Global Information Assurance Certification Paper

Designing a Secure Remote Desktop Support Methodology

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 – Case Study in Information Security

Submitted by: Keith Wingate
Location: SANS Twin Cities: June 25-30, 2004 in Minneapolis, MN

Table of Contents

List of Figures

Summary

My company (MyCompany, Inc.) provides Information Service Solutions to Fortune 500 companies. In this particular case, we provide support for a large corporation, which for the purpose of this document; we will call ABC, Inc. This support contract includes LAN/WAN connectivity, backend server support, desktop support and many other services. My team manages an extranet service for ABC, Inc. that allows them to connect with 3rd parties for secure business communications. Our extranet is nestled between the ABC, Inc. enterprise and the Internet.

We were approached by ABC, Inc. to provide a solution that will allow the desktop technicians to connect and control a user's PC and resolve technical issues. ABC, Inc emphasized that this solution must be secure and scalable. The catch was that there were two different support teams located in two different locations. One of the teams (Team A) was stationed at an ABC, Inc. campus. Team A supports local ABC, Inc. enterprise users. They were given the responsibility to provide desktop support to home users that connected to the ABC, Inc. enterprise via a personal IPSec VPNs. The second team (Team B) was stationed at an offshore location of MyCompany, Inc. This was a new team being developed to provide after-hours support for the same type of users as Team A. There was no connection between MyCompany, Inc.'s offshore location and the ABC, Inc. enterprise. Team B would need to connect to ABC, Inc. via the Internet.

According to the project guidelines, the solution had three requirements. It need to be secure, provide two-factor authentication and utilize the central manageability of Active Directory. As Team Lead of this project, I presented a solution comprised of three major components; Windows 2000 Active Directory, Microsoft's Enterprise Certificate Authority services and Juniper's NetScreen SSL VPN appliance with the Secure Meeting feature. This document will explain how I was able to combine all these components into one secure and easily manageable solution.

Before

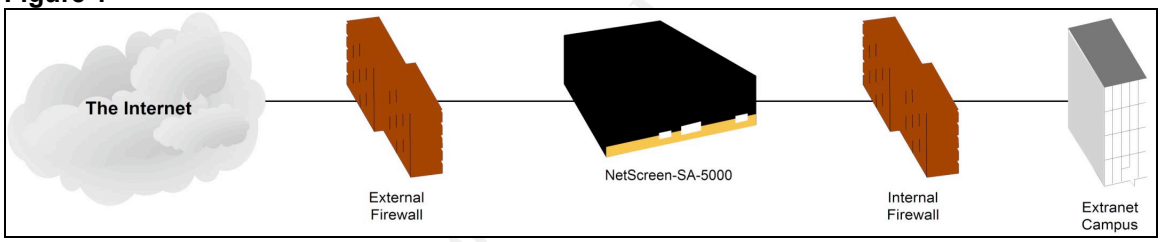
Microsoft's NetMeeting, along with its desktop sharing feature, had long been the solution to support local users on the ABC, Inc. enterprise. This solution was not a secure method for home users behind broadband firewalls. It was possible to configure the broadband routers to allow the NetMeeting ports inbound, but it left users vulnerable to attack. Plus NetMeeting was not a secure troubleshooting method across the Internet since the traffic was not encrypted.

At one point it was suggested that since all desktops had been upgraded to Microsoft Windows XP, then we should utilize its Remote Assistance feature. This feature in XP allows users to send an email invitation to a technician allowing them to remotely manage their PC via a scaled-down version of

Windows Terminal Service. This solution was quickly ruled out because of issues with Network Address Translation (NAT) on the home networks behind broadband routers. When a user compiled the invitation using the Microsoft suggested method, the user's IP address was listed with the network interface card (NIC) assigned address. Typically a broadband router assigns an IP address to the NIC using a DHCP scope in the reserved 192.168.1.0/24 subnet. Providing an IP address in this scope makes it impossible to connect to the user's PC via the Internet.

We recently purchased Juniper's NetScreen-SA-5000 SSL VPN appliance to provide remote access to services provided by our extranet. We chose this device because of its strength, manageability and Secure Meeting feature. The appliance sits between an internal and an external firewall. Only http and https are allowed inbound to the appliance. Various ports are allowed outbound from the appliance to the internal network depending on the nature of the service required. For instance, TCP 3389 is allowed from the appliance to several extranet servers through the internal firewall to provide Windows Terminal Server access to these servers for our administrators.

Figure 1



While the NetScreen appliance is quite capable of sitting in-line with the external firewall, that design does not follow the Defense-in-Depth principal outlined within the SANS Security Essentials course. We provide another layer of security by securing our border Internet router with firewall feature-set to help filter unwanted traffic before it reaches the external firewall. We ran numerous vulnerability scans against this appliance on both the internal and external interfaces using utilities such as; Nessus, nmap and Nikto. All of these scans returned the same results time and time again… nothing. The only ports found open were http and https and there were no successful exploits made on either of those ports.

The NetScreen appliance has a central management utility that makes it very easy to configure and implement its many features. However, it is the Secure Meeting feature that provides a solution to this dilemma. It allows a meeting to be held between multiple parties anywhere via the Internet utilizing SSL for security. Meeting attendees have the ability to share individual applications or their entire desktop with other attendees. This allows remote support technicians to see the types of errors users might be receiving without ever leaving their desk. They also have the ability to take control of the user's session for troubleshooting purposes. This appliance alone, however, does not meet all the requirements mandated for this solution.

The solution also requires two-factor authentication. Because support personnel will have the ability to control user's PCs, it is good practice to require a second authentication method. The second method chosen for authentication was client-side certificates. These certificates utilize the Public Key Infrastructure (PKI) technology to create digital IDs for the users. "Microsoft built a comprehensive PKI into the Windows 2000 operating system."[1] The Microsoft CA solution was chosen because it seamlessly integrates with the security features of Active Directory. For this solution, only the user certificates were necessary. *(The terms user certificate and client-side certificate will be used interchangeably within this paper.)* When a user certificate is created, the CA ties the certificate to the user's account in Active Directory. Windows 2000 was used in lieu of Windows 2003 primarily because of budget constraints for the Windows 2003 licensing

Active Directory in its own right is an extremely powerful and complex technology. The planning, designing and configuration of an Active Directory implementation is far beyond the scope of this paper. In this instance, Active Directory had been in place for quite some time and required no additional fine tuning. It is a native-mode configuration with two Windows 2000 domain controllers and a multitude of Windows 2000 application servers.

During

The design was simple. Remote Desktop Technicians *(this document will also refer to these individuals as meeting conductors)* would login to the NetScreen appliance via the Internet. The meeting conductors would use their Active Directory account for this purpose. Before they are authenticated, they must first provide a user certificate that was issued by the Enterprise Certificate Authority (CA). Once logged in, the only available resource for them would be the Secure Meeting application.

As stated earlier, Active Directory was already in place and functioning. Since Microsoft provides CA services with Windows 2000 that will integrate into Active Directory, we decided to utilize this technology. The design for the certificate services piece of this solution was chosen to provide both flexibility and scalability. There is the possibility that the need for certificates will grow and I decided it was best to implement a solution that would best accommodate future expansion needs. It was decided that an Enterprise Certificate Authority would be used versus a Stand-Alone CA to utilize the Active Directory integration. This would require a two-tier Certificate Authority hierarchy which includes a root CA and a subordinate CA.

The root CA would issue a certificate to the subordinate CA and it would then be taken offline. This allows for the most secure means of protecting the root CA's

[1] Shinder (p.669)

private key from attackers. The root CA would only be brought back online to issue a certificate to a new subordinate. Renewing or revoking a certificate for an existing subordinate would also be cause to bring it back online. The subordinate CA would then have the responsibility of issuing all user certificates.

Now this provided the ability for users connected to the enterprise to request a certificate, but there was still the matter of MyCompany, Inc. meeting conductors on the Internet that needed to request a certificate as well. The first thought was to create a second subordinate CA and place it in a DMZ area for Internet users. This is the recommended Microsoft solution. However, I was just not comfortable with that solution, because exposing any device to the Internet dramatically increases your security risks. To help minimize the risk, NetScreen appliance was elected to supply another piece of the equation. The NetScreen appliance has the flexibility to configure many different authentication realms. Each of these authentication realms can be presented in the Sign-in page. When a user selects one realm from the Sign-in page, he might see different resource selections than if he selected another realm. This is dependant upon which resources are mapped to him by the Administrator within that particular authentication realm.

Meeting conductors only need to click on one URL to access both certificate requests and Secure Meetings. Depending on the realm the user selects on the Sign-in page he would see either resource. Since the meeting conductors are not allowed to access the Secure Meeting section without a certificate, they must first login using the certificate request realm before the Secure Meeting realm.

The Configuration

Active Directory

The first step was to create a Global Group in Active Directory called G_Meeting_Conductors. The majority of the meeting conductors belonged to different domains and did not have accounts in this domain. A script was written to create all necessary accounts and add them to the G_Meeting_Conductors group. The flag was set to require the users to change their password at next logon.

Certificate Authorities

Next, the root CA was configured on a Windows 2000 server. Certificate Services was installed as an Enterprise root CA from the Add/Remove Windows Components section of Add/Remove programs. The Microsoft Base Cryptographic Provider was used for the CSP and SHA-1 was selected as the hashing algorithm. The key length was set to 2048 to provide a stronger key but still remain small enough for today's modern PC to calculate quickly without crippling system resources.

In order to make it easy for the meeting conductors to submit and retrieve certificates, I decided to install the subordinate CA with Certificate Services Web Enrollment Support. However, this does require that Internet Information Services (IIS) be installed previous to the CA installation. IIS 5.0 was installed since this was a Windows 2000 server. By default, everything in IIS 5.0 is selected during installation. I deselected such services as ftp and SMTP because they were not required for this solution and would pose unnecessary security risks if installed. I selected the minimal options needed to run this website. Those options included, Common files, Internet Information Services Snap-In and the World Wide Web Server. After IIS was installed, I ran the IIS Lockdown Tool on the server. This utility removes all the extra files installed with IIS that are needed depending on the role of your website. There are several templates to choose from that range from a static web site to a Microsoft Exchange 2000 Server. Unfortunately, there was not a template for a CA server with Web Enrollment. Because the Web Enrollment site is comprised of Active Server Pages, I chose the template to allow ASP extensions.

The subordinate CA was installed in relatively the same manner as the root. Except the Enterprise subordinate CA option was selected and the name of the root CA was required for the subordinate CA to request its own certificate. Also, as stated above, the Certificate Services Web Enrollment Support option was selected. Another requirement was that only select individuals were allowed to request certificates. Permissions were assigned to only allow the G_Meeting_Conductors group to access the web site. Also, within IIS, the web site's authentication method was configured as Integrated Windows authentication and anonymous access was removed. The root CA was not installed with the Web Enrollment feature because convenience is not a requirement for issuing and revoking subordinate CA certificates.

By default the Web Enrollment directory is installed in c:\\winnt\system32\certsrv. This directory stores all of the Active Server Pages necessary for the certificate enrollment process. I decided to move the certsrv directory off of the system partition and onto another partition to add another level of security. Microsoft does not provide the option during setup to select an alternative location for this directory. So the move process was done manually. I was able to change the Certificate Revocation List and the CA certificate distribution points using the certutil command. This command allowed me to easily modify the CRLPublicatoinURLs and CACertPublicationURLs registry entries. I was able to place them in a location that would be less damaging to the server in the event of a compromise.

The NetScreen Appliance

The most complicated process was configuring the NetScreen appliance. In order to understand this configuration it is important to discuss a bit about how the NetScreen appliance operates. The NetScreen appliance is comprised of several layers that must be configured in order for everything to work together.

First is the authentication server. The NetScreen appliance can authenticate users based on accounts created on the appliance itself (also called local accounts) or it can be configured to use Lightweight Directory Access Protocol (LDAP). There are several other options for authentication servers, but they are beyond the scope of this paper.

Once the authentication server is configured, the next step is to configure a user role. A role sets the options and resources available to the user once he successfully logs in. There are literally hundreds of options to choose from including web bookmarks and meetings. After all the options are configured it is time to setup the authentication realm.

The authentication realm is the piece that maps users to a particular role based on criteria defined by the Administrator. It is also linked to an authentication server in order to verify a user's credentials. There is also the ability set restrictions on certain parameters that users or their machines must meet. For instance, this is where the requirement for client-side certificates is set.

The final piece is the Sign-in Policy. This allows for a custom Sign-in page and the ability to dictate which authentication realm(s) are provided for the user. So in order to make this solution work, the following configuration was implemented:

Authentication Server

During the early stages of this design, local accounts were chosen as the method of authentication for all the meeting conductors. It was later determined that Active Directory should play a roll in this process because of its strong security features and central manageability. So for that reason, LDAP was chosen for the authentication server type. The NetScreen appliance can connect to an Active Directory domain controller via LDAP to provide authentication. LDAP alone, however, is not at all secure because it passes login credentials (which include passwords) in clear text. So LDAPS, which employs SSL to secure LDAP communication, was used. The NetScreen appliance already has this functionality built in. The only requirement was for Enterprise Certificate Services to be configured in Active Directory and we already took care of that.

An Authentication Server named Server1 was created. The two Active Directory domain controllers were listed as its primary and secondary LDAP servers. They were configured to communicate on TCP port 636 which is the default port for LDAPS. The LDAP Server Type was set to Active Directory. This helps the NetScreen appliance compile the LDAP communication in the correct format.

Since this was the only way for the meeting conductors to access the Active Directory domain, the password management feature was enabled to allow meeting conductors to manage their password.

This allows users the ability to change their passwords. It basically enforces the policies set in the Active Directory Global Policies. During the authentication server setup, a user account and password are required for the NetScreen appliance to use in order to query the policies in Active Directory. The NetScreen documentation calls for this account to be an administrator. However, hard coding an administrator account's username and password into the configuration to perform LDAP queries did not seem to be the most secure method even across LDAPS. After some testing I discovered that a simple user account could make the same queries and still provide all the functionality needed to enforce the password policies set forth in Active Directory. I notified Juniper of these findings and they confirmed that they were also able to make these same queries using a simple user account. It is not known whether or not any future Juniper documentation will be updated to reflect these new findings.

Roles

Earlier it was mentioned that two separate Sign-in Policies would be used in this solution. That would also require two roles and two authentication realms. The first role that was created was for the ability to submit a certificate request. We called this role Certificates. The only resource made available to the Certificates role was the Web Bookmark for the Certificate Services Web Enrollment site on the subordinate CA. The second role was for the Secure Meeting. The only resource available to this role was the ability to create meetings so it was given the name, Meetings. It is important to note here that there must also be a Resource Policy created for each role to access an available resource. The Resource Policy acts as the NTFS permissions for the NetScreen appliance.

Authentication Realms

As stated above, two authentication realms were created to map users to the appropriate roles when they logged in. The first realm was named Certificate_Rlm. This realm did not have any Authentication Policies configured. In other words, there were no special requirements for the user or his PC to meet. All that was needed was a username and password in Active Directory. Remember the G_Meeting_Conductors Global Group created in Active Directory? Well this is where it comes into play again. The authentication realm configuration provides the ability to map users in that group to a particular role. It can be configured for any attribute in LDAP, a certificate attribute, local group membership or a custom attribute. For this particular realm a rule was created using an LDAP attribute that stated:

> If a user has the attribute value of *CN=G_Meeting_Conductors,OU=Global,OU=Groups,DC=MyDomain,DC=com* in the *memberOf* attribute, then assign the role of *Certificate*.

So when a user logs in using this realm, he would be assigned to the Certificate role and limited to those available resources.

The second realm created we named Meeting_Rlm. We did place restrictions on this realm. Under the Certificate section of the Authentication Policy

configuration for Meeting_Rlm, the option to only allow users with client-side certificates signed by the Certificate Authority was selected. That forces the users to provide a client-side certificate issued by the CA listed in the CA section of the NetScreen configuration. *(The CA configuration will be covered in the next section.)* Then in the Role Mapping configuration the following rule was created using an LDAP attribute:

> If a user has the attribute value of *CN=G_Meeting_Conductors,OU=Global,OU=Groups,DC=MyDomain,DC=com* in the *memberOf* attribute, then assign the role of *Meeting*.

Notice how the same Active Directory group was used to assign users to two different roles. This allows us to make changes in one location instead of many.

CA Certificates

A copy of the CA's certificate was imported into the NetScreen appliance's CA Certificates section. This gives the appliance the ability to validate client-side certificates issued by our Enterprise CA. I was also able to configure it to query and upload the CA's Certificate Revocation List (CRL) on a weekly basis. The CRL is a list of certificates that have been revoked by the CA for one reason or another. Without the ability to query to the CRL, the NetScreen appliance would continue to accept the user's certificate as valid after it was revoked. There is also an option to manually update the CRL in the event of an emergency.

Sign-in Policy

The final configuration piece was the Sign-in Policy. Since the appliance has the ability to provide multiple login URLs but can only store one SSL certificate, Juniper recommends that you use a wildcard certificate. The wildcard certificate provides the ability to secure multiple websites with one certificate. The wildcard certificate can only be installed on one server. In this case, remote.mydomain.com and meetings.mydomain.com were configured on the NetScreen appliance using the same SSL certificate.

In the Sign-in Policy configuration section, a new URL was created. The meetings.mydomain.com URL was configured to us a custom Sign-in page that was designed to follow MyCompany, Inc.'s color scheme. I selected the option to allow the user the ability to select the appropriate realm they require. Next, I selected the Meeting_Rlm and Certificate_Rlm realms to be presented to users. This provided the meeting conductors the option to create a user certificate if they didn't have one or setup a Secure Meeting if they already had a certificate.

After

With all the pieces in place, the steps needed to conduct a Secure Meeting are as follows:

1. A meeting conductor goes to meetings.mydomain.com for the first time.
2. He enters his Active Directory username and password and selects the Certificate_Rlm realm and clicks the Sign In button.

3. Since he is a new user, he is prompted to change his password. Upon completion of the password change, he is automatically logged out.
4. He repeats step 2.
5. This time he is presented with a link to the certificate enrollment process.
6. He follows the steps to request and install his digital certificate and promptly logs out.
7. He is back at the meetings.mydomain.com Sign-in page. Again he enters his Active Directory username and password, but this time he selects the Meeting_Rlm realm and clicks the Sign In button.
8. A window pops up requesting the user provide a digital certificate. A list of available certificates is supplied.
9. He selects the certificate assigned to his Active Directory account and clicks the OK button.
10. His certificate is verified by the NetScreen appliance to make sure it was issued by the appropriate CA and is not on the revocation list.
11. If successful, the user is presented with only the option to schedule or join secure meetings.

This solution completely meets the criteria mandated by the project guidelines.

- The solution had to be secure.
  - By using the SSL base web site, all communication is encrypted.
- The solution required the use of two-factor authentication.
  - By forcing the meeting conductors to provide a user certificate also well as a username and password, two-factor authentication was accomplished.
- The solution had to utilize Active Directory
  - By providing an Enterprise CA and using accounts and groups created in Active Directory, this goal was accomplished.

The SANS Security Essentials course helped me better understand the PKI technology. Without the PKI implementation, this project would not have succeeded. I was able to apply the knowledge directly gained from the course into a successful and secure real world project.

References

Shinder, Thomas W., and Debra Littlejohn Shinder. Dr. Tom Shinder's ISA Server and Beyond: Real World Security Solutions for Microsoft Enterprise Networks. Rockland: Syngress Publishing, 2002.

Komar, Brian, and the Microsoft PKI Team. Microsoft Windows Server 2003 PKI and Certificate Security. Redmond: Microsoft Press, 2004.

"Overview of Remote Assistance in Windows XP" Version 2.1. 10 May 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;300546

"Description of the Remote Assistance Connection Process" Version 6.0. 13 Oct. 2003. URL: http://support.microsoft.com/kb/300692

Christman, Sheila. "Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services" Version 2.1.1. 10 Oct. 2001. URL: http://www.nsa.gov/snac/os/win2k/w2k_cert_services.pdf

Harding, Carolyn A., and deGiere, Claudette. NetScreen Instant Virtual Extranet Platform Administrative Guide, Release 4.1. Juniper Networks, Inc. 17 June 2004.

"IIS Lockdown Tool" 10 Oct. 2002. URL: http://www.microsoft.com/technet/security/tools/locktool.mspx