Best Practices for CounterACT® Deployment: Wired Post-Connect

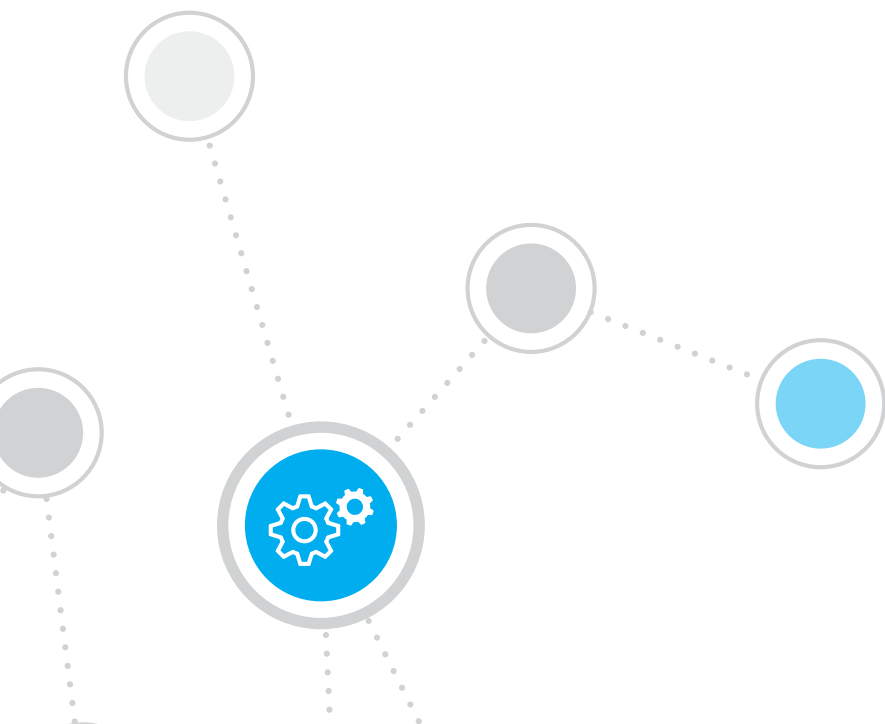# Table of Contents

Introduction

ForeScout CounterACT® deployment scenario documents provide an overview of the different approaches that can be employed when implementing CounterACT as a network visibility and access control solution, including the advantages, potential constraints and best practices associated with each approach. Our goal is to help your organization determine which approach best suits your environment and security policy. Wired post-connect is one of the various deployment scenarios supported by ForeScout. Visit http://www.forescout.com/company/resources/ for additional deployment scenario guides.

Purpose

This document will describe a CounterACT 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 C's 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

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 may help minimize impact to the user experience. Avoiding on-boarding delays in user access to network resources may help maintain productivity for your organization.

Ease of deployment

A post-connect deployment may involve less pre-configuration of network devices and reduce some of the strain on operational staff. Pre-connect environments or 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 strategy 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 non-compliant 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 passed to compliance, and non-corporate devices are passed directly to control.

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 that vendor.

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.

Switch Integration

CounterACT integrates natively with more than 25 switch vendors and provides generic integration with Linux-based systems. Depending on the vendor, various methods are used individually or in combination, including Simple Network Management Protocol (SNMP), command-line interface (CLI) and Network Configuration Protocol (NETCONF). For any given vendor, 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 an endpoint 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

Depending on the vendor, 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 will gather MAC tables from access layer switches and from other switches where endpoints are connected or may connect. This is done at a default interval of 60 seconds (configurable per-switch).

ARP tables

CounterACT will gather Address Resolution Protocol (ARP) tables from network devices that contain ARP information, including layer 3 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 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.

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 of the Open Systems Interconnect (OSI) model though the use of Transmission Control Protocol (TCP) resets

NetFlow data

In addition to monitoring mirrored traffic, CounterACT also collects Netflow data from network devices, providing another source of actionable session-based properties for use in network behavior control. Flows that show an IP address of which CounterACT was not previously aware will trigger an admission event and initial detection. Other advantages of mirrored traffic monitoring do not exist with NetFlow, however, so it is typically used only as a supplemental data source where mirroring traffic is not possible.

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 switches, CounterACT will query MAC address tables on switches 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 the switch can support more frequent queries.

Switch 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 notification or linkUp and linkDown SNMP traps from all switches. This provides instant change notification and is available with all switch vendors that CounterACT supports.

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 requests and replies

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 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 CounterACT to configure switches 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. It is available on all supported switch vendors. 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, switch logs reporting endpoint disconnect times will be inaccurate, reducing their forensic usefulness.

Layer 2 controls

MAC ACL – With vendors that support it, 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 – CounterACT's Assign to VLAN action is available on all supported switch vendors and is commonly used in a post-connect 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 – Some switch vendors can differentiate voice and normal data VLANs on a single port. In these instances, 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. The CounterACT software agent, SecureConnector™, while not required in any other circumstance presented within this document, has the ability to overcome this issue by forcing 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 – With supported vendors, 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 – 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, and there may be limitations on traffic visibility based on the availability and visibility of mirrored traffic. For example, if CounterACT is distributed to all physical locations and receives mirrored traffic at each, there is more coverage than if it is deployed centrally, within a data center, and unable to see external site traffic. If CounterACT only sees traffic that crosses the core switch, it will not see traffic that remains localized to the distribution or access layers. Virtual firewall is often used as a best-effort block where a switch port cannot be directly modified. It is not recommended as a primary control method.

Summary

Before CounterACT can control the endpoints connecting to switches it must first manage the switches 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 CounterACT to 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 website 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, showing one example of how CounterACT can interface with a switch framework.
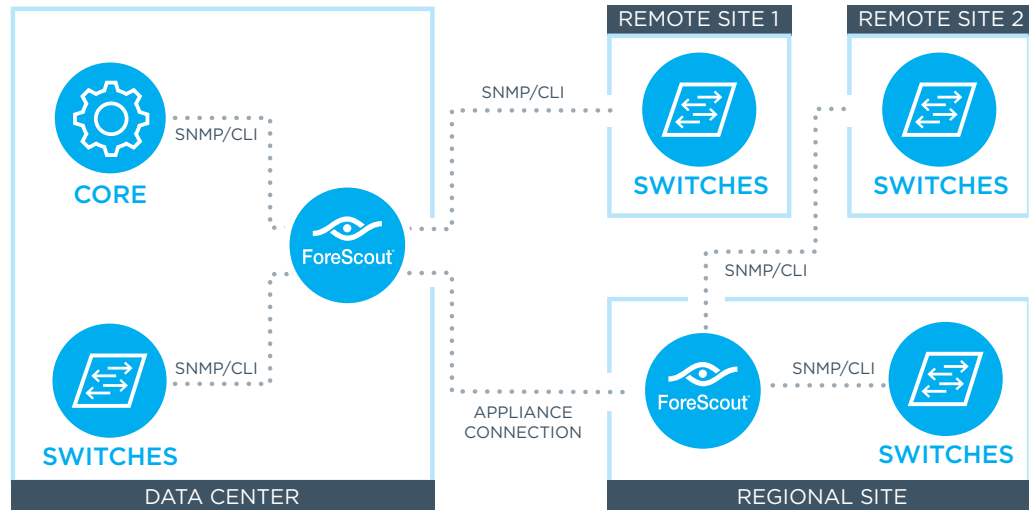

Figure 1: Switch communications.

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.
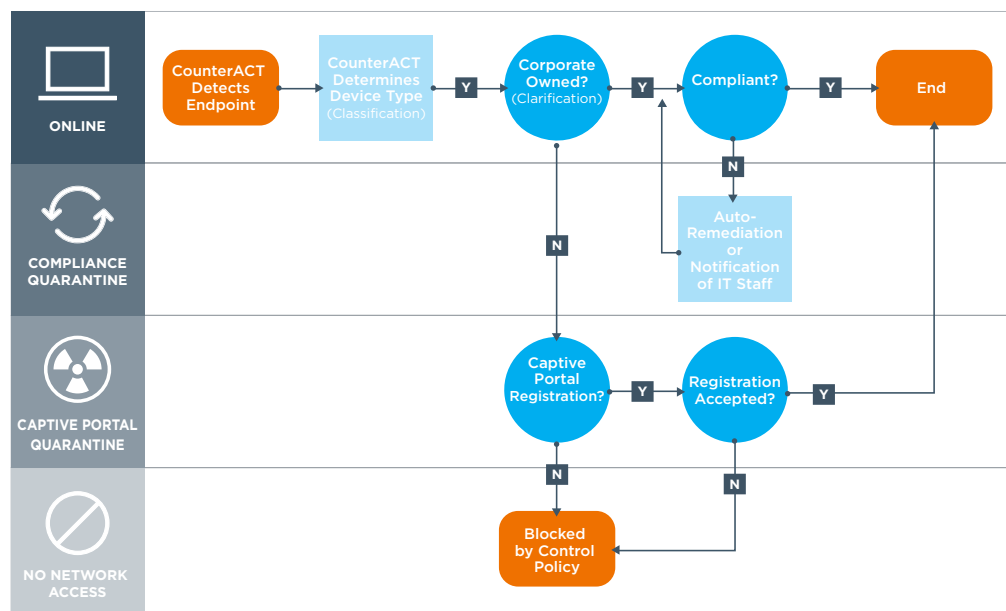

Figure 2: A sample wired post-connect policy flow.

This policy flows 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 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 subjected to an access control action. SNMP traps are configured on the switch device in this example.
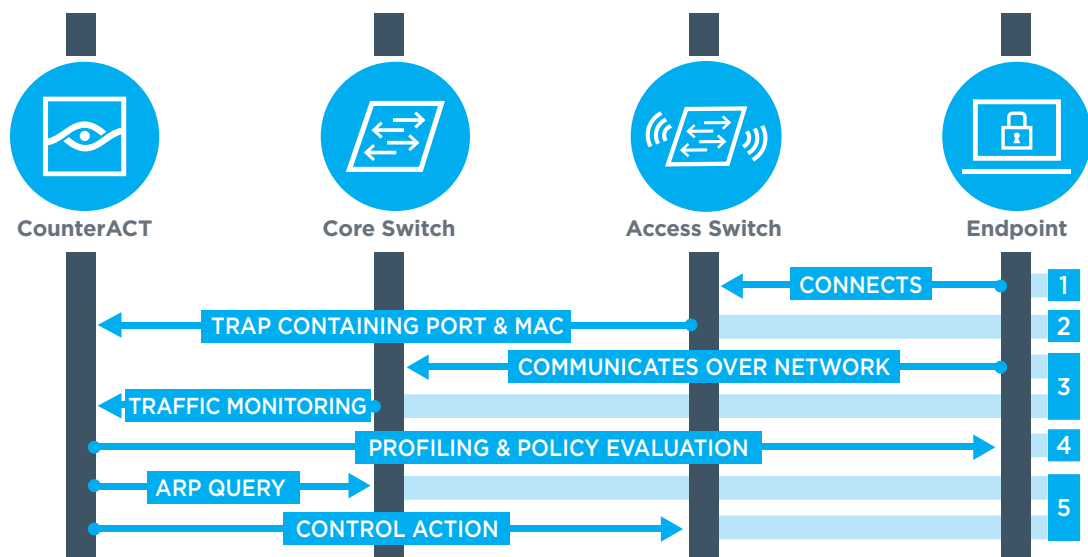

Figure 3: A sample CounterACT control flow.

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.

CounterACT requirements

CounterACT must have the ability to read ARP and MAC address tables from switches and routers. This requires the Switch plugin, a core component that is supplied with a basic CounterACT install. The latest release should always be used to ensure that the full range of features is available. Each switch must be added into the plugin, a process that is covered in more detail later in this document.

Customer environment requirements

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 endpoints

Configuring CounterACT

Configuring CounterACT to interact with switches 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.

- Enter the IP address of the switch
- Select the managing appliance

  - To reduce dependencies it is best practice to, wherever possible, assign switches to the same appliance that manages the network ranges which may connect to it
- Select the switch vendor
- Enter CLI management credentials
- Enter SNMP version and management credentials
- Enter permissions

  - Enable discovery permissions

  - Enable MAC permissions when the network device contains relevant MAC tables

  - Enable ARP permissions when the network device contains relevant ARP tables
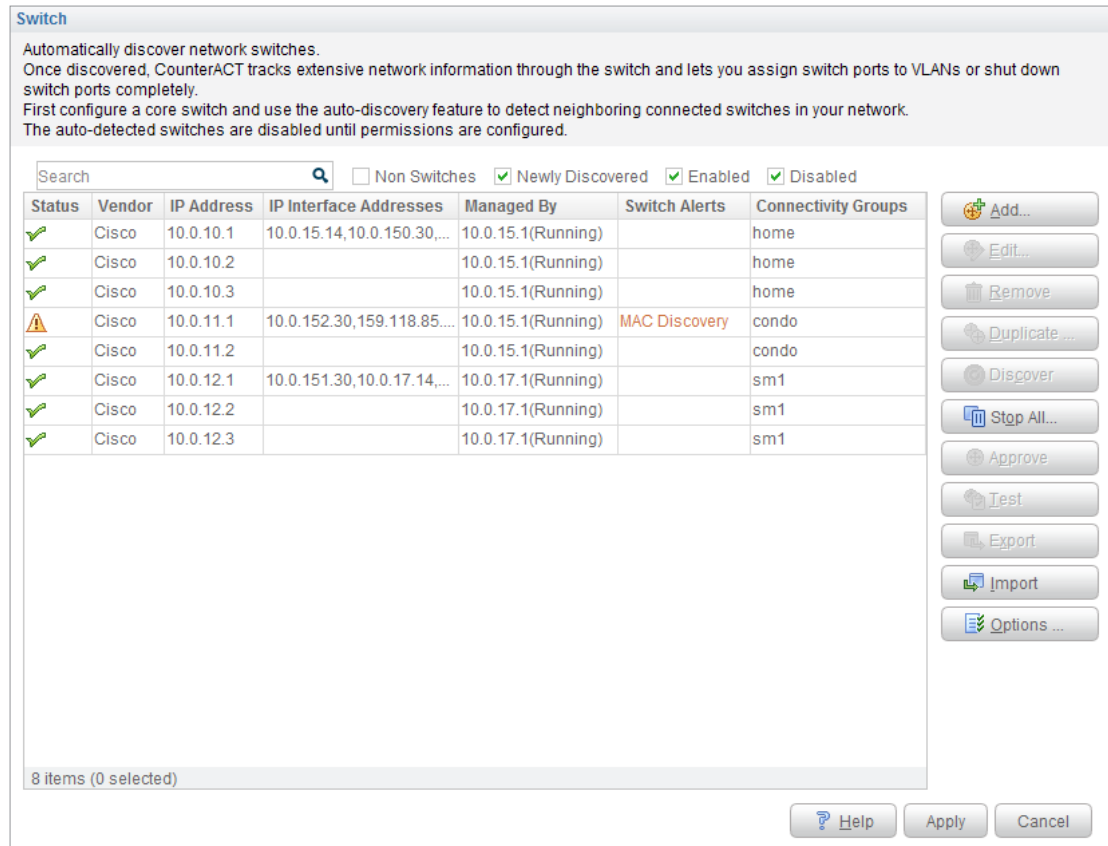- Configure ACL settings

Figure 4: The switch plugin configuration screen.

The CounterACT console

Figure 4 depicts the CounterACT console's switch plugin configuration screen, showing all switches managed by CounterACT. From here you can see alerts showing any configuration issues, as well as edit or test individual or groups of switches.

Figure 5 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. All of the checkboxes, from top to bottom, do the following:

- Enable Cisco Discovery Protocol (CDP) / Link Layer Discovery Protocol (LLDP) / Foundry Discovery Protocol (FDP) to automatically detect new switches as they are connected to the network

- Enable MAC read permissions, allowing CounterACT to query the device's MAC table

- Enable MAC write permissions, allowing CounterACT to perform blocking actions on switch ports

- Enable ARP read permissions, allowing CounterACT to query the device's ARP table

- Enable ARP write permissions, allowing CounterACT to clean up duplicate ARP entries
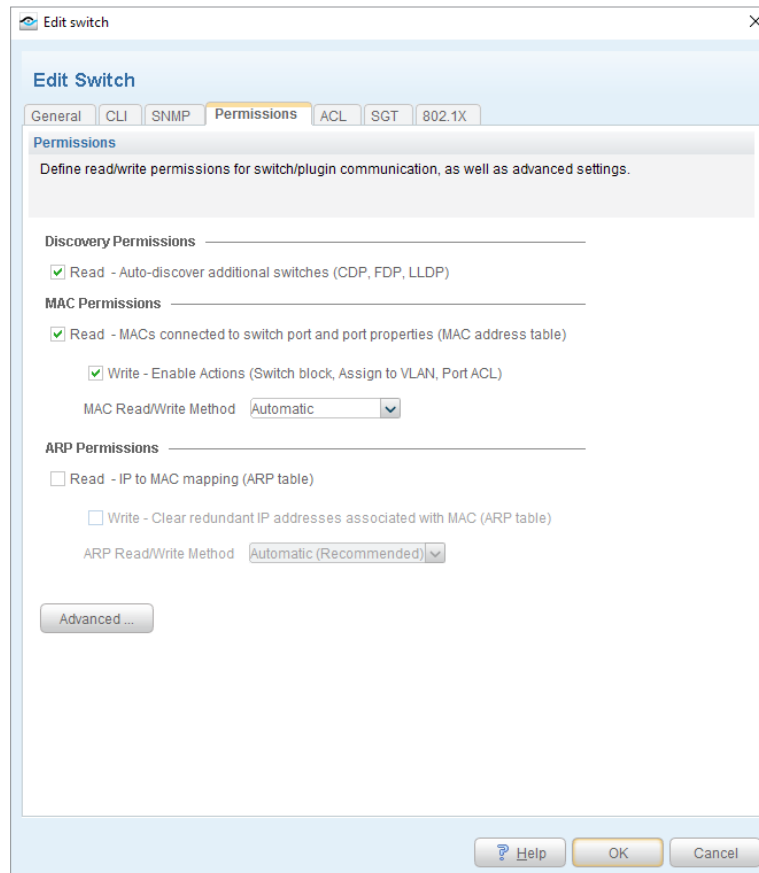
Figure 5: Configuring switch permissions.

Special situation configurations

CounterACT offers some additional features and capabilities that can be configured to support switch management and control development for certain situations.

Switch auto discovery

To help operators stay on top of a growing environment where new network devices are added regularly, CounterACT has the ability to detect new switches as they are added and connected to existing switches that it currently manages. This helps to ensure complete and continuous switch integration across the entire enterprise. Based on the vendor, this is done with CDP, FDP or LLDP.

VoIP detection

In order to effectively build wired post-connect control policies in organizations where VoIP phones are in use, CounterACT can use this property to identify which switch ports have VoIP phones on them. This information can be used, for example, in a control policy to apply different actions to ports with and without a VoIP phone.

PoE connected device

CounterACT can obtain this property from switch ports on select vendors. It can be used, for example, to help identify device types such as VoIP phones in the classification policy, or simply as an information policy that shows what VoIP phone models are on the network, and where. Similar to VoIP detection, these properties can be used to fine tune wired post-connect control policies.

For More Information

This completes our overview of design considerations and best practice tips for deploying ForeScout CounterACT in a wired post-connect scenario. For additional information on this deployment scenario or other network visibility and access control strategies based on CounterACT, current ForeScout customers should contact ForeScout Customer Support. Other interested parties should visit http://www.forescout.com/contact-us/ for more information.

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of September 30th, 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. **See** devices. **Control** them. **Orchestrate** multivendor response. Learn how at www.forescout.com