Global Information Assurance Certification Paper

Network Access Control Technology – Is the Time Right?

Angela E. Triola
Submitted: March 7, 2005

GIAC Security Essentials Certification (GSEC)
Practical Assignment

Version 1.4C - Option 1

Abstract
Network access control technology is not completely new; however, products that scan nodes or end-points as they join a corporate network, quarantining them or denying them access if they do not comply with established security policies, are coming of age. More vendors are beginning to join this market space, offering various products and suites of products to address this emerging security need. The question this paper addresses is whether or not the technology and timing is right for these network access control products as a necessary next step in a defense-in-depth strategy.

Threats to corporate networks are evolving quickly while administrators work to keep pace. Recent legislation such as the Gramm Leach Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPPA) has increased regulatory focus on security and increased the urgency for protecting our networks. Research indicates that while network access control technology is maturing there is still a gap between software/agent-based control operating at Layer 3 and true port-based, Layer 2 access control which is based on the evolving 802.1x standard. The cost to implement network access control technology is significant both in terms of hardware and man-hours. Given the complexities and challenges associated with managing remote and mobile environments, this report argues that migration to a network access control solution would be most beneficial for companies with a high number of mobile users. Conversely, companies with fewer mobile users, less critical reliance on remote access or internally managed core functions should monitor advances in 802.1x for future implementation. Unless your network is at significant risk from mobile devices, over which you have no other control, network access control technology may not yet be a necessary next step in a defense-in-depth network security strategy.

Introduction

With the rapid pace of change and increasing number of threats facing businesses today, there is little argument that employing a defense-in-depth strategy is wise to protect the corporate network environment. A short list of example threats to corporate security includes:

- Equipment and software vulnerabilities and exploits exist by the thousands and vary widely from their method of deployment to the way they behave.
- Hackers actively scan corporate networks gathering information and looking for chinks in the armor – or better yet, a door left wide open. They take advantage of available and unprotected ports, dropping Trojans and leaving themselves backdoor access for later use.
- Viruses find their way into the network through email opened by unsuspecting and uneducated end-users.
- Trojans piggyback on viruses or are downloaded and cached to a machine while browsing a compromised or malicious website.
- Road warriors travel the globe working from hotel rooms, coffee shops and the networks of their clients. They run the risk of picking up an array of exploits and walking them through the front door of your corporate offices. Effectively, they breach your defenses by walking the evil in and presenting it to the network from behind your firewall

The goal for each corporation is to find a balance between a secure network, protecting internal corporate assets, and making the networked resources available for business needs. Over the years network administrators have battled to defend against these ever-changing threats while maintaining the functionality and usefulness of the network.

II. Threat Evolution

Over the course of time threats to the corporate network have proliferated and evolved. Layering defenses has become necessary as threats have taken advantage of different attack vectors.

Port scans and brute force attacks against your network are generally classified as manual attacks. Someone somewhere is knocking at your door looking for a weak or unprotected point of ingress.

Viruses, worms and Trojans are a constant threat and find their way into your corporate network environment in quiet ways. A brief review of a few major outbreaks illustrates how quickly exploits can change and take advantage of newly discovered attack vectors.

Melissa
Melissa hit the cyber streets in March 1999 and is classified as a Macro Virus. This is a particularly damaging virus as it creates a new macro in Word97 or 2000 and "infects" all Word files at the normal.dot level. Considered an availability attack, Melissa also uses MSOutlook attempting to mail itself to up to 50 addresses, overloading email servers and creating a denial of service situation. It relies on the recipient agreeing to open the new email.[1]

Melissa, while it made a mess of MSWord documents, generated a lot of unnecessary email, spread very quickly, modified documents and infected thousands of machines, wasn't nearly as malicious as more recent viruses and exploits have been. A well-maintained anti-virus application and efforts to educate end-users would have significantly reduced the effectiveness of this virus.

Code Red
Code Red reared its head in July 2001. A worm by definition, Code Red is self-replicating code and in this case targeted Microsoft IIS servers. According to CERT, this worm scans TCP port 80 on random hosts then "the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service."[2] Infected machines then become attackers and begin scanning. In addition to website defacement, Code Red caused severe denial of service attacks because of its excessive scanning activity. The potential impact of the Code Red worm was heightened by the method with which it exploited the Indexing Service in the local system security context potentially allowing remote code execution.[3]

Mitigation of Code Red damage could have been partly achieved by keeping IIS server patches current, segmentation of the network to limit the spread of the worm and the implementation of Intrusion Detection systems for earlier identification of the anomalous scanning traffic.

Nimda
Nimda took the idea behind Code Red and went a step farther. Nimda is classified as a complex virus and includes a mass-mailing worm component. Nimda proliferates via email attachments, specifically those named "README.EXE." This virus was able to easily evade firewalls and use the end-user workstations to scan for vulnerable websites – a feat Code Red was unable to accomplish.

---

[1] Unknown. Melissa Virus. Proland Software, 2005 http://www.pspl.com/virus_info/w97m/melissa.htm
[2] Unknown. CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. CERT Coordination Center: Carnegie Mellon University. 2001 http://www.cert.org/advisories/CA-2001-19.html
[3] Unknown. CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL.

According to F-Secure Nimda took the following steps throughout its lifecycle:

> "1) File infection
> Nimda locates EXE files from the local machine and infects them by putting the file inside its body as a resource, thus 'assimilating' that file. These files then spread the infection when people exchange programs such as games.
>
> 2) Mass mailer
> Nimda locates e-mail addresses via MAPI from your e-mail client as well as searching local HTML files for additional addresses. Then it sends one e-mail to each address. These mails contain an attachment called README.EXE, which might be executed automatically on some systems.
>
> 3) Web worm
> Nimda starts to scan the internet, trying to locate www servers. Once a web server is found, the worm tries to infect it by using several known security holes. If this succeeds, the worm will modify random web pages on the site. End result of this modification is that web surfers browsing the site will get automatically infected by the worm.
>
> 4) LAN propagation
> The worm will search for file shares in the local network, either from file servers or from end user machines. Once found, it will drop a hidden file called RICHED20.DLL to any directory which has DOC and EML files. When other users try to open DOC or EML files from these directories, Word, WordPad or Outlook will execute RICHED20.DLL causing an infection of the PC. The worm will also infect remote files if it was started on a server. "[4]

Clearly, Nimda's methods of attack and means of deployment were far superior to those of Melissa and more advanced than Code Red. Protecting against Nimda required multiple defensive layers including up-to-date antivirus signatures, up-to-date patches, end-user education, network segmentation and placing web servers in protected DMZs, to name a few. Exploits were becoming more complicated.

Korgo

Korgo.A was first discovered in May 2004. There are multiple variants of this worm and successful execution can result in remote code execution. Korgo takes advantage of the LSASS vulnerability, (which Microsoft addressed with Security Bulletin MS04-011,)[5] by creating specific registry keys, killing certain

[4] Tocheva, K., Erdelyi, G., Podrezov, A., Rautiainen, S. and Hypponen, M. F-Secure Virus Descriptions : Nimda. F-Secure Corp.; September 18-19th, 2001 http://www.f-secure.com/v-descs/nimda.shtml

[5] Unknown. Microsoft Security Bulletin MS04-011: Security Update for Microsoft Windows

processes, and opening various TCP ports for listening to and contacting remote computers. Compromised computers could be completely controlled remotely.[6]

Patch level compliance was a primary means of mitigation for this exploit. Blocking unused ports at the firewall could have prevented unwanted traffic and an intrusion detection system could have assisted in the identification of anomalous communication behaviors.

Berbew

Berbew or BackdoorBerbew is particularly malicious to financial institutions. Information theft is the driver for this exploit. Classified as a Trojan, Berbew exploits a known issue with the ADODB/JavaScript redirection in Internet Explorer. A user simply visits a compromised website and the Trojan is downloaded and executed in the background on the workstation. If a user logs into Ebay or PayPal, or Earthlink, Juno and Yahoo webmail accounts Berbew collects the user and password information and periodically sends that information back to the collector.[7]

Up to date anti-virus files on the workstation to detect and eliminate the Trojan, firewall modifications to block known-malicious sites, and intrusion detection systems to discover the "phone home" traffic back to collectors are defensive measures that could have helped mitigate the effects of this exploit.

Based on these examples it is clear that over the recent years exploits have evolved to take advantage of various vulnerabilities and multiple attack vectors.

Legislation and Penalties

The cost associated with malicious exploitation adds up quickly. Man hours are chewed up mitigating and recovering from the damage and the cost of compromised or lost critical data has the potential to be greater than a company's overall worth.

Recent legislation presents new challenges to US and International companies. Security and customer data privacy is no longer a concern just for information technology professionals; it has become a critical component of business. External auditors and regulators evaluate security programs with increased scope, expertise and depth of testing and now, with legislative backing, are well

---

(835732). Microsoft Corporation. 2005
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

[6] Podrezov, Alexey. F-Secure Virus Descriptions : Korgo. F-Secure Corp. 2004
http://www.f-secure.com/v-descs/korgo.shtml

[7] LURHQ Threat Intelligence Group. Berbew/Webber/Padodor Trojan Analysis. Lurhq Corporation. 2004
http://www.lurhq.com/berbew.html

equipped for enforcement through financial penalties. Today, network administrators have even more reason to defend the corporate network with greater diligence.

GLBA (Gramm-Leach-Bliley Act) and HIPPA (Health Insurance Portability and Accountability Act) legislation has drastically impacted how many companies secure their critical data. Under GLBA, "the Federal Trade Commission can seek injunctive relief …and demand that an institution make restitution to any customer whose information is improperly used." Corrective action and the imposition of stiff civil monetary penalties for violations are not outside the scope of this legislation.[8]

HIPPA penalties are no less severe. According to HIPPAAntidote, a service made available by Strategic Healthcare Initiatives, Inc.(SHI):

> "The civil penalties for violation of these standards include civil money penalties of $100 per incident, up to $25,000 per person, per year, per standard. There are also federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information under false pretenses. Penalties are higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing PHI; up to $100,000 and up to five years in prison for obtaining health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm."[9]

Common Defense-in-Depth Layers

Over the years network administrators have attempted to keep pace with emerging exploits and meet regulatory security requirements by layering defensive mechanisms. Examples of these defenses include: border routers, firewalls, intrusion detection systems, network segmentation and anti-virus software. Each has strengths and weaknesses and each contribute to a robust security posture. The key is coordination or layering of these mechanisms to take full advantage of their unique security capabilities.

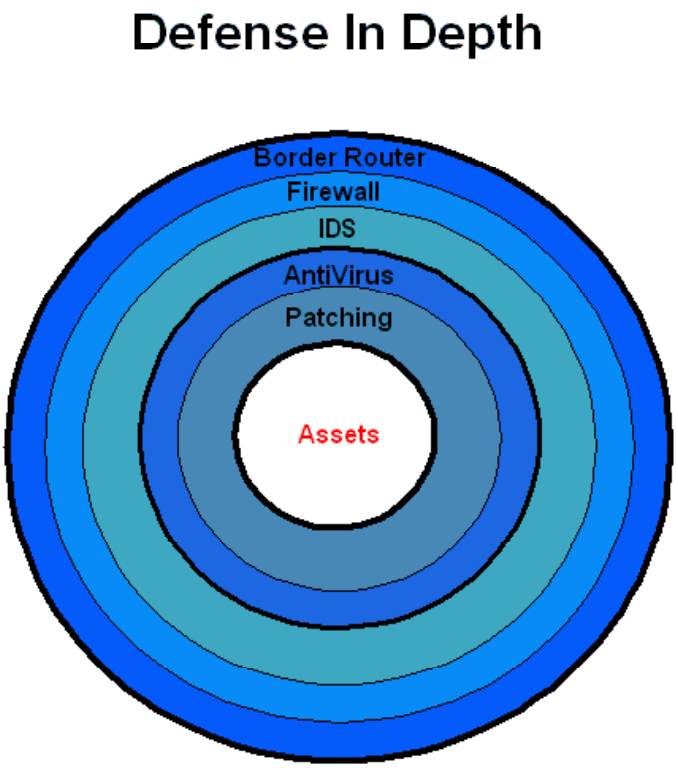
This layering of defensive measures is commonly referred to as "defense-in-depth" and is usually represented as a bull's eye-style graphic as illustrated

---

[8] Unknown. Barbedwire GLBA Solution**.** Barbedwire Technologies, Copyright © 2001-2004 http://www.barbedwiretech.com/solutions/glb.htm

[9] Unknown. Frequently Asked Questions About HIPPA. Strategic Healthcare Initiatives, Inc. ©2001, 2002 http://www.hipaantidote.com/ha/faq.asp

below.



Border routers are situated at the outer-most point of the network perimeter and filter all traffic between the outside world and the internal network. When correctly configured, a border router can filter all incoming and outgoing traffic using predetermined parameters such as those found in Access Control Lists (ACLs.) Border routers can also provide Network Address Translation (NAT.) NATting is the process of assigning an external IP address to a corresponding internal IP address, which is an effective defensive mechanism for masking or hiding internal addresses from the outside world and hackers who would like detailed internal network information. Because border routers interface with the outside world their configuration or mis-configuration can be a critical flaw in designing a secure network. Border routers should be a critical first layer of defense.[10]

An equally critical defensive layer is the firewall. Although it is possible to achieve sophisticated filtering and traffic management with a properly

[10] Northcutt, Stephen. Et. All. Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers and Intrusion Detection Systems. New Riders, San Francisco. 2003. p4, 138.

configured, high-end border router a greater level of security can be achieved by incorporating a firewall into the network topology. Firewalls come in various flavors: static packet filters, stateful firewalls, and proxy firewalls all of which can be deployed in multiple locations within a network, depending on the network topology. Many border routers do not handle the inspection and analysis of excessive amounts of traffic very well. Firewalls, however, are better equipped to inspect and analyze the traffic that is allowed past the border router. This thorough traffic analysis and filtering make the firewall a natural next defensive layer. Like router ACLs, firewalls use rules to either allow or deny traffic between network segments. For example, the firewall will regulate data transfer between a DMZ and private network or between a private network and the border router.[11]

Network segmentation is another useful defensive mechanism. By separating natural portions of the internal network, such as functional groups or common business users and by using VLANs or separate switches, companies are better able to trap or corral exploits in a defined space before they have an opportunity to spread throughout the network. Worms, like Korgo for example, often attempt to propagate by traveling to other machines in a common network segment. Compromised segments can be unplugged from the network, trapping the maliciousness in a confined space.

Best practice network design will position semi-public servers, such as email and DNS servers, in a DMZ, which is a virtual zone behind the firewall that allows secure communication and data exchange between internal and external facing servers. Although penetration of the DMZ servers may occur if the DMZ firewall rules are not properly configured and managed, this layered network design structure will slow and prevent infiltration of critical internal servers and data.

Intrusion Detection Systems (IDS), either network-based (NIDS) or host-based (HIDS), are early warning systems. They actively monitor network traffic for suspicious activity, watching for predefined signatures. They differ from border router and firewall defensive measures in that they do not actively allow or block types of traffic. NIDS and HIDS identify anomalies in traffic patterns based on predetermined conditions. This reactive defense can provide important forensic information for the network engineer responsible for investigating or remediating an attack.

Antivirus software is a critical defensive measure. Locally installed on each server and workstation, antivirus software attempts to identify new viruses by using frequently updated data or signature files. Key to antivirus effectiveness is a management program that includes sound software configuration, ongoing maintenance and user education. All must comply with a company's antivirus and end-user policies pertaining to the frequency of anti-virus scanning as well

[11] Northcutt, Inside Network Perimeter Security, p5.

as email and Internet usage.

Patch Management and service pack standardization, while not historically considered a “defense-in-depth” layer, is an easily achieved and extraordinarily useful means of providing more protection for your corporate network. Software development is not an exact science. It is all too common, in the mad rush to get a new product or release to market, to leave bugs and holes in software. Hackers and script kiddies spend countless hours looking for these holes and the opportunity to be the one to disclose the vulnerability to the public. Software vendors must often race to keep up. Some point a finger at Microsoft as the worst offender. Perhaps they are right. Or perhaps Microsoft just has the lion’s share of the market for basic consumer software and thus presents an easy target. Regardless of the operating systems and software running in your environment there will always be patches rolled out to address known vulnerabilities. Keeping your patch levels current will help guard against exploits that do make it through your defenses. Remember the Road Warrior walking exploits through the front door?

Finally, effective end-user education can be a highly effective defensive measure. Users who are well-educated to the threats of exploits arriving in their email boxes, on questionable websites, and via the use of other unsecured networks, can significantly reduce the number of opportunities for evil to find its way into the corporate network.

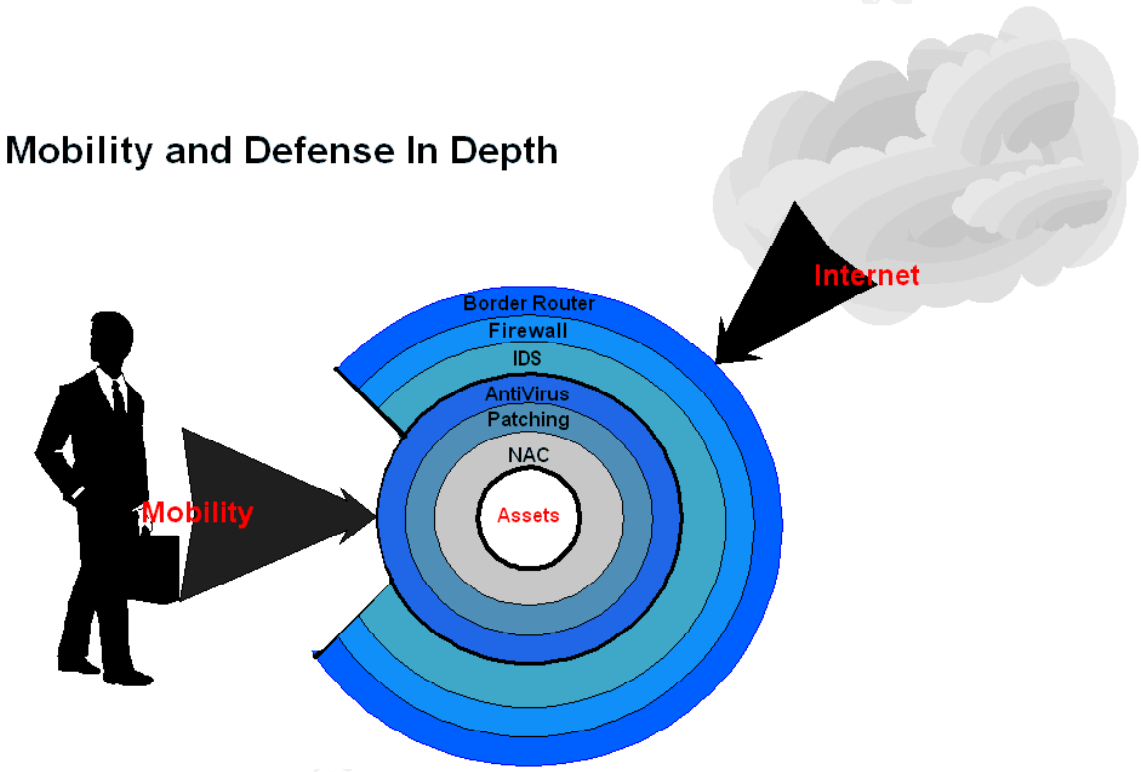
Alone, each of these security measures and strategies is insufficient to adequately protect a corporate network environment. Exploits are just too varied and complex for a single defensive mechanism. Security risk can be greatly mitigated and regulatory requirements met with the standard defenses discussed above, combined, of course, with sound policies and standards by which to deploy and manage them. With these defensive layers in place the newest problem facing network administrators today is managing the risk introduced by mobility.

Network Access Control Technologies

As it relates to network access control, mobility creates risk. Mobility has an obvious upside – users can work from home, their local coffee shop, airports, or anywhere they can obtain a connection. Given a mobile workforce, corporate network administrators must concern themselves with the liabilities mobility presents, must address these new risks and implement solutions not otherwise required for a permanently positioned staff. Sometimes that convenient or necessary remote connection may be through a wireless access point on someone else’s network and there is no telling what exploits the PC is being exposed to there! Other times that access may be at home where the user plugs their laptop directly into their cable modem or DSL, without the protection

of a personal firewall, leaving themselves wide open to common malicious activity. That same laptop walks through the door of your corporate environment on Monday morning, circumvents standard defensive measures, snaps into its desktop docking station and your entire network is suddenly exposed to everything that laptop may be harboring.

Using the defense-in-depth model as a starting point, it is easy to see how mobile users easily circumvent more traditional defensive measures that work well for stationary, non-mobile devices.



Should network administrators deny end users the option of mobility? Should we take away laptops? Restrict PDA's? Ban Bluetooth-enabled devices? Is it possible to control and secure the end user's home environment to ensure that they do not bring unwanted exploits with them into the corporate environment?

Network administrators cannot control these variables, nor should we be required to do so. Accountability for corporate network security must be shared among executives who set risk thresholds, administrators who recommend and manage technology solutions and end-users who must understand both the risks as well as the approved corporate behaviors associated with their transient or mobile status. In the end, as network administrators and guardians of corporate data assets, we must focus on the corporate environment and find a balance between mobile productivity and security policy compliance.

Network access control technology is evolving to address the security and compliance challenges presented by laptops and mobile devices – and the pace of development and availability is starting to pick up.[12]

November 2003 saw the announcement of Cisco's Network Access Control (NAC) program. NAC, relies on close partnership with leaders in the anti-virus space: Network Associates, TrendMicro and Symantec and allows certain Cisco equipment to enforce endpoint access by evaluating the status of anti-virus software and OS patches. As the NAC program continues to evolve Cisco will be extending the technology to other Cisco equipment such as Catalyst switches and VPN concentrators.[13]

Microsoft entered the fray in July 2004 with Network Access Protection (NAP.) Although the software giant is holding off development of this technology for the moment, there is no doubt that they are very interested in maintaining a presence in this space.

Enterasys and Alcatel both have significant presence in the network access control market space. As of the fall semester of 2004, The University of North Carolina has implemented network access control by employing Alcatel OmniStack, Cisco Catalyst and Enterasys Matrix switches in their infrastructure which supports 50,000 end users, has 75,000 Ethernet LAN ports and 400 wireless LAN access points. According to Mike Hawkins, associate director of networking at UNC, the UNC network is "particularly nasty… in the sense that we have users coming online with a lot of bad stuff. Not one solution will hit all the things we need to hit."[14] IDS, antivirus and security appliances on their network just are not enough protection. Enterasys' TES (Trusted End-System Solution) technology assesses every corporate PC or laptop attaching to the network. Even before clients obtain Layer 2 network access or receives an IP from a DHCP server, an assessment server audits the device for compliance with security policy.

Network access control basically takes the form of server/agent architecture. End-points are called supplicants and the servers or resources they are attempting to access are called Authenticators. Supplicants request access to the services offered by the authenticator, an authentication server checks the credentials of the supplicant and determines whether the supplicant is authorized to access the Authenticator's services.[15] If authorized, the supplicant

[12] Messmer, Ellen. NetworkWorldFusion, The Enforcers. 5/17/2004 http://www.nwfusion.com/weblogs/security/005122.html
[13] Roberts, Paul. NetworkWorldFusion. "Cisco buys network security company Perfigo." 10/21/2004.
[14] Hochmuth, Phil. NetworkWorldFusion, Enterasys delivers switch-based security. 6/28/2004 http://www.nwfusion.com/news/2004/0628enterasys.html.
[15] Unknown. IEEE Std 802.1x-2001, IEEE Standard for Local and metropolitan area networks – Port Based Network Access Control. Institute of Electrical and Electronics Engineers, Inc.

is allowed connectivity to the network. If not authorized, the supplicant is shunted off into quarantine VLAN or simply denied access to the network altogether as the switch port they are connected to is disabled.

Software and switch companies are approaching network access control from two fronts: software-based and 802.1x-based solutions. Software-based solutions rely on software installed on the supplicants and authentication servers to assess compliance and allow or deny further access to network resources. Operating at Layer 3, software-based solutions require multiple layers of authentication servers and block access to the network by methods such as enforcement utilities on the end-points or by dynamic ACLs. Software-based solutions do not control switch hardware or interface directly with the switch port to which the supplicant or end-point is connected.

802.1x continues to gain further acceptance as greater numbers of hardware manufacturers are incorporating 802.1x support into their products. The 802.1x solution provides network access control at the switch-port level and the ability to assess compliance prior to the distribution of an IP address. Working in conjunction with an authentication server, 802.1x-enabled switches are capable of redirecting non-compliant supplicants into a quarantine VLAN and disabling switch ports to which non-compliant supplicants are connected.

At present, Sygate seems to be at the lead in the network access control technology market. Not only did the Sygate Secure Enterprise technology take Gold in the Security Management Systems category of InfoSecurity Magazine's 2004 Products of the Year, but it appears that Sygate technology is driving and enabling other end-point security offerings.

The Sygate Secure Enterprise solution provides software-based network access control. It relies on a security agent that runs on each endpoint, one or more distributed policy management servers and one or more enforcement mechanisms – which include enforcement servers on the LAN, on remote network access points and even via enforcement utilities built into the endpoints.[16] One serious advantage of Sygate's Secure Enterprise technology is the ability to evaluate a variety of "security-critical parameters" on the client including: patch levels, OS and application configurations, anti-virus and personal firewall status.[17] The only clear drawback to Sygate's solution is the fact that it is completely software-based and requires the presence of multiple policy management and enforcement servers which can mean significant hardware and man-hour costs to implement and maintain. Sygate Secure Enterprise, as it exists today, would be a good network access control solution for implementation on smaller corporate networks with many mobile end users

NY:NY, 2001. P7.

[16] Sygate, Sygate Changes the Game. Sygate Technologies: Fremont, CA. P3.

[17] InfoSecurity Magazine. December 2004, Products of the Year. http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss526_art1054,00.html#sms

and may even be more cost effective, in the short term, than replacing existing switches with those that support 802.1x .

When bundled with 802.1x enabled switches Sygate technology is even more powerful.

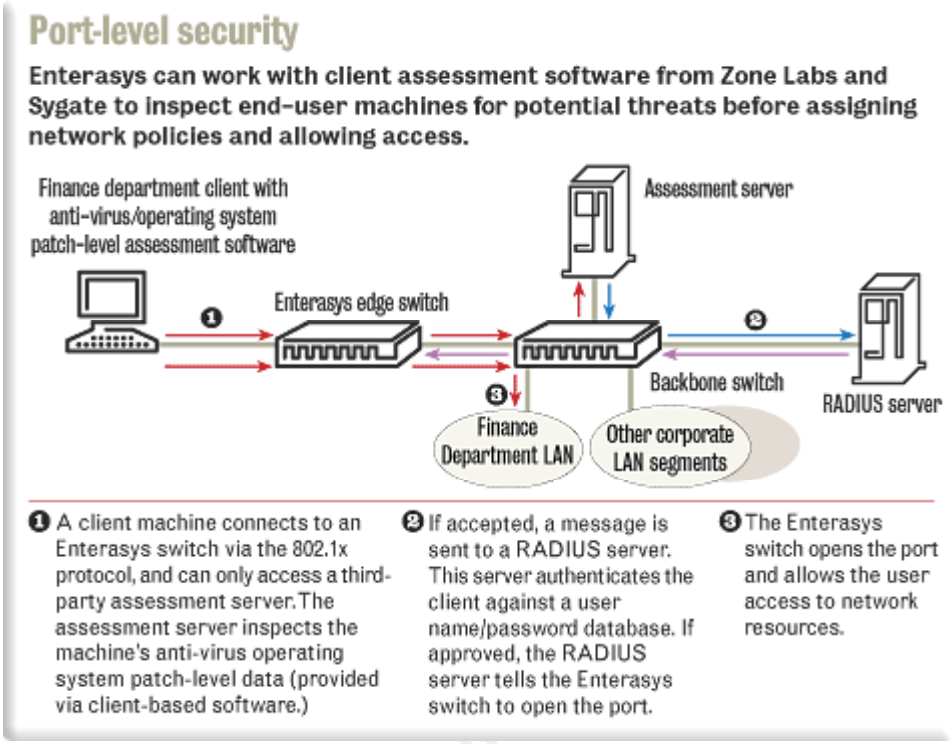
Alcatel's OmniStack 6600 switches and its modular 7700 and 8800 series products combine 802.1x authentication technology, Sygate's Host Integrity Server, and client-side anti-virus software from Network Associates, Symantec or TrendMicro to block virus-infected PCs from accessing the network. At logon, supplicant information is sent to a Sygate server. If the supplicant does not have up to date antivirus software the Alcatel switch re-routes the PC into a quarantine VLAN.[18] 802.1x support is a clear advantage to Alcatel's solution as it manages network access at the switch port level. It incorporates 802.1x authentication to the corporate network at this early stage of development and lays the groundwork for future enhancements using the 802.1x technology. The main disadvantage is the current limitation to anti-virus compliance. Corporate networks with Alcatel switches already in place would benefit from the additional inspection and anti-virus compliance control offered by this solution and could look forward to future enhancements.

True 802.1x port-level access control is achieved by Enterasys Network's Trusted End-System Solution (TES) which combines their Matrix C-, E- and N-series switches, ZoneLabs Integrity products and Sygate's Secure Enterprise. In this configuration each switched Ethernet port can act as a security gateway into the network. At logon, a Sygate or ZoneLabs assessment server audits the end-point against an assessment server before that end-point obtains Layer 2 network access or an IP address from a DHCP server. If the end-point meets inspection a message is sent to a RADIUS server which authenticates against a user name/password database. If approved the RADIUS server instructs the Enterasys switch to open the port. Enterasys also has the ability to tie this technology into their Policy Manager product for finer granularity of network access authentication and privilege. Unlike Alcatel's solution, which shunts non-compliant end-points into quarantine VLAN, TES can assign pre-defined network identities to clients. This, according to John Roese, CTO at Enterasys, "… is easier to deploy and manage because it does not require setting up special VLANs on the network." He also adds that "assigning user-based policies allows for a tighter level of control than the admit/deny/quarantine approach…." The "Port-Level security" graphic below, taken from Phil Hochmuth's Network World "Enterasys delivers switch-based security" article, clearly shows how an end-point authenticates and gains access to the network through Enterasys' port-based access configuration.[19]

---

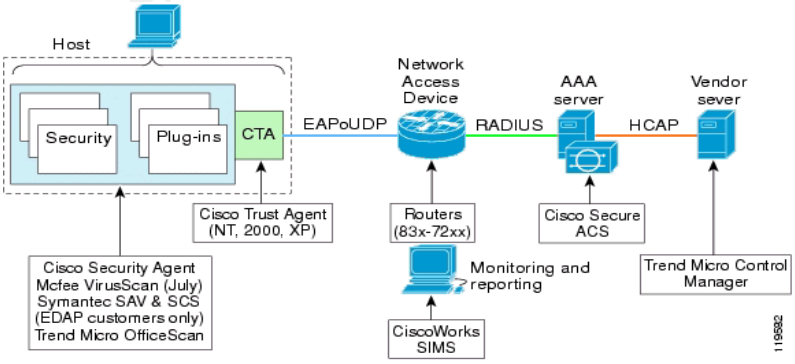
[18] Hochmuth, Phil. NetworkWorldFusion. "Alcatel Switches gain security support." http://www.nwfusion.com/news/2004/081604alcatel.html

[19] Hochmuth, Phil. NetworkWorldFusion "Enterasys delivers switch-based security." 06-28-2004. http://www.nwfusion.com/news/2004/0628enterasys.html



Enterasys' TES is a robust solution with great future-growth potential in the 802.1x space. The large scope of this solution may be a deterrent for smaller and less mobility-impacted networks. Large networks, however, with large numbers of mobile supplicants, such as the University of North Carolina discussed above, would find significant value in this network access control solution both in the short and long term.

Cisco has also been working on a network access control solution that they've dubbed Network Admission Control. NAC – considered a first step in the Cisco Self-Defending Network initiative – is currently a software-based solution that requires multiple layers of implementation as you can see in their published graphic below.



Each supplicant or end-point requires the installation of the Cisco Trust Agent and the Cisco Security Agent. The Security Agent assesses Operating System, patches and hot fixes and sends this information to the Trust Agent. The Cisco Trust Agent is also being bundled into software with Cisco anti-virus co-sponsors to provide the ability to report on anti-virus protections. NAC relies on Network Access Devices (NADs)– such as routers, switches, wireless access points which demand host security "credentials," from the Trust Agent, which it then relays to policy servers where the decision is made to permit, deny, quarantine or restrict access. At its foundation, NAC relies on a policy server – a Cisco Secure Access Control Server (ACS) to provide authentication, authorization and accounting. This RADIUS server evaluates information relayed from the network access devices and determines the appropriate applicable policy. Co-sponsor servers, such as antivirus, provide additional validation.[20]

Cisco is touting this technology as a "multiphased security initiative" and at present, only certain Cisco IOS Layer 3 equipment is compatible in the NAC offering. A small population of Cisco equipment is compatible with NAC and requires IOS version (12.3(8)T) or later. Additionally, the current phase focuses only on anti-virus compliance by ensuring that all end-points are properly up to date with their anti-virus signatures. Cisco enforces connectivity via dynamic ACLs and URL redirection, rather than true Layer 2 port-level access control where by the switch port would be enabled/disabled.[21] Cisco advertises the future growth of this technology and the incorporation of 802.1x support on their hardware. Until enhancements and upgrades are available the capabilities of Cisco's NAC are limited. Companies with Cisco equipment already installed would benefit from the additional access control offered by NAC and could look forward to slowly incorporating additional enhancements as they become available.

Solutions are readily available from a select few companies and they may or may not be the right solution for your corporate network needs at this time. The ultimate goal is Layer 2, port-based network access control via 802.1x technology, but as research shows, very few companies are offering this functionality yet. With a few exceptions, network access control is being handled at Layer 3 using software and dynamic ACLs to permit/deny access. It is expected that 802.1x will continue to mature until true Layer 2 port-level control is achieved.

Is it Worth the Cost?

---

[20] Cisco Systems. Release Notes for Network Admission Control, Release 1.0. Cisco Systems, Inc. 2004. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_release_note09186a0080270825.html

[21] Cisco Systems. Implementing Network Admission Control Phase One Configuration and Deployment. OL-7079-01, Version 1.1.Cisco Systems, 2005. Section 1-2 through 1-3.

Network administrators must determine whether the need for network access control technology, as an addition to the defensive strategies currently deployed in their environment, is worth the cost of implementation at this time. Each of the solutions discussed herein require multiple layers of implementation, usually including one or more software agents on the end-points and specific network devices (routers, switches, etc) from various companies running specific versions. In addition, each offering also requires authentication servers of various types. The point is that this is not an easy/fast fix/cheap technology. At a minimum, analysis should consider following:

a) cost of new equipment or upgrades,
b) cost of licensing all necessary software,
c) amount of network traffic/bandwidth consumed by daily authentication,
d) cost in man-hours for implementation
e) long-term scalability and finally,
f) ongoing maintenance and administrative costs.

Conclusion

Is network access control technology a necessary next step in a defense-in-depth strategy? Is the time right? The answer to both questions is yes and no.

IT professionals are required to manage and protect corporate network environments and critical data with fewer resources while the complexity of exploits continues to evolve. IT professionals are now discovering that they must protect corporate assets not only from known threat vectors outside the corporate network but from those threats that circumvent standard defenses, such as border routers and firewalls, and present themselves from the inside.

Over time network administrators have implemented a defense-in-depth strategy. As a security strategy, defense-in-depth is nothing more than multiple layers of defensive measures to protect the corporate network against varied threats. Network access control technology provides another useful tool and defensive layer in the battle to protect corporate data assets against threats that circumvent the more standard defensive layers.

Some present offerings such as the Alcatel and Cisco's solutions are still fledglings in this market space and are presently limited to anti-virus compliance assessment. Others, such as Sygate's Secure Enterprise and Enterasys' Trusted End System have more advanced assessment and compliance capabilities. In the near future, network security efforts will benefit from the maturation and eventual implementation of 802.1x port-based network access control technology, providing another, smarter, weapon in the battle we wage daily.

Large networks, such as the University of North Carolina discussed above, have discovered the usefulness of network access control technology in their environment and have implemented it to protect against the threats introduced by mobile devices. In a university setting, with possibly hundreds or thousands of workstations, laptops and other devices randomly connecting to the network the cost of implementing network access control technology, even at this infant stage of development, offers more protection from internally-introduced threats than was previously available. If you are managing a network on which mobile devices over which you have little to no maintenance control, constantly come and go, network access control technology may well be a necessary next step in your defense-in-depth security strategy.

Smaller businesses with fewer mobile devices may find that this technology simply does not yet offer the return on investment that other solutions still can. A small business with several road warriors may still do well insisting that those mobile devices connect to the corporate network via a secure VPN or Citrix Secure Gateway – even when they are at their home offices. Managing antivirus and patch levels on these few mobile devices may still be more cost effective. Small businesses would still do well to begin considering network access control technologies to address future growth.

The decision to implement this technology at this time should not be taken lightly as there are many factors and solutions to consider. If not already in place, a risk analysis of the corporate network must be conducted to determine the level to which the network is at risk from threats that circumvent the standard defenses, such as mobile devices and laptops walking threats into the environment. If it is found that the network is at moderate to significant risk then a cost analysis must be completed to determine if the cost of this new defensive measure is worth the additional security it can provide.

It is not the place of this research to make a final need determination for each and every corporate network. Only network administrators and managers can decide if the technology and time is right for adding network access control to the current defense-in-depth strategy. Research does suggest that if you discover the time is right for your network you would do well to plan for a future that includes the advanced assessment and compliance capabilities that implementation of 802.1x technologies can offer.

References

Cisco Systems. Implementing Network Admission Control Phase One Configuration and Deployment. OL-7079-01, Version 1.1.Cisco Systems Inc., 2005

Cisco Systems. Release Notes for Network Admission Control, Release 1.0. Cisco Systems, Inc. 2004. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_release_note09186a0080270825.html

Hochmuth, Phil. NetworkWorldFusion . "Alcatel Switches gain security support." 8/16/2004 http://www.nwfusion.com/news/2004/081604alcatel.html

Hochmuth, Phil. NetworkWorldFusion, "Enterasys delivers switch-based security." 6/28/2004 http://www.nwfusion.com/news/2004/0628enterasys.html.

IEEE Std 802.1x-2001, IEEE Standard for Local and metropolitan area networks – Port Based Network Access Control. Institute of Electrical and Electronics Engineers, Inc. NY:NY, 2001

LURHQ Threat Intelligence Group. Berbew/Webber/Padodor Trojan Analysis. Lurhq Corporation. 2004 http://www.lurhq.com/berbew.html

Messmer, Ellen. NetworkWorldFusion, "The Enforcers." 5/17/2004 http://www.nwfusion.com/weblogs/security/005122.html

Northcutt, Stephen. Et. All. Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers and Intrusion Detection Systems. New Riders, San Francisco. 2003.

Podrezov, Alexey. F-Secure Virus Descriptions : Korgo. F-Secure Corp. 2004 http://www.f-secure.com/v-descs/korgo.shtml

Roberts, Paul. Network World Fusion. "Cisco buys network security company Perfigo." 10/21/2004 http://www.nwfusion.com/news/2004/1021ciscobuys.html

Tocheva, K., Erdelyi, G., Podrezov, A., Rautiainen, S. and Hypponen, M. F-Secure Virus Descriptions : Nimda. F-Secure Corp.; September 18-19th, 2001 http://www.f-secure.com/v-descs/nimda.shtml

Unknown. Melissa Virus. Proland Software, 2005

http://www.pspl.com/virus_info/w97m/melissa.htm

Unknown. CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. CERT Coordination Center: Carnegie Mellon University. 2001
http://www.cert.org/advisories/CA-2001-19.html

Unknown. Microsoft Security Bulletin MS04-011: Security Update for Microsoft Windows (835732). Microsoft Corporation. 2005
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Unknown. Barbedwire GLBA Solution. Barbedwire Technologies, Copyright © 2001-2004
http://www.barbedwiretech.com/solutions/glb.htm

Unknown. Frequently Asked Questions About HIPPA. Strategic Healthcare Initiatives, Inc. ©2001, 2002
http://www.hipaantidote.com/ha/faq.asp

Unknown. Sygate Changes the Game. Sygate Technologies: Fremont, CA. P3.

Unknown. InfoSecurity Magazine. "December 2004, Products of the Year."
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss526_art1054,00.html#sms

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event