Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Reining in the LAN client

We'll often see inadequate access control for the local area network (LAN). It is usually considered a "trusted zone" thus unfortunately a frequently neglected zone. While the LAN may well be the most trusted zone, to achieve an appropriate level of layered security, authorizing clients attaching to the LAN is paramount. Access to a building or office space is almost certainly regulated but what is not usually controlled is what/who can physically connect to the network medium. Whether it is a consultant, summer intern...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics
for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Reining in the LAN client

© SANS Institute 2004, Author retains full rights.

David G Monaco

September 15th, 2004

GSEC Practical Requirements (v1.4b)(August 2002)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

1. ABSTRACT 3

2. THE PROBLEM – DO YOU KNOW WHO'S ON YOUR LAN? 4

1.1 UNSECURED DEVICES WITHIN THE PERIMETER 4

1.1.1 Malicious code from unauthorized devices 4

1.1.2 Rogue services from unauthorized devices 6

1.1.3 Malicious intent and corporate espionage from unauthorized devices 7

1.2 WHAT IS USUALLY BEING DONE TO BATTLE THIS? 8

3. THE REMEDY – IDENTIFY AND AUTHORIZE 9

1.3 CONFIRMING THE GENERAL REQUIREMENTS 11

1.4 CONFIGURING THE ACTIVE DIRECTORY 12

1.5 CONFIGURING RADIUS / INTERNET AUTHENTICATION SERVICE (IAS) 13

1.6 CONFIGURING THE PUBLIC KEY INFRASTRUCTURE 14

1.7 CONFIGURING THE CLIENT 14

1.8 CONFIGURING THE AUTHENTICATOR 15

1.9 NOW FOR SOME CAVEATS 15

4. CONCLUSION 17

5. LIST OF REFERENCES 18

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Abstract

We'll often see inadequate access control for the local area network (LAN). It is usually considered a "trusted zone" thus unfortunately a frequently neglected zone. While the LAN may well be the most trusted zone, to achieve an appropriate level of layered security, authorizing clients attaching to the LAN is paramount. Access to a building or office space is almost certainly regulated but what is *not* usually controlled is what/who can physically connect to the network medium. Whether it is a consultant, summer intern or an employee who decides to bring in a personal laptop or use a non-approved computing device at the workplace, there will be the ability for a user (malicious or not) to connect a potentially dangerous device at the heart of your network.

This paper will demonstrate an effective way to protect against the threat of unauthorized client devices on a LAN while using common hardware/software combinations that are already deployed at many companies. These readily available tools allow almost any company to implement this solution to achieve an additional layer of security critical to maintaining a secure network.

What this document does not include

Though relevant content will be provided regarding an effective means of providing authenticated and authorized access for client devices on the LAN, the methods discussed MUST be combined with all other Information Security (Infosec) facets to properly secure your environment. Although not discussed in this paper, firewalls, host and network based IDSes, encryption, end-point security, etc, must all be deployed in tandem to achieve the highest level of security possible.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. The Problem – Do you know who's on your LAN?

The security focus at many firms typically revolves around securing the higher risk points of entry first, such as their Internet connection or wireless access points, ensuring that only authorized devices are granted access to the corporate network from *external* sources. Although assessing and prioritizing risks in order to apply resources to the most critical areas first *is* the appropriate strategy in securing one's environment, this must be followed with a program to ensure only authorized devices are granted access to a corporate network from *internal* sources.

Most larger companies will expend huge efforts to centrally control and distribute antivirus (AV) software and signature updates, deploy security patches to workstations and even lock down workstations builds to maintain their integrity as much as possible. While the required effort and investment may be substantial, a properly managed and controlled environment of desktops is an achievable goal that all companies need to achieve. Let's envision an ideal scenario pertaining to client environments on a local area network.

- Client antivirus (AV) software on all workstations with distribution servers issuing configuration policy and frequent signature updates.
- Distribution of Operating System (OS) and application security patches via Microsoft's Systems Management Server (SMS), Microsoft's Software Update Server (SUS) or any other 3rd party patch management tool.
- A group policy locked-down workstation build that reduces the attack surface, prevents users from modifying local settings or from logging on with excessive user rights.
- Network based Intrusion Detection System (IDS) firing on properly configured triggers to alert of any inappropriate activity generated by client devices.

These are four key items regarding securing a client environment and obtaining reporting and alerting capabilities. Still, there are excellent reasons for improving upon those existing measures already implemented.

1.1 Unsecured devices within the perimeter

1.1.1 Malicious code from unauthorized devices

What happens when a non-corporate client device isn't running appropriate antivirus software and does not run the most current security patches? With today's constant barrage of worms, viruses and other forms of malware, a device with this type of configuration that actively accesses Internet resources WILL get infected, often within minutes if not protected by a firewall or similar filtering type device. While securing devices that are not corporate assets is understandably

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

out of scope for any corporation, if they are free to connect to your network, they quickly become a risk that requires mitigation.

One may ponder how a single "uninvited" client device compromised with some form of malicious code connecting to a local area network can have such a large impact within the aforementioned environment above. One reason is that no IT system works perfectly all the time. Through my experience I've witnessed that there is always a small percentage of client workstations that do not have current antivirus signature files or do not receive required security patches as expected, even with aggressive and well regimented programs in place. Antivirus client software can become "stuck" where communication with the distribution servers gets severed, preventing policy and signature updates from being processed. Security patches also have a failure rate when applying them either with patch management tools or through manual application. In addition to possible software failures, unknowingly misconfiguring AV software or security devices also account for instances of unprotected devices.

Most well conceived applications dealing with deployment of security software will have effective methods of identifying clients that have malfunctioning or out of date antivirus configurations, as well as those workstations that did not successfully receive a required security patch. What this does allow however is a window of opportunity for malicious code to impact those workstations while they are in an exposed state. Whereas a vulnerable authorized client may be able to temporarily rely on the layered perimeter antivirus defenses while awaiting corrective measures, an unauthorized machine effectively bypasses all these additional defenses by arriving from external sources and gaining direct access to the unprotected local area network.

It is important to note that there does not have to be a large number of affected machines for there to be a noticeable negative impact within an environment. As few as nine or ten client machines infected with malicious code that generate large amounts of traffic while trying to spread can quickly affect network performance. Even if we were to estimate a conservative 1% of managed clients on a local area network of one thousand workstations being vulnerable due to malicious code due to misconfiguration or software failure, combined with a dozen non-managed and non-approved workstations plugged into the local area network, we could quickly have an incident that adversely impacts a production network.

While personal experience has shown that AV software has an operational failure rate, an article from Information Security Magazine[1] featured a sobering report on the current state of antivirus software. The article featured a survey of ten major antivirus software products that revealed many deficiencies amongst almost all the major vendors, further demonstrating the need to provide defense in depth

1 Skoudis, Ed. "Exposed." Information Security Magazine. June 2004 (2004): 22 – 33.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

also at the antivirus level. Corporate controlled clients can benefit from the protection of various AV vendor products set at different devices such as at the proxy gateway, mail relay and file server level. However, an infected foreign host able to connect to your LAN would have direct access to clients and servers, thus removing the benefit of the multiple layers of AV protection in place for those foreign devices. The testing results also indicated that protection provided for threats of spyware and backdoors is typically weak among almost all AV products. It can be safely assumed that the introduction of these types of malicious code threats from unsecured machines will be able to go unnoticed in many environments as a result.

1.1.2 Rogue services from unauthorized devices

Another threat to LAN security is rogue services. While the unauthorized devices may not contain malicious code they can instead provide illegitimate services on a network. Rogue Dynamic Host Configuration Protocol (DHCP) servers can wreak havoc by assigning incorrect Internet Protocol (IP) addresses to users or providing rogue Domain Name Service (DNS) servers as part of the DHCP scope options to then be able to redirect users to fake or malicious web sites. Even security features such as Microsoft's Active Directory requirement to authorize DHCP servers before address leasing can occur is easily defeated by running a Microsoft NT 4 or non-Microsoft DHCP server.

Other instances of danger include non-authorized machines running services such as Microsoft's Internet Information Server (IIS) or Microsoft Data Engine (MSDE) that are the top two vulnerabilities for the Microsoft Windows platform in the SANS Top 20[2] vulnerabilities list. They are especially dangerous as many users are unaware that they are installed, with Microsoft Windows 2000 Server installing IIS by default, and many Microsoft applications installing MSDE. As a result, these services are left in an unsecured, unpatched and often-compromised state. These unapproved and unauthorized network services may cause disruption to production networks and are key targets for malicious code. Therefore, the need to prevent these types of devices from connecting to your physical network is necessary.

2 SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities." Version 4. 8 October 2003. URL: http://www.sans.org/top20/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.1.3 Malicious intent and corporate espionage from unauthorized devices

Finally, there exists the often-ignored threat of intentional malicious attack or corporate espionage. As evidence of this, some companies are dedicated to this task such as Strategic Operations Ltd[3] who proudly display the following statement on their web site:

"We get information for your company. Whether you need to know when a competitor will be launching their new product, or what your competitor is spending their research money on, we will find out. There isn't anything we don't do."[4]

This is an excellent warning to all companies that the threat of corporate espionage is real. Furthermore, in "Corporate Espionage: A Real Threat"[5] we see a number of large corporations that have suffered such breaches. When faced with an especially robust security perimeter, determined attackers are left with few options to obtain access to a network, one of them being attacking from within. If the value of the data is high enough, possibilities of attacks from within the secure perimeter are possible. Gaining access to a secure building is not necessarily difficult under the right guises. An attacker can use any number of social engineering methods to gain access to the physical network medium. Masquerading as a sales person wishing to demo a product or running through the interview process at a company will often provide an opportunity for a malicious user to gain access to the physical network and connect a mobile client device. Within a short timeframe, malicious code could be released onto the network or data gathered from sources that are not properly secured.

Although a more sophisticated attack on a switched network, user passwords could also be sniffed off the network with tools such as dsniff[6], brute forced offline at a later time and used to remotely access the network from a safe distance.

3 Strategic Operations, Inc. URL: http://www.strat-ops.com

4 Strategic Operations, Inc. "Your Personal Spy Agency." URL: http://www.strat-ops.com/aboutus.htm

5 Luong, Minh. "Corporate Espionage: A Real Threat." Optimize Magazine. 10 Oct 2003. URL: http://www.internetweek.com/story/showArticle.jhtml?articleID=15202264

6 Song, Dug. "dsniff Frequently Asked Questions." 7 Dec 2001. URL: http://www.monkey.org/~dugsong/dsniff/faq.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2 What is usually being done to battle this?

So why the need for any form of client authentication in the LAN as opposed to earlier methods of controlling access to the physical medium? Traditionally, four methods were and are still are used when attempting to control access to the local area network.

1. Disabling unused ports on switches.
2. Enabling port security on switches to allow only preauthorized Media Access Control (MAC) addresses.
3. Assigning unused ports to a disabled Virtual LAN (VLAN).
4. Populating DHCP scopes with MAC reservations of valid clients so that only they will receive an IP address dynamically.

These four methods all provide some measure of effectiveness. However, they all have manageability and scalability issues when extended to larger environments. There is also nothing in place to prevent an unauthorized user from disconnecting an existing workstation from a live connection or for a malicious user to sniff valid MAC addresses or other traffic off the network.

Of course, physical security comes into play when dealing with non-authorized personnel attempting to connect to physical network ports or bringing devices such as laptops into your corporate space. Most large corporations are not equipped with a “choke point” where visitors may be scrutinized for laptop and communication devices. Many visitors will also find it unacceptable to leave a laptop device with another party if it contains sensitive data, as well as the potential “political” repercussions of demanding devices such as laptops from executive level personnel arriving from other companies. So, although being vigilant and challenging an unknown user who is plugging into your network is desirable, many corporate environments are very open and visitors find themselves with unfettered access to the physical network.

Now that we’ve identified some of the risks in permitting unprotected access to the local physical network, we must remember that removing either the threat or the vulnerability are acceptable methods to mitigate a risk. I’ll demonstrate a method to remove the vulnerabilities since removing the threats would be much more difficult, if not unrealistic.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. The Remedy – Identify and Authorize

Now that we've identified the threats and where the vulnerability lies, an appropriate course of action is required to mitigate the risk. In comes client authentication for the wired local area network.[7]

So what is client authentication for the LAN? Only clients that can successfully authenticate against an approved list of valid devices can gain access to the local network. A compliant network switch will only permit Extensible Authentication Protocol over LAN (EAPOL) traffic from a client until successful client authentication, at which point that particular switch port will become authorized. Unsuccessful authentication will result in a switch port remaining in an unauthorized and therefore, secured state. This has become a common and popular method in creating secure wireless infrastructure access but has yet to be utilized extensively for local area network access control.

Although many hardware vendors now support 802.1x port-based authentication, this document will site examples using 802.1x/Radius compliant Cisco network switches combined with a Microsoft Windows Active Directory environment as they are common in many companies. Since no other software purchase or licensing would be required, companies with a more modest IT security budget can look at implementing this solution to defend against unauthorized LAN clients.

Here briefly, is how the authentication takes place. Three components make up the 802.1x port control authentication as illustrated in Figure 1.

1. Supplicant
2. Authenticator
3. Authentication server

The Supplicant is the device or client that must identify itself by providing credentials to obtain access to the network, such as a Microsoft Windows XP operating system.

The Authenticator is simply the network device port, in this case a port on a Cisco 2950 switch that requests the identity and forwards the credentials from the Supplicant to the Authentication server while preventing access until successful authentication.

[7] While many details will be provided regarding some required and ideal configuration for an 802.1x LAN implementation with Microsoft and Cisco products, there are many other possible variations with many different vendors. Although the next section will only cover the high level configuration requirements for the aforementioned scenario, a proper desktop management program must be in place along with the other Infosec facets required to achieve the required defense in depth for a more robust security posture. If users are free to install applications and services on their machines, are not properly patched with security updates, and are not running an anti-virus software with regular auto-updating signature files, then implementing a solution such as 802.1x will only have minimal benefits.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Authentication server, in this case the Microsoft implementation of Radius (Remote Access Dial in User Service) known as Internet Authentication Service (IAS), validates the credentials forwarded by the Authenticator and instructs it either to authorize access to the supplicant or to remain in an unauthorized state.

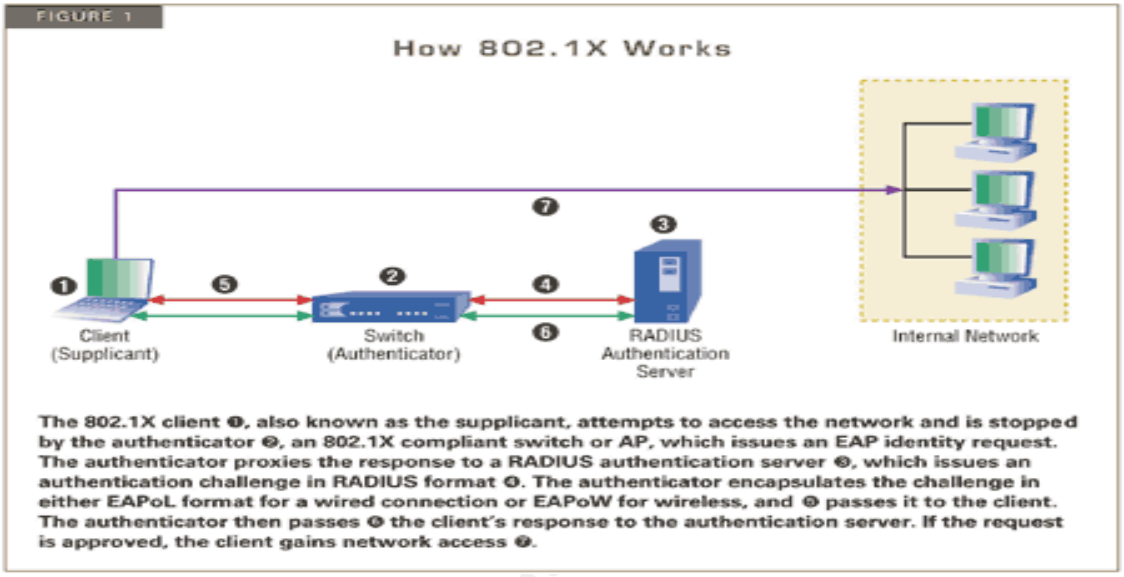

Figure 1. How 802.1x works[8]

Now that we have a general understanding of the authentication process, we'll delve a little further into the requirements and high-level configuration of the authentication system. While not meant to be a step-by-step guide, we'll focus on six areas to break down the deployment into manageable pieces.

1. Confirming the General Requirements
2. Configuring the Active Directory
3. Configuring Radius
4. Configuring the Public Key Infrastructure
5. Client Configuration
6. Authenticator Configuration

[8] Kelley, Diana. "The X Factor." Information Security Magazine. August 2003. URL: http://infosecuritymag.techtarget.com/images/2003/aug/802-Fig-1.gif

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3 Confirming the General Requirements

As previously mentioned, many companies already possess most of the required components to implement an authenticated LAN client. First and foremost, an authentication type must be selected. Ideally if a Public Key Infrastructure (PKI) is already in place, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is the EAP method of choice due to its overall additional security benefits (see Figure 2), therefore we'll select this for our scenario. It is also the default-configured client EAP authentication method for Microsoft Windows clients.

However, initially it may be more cost-effective for a company to opt for Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol v2 (MS-CHAPv2), which is a password based authentication scheme, not requiring client side certificates and full PKI to support it.

Choosing the Right EAP

Your security needs and authentication infrastructure should guide your choice from among a daunting—and growing—menu of options.

	EAP-TLS	EAP-TTLS	PEAP	LEAP
Recommendation	Good choice if you have PKI or cert distribution method in place. Otherwise, it may be cost prohibitive.	Good choice for organizations with heterogeneous environments.	Strong choice for Windows/Cisco shops, less so for more heterogeneous environments.	Reasonable choice for all-Cisco shops.
Security	Highest	High	High	Medium
Mutual Authentication	✔	✔	✔	✔
WEP Key Management	✔	✔	✔	✔
RADIUS Server Support	Cisco, FreeRADIUS, Funk, Interlink, Meetinghouse, Microsoft, Radiator	Funk, Interlink, Meetinghouse, Radiator	Cisco, Funk, Meetinghouse, Microsoft, Radiator	Cisco, FreeRADIUS, Funk, Interlink, Meetinghouse, Radiator
Client Support	Cisco, Funk, Meetinghouse, Microsoft, Open1X	Alfa-Ariss, Funk, Meetinghouse, Open1X	Funk, Meetinghouse, Microsoft	Cisco, Funk, Meetinghouse
Client Platforms	Mac OS X, BSD, Linux, Windows XP/2000/2003, Win32	Mac OS X, BSD, Linux, Win32	Windows XP/2000/2003, Win32	Win32
Server Authentication	Certificate	Certificate	Certificate	Password hash
Supplicant Authentication	Certificate	CHAP, PAP, MS-CHAPv2, EAP	Any EAP, such as EAP-MS-CHAPv2, or certificate	Password hash
Pros	Strongest security; native to Windows.	Encrypted creden-tials; reuse LDAP.	Encrypted credentials; availability (Windows/Cisco).	Native Cisco support; CCX for non-Cisco hard-ware; LDAP reuse.
Cons	Requires PKI for client management; user ID can be exposed.	Proprietary clients.	Vulnerable to man-in-the-middle attacks; lack of interoperability.	Proprietary; vulner-able to dictionary attacks; user ID can be exposed.

Figure 2. Choosing the right EAP [9]

[9] Kelley, Diana. "The X Factor." Information Security Magazine. August 2003. URL: http://infosecuritymag.techtarget.com/images/2003/aug/EAP-diagram.gif

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Below are the major requirements and selections for the scenario.

- Active Directory implementations based on either Windows 2000 (with SP4) or Windows Server 2003 can be used. For the purpose of this document, we'll use a single Active Directory based forest/domain on Windows Server 2003.
- From a client perspective, Microsoft Windows XP, Windows Server 2003 and Windows 2000 SP3 (with 802.1X Authentication Client patch) or SP4 all natively support and can participate in an 802.1X environment. To facilitate the scenario, we'll assume an environment of all Windows XP SP1 clients.
- A Radius (the Authentication Server) server is required to authenticate and authorize devices and the native Microsoft implementation of Radius, Internet Authentication Service (IAS), can be deployed. It is the ideal choice for this scenario with its integration into the existing Microsoft AD, as well as its low cost (included free) with the Windows Server 2003 Standard and above operating systems.
- A PKI is required for the certificate-based authentication we've selected. Again, the PKI capabilities that are included with Windows Server 2003 are ideal with its Active Directory integration capabilities. Only computer-based authentication[10] will be used as this meets our requirement to only allow authorized machines to connect to the network, as well as reduces the complexity.
- Network switches that support the Radius client and 802.1x are required to act as the Authenticators that proxy information between the Supplicant and Authentication server. Configuration details pertaining to the Cisco Catalyst 2950 switch will be used.

1.4 Configuring the Active Directory

The first configuration step required is to confirm the required Active Directory account settings for all computers that will be authenticating against your Radius/IAS servers. The remote access permissions for the computers accounts should be set to "Control access through Remote Access Policy" in the Dial in-tab of those objects, to be able to easily configure access centrally via the Remote Access Service (RAS) policies. This is the default object setting in Windows Server 2003 Active Directory. For manageability and supportability reasons, you'll

[10] User based authentication required user certificates to be deployed to all users and these cannot be deployed via group policy with the standard version of Windows Server 2003 as can the machine certificates. Either the Enterprise/Datacenter edition of Windows Server 2003 is required to be able to automatically deploy user certificates via group policy, a CAPICOM script or individual user self-enrollment to the CA web server. We'll use only machine authentication as it will accomplish our objectives, as well as allow more companies to be able to deploy this with their existing infrastructure.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

want to create an appropriate security group for your computers to be able to easily apply the Remote Access Policies to the required objects.

1.5 Configuring Radius / Internet Authentication Service (IAS)

In order to authenticate and authorize valid devices, the Internet Authentication Service (IAS) must be installed and configured. A common and simple configuration location for IAS is on a Domain Controller. While this provides improved response times and reduced network traffic, IAS can also be installed on any other Infrastructure server. If a non-Domain Controller is selected, the IAS server must be registered[11] (see footnote for link details) in Active Directory in order to be able to read account property information.

As maintaining the availability to access the network depends on successful authentication and authorization by an IAS server, two or more IAS servers should be installed as well as all Authenticators (Cisco 2950 switches) configured to use multiple IAS/Radius servers to provide fault tolerance. If a single IAS server environment were to be deployed, an attack, hardware failure or even routine maintenance of the IAS server would result in a network availability loss and disruption of network services.

Be sure to enable authentication and accounting logging in IAS to ensure that appropriate records are kept. If a firewall or filtering device separates the Radius clients and IAS servers, ensure that the appropriate ports[12] are open to permit the required traffic.

The authenticating switches must be added as Radius clients of the IAS servers. The IP address of each Radius client as well as a "shared secret" must be configured in IAS. A strong and different password (or ideally pass phrase) should be used for each Radius Client to reduce the risk of password attacks, as well as reduce the impact on the network should one of the Radius client passwords be compromised[13].

Finally, a remote access policy in IAS needs to be configured to permit the authorized clients to access the network. The access method, appropriate security group containing the computer accounts, the authentication method to be used and any required specific vendor attributes will be configured here.

All configuration performed on the primary IAS server can be quickly duplicated[14] (see footnote for link to configuration details) to the other IAS servers to ensure

---

[11] Microsoft Corporation. "Enterprise Deployment of Secure Wired Networks Using Microsoft Windows." Version 1, April 2004. URL: http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc Page 3.

12 IAS Authentication uses UDP ports 1812/1645 and accounting messages use UDP ports 1813/1646.

13 If the authenticating switch supports IPSEC, this can be used to further protect the exchange of Radius.

14 Microsoft Corporation. "Enterprise Deployment of Secure Wired Networks Using Microsoft Windows." Ver 1. April 2004. URL: http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc Page 11

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

identical configuration and minimize errors. This procedure can and should be used for any changes to the primary IAS server configuration. Computer certificates for the IAS servers are also required for mutual authentication between client and server.

1.6 Configuring the Public Key Infrastructure

The machine certificates required for computer authentication can be generated by the native PKI included with Windows Server 2003 Standard edition and higher. Depending on the size of the company, a different hierarchy of PKI may be required and best practices[15] (see footnote for link to configuration details) in securing your PKI should be followed in accordance with the size of your deployment. If a PKI is already in place for Internet Protocol Security (IPSEC), VPN remote access or any other authentication requirements in your domain, the same PKI can be leveraged for use in an 802.1x deployment.

1.7 Configuring the Client

Unfortunately, no group policy methods exist to configure 802.1x settings for LAN interfaces as can be accomplished for wireless network interfaces. As the use of 802.1x for wired networks grows, I expect this group policy capability will be available in future service packs of Microsoft Windows products. Fortunately, Windows XP clients are configured by default to use 802.1x authentication, if available. This means that your Windows XP clients are ready to participate in an 802.1x authentication scheme out of the box.

The required machine certificates from your Certificate Authority (CA) hierarchy can easily and automatically be distributed to all your client devices participating in 802.1x authentication. The same group policy setting can also be used to deploy the required machine certificates for the IAS servers. Since only computer authentication will be used, client stations must be configured via the registry[16] (see footnote for link to configuration details) to disable user authentication. A number of enterprise tools are available to configure registry settings remotely such as SMS or group policy scripts.

15 Microsoft Corporation. "Enterprise Deployment of Secure Wired Networks Using Microsoft Windows." Version 1. April 2004. URL: http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc Page 12

16 Microsoft Corporation. "Enterprise Deployment of Secure Wired Networks Using Microsoft Windows." Version 1. April 2004. URL: http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc Page 35

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.8 Configuring the Authenticator

The Authenticator selected for our scenario is the Cisco 2950 Catalyst switch as it is a robust and commonly used network device. In order to meet the minimum software requirements for any desired 802.1x features; ensure your device is at the appropriate IOS version 12.1.

Once this requirement has been met, the switch must be configured to use the configured Radius/IAS servers along with the previously configured shared secret pass phrases. Once defined, 802.1x port authentication can be enabled on the switch allowing the EAP negotiations to occur. All network switches should be configured in the same fashion. Finally, the authorization mode must be configured on the switch, which in this scenario is "Auto"[17] (see footnote for link to configuration details) mode to ensure only authenticated and authorized clients are permitted network access.

After successful implementation of the required components for 802.1x authentication, only YOUR clients will be successfully authenticated, authorized and permitted to communicate freely on your LAN.

1.9 Now for some caveats

Some caveats exist with the illustrated scenario as with almost any solution. Most environments contain devices that do not support 802.1x authentication, such as network printers. For the instances where a device cannot support the desired client authentication, one of the four previously used methods can still be employed, such as restricting the specific switch port to the MAC address of the printer Network Interface Card (NIC). Although this is not an insurmountable security control, it is easily managed for a small and well defined scope, as well as easier to identify abuse since a non-functioning network printer will attract attention quickly, as will an unknown user attempting to plug into a network printer wall jack in plain site! Furthermore, these types of devices are typically not located in the most common locations that visitors could potentially connect to the network, such as conference rooms and guest areas.

Finally, there may be a need for trusted, but not managed, devices to temporarily gain access to your network. Often, a limited set of services are provided to allow basic functionality for these devices, whether it be to access a special intranet/Internet web sites or allowing outbound Virtual Private Network (VPN)

---

[17] McQuerry, Steve. "IEEE 802.1x: Practical Port Control for Switches." Cisco World Magazine. 4 October 2002. URL: http://www.ciscopress.com/articles/article.asp?p=29600&seqNum=3
Cisco Systems, Inc. "Cisco Catalyst 2950 Series Switches: Configuring 802.1x Port-Based Authentication." Date Unknown. URL: http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6c72.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

connections so that consultants and 3rd party vendors may connect to their corporate networks. For this task, Guest VLANS are becoming more popular as a means to provide some form of network connectivity for devices that cannot successfully authenticate to the network. While this may be an advantageous feature to those desiring external access, care must be taken when permitting unknown users to potentially connect to external sites. Any form of outbound malicious or inappropriate activity will still be considered to have originated from your corporate network and public IP space and the unknown users may not be governed by your security policy, resulting in the risk of downstream liability.

A plausible option would be to require some form of acceptable usage policy signoff for any outside user that would like specific external network access. While this may assist from a liability perspective, the optimal solution for many companies may be to simply prevent any form of non-monitored and non-corporate outbound network access from unauthorized devices.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. Conclusion

Permitting unauthorized client devices to connect at the heart of your network can result most notably in serious availability and confidentiality incidents. Security controls need to be implemented at multiple levels in order to thwart even common attacks. However, the location of each layered security control is a key component not always taken into consideration. Even with multiple security measures implemented, if an attacker or device with malicious code can enter onto your network directly, many layers of defense will have already been bypassed with little or no effort, reducing the effectiveness of your layered defenses. What this does demonstrate with regards to the importance of defense in depth is that security practitioners must also be vigilant to ensure that when possible, layered security controls must apply to threats coming from all sources and all directions.

Providing authenticated access to your network will increase your overall security posture by removing a dangerous variable, non-authorized local area network clients. Restricting client device access to devices under your control increases the likely-hood of maintaining a high level of integrity within your environment. Client authentication with 802.1x is an ideal method to achieve this goal. While 802.1x provides a reliable method to prevent access from unauthorized devices, we are also beginning to see more and more products that extend this concept further.

A number of products are in development or have recently been introduced to provide means to measure the overall integrity of systems connecting to the local area network. Products such as Cisco's new "Network Admission Control"[18], Zonelab's "Endpoint Security"[19] or Microsoft's future "Network Access Protection"[20] all can provide additional security for approved network clients. Verifications such as security patch level, antivirus signature level and other required security settings can be prerequisites for accessing the corporate servers. These technologies will often work in conjunction with 802.1x to provide additional security for devices that are authorized but not compliant with the standard security guidelines. Issues previously identified such as malfunctioning or out of date antivirus software and missing security patches could be captured with such a system and network access prevented until corrected. Although this type of security control is more prevalent in securing remote access systems, it should quickly become accepted as a standard offering in secure environments, complimenting 802.1x.

The threat is out there. Rein in your LAN client devices now!

---

[18] Cisco Systems, Inc. "Cisco NAC: The Development of the Self-Defending Network." 7 June 2004. URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/csdni_wp.htm

[19] Zonelabs, LLC. "Enterprise Solutions: Security Policy Enforcement." Date unknown. URL: http://www.zonelabs.com/store/content/company/corpsales/solutionPolicyEnforcement.jsp

[20] Bekker, Scott. "Quarantining Part of Windows Server 2003 'R2' Fleshed Out." 13 Jul 2004. URL: http://www.entmag.com/news/article.asp?EditorialsID=6301

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. List of References

McQuerry, Steve. "IEEE 802.1x: Practical Port Control for Switches." Cisco World Magazine. 4 October 2002. URL: http://www.ciscopress.com/articles/article.asp?p=29600 (6 September 2004).

Kelley, Diana. "The X Factor." Information Security Magazine. August 2003. URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art108,00.html (17 August 2004).

Davies, Joseph. "Microsoft 802.1X Authentication Client." December 2002. URL: http://www.microsoft.com/technet/community/columns/cableguy/cg1202.mspx (8 September 2004).

Funk Software, Inc. "Using 802.1X for Wired LAN Authentication." Date Unknown. URL: http://www.funk.com/radius/Solns/wired_8021x_ah.asp (25 August 2004).

Microsoft Corporation. "5-Minute Security Advisor – Deploying 802.1x with Windows XP." Date unknown. URL: http://www.microsoft.com/technet/community/columns/5min/5min-303.mspx (24 August 2004).

Snyder, Joel. "What is 802.1x?" Network World Fusion. 06 May 2002. URL: http://www.nwfusion.com/research/2002/0506whatisit.html (25 August 2004).

Hewlett-Packard Development Company, L.P. "ProCurve Networking security solution: 802.1x and Guest VLANS." Date Unknown. URL: http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm (16 August 2004).

Microsoft Corporation. "To set up 802.1x authentication." Date unknown. URL: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/8021x_client_configure.mspx (24 August 2004).

Institute of Electrical and Electronics Engineers, Inc. "Port-Based Network Access Control." 13 July 2001. URL: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf (20 August 2004).

Microsoft Corporation. "Enterprise Deployment of Secure Wired Networks Using Microsoft Windows." Version 1. April 2004. URL: http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc (5 September 2004).

Bekker, Scott. "Quarantining Part of Windows Server 2003 'R2' Fleshed Out." 13 Jul 2004. URL: http://www.entmag.com/news/article.asp?EditorialsID=6301 (20 August 2004).

Zonelabs, LLC. "Enterprise Solutions: Security Policy Enforcement." Date unknown. URL: http://www.zonelabs.com/store/content/company/corpsales/solutionPolicyEnforcement.jsp (2 September 2004).

Cisco Systems, Inc. "Cisco NAC: The Development of the Self-Defending Network." 7 June 2004. URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/csdni_wp.htm (2 September 2004).

Song, Dug. "dsniff Frequently Asked Questions." 7 Dec 2001. URL: http://www.monkey.org/~dugsong/dsniff/faq.html (18 August 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Tulloch, Mitch. “DHCP Server Security (Part 1).” 20 Jul 2004. URL: http://www.windowsecurity.com/articles/DHCP-Security-Part1.html (18 August 2004).

Luong, Minh. “Corporate Espionage: A Real Threat.” Optimize Magazine. 10 Oct 2003. URL: http://www.internetweek.com/story/showArticle.jhtml?articleID=15202264 (1 September 2004).

Strategic Operations, Inc. “Your Personal Spy Agency.” URL: http://www.strat-ops.com/aboutus.htm (2 September 2004).

Cisco Systems, Inc. “Cisco Catalyst 2950 Series Switches: Configuring 802.1x Port-Based Authentication.” Date Unknown. URL: http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6c72.html (24 August 2004).

Strategic Operations, Inc. URL: http://www.strat-ops.com/ (2 September 2004).

SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities.” Version 4. 8 October 2003. URL: http://www.sans.org/top20/ (20 August 2004).

Skoudis, Ed. "Exposed." Information Security Magazine. June 2004 (2004): 22 – 33.

Minasi, Mark; Anderson, Christa; Beveridge, Michele; Callahan, C.A. Mastering Windows Server 2003. Alameda: Sybex, Inc, 2003

Khnaser, N. Elias; Snedak, Susan; Peiris, Chris; Amini, Rob; MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide. Rockland: Syngress Publishing, Inc, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced