



NETWORK ACCESS CONTROL AND 802.1X

ADVANTAGES, CONSTRAINTS AND CAPABILITIES

A Spire Research Report
Sponsored by ForeScout Technologies

Executive Summary

Network Access Control (NAC) and 802.1x have become popular discussion items as security professionals seek to address the problem of dynamic endpoints – laptops and other devices that enter and exit networks at will. They are difficult to manage and can often introduce malware into an otherwise “clean” network.

A NAC environment offers security posture checking, network port-based authentication, context driven quarantine and remediation, and sometimes persistent monitoring. 802.1x participates within the authentication functionality to allow or deny a device onto a network based on identity.

Sometimes, organizations believe that 802.1x is sufficient and similar enough to a full NAC solution to start down the path of implementation. What organizations often find is that the 802.1x story seems fairly simple and easy, but the deployment is much more difficult. Architectures are often brittle and provide little resilience. Perhaps more importantly, an entire user population – those using unmanaged devices – is completely unaddressed by 802.1x.

This white paper describes a NAC environment in detail and then compares and contrasts NAC to an 802.1x deployment. It provides a case study that is a real-world example of the need for a solution – in this case ForeScout’s CounterACT - that is more forgiving in its deployment and broader in scope than 802.1x.

Ultimately, the significant benefits of NAC outweigh the basic standards and support provided by network and client vendors for 802.1x.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues. Spire provides clarity and practical security advice based on its “Four Disciplines of Security Management,” a security reference model that incorporates and relates the functions of identity management, trust management, threat management, and vulnerability management. Spire’s objective is to help refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by ForeScout Technologies. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and risk management experience.

NETWORK ACCESS CONTROL AND 802.1X ADVANTAGES, CONSTRAINTS AND CAPABILITIES

Table of Contents

AN INTRODUCTION TO NETWORK ACCESS CONTROL (NAC)	1
THE PRIMARY NAC USE CASES	1
Managed Endpoints Reconnecting to a Controlled Network	1
Unmanaged Endpoints Requiring the Use of Network Resources	2
The Need for NAC	2
WHY NAC PROVIDES “BEST PRACTICE” CAPABILITY	2
Security Posture Check	3
Network Port-Based Authentication	3
Context-Driven Network Quarantine (and Remediation)	3
Persistent Monitoring	3
Getting the NAC of 802.1x	4
WHAT IS 802.1X	4
How 802.1x works	4
802.1x Advantages	4
802.1x Constraints	5
COMPARING NAC TO 802.1X	6
FORESCOUT NAC AND 802.1X	8
SPIRE VIEWPOINT	8

An Introduction to Network Access Control (NAC)

Business IT environments are getting more dynamic as the world gets more accessible. The days of the static environment where all users and resources remain within one perimeter are long gone. Nowadays, we must deal with transient computers that are connecting to many networks, picking up malware flotsam and jetsam as they go.

NAC was born as a security response to these increasingly dynamic networks. Its focus is on ensuring that a client PC, typically a laptop but increasingly including other devices, will not introduce malware or other nefarious functions that increase risk to our networked environments. NAC is a form of due diligence performed on the endpoint resource at the point it requests to enter a trusted, or at least managed, network. In providing this capability, NAC may conduct various security posture assessment techniques and/or authentication procedures to validate the sanctity of the endpoint.

The Primary NAC Use Cases

With portable laptops and other devices significantly more popular than traditional desktops these days, endpoints on any network are in a constant state of flux. They enter the network one day, then drop off for a week or two after connecting to the Internet at home, a hotel's wi-fi hotspot, and a customer's network. Then, they are back on the network again.

There are two primary scenarios that enterprises need to deal with from a security perspective - 1) enterprise-managed endpoints "returning home" after significant activity outside of the organization's network boundaries (like the previous example); and 2) unmanaged endpoints - neither controlled nor owned by the organization in question - with some legitimate need to connect to an organization's network environment. The most prominent case here is the guest laptop that needs access to the Internet, but it also includes personal smartphones and tablet devices. NAC is an ideal technology to help the organization mitigate the risks associated with both of these scenarios.

Each of these scenarios is worth exploring more in-depth.

Managed Endpoints Reconnecting to a Controlled Network

It is not uncommon for today's end user laptops to spend more time outside of a controlled network environment than they do inside one, yet common security mechanisms are often situated inside the network. The network-centric approach to protection is cost effective and scalable, but its effectiveness is reduced over time as the networked laptops and other devices leave the enclave for other environments

with unknown risk tolerances and security postures and then return to the network fold. Prodigal Son parables are dandy, but not without a decontamination scrub.

When managed endpoints are disconnected from the enterprise network, they become susceptible to changed configurations, missing patches, and out-of-date antivirus signatures. All of these security deficiencies need to be addressed prior to entering the “clean” network. Although managed endpoints often have security agents installed – anti-malware and personal firewalls, typically – managing these agents can be challenging. With all the “moving parts” complexity available for endpoints today, even managing static PCs on the network can be problematic.

Unmanaged Endpoints Requiring the Use of Network Resources

The case of unmanaged endpoints that require some network access is extremely common in enterprises today. Most typically characterized by consultants and vendors with basic print and Internet needs, these “guests” on the network may be infected and could cause harm to other nodes on the same network. Sometimes, these devices are employee-owned devices like laptops, tablets, and smartphones that highlight the “consumerization” of IT yet also illustrate its security challenges through loss of full management authority.

Unmanaged endpoints have the same (or worse) potential for introducing malicious activity inside a network perimeter as managed endpoints, except the lack of controls is explicit. As basic network resource access becomes a common courtesy extended to any device, the promiscuity of devices accessing many different networks significantly increases the risk to the network.

The Need for NAC

This transitive nature of resources, coupled with the lessening of control over the endpoint, paves the way for “just-in-time” approaches that add more diligence into the connection process. As with fans at sports stadiums, it has become more important to “frisk” the endpoints prior to, simultaneous with, or just after allowing them into a network environment. This is exactly what NAC does well.

Why NAC Provides “Best Practice” Capability

NAC is more like a security ecosystem applying controls at just the right time and governed by a set of triggers and dependencies than it is a “product category.” These controls taken together create a best practice control environment for endpoints as they operate on and off the network.

More specifically, the controls provided by NAC include the following capabilities: 1) security posture check; 2) authentication; 3) network segmentation; and 4) persistent monitoring.

Security Posture Check

A primary capability for a NAC solution is its ability to assess the security posture of the endpoint before, during, or just after its entrance onto the network. That is, it provides something more than traditional authentication, which has been in use for years. Assessing the security posture can encompass a handful of techniques, including:

- Verifying that antivirus and firewall software is up-to-date and configured according to policy.
- Conducting an independent vulnerability scan of the endpoint to determine whether it is infected or in violation of policy.
- Monitoring and assessing network traffic communicating with the endpoint to determine whether it is infected. (Many consider this a separate function from a posture check and will be discussed more later in this paper).

Network Port-Based Authentication

When NAC was introduced in late 2004, it was focused on the security posture assessment, but interest shifted to network port-based authentication via 802.1x quickly as timing, network capabilities, and perhaps a bit of semantic confusion (802.1x also uses the term NAC in its specification) took over the market. And so network authentication became a key component to the NAC ecosystem, in some ways to the detriment of posture assessment. While authentication techniques have been around for some time, tying it directly to a network port was relatively new and is still in development. This control will be discussed in detail in further sections of this paper.

Context-Driven Network Quarantine (and Remediation)

Context-driven quarantine is the other “big win” for NAC. That is, when an endpoint is deemed to be compromised, it may be dynamically assigned to a separate network which typically includes remediation resources. The quarantine network removes the endpoint from other ‘clean’ endpoints. The compromised endpoint is allowed to communicate only with a remediation server, and it is then provided a re-entry opportunity post-remediation.

Persistent Monitoring

Although not always considered part of the NAC ecosystem, some solutions leverage continuous monitoring of network traffic to maintain real-time awareness. Monitoring can provide immediate knowledge of any changes to the endpoint. Rather than “just-in-time” it is more like “all-the-time” but complements the rest of the controls well.

There is nothing particularly new about monitoring network traffic. However, monitoring solutions have traditionally been left at Internet access points and in the core network, and they specialize in detecting attacks. A NAC system that includes

post-connect traffic monitoring can detect not just attacks but also *unexpected* traffic. For example, if a device that appears to be a printer enters the network, but then it starts reading documents from a file server, the NAC system can raise an alarm.

Getting the NAC of 802.1x

As mentioned, while NAC was introduced with a focus on security posture assessment, much attention has been given to the capabilities (and constraints) of 802.1x. In some cases, there is confusion about the functional value that warrants a fuller understanding of the standard.

What is 802.1x

Officially, 802.1x (“Dot one x”) is a port-based network access control standard. It defines the network protocol for authentication communications between a client *supplicant*, the network device *authenticator*, and an *authentication server*. 802.1x defines the use of Extensible Authentication Protocol (EAP) over LAN (EAPOL) so that it can support various authentication schemes using userid/passwords, certificates, challenge/response tokens, etc.

How 802.1x works

The 802.1x process is fairly straightforward. When a device first attaches to a network, the client supplicant software on that device transmits an authentication request to the authenticator, which is usually a network switch. The switch recognizes the request and is preconfigured to forward it to the appropriate authentication server. The authentication server makes its determination and transmits an ‘allow’ or ‘deny’ message back to the switch. Finally the switch makes the port assignment and notifies the supplicant software on the client. At that point, the 802.1x process is complete.

802.1x Advantages

802.1x has three major benefits: 1) it is a standard adopted by IT vendors for basic interoperability in authentication capabilities; 2) it is built into modern IT infrastructure, allowing for potential cost savings; and 3) it works at layer 2 so no network traffic is allowed through prior to authentication.

The 802.1x Standard

802.1x is an IEEE standard adopted for use by many technology providers in a fundamental way. In some respects, this is a simple signal to the IT community that interoperability is desired and the standard provides a roadmap for this type of support. As organizations consider deployment of 802.1x, their feedback and experiences are essential for addressing drawbacks and defining new requirements so that future standards can be developed that can be leveraged in the real world.

Built Into Modern Components

Since traditional operating system, network device, and authentication vendors are building in support for 802.1x, there is an opportunity to save money by utilizing this “free” capability. Supplicants and authenticators in particular are being included in native devices so that a static homogeneous environment has options for integrating the capability across the network environment.

Works at Layer 2

Since the 802.1x conversation between the switch and the endpoint is done without an IP address, there is no potential for the endpoint to attack the network prior to network admission. This advantage may be useful in high-risk environments.

A Basic Review of Benefits

It is difficult to wholeheartedly endorse the benefits of 802.1x simply because they provide almost a strawman approach to NAC that can be deceiving. While the benefits are real at a nominal level, today’s complex networks can provide serious challenges for an 802.1x deployment.

802.1x Constraints

Using 802.1x to solve your NAC problems is like trying to build the Eiffel Tower with an erector set. There is nothing wrong with the erector set, per se, but it wasn’t designed with the Eiffel Tower in mind. The simplistic nature of .1x makes it functional for its single purpose – to provide an authentication framework for network devices – but the standard falls short of the expectations associated with a full NAC solution.

Though it is probably unfair to assert there are “shortcomings” to the standard, enterprises must significantly lower their expectations for a NAC solution if 802.1x is all they want. The limitations are significant, and described below.

Brittle Architecture

The tricky part with 802.1x is that any failure means the whole procedure fails. So any minor problem immediately creates a major challenge with a system that has little resilience and no graceful means for failover. For example, an increasingly common problem concerns laptops with supplicants from another 802.1x environment – for example, a contractor’s home environment. These supplicants are not recognized by alternative environments and therefore the authentication process fails. The contractor can’t get onto the network, even the guest network, without manual intervention.

One Trick Pony

General authentication processes have been around for years. While authentication at the network layer is somewhat new, there is no need to attempt to elevate the notion to something bigger than it really is. The dynamics of NAC that make it worthy of notice involve the real-time, contextual posture assessment, network assignment, and remediation capabilities of a fully implemented solution.

Authentication is a welcome control to the NAC ecosystem, but it is insufficient on its own when considering the key benefits of a NAC solution.

Limited Visibility

As designed, 802.1x makes no attempt to assess the security posture of an endpoint or identify device types or attributes. It assumes every device is “clean enough” and will have supplicant software to initiate the authentication request; there is no attempt at introspection. In addition, the process is a point-of-entry process and so there is no way to identify changes that occur after an endpoint is allowed on the network. For example, 802.1x makes no attempt to determine whether printers have become users, patches have been rolled back, or malware is propagating.

Binary Outcomes

As a standard, 802.1x doesn’t get into prescriptive details or elegant approaches to real-world exceptions. The return result from an authentication request is simple: either allow or deny. There are no considerations for context of the device, tolerances for configuration errors, further actions on failure, or any other outcome. This assumes that all of an organization’s legitimate devices will always have properly configured legitimate supplicants. Unfortunately, there are many real-world scenarios, such as unmanaged devices or configuration exceptions, where organizations would want to allow endpoint devices without this functionality.

Unsupported Devices

There is a presumption that all devices in an 802.1x NAC environment will be managed and support the applicable supplicant software. This requirement has the same limitations as any solution that requires an agent on the endpoint – devices that are unmanaged due to ownership constraints or simply don’t have supplicant support cannot authenticate. At best, these solutions may be able to bypass the authentication process through the use of an exception list, but that defeats the purpose of the control and creates more management overhead.

Comparing NAC to 802.1x

The advantages of NAC become clear in this quick summary table:

Feature	NAC	802.1x
Access Options	Allow, Deny, Limit	Allow, Deny
Non-802.1x Device Handling	Automatic	Manual, by Exception
Supplicants	Not Required	Required
Security Posture Check	Various Options	None
Quarantine and Remediation	Various Options	None
Guest Registration	Yes	No
Persistent Monitoring	Optional	No

Case Study

Meeting Government NAC Requirements

Many US government agencies are in the process of implementing NAC. Different Federal agencies have looked to different authorities for guidance regarding the best NAC architectures. Civilian agencies take guidance from the National Institute of Standards and Technology (NIST) and Department of Defense organizations look to recommendations provided in the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for Access Control in Support of Information Systems.

The DISA STIG lists the 802.1x architecture as the preferred option for authentication and port control, but it lists other options which are better able to accommodate environments with older switches (that do not support 802.1x), environments with devices that do not have .1x supplicants, and environments where you need more complete verification of endpoint security posture prior to network admission.

Over a three year period, one large U.S. defense agency has tested and studied over thirty different NAC solutions. Their experience has proven illuminating.

The agency initially tried rolling out an 802.1x system, but they quickly learned that deploying .1x is neither simple nor trouble-free. The lead consultant on the job cited the unforgiving nature of .1x as a major stumbling point, wishing that the technology had been designed to solve human problems and not force humans to conform to the technology.

On three separate occasions, a large number of users were blocked from the network due to a simple configuration mistake within the .1x system. The consultant points out the challenge of configuring appropriate GPO policies on the supplicant and the need to manage software on all clients to ensure it is up-to-date. The lack of thresholds and the inability to deal gracefully with non-compliant systems has caused this organization to slow down its .1x deployment and look to other NAC architectures that are easier and more capable.

When the agency realized the brittle nature of 802.1x, they turned to ForeScout CounterACT as an alternative. It has proven easier to roll out than .1x, plus it includes a broader set of functions and features than their previous .1x solution. The agency has especially appreciated ForeScout's strong network discovery and reporting capabilities which allow it to identify assets as they enter the network and classify them according to type. The ForeScout solution has been deployed to multiple environments and is answering the age old question of "what is on the networks" from both hardware and software perspective. The unique capabilities of the ForeScout solution then provides the agency with reports on network devices such as anti-virus software, USB devices, Retina scans, applicable users, and other critical artifacts.

Although they are still in pilot phase, ForeScout's NAC solution is currently prepared to support more than 4,000 end points (with 13,000 planned by late-2011). The results to date when comparing the ForeScout solution to 802.1X has yielded cost savings, enhanced security features, enterprise management, auto-remediation, and mission enabler.

ForeScout NAC and 802.1x

To address the limitations of 802.1x, vendors such as ForeScout have developed broader-featured NAC solutions. While these systems can utilize 802.1x, they also have alternative capabilities which may be preferable in situations where the 802.1x constraints (described above) are considered too severe. The benefits of a system such as ForeScout's NAC solution are:

- Fewer components to integrate. ForeScout removes the “erector set” characteristics of 802.1x by providing everything you need for a complete network access control system in one integrated appliance. With respect to authentication, ForeScout's product ties into existing network directory.
- Faster roll-out of NAC. Because there are fewer components to configure and test, the alternative network access control technologies built into ForeScout's NAC product can be implemented more quickly than 802.1x, especially if the environment is large.
- Rich network visibility. ForeScout's NAC product contains a built-in asset inventory, complete with device characteristics, for everything on your network: computers, switches, VoIP phones, printers, smartphones, wireless access points, USB drives, and more.
- No agent software required. ForeScout's product can work without agents, which means it works with all types of endpoints – managed and unmanaged, known and unknown, authorized and rogue. ForeScout handles the “consumerization of IT” problem that 802.1x can't handle.
- Automatic handling of non-802.1x devices. ForeScout's product automatically detects and manages non-802.1x devices such as printers and VoIP phones without the need for static MAC exception lists.
- Non-disruptive deployment. ForeScout's NAC product can be deployed in a phased approach which minimizes disruption. Starting with discovery to identify trouble spots and hidden infrastructure, ForeScout's product then provides a way to gradually move forward with automated control in the most problematic locations.
- Transition path to 802.1x. ForeScout enables a gradual transition to 802.1x, providing time to upgrade switches and install 802.1x supplicants.

Spire ViewPoint

A full-fledged NAC solution should provide security capabilities based on context:

- Where is the endpoint on the network?
- Who is using the device?
- What is the endpoint's security posture?

In order to keep up with today's increasingly mobile business environment, a NAC solution should gracefully handle unmanaged devices such as contractor PCs, smartphones and tablet computers. Finally, NAC should provide "healing" capabilities to address security weaknesses in a way that caters to legitimate endpoints that need assistance after being compromised.

802.1x is really just about authentication, and as such, it provides a subset of the NAC functionality described above. A NAC system that is based on 802.1x may be a good choice for an organization that has already invested in devices (switches and endpoints) that support 802.1x in a static, homogeneous network environment. At some point, it is likely that the environment will become too dynamic (i.e. where the number of exceptions exceed those that define the rule) and may need to upgrade to a more full-featured NAC system.

802.1x can appear attractive because it is "free". But the economics have proven illusory. In practice, 802.1x has been costly and cumbersome to roll-out, particularly for large organizations. The erector-set characteristic of 802.1x is not for the faint-of-heart or for anyone who wants to implement NAC quickly.

When choosing between 802.1x and alternative NAC approaches, enterprises should assess their needs for:

- Types of devices supported – both from a management perspective and a technical one;
- Dynamic nature of the environment – more variability in network endpoints create higher risk and generally demand more security; and
- Flexibility of solution – the ability to remediate, account for configuration errors, and gracefully deal with legitimate people that have endpoint problems.

Many enterprises will realize that a fuller, context-driven, NAC environment provides more capabilities and room to grow than one solely based on 802.1x.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was commissioned by ForeScout Technologies. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.