ForeScout

Deployment Guide

Best Practices for CounterACT® Deployment: Guest Management

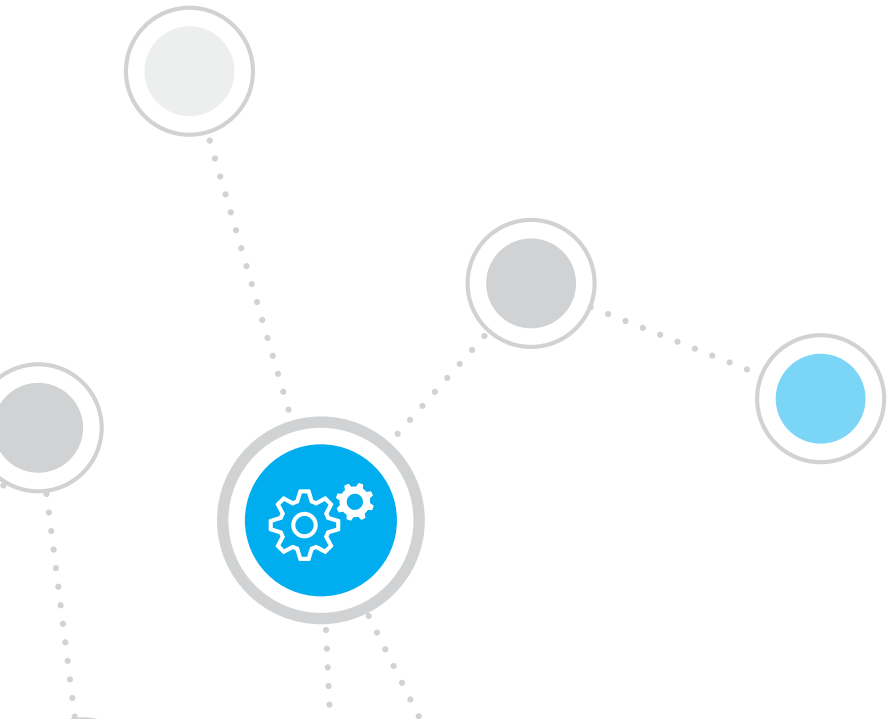

Table of Contents

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. Guest management is one of the various deployment scenarios that ForeScout supports. Visit https://www.forescout.com/company/resources/ for additional deployment scenario guides.

Purpose

This document will describe a CounterACT guest management solution on wired and wireless 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 architecture
  - Centralized
  - Distributed
  - Hybrid
- CounterACT deployment phases
  - See
  - Control
  - Orchestrate
- CounterACT endpoint inspection and management
  - Remote inspection
  - SecureConnector™
- CounterACT redundancy models
  - High availability
  - Disaster recovery
- Common data center network model concepts
  - Core layer
  - Distribution layer
  - Access layer
- 802.1X authentication
  - RADIUS
  - NAS
  - Supplicant
- Deployment scenarios
  - Post-connect
  - Pre-connect

About Guest Management Deployment

Guest management with ForeScout CounterACT is an access control strategy in which non-corporate devices are allowed highly restricted access to network resources while they undergo a registration process. Guest registration can be enforced on devices connecting to a network segment from a physical entry point; those that successfully complete the process may be granted additional resource access.

You can use guest management to safely grant network access to guests' devices and employees' personal devices. For the latter, CounterACT can facilitate authentication to a user directory whereas guest users must complete a registration process, which requires a user interface for data entry. For devices with no user interface, manual methods can provide permanent or temporary exemption within CounterACT policy. Custom database integration can also be used to identify guests without manual interaction.

While this approach can replace outright blocking of non-corporate systems, it can also be applied selectively to specific areas of the network: wireless but not wired, or one VLAN (virtual local area network) but not another. Selective deployment can enable controlled guest access to some network segments while completely blocking access to others.

Advantages of this approach

Automation

A complete guest management process can automatically identify and manage guest devices on your network without the need to manually create, track and remove NAC (network access control) policies for specific guest devices.

Guest visibility

CounterACT guest management shows where active guest devices are connected. Registered information about the device and its user is visible in either the CounterACT GUI (graphical user interface) or a web portal. Either the GUI or web portal can be used to manually add guests or revoke previously granted privileges.

Challenges of this approach

Relaxed controls

On any network space where guest management is enforced, some access concessions must be made for non-corporate devices.

- ***In post-connect*** environments, the network restrictions enforced on non-corporate devices must allow communication to CounterACT as well as to basic network services like DNS (domain name system) and possibly a user authentication directory. These allowances may expose your network to additional threats in the event that a device connects but remains unregistered.
- ***In pre-connect*** environments, these same concessions should be incorporated in an assessment VLAN or pre-connect ACL (access control list) for all connecting devices. Additionally, automated guest registration to a pre-authenticated 802.1X network is possible if the NAS (network access server) supports it. This is typically an assignment to a dedicated guest VLAN following authentication failure.

Basic concepts

CounterACT guest management has four basic concepts which occur in steps as part of the normal 4 C (classification, clarification, compliance, control) policy flow. Each of these steps can be achieved multiple ways, and the options you select from the choices available define your guest management process.

Guest assessment

The first step in a guest management process is to identify devices that are either corporate-owned or otherwise entitled to equivalent network access privileges. All other devices are assessed as potential guests.

Network restriction

Potential guest devices are allowed access to only those services necessary for the guest registration process. For devices that fail to register, this restriction is permanent.

Registration process

Potential guests are funneled to a web portal, where a CounterACT registration process distinguishes known guest devices from unregistered, unknown devices. Options for user registration are discussed later in this document.

Guest-only access

The initial access restriction for unregistered devices can be lifted, allowing immediate access to guest resources. These are typically (but not necessarily) limited to Internet access only.

Policy flow

Basic policy flow concepts are at the core of CounterACT policy methodology. To understand CounterACT deployment methodologies, it is important to understand how they affect the normal flow of policy. This section covers these concepts as they pertain to guest management.

Classification

Classification is the first CounterACT policy to which devices are subjected and is where device types are broadly organized. For guest management it is especially important to follow best practices for a clean and efficient classification policy, as this strongly affects the time required to determine and deliver the correct level of resource access. Because classification sets the stage for the rest of the policy set, speed is important, but accuracy is essential.

Clarification

In the second stage of CounterACT policy, devices are sorted based on ownership (corporate, employee, partner, guest) and whether or not they are under management. In the absence of a guest management process, non-corporate devices are passed to control policies for immediate access restriction. With guest registration, these devices are instead allowed to remain online with restricted resource access as they are funneled through the registration process.

Guest registration

Guest registration works somewhat differently in pre-connect and post-connect environments.

- ***Post-connect*** - The guest registration policy enforces an initial set of access restrictions on a guest device, and then redirects it to a registration page. Successful registrants proceed to the control policy and are granted guest-only access. Devices that fail the registration process remain under the initial access restrictions.
- ***Pre-connect*** - This deployment strategy, which is more common on wireless networks, features an assessment VLAN or a pre-connect ACL to which all connecting devices are initially assigned and which provides the initial access restrictions that are enforced by policy in post-connect environments. Devices that successfully register as guests are passed to the control policy and are transferred to a guest-only VLAN. Unsuccessful registrants remain with the initial, limited access restrictions.

Compliance

Your organization doesn't own the guest devices that connect to your network, so you don't have management capabilities on them. You can't control them remotely or assess them for compliance with your security policies. CounterACT, however, can force the guest user to install its SecureConnector™ agent to perform these checks before granting full guest-only access. Once installed, SecureConnector can discover device settings and properties that are accessible to the user. The agent will then inherit the user's privilege level and the SecureConnector install can be configured to dissolve on reboot.

Control

When a device passes from guest registration to the control phase, the initial access restrictions are exchanged for a new set of guest-only restrictions as defined in policy. These controls can be customized for different registration circumstances. For example, one set of controls can be defined for employee personal devices that are user-authenticated only while a different control set can be created for devices belonging to unauthenticated guests.

Summary

Potential guest devices are first classified and their ownership is clarified, then they are funneled through registration. If desired, an additional level of security can be added by checking security compliance through a dissolvable install of the CounterACT agent, SecureConnector. Finally, successful registrants are granted guest-only access.

Guest Registration Options

The remainder of this document addresses topics and optional tools that can enhance your guest management process.

Mirrored traffic monitoring

CounterACT can leverage common switch features to provide mirrored traffic monitoring. When enabled, this capability can help ensure that guest systems stay in segmented networks and away from production networks. It also helps CounterACT identify guest devices, discover traffic patterns and find open ports. For these reasons it is considered best practice to allow mirrored traffic monitoring for all networks where guest registration is enforced. Mirrored traffic monitoring benefits guest management in the following ways:

Mirrored traffic monitoring benefit	Guest management benefit
Packets sourced by an IP address that is not currently known by CounterACT trigger an admission event.	Faster recognition of guest devices.
Actionable, session-based properties can be created so that CounterACT can monitor and take action on network behaviors.	Guest device traffic visibility.
Observed TCP (Transmission Control Protocol) sessions served from a device on the network will mark that port as open for the server system, if it was not already.	Guest device open service visibility.
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.	Detection of guest device malicious activity.
HTTP (Hypertext Transfer Protocol) redirection allows CounterACT to force endpoints to a captive portal.	Guest registration via captive portal.
ForeScout Virtual Firewall (vFW) technology enables CounterACT to block systems at layer 4 of the OSI (Open Systems Interconnect) model though the use of TCP resets.	Addition of vFW as a quarantine option for guest devices.

Guest sponsors

Sponsors are individuals who have been configured in CounterACT to manage guest device access before or after connection. Typically, a guest user will enter a sponsor's email address in the registration portal form, triggering an email to the sponsor with a live link to approve the guest's device registration. Sponsors can be configured as individuals or as Active Directory groups, which passes sponsor management to Active Directory administrators. Sponsors also have the ability to manually input a guest device's details before it connects, which can help streamline its registration process and expedite time-to-access. You can also enable all domain members to act as sponsors. The use of sponsors is an option in guest management, not a requirement.

Redirection

While other methods exist, there are three main options for funneling a potential guest device to a registration portal: 1) by manipulating HTTP sessions discovered through mirrored traffic monitoring; 2) RADIUS redirection, or 3) by manipulating DNS.

HTTP redirection

CounterACT can intercept and redirect traffic through its native ability to monitor mirrored traffic. It can redirect a session to either a URL on the CounterACT appliance itself or to a URL on another system. This effectively funnels a target device to a captive portal where the registration process can be presented to the user. Redirection requires that CounterACT can:

- See the traffic in question through mirrored traffic monitoring, and
- Terminate and hijack HTTP sessions

However, this may not be possible if CounterACT communicates through a firewall on a separate interface from the potential guest device.

For example, if CounterACT is located in a data center network and the guest device in a DMZ segment, CounterACT's attempts to terminate the device's actual session will fail when it attempts to replicate traffic using the device's IP address. The firewall will recognize the DMZ IP address coming in on a data center interface and drop it. The CounterACT appliance performing redirection should be located on the same firewall interface as the guest itself.

To make this happen, a layer 2 mirrored traffic monitoring session from a network on which guest registration is occurring can be sent to CounterACT, allowing it to respond at layer 2 instead of layer 3.

Use HTTPS to secure guest user information

If your management process requires guests to submit personal information, ForeScout recommends that you use HTTPS to secure the communication. Because you don't own or manage guest systems, they will not authenticate to your internal certificate authority. Authentication to an external authority will be necessary for guests to view the connection as trusted.

RADIUS redirection

CounterACT can instruct a NAS to redirect devices to a captive portal as part of an 802.1X transaction using technologies such as Central Web Authentication. For NAS systems that support Media Access Control (MAC) filtering, which is common on modern, enterprise wireless hardware, 802.1X authentication need not occur. Thereby, Remote Authentication Dial-In User Service (RADIUS) redirection can take place on unsecured networks such as an open Service Set Identifier (SSID).

The distinct advantage to RADIUS redirection is that only CounterACT and the NAS need to be configured, and there is no reliance on tertiary factors such as mirrored traffic visibility or the reconfiguration of DNS systems. At this time, however, the redirect RADIUS attribute is only present on wireless NAS systems, and not commonplace on wired NAS systems, which limits where it can be used.

DNS redirection

DNS enforcement was developed to overcome inherent limitations in HTTP redirection, including CounterACT's inability to see network traffic in some locations and the tendency of firewalls to drop reset and redirection packets. Unless CounterACT has mirrored traffic or RADIUS redirection at all physical locations, DNS enforcement should be used.

To use DNS as a redirection tool, CounterACT must be configured in the list of DNS servers for networks on which guest registration is occurring. This allows CounterACT to respond with its own IP address as the result of any DNS query, redirecting the endpoint to an internal website and captive portal for registration. Blocking a potential guest device's access to other DNS servers as part of the initial network restriction is an effective way to keep CounterACT from having to be at the top of the DNS list. Alternatively, for endpoints not requiring redirection, CounterACT can simply forward to a valid DNS server, or respond with a "not implemented" result. This forces the endpoint to its configured secondary server.

Summary

The options available for funneling guest devices to a captive portal are HTTP, DNS and RADIUS redirection. HTTP redirection can only occur where CounterACT can see mirrored traffic. RADIUS redirection is a great solution when available on wireless networks, and DNS redirection should be used where the others cannot.

Registration Options

Both the criteria for successful guest registration and the information required of guest users can be configured in multiple ways. In addition, the registration web page is customizable, offering you the flexibility to modify it with your own corporate language and logos. This section covers these options.

Self-registration

Self-registration allows guest users to obtain guest-only access without human intervention. CounterACT will automatically channel the guest device to a captive portal and prompt the user to enter several customizable fields of information. Once complete, CounterACT will grant the device guest-only access and store the collected information for visibility, reference and reporting within CounterACT's guest management pane and web portal. CounterACT can optionally send a validation code to a guest user's email or phone to help facilitate self-registration. Self-registration is best used when your guest network is already segregated from production, but you would still like to identify, log and monitor the guests that are connected to your network.

Sponsored registration

Adding sponsors into the registration process creates a situation where there is additional trust for that device. Someone within your organization must approve the guest to be on your network for a set period of time. Additionally, sponsors manage the duration of the guest access, taking away the guest device's ability to connect to the network without sponsor intervention. Sponsored guest access is ideal where there is no guest-specific network. In this case, guests connecting to the production network will remain there, and are restricted from normal production access through ACL assignment.

Pre-registration

Pre-registration is when a CounterACT administrator or guest sponsor, manually and prior to the initial guest connection, provides the guest details that are normally requested during an automated registration process. This information can also be entered on an external, existing system when a custom integration has been created between CounterACT and the relevant system.

Guest user information

CounterACT can prompt guest user information listed below. Each field can be set as mandatory, optional (an empty field is a valid response) or excluded from the registration screen entirely.

- Phone number
- Company
- Title
- Location
- Contact person
- Contact person email
- Access duration

The contact person would be someone within your organization—the sponsor if sponsored registration is in effect. The access duration allows the guest user to request a specific timeframe for access. In addition to these available options, you may also develop your own fields for information collection.

Summary

Guest management can be automated or require sponsorship. Automated registration may be acceptable if the existing security of your dedicated guest network is already sufficient, but you still want to see what guests are connected to it. Sponsorship requires someone in your organization to approve the guest device. It is best used when there is no differentiation between your production and guest networks.

Guest Control

Guest-only access restrictions are enforced primarily through the use of ACLs that prevent guest devices from accessing some or all of your production resources. There are two main approaches to applying ACLs. The first is a dynamic ACL application directly upon the guest device's network connection, in which the device retains a normal production IP address. The second is a traditional VLAN statically configured with an ACL at its layer 3 boundary. In the VLAN approach, CounterACT simply changes the device's VLAN assignment. It does not implement the ACL, which is already configured on your network equipment. If CounterACT is performing mirrored traffic monitoring on a network segment, then vFW becomes a third option. These approaches are not mutually exclusive, and all may be in use on separate network segments.

Dynamic ACL application

Dynamic ACL application is the best approach for a relatively small number of guest devices that will be allowed to connect anywhere and will not be assigned to a dedicated guest network. Using this approach, CounterACT can place restrictions on a guest device's switch port or wireless connection that might otherwise be enforced on a dedicated guest network VLAN. The same restrictions can be overlaid on production VLANs. Packets transmitted from the device that do not match the definition of "guest-only" destinations are dropped before they enter your network. In this scenario, guest devices will be connected to an internal network segment both before and after registration, so it is very important to carefully plan the appropriate access restrictions for both pre- and post-registration ACLs.

Initial network access restriction

A potential guest device needs only to obtain and retain network access, and to communicate with the local CounterACT instance. During registration, a device should be permitted only the following access:

- ***CounterACT*** – The captive portal lives on CounterACT, so the guest device must be able to communicate with it. In some cases, a permit line to and from CounterACT is all that is required. CounterACT's default method of switch port ACL application will apply ACL lines between the device and itself without configuration. This eases ACL configuration management where many CounterACT appliances are deployed.
- ***DHCP*** – This can be important if a guest device needs to re-address itself for any reason, such as a VLAN move or a restart. It is only absolutely necessary if your guest access plan involves a VLAN move.

- ***DNS*** – The ability to perform name translation is important for a guest device to access resources, and for redirection to a captive portal. To enable DNS enforcement and protect against recursive DNS attacks, ensure that no internal DNS servers other than CounterACT are accessible to the device.
- ***HTTP*** – A guest device must be able to generate HTTP traffic for CounterACT HTTP redirection. If DNS redirection is the only redirection method, this line is not necessary.

VLAN moves

When a dedicated guest network is already in place, the best approach is to have CounterACT assign potential guest devices to it. This may also be necessary if the network equipment in use will not support dynamic ACL application. If CounterACT's captive portal will be used to record guest user information, the appliance that manages the guest network should be on the same side and interface of any firewall that separates it from production. Since unknown systems will be moved to the guest network and potentially prompted for registration, it is not necessary to plan a separate initial network access restriction.

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.

Wired vs. wireless controls

The only difference in the way CounterACT manages guest devices connecting on wired and wireless networks lies in the control commands it sends to the network infrastructure. For a list of supported wired and wireless vendors, see the help files for our switch and wireless plugins.

Wired

On a wired network, CounterACT moves a device to a guest VLAN by changing the network assignment on the switch port to which the device is connected. It applies an ACL by creating the ACL in a global configuration and assigning it to a device's switch port in the switch configuration settings.

Wireless

On a wireless network, both the VLAN move and ACL application occur the same way. Depending on the wireless vendor, a guest "interface" or "role" is permanently created with the desired outcome being either the guest VLAN or the guest-only ACL. CounterACT will change this assignment when a potential guest is identified or a guest successfully registers.

Summary

Whenever a potential guest device is identified, a network access restriction should be placed on it that accommodates the registration process but otherwise protects your production assets. This can be accomplished either through a VLAN move to a dedicated guest network or by the application of an ACL to the device's network connection. If the device registers successfully, the initial restriction should be changed to guest-only access (assuming the initial restriction and guest-only access are not identical). If the device does not register, the initial restriction should remain indefinitely. From CounterACT's perspective, these control changes are technically the same on wired and wireless networks, but different command sets are used to enforce them.

Architectural Examples

There are two main ways to design guest management with CounterACT.

Dedicated guest appliance example

Having a dedicated CounterACT appliance for guest-only networks is considered best practice when the guest network is already segregated from production, such as a guest wireless network located in a DMZ. The appliance will require mirrored traffic monitoring, and should be placed on the same side of the firewall as the guests themselves. Communication back to the Enterprise Manager through any firewall or other security device will happen on a single TCP port. This example simplifies firewall rule creation and CounterACT configuration. The guest management flow is as follows:

1. A connecting device is identified at the clarification policy level as a non-corporate asset.
2. CounterACT moves the device into the segregated guest VLAN. Management of the device passes from the original CounterACT appliance to the dedicated guest appliance, which takes over inspection and policy actions. All interaction with the host is now contained within the segregated guest network.
3. CounterACT places network restrictions on the device, disallowing traffic that is not necessary for guest registration.
4. CounterACT checks for any manual pre-registration entries, which allow a CounterACT administrator or guest sponsor to exempt known guest devices from registration. Pre-registered devices are immediately granted full guest-only access.
5. CounterACT prompts the device for registration.
6. If the device registers successfully, CounterACT removes the restriction from step 3 and grants full guest access.

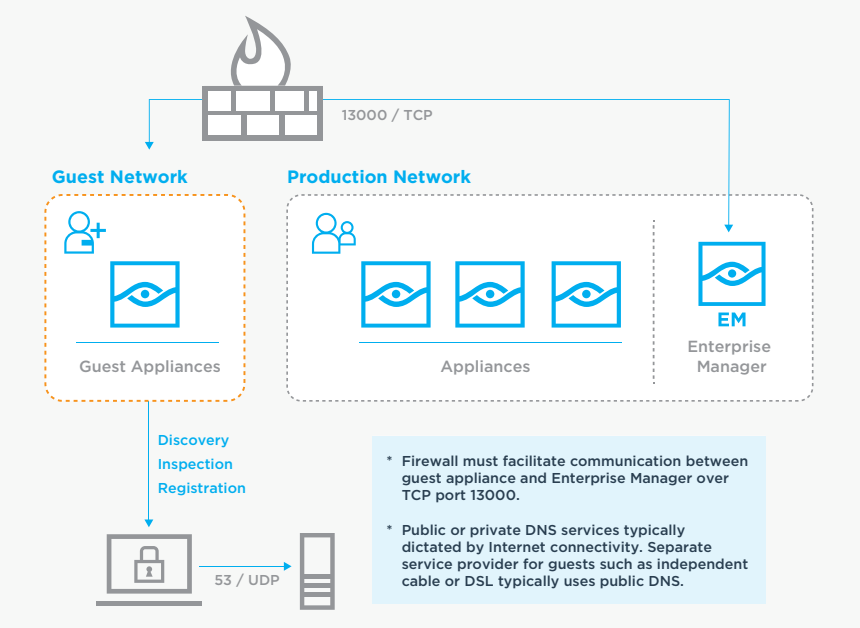

Figure 1: Dedicated guest appliance example.

The benefits of a dedicated guest appliance include:

- Minimal security footprint between guest and production networks
- Effective isolation for non-corporate devices during guest registration
- Redirection is localized to the guest network, avoiding the need for anti-spoofing controls at the firewall

Shared appliance example

Working with a shared appliance is considered best practice in the absence of a segregated guest network, where guest-only access restrictions are enforced directly on a guest device's connection to a production network. Sharing an appliance across guest and production networks requires extra planning and more complex configuration to determine what inspection and control traffic should be allowed to and from CounterACT through a given firewall.

The guest management workflow in this shared appliance example is as follows:

1. A connecting device is identified at the clarification policy level as a non-corporate asset.
2. CounterACT checks for any manual pre-registration entries, which allow a CounterACT administrator or guest sponsor to exempt known guest devices from registration. Pre-registered devices are immediately granted full guest-only access.
3. CounterACT places the initial network restriction on the potential guest, allowing it to access only those resources necessary for the registration process.
4. CounterACT prompts the device for registration.
5. If registration is successful, CounterACT removes the initial network restriction, replacing it with guest-only access controls.

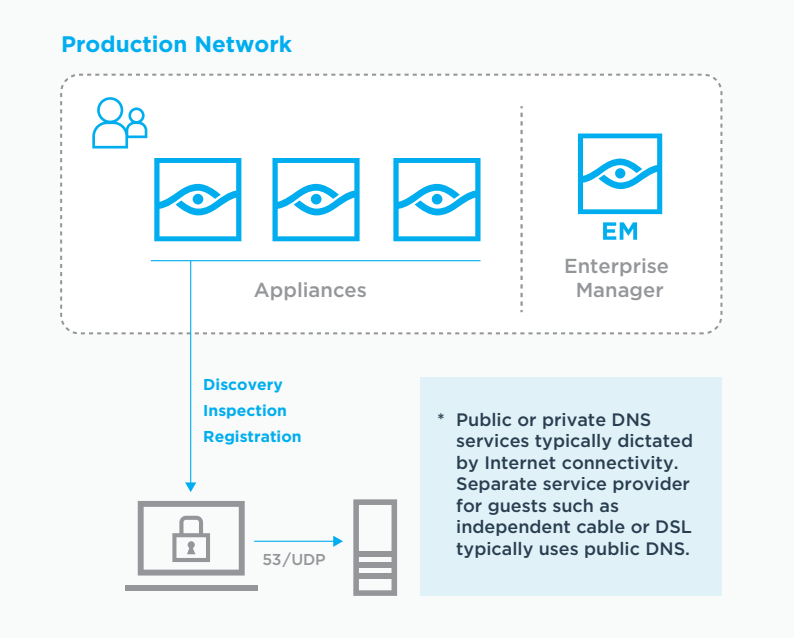

Figure 2: Shared guest appliance example.

The benefits of a shared guest appliance include:

- Less hardware required
- Less configuration
- Works with any guest network configuration

Workflow Diagrams and Flowcharts

The following examples depict typical high-level guest management workflows in post-connect and pre-connect CounterACT scenarios using emailed sponsor approval. They illustrate a guest device connecting to the network and the circumstances under which it can obtain guest access.

Post-connect guest management workflow

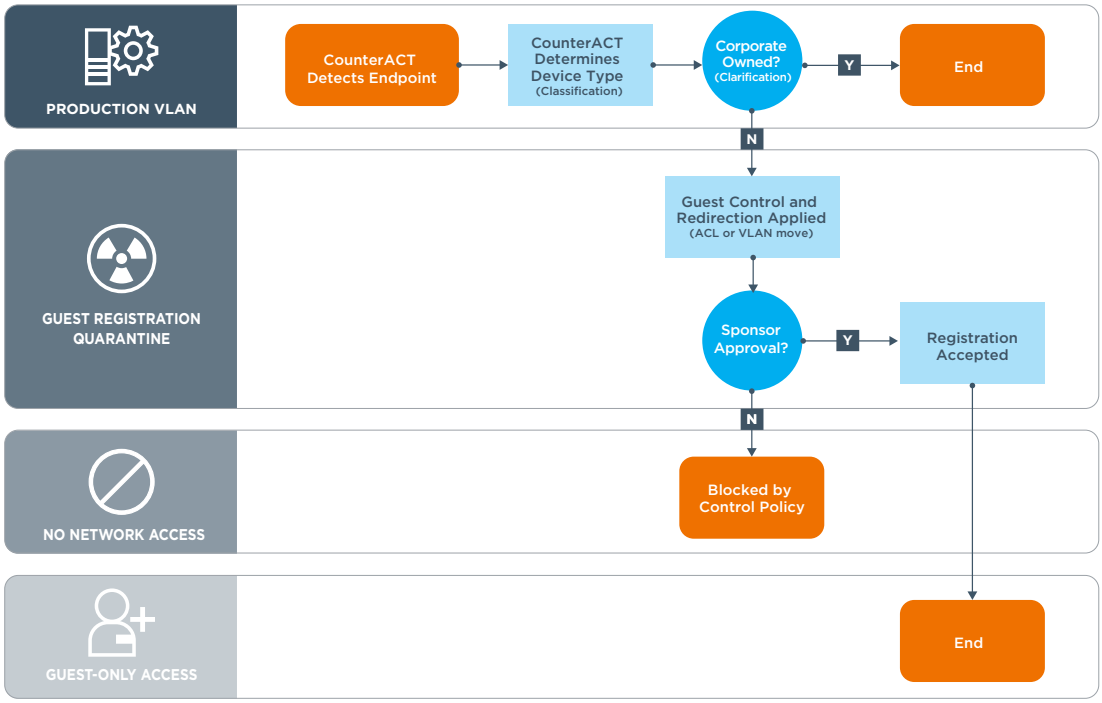

Figure 3: Post-connect guest management workflow.

1. An endpoint joins the production network.
2. CounterACT detects and classifies the device in a broad endpoint type category.
3. CounterACT determines if the device is corporate-owned using methodologies that vary with the classification category.
4. CounterACT applies the initial network access restriction and attempts to redirect the device.
5. CounterACT emails the sponsor specified by the guest user, and the sponsor either accepts or denies network access.
6. If accepted, the initial network access restriction is lifted and guest-only access is granted. If denied or otherwise not received, the initial network access restriction is replaced with a greater restriction.

Pre-connect guest management workflow

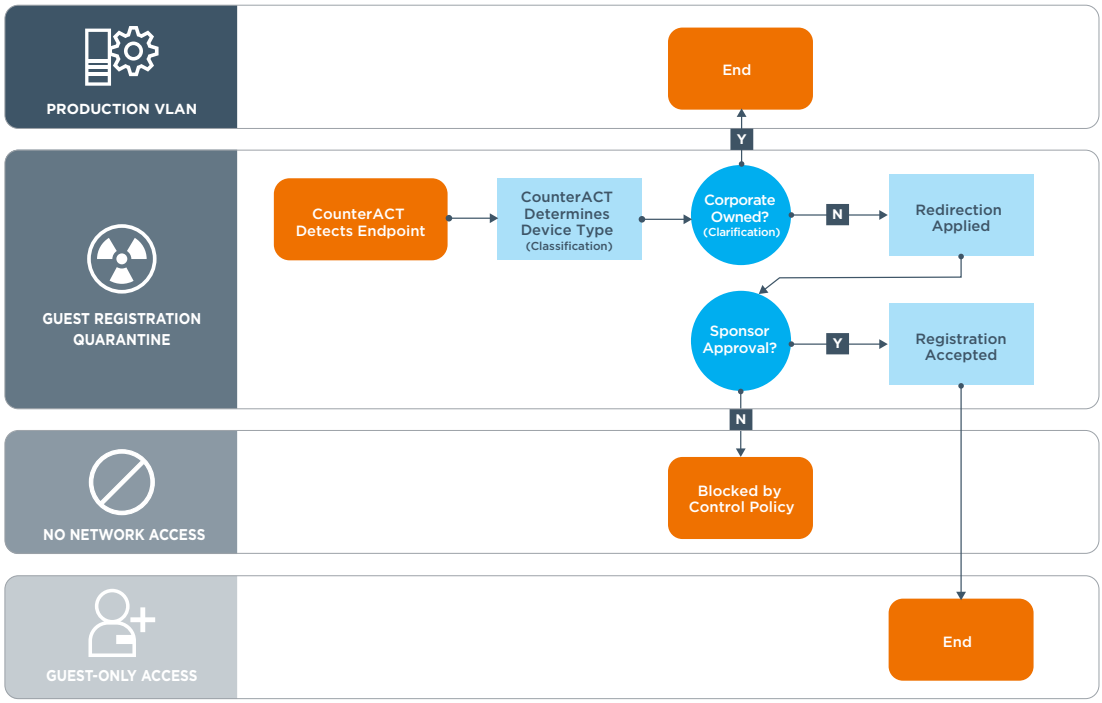

Figure 4: Pre-connect guest management workflow

1. An endpoint joins the network with limited access.
2. CounterACT detects and classifies the device in a broad endpoint type category.
3. CounterACT determines if the device is corporate-owned using methods that vary depending on the classification category. If the device is corporate, CounterACT grants production network access.
4. If the device is not corporate-owned, CounterACT attempts to redirect its traffic.
5. CounterACT emails the sponsor specified by the guest user, who either accepts or denies network access.
6. If accepted, the initial network restrictions are lifted and guest-only access is granted. If the registration request fails or is otherwise not received, the initial network access restriction is replaced with a greater restriction.

Environment Requirements

This section provides an overview of what must be in place for the guest management scenario to operate successfully within an enterprise network.

CounterACT requirements

- Working clarification policies – To know what differentiates a guest device from other devices
- Network device management – To place controls on the guest device
- Mirrored traffic monitoring channel configured – If HTTP redirection will be used
- DNS enforce plugin – If DNS redirection will be used

Customer environment requirements

- Planning – To develop strategy for all guest management use cases across the enterprise
- Network device management accounts – Account must be created for management of each network device, at each management point: SNMP (Simple Network Management Protocol), CLI (Command Line Interface) or NETCONF (Network Configuration Protocol)
- Mirrored traffic monitor port configured – If HTTP redirection will be used
- Dedicated appliance assignment – If HTTP redirection will be used and the dedicated guest network is on its own interface, then CounterACT needs to be on that same interface
- DNS list – If DNS redirection will be used, CounterACT needs to be added to the list of DNS servers for any network segment where guest registration is required
- DMZ considerations – If CounterACT is connected to a guest-only network, rules that allow it to talk back to the Enterprise Manager are necessary, as well as email communication to potential approving sponsors

Configurations

CounterACT guest management involves working with registered guest devices and their registered properties, as well as potentially managing sponsor accounts.

Captive portal page

CounterACT's captive portal page can and should be customized to show your company branding. This can be done separately for standard and mobile devices.

CounterACT console

Figure 5 shows the CounterACT guest management screen, displaying registered guests. From here you can manually approve new guests, revoke access for currently approved guests and update guest information. You may also configure guest tags, which are used to place guest devices in groups and to describe what level of network access is granted. While this image is from the CounterACT GUI, there is also a web portal where sponsors who do not have GUI access can perform the same functions.

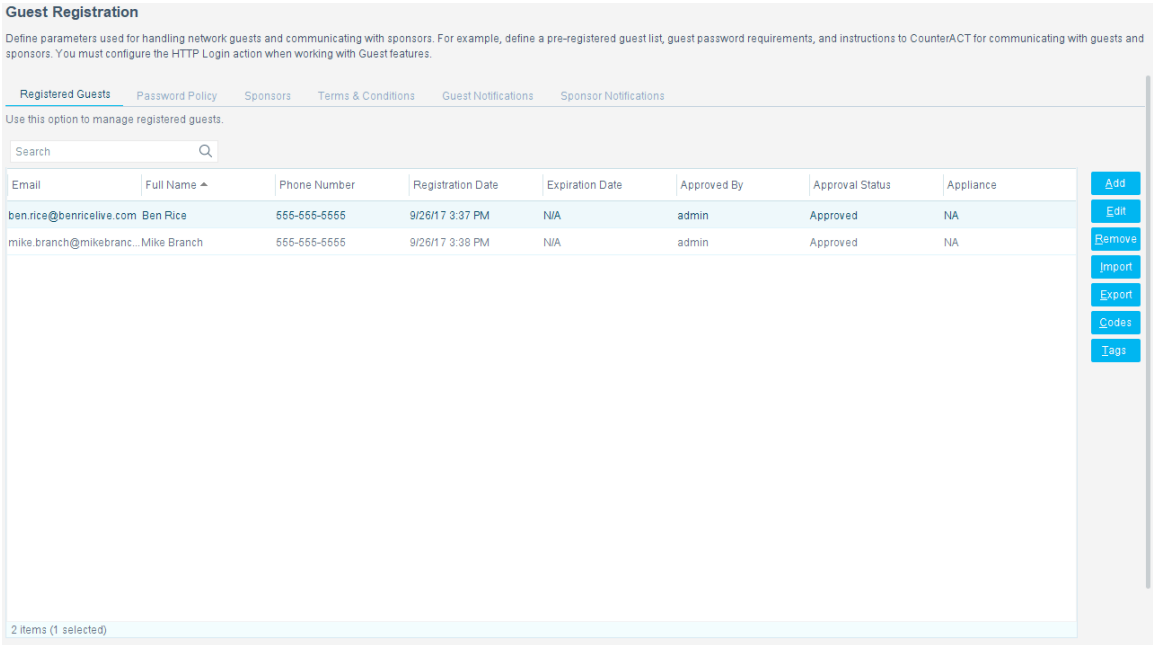

Figure 5: The CounterACT guest registration pane.

Specific to the GUI configuration for CounterACT operators, the following can also be configured in the guest registration options:

- Sponsors – The addition or removal of corporate employees as guest sponsors who can use the sponsor web portal to approve and manage guests
- Password policy – Configuring password requirements for guest users
- Terms and conditions – Configuring the terms that a potential guest user must agree to before connecting to the network
- Guest notifications – Configuring how and when to notify guest users with responses to their requests for network access
- Sponsor notifications – Configuring how and when to notify sponsors that a guest user who has listed them as a sponsor has requested access, was approved or denied access, or has had network access revoked
- Automated purging – Configuring when to purge inactive guests

For More Information

This completes our overview of design considerations and best practice tips for deploying ForeScout CounterACT guest management. 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 https://www.forescout.com/contact-us/ for more information.

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 June 30, 2017, more than 2,500 customers in over 70 countries improve their network security and compliance posture with ForeScout solutions. **See** devices. **Control** them. **Orchestrate** system-wide threat response. Learn how at www.forescout.com

ForeScout®

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