
  - MAC Address
- The optional DHCP Classifier Plugin can also parse mirrored traffic for more detailed device information. This information is reported in the following host properties:
  - DHCP Hostname
  - DHCP Vendor Class
  - DHCP device Class
  - DHCP device OS
  - DHCP request fingerprint
  - DHCP options fingerprint
  - MAC Address
- Information reported by other plugins contributes to the decision to initiate an admission event.

DHCP Server Detection and Mapping: Based on observed DHCP interactions, the Packet Engine detects hosts that are acting as DHCP servers and DHCP relays.

- Information is reported in the following host properties:
  - Device is DHCP Relay
  - Device is DHCP Server
  - DHCP Server IP Address

DICOM

Benefits

- Detect endpoint classification properties of DICOM-recognized medical equipment.

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`***

HTTP

Benefits

- Detect and classify NAT devices, identifying potential threats.
- Detect malicious activity with ActiveResponse technology.
- Enhance endpoint classification.

Endpoint Detection: HTTP headers are parsed to help detect admission of new endpoints, and to provide additional information for endpoint classification.

- Information is reported in the **HTTP User Agent** and **Admission** host properties.
- Information from other sources contributes to the initiation of an admission event.
- Account credentials are not parsed.
- Data payload is not parsed.
- This information is also reported by other plugins, and is learned when policy actions, such as the HTTP Notify action, establish HTTP sessions between endpoints and Appliances.
- Secure HTTP (HTTPS) message headers are not parsed unless the optional DNS Enforce Plugin has been installed. Data payload is never parsed for these messages.

NAT Detection: By monitoring traffic and retransmitting certain packets, Forescout 8.1 can detect and classify NAT devices.

- Information is reported in the **Device is NAT** host property.
- Data payload is not parsed.
- For managed endpoints, this information can also be learned from the HPS Inspection Engine, the OS X Plugin, and the Linux Plugin. However, traffic-based detection is more comprehensive, and does not require managed endpoints behind the NAT.
- This feature is enabled when the Appliance operates in Full Enforcement mode. Refer to the Forescout Administration Guide for more information about the Enforcement mode.
- Forescout 8.1 uses a proprietary, patented technology involving the detection and retransmission of packets. This enables the detection of network devices, such as commodity wireless routers and VPN concentrators, that perform one-to-many Network Address Translation (NAT).

  Examples of devices that are ***not*** detected include:

  – VMWare virtual machines configured for NAT
  – Security devices, such as certain firewalls/VPNs (for example, SonicWall)

ActiveResponse™ Threat Protection

Forescout 8.1 technology actively identifies malware infection attempts, network scans, and other malicious behavior. HTTP is one of several traffic types that are monitored to identify malicious network scanning and redirection activities on endpoints. Refer to the Forescout Administration Guide for more information.

- Data payload is not parsed.

NetBIOS/SMB

Benefits

- Crucial for the resolution of information related to the User Directory.
- Maps users/endpoints to domains as a basis for further inspection.

Endpoint Detection and Mapping: NetBIOS header fields are parsed to yield domain and hostname information for endpoints, and to map endpoints to domains. NetBIOS headers also provide IP/MAC address information.

- Data payload is not parsed.
- Account credentials are not parsed.
- Information is reported in the following host properties:

  – NetBIOS Domain
  – NetBIOS Hostname
  – User
  – MAC Address

- This information is also reported for endpoints managed by either the HPS Inspection Engine, the OS X Plugin, or the Linux Plugin.

- This information is distinct from DNS information and properties.

TCP / UDP

Benefits

- Detects client/server sessions as they are established.
- Verifies endpoint authentication by specified servers.
- Maps open ports on endpoints, enabling port-level security management.
- Assists in device classification.
- Used to implement Virtual Firewall and HTTP Redirection Actions.

Session Detection: The Packet Engine parses most session-based messaging protocols, including:

- EMAP
- FTP
- HTTP
- MAPI
- Microsoft-DS
- NetBIOS
- POP3
- rLogin
- SMTP
- Telnet

This enables the Packet Engine to detect sessions as they are established, and to determine which entity acts as client and which acts as server.

- The parsed protocol information is reported in the **Sessions as Server** and **Sessions as Client** host properties. When specific authentication servers are defined in ForeScout 8.1, a login to these servers is reported in the **Authentication Login** host property.
- Data payload is not parsed.
- Account credentials are not parsed. However, authentication success/failure is tracked.
- Detected attempts to establish HTTP or other sessions can trigger **Virtual Firewall** or **HTTP redirection** actions.
- When NetFlow reporting is enabled in the network environment, this information can also be provided by the Flow Collector Plugin.

Port Detection: Header fields are parsed to extract port information that is used to map open ports on endpoints.

- The information is reported in the **Open Ports** host property.

- Data payload is not parsed.
- Account credentials are not parsed.
- The HPS Inspection Engine, the OS X Plugin, and the Linux Plugin may report partial port information on managed endpoints. These plugins might not report all ports due to firewalls or other network topography.
- When NetFlow reporting is enabled in the network environment, this information can also be provided by the Flow Collector Plugin.

Endpoint Lifecycle

Forescout 8.1 defines several endpoint lifecycle events and host properties based on a broad spectrum of learned information, which is augmented by the Packet Engine's inclusive view of network traffic.

Endpoint Admission is based on detection of a broad range of login and authentication interactions.

- These interactions include the following protocols:
  - ARP
  - DCE/RPC
  - DHCP - the Packet Engine detects hosts that act as DHCP servers and DHCP relays
  - DICOM
  - HTTP
  - NetBIOS/SMB
- Data payload is not parsed.
- Account credentials are not parsed.
- Additional information based on other protocols is provided by the RADIUS Plugin and the User Directory Plugin.
- Additional admission triggers are reported by the Switch Plugin, Wireless Plugin, RADIUS Plugin, Flow Collector, and other data sources.

Endpoint Visibility is sustained as long as any traffic from the endpoint is detected, using any protocol. Information is reported in the **Traffic seen** host property, and supports derived properties such as **Host is Online**.

SecureConnector events are used for admission and visibility tracking on endpoints already managed by the Forescout platform.

When NetFlow reporting is enabled in the network environment, the optional Flow Collector Plugin supports endpoint admission and visibility by:

- Reporting endpoints that establish client/server connections.
- Reporting information used to evaluate the **Traffic seen** host property.

Active Endpoint Management Using the Port Monitoring Interface

Typically the port mirroring implementation includes a response interface in addition to a passive monitoring interface. This allows Forescout 8.1 to inject packets into the data stream to support sophisticated management and threat detection features.

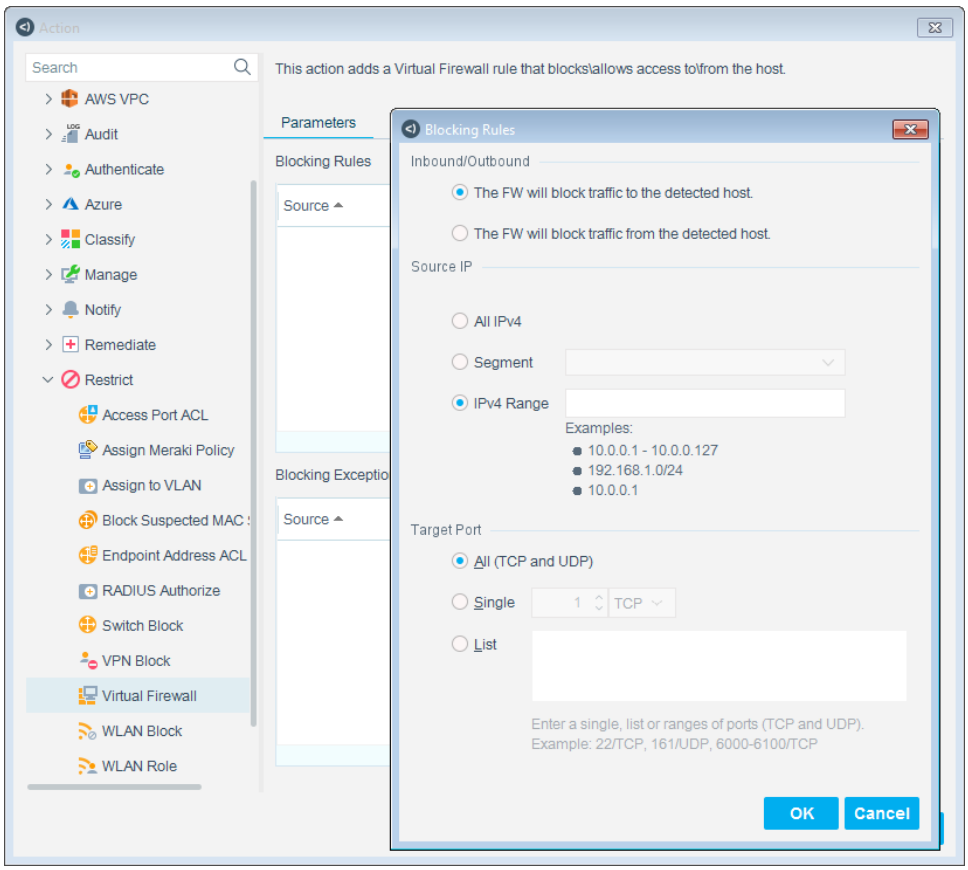
Virtual Firewall

The Virtual Firewall action lets you block access to and from detected endpoints with high granularity. You can define a range of addresses to block, as well as exceptions to these blocking rules.

The Forescout solution restricts access to configured network addresses by injecting TCP *reset* and UDP *unreachable* messages into sessions as they are opened.

Without the port monitoring response interface, this functionality can only be approximated using other actions that perform ACL/VLAN/WLAN reassignment, or actions that block the endpoint.

Automated, focused access management provided by the Virtual Firewall action cannot be reproduced as effectively on switches, controllers, and other network equipment to block non-compliant endpoints. This is because endpoint blocking is best performed directly at those devices.



HTTP Redirection Actions

The Forescout solution can display login, registration, or notification pages on an endpoint by injecting HTTP redirects into an endpoint's browser session. The endpoint receives and presents the served portal page before a response is received from the browsing target site.

Endpoints already managed by Forescout 8.1 can execute these actions without using the port mirroring response interface.

ActiveResponse Threat Protection and Malicious Event Detection

To detect threats and malicious events, the Forescout solution combines passive detection methods with ForeScout's ActiveResponse threat protection technology. Typical methods implemented by the Packet Engine include:

- detection of behavior patterns such as port scanning
- injection of test messages similar to Nmap diagnostics

These advanced techniques leverage the broad-spectrum detection and timely response that is only possible using port mirroring and the Packet Engine.

Data Retention and Purging

Only resolved property values from parsed fields are retained.

The following traffic data is not retained:

- All unparsed traffic
- All unparsed data
- All raw data used to resolve properties
- All credentials

Typically, raw values from parsed fields are processed to evaluate host properties. In many cases, input from several data sources is used to resolve a property value, which adds another layer of abstraction.

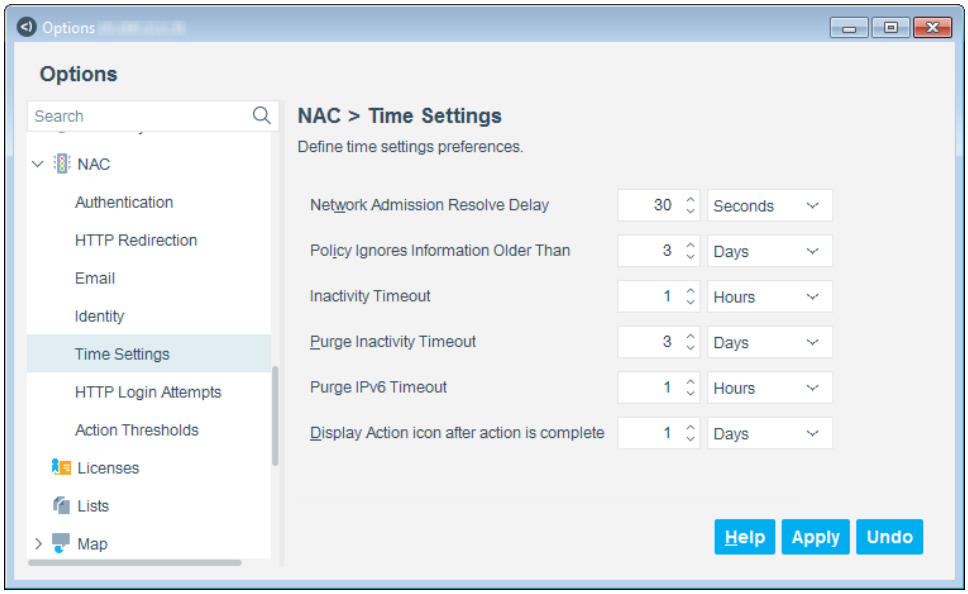
This means that raw data is not always retained 'as is' in host properties.

The raw values observed in message packets are discarded once the property evaluation process concludes. Only the final host property value is retained. For example, when the host property is a Boolean value, the original observed value is discarded after logical resolution of the property to *True* or *False*.

By default, malicious traffic is not retained. When ActiveResponse features are activated, administrators can optionally enable a FIFO buffer of intercepted malicious messages for threat tracking and review.

You can control data retention by configuring endpoint lifecycle timeouts. The Forescout Console provides configuration settings that determine the validity

period and purging behavior for endpoint information learned from the Packet Engine and other sources.



You can retain data related to malicious activity. An optional configuration setting saves records of malicious activity detected by ActiveResponse features.

Optimization and Considerations

For Packet Engine performance optimization and considerations, refer to the ForeScout Packet Engine Configuration Guide.

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).