

White Paper

Missing Link 
Security Services
Mark Bouchard, Founder

Achieving NAC Now and in the Future: The Role of SSL VPNs

About the Author

Mark Bouchard, CISSP, is the founder of Missing Link Security Services, LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for nearly 10 years. He has established a reputation for thought leadership and is a sought after speaker in the areas of security architecture, DMZ design, secure remote access, network security, and related technologies (e.g., firewalls, intrusion prevention systems, and virtual private networking). During his career he has assisted hundreds of organizations world-wide with everything from strategic initiatives to tactical decisions involving the justification, selection, acquisition, implementation and ongoing operations of individual technologies and products.



Introduction

It goes by many names: network admission control, network access protection, network access control, trusted network connection, unified access control, total access protection, and endpoint admission control ... just to name a few. It is one of the hottest items in information security today, and for the purposes of this paper, we will simply call it NAC.

NAC is a multifaceted solution typically requiring the coordination of a wide variety of pre-existing networking gear and additional NAC-specific components. Its purpose is to thoroughly control who and what gets access to networked resources, and it is hot because, in fulfilling this objective, it also addresses one of the greatest security issues plaguing organizations over the past several years. Specifically, NAC assists with the very real problem of keeping malware from entering the enterprise – and not just at Internet and WAN boundaries, but at local points of connection as well (i.e., within the LAN).

Unfortunately, equally real are the challenges that will inevitably arise when attempting to implement as-yet-immature NAC solutions on an enterprise-wide basis. Gaps in coverage, convoluted integration requirements, inadequate inspection capabilities, and weak policy management are just a handful of the more significant issues that will confront organizations which are eager to “NAC-ify” their networks sooner rather than later.

In contrast, by virtue of their in-depth access control capabilities, SSL VPNs – the actual progenitors of the NAC concept and technology – provide an efficient and effective dose of NAC where it is needed most and with far fewer complications. Essentially, they offer organizations the opportunity to ease their way into broader and more complex NAC initiatives. Furthermore, it is expected that today’s SSL VPN technology will remain a valid component of future enterprise-wide NAC implementations – if not also play an instrumental role in NAC’s eventual maturation.

NAC: The Promise

In general, NAC is a security mechanism that involves having access to a network be conditional to the outcome of an audit of the security characteristics and other configuration settings of the involved client device (e.g., desktop, laptop, PDA). The primary benefit of this approach is the ability to stop viruses, worms, and other types of malware from entering enterprise networks by controlling the degree of access granted to potentially compromised machines. For example, a laptop found to be lacking an important patch and not running updated anti-virus software could be denied access to the corporate LAN. Alternately, it could still be granted access, but only to a quarantine zone that provides minimal services, such as access to the Internet or other resources that can be used to remedy its deficiencies.

In addition, NAC can also help with malware containment and compliance-motivated adherence to the principle of least privileges. This is by virtue of the ability to control/minimize allowable destinations once a machine has been cleared for access, and typically involves also accounting for the user’s identity.

From an architectural perspective, it is helpful to understand that realizing the benefits of NAC depends on anywhere from two to potentially dozens of components working together to support three main functions: client audit/inspection, policy derivation, and policy enforcement.

Client Audit/Inspection entails establishing the identity/ownership and state of the user’s computing device, particularly in terms of security related configuration details (e.g., presence of critical patches, anti-virus software, and personal firewall). Common approaches include use of: pre-deployed, persistent NAC agents; dynamically downloaded, ephemeral (or persistent) NAC agents; integration between NAC agents and other client-based software (e.g., anti-virus, personal firewall); and remote scanning techniques, which use no agents at all. The primary differences between the various approaches include:

- scope of coverage (e.g., pre-deployed agents do not support unmanaged nodes);
- depth of visibility, which refers to the type and scope of attributes that can be audited;
- amount of administrative effort required for implementation and maintenance; and
- the periodicity with which audits are conducted (e.g., remote scanning is not conducive to frequent re-checks).

Policy Derivation is the dynamic calculation of access rules based on the results of the client audit. This function is typically handled by a dedicated, policy management server and is also dependent on interpretation

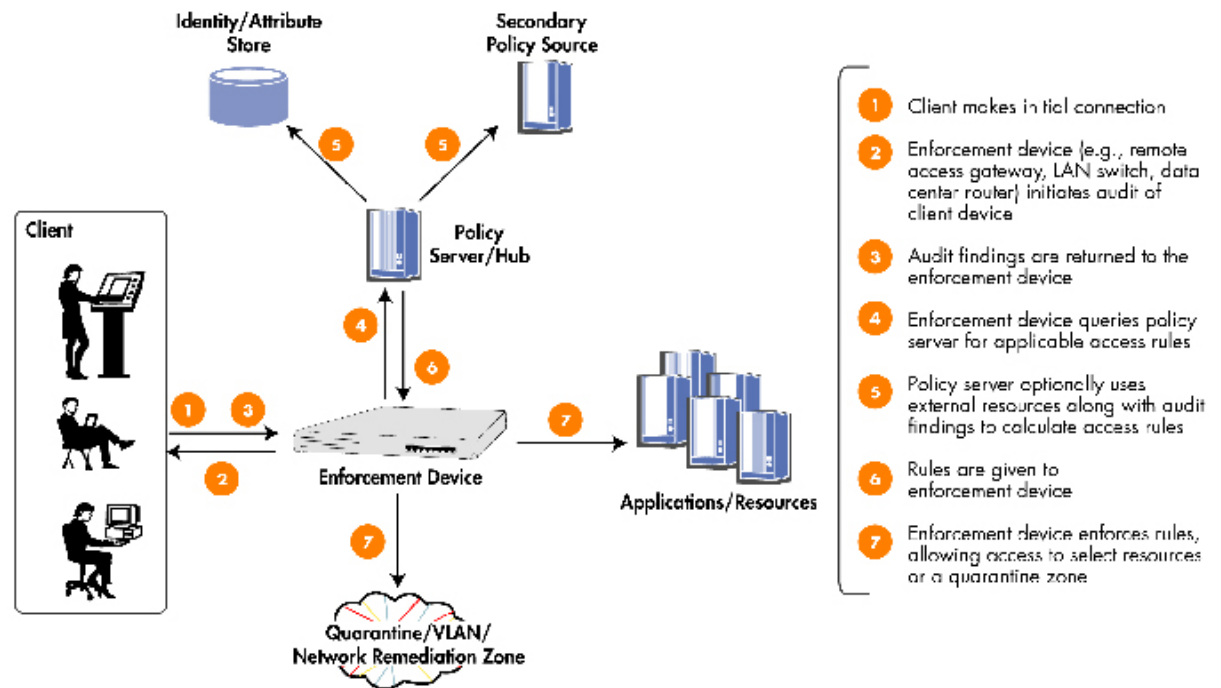


of the inspection findings. This may involve coordination with numerous, additional sources of “policy” information (e.g., configuration, patch, and anti-virus management tools).

Policy Enforcement is typically accomplished by a device that sits directly in the stream of network traffic (e.g., router, switch, security gateway) and involves implementing the access rules that have been derived (e.g., admit unrestricted, quarantine, block all).

Figure 1 provides a graphical representation of the components involved in the NAC process.

Figure 1. NAC in action



NAC: The Reality

It is beyond the scope of this paper to consider all of the approaches and combinations of components used to achieve the three NAC functions. Suffice to say, they are many and varied, with the possible permutations far exceeding the number of vendors involved. However, this condition is only one factor contributing to a host of potentially significant challenges that are poised to limit the effectiveness of NAC solutions, at least until they mature a bit further.

Incomplete Network Coverage is practically inevitable, at least at this point in time. There are simply too many bases to cover, particularly given that every switch port on the LAN and many more points of entry at the perimeter are all possibilities for gaining access to a network. The challenge is compounded by a lack of associated standards and, therefore, interoperability between components from different vendors. However, even single-vendor environments can be an uphill battle, typically requiring costly upgrades to account for older, NAC-incapable, would-be enforcement devices.

Inadequate Client Inspection Capabilities refers primarily to the relative paucity of client attributes that many NAC offerings can check. Such a condition clearly jeopardizes the effectiveness of a NAC solution. In general, supporting a greater number of checks will be beneficial. However, there is also the uncontrollable reality that no number of checks will ever be sufficient to absolutely guarantee that a client device is incapable of spreading a threat. Ultimately, this simply reinforces the point that, like every other countermeasure, NAC has its limitations, and compensating for this condition requires adherence to the principle of defense in depth.

Weak Policy and Configuration Management is closely related to each of the previous items. Specifically, many NAC solutions, even if they are capable of numerous client inspections, are hampered by an inability to efficiently utilize the results. This stems in part from policy management interfaces and constructs that, if



present at all, are cumbersome to use. Primarily, they are not geared to support the creation and maintenance of tens-to-hundreds of access rules, each potentially involving tens of attributes and associated conditional logic. The other part of the issue is that a similar deficiency exists when it comes to configuring the array of devices responsible for enforcing the policies. This step is far from automatic, often requiring the use of several, separate, device-specific, configuration management utilities.

Complex Integration is often necessary to establish and maintain communications between the various agent, policy information, and enforcement components of a NAC solution. The need to implement a mix of proprietary and standards-based protocols is not uncommon. Clearly, this challenge will be even greater for networks comprised of equipment from multiple vendors.

To be clear, NAC is indeed a promising information security countermeasure. It's just that (a) not all of the kinks have been worked out yet, and (b) an enterprise-wide implementation, to paraphrase one of the leading networking vendors, "is an initiative, not a product." In contrast, SSL VPN solutions provide mature, NAC-equivalent capabilities now and in the very location where they are needed most.

SSL VPNs: Fulfilling the NAC Promise Now

SSL VPN gateways are the fast-rising alternative to IPSec-based VPNs, in particular for remote user-to-site connections (as opposed to site-to-site connections). SSL VPN technology is attractive for this use case – which includes mobile employee, telecommuter, and even some extranet scenarios for partners – primarily because it does not require the pre-deployment and ongoing management of any client software on the end-user's computing device. In addition to fostering ease of use and reducing total cost of ownership, this feature also conveys better flexibility and scope of coverage by enabling organizations to easily provide remote access to devices that they do not own, manage, or otherwise directly control.

One consequence of this added flexibility, however, is a reduction in the degree of assurance regarding the security and configuration status of a client device. With managed end nodes, organizations have the benefit of knowing the extent to which client-based countermeasures are being employed (e.g., personal firewalls, anti-virus software, browser and operating system hardening, patch management). This in turn, at least theoretically, reduces the risk of having a compromised host connect to the network and subsequently infect it with some sort of malware.

To address this shortcoming, one of the features added to the majority of SSL VPN solutions early in their evolution was host integrity checking. With this feature, the initial connection to an SSL VPN gateway causes an Active-X or Java-based client inspection agent to automatically download to the remote user's computing device. Host inspection findings are then used as attributes in the dynamic calculation of access rules which are enforced by the gateway. The result is essentially NAC functionality but with a level of access control granularity that far exceeds today's average NAC offering.

That said, indicating that this capability of SSL VPNs is "essentially NAC functionality" is actually a bit backwards. After all, along with similar features that had been engineered for IPSec VPNs, this capability preceded – and in all likelihood inspired – the initial introduction of NAC, late in 2003. It is also an unfair comparison from the perspective that SSL VPN-based NAC does not suffer from the same challenges that plague broader NAC offerings – or at least not to the same extent.

- Network coverage will still be incomplete with SSL VPN-based NAC. However, it does provide this capability at a particularly critical location. While unknown/untrusted hosts may occasionally connect directly to an organization's LAN, they are far more likely to be encountered in a remote access scenario.
- In most cases, the number of client checks that are supported will be greater based on the relative maturity of SSL VPN-based solutions. Furthermore, stronger capabilities in the next area (i.e., policy management) will generally enable better/fuller advantage to be taken of those inspections that are available.
- Primarily by virtue of having dealt with the issue for a longer period of time, SSL VPN-based NAC solutions have significantly better policy and configuration management capabilities. Even so, not all solutions are created equal. The essential characteristics that organizations should look for to ensure they are getting simple yet efficiently scalable administration capabilities include: flexible, automatic, attribute-based grouping; an object-based architecture that supports hierarchical policy arrangements, flexible grouping of



related items, and reuse of individual elements/portions of rules; and a unified policy model that accounts for all attribute categories (e.g., user, client, network, resource being accessed) but in a way that reduces complexity (e.g., by having clusters of related rules represented as a single, higher-level object).

- There are no associated integration issues with SSL VPNs. All three of the core NAC functions – client audit/inspection, policy derivation, and policy enforcement – are natively accomplished by an individual SSL VPN gateway. However, this does not preclude the possibility of having a separate, centralized management application for those enterprises that deploy multiple SSL VPN devices.

The key point here is that SSL VPN solutions that incorporate host integrity checking are quite capable of delivering now on the benefits that many organizations ultimately hope to realize with NAC – at least when it comes to those users/nodes that are accessing their networks remotely. It is also reasonable to expect that this technology will have even greater applicability going forward.

SSL VPNs: Contributing to NAC in the Future

The future, of course, holds no guarantees. Still, it is hard to imagine a scenario where the remote access needs of most enterprises do not continue to grow. Indeed, it also seems likely that some organizations will eventually turn their networks inside-out, eliminating the majority of their LAN infrastructure and embracing an approach where all users are effectively accessing corporate applications “remotely”. In either case, the result should be a continuing if not burgeoning role for SSL VPN-based secure access gateways.

For those organizations that do take the approach of “externalizing” all of their internal users, secure access gateways would be a logical choice to front-end the remaining application zones and data-center infrastructure. In this case, the host integrity checking and access control capabilities included in these gateways should provide all of the NAC functionality these organizations will ever need.

For those organizations that retain a traditional LAN infrastructure – and for the near term in any event – it will be essential for SSL VPN-based NAC implementations to work in conjunction with the broader LAN-focused NAC solutions that eventually achieve dominance. At a minimum, this will entail having sufficient integration to enable the secure access gateway to act as an enforcement point under the direction of a third-party NAC management/coordination application. Further degrees of integration could include supporting standards-based NAC interfaces (once they are established) as well as a range of third-party client audit and remediation agents.

Speculating a bit, it is also quite possible that SSL VPN vendors and their solutions will do far more than just cohabitate with the more broadly applicable, LAN-focused NAC offerings. Indeed, extensive experience with dynamically downloaded client agents (to account for unmanaged nodes) and efficient management of complex access policies gives them some advantages over the majority of current NAC vendors/solutions. In most instances, the better techniques and functionality will simply be mimicked as part of the general maturation process of NAC. However, top-notch policy and configuration management will be harder to replicate, and thus represents an opportunity for a vendor with strong capabilities in this area to develop a stand-alone NAC management application. Notably, such an application would also have the potential to vastly improve the prospects of achieving comprehensive NAC coverage for networks comprised of hardware from multiple vendors.

Conclusions and Recommendations

There is little question that NAC holds significant promise as an information security countermeasure. Helping to keep compromised hosts from infecting enterprise networks and further enabling implementation of the principle of least privileges are tremendous value propositions. However, realizing these benefits will depend on associated solutions evolving a bit further to better address current challenges regarding scope of network coverage, depth of client audits, integration requirements, lack of standards, and robustness of policy management capabilities.

In the meanwhile, it is recommended that organizations take advantage of mature NAC capabilities that are already present in some of the leading SSL VPN secure access gateways. Not only are these solutions an ideal approach for achieving secure remote access, but they can also provide an efficient and effective dose of NAC in those locations where unknown/untrusted nodes are most likely to be encountered.



This white paper is sponsored by SonicWALL | Aventail

(The following section has been prepared by SonicWALL)

SonicWALL® is a recognized global leader in secure networking infrastructure and data protection. The company designs, develops and manufactures solutions that provide comprehensive network and data protection including network security, secure remote access, Web and e-mail security, and backup and recovery. With appliance-based solutions—as well as value-added subscription services—SonicWALL's rich portfolio of solutions delivers the comprehensive enterprise-class Internet and data protection necessary to safeguard organizations of all sizes. In July of 2007 SonicWALL acquired Aventail Corporation, a leading SSL VPN solution provider. For more information, go to www.sonicwall.com.

(The following section has been prepared by Aventail)

SSL VPNs are the progenitors of the NAC concept and technology, and Aventail, acquired by SonicWALL, launched the industry's first SSL-based product for remote access in 1997. Since then, Aventail has been an award-winning innovator in the field, continually focusing its resources on delivering the best-of-breed secure remote access solution.

Aventail delivers on the promise of NAC today with its remote access control platform. Aventail SSL VPNs detect the trustworthiness of a wide range of end-point environment criteria prior to authentication, connect authorized users to a broad range of applications according to unified policy, and protect resources based on the security and identity of both the user and the end-point using a single, easy-to-control gateway.

Aventail® Unified Policy™ provides centralized management and control of all users, groups, resources, and devices, including Windows, Windows Mobile, Macintosh, and Linux platforms. This allows administrators to establish policy with a single rule set across all these objects, in a fraction of the time of competing SSL VPNs.

As a market leader in the SSL VPN industry, Aventail will continue to build on its experience in access control technology to play a central role in the NAC initiative into the future.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com



PROTECTION AT THE SPEED OF BUSINESS™

