Choosing a Network Access Control (NAC) Solution That is Right for Your Network

Best Practices In Network Access Control

Whitepaper

© 2012 ForeScout Technologies, Inc. All rights reserved.

Cutting Through the Network

Access Control (NAC) Confusion

Confused about network access control? You are not alone. Over the last year, there has been an explosion of interest in network access control as a way to deal with the myriad of mobile devices that users are bringing into the workplace and attempting to connect to the network. IT security managers are looking for new security controls that can help them shift from a relatively static and well-controlled IT environment to one that is dynamic and very difficult to control. The Bring Your Own Device (BYOD) movement is the epitome of loss-of-control, because these devices are not owned or under the direct control of the IT organization.

Enter Network Access Control (NAC)

NAC has emerged as an excellent technology to answer the burning question of "how do I secure my IT infrastructure in increasingly fluid environment?" In this context, NAC is a very attractive technology, because the network is the one thingyou still do control, and you can use the vantage point of the network to protect all corporate assets and resources regardless of what type of device the user has.

Not all NAC products provide all of the following functions, but the most advanced NAC products provide:

» Immediate discovery of any device when it attempts to connect to the network

» Categorization of each device by type (Windows PC, Mac, printer, Android, iOS, etc.) and ownership (corporate vs. personal)

» Health check of each device, based on pre-determined security compliance rules

» Network access actions such as block, allow, or limit to specific network resources. The decision can be based on attributes such as user name, device type, security posture of the device, time, place and location.

» Remediation of security problems on the device, such as anti-virus, encryption, password, unauthorized peripheral, unauthorized software, etc.

» Continuous monitoring of the device throughout the connection session to ensure the device remains compliant and non-threatening.

The most advanced network access control products will integrate with various existing infrastructure resources to provide advanced policy control and automation. For example:

» Integration with user directories to facilitate role-based network access control. In this scenario, network access is limited on the basis of role and job function.

» Integration with desktop management systems to allow these systems to be aware of unmanaged, rogue devices on the network. NAC also helps remove the blind spots that these systems often have with respect to corporate-owned endpoints that, for one reason or another, lack the proper security agents.

» Integration with mobile device management (MDM) systems to provide unified visibility and control over a wide range of non-traditional endpoint devices.

» Integration with vulnerability management systems to support advanced network access control policies based on security posture

» Integration with SIEM systems to provide additional information to the SIEM system about unmanaged devices on the network which may be the target or the source of an attack, and to provide automated security response from the SIEM system to the network control points, leveraging the NAC system.

Enter Real World Networks

Challenges arise when attempting to apply theoretical concepts into real world networking environments. Complex heterogeneous network environments introduce a significant level of complexity in attempting to implement network access control. A typical corporate network is anything but typical, comprised of endpoints and infrastructure components from numerous vendors with varying configurations. As most companies grow organically, infrastructure and device upgrades are implemented on an "as-needed" basis to handle increasing computing demands and/or to gain additional functionality from newer versions of network equipment (i.e., switches, routers, etc). Additionally, the proliferation of low-cost mobile devices and wireless networks enable end-users to bypass existing security measures by introducing personal devices into the corporate network.

This white paper will look at three key functionality criteria a NAC solution must deliver in order to effectively operate in complex and diverse real-world networks. These criteria are:

1. **Detection and Interrogation of Endpoints**
   Before enforcement of network security policies can be enabled, all connecting devices must be detected. Additionally, several types of inspection mechanisms need to be considered in order to get maximum interrogation with minimum IT management overhead for all detected and identified endpoints.

2. **Policy Creation and Enforcement Actions**
   How easy is it to create policies? What level of policy granularity is necessary for effective device inspection and enforcement actions? Will enforcement of policies disrupt the network or users? These are the questions that must be considered to ensure that the NAC solution will effectively deliver granular levels of access control without disrupting network operations.

3. **Deployment and Integration**
   In order to maximize the benefits of a NAC solution, it has to be seamlessly integrated into the network infrastructure without causing network disruptions. Therefore, multiple approaches to deployment (e.g., out-of-band vs. inline) must be considered to determine the potential impact and level of disruption a deployment method will have on the overall infrastructure. Another determining factor is a NAC system's ability to leverage the existing investment into network infrastructure and equipment without requiring costly upgrades or causing network downtime.

Section 1
Detection and Interrogation of Endpoints

One of the most critical aspects of controlling access is detecting connecting devices and ensuring those devices are in compliance with network security policies. The question remains: How to accomplish access control in a complex network where not all of the access endpoints are not easily defined or even known? A number of methodologies have been introduced to address this primary challenge, but no silver bullet exists. In considering the different approaches to detection, a key question is whether prior knowledge of an endpoint should be required in order to detect it. Prior knowledge of a device implies some form of installed agent be present on the connecting endpoint prior to connection, which identifies the device and provides some type of system diagnostic result to the NAC system.

Agent vs. Agentless NAC

Software agents have become a common component of endpoint security. It is not unusual to have multiple agents providing a variety of system assessments and controls. This is a positive way to defend an individual system against malware, to protect sensitive data, and to manage VPN connections. An agent has the ability to obtain detailed knowledge of the system on which it resides. Access to the system's registry and file structure provides intimate knowledge of installed applications, active processes, and a host of other system configuration details to provide a system "health" assessment prior to allowing network access. At the point of connection, the software agent identifies the endpoint as a managed user device and initiates a further inspection.

Conceptually, this is a good story. The agent obtains in-depth information of the system's level of compliance and provides this compliance information to the NAC system at the time of connection. However, the NAC system is rendered virtually useless when unmanaged or non agent-based devices are introduced into the network. Any device that does not have an agent installed is either summarily denied access to the network or is allowed complete access without any form of endpoint inspection. Neither scenario is an acceptable business practice — while the former disrupts productivity and requires an increased level of manual device processing by the IT staff, the latter introduces an array of security threats and vulnerabilities directly into the network.

Unmanaged systems are only one of the many daunting challenges faced by agent-based NAC systems. Requiring an agent on all managed endpoints introduces a significant management burden associated with the NAC solution deployment. While an agent-based approach may work in a small networking environment with a limited number of endpoints, it quickly becomesmay become impractical as the number of managed or unknown devices increase.

Agent-based NAC systems also pose additional challenges due to OS compatibility issues. Most NAC solutions support the latest versions of Windows and possibly some Macintosh devices, but anything beyond this becomes problematic. This issue becomes even more critical when considering any other type of IP-based devices that are connected to the network for which an agent is simply not an option (e.g., printer, VoIP phone, MES systems, medical devices, personally-owned smartphones, etc.). Because an agent can never be deployed (or would be too costly to deploy) onto into these devices, they become potential vulnerabilities that remain undetected and therefore unprotected by the NAC system.

Not all agents are alike. Some agents (for example, 802.1x) may require specific configurations and need to be installed by the IT organization. These agents may not "travel" well, and it is possible that an endpoint containing one of these agents will not be permitted to join any other network unless the agent is reconfigured. These agents are typically not a good solution for guests and contractors.

Some agents (for example, MDM agents and the agents included with ForeScout Mobile) are easily installable by the end user, and they are highly portable and play well with other networks.

Some agents are considered "dissolvable" or non-persistent. These agents can agent which can be downloaded and temporarily installed at the point of connection and is then removed once the device is no longer on the network. This approach can alleviate some of the IT management burden in dealing with non-managed devices and provide a solution for addressing network guest and contractors.

Going Agentless

Agentless NAC systems provide a number of advantages over agent-based solutions, especially when considering network protection scope and scalability, decreased levels of manual IT management and reduction of disruptions to network services.

Scalability

If a software agent is not required to be installed or downloaded onto the endpoint, the scalability of an agentless NAC system is virtually unlimited. While there may be other factors that determine how well a NAC system will perform (e.g. geographically-dispersed networks), the system itself is not restricted by the type or number of devices it can detect and manage. Agentless systems provide the ability to detect any IP-based device, allowing the complete coverage of a global infrastructure without prior knowledge of any of the connecting devices. This is clearly an advantage when dealing with Bring Your Own Device (BYOD) situations.

Another clear advantage of an agentless NAC system is that it does not require network managers to educate the users on how to use yet another agent or altering their established logon process in any way. With all detection and inspection being conducted without an agent, end users are not aware that a policy check is taking placeas long as their device is compliant with the corporate security policies. This allows for the least amount of change to end user behavior and experience, which further alleviates the burden on IT resources and staff and significantly contributes to the overall success of a NAC rollout.

Management

Agentless NAC systems significantly reduce the amount of management required to enforce network security policies. Since there are virtually no interoperability issues among the connecting devices, IT management can focus on addressing more critical business issues. By design, an agentless system should cover all IP-based devices, enforcing policies on all devices and thus providing more comprehensive coverage of the network. When a policy violation is discovered (e.g., the NAC system detects a rogue wireless access point) IT management is informed immediately and is able to efficiently respond to the threat or vulnerability. In the meantime, more trivial violations are automatically addressed by the NAC system (e.g., anti-virus definitions are out of date and user is linked to self-remediation).

In addition to the benefit of low management overhead, agentless NAC solutions provide IT administrators with a better understanding and control over what users and devices are attempting to gain access to the network. This functionality is particularly beneficial when it comes to detecting and managing contractors and other types of network guests who need limited network and/or Internet access but do not have an agent installed on their device. An agentless NAC system is inherently better at handling unknown and unmanaged devices than an agent-based NAC system..

For example, when a contractor/guest attempts to connect to the network with an agentless NAC system in place, the device would be detected and identified as a guest and forced into either a pre-configured network segment or a virtual local area network (VLAN). The contractor/guest would then immediately gain access to a pre-determined set of appropriate network resources without diminishing the level of security or introducing any threats to the enterprise network. When this process is automated, IT administrators can be sure that only known and authorized devices are gaining access to the production network, while all others are detected and controlled by the agentless NAC system.

NAC AT WORK

Agentless Device Detection

A large hospital under pressure to meet regulatory compliance requirements urgently needed to obtain an accurate count of all devices on their network such as desktops/laptops and peripherals, as well as EKG, CRT and ultra-sound machines.

Within hours of deploying ForeScout's NAC appliance, network managers had a complete inventory of all IP-based devices connected to the hospital network. With all of the devices detected and identified, network managers quickly defined and implemented a set of hospital-wide access policies to gain awareness of all connecting endpoints.

Section 2
NAC Policy Creation and Enforcement

The primary reason to deploy a NAC solution is to ensure that all connecting and connected devices on the enterprise network are in compliance with network security policies. Although policies vary greatly between enterprise networks, there are some basic network security policies that are fairly consistent. The policy of checking whether antivirus software is installed on a device and the antivirus definitions are up-to-date is an example of a best practice policy common to most security-minded organizations.

Perhaps one of the biggest challenges when deploying a NAC solution is determining which policies need to be enforced and what actions need to be taken to enforce them. One of the most important criteria in selecting a NAC system is the policy creation process. An enterprise-level NAC solution must enable IT management to create customized, granular, and enterprise specific policies to effectively address the security concerns of any organization. Figure 1 features examples of system variables that could be used as the basis for creating a NAC policy.

USER BEHAVIOR	• Network policy violations • Audited responses • Self-remediation success	
USER INFORMATION	• Username • Authentication status • Workgroup	• Email address • Role/Department • Phone number
APPLICATIONS	• Illegitimate applications • Application versions • Registry values	• File information • Modification date
OS INTEGRITY	• OS fingerprint • Antivirus update status • Jailbroken / rooted	• Un-patched vulnerabilities • Open services • Running processes
DEVICE INFORMATION	• IP address • MAC address • Hostname	• Device type (PC, smartphone, tablet, printer, wireless, etc.)
PHYSICAL LAYER	• Physical switch • VLAN • Switch port	• 802.1X • Number of devices sharing a port

Figure 1: Table of Enforceable Basic Policy Variables

NAC Policy Enforcement

The term "policy enforcement" typically causes apprehension among IT management. Any time an automated system is tasked with enforcing policy, there is a risk of network disruption. Network service and user experience disruptions typically arise as a result of binary enforcement by a NAC system (i.e., only allow or deny), resulting in loss of productivity. The disruptive nature of a NAC system that does not provide an array of flexible enforcement actions could outweigh the benefit derived from access control security.

Flexibility is Key

In addition to differentiating between minor, moderate and critical security threats, it is imperative that any NAC solution provides a full spectrum of enforcement options. The ability to match the level of enforcement to the exact level of policy violation is a critical aspect of a successful NAC implementation.

For example, some organizations consider instant messaging to be a critical business communication tool, while other enterprises may view it as a security threat. In the latter, even though the presence of IM is considered a threat, management does not want to keep the user from being productive, and only wants to notify the user of the policy violation or perhaps disable the application. A NAC system with a binary enforcement approach will cause disruptions to user productivity by revoking the device's access to the network while IT management addresses the issue. On the other hand, a NAC system with a range of enforcement options could prompt the user to remove the application, notify the appropriate staff of the problem, or simply disable the application remotely without causing any downtime or disruptions.

Network-based Enforcement

As the industry matures and enterprises determine suitable methods of NAC deployment for their specific environments, there has been a notable trend towards network-based enforcement. While some enforcement can be done on the endpoint by a client-based solution, the deployment and management challenges associated with an agent-based NAC system has led the industry towards a network-based approach. In a recent white paper published by Infonetics Research, it is noted that 80 percent of survey respondents planned apply enforcement actions over the network rather than relying on any form of installed client. (See Figure 2.)

NAC AT WORK

Mobile Device Policy Enforcement

A financial services company deployed ForeScout CounterACT in conjunction with a 3rd party MDM system, linking them together via ForeScout Mobile. Their objective was to provide a secure wireless network for employees who were carrying specific types of healthy smartphone and tablet devices, and provide a simple guest network with Internet access for all other wireless devices. In this scenario, ForeScout CounterACT immediately checked each wireless device as it came onto the network to see if it contained the requisite MDM agent. If it did not, the user was given the opportunity to install the agent or proceed to the guest network. Once the agent was installed, the MDM system provided CounterACT with security posture information, and CounterACT enforced network access policies. The wireless network access policies were consistent with the wired network access policies that the bank used for corporate-owned desktop PCs. The combination of ForeScout CounterACT with the MDM system provided the financial services company with a high degree of confidence that their security policies were consistently and strongly enforced, and the unified reporting from CounterACT allowed them to easily measure compliance across the entire range of endpoints.

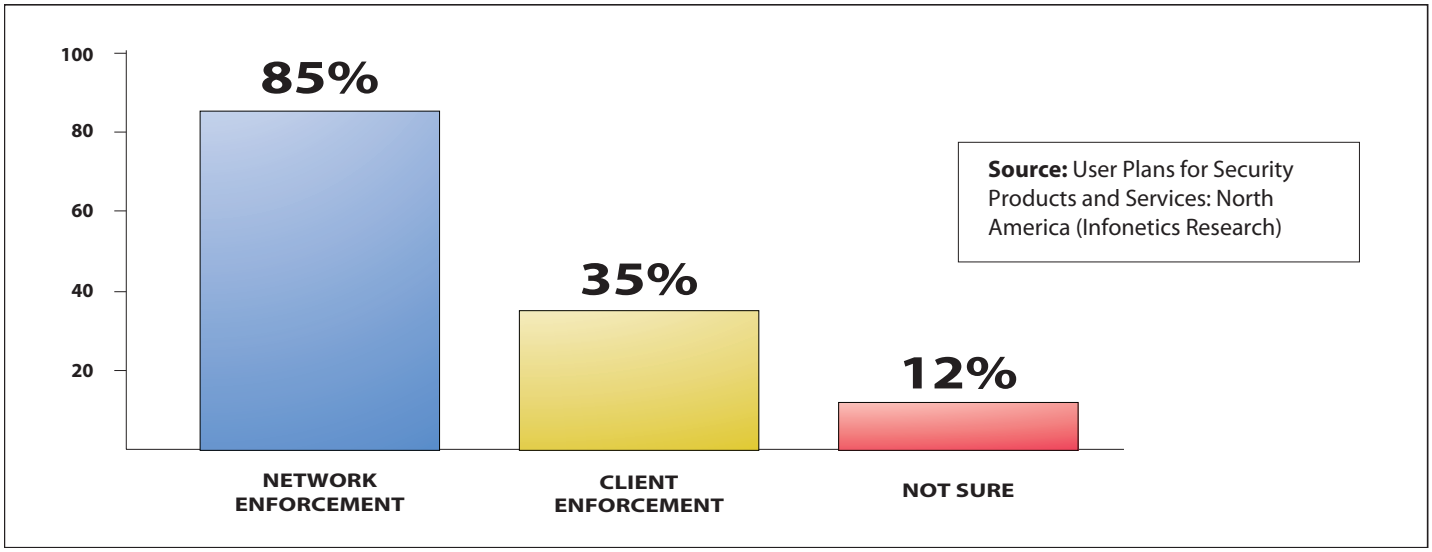

Figure 2: Preferred type of NAC enforcement

Post-connect Monitoring and Enforcement

If a device connects and is found compliant, is it allowed access to the network indefinitely? What happens if it's connected for a period of time and then violates a security policy? Will the NAC solution be able to detect this violation and offer the same level of flexibility in enforcement as was offered at the point of connection? Regardless of the benefits of device detection and inspection at the point of connection, post-connection policy enforcement is a critical feature of any effective NAC system.

A NAC solution must continue to monitor all connected devices throughout their network session to ensure that they remain in compliance with corporate security policies and are not acting in a malicious manner. For example, if a user decides to install an unauthorized application after passing the initial inspection, a NAC system that only inspects devices at the point of connection is rendered powerless against the policy violation.

NAC AT WORK

Defending Against Malware

A Fortune 100 software company was in the process of deploying ForeScout CounterACT when the corporate network was hit by a previously unknown worm, infecting devices throughout the enterprise network.

When the smoke cleared, the only segment of the network that did not experience massive outages caused by the worm was the building protected by ForeScout CounterACT. With its full-blocking mode enabled, the device identified the few infected sources on the protected segment of the network, completely blocked all worm traffic, and removed or quarantined any remaining infected devices.

Enforcement Against Malware and Self-Propagating Threats

Many NAC solutions available today are missing a key element of ensuring secure network access control: self-propagating threat detection and mitigation. While the system configuration check is a critical step in determining whether a device should be allowed to connect, it is a pre-emptive method of ensuring policy compliance. However, the presence of malware or any other type of self-propagating code poses an immediate security threat to the enterprise network.

Most enterprise networks already have some sort of anti-malware solution in place, but a NAC system is truly a front-line defense mechanism against such threats. Malicious code is designed to propagate itself as quickly as possible, and can be unleashed onto the network in a matter of seconds. Malware detection and mitigation is a must-have feature for any NAC system, to ensure infected devices are detected and blocked/quarantined before they have a chance to unleash an outbreak across the entire enterprise network.

<table>
<tr><th>ALERT AND INFORM</th><th>RESTRICTIVE ACCESS</th><th>MOVE AND DISABLE</th></tr>
<tr><td>Open Trouble Ticket</td><td rowspan="2">Deploy a Virtual Firewall around an infected or non-compliant device</td><td rowspan="2">Reassign device from production VLAN to a quarantine VLAN</td></tr>
<tr><td>Send Email</td></tr>
<tr><td>SNMP Traps</td><td rowspan="2">Reassign the device into a VLAN with restricted access to resources and services</td><td>Block access with 802.1X</td></tr>
<tr><td>Syslog</td><td rowspan="2">Alter the end user's login credentials to restrict or completely block access</td></tr>
<tr><td>HTTP Browser Hijack</td><td rowspan="2">Update access lists on switches, firewalls and routers to restrict access</td></tr>
<tr><td>Auditable End-User Acknowledgement</td><td>Block access with device authentication</td></tr>
<tr><td>Self-Remediation</td><td rowspan="2">Automatically move device to a pre-configured guest network</td><td>Turn off physical switch port</td></tr>
<tr><td>SMS, PatchLink Integrations</td><td>Terminate unauthorized applications</td></tr>
</table>

Figure 3: Flexible policy enforcement options

Section 3
Deploying Network Access Control

In evaluating a NAC solution, it is essential to fully understand the complete scope of the deployment process. Similar to the agent vs. agentless considerations, there are a variety of ways to deploy NAC into the network infrastructure. For the purposes of this examination, three NAC deployment approaches will be discussed: Switch-based NAC, inline and out-of-band appliances.

NAC as part of the Switching Infrastructure

The concept of NAC originated from the switch industry, with the idea of integrating some form of admission control directly into the switch to add an additional layer of security. Like many other theories, this one had great merit conceptually but faced a number of implementation challenges. For instance, the integrated switch approach was designed to only look at endpoint compliance at the moment that the device connected to the network, not afterwards. Admission mechanisms rely on the endpoint communicating through an open standard communication protocol (802.1x) in order to gain access to the network. The switch would look for the 802.1x supplicant upon connection and grant or deny admission based on the identification result

Other shortcomings of this approach include poor detection and posture assessment of unmanaged system and devices such as printers and smartphones. More importantly, this method creates a highly restrictive enforcement environment that is extremely disruptive to network operations. Some legacy switching hardware is not 802.1x compatible, so deploying this technology requires a "forklift" upgrade of the switching infrastructure, which is disruptive and costly. The 802.1x architecture is also brittle and non-tolerant of configuration errors. Tales abound of widespread outages and business disruption caused by an 802.1x configuration failure. For all these reasons, 802.1x architectures have yet to achieve broad-based acceptance and deployment.

Inline NAC

Aninline NAC deployment is based on the premise that all data traffic passes through the device to successfully detect, inspect and enforce policy. Once a device connects, the inline NAC appliance begins the process of inspecting each packet. Based upon the traffic emanating from the endpoint, the connecting device can be granted full access or some form of limited access to network resources. Typically, this approach utilizes a 'quarantine by default' method to ensure the system has enough information to determine the health of the endpoint and the access rights associated with the device user. Inline systems typically depend on an agent to achieve a thorough endpoint compliance status inspection.

A bigger challenge of deploying an inline product is the physical effects of introducing another hardware component into the flow of traffic. Inline deployments introduce an addi-tional point of failure and create significant latency risks, both of which are disruptive to users and restrict network performance. If an inline appliance fails, it subsequently blocks any device trying to pass network traffic through it. Both of these downsides negatively impact the end user's experience and are likely to cause network disruptions.

Another point for consideration is the number and location of inline appliances required to achieve a comprehensive NAC deployment. Inline products work best when they are close to the connecting device. Invariably, an inline appliance has to be paired with, and in some cases replace the access layer switch. For a small to medium business, this may be limited to just several appliances, but a global enterprise-wide deployment would require a significant investment in cost, time and resources to implement a complete NAC deployment.

Out-of-Band NAC

Out-of-band NAC deployments leverage the existing network infrastructure to detect, inspect, and enforce policy on connecting and connected devices. This approach requires the NAC appliance to be attached to the network either through a span port on a managed switch/router or through a network tap. From this point of connection, the NAC appliance is able to monitor all network traffic without data actually passing through the device. By deploying in this manner, enterprises can avoid the de ployment challenges caused by inline deployments, even if a specific network configuration limits some of the available enforcement actions that are otherwise available in a switch span port type of deployment (i.e., physical switch port block).

Leveraging an existing switch infrastructure allows IT organizations to deploy a NAC system with few, if any, modifications to the existing network configuration. This prevents immediate and costly switch upgrades allowing a lifecycle extension to existing infrastructure. Additionally, this approach further reduces deployment costs by placing the NAC appliance at a higher level on the network (typically from a distribution layer switch), which provides a greater level of

coverage while requiring a smaller number of appliances.

Infrastructure Integration

Seamless integration into the switch infrastructure is a very important requirement for any NAC solution. However, a comprehensive NAC system must extend beyond just hardware in order to fully leverage its policy enforcement capabilities. For example, if a connecting device does not have the required security patches installed, a comprehensive NAC system can streamline the remediation process by leveraging an existing ticketing or remediation systems, or even prompt the end user with self-remediation options to quickly bring the device into compliance and back onto the network. A well integrated NAC system maximizes the value of its policy enforcement offering as well as the value of the existing investment into network infrastructure components.

Non-disruptive Deployment and Policy Enforcement

The out-of-band approach is by far is the least disruptive method for a NAC deployment. However, the level of network disruptions caused by the implementation of policy enforcement actions is one of the most visible factors in determining the rate of success of a NAC deployment. Adding to the above-mentioned requirement for a flexible range of enforcement actions, it is critical that a NAC system provides administrators with the ability to monitor network security events per their defined policies without taking any actual enforcement actions. By determining the state of the network devices in relation to the requirements defined in the security policies, IT managers can make educated decisions on what type of enforcement actions to take against specific violations to eliminate security vulnerabilities without disrupting end-user experience or network operations.

NAC AT WORK

Seamless Integration

An agency of the United States Government deployed CounterACT on their inter-bureau backbone as well as VPN gateways and remote locations without making any changes to the intricate infrastructure. In addition to seamlessly integrating with all hardware components, CounterACT integrated with a number of third-party systems including vulnerability assessment, helpdesk and remediation.

Conclusion

Network Access Control is quickly becoming a critical network infrastructure element as enterprises work to defend their networks from non-compliant, unauthorized, unknown and/or infected devices. However it is important to have a clear understanding of all decision-determining factors in order to attain a NAC system that meets the enterprise security policy requirements. NAC can be powerful tool, but it needs to be evaluated with business process in mind as security always needs to be balanced against business goals and user productivity.

A comprehensive NAC system must provide flexible and granular policy-based coverage with the least amount of network and user disruption. ForeScout's flagship NAC product, CounterACT (see appendix 1 for a detailed description), is a clientless, out-of-band NAC appliance that provides granular policy creation matched with a full spectrum of enforcement actions. ForeScout CounterACT enables IT managers to define the appropriate responses to policy violations, effectively delivering a measured approach of enforcement to keep networks safe while minimizing the end-user disruptions. Striking a balance is key and deploying a flexible NAC product, like ForeScout CounterACT, is the only way to accomplish this critical task.

Appendix

ForeScout's NAC Solution: CounterACT

ForeScout CounterACT is an automated security control platform that lets you see and control everything on your network—all devices, all operating systems, all applications, all users. ForeScout CounterACT lets employees and guests remain productive on your network while you protect critical network resources and sensitive data.

Based on third-generation network access control (NAC) technologies, ForeScout CounterACT is easy to install because it requires no software, no agents, no hardware upgrades or reconfigurations. Everything is contained within a single appliance.

ForeScout CounterACT delivers a wide range of policy enforcement options to custom-fit response actions to policy violations to ensure there are no disruptions to the network or normal business operations. CounterACT is deployed completely out-of-band, and requires no equipment upgrades or costly infrastructure changes.

The ForeScout Difference

ForeScout's agentless NAC is the only solution in the industry that delivers these essential features:

» **One box, one day to install —** Everything is contained in a single appliance. Setup is easy with built-in configuration wizards.

» **ForeScout works with what you have —** All your existing switches, routers, firewalls, endpoints, patch management systems, antivirus systems, directories, ticketing systems—ForeScout CounterACT works with them. No infrastructure changes are needed.

» **No software required —** ForeScout CounterACT is agentless, which means it works with all types of endpoints—managed and unmanaged, known and unknown, authorized and rogue. The moment that a device connects to your network, CounterACT determines if the device is company owned or whether it belongs to a guest or contractor. If the device is a part of the domain, CounterACT can launch a device scan to check for policy compliance status. If the device is not part of the domain, CounterACT can provide multiple enforcement mechanisms to automatically ensure the guest/contractor has enough access to remain productive without compromising the security of the enterprise network. The in-depth scan of managed and unmanaged devices requires no client or agent to reside on the device. For customers that have specific need for agents, or who want deep inspection of Android devices, ForeScout provides lightweight agents that can be deployed in a variety of manners, including dissolvable.

» **Non-disruptive —** Unlike first generation NAC products that immediately disrupt users with heavy-handed access controls, ForeScout CounterACT can be deployed in a phased approach which minimizes disruption and accelerates results. In the initial phase, CounterACT gives you visibility to your trouble spots. When you want to move forward with automated control, you can do so gradually, choosing an appropriate enforcement action. CounterACT provides a full spectrum of enforcement actions to provide a high level of flexibility in addressing minor and moderate policy violations. This ensures that user productivity is limited only to critical network security violations.

» **Accelerated results —** ForeScout CounterACT provides useful results on Day 1 by giving you visibility to problems on your network. The built-in knowledge base helps you configure security policies quickly and accurately.

» **Scalability —** ForeScout offers a variety of capacity, management, and support options to satisfy smaller, mid-tier networks, as well as more expansive deployments within larger, global enterprises. A single CounterACT console is capable of managing over 250,000 endpoints.

» **Tiered mobile security solutions —** ForeScout provides IT organizations the means to cost-effectively offer a tiered level of service to meet the needs of mobile users throughout your organization. Starting with network access control, you can add ForeScout Mobile and integrate with 3rd party MDM systems for a select population of high-value users.

» **Post-connection monitoring —** CounterACT monitors the behavior of all devices throughout the duration of the connection. Each device is monitored for any form of self-propagating malicious threat. CounterACT's integrated IPS provides real time detection and protection from the spread of the threat. This is accomplished without quarantine by default requirement, so that compliant users do not experience any change in login behavior.

» **Out-of-Band Deployment** CounterACT typically is deployed from a distribution switch. The out-of-band deployment ensures that there is no disruption to the network. See typical deployment architecture in the diagram below:

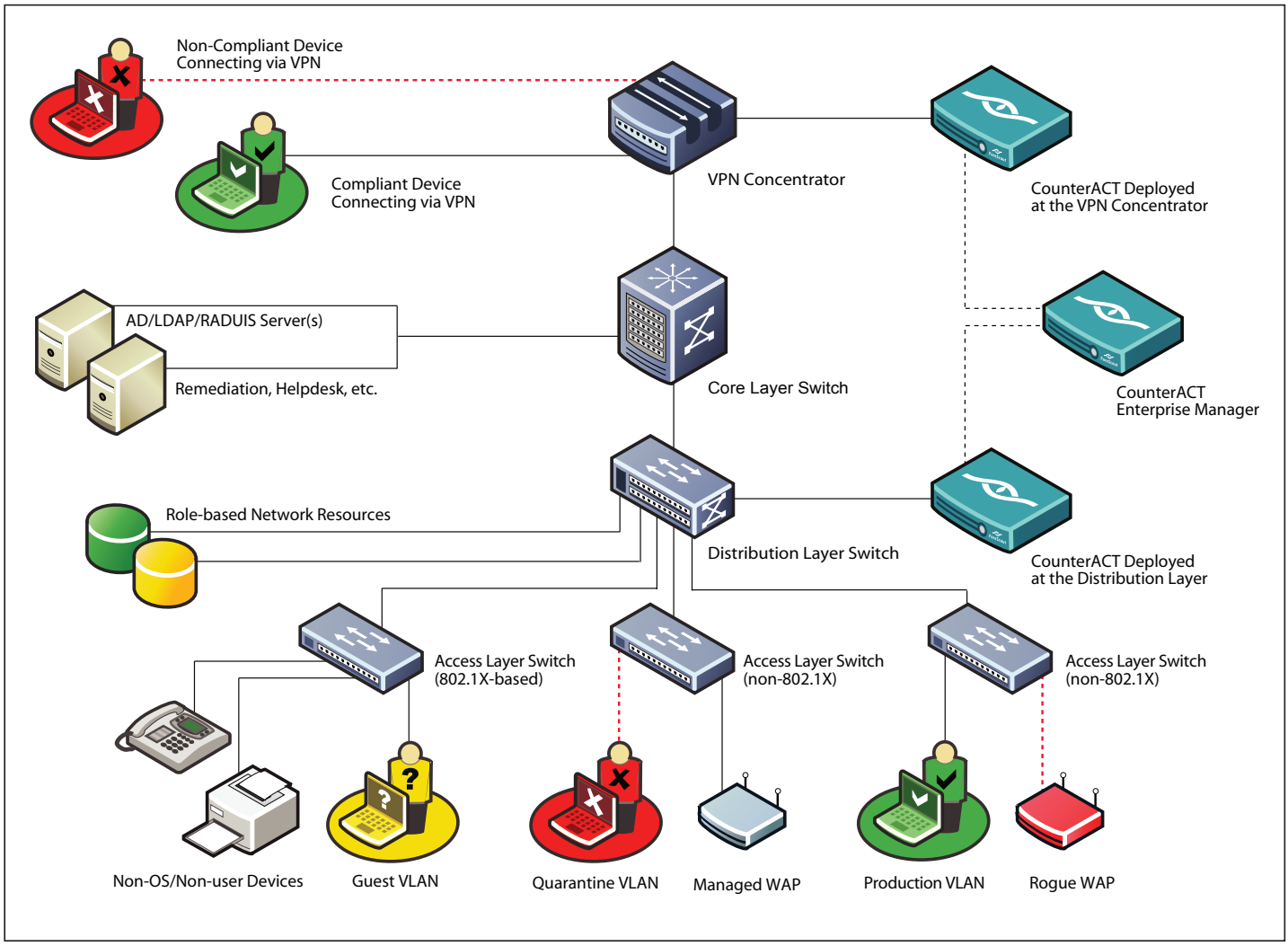

Figure 4: Typical ForeScout CounterACT deployment scenario

ForeScout Technologies, Inc.
10001 N. De Anza Boulevard, Suite 220
Cupertino, CA 95014, USA

Toll-free: 1.866.377.8771 (US)
Tel: 1.408.213.3191 (Intl.)
Fax: 1.408.213.2283

www.forescout.com

© 2012 ForeScout Technologies, Inc. Products protected by US Patent #6,363,489, March 2002. All rights reserved. ForeScout Technologies, the ForeScout logo, CounterACT, CounterACT Edge and Active Response are trademarks of ForeScout Technologies, Inc. All other trademarks are the property of their respective owners. FS-WP071812