

# Understanding Terms and Technologies

You've all heard the old analogies: Do you call a tomato a "tuh-mey-toh" or do you call it a "tuh-mah-toh"? Do you pronounce Illinois "il-uh-noi" or "il-uh-nois." Is a roll with salami, ham, cheese, and so on a submarine sandwich, a hero, or a hoagie? Likewise, is it NAC? Is it NAP? Is there a difference? What about TNC? And what the heck is Network Access Quarantine Control?

There's no lack of acronyms out there to describe technologies that are pretty darn similar. Adding to the confusion is the addition of these technologies to everyday vocabulary as used in a generic sense. Remember Xerox copy machines? It wasn't long before office workers were saying, "Hey, go Xerox me a copy of this report . . ." The brand name Xerox became a verb and part of the everyday vocabulary. It didn't necessarily represent the brand of copier actually being used to perform the document copying function.

NAC is faring a pretty similar fate. Generically speaking, many people and enterprises refer to many different technologies as NAC. Does this mean that they are all actually and officially called "NAC"? Does it matter?

For this book, we are going to break out the various NAC/NAP technologies into the following categories:

- Cisco NAC
- Microsoft NAP
- Mobile NAC
- NAC in other products

Let's start by looking at how a few of the vendors define the different technologies.

## 2 Chapter 1 ■ Understanding Terms and Technologies

---

Cisco defines NAC as follows:

*Cisco® Network Admission Control (NAC) is a solution that uses the network infrastructure to enforce security policies on all devices seeking to access network computing resources . . . NAC helps ensure that all hosts comply with the latest corporate security policies, such as antivirus, security software, and operating system patch, prior to obtaining normal network access.*

Microsoft defines NAP as follows:

*Network Access Protection (NAP) is a platform that provides policy enforcement components to help ensure that computers connecting to or communicating on a network meet administrator-defined requirements for system health.*

The leader in Mobile NAC solutions is a company called Fiberlink Communications Corporation, and they define Mobile NAC as follows:

*An architecture that performs most NAC functions on endpoint computers themselves rather than inside the corporate network . . . with a focus on extending extremely high levels of protection out to mobile and remote computers, as opposed to emphasizing defenses at the perimeter.*

You can tell by looking at the descriptions that NAC and NAP focus on protecting the corporate LAN, while Mobile NAC focuses on protecting endpoints as they are mobile. This is the key fundamental difference between Mobile NAC and the other NAC/NAP types, which brings up an important theme throughout this book: *What exactly are you trying to protect with your NAC solution?*

In addition to the NAC/NAP types, variations on NAC/NAP can be found in a variety of different products and technologies. It's interesting to see how technologies that have been around for quite some time are now being touted and positioned as NAC. This isn't necessarily bad, as many of them certainly do provide NAC-type functions. The point to understand is that these functions existed and were implemented well before the terms NAC or NAP were ever invented.

So, what are some of these "other" technologies that implement NAC? Well, two that have been around for some time are IPSec and Secure Socket Layer (SSL) based virtual private network (VPN) solutions. Here's a quick description of how these two technologies implement NAC:

- **IPSec VPN** — Many devices are able to perform at least a rudimentary assessment of a device attempting to gain Layer 3 access into the corporate network. If the device's security posture is deficient, access to the corporate network via the VPN can be denied or limited.
- **SSL VPN** — This is similar to IPSec VPN's assessment, although sometimes the assessment can be much more granular, because an ActiveX or Java component may be automatically downloaded to assess the

machine. For example, Juniper's SSL box can run quite a detailed assessment. Based upon the security posture of the endpoint seeking to connect to the corporate LAN, access can be denied or limited to certain areas of the LAN, and Layer 3 access can be denied, while browser-based SSL access can be allowed.

The "other" technologies aren't limited to VPN devices. McAfee and Symantec both have NAC-type solutions, as do a number of other vendors. Later chapters in this book will cover a slew of these technologies in much greater detail.

The big point to get out of this section is that regardless of whether or not it is called NAC, NAP, or whatever, the area to focus on is what is the purpose of each technology and what is it trying to protect. Again, many of the solutions are geared toward protecting the corporate LAN, whereas Mobile NAC is geared toward protecting mobile endpoints while they are mobile. This point will be further discussed in great detail later in this chapter. Personally, I don't care if the solution I implement is officially called NAC or NAP; I simply want it to secure the items that I feel need to be secured.

So, now we know what the actual vendors themselves are calling the technologies at a high level. In the upcoming chapters, we are going to cover all of these options in great detail.

## Who Is the Trusted Computing Group?

Inevitably, if you are researching NAC/NAP, you will come across information about the Trusted Computer Group (TCG).

The TCG describes itself as follows:

*The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, and so on) from compromise due to external software attack and physical theft. TCG has adopted the specifications of TCPA [Trusted Computing Platform Alliance] and will both enhance these specifications and extend the specifications across multiple platforms such as servers, PDAs, and digital phones. In addition, TCG will create TCG software interface specifications to enable broad industry adoption.*

So, what does this mean? Well, it means they essentially try to create standards that different companies and technologies would use to allow for interoperability between products.

Why is this important? Think of it from a Wi-Fi perspective. If every Wi-Fi vendor used its own, non-standards-based technology, then there would be big problems. Users utilizing Dell Wi-Fi cards wouldn't be able to connect to Cisco

## 4 Chapter 1 ■ Understanding Terms and Technologies

---

Wireless Access Points (WAPs). Users utilizing Cisco Aircards wouldn't be able to connect to D-Link WAPs. Fortunately, there are Wi-Fi standards (802.11a, 802.11b, 802.11g, and so on) that are not limited to only specific vendors. Thus, consumers and enterprises have a choice, and can mix-and-match vendor technologies based upon their needs and desires. Also, having a standard that everyone else uses simply makes the standard better and more robust.

The specific standard that TCG has created for NAC/NAP is called "Trusted Network Connect" (TNC). Per TCG, TNC is described as follows:

*... An open, nonproprietary standard that enables application and enforcement of security requirements for endpoints connecting to the corporate network. The TNC architecture helps IT organizations enforce corporate configuration requirements and to prevent and detect malware outbreaks, as well as the resulting security breaches and downtime in multi-vendor networks. TNC includes collecting endpoint configuration data, comparing this data against policies set by the network owner, and providing an appropriate level of network access based on the detected level of policy compliance (along with instructions on how to fix compliance failures).*

Clearly, the goal of TNC is to allow the various NAC/NAP solutions to interoperate and play nicely together. This is an admirable goal that has merit and would ultimately be of benefit to enterprises. The problem, of course, is getting everyone to agree to participate. Even if a vendor does participate, it may not necessarily want to adhere to everything the standard dictates, and it may only want to have a small portion of its solution adhere to this standard. This is where the posturing and bickering enters into the equation.

A quick example has to do with Cisco NAC. Cisco NAC doesn't conform to the TNC standards. Certainly, Cisco is a huge company with some of the best talent in the industry, not to mention a very impressive customer base. Plus, if you're Cisco and your goal is to sell hardware, why on Earth would you want to give the option of using non-Cisco hardware? It doesn't necessarily make bad business sense, and, depending upon whom you talk to, Cisco may not even be being unreasonable about it. It has its interests to protect.

It's kind of funny to see TCG's response to the question of, "How does TNC compare to Cisco Network Admission Control?" Clearly, there is a little bit of animosity present. Their response to this question, per the document titled "Trusted Network Connect Frequently Asked Questions May 2007" (available at [https://www.trustedcomputinggroup.org/groups/network/TNC\\_FAQ\\_updated\\_may\\_18\\_2007.pdf](https://www.trustedcomputinggroup.org/groups/network/TNC_FAQ_updated_may_18_2007.pdf)) is:

*The TNC Architecture is differentiated from Cisco Network Admission Control (C-NAC) by the following key attributes and benefits:*

- *Support multivendor interoperability*
- *Leverages existing standards*
- *Empowers enterprises with choice*

*Also, the TNC architecture provides organizations with a clear future path. . . . TCG welcomes participation and membership by any companies in the TNC effort and believes interoperable approaches to network access control are in the best interests of customers and users.*

If you're looking to be empowered with a choice and want a clear future path with your NAC solution, then it appears as though TNG doesn't think Cisco NAC is an option for you. The real point of showing this information is to realize that NAC/NAP haven't yet really been standardized. TNC is right that interoperable approaches to NAC are in the best interest of customers and users; that is quite obvious. When will this actually take place, that all major players will utilize the same standards? No one knows, but I personally am not counting on it any time soon. Let me put it this way. I wouldn't wait on implementing a NAC/NAP solution until it happens. Companies should be smart in ensuring that their existing technologies will be supported and that they understand key areas of integration with any NAC/NAP solution they are considering.

Now, you're probably wondering where does Microsoft stand with TNC? On May 21, 2007, Microsoft and TCG announced interoperability at the Interop event in Las Vegas, Nevada. This was a significant step both for parties and for enterprises. Basically, it means that devices running Microsoft's NAP agent can be used with NAP and TNC infrastructures. In fact, this TNC-compliant NAP agent will be included as part Microsoft's operating system in the following versions:

- Windows Vista
- Windows Server 2008
- Future versions of Windows XP

Later in this chapter, you will learn about the various technical components that make up NAC/NAP solutions. In doing so, this interoperability will be put into perspective.

As of this writing, the list of companies that currently have interoperability with the TNC standard, or have announced their intent to do so, is:

- Microsoft
- Juniper Networks
- Sygate
- Symantec

## **Is There a Cisco NAC Alliance Program?**

---

Just as Trusted Computer Group has its Trusted Network Connect alliance to support NAC/NAP standards, Cisco has its own program to promote interoperability with Cisco NAC.

Per Cisco, its Cisco NAC Program is described as follows:

*The Network Admission Control (NAC) Program shares Cisco technology with third-party participants and allows them to integrate their solutions to the NAC architecture. Program participants design and sell security solutions that incorporate features compatible with the NAC infrastructure, supporting and enhancing an overall admission control solution.*

There is a key difference you will note between Cisco's program and TCG's. TCG's is encouraging vendors to comply with a common standard, while Cisco is soliciting vendors to interoperate with its NAC infrastructure. What does this mean for enterprises? Well, it really depends on what your NAC plans are, what type of infrastructure you have in place, and what type of technologies you use. If you are a Cisco shop, and you use software that is a part Cisco's NAC program, you may not care that Cisco doesn't adhere to the TNC standard. In fact, in that case, it may not really matter for at least a while, or maybe for quite some time. The adage "No one ever got fired for choosing Cisco" still runs true with a lot of companies.

Cisco has broken up its partners into two different groups: those that are NAC-certified and are actively shipping product, and those that are currently developing their products to work with Cisco NAC.

## **NAC-Certified Shipping Product**

As of this writing, the Cisco NAC program partners that are NAC-certified and shipping product are:

- AhnLab
- Belarc
- BigFix
- Computer Associates
- Core
- Emaze Networks
- Endforce
- F-Secure
- GreatBay Software
- GriSoft
- Hauri
- IBM
- InfoExpress

- Intel
- IPass
- Kaspersky
- LANDesk
- Lockdown Networks
- McAfee
- Norman
- Panda Software
- PatchLink
- Phoenix Technologies
- Qualys
- Safend
- SecureAxis
- Secure Elements
- Senforce
- Shavlik
- Sophos
- StillSecure
- Sumitomo Electric Field Systems CO, LTD.
- Symantec
- TrendMicro
- TriGeo Network Security
- Websense

## Developing NAC Solutions

As of this writing, the Cisco NAC program partners that are developing NAC solutions are:

- Applied Identity
- AppSense
- Aranda Software
- Beijing Beixnyuan Tech Co, LTD.
- Cambia
- CounterStorm

## 8 Chapter 1 ■ Understanding Terms and Technologies

---

- Credant Technologies
- Criston
- Dimension Data
- EagleEyeOS
- Ecutel
- eEye Digital Security
- Envoy solutions
- ESET
- Fiberlink
- GuardedNet
- HP
- INCA
- Kace
- Kingsoft
- Lancope
- Mi5 Networks
- nCircle
- netForensics
- Nevis
- NRI-Secure
- NTT
- OPSWAT
- Phion
- Promisec
- Rising Tech
- ScanAlert
- SignaCert
- SkyRecon
- SmartLine
- Softrun,Inc.
- Telus
- tenegril

- Trust Digital
- VMWare ACE
- Webroot

Here are a few very important points to keep in mind regarding these lists. First, the lists have quite a few noteworthy members. This shows that there really is a desire to integrate with Cisco NAC, regardless of the fact that it isn't a member of TNC. Cisco is still a very formidable force.

Also, be a little bit wary of the list. Just because a company is currently shipping a NAC-certified product, that doesn't necessarily mean that the product has the type of integration that you are actually seeking. I won't single out any companies; just do your homework on what the integration actually means to you.

Likewise, you need to be wary of companies that are mentioned as actively developing integration. The terms are quite subjective, and some companies undoubtedly will actually be working head-down to get the integration quickly, while others simply want their name on the list and aren't really doing much to actually get the integration. Again, check the specifics yourself, and don't be afraid to ask the vendor pointed questions.

The key both to the Cisco NAC Program and TNG's TNC program is what does it actually mean to you and your company? You are still responsible for defining your own requirements and using your own best judgment when looking at technologies, so don't be fooled simply because a company is a member of either group's lists. At the same time, knowing who is on the list can help you in your research and planning, and assist you in prompting discussions with vendors to whom you wish to speak.

## Understanding Clientless and Client-Based NAC

While NAC solutions may be different, they do basically fall into two categories:

- **Clientless** — No software is installed on the device to assist with the NAC process.
- **Client-based** — A software component is preinstalled on the device to assist in the NAC process.

There are a number of factors that determine which type of solution makes the most sense for a particular organization. As you'll see, client-based NAC provides the most detail about a device, although installing software on every machine trying to gain access to a network may not always be possible.

## Clientless NAC

A good example I've seen of clientless NAC came from my dealing with a university. They were a fairly good-sized university that was known around the country as being extremely strong academically. It had a network throughout its campus that both students and faculty would access. This network provided access to campus resources, as well as access to the Internet. Because of the mix of users and the fact that campus resources and the Internet were both accessed, the university felt the need to perform a level of analysis on devices trying to gain access to the network.

The major issues the university ran into with trying to put together this type of solution was the sheer number and diversity of devices that needed access and the fact that it couldn't possibly support putting software onto all of them. It wasn't just a question of physically getting the software onto the devices. Once an organization puts software onto a machine, it is responsible for supporting that software and dealing with any problems that may arise from that software being on the device. That would simply not be possible to manage for the tens of thousands of devices that would be accessing the network over the course of year. Not to mention it would be a licensing nightmare to try to manage who had the software, to uninstall the software when a student left, and so on.

For this type of scenario, the answer was simply not to put software onto the devices. Instead of using software, the university would simply use a technology to scan the devices when they came onto the network. If they met the minimum requirements, then devices were allowed access. If they didn't, then they weren't allowed access. This sounds easy, so why doesn't everyone go clientless?

The big reason is that clientless solutions do not offer a very granular level of detail about the devices. If properly configured and secure, a device should give very little detail about its security posture to an external technology that is attempting to get further information. For example (and under normal circumstances), it's not possible to tell if a device that is attempting to gain access to the network has antivirus software installed and running with the antivirus definition files up to date. There isn't a mechanism that computer systems use to communicate this to an unknown technology that is requesting this information. In fact, there is good reason *not* to give out this type of information. Why on Earth would a computer system want to advertise the fact that its antivirus software is outdated?

The same is true for patches, such as Microsoft security updates. If the university wanted to ensure that devices coming onto the network had particular critical Microsoft patches, that isn't necessarily an easy thing to do. It's not as though anyone would want a laptop to actively communicate that it is missing a critical patch that would make it vulnerable to exploitation.

That notwithstanding, there are clientless methods to see if devices are vulnerable to particular exploits. For example, it's possible to scan to see if Microsoft patches MS03-026 and MS03-039 are missing. These particular patches help fix a rather large, gaping, and well-known vulnerability. Some quick information about these particular patches is:

- MS03-026: A buffer overrun in RPC interface may allow code execution.
- MS03-039: A buffer overrun in RPCSS could allow an attacker to run malicious programs.

Clearly, anything that allows code execution and that allows an attacker to run malicious programs is bad. That is why Microsoft developed an easy-to-use tool to help administrators know if these patches were missing. This didn't require any knowledge about the devices to be scanned, and didn't require that any particular software be installed on the devices. The name of this particular tool is `KB824146scan.exe`. To run the tool, someone would simply go to a command line, type in the name of the tool, and put in the IP address range and subnet information for the network to be scanned. The following is example of this being done, with the results also being shown:

```
C:\>kb824146scan 10.1.1.1/24

Microsoft (R) KB824146 Scanner Version 1.00.0257 for 80x86
Copyright (c) Microsoft Corporation 2003. All rights reserved.

<+> Starting scan (timeout = 5000 ms)

Checking 10.1.1.0 - 10.1.1.255
10.1.1.1: unpatched
10.1.1.2: patched with both KB824146 (MS03-039) and KB823980 (MS03-026)
10.1.1.3: Patched with only KB823980 (MS03-026)
10.1.1.4: host unreachable
10.1.1.5: DCOM is disabled on this host
10.1.1.6: address not valid in this context
10.1.1.7: connection failure: error 51 (0x00000033)
10.1.1.8: connection refused
10.1.1.9: this host needs further investigation

<-> Scan completed

Statistics:

Patched with both KB824146 (MS03-039) and KB823980 (MS03-026) .... 1
Patched with only KB823980 (MS03-026) ..... 1
Unpatched ..... 1
TOTAL HOSTS SCANNED ..... 3

DCOM Disabled ..... 1
```

## 12 Chapter 1 ■ Understanding Terms and Technologies

---

```
Needs Investigation ..... 1
Connection refused ..... 1
Host unreachable ..... 248
Other Errors ..... 2
TOTAL HOSTS SKIPPED ..... 253

TOTAL ADDRESSES SCANNED ..... 256
```

This is some rather valuable information. Something to keep in mind is that this can be used for good intentions and for bad. Imagine a hacker at a busy Wi-Fi hotspot running this tool in hopes of finding a victim.

There are also other tools available that can do clientless scanning. Among these are the following:

- Nessus
- Core Impact
- Sara
- GFI LANGuard
- Retina
- SAINT
- ISS Internet Scanner
- X-Scan

**NOTE** It is important to keep in mind that scanning utilities have the potential of causing instability on the systems being scanned.

The following is the bottom line about clientless NAC:

- It doesn't require software on the devices attempting to gain access, so deployment and management of client-side software is not necessary.
- The level of technical detail about the devices gaining access is dramatically less than using client-based NAC (unless the device is configured quite poorly and lacks security software).

### Client-Based NAC

Client-based NAC is what most companies think about with today's NAC solutions. Not only will the software give more detail about the security posture of the device, the software can be used to perform other NAC functions, as well. (See Chapter 2 for more on this.)

NAC solutions that use a client can install the client via a number of different methods. It's not always as straightforward as an administrator installing NAC

software on every device; it depends on the type of NAC solution being used. NAC software can be installed as:

- An executable with the sole purpose of performing NAC functions
- A component of other security software, such as personal firewalls
- A component of the VPN client
- An ActiveX component that is automatically downloaded
- A Java component that is automatically downloaded

Take, for example, the Cisco Security Agent. This agent includes the Cisco Trust Agent functionality that, in the past, may have been installed separately.

The ActiveX and Java components are pretty interesting. These can be seen with SSL VPN devices that are performing NAC-type functionality. Juniper's SSL device (formally NetScreen and Neoteris) has the ability to perform Host Checker functionality. This allows the SSL device to assess at a granular level the device attempting to gain access. Of course, the big thing with SSL VPNs is that they are considered to be clientless. So, how does a clientless VPN solution provide client-based NAC assessment?

The answer is pretty simple. When an end user logs into the SSL device by accessing a web page, the browser downloads an ActiveX, or similar component. This component is the software and allows the detailed, client-based assessment to take place. In essence, the ActiveX component becomes the NAC client software.

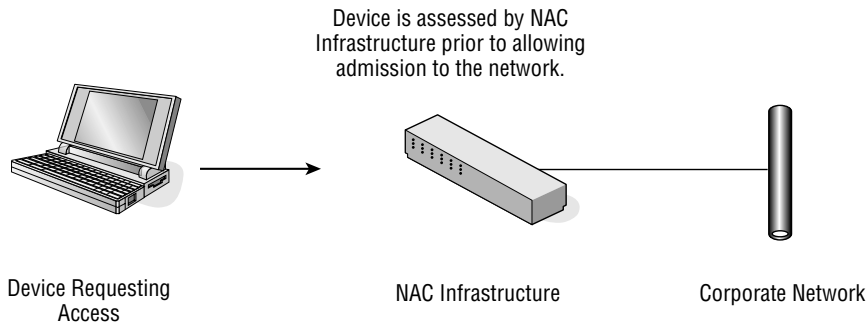
## Pre-Admission NAC

Pre-Admission NAC relates to NAC technology that performs an assessment prior to allowing access to a network. When most companies I speak to think of NAC, this is the technology to which they commonly refer.

The idea of Pre-Admission NAC is fairly simple. Assess a device against a predetermined set of criteria prior to allowing full access to the network. If those criteria are not met, then don't allow the device onto the network, or restrict the device in some manner. Commonly, you will see Pre-Admission NAC in the following solutions:

- Microsoft NAP
- Cisco NAC
- Mobile NAC
- IPSec VPN concentrators
- SSL VPN concentrators

Figure 1-1 shows a graphical representation of Pre-Admission NAC.



**Figure 1-1** Pre-Admission NAC example

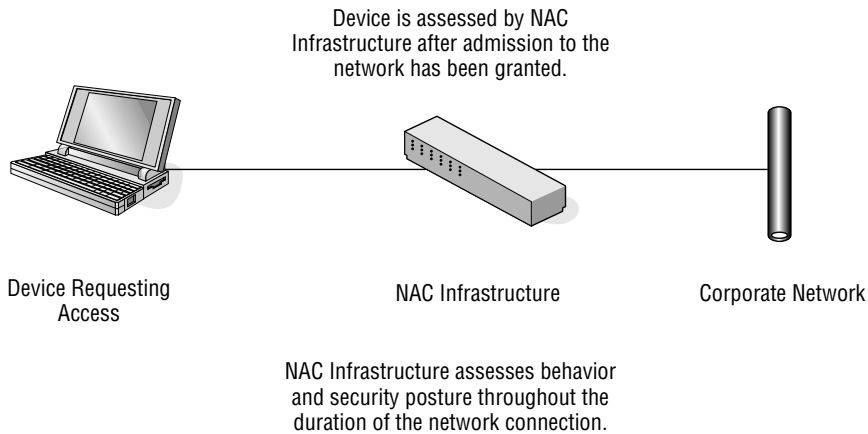
## Post-Admission NAC

Post-Admission NAC differs from Pre-Admission as it relates to the point at which assessment takes place. Post-Admission takes place as it is described, after admission to the network has been granted.

This functionality is important because a device's security posture can change from the time it was first granted access to the network. In addition, the behavior of that device once it is on the network can be cause for restriction.

Figure 1-2 shows a graphical representation of Post-Admission NAC.

## Summary



**Figure 1-2** Post-Admission NAC example

The following are key points from this chapter:

- NAC and NAP essentially perform the same functions, and these terms are commonly used interchangeably.
- The Trusted Computer Group is an organization that is striving to bring standardization to NAC/NAP solutions.
- The Cisco NAC program provides a mechanism for other technologies to integrate with Cisco NAC.
- Clientless NAC relies on scans, not software, to assess devices.
- Client-based NAC utilizes software to provide a more granular assessment of the system attempting admission.
- Client-based NAC software doesn't have to be preinstalled. It can be installed as an ActiveX or other component at the time of network entry.
- Pre-Admission NAC performs NAC functionality prior to allowing a device onto a network.
- Post-Admission NAC performs NAC functionality after a device has been granted access to a network.

This chapter laid a foundation on basic NAC/NAP concepts and key players in the marketplace. Chapter 2 describes in detail the technical components of all NAC/NAP solutions.

