

A guide to model and compare NAC solutions

Feature Guide

Universal NAC Feature Model

All NAC products are not created equal and there is not a one-NAC-fits-all solution. This is a guide to model network access control features from a variety of vendors. It aids in the comparison and analysis of available features and provides a common language to identify and describe methods and execution of technology. This allows for useful comparisons across vendors who offer the same features, but with drastically different methods.

**RSA Release
2010-03-03**



Universal NAC Feature Model

A guide to model and compare NAC solutions

All NAC products are not created equal and there is not a one-NAC-fits-all solution. This is a guide to model network access control features from a variety of vendors. It aids in the comparison and analysis of available features and provides a common language to identify and describe methods and execution of technology. This allows for useful comparisons across vendors who offer the same features, but with drastically different methods.

Jennifer Jabbusch

Carolina Advanced Digital, Inc.

<http://cadinc.com>

<http://SecurityUncorked.com>

© 2010 Carolina Advanced Digital, Inc., all rights reserved

This document may not be reproduced in part or whole without explicit written permission from Carolina Advanced Digital, Inc. To request permission, see contacts in Appendix B.

Table of Contents

Table of Contents.....	5
I. Overview	7
II. The four feature components of NAC	8
Access Management versus Threat Management	10
III. Vendor Mechanics of the Four Feature Components.....	11
IV. Hierarchy of NAC Functions and Vendor Mechanics	13
V. Explanation of the mechanics.....	15
Endpoint Discovery	15
Authentication	16
Enforcement	17
Endpoint Evaluation	18
VI. About the Author	21
About Carolina Advanced Digital, Inc.....	21
Contact	21
VII. Appendix A: Resources.....	22
VIII. Appendix B: Feedback	23

I. Overview

All NAC products are not created equal and there is not a one-NAC-fits-all solution.

The Universal NAC Feature Model was developed for internal use at Carolina Advanced Digital and is invaluable in informing and guiding discussions with clients evaluating NAC solutions. Initially intended for private use, the value to the larger industry has led to the development of this material in guidebook form.

One of the leading challenges in discussing NAC is the terminology. Instead of referring to vendor terms or the random acronyms and naming convention used in the NAC frameworks, this guide uses plain English to describe the four feature components of network access control systems and the specific mechanics used to implement the technologies.

This Universal NAC Feature Model is a guide for organizations to model network access control (NAC) features from a variety of products and vendors. It aids in the comparison and analysis of available features and provides a common language to identify and describe required methods and execution of technology. This allows for useful comparisons across vendors who offer the same features, but with drastically different methods.

This document breaks down all the components and mechanics employed by various vendors, explains each piece in detail, and provides commentary on factors to consider while investigating NAC products. The tables and explanations in this guide can be used to map key concepts to their vendor-specific counterparts and map a desired feature to the mechanics that support it.

To all readers, I hope you enjoy the information in this guide and find the layout and explanations useful. As far as I know this is the first document of its kind, outlining the full depth and breadth of NAC features, functions and mechanics from all vendors, in a single guide. I expect it to serve as a foundation for discussions in the industry and in dialogue between consumers and vendors.

This document provides:

- A uniform terminology and descriptions of features and technical mechanics to compare all NAC products currently available.
- A hierarchical view of NAC features and mechanics in a simple one-page table.
- An explanation of the technical mechanics of NAC and commentary on considerations as you investigate NAC solutions.
- A foundation that will grow and be updated as technologies and products change in the market.

II. The four feature components of NAC

This section of the document was taken directly from the accompanying whitepaper “*Catching the Unicorn: a technical exploration of why NAC is failing*”, available online at <http://SecurityUncorked.com> and <http://www.cadinc.com>.

This section will clarify terminology by defining four feature components of NAC, used for describing and comparing various NAC solutions, and explore how these pieces fit together and overlap. In the following section, we’ll see how vendors apply various technologies to offer these feature components.

At first consideration, many colleagues don’t agree with my breakdown of the four feature components. However, after explaining the theory behind each one, they usually are in agreement by the end of the conversation. If you ask most professionals and vendors, they’ll each tell you NAC has two or three (not four) components.

Some components are interdependent, while others remain independent. I’ve arranged them in the most logical order I can, with the understanding that they are not necessarily in a specific order of chronology or dependency.

The four feature components of NAC are: Authentication, Access Rights, Endpoint Integrity and Behavior Monitoring.

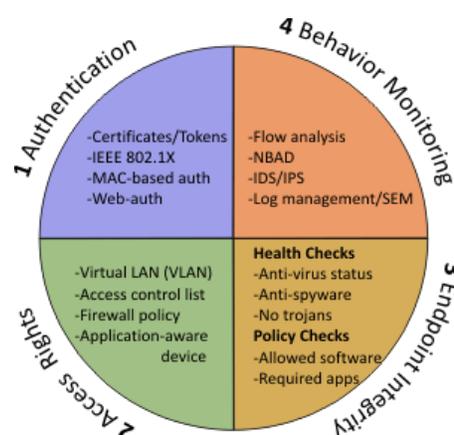


Figure 1 Four feature components

1. Authentication

Who or what are you?

The first of the four components, authentication is much broader than it may initially appear. Authentication frequently refers to user authentication, where a person submits credentials (such as username and password) to be verified. Authentication in NAC could also mean device authentication using certificates, or even more generally, it could mean device *identification*, by way of MAC address.

Certain processes of authentication are actually only identification by virtue of the fact that nothing is in place to validate or verify that the device is who or what it says it is. A MAC address can be easily spoofed, and systems using MAC addresses for access are really only identifying the system, not authenticating it. For our purposes here though, identification will be described as a type of authentication.

2. Access Rights

Where are you allowed to go?

Access rights dictate what resources a user or device on the network can access. Again, the term is broad since access rights can be dependent on a variety of variables and enforced by an assortment of methods.

Frequently, organizations apply access rights via role-based VLANs (virtual LANs), user-based resource access or location- and time-based rules that dictate who can access what resources when. Access rights may be dependent on such things as:

- User type or role (user group membership)
- Access location (geographic)
- Access method (direct via LAN, remote access/VPN or wireless)
- Device posture (whether the device is healthy and compliant)
- Date and time (standard business hours use or after-hours access)
- Combinations of any of the above

Access rights may be enforced by VLANs, access control lists, firewall policies, layer 7 application-aware devices, self-enforcing software agents and other means.

3. *Endpoint Integrity*

What is the current condition of the device?

To most consumers of the technology, endpoint integrity *is* NAC. The correlation is odd, since the vast majority of organizations looking at NAC are *not* looking at it to satisfy endpoint integrity needs.

Endpoint integrity is an evaluation of the endpoint, or device connecting to the network, on several criteria. These endpoint evaluations fall under two primary categories: health-based endpoint integrity checks and policy-based endpoint integrity checks.

Health-based endpoint integrity checks evaluate the device for potential security risks directly related to its health posture. These tests would include checking for up-to-date anti-virus definitions, the presence of anti-spyware, any matches on known virus signatures and so on. If the endpoint appears to be infected with malicious code or is a likely candidate to become infected, it should not pass an organization's health checks.

Policy-based endpoint integrity checks, on the other hand, evaluate an endpoint's posture against allowed configurations in the corporate policy. These policies may address acceptable use or compliance issues and restrict the use of, or access to, resources and applications which may be harmful to the organization indirectly. Examples of common policy-based checks may be to disallow the use of peer-to-peer software or instant messaging.

The upcoming section on *Access Management versus Threat Management* explores how the four components of NAC and the two sub-components of endpoint integrity fit in the access versus threat model.

4. *Behavior Monitoring*

Are you behaving strangely on the network?

Discussing behavior analysis as a component of NAC is where the most eyebrows get raised. It's imperative that we include it in the list since a handful of current vendors essentially have entire NAC solutions built around behavior analysis, and I believe it will become a more significant piece of NAC solutions of the future.

Behavior monitoring (or analysis), like other feature components, can be attained through a variety of means. It may happen in the form of flow analysis (from technologies such as sFlow and NetFlow) that samples traffic on the network, it may happen by other network behavior anomaly detection (NBAD) methods or even by monitoring from an IDS or IPS device that's trained to match behavior against a baseline of expected network traffic. In certain cases, log management and security event management (SEM) can provide various levels of anomaly detection as well. In the most extreme cases, behavior monitoring may include a component that identifies and interacts with malicious traffic, such as answering reconnaissance and scanning applications.

Behavior analysis, in whatever form it materializes, will usually identify both malicious behavior (attacks, ping sweeps, failed login attempts) as well as potentially harmless but unusual actions on the network (traffic over strange ports, or two devices talking that don't usually communicate).

Access Management versus Threat Management

The concepts of NAC are really meant to address access management, threat management or a combination of both. Access management controls who gets on the network and what resources they have access to once they're connected. Of the four feature components, access management generally encompasses Authentication and Access Rights as well as some aspects of Endpoint Integrity.

Threat management addresses direct security liabilities on the network such as protection against viruses, malware and other malicious attacks or activity to or from a device. Of the four feature components, threat management includes most Endpoint Integrity checks and Behavior Monitoring.

We can apply the access management versus threat management model to a variety of security technologies outside the scope of NAC.

Table 1 Access management vs threat management

Access Management		Threat Management	
Authentication	Access Rights	Endpoint Integrity	Behavior Monitoring
-Certificates/Tokens	-Virtual LAN (VLAN)	Health Checks	-Flow analysis
-IEEE 802.1X user auth	-Access control list	-Anti-virus status	-NBAD
-MAC-based auth	-Firewall policy	-Anti-spyware	-IDS/IPS
-Web-auth	-Application-aware device	-No trojans	-Log management/SEM
		Policy Checks	
		-Allowed software	
		-Required apps	

III. Vendor Mechanics of the Four Feature Components

Now that we've outlined the basic features offered by NAC solutions, we can look at the different methods vendors employ to offer those features. Again, many products offer the same functions, but they may go about it in very diverse ways. Disappointment with NAC products in organizations with failed implementations is most often caused by a poor choice of technology, specifically vendor mechanics that don't mesh with the environment they're integrated with. Selecting the right type of technology is key to finding the right NAC solution for your organization. The following sections will outline what to look for.

We'll refer to the underlying processes and methods by which vendors support a feature as the vendor mechanics. We can then correlate the vendor mechanics to the four common feature components to understand how different products will operate in environments.

At a very high level, we can match a few fundamental vendor mechanics to the feature components, such as:

Feature Component	Fundamental Vendor Mechanics
1. Authentication	1. Endpoint Discovery mechanics
2. Access Rights	2. Enforcement mechanics
3. Endpoint Integrity	3. Endpoint Evaluation mechanics
4. Behavior Monitoring	3b. Subset of Endpoint Evaluation mechanics

At this point, I'd recommend looking over the Vendor Mechanics Hierarchy table and getting acquainted with the concept of the four feature components and the corresponding fundamental mechanics. It's a good visual of how everything fits together and serves as a good launching point before diving into the detailed explanations of the vendor mechanics.

IV. Hierarchy of NAC Functions and Vendor Mechanics

Feature Component	Fundamental Mechanic	Specific Mechanics							
Authentication	Endpoint Discovery	<ul style="list-style-type: none"> ▪ DHCP watching ▪ ARP/MAC table gathering ▪ Port authentication requests ▪ Registration ▪ LLDP-MED 							
	Authentication	<table border="0"> <tr> <td> <ul style="list-style-type: none"> ▪ Device MAC registration </td> <td> <ul style="list-style-type: none"> ▪ Pre-registration ▪ Registration on discovery </td> </tr> <tr> <td> <ul style="list-style-type: none"> ▪ 802.1X port security </td> <td> <ul style="list-style-type: none"> ▪ Certificates ▪ Username/Password ▪ Tokens/Smart Cards </td> </tr> <tr> <td> <ul style="list-style-type: none"> ▪ MAC port security </td> <td></td> </tr> <tr> <td> <ul style="list-style-type: none"> ▪ Web or captive portal </td> <td></td> </tr> </table>	<ul style="list-style-type: none"> ▪ Device MAC registration 	<ul style="list-style-type: none"> ▪ Pre-registration ▪ Registration on discovery 	<ul style="list-style-type: none"> ▪ 802.1X port security 	<ul style="list-style-type: none"> ▪ Certificates ▪ Username/Password ▪ Tokens/Smart Cards 	<ul style="list-style-type: none"> ▪ MAC port security 		<ul style="list-style-type: none"> ▪ Web or captive portal
<ul style="list-style-type: none"> ▪ Device MAC registration 	<ul style="list-style-type: none"> ▪ Pre-registration ▪ Registration on discovery 								
<ul style="list-style-type: none"> ▪ 802.1X port security 	<ul style="list-style-type: none"> ▪ Certificates ▪ Username/Password ▪ Tokens/Smart Cards 								
<ul style="list-style-type: none"> ▪ MAC port security 									
<ul style="list-style-type: none"> ▪ Web or captive portal 									
Access Rights	Enforcement	<table border="0"> <tr> <td> <ul style="list-style-type: none"> ▪ Inline appliance </td> <td> <ul style="list-style-type: none"> ▪ Standard communications ▪ Proprietary communications </td> </tr> <tr> <td> <ul style="list-style-type: none"> ▪ Client software </td> <td> <ul style="list-style-type: none"> ▪ Self-imposed ACLs ▪ Controller-imposed ACLs ▪ Tunneled enforcement </td> </tr> <tr> <td> <ul style="list-style-type: none"> ▪ Out of band management </td> <td> <ul style="list-style-type: none"> ▪ Layer 2 VLANs ▪ Layer 3 IP/ACLs </td> <td> <ul style="list-style-type: none"> ▪ SNMP config ▪ CLI config ▪ RADIUS attribute ▪ Firewall rules </td> </tr> </table>	<ul style="list-style-type: none"> ▪ Inline appliance 	<ul style="list-style-type: none"> ▪ Standard communications ▪ Proprietary communications 	<ul style="list-style-type: none"> ▪ Client software 	<ul style="list-style-type: none"> ▪ Self-imposed ACLs ▪ Controller-imposed ACLs ▪ Tunneled enforcement 	<ul style="list-style-type: none"> ▪ Out of band management 	<ul style="list-style-type: none"> ▪ Layer 2 VLANs ▪ Layer 3 IP/ACLs 	<ul style="list-style-type: none"> ▪ SNMP config ▪ CLI config ▪ RADIUS attribute ▪ Firewall rules
<ul style="list-style-type: none"> ▪ Inline appliance 	<ul style="list-style-type: none"> ▪ Standard communications ▪ Proprietary communications 								
<ul style="list-style-type: none"> ▪ Client software 	<ul style="list-style-type: none"> ▪ Self-imposed ACLs ▪ Controller-imposed ACLs ▪ Tunneled enforcement 								
<ul style="list-style-type: none"> ▪ Out of band management 	<ul style="list-style-type: none"> ▪ Layer 2 VLANs ▪ Layer 3 IP/ACLs 	<ul style="list-style-type: none"> ▪ SNMP config ▪ CLI config ▪ RADIUS attribute ▪ Firewall rules 							
Endpoint Integrity Behavior Monitoring	Endpoint Evaluation	<table border="0"> <tr> <td> <ul style="list-style-type: none"> ▪ Preventative </td> <td> <ul style="list-style-type: none"> ▪ Heavy client agent ▪ Dissolvable agent ▪ Local host scan ▪ Remote host scan </td> <td> <ul style="list-style-type: none"> ▪ Health scans ▪ Policy scans </td> </tr> <tr> <td> <ul style="list-style-type: none"> ▪ Reactive </td> <td> <ul style="list-style-type: none"> ▪ IDS/IPS ▪ Flow analysis/NBAD </td> <td> <ul style="list-style-type: none"> ▪ Feedback to controller, infrastructure, host or IF-MAP </td> </tr> </table>	<ul style="list-style-type: none"> ▪ Preventative 	<ul style="list-style-type: none"> ▪ Heavy client agent ▪ Dissolvable agent ▪ Local host scan ▪ Remote host scan 	<ul style="list-style-type: none"> ▪ Health scans ▪ Policy scans 	<ul style="list-style-type: none"> ▪ Reactive 	<ul style="list-style-type: none"> ▪ IDS/IPS ▪ Flow analysis/NBAD 	<ul style="list-style-type: none"> ▪ Feedback to controller, infrastructure, host or IF-MAP 	
<ul style="list-style-type: none"> ▪ Preventative 	<ul style="list-style-type: none"> ▪ Heavy client agent ▪ Dissolvable agent ▪ Local host scan ▪ Remote host scan 	<ul style="list-style-type: none"> ▪ Health scans ▪ Policy scans 							
<ul style="list-style-type: none"> ▪ Reactive 	<ul style="list-style-type: none"> ▪ IDS/IPS ▪ Flow analysis/NBAD 	<ul style="list-style-type: none"> ▪ Feedback to controller, infrastructure, host or IF-MAP 							

V. Explanation of the mechanics

Authentication

Endpoint Discovery is how a NAC solution learns about endpoints connecting to the network. Inline devices have an obvious method by which to make this discovery; the endpoints are connecting through the device directly and are therefore immediately seen by the system. Out of band and software-based solutions use a range of mechanics to gather knowledge of connecting devices, including:

DHCP Endpoint Discovery. Many out of band products will listen for DHCP requests and replies, frequently through a switch port configured to mirror traffic to and from one or more DHCP servers. The process is pretty clean but clearly this method of discovery loses value if portions of the network have statically-configured IP addresses. There are some professionals that would argue this method is less secure since it doesn't discover statically configured devices and because it will miss traffic to DHCP servers (rogue or otherwise) that the system isn't aware of. Although the argument is true, most enterprises have the ability to manage and monitor DHCP via the infrastructure, for example with DHCP snooping and ARP protection technologies on switches.

ARP/MAC Endpoint Discovery. Many NAC products (especially from switch vendors) will learn about connecting endpoints by capturing traps or pulling ARP and MAC tables from the switches. Systems that rely on traps for notification will have the switches send link up, link down and MAC learn traps to the NAC controller. Some solutions layer these notifications with occasional polling of the network devices for ARP and MAC table updates.

Port Authentication Endpoint Discovery. In a method similar to the notifications described in the previous method, switches can also alert a NAC controller when a port authentication request is made. This configuration is used when the organization has edge port security, such as 802.1X or MAC-authentication configured. At the time of authentication, the switch learns of the endpoint and can pass any information to a NAC controller or authentication server.

Registration-based Endpoint Discovery. A number of NAC solutions offer device registration options. With these systems, users can register their own devices upon connecting, or network administrators can pre-register authorized devices in bulk. The former is especially popular in higher education environments that have a high turnover in student population and the desire to support multiple devices (laptop, iPod) attached to a single user account. With this type of on-demand registration, the primary discovery method is one of the three mentioned above. In the latter scenario with pre-registration, the system is already aware of the device's existence and may not need to discover it in the traditional sense each time it connects. Registration systems tie in directly with authentication (discussed in later sections).

Link Layer Discovery Protocol- Media Endpoint Discovery. LLDP-MED is an enhancement of LLDP commonly used to provision headless devices such as voice over IP (VoIP) phones in an enterprise environment. The LLDP facilitates endpoint discovery by announcing the new device while the MED extension grabs appropriate network settings (VLAN, quality of service and PoE configurations) for the device.

Authentication is the method by which the NAC solution identifies the connecting user or device as being an authorized user of the network. I use the term *identifies* here since some of the methods of authentication are really, in fact, only identification (ie MAC addresses). This is explained more in the *Catching the Unicorn* whitepaper. It's important to note that some NAC solutions omit this feature and simply use Endpoint Discovery in combination with Endpoint Evaluation to make a determination of whether the user or device should be on the network. For solutions that do incorporate Authentication, they're most often using one of the following mechanics:

Device MAC Registration. I'll lead off with this as a continuation of the Registration bullet under Endpoint Discovery. As mentioned earlier, a number of NAC products use a registration system that serves as a white list of allowed devices. In addition to the device registration (via MAC address) the system may also enforce a user logon of some sort to authenticate the user in addition to the device. Other products will allow a user to attach a few devices (again, laptops, iPods) to their user account as a one-time registration and not require re-authentication of the user unless another new device is added to their account. Device MAC registration can be compared to MAC filter lists on switches, but incorporated in a NAC solution, it offers a central point of management, direct attachment to a directory server for a single pool of users and devices and the ability to layer additional integrated security such as host checking and more advanced access rights.

802.1X Port Security. Also referred to as layer 2 enforcement, 802.1X uses an IEEE standard for port security to force endpoint authentication at the edge, on the switch port. This mechanic is a stark contrast to solutions that use MAC registration. With 802.1X enabled, the traffic from a connecting endpoint cannot be passed through a switch to a NAC controller (or anywhere) until the switch confers with an authentication server and gives the go-ahead. Once the switch authenticates the device it can either simply enable the port for communication or enable the port *and* move it to a different layer 2 VLAN, thereby imposing VLAN-based access control (discussed later in the Enforcement section). The 802.1X process can also be used to impose layer 3 ACLs, but this is so rarely used I've decided to omit it from discussion here. If using 802.1X, the process may be used to authenticate a device (via certificates) or a user (via logon credentials or tokens/smartcards). Although extremely secure, 802.1X implementations are very difficult to implement and even harder to maintain.

MAC Port Security. A mechanic exceptionally similar to 802.1X Port Security, MAC Port Security uses the same underlying authentication infrastructure, but instead of passing user or device credentials, it uses only the device MAC address to authenticate. These two mechanics are frequently comingled and lumped together but they are in fact different, and MAC-auth is not a part of the 802.1X standard. MAC Port Security is slightly easier to implement than 802.1X (for reasons described in more detail in *Catching the Unicorn*) but still has many of the same obstacles. Due to the complexity of these technologies (802.1X and MAC-auth), many organizations are moving toward NAC solutions that use Device MAC Registration systems (described above) in lieu of these edge port security options. To argue the other side of the point, these two authentication options intercept and authenticate endpoints at the point of connection and can offer a few security advantages because of that. Even NAC products that use a registration system with VLAN-flipping capabilities are not actually authenticating at the edge; the traffic is sent to a NAC controller inside the network.

Web or Captive Portal. Most users are familiar with the captive portal experience at hotels and coffee shops. This Authentication option is offered by most NAC products and is a good way to extend network services to guest users on the network.

Access Rights

Enforcement mechanics are the processes by which a NAC solution enforces decisions about network access upon an endpoint. Enforcement is how the system carries out actions such as moving endpoints to a different VLAN, applying access restrictions via ACLs or granting additional access rights. Options for Enforcement differ drastically among NAC products. Enforcement is by far the most challenging function of a NAC solution to implement and integrate into the network because it requires some manner of modification to either the endpoint or the network, in order to enforce the changes in Access Rights. Because of the complications with Enforcement, finding a vendor mechanic that works in your environment will likely be the deciding factor in selecting a NAC solution for your organization. The most popular mechanics of NAC Enforcement are:

Inline Appliance Enforcement. As noted earlier, inline appliances have unique advantages (and disadvantages) when it comes to Endpoint Discovery and Enforcement mechanics. An inline device is a switch-like appliance that sits between the endpoint and the rest of the internal network. It's the gatekeeper. The advantage of an inline NAC is that you don't have to muck around with the intricacies of configuring a NAC controller (out of band) to communicate with all of your network edge switches. Inline solutions can indeed offer a plug-and-play implementation with little to no impact on the end user or remainder of the network. The disadvantages can be numerous. Inline NAC solutions can be costly since you need to purchase hardware and physically install and manage more devices at the edge. It usually means more rack space, more support fees, more cables, another point of failure and possibly a dead end when it's time to upgrade. NAC solutions that integrate with the network switches already in place are using the technology you have. If and when you upgrade your switches to Gig PoE or 10GbE (for example) you can use the same NAC solutions and configurations. Inline NAC products frequently use proprietary vendor communications, so you may have an all-or-nothing solution with certain vendors when it's time to change, expand or upgrade.

Client Software Enforcement. NAC offerings that rely on software for Enforcement have grown as more antivirus and endpoint security vendors enter the NAC arena. These products leverage client software installed on the endpoint to enforce Access Rights dictated by the NAC controller. In many cases with client software Enforcement, the NAC controller may be a server (versus an appliance) although a few vendors offer both options. These software-based products receive instructions from the NAC controller then enforce the instructions on the host, either as a self-imposed ACL or through a controller-imposed ACL managed through a tunnel from the client to the controller. Although some argue self-imposed host ACLs are not reliable, in theory they should be no less effective than network-based NAC solutions that configure the host to use the controller as a default gateway (thereby controlling its traffic). The two are similar in nature but imposed differently. The client-to-controller tunneled Enforcement is an unattractive option for many organizations since they lose some of the visibility and network-based control of the traffic. Software-based enforcement will always operate at layer 3 (described in the next section) or higher.

Out of Band Enforcement. Most switch vendors in the NAC market offer an out of band (OOB) solution. OOB NAC products have a central NAC controller that communicates with an authentication server and all edge network devices, such as switches and access points. The OOB products offer advantages in scalability and flexibility over the inline products but the advantages come at a price; the NAC controller must communicate reliably and predictably with the rest of the network.

OOB solutions offer basic layer 2 and layer 3 enforcement options, in addition to a few proprietary vendor options (such as integration with firewalls). Layer 2 enforcement uses VLANs to control where an endpoint can go once it's on the network. VLANs are a layer 2 protocol, hence the term "layer 2 enforcement". Most layer 2 vendor solutions use (or support) 802.1X Port Security for the Authentication and can return RADIUS-assigned VLANs to the switch. A few vendors offer layer 2 enforcement using Device MAC Registration then flip VLANs at the edge port using SNMP strings or CLI commands to modify the switch configuration. Layer 3 enforcement uses IP addresses, default gateway assignments and ACLs to control where an endpoint can go on the network. The mechanics of layer 3 enforcement can also vary slightly. Some NAC products use the controller as the DHCP server to control endpoint IP configurations. Others use a combination of layer 2 (VLAN) assignment and layer 3 (IP) addressing to impose ACLs on switches, routers or firewalls.

Endpoint Integrity

Behavior Monitoring

Endpoint Evaluation is the analysis of an endpoint to determine its current health posture and/or compliance with organizational policies. Endpoint Evaluation can happen in countless ways. Vendors are incredibly creative when it comes to finding new ways identify potentially harmful endpoints. To start the breakdown, I group all Endpoint Evaluation mechanics in to two main categories:

Preventative Endpoint Evaluation. Preventative Endpoint Evaluation means the NAC solution is pro-actively looking at the endpoint to discover potentially harmful configurations or behavior. Preventative evaluation can help an organization verify endpoints are healthy and in compliance with corporate policy. In section II-3 of this document we outlined the difference between health checks and compliance checks; this evaluation offers visibility into both. When looking at Endpoint Evaluation options, organizations should also consider whether they want pre-connect or post-connect testing. Since an endpoint may become unhealthy after it's connected to a network, I strongly recommend pre- and post-connect evaluations for anyone using preventative endpoint evaluation. Pre-connect testing is not enough for most environments. Most NAC solutions with Endpoint Integrity features will offer evaluations in the form of heavy agents, dissolvable agents, local scanning, remote scanning, or a combination of two or more.

The most robust Endpoint Evaluation mechanic uses a heavy agent or client that sits on the endpoint (such as a computer), actively scans for configuration attributes, and reports findings back to the NAC controller. Heavy agents are advantageous when an organization needs granular visibility into, and control over, its managed endpoints. It can see more on the host and report back in a more timely manner than other evaluation methods. More advanced heavy agents can interact with the NAC system to remediate issues, such as re-enabling an antivirus automatically should the end user disable it. This type of auto-remediation greatly reduces the exposure time for vulnerabilities it's correcting. The disadvantages of heavy agents are the requirements to install and manage software on the endpoints, the possible need to support multiple operating systems and the inability to address evaluation of endpoints that the organization doesn't own (and therefore, on which it can't install software). Heavy agents are popular in homogenous environments, corporate and government settings and in organizations that are considered high risk and in need of the additional control of a full-time agent. Conversely, heavy or persistent agents are rarely used in higher education and similar heterogeneous settings.

Dissolvable agents are a popular choice for organizations that want to evaluate an endpoint they don't own or don't manage. These agents run on-demand, usually as a Java or ActiveX application, and then

tear down after the scan. Dissolvable agents offer visibility similar to heavy agents, but do not offer auto-remediation and real-time checks. Most dissolvable agents run once at the time of connection and do not offer persistent evaluation. The advantage of a dissolvable agent is the ability to perform a fairly thorough scan without installing a client on the endpoint. The browser-based applets are supported universally across operating systems and require no configuration.

In addition to agents, scans are another way to evaluate an endpoint. A local host scan is one method of active scanning that uses administrative credentials or domain privileges to gain access to an endpoint and run local scans of its configuration. Although rarely seen in NAC products, this evaluation mechanic can be an effective way to gather host data and report back to a NAC controller. It would have similar limitations to heavy agents; the organization would need to have domain management of the endpoint in order to use this technique. A more popular endpoint scan is the passive remote host scan, a method in which the NAC controller directly or indirectly (through 3rd party integration) initiates a scan of the endpoint (think Nessus or NMAP). Although placed in the preventative Endpoint Evaluation category, these scans are only preventative if configured correctly and run frequently enough to catch mis-configurations before they're a problem.

Reactive Endpoint Evaluation. We'll refer to reactive endpoint evaluation as an *evaluation* but understand that we've now moved from the feature of Endpoint Integrity to the feature of Behavior Monitoring. The workings of both features fall under the Endpoint Evaluation mechanics, but the resulting features are a bit different. If that sounds confusing, refer to the Vendor Mechanics Hierarchy table earlier in this document and see the yellow section labeled Endpoint Evaluation.

A reactive evaluation is the most rudimentary method a NAC solution can employ to offer Endpoint Evaluations. These mechanics are just as they sound; instead of proactively scanning an endpoint for posture analysis, these processes monitor the behavior of the endpoints and then take action once they see something negative. More and more NAC vendors are including 3rd party integration with their products. Today, many network-based NAC solutions can receive feedback from security devices on the network such as a firewall or IDS (intrusion detection system). These security devices can provide input to the NAC controller through SNMP traps, alerts or integration with TNC's IF-MAP framework. The IF-MAP framework includes a server that acts as a silo for security data from all parts of the network. Participating devices can contribute to the silo and pull information from it. (For more on IF-MAP see the resources at the end of this guide).

Along similar lines, NAC products may offer support for (or integration with) NBAD (network behavior anomaly detection) engines and flow analysis. Just as a firewall or IDS can provide feedback to the NAC controller, an NBAD engine can do the same. NBAD engines detect anomalous traffic on the network, a telltale sign of the presence of a worm or malicious traffic.

In both cases, the NAC controller uses the input from other network devices to make decisions about the health of an endpoint. In most instances these are best used for pinpointing and remediating endpoints with security issues, but many products will showcase the integration to enforce corporate policy; such as enforcing a quarantine action if an endpoint starts running Kazaa or an unapproved file sharing application.

VI. About the Author

Jennifer Jabbusch is a network security engineer and consultant with Carolina Advanced Digital, Inc. Jennifer has more than 15 years of experience working in various areas of the technology industry. Most recently, Ms. Jabbusch has focused in specialized areas of infrastructure security, including Network Access Control, 802.1X and Wireless Security technologies.



Jennifer has consulted for a variety of government agencies, educational institutions and Fortune 100 and 500 corporations. In addition to her regular duties, she participates in a variety of courseware and exam writings and reviews, including acting as subject matter expert on Access Control, Business Continuity and Telecommunications, and lead subject matter expert in the Cryptography domains of the official (ISC)2 CISSP courseware (v9).

Ms. Jabbusch speaks about network security at a diverse mixture of national and international conferences, including INTEROP, SecTor, Infosec World, ISSA, Techno Security and government-hosted events by the FBI and US Secret Service.

You can find more security topics on her security blog at <http://SecurityUncorked.com> and at LinkedIn <http://www.linkedin.com/in/jenniferjabbusch>.

About Carolina Advanced Digital, Inc.

Carolina Advanced Digital, Inc. (CAD) is a woman-owned, veteran-owned and privately-held small business specializing in IT infrastructure, security and management solutions. For more than 25 years, CAD has been the leading engineering service and product provider for federal, state and local government agencies as well as healthcare, education and corporate markets. Most of CAD's professional services and products are available via open market, federal GSA and various state contracts.

Contact

Carolina Advanced Digital, Inc.
Cary, NC | 919.460.1313 | 800.435.2212
<http://www.cadinc.com>

VII. Appendix A: Resources

Bradford Networks

Company site at www.bradfordnetworks.com

Cisco

Company site at www.cisco.com

Enterasys

Company site at www.enterasys.com

ForeScout Technologies

Company site at www.forescout.com

Juniper Networks

Company site at www.juniper.net

McAfee

Company site at www.mcafee.com

Security Uncorked

Blog site at www.securityuncorked.com

StillSecure

Company site at www.stillsecure.com

Symantec

Company site at www.symantec.com

TCG (Trusted Computing Group)

Primary site at www.trustedcomputinggroup.org

Trustwave (Mirage)

Primary site at www.trustwave.com

VIII. Appendix B: Feedback

We appreciate your feedback. If you are a consumer of the technology and would like to see specific additional information, please let us know. If you are a NAC vendor and feel your technology and methodologies are not reflected in this document, we'd like to discuss your solution with an appointed systems engineer for inclusion in the next release.

Please send technical inquires and feedback to:

Jennifer Jabbusch, CISO, Infrastructure Security Specialist, jj@cadinc.com

For permission to publish or reproduce this document, please send a request to:

Sarah Burris, Communications Director, sarah@cadinc.com

© 2010 Carolina Advanced Digital, Inc., all rights reserved

This document may not be reproduced in part or whole without explicit written permission from Carolina Advanced Digital, Inc.