Integrating Juniper Networks Devices and ForeScout CounterACT® - Wired Post-Connect Deployment

Deployment Guide

August 2017

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Table of Contents

Introduction

This document will describe how to deploy Juniper Networks devices with ForeScout CounterACT® using their post-connect deployment on wired networks, including design considerations, requirements and an overview of CounterACT operation within this specific methodology.

Audience

This guide is intended for security managers, architects, designers and other security professionals. It can help you determine how best to implement a CounterACT network visibility and access control strategy for your organization, and assumes you are familiar with the following basic concepts:

- The 4 Cs of CounterACT policies
  - Classification
  - Clarification
  - Compliance
  - Control
- Physical CounterACT deployment architectures
  - Centralized
  - Distributed
  - Hybrid
- CounterACT deployment phases
  - See
  - Control
  - Orchestrate
- CounterACT endpoint inspection and management
  - Remote inspection
  - SecureConnector™
- Common data center network model concepts
  - Core layer
  - Distribution layer
  - Access layer

For more information on these concepts, visit https://www.forescout.com/products/counteract/.

About Wired Post-Connect Deployment

Wired post-connect deployment of ForeScout CounterACT is a network visibility and access control strategy in which endpoints are initially allowed access to the network while CounterACT profiles them to determine ownership and compliance. Access to the wired network is then adjusted based on profiling results and security policy.

Advantages of This Approach

Optimal user experience and productivity

Because endpoints are granted initial network access during the profiling process, this approach minimizes the impact on user experience. Avoiding on-boarding delays in user access to network resources also helps maintain productivity for your organization.

Ease of deployment

A post-connect deployment generally involves less pre-configuration of network devices and reduces some of the strain on operational staff. Pre-connect environments and 802.1X configurations are not required.

Network access control fails open

A post-connect model implies initial trust when an endpoint first connects to the network. If connectivity to CounterACT is lost—by a single site or by the entire enterprise network—endpoints retain normal access to network resources.

Gradual rollout

A post-connect model allows more flexibility during deployment, and simplifies the transition from “See” to “Control”; CounterACT can first acquire full visibility of endpoints on the network, then enforcement actions can be overlaid incrementally as environmental readiness increases.

Because endpoints are not initially restricted, CounterACT can be deployed before your access control strategy is developed, to determine what types of devices are connecting to the network. Access controls can then be configured for specific device types and enabled separately in stages. Your security team can better focus on appropriate strategies for specific device types, as well as the desired conditions for and types of controls to use.

Challenges of This Approach

Time to enforcement delay

The initial trust implicit in a post-connect model means that a potentially threatening endpoint will be allowed on the network for a brief interval while CounterACT completes its profile and discovers the need to restrict access. This interval can vary depending on your organization’s CounterACT policy flow, and your security policy, which dictates what is allowed on the network and what is not.

Policy Flow

Basic policy flow concepts are at the core of CounterACT policy methodology, and it is important to understand how different deployment approaches affect the flow of a policy. This section covers these concepts as they pertain to a wired post-connect scenario. Before an endpoint is subjected to a policy, and before CounterACT profiles a device it has not previously seen on the network, there is a built-in, configurable, 30-second delay. This allows time for systems to fully boot and return accurate external profiling results.

Classification

Classification is the first CounterACT policy to which endpoints are subjected. In a post-connect model, it is particularly important to follow best practices for a clean and efficient classification policy, as this strongly

affects the eventual time to control. Because classification sets the stage for the rest of the policy set, speed is important, but accuracy is essential.

Clarification

Non-manageable systems that are recognized corporate endpoints (VoIP phones, printers or IoT devices) typically end their policy flow here. They may either retain normal network access or have their network access restricted to only what is operationally necessary. Managed corporate devices are further checked for compliance policies and non-corporate devices are redirected to Guest/BYOD flows.

Compliance

Devices that are deemed compliant typically end their policy flow here, retaining network access as normal. Those deemed non-compliant can have remediation actions applied to them that essentially automate many security policies. Those that fail remediation or are exempted from remediation by policy are passed to control policies.

Control

At this stage devices are removed from the network, quarantined, or otherwise restricted as required by their circumstances or conditions. The types of controls available are primarily dictated by the capabilities of your organization's switch framework and CounterACT's level of integration with those devices.

Best practice for control policy implementation is to have policies configured during initial deployment, but with their enforcement actions disabled. This provides time for your security and operations teams to determine what endpoints will be restricted by a policy, whether to refine the policy accordingly, and what endpoint issues need to be fixed. To optimize the end user experience during CounterACT deployment, control actions should only be enabled after policy testing, with notification-only actions for both users and IT personnel, allowing time for endpoint issues to be resolved.

Timing the control decision

There are various approaches to moving a device off the assessment VLAN and onto a production network. Access can be awarded (or denied) as soon as the clarification assessment is complete, delayed until compliance assessments are complete, or provisionally allowed at some point in between. Making the move immediately after clarification expedites user access to network resources and optimizes productivity. Waiting for full compliance makes the process more secure, because systems are not allowed on a production network without being checked for potential risks. Compliance policies can be included as requirements for movement off the assessment VLAN, and many organizations opt for a practical, intermediate stance that balances security and user experience.

Integration with Juniper Networks Devices

CounterACT integrates with Juniper Networks EX Series switches, QFX Series switches, and SRX Series Services Gateways.

Various methods are used individually or in combination, including SNMP, CLI, and NETCONF. Allowing CounterACT read/write access with all management methods results in the most efficient use of resources when gathering data, and the widest range of potential endpoint control options. This section describes how CounterACT will interact with your organization's switch framework, including the options available for endpoint access control.

Switch Integration Basics

Three capabilities become important in a wired, post-connect environment:

1. the ability to quickly detect a device entering the network,
2. the ability to map IP and MAC addresses together, and
3. the ability to attribute a MAC address to a specific switch port.

The speed at which these functions occur will play a major role in how quickly CounterACT will discover the switch port to which an endpoint has connected, which is necessary for control action application.

Data Gathering

CounterACT uses SNMP, CLI, NETCONF, or a combination thereof to gather data from an organization's switch framework, including routers and firewalls.

MAC tables

CounterACT gathers MAC tables from access layer switches and from other devices where endpoints are connected or may connect. This is done at a default interval of 60 seconds (configurable per switch).

ARP tables

CounterACT gathers ARP tables from network devices that contain ARP information, including switches, routers, and firewalls. This is done at a default interval of 600 seconds (configurable per device), and is required for CounterACT to map an endpoint's IP address to a MAC address. The combination of the MAC and ARP table information tells CounterACT the physical switch port to which an endpoint is connected, allowing it to place access controls on that port.

Initial Detection

CounterACT sees real-time endpoints as real-time IP addresses. An endpoint without an IP address cannot be inspected, and thus cannot be evaluated by policy. In essence, the challenge of initial detection is in how quickly CounterACT can find an IP address when a device joins the network.

ARP table queries

Initially, CounterACT discovers IP addresses by querying ARP tables through its core integration with switches and other network devices. This provides both the IP and MAC address for endpoints whose traffic is routing throughout the network, and achieves both initial detection and IP-to-MAC address mapping. These tables and values are rechecked once every 600 seconds by default. This value should be increased if Expedite IP Discovery (described later in this section) is enabled, or decreased if the network device being queried has the resources to support a shorter interval. Because of the 600-second gap between queries, CounterACT employs additional methods which serve to supplement initial discovery, identifying IP addresses on a more immediate basis. For more details on discovery methods, refer to the *ForeScout Agentless Visibility and Control* white paper.

Mirrored traffic monitoring

CounterACT's initial discovery process can be enhanced by using common switch vendor features that enable mirrored traffic monitoring. This also provides CounterACT with several extra capabilities that can be helpful in a wired post-connect scenario, and for this reason, allowing CounterACT to monitor mirrored network traffic is considered best-practice design. These benefits include:

- Packets sourced by an IP address that are not currently known by CounterACT trigger an admission event, achieving initial detection
- Actionable, session-based properties can be created so that CounterACT can monitor and take action on network behaviors
- Threat Protection watches for network probing and can create virtual systems to bait and confirm malicious behavior, creating an actionable property on the attacking endpoint
- HTTP redirection allows CounterACT to force endpoints to a captive portal for any purpose
- ForeScout Virtual Firewall (vFW) technology enables CounterACT to block systems at Layer 4 through the use of TCP resets

Switch Port Detection

Switch port detection begins with the knowledge of what MAC addresses are connected to which switch ports. For CounterACT to know the switch port to which an endpoint is connected, it must constantly communicate with your organization's switch framework to remain apprised of ongoing changes in MAC address connectivity.

MAC table queries

Through its core integration with Juniper devices, CounterACT queries MAC address tables on the devices at a default interval of 60 seconds. This value may be increased if SNMP traps are in use, or decreased if they are not available and a switch can support more frequent queries.

SNMP traps

Using SNMP traps is considered best practice in wired post-connect design. The fastest way for CounterACT to stay on top of changing connections in a switch framework is to receive either MAC address notifications or linkUp and linkDown SNMP traps from the Juniper switches. This provides instant change notification.

IP-to-MAC Address Mapping

When CounterACT knows the MAC addresses on the switch framework and it detects a new IP address, all that remains is to associate the unknown IP address to a known MAC address. At a basic level, this is accomplished by querying ARP tables as discussed in previous sections. Other methods exist to expedite this process, and are discussed below.

DHCP fingerprinting

A common way to associate IP addresses with MAC addresses is by viewing both sides of a DHCP conversation, which requires mirrored traffic monitoring. In each request, the connecting system announces several properties that CounterACT policy can use, including device- and OS-specific information, along with its MAC address. The reply provides the IP address to which the connecting system has been assigned, allowing CounterACT to correlate these addresses simultaneously with the endpoint itself.

Expedite IP Discovery

Developed specifically to eliminate the challenge presented by the 600-second default interval for ARP table queries, this feature allows you to use CounterACT to configure Juniper devices in connectivity groups. When CounterACT discovers a new MAC address within a connectivity group, it interrogates other group devices that are configured for ARP table queries. The switch containing the relevant ARP table will aggregate requests within a configurable 10-second interval, helping to reduce the potential time to obtain this information. Expedite IP Discovery helps accelerate IP address collection by creating a targeted, as-needed discovery process.

Switch Port Controls

Switch integration affords CounterACT several endpoint control options, at multiple layers of the OSI model.

Layer 1 controls

Switch block – The switch block action shuts a port off, effectively severing communication over the wire as if the network cable were disconnected. While it is available for Juniper switches, this control is not optimal due to its simple on-off nature, and is typically used only when no other options exist. CounterACT must re-enable a port periodically to see if the unwanted endpoint is still connected, so a port may be disabled even after the unwanted endpoint has disconnected. Also, logs reporting endpoints' disconnect times will be inaccurate, reducing their forensic usefulness. This action is best used only when total network restriction is necessary, or when no other options are available.

Layer 2 controls

MAC ACL – With Juniper switches, this control causes a switch to drop Ethernet frames from the blocked

device right at the network edge, while retaining visibility of the device's connectivity for release of the action when the device disconnects. This control is best used in any scenario where the desired effect is to completely remove an endpoint's network access.

Assign to VLAN – This control is commonly used in a post-connect deployment model to move non-compliant devices to a restricted or quarantine VLAN. These VLANs must be pre-configured, and CounterACT must manage their IP address space. This control is best used on networks where a robust, properly segmented VLAN infrastructure is already in place, where only one device is assigned to each switch port, or where the use of DNS enforcement for redirection is necessary.

There are additional considerations for the Assign to VLAN control in two common special cases:

VoIP VLANs – When a switch configuration uses a voice VLAN and data VLAN on a single port, CounterACT will reassign the data VLAN, presenting a unique challenge. Affected endpoints won't recognize the switch port change, and in turn they won't request a new IP address for the data VLAN. Therefore, as part of the normal VLAN change process, CounterACT will disable and re-enable the port. The endpoint sees the connection go down and requests a new IP address on reconnect. Connected devices utilizing PoE, such as a VoIP phone, will lose power temporarily.

This issue can be overcome by using SecureConnector, CounterACT's optional software agent, which can directly force an endpoint to renew its DHCP lease.

Null VLAN – A null VLAN is a specific, near-connectionless VLAN configured for endpoints that should not be on the network, creating a full quarantine without resorting to the switch block action. This concept is best implemented where MAC ACLs cannot be used.

Layer 3 Controls

IP ACL – This control gives CounterACT the ability to dynamically regulate granular access controls specific to a blocked endpoint without the need to pre-configure VLANs. It can be used to drop some IP packets right at the network edge, effectively creating a dynamic, endpoint-specific quarantine that can be tailored to a specific non-compliance issue. As a Layer 3 control, it allows endpoints to continue passing Ethernet frames, so it is best used for compliance- based actions or when dynamic network segmentation is desired among known internal assets.

Layer 4 Controls

Virtual Firewall (vFW) – This feature, which requires CounterACT to see mirrored network traffic, resets TCP traffic and attempts to terminate any UDP traffic by sending a "destination host unreachable" result to the sender. It does not require switch management. vFW is often used as a best-effort block where a switch port cannot be directly modified. This should be treated as a fallback option when no other control method is available.

Summary

Before CounterACT can control the endpoints connecting to Juniper devices, it must first manage the devices themselves. In a post-connect model, the speed at which CounterACT can identify the switch where an endpoint connects strongly affects the length of time a potential threat remains online. The functions of discovering an endpoint's IP address as it comes online, mapping that IP address to a MAC address, and knowing to which port the MAC address connects all contribute to the output of this equation. Ideally, the entire process should take no more time than is required to evaluate an endpoint against policy and determine whether it poses a potential threat. Finally, the control methods used and the strategy for deploying them should be aligned with the capabilities of the switches themselves, the security goals of the organization, and the end user experience impacts they may impose.

Notifications and Redirects

Because post-connect methodology begins with network access and restricts only after inspection, it becomes possible to notify users of actions being taken on their endpoints simultaneously, prior to or in place of enforcement. These actions assist in the deployment of CounterACT across the enterprise by

ensuring that users at various levels are informed of new security policies as they are implemented. Best practice is to have all control policies first utilize notification actions during initial rollout rather than control actions, changing to control actions as environmental and user readiness dictate.

Email Notifications

CounterACT can send email notifications based on policy rules or sub-rules to users or groups using custom messages and including detected endpoint properties, inspection results, policy results, or switch information. This powerful ability puts precise, actionable knowledge into the correct hands.

Managed Systems

CounterACT provides multiple options for direct notification of devices under its management to inform users of upcoming actions to address non-compliance or other endpoint conditions. These include:

- Opening a Web browser to any address
- Opening a balloon or banner notification with SecureConnector
- Sending an email to the logged-in user

Unmanaged Systems

Because CounterACT cannot take direct action on endpoints that it does not manage, external methods of notification must be used. CounterACT can intercept a device's network traffic in two different ways.

Redirects

The most efficient way to intercept, and therefore redirect, traffic is through CounterACT's native ability to monitor mirrored traffic. CounterACT can redirect traffic from a target endpoint to either a URL on the CounterACT appliance itself, or to a URL on another system. In this way the endpoint's Web-based traffic is initially funneled to a captive portal, a method frequently used to force guest systems through a mandatory registration process as they connect.

DNS enforcement

DNS enforcement was developed to overcome a limitation inherent in HTTP redirection—the inability to see network traffic in some locations. This method requires that CounterACT be the endpoint's primary DNS server. It responds to target endpoints, showing itself as the DNS result for queries, forcing the endpoint to an internal Web site and effectively forcing it through a captive portal. Potential challenges associated with having CounterACT function as the primary DNS server on a network can be overcome in various ways:

- CounterACT can forward DNS queries to another server by default
- CounterACT can respond with an "unknown" result, forcing the endpoint to the secondary DNS server
- Target endpoints can first be moved into a dedicated VLAN where CounterACT is the primary DNS server
- CounterACT can take a tertiary or later DNS server position, and an ACL can be applied to a target endpoint's switch port, denying it access to the typical DNS servers.

Summary

The primary method used to inform IT staff of access control actions is email notification. Managed systems can be directly controlled to affect internal user notification, and unmanaged systems can be redirected either through HTTP redirect or DNS enforcement to achieve external user notification. Using notifications both before and after control actions are enabled raises security awareness at all levels and plays a key role in ensuring a smooth CounterACT deployment.

Solution Architecture

Figure 1 depicts a typical hybrid deployment, providing a basic overview of how CounterACT interfaces with other networking devices.

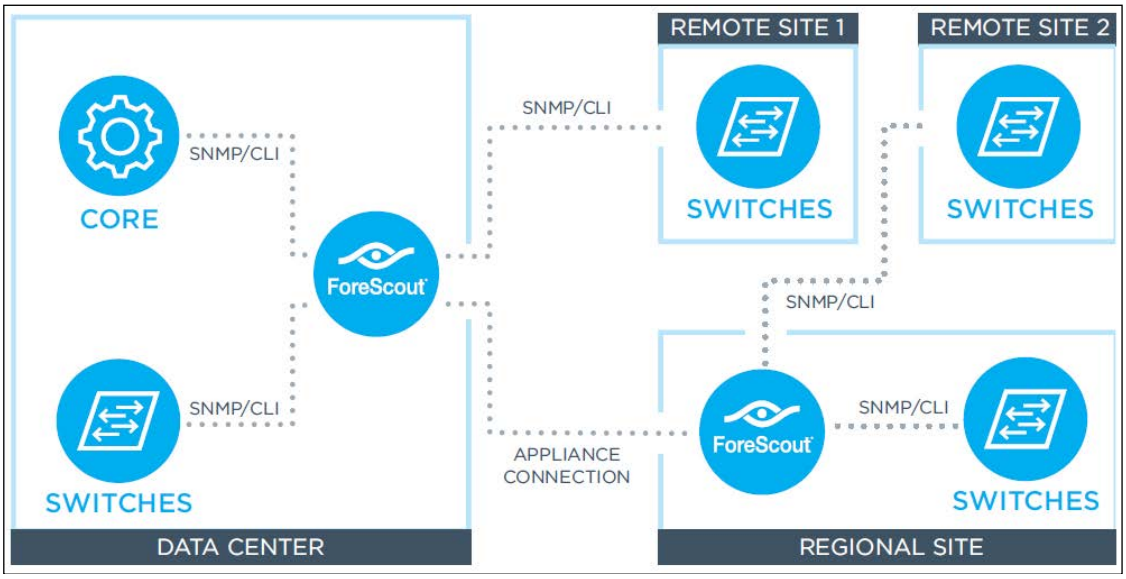

Figure 1: CounterACT communication with network devices

Workflow Diagrams and Flowcharts

Sample Policy Flow

Figure 2 depicts a typical high-level flow of the basic CounterACT policy set, showing an endpoint connecting to the production network and the circumstances under which it may be removed.

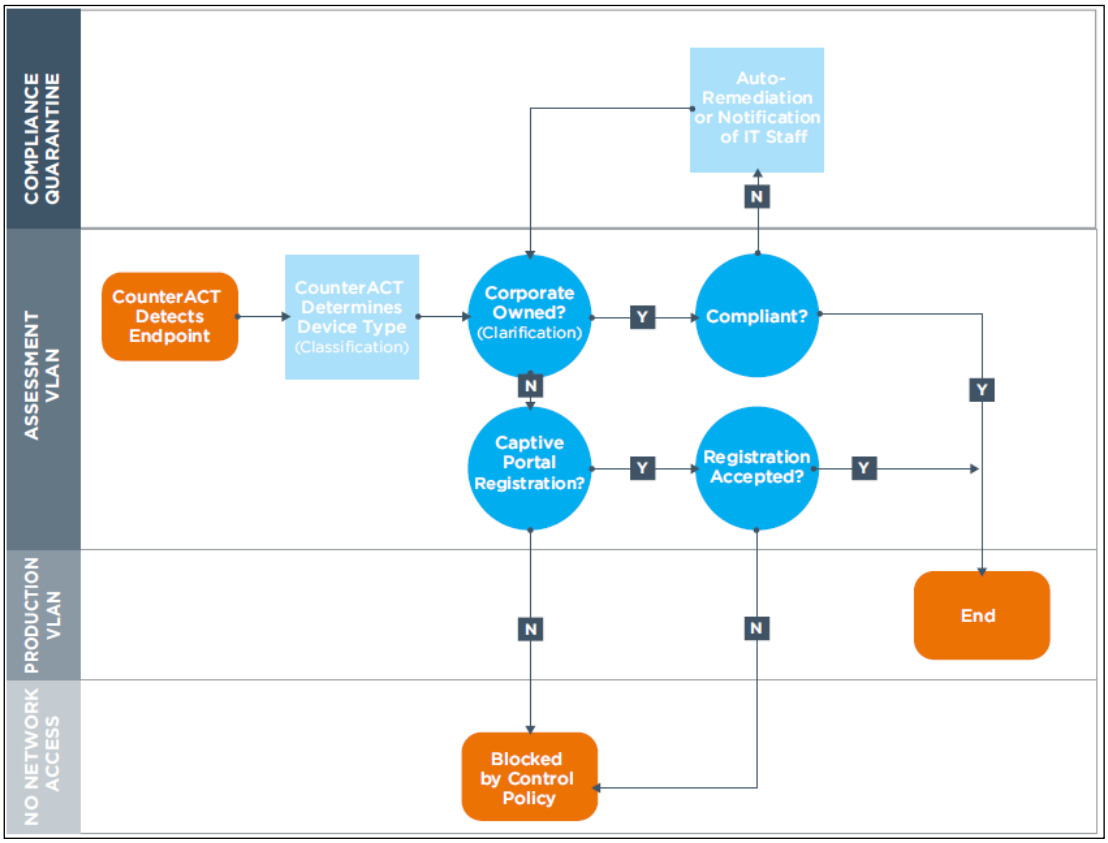

Figure 2: A sample wired post-connect policy flow

This policy flow shows a sequence in which CounterACT first detects a new endpoint connecting to the network, and then determines the device type (classification). Next, the clarification policy stage determines whether the device is owned by the organization, in which case it is passed on to compliance assessment and remediation (or IT staff notification) if necessary. Guest and BYOD devices are checked for registration credentials and either connected to a limited-access subnet or blocked (denied access). A guest registration process is available with CounterACT as shown in this example, but guest registration is not unique to wired post-connect deployments and not covered in this document.

Switch Communication

Figure 3 illustrates a sample communication sequence between CounterACT and a network switch framework as a new endpoint joins the network, is inspected and evaluated by CounterACT, and is subjected to an access control action. SNMP traps are configured on the access switch in this example.

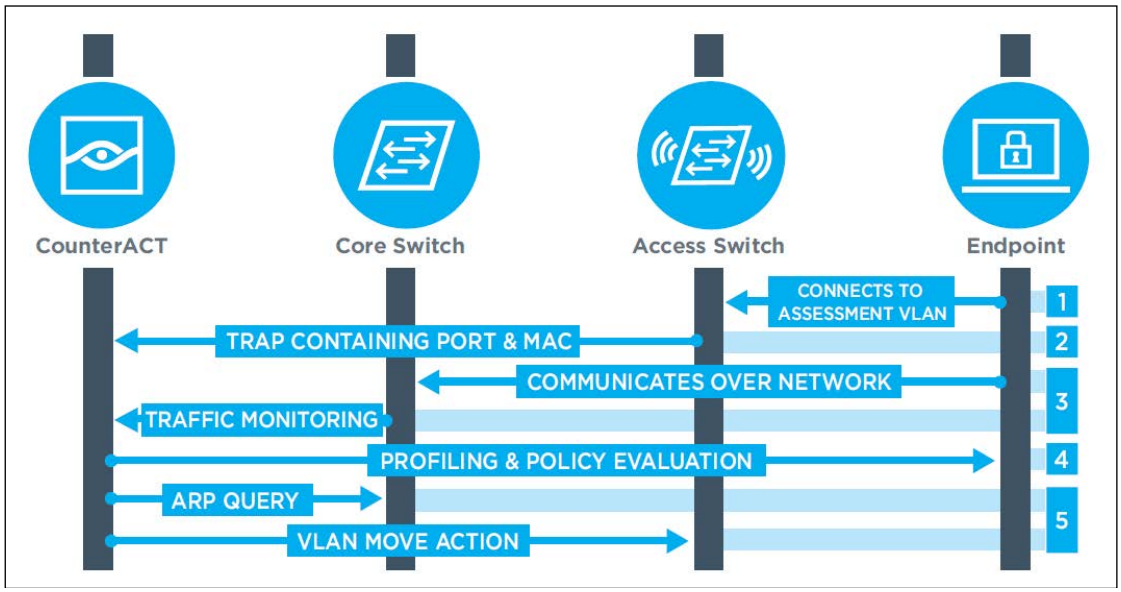

Figure 3: A sample CounterACT control flow

The sequence of events and communications in this example is as follows:

1. An endpoint connects to an access switch port.
2. The access switch sends an SNMP trap to CounterACT, which is now aware of a new MAC address online and the port to which it is connected.
3. The endpoint communicates through the network and the core switch sees its traffic.
4. CounterACT monitors mirrored traffic from the core switch and sees the endpoint's IP address.
5. CounterACT profiles the endpoint's IP address to determine what it is, and begins policy evaluation to ascertain ownership and compliance.
6. Simultaneously, CounterACT queries the relevant ARP table residing on the same or a separate network device using Expedite IP Discovery, mapping the known MAC address and switch port to the IP address that is being profiled.
7. CounterACT places a control action on the switch port, provided the endpoint falls within an active control policy.

Environment Requirements

This section provides an overview of what must be in place for the wired post-connect scenario to operate successfully within an enterprise network that includes Juniper devices.

CounterACT Requirements

CounterACT must have the ability to read ARP and MAC address tables from Juniper devices. This requires the Switch plugin, a core component that is supplied with a basic CounterACT installation. The Switch plugin, together with the DHCP Classifier plugin, can effectively profile endpoints. Details of the DHCP plugin can be found in the help file.

The latest release should always be used to ensure that the full range of features is available. Each Juniper device must be added into the plugin, a process that is covered in more detail later in this document.

Customer Environment Requirements

When integrating CounterACT with the existing switch framework, it may be necessary to configure the following items, depending on switch capabilities and the features required to achieve the desired outcome:

- SNMP access to all switches for queries and configurations
- CLI access to all switches for queries and configurations
- SNMP trap configuration to CounterACT to speed discovery of connecting endpoints
- Pre-configured VLANs for any network where CounterACT will be reassigning devices

Configuring CounterACT

Configuring CounterACT to interact with Juniper devices and provide controls in a post-connect model is a straightforward process. Configuration instructions may vary with Switch plugin versions, and specific instructions are provided in the Switch plugin help file, which is accessible directly from the CounterACT management software.

The general steps to add Juniper devices into the CounterACT system are as follows:

- Enter the IP address of the device
- Select the managing appliance
  - To reduce dependencies it is best practice to, wherever possible, assign devices to the same appliance that manages the network ranges it may connect to.
- Select the vendor “Juniper” from the drop-down menu
- Enter CLI management credentials
- Enter SNMP version and management credentials
- Enter permissions
  - Enable MAC permissions when the network device contains relevant MAC tables
  - Enable ARP permissions when the network device contains relevant ARP tables
- Configure ACL settings

The CounterACT Console

Figure 4 depicts the Switch plugin configuration page, showing Juniper devices managed by CounterACT. From here you can see alerts showing configuration issues, and edit or test individual or groups of devices.

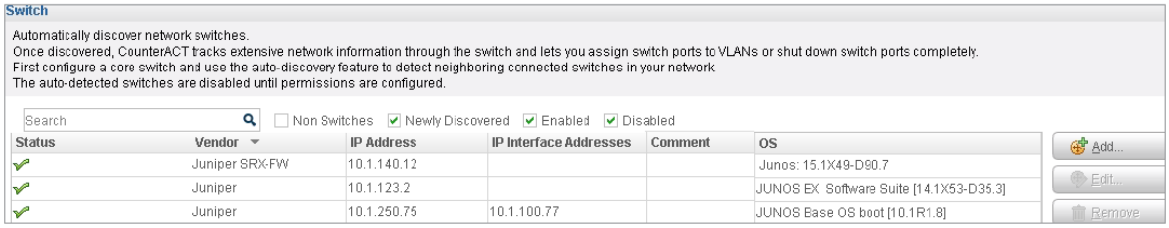

Figure 4: Switch plugin configuration screen

To add a new Juniper device, click Add. Figures 5-9 illustrate the steps you must complete, as noted above.

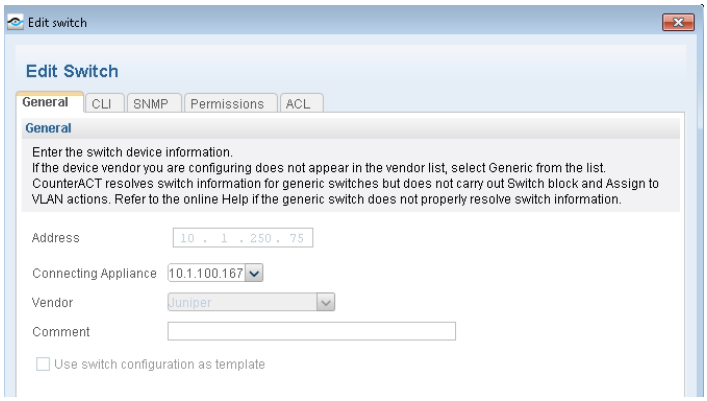

Figure 5: Device configuration - General information

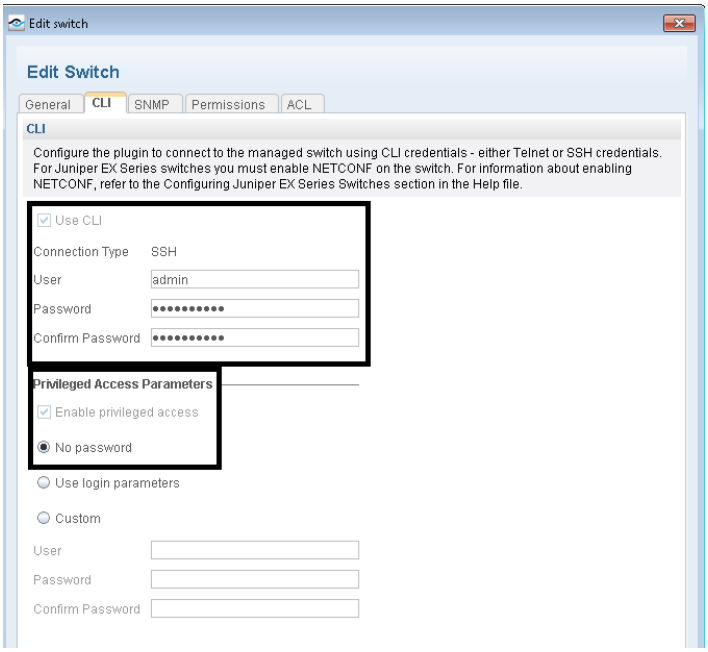

Figure 6: Device configuration - CLI information

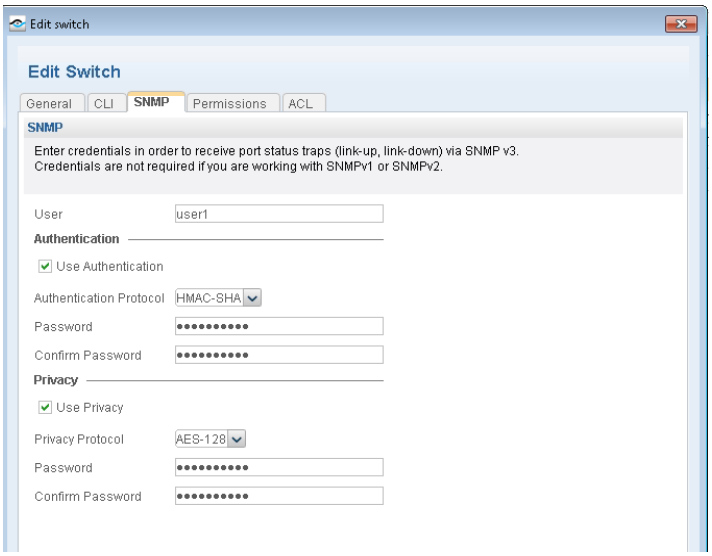

Figure 7: Device configuration (switch page shown) - SNMP information

Figure 8 shows the configuration screen for an individual switch's permissions. Each network device managed by CounterACT should have both the read and the write checkboxes selected for MAC if endpoints connect to it, for ARP if it serves as a gateway for any networks, and for both if needed. Except in rare circumstances, allowing CounterACT to automatically use SNMP, CLI, or NETCONF ensures that the most efficient method is used for the specific query or command being performed. The checkboxes on the screen, from top to bottom, do the following:

- MAC Read – Allow CounterACT to query the device's MAC table
- MAC Write – Allow CounterACT to perform blocking actions on switch ports
- ARP Read – Allow CounterACT to query the device's ARP table
- ARP Write – Allow CounterACT to clean up duplicate ARP entries

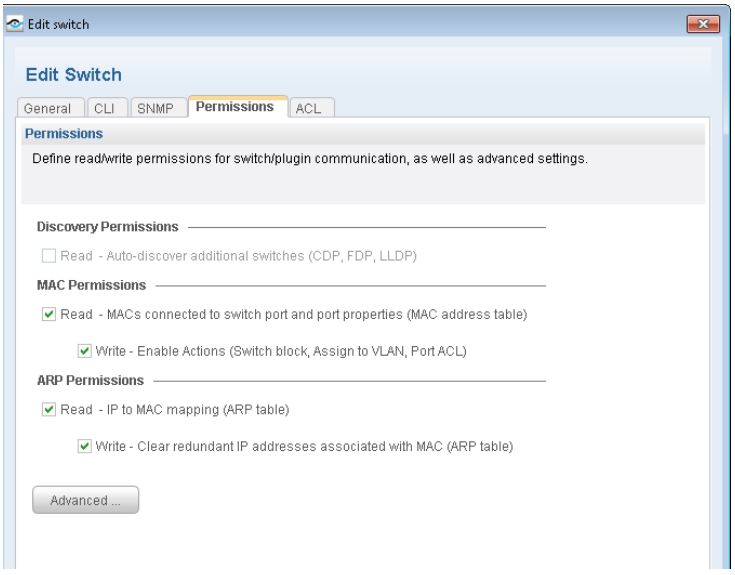

Figure 8: Device configuration (switch page shown) - Permissions

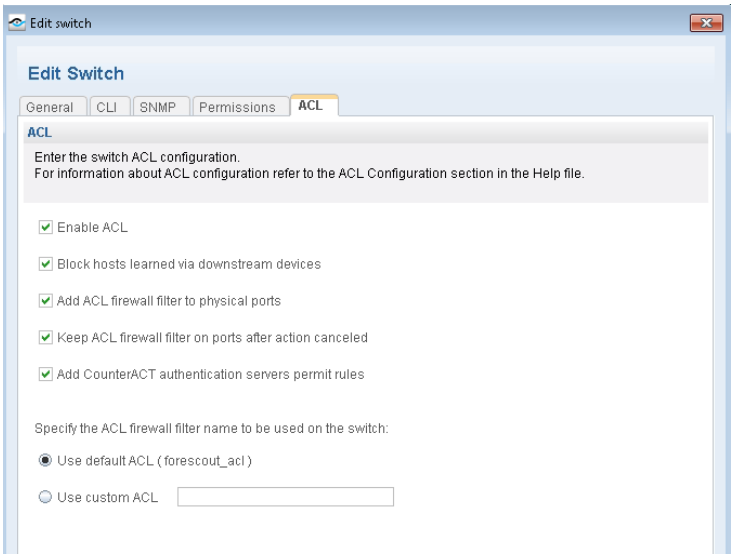

Figure 9: Device configuration (switches only) - ACLs

Configuring Juniper Devices

On all Juniper devices that will interact with CounterACT, add configuration that matches the following sample:

```
system {
    login {
        user admin {   ## must match settings entered in the CLI page sbove
            class super-user;
            authentication {
                encrypted-password "$ABC123";
            }
        }
    }
    services {
        ssh {
            root-login allow;
        }
        netconf {
            ssh;
        }
    }
}

snmp {
    v3 {
        usm {
            local-engine {
                user user1 {  ## must match settings entered in the SNMP page sbove
                    authentication-sha {
                        authentication-key "$ABC123";
                    }
                    privacy-aes128 {
                        privacy-key "$ABC123";
                    }
```

```
                }
            }
        }
        vacm {
            security-to-group {
                security-model usm {
                    security-name user1 {  ## must match username above
                        group group1;
                    }
                }
            }
            access {
                group group1 {
                    default-context-prefix {
                        security-model usm {
                            security-level privacy {
                                read-view view-all;
                                write-view write-all;
                            }
                        }
                    }
                }
            }
        }
        target-address ta2 {
            address 10.1.100.167;
            address-mask 255.255.255.0;
            target-parameters tp1;
        }
        target-parameters tp1 {
            parameters {
                message-processing-model v3;
                security-model usm;
                security-level privacy;
                security-name user1;  ## must match username above
            }
        }
    }
    engine-id {
        local 62;
    }
    view view-all {
        oid 1 include;
    }
}
```

Verifying Connectivity Status

To verify that CounterACT has proper connectivity to the Juniper devcies, use the Test button on the Switch plugin page.

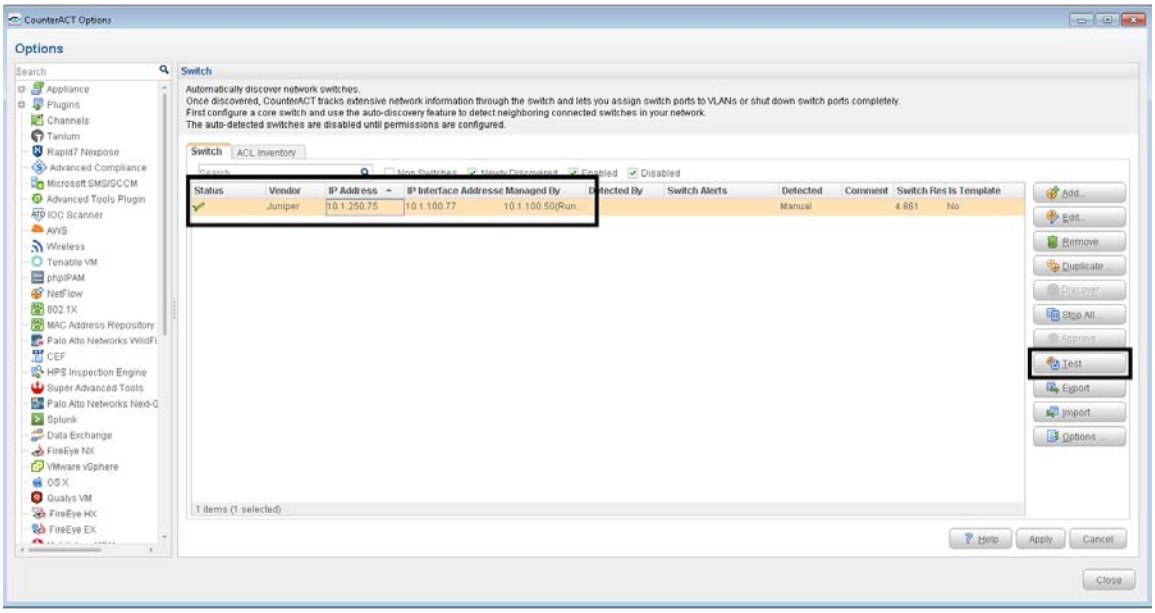

Figure 10: Test button on Switch plugin page

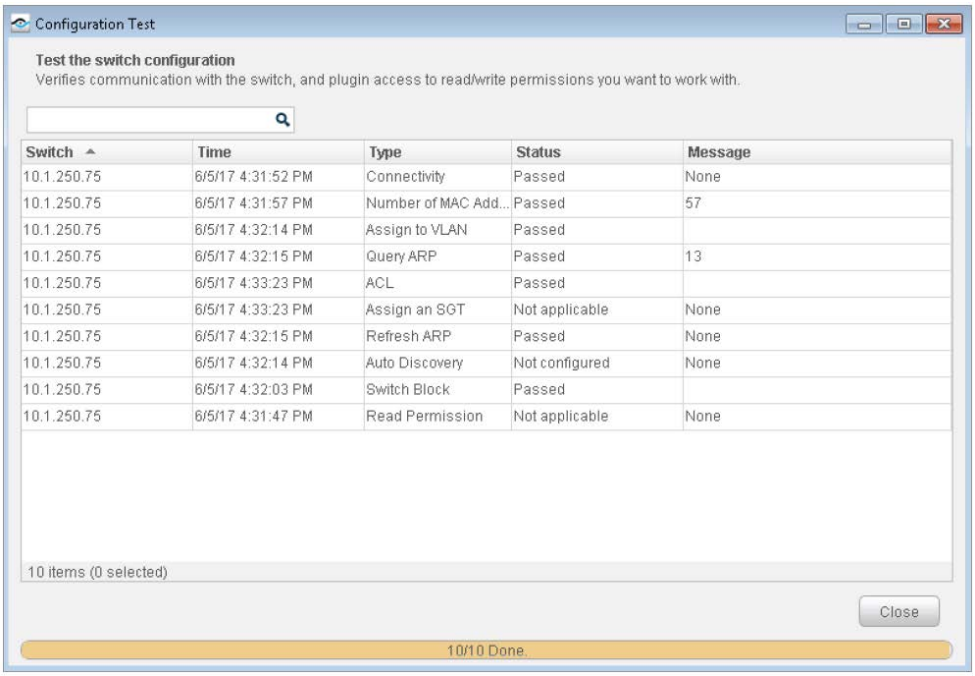

Figure 11: Test button output.

For More Information

This completes our overview of design considerations for deploying ForeScout CounterACT with Juniper devices in a wired post-connect scenario. For additional information, see the following resources:

Solution Brief: Juniper-ForeScout Joint Solution for Endpoint Visibility and Control

Product Page: ForeScout CounterACT®