ForeScout

Port Mirroring in CounterACT®

CounterACT Technical Note

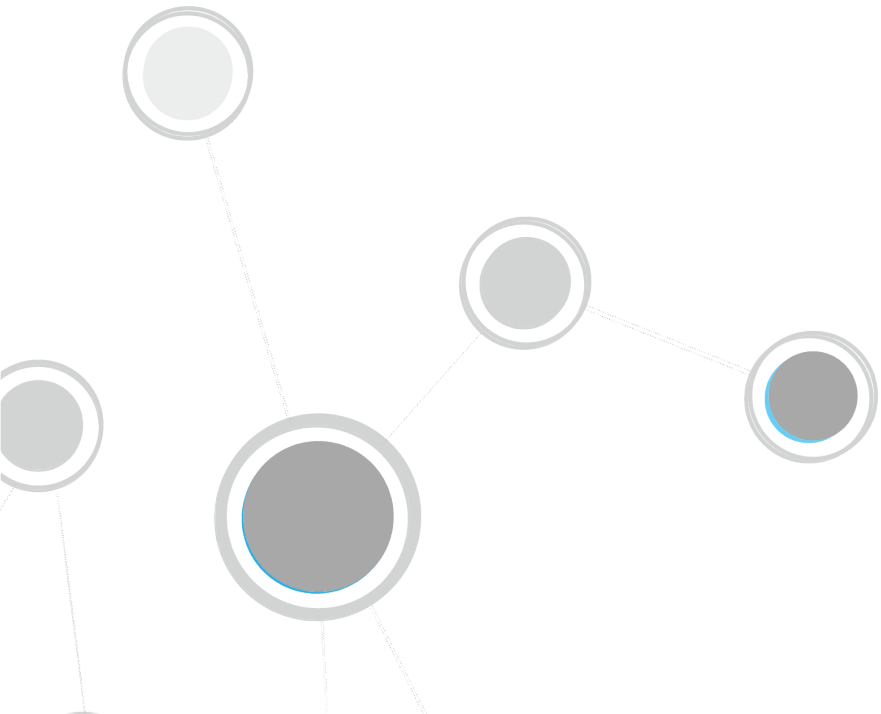


Table of Contents

About Port Mirroring and the Packet Engine

The ForeScout CounterACT® solution is distinguished from other network access, security, and management tools by providing unprecedented network visibility. To support this visibility, CounterACT is deployed to allow real-time port mirroring in the network.

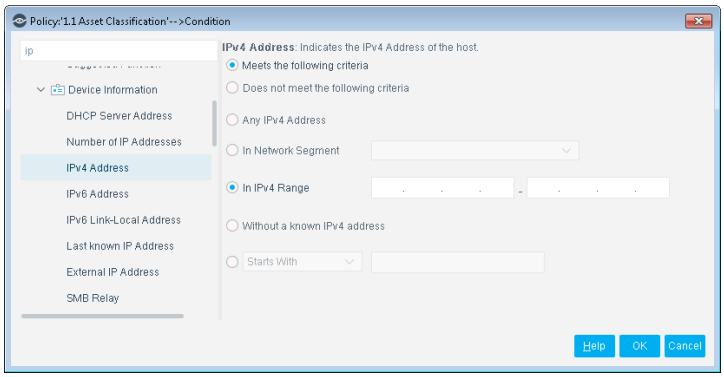
Port mirroring – known in Cisco networks as Switched Port Analyzer (SPAN) configuration and in 3COM networks as Roving Analysis Port (RAP) configuration – allows CounterACT to directly monitor traffic in the network. This supplements other methods and sources that CounterACT uses to learn information from the network, such as the NetFlow plugin, the Switch plugin, the DHCP Classifier plugin, and the DNS plugin.

The Packet Engine is the software component of CounterACT that parses and analyzes mirrored data, and injects management communication into the network.

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 first query
- Passive learning of configuration settings, installed applications, and other endpoint properties
- Detection of NAT behavior, spoofing, port scanning, and other suspicious or malicious behavior patterns.
- Support for active management using injected messages for virtual firewall enforcement and HTTP session redirection.

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



Some of the actions CounterACT can implement also require monitoring of network traffic. These actions are implemented by parsing session establishment interactions on the network, and by injecting packets into the data stream.

This document provides an overview of the messages that the Packet Engine selects from the mirrored traffic and parses to discover endpoints and 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 CounterACT host properties. Protocols analyzed by the packet engine include:

- ARP
- DHCP
- HTTP
- NetBIOS
- TCP/UDP

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 CounterACT by other sources, such as the HPS Inspection Engine and other plugins.

ARP tables on switches are queried extensively by the Switch Plugin, a core plugin of the system. See the CounterACT Administration Guide *and the* Switch Plugin Configuration Guide*.*

CounterACT 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, the response interface should *not* be configured as IP Layer. Refer to the section on working with Appliance channel assignments in the *CounterACT Administration Guide* for more information.
  - Your network should be set up to hear ARP traffic on VLANs.

  - The CounterACT device should be configured with an IP address per monitored VLAN.

ActiveResponse™ Threat Protection

CounterACT injects targeted ARP replies, structured to detect malicious scanning in the broadcast domain.

- This feature is enabled when the Appliance operates in Full Enforcement mode. See the *CounterACT 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 CounterACT processes.

- Information is reported in the following host properties:
  - Admission
  - DHCP Request
  - MAC Address
- The optional DHCP Classify 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

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, CounterACT can detect and classify NAT devices.

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

  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

This ForeScout 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. See the *CounterACT Administration Guide* for more information.

- Data payload is not parsed.

NetBIOS

Benefits

- Crucial for 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 the HPS Inspection Engine or the Macintosh/Linux Property Scanner 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, to allow 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 protocol messaging to detect sessions as they are established, and to determine which entity acts as client and which acts as server.

Parsed protocols include:

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

- Information is reported in the **Sessions as Server** and **Sessions as Client** host properties. When specific authentication servers are defined in CounterACT, 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 NetFlow Plugin.

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

- Information is reported in the **Open Ports** host property.
- Data payload is not parsed.
- Account credentials are not parsed.
- The HPS Inspection Engine and Macintosh/Linux Property Scanner Plugin may report partial port information on managed endpoints. These plugins may 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 NetFlow Plugin.

Endpoint Lifecycle

CounterACT 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, including the following protocols:

ARP	HTTP
DHCP	TCP/IP

- 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, and other data sources.

Endpoint Visibility in CounterACT 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 CounterACT.

When NetFlow reporting is enabled in the network environment, the optional NetFlow 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 CounterACT to inject packets into the data stream to support sophisticated management and threat detection features.

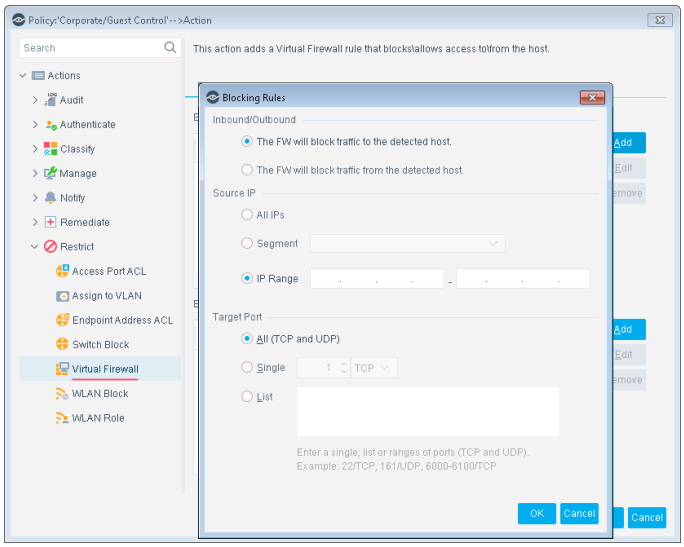
Virtual Firewall

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.

CounterACT 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.

Because the detailed configuration of switches, controllers, and other network equipment to block non-compliant endpoints must be performed directly at those devices, the automated, focused access management provided by the Virtual Firewall action cannot be reproduced as effectively.



HTTP Redirection Actions

CounterACT 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 a portal page served by CounterACT before a response is received from the browsing target site.

Endpoints already managed by CounterACT can execute these actions without use of the port mirroring response interface.

ActiveResponse Threat Protection and Malicious Event Detection

To detect threats and malicious events, CounterACT 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, and 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

CounterACT retains data from parsed traffic as follows:

Unparsed traffic and all unparsed data, credential, and other fields are not retained.

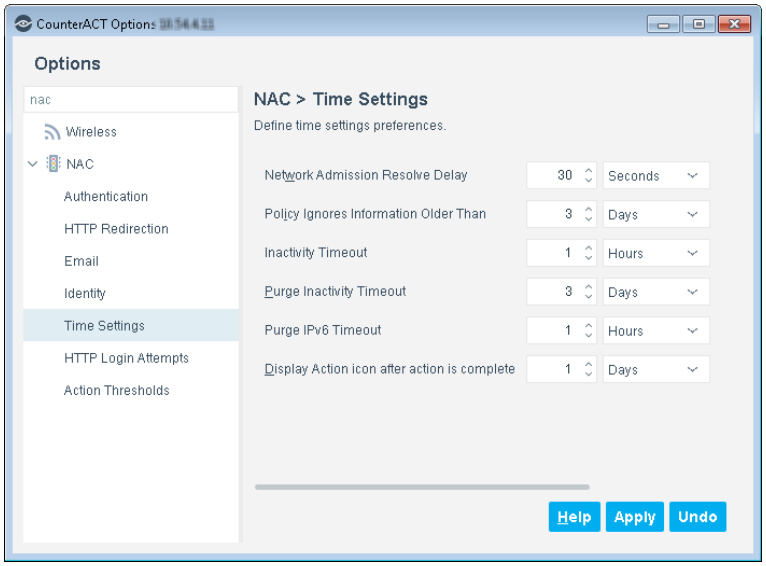
For parsed fields, CounterACT retains resolved values, not raw data. Typically, raw values from parsed fields are processed to evaluate host properties. In many cases input from several data sources is used to resolve a property value, which adds another layer of abstraction.

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

CounterACT discards the raw values observed in message packets once the property evaluation process concludes, and retains only the final host property value. 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 CounterACT 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 relating to malicious activity.
An optional configuration setting saves records of malicious activity detected by ActiveResponse features.

Legal Notice

2018-04-10 09:21