GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

VPN Deployment: Remote Access via Cisco PIX

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

Option 2: Case Study in Information Security

Author Dwayne Foley

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Summary....3
Before....3
Key Points in the decision process for deploying a VPN Solution:....4
Security....4
Cost....4
Support....4
Future upgrade....4
Current Hardware Environment....5
Current External Access....5
During....6
VPN Solution Decision Summary....6
Software Needed....7
Cisco PIX Configuration....7
Key Areas of PIX VPN Configuration for VPN Access....7
Xauth....8
IKE Mode....8
AAA....8
Wildcard Pre-Shared Key....8
Sample VPN configuration for the PIX:....9
RADIUS Server Setup....10
Sample Configuration....10
Cisco Client setup....11
Personal Firewall (CyberArmor)....12
Pilot Test....12
After....13
Conclusion....13
Security....13
Cost....13
Support....13
Future upgrade....14
References....15

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Summary

A company, for which the author of this paper works for, will be the subject of this case study. The company will be referred to as "XYZ". The author of this paper has been employed at company XYZ for 12 years and qualified to manage, configure and document the VPN solution in this case study.
Company XYZ operates in an office building with a self-contained data center. Company XYZ broke off in a different direction and created a Spin-off company and will be referred to in this paper as "ABC Company." Company XYZ rents space in its building and data center to Company ABC. Although the companies share space in the data center, the infrastructures are kept completely separated.

Company ABC now had requirements of it's own. For it's many home users and it's travelers working remotely, a solution for remote accessibility was required. The author of this paper was charged with providing a solution. A Virtual Private Network (VPN) solution was chosen as the best option.

This paper will cover the deployment of a VPN solution for Company ABC. This paper will show how the utilization of the current PIX firewall and a latest release of the Cisco VPN client software facilitated the process. The author will also discuss the RADIUS server that will handle the authentication and authorization issues. A personal firewall will be deployed along with the VPN client. Doing so will keep the client environment in line with the Company XYZ's VPN configuration. The decisions and choices made in this process will be further discussed in this paper.

Before

The author currently manages the network, Local Area Network (LAN), Wide Area Network (WAN) and firewalls for both companies. The experience gained from the successful implementation of a VPN solution for the Company XYZ granted this writer the knowledge to successfully identify, configure, test and deploy the solution for Company ABC as well.
Several things were considered in the decision process for deploying a VPN solution. The considerations included security, cost, support, upgrades, current hardware environment and current external access.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Key Points in the decision process for deploying a VPN Solution:

Security

Company ABC was created in March 2002. The Information Technology (IT) staff of the parent company provided support for the new company. A great amount of process and expertise was available in building a secure and productive internal infrastructure for Company ABC. In deploying the VPN solution, remote access needed to be just as secure and productive as was available in Company XYZ.

Cost

Company ABC required costs to be kept to a minimum. A PIX 515 firewall for Internet access had recently been deployed and a VPN option was purchased with the firewall license. With a VPN license on the PIX available for use, no additional licensing costs were incurred. The PIX replaced a Cisco router with firewall IOS options. Utilization of hardware and software that was currently in place was encouraged.

Support

In supporting the ABC Company, every effort was made to keep systems, policies, and procedures similar to that of XYZ Company. Keeping policies and procedures similar allowed the current knowledge base of the IT staff to be utilized.

Future upgrade

The XYZ Company currently has VPN access via a Cisco 3000 and utilizes the Cisco VPN client software. A personal firewall package was also deployed with the parent company's VPN client. The knowledge gained in deployment of the newer versions of the Cisco VPN client software, and the personal firewall software will be beneficial in the future upgrade of Company XYZ's VPN.

The afore-mentioned issues, security, cost, support, future upgrades, were considered in this decision making process. Other important factors were current hardware environment and current external access. These factors were used in formation of the VPN solution.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

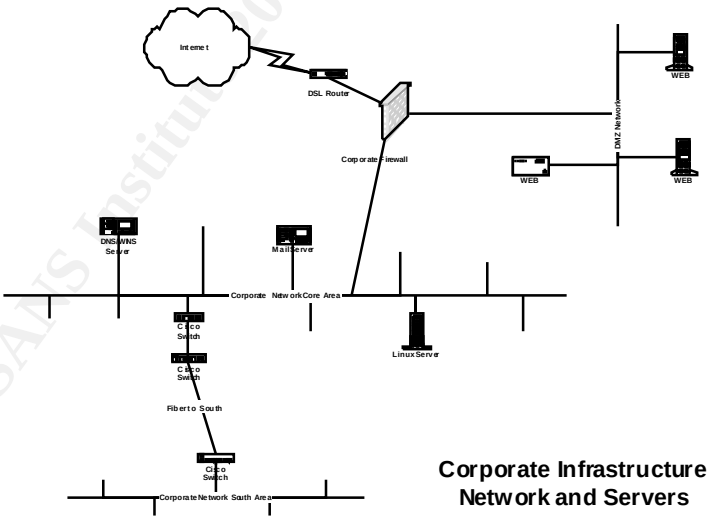
Current Hardware Environment

- PIX 515 version 6.1(4) VPN-3DES, Three Interfaces
- 256K DSL connection to Internet
- Laptops for end users running Windows 2000
- Internal Linux PC for IT support and monitoring

Current External Access

ABC Company's current external access level was limited to Web access for several systems in the DMZ. These systems were used for customer demos. The PIX filters allowed mail and DNS services inbound to the appropriate systems. All analog lines for dialing out are provided through the phone system. Analog lines were not in a Direct Inward Dial (DID) block. No inbound remote access via analog lines was possible. The VPN solution will become the only company-authorized method to access the corporate network remotely.

Current Environment Diagram:



Corporate Infrastructure Network and Servers

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Many factors were considered in designing a VPN Solution for Company ABC. The Second part of this case study describes the implementation of the VPN Solution.

During

VPN Solution Decision Summary

Company ABC's internal computing environment is used mainly for software development. Once a remote connection is established, the end-users require complete access to the computing resources. No remote access departmental restrictions were required to be put in place. A pilot group, of five software developers from different departments, was selected. The production target was for 20 to 30 remote users.

After a meeting with management from Company ABC, it was decided that the use of the parent company's remote access policy would be used as a template for the new company's policy. Written permission from the XYZ's company's management was obtained. This insured that the access policy and the IT staff support procedures, that were currently in place with parent company could be followed. This kept the theme of scaling the IT support staff's knowledge and practices in place.

The parent company had in place a Cisco 3000 Concentrator. The parent company also had an Ace server with Secure ID fobs for authentication. Due to the high costs of these servers company ABC choose not to purchase them Without a Cisco 3000 and an Ace server, another method of authentication had to put in place.

A RADIUS server offered another method of authentication. One option was to purchase a RADIUS add-on to be installed on a Windows 2000 Domain server already currently in use. Management was not willing to spend $2000 for the RADIUS add-on. Using the RADIUS add-on for Windows 2000 server would have allowed user accounts to be centralized onto one server. A Linux server was already in place for internal IT use, thus the search began for a free authentication server that would run on the Linux server. The Open Source RADIUS server from FreeRADIUS.org was chosen. The use of this RADIUS server would also be leveraged in the future. The RADIUS server could be used to centralize authentication and authorization to other routers and switches that reside on the corporate network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Software Needed

As the hardware required for the solution was in place, new pieces of software were needed. The following software was downloaded:

- Cisco VPN client 3.6.2
- Personal Firewall (CyberArmor 2.0)
- FreeRADIUS 1.103

The latest revision of the Cisco VPN client was downloaded to be use in the pilot. A version of the client software that was newer, than that of the parent company, was chosen. Use of the newer version would not affect the IT staff's ability to support the VPN solution. A 30-day trial version of the personal firewall software, CyberArmor version 2.0, was downloaded from the vendor. CyberArmor version 1.1 had been deployed with the XYZ Company's VPN solution. CyberArmor version 1.1 had been in place for several years at the parent company.

Some of the reasons behind using the new versions of the Cisco VPN client and Cyber Armor are:

- Compatibility with the PIX
- Deploy VPN client and personal firewall software with the latest bug and security fixes
- Pre-test the new versions with an upgrade to the XYZ Company's VPN solution in mind.

The current PIX firewall, needed configuration changes for VPN access and authentication.

Cisco PIX Configuration

Key Areas of PIX VPN Configuration for VPN Access

- Extend Authorization (Xauth)
- IKE Mode
- AAA authorization with RADIUS
- Wildcard Pre-Shared Key

The VPN configuration on the PIX setup is significant. The Cisco VPN client appears as if it is communicating with a Cisco 3000 concentrator. A VPN group is defined on the PIX and mimic's the group setup of a Cisco 3000. In this case only one group is needed, as we will not be restricting access to systems once the client is connected. The group name and password, defined on the PIX, are to be used on the VPN client. An address pool is defined on the PIX and assigned to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the group. The clients use this pool after they are authenticated. Routes are also set up for the addresses in the pool, as well as NAT (Network Address Translation). An ACL (Access-List) rule is set up, so that the clients using the internal address assigned from the address pool will be allowed to route.

Xauth

Extended Authentication on the PIX is used to deploy IPSEC with authentication using a RADIUS server. When a VPN client connects to the PIX, the username and password, are sent to the RADIUS sever over port 1812 (default port). The PIX configuration is authorized to send the request to the RADIUS server. The username and password are then the passed to the RADIUS server for authentication and the response is sent back to the PIX.

IKE Mode

Configuring Internet Key Exchange (IKE) allows the client to download the IP address from the address pool and additional networking info, such as WINS and DNS. The downloaded address is the encapsulated the IP address, used in the IPSEC (Internet Protocol Exchange) rules that are defined on the PIX.

AAA

Cisco's AAA (authorization-authentication-accounting) is configured to use the RADIUS server for authentication. The RADIUS server is installed on the inside interface of the PIX. The type of authentication server is defined as RADIUS, "aaa-server radius protocol radius." The server protocol is defined as RADIUS "aaa-server local protocol radius." The port to communicate with the RADIUS server is defined as "aaa-server radius-authport 1812." The RADIUS server's address is defined as "aaa-server partnerauth (inside) host xxx.xxx.xxx.xxx XXXXXX timeout 5." The RADIUS server is set up as an authorization partner with the PIX to allow the requests to be processed.

Wildcard Pre-Shared Key

Wildcard Pre-Shared Key is defined to allow all IP numbers, (Broadband users) to access the VPN using the same pre-share key. The Pre-share key is a shared secret key that is sent from the client. In this case, it is the encrypted group password, which is distributed with the Cisco VPN client. The pre-shared key configured, is used to set up IKE security associations (SA) with the PIX.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sample VPN configuration for the PIX:

```
aaa-server
aaa-server radius-authport 1812
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol tacacs+
aaa-server local protocol radius
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host xxx.xxx.xxx.xxx XXXXXX timeout 5

crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 30 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address respond
crypto map mymap client authentication partnerauth
crypto map mymap interface outside

isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

vpngroup vpnxxx address-pool vpnusers
vpngroup vpnxxx dns-server xxx.xxx.xxx.xxx
vpngroup vpnxxx wins-server xxx.xxx.xxx.xxx
vpngroup vpnxxx default-domain XXX.com
vpngroup vpnxxx idle-time 1800
vpngroup vpnxxx password ********

access-list 101 permit ip xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.0
255.255.255.0
ip local pool vpnusers xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx
global (outside) 1 interface
nat (inside) 0 access-list 101
nat (inside) 1 xxx.xxx.xxx.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx 1
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:00:00 absolute uauth 2:00:00 inactivity
sysopt connection permit-ipsec
no sysopt route dnat
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

RADIUS Server Setup

The RADIUS software server was downloaded from FreeRADIUS.org. The software was compiled and installed on a Linux server that is currently used to provide backend IT services. The RADIUS server may be used to authenticate access to other devices in the future.

The FreeRADIUS server has several options that allow different types of authentication repositories to be configured, such as, PAM, UNIX style, Chap, eap, and PAP. The authorization method set up on the Linux server is Unix style. In the future, a more robust method may be configured. The configuration was fairly minimal. Configuration consisted of, editing a few lines in the radius.conf and users files, and starting a daemon. Basically, a group for the radius users was set up and the users were added to the password file. Remote user accounts were added to the radius group. User accounts are set up with /bin/false shell so they cannot login to the server directly. The Linux server was hardened, following standard security principals.

Logs are saved, zipped, and archived. The RADIUS server daemon (radiusd) starts on server boot through an init script. An additional process is also started, that will monitor and restart the daemon if it stops (radiuswatch).

Sample Configuration

Portion of the users file:

```
#
# First setup all accounts to be checked against the UNIX /etc/passwd.
# (Unless a password was already given earlier in this file).
#
DEFAULT Group == "radius",Auth-Type:= System
#DEFAULT        Auth-Type:= System
                Fall-Through = yes
```

Portions of the radius.conf file:

```
# Unix /etc/passwd style authentication
 unix {
    #
    #  Cache /etc/passwd, /etc/shadow, and /etc/group
    #
    #  The default is to cache them.
    #
    #  For FreeBSD, you do NOT want to enable the cache,
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
#  as it's password lookups are done via a database.
#
# allowed values: {no, yes}
#cache = yes
usegroup = yes
# Reload the cache every 600 seconds (10mins). 0 to disable.
#cache_reload = 600
#
#  Define the locations of the normal passwd, shadow, and
#  group files.
#
#  'shadow' is commented out by default, because not all
#  systems have shadow passwords.
#
#  To force the module to use the system password functions,
#  instead of reading the files, comment out the 'passwd'
#  and 'shadow' configuration entries.  This is required
#  for some systems, like FreeBSD.
#
passwd = /etc/passwd
shadow = /etc/shadow
group = /etc/group
```

Cisco Client setup

The IT staff will perform all installs of the Cisco VPN client software and personal firewalls. The company policy states that only company owned computers are allowed to access the corporate network. The install media will not be distributed.

A profile file is set up on the Cisco VPN client. In this file, several parameters are defined. First is the name of the connection (ie: Company ABC), next being the group name. The group name is the same as the VPN group on the PIX. The password is equivalent to the Preshare-Key which is defined on the PIX. The IP number of the gateway is also stored in the profile configuration file. In this case, the external address of the PIX is the gateway. This file is saved with a .pcf extension, and the password is encrypted. The file is distributed with the software when installed.

An option to have the Cisco client launch, before a user logs in to the laptop, is available. Enable Start Before Login, allows the user to establish a connection to the VPN before the ctl-atl-del screen. When the user logs in to the laptop, and authenticates to the NT domain, the user's login script is executed. This will allow the mapping drives, updating of virus patterns, and provide a more robust

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

audit trail. This option has been configured and is the preferred connection method. A user could choose to connect to the VPN after logging into the laptop.

Personal Firewall (CyberArmor)

CyberArmor is the personal firewall that both companies have standardized on. CyberArmor comes with a program called a "policy editor." This is used to define a set of the rules that will determine which filters get applied to different connection types. The personal firewall has the ability to apply different rules depending on the network you are connected to.

The CyberArmor configuration has three connections to detect. One is connected to the corporate network (in the office), the second is connected to the VPN, and all others, the Internet. The software detects which network you are connected to and applies the appropriate filter. Basically, the personal firewall performs three functions. It gets out of the user's way when in the office, protects the user when connected via broadband, and then protects the user while allowing encrypted access over the VPN tunnel.

The software is password protected, so end users cannot turn it off. It uses a registry key, that Cisco sets, to determine that the VPN is active. The software can be rolled out with an internal log server to capture individual logs and aggregate data. The high cost prohibited the deployment of this added functionality at this time.

Pilot Test

The pilot had five end users and lasted 25 days. The pilot was deployed with split tunneling turned on. Knowledge gained from the pilot included:

- Timeout was extend to 2 hours of inactivity
- CyberArmor prompts you about running certain programs but soon learns and stops prompted the end user.
- Speed over Cable and DSL is acceptable.
- How to use tunnel IP for certain applications (Xwindows, etc.)
- CyberArmor does block and alarm end users of probing activity

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After

Conclusion

Thirty end user licenses were obtained for the CyberArmor software. The Cisco client right-to-use was unlimited with the VPN-3DES license key on the PIX firewall. After consulting with management about the dangers of split tunneling, it was disabled for production. The IT staff installed each user's VPN client software and personal firewall software.

Each end user received, read, and signed a remote use access policy. At the time of install, all home broadband users were educated and encouraged to install a cable modem router/firewall-type device to protect the company's laptops and user's own home computers.

With spilt-tunnel disabled, a proxy server may be installed in the future to allow Internet access for VPN users while connected.

Factors at the start of the process included, security, cost, ongoing support, and future upgrades for parent company. To what extent were these objectives met?

Security

The VPN solution uses 3Des encryption and the group password is restricted and encrypted. The Pix was configured to use a RADIUS server for authentication and the Linux server was hardened. Access logs are saved and archived. A personal firewall on each client protects the company's assets.

Cost

The VPN solution was deployed using existing hardware (PIX 515). The Cisco VPN client software right to use comes with the PIX license. The FreeRADIUS server, which was installed on an existing Linux server, is Open Source. The only costs incurred were for the 30-user CyberArmor licenses and Labor.

Support

From Company ABC end user's perspective, the VPN client works the same as that of the parent company. More than half of the new users were familiar with the Cisco VPN client. The IT staff can easily support the new VPN users, as their method of access is very similar to that of the parent company's solution.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Future upgrade

Testing was completed on the new release of the Cisco VPN client on configurations that are very similar to that of the parent company's client setup. Testing and configuration of a new version of CyberArmor Policy editor and new filter rules will make upgrading the parent company's VPN solution easier and should shorten the pilot length of that project.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Cisco Systems Inc. “Configuring VPN Client Remote Access” Chapter 6
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b5.html (February 10, 2003)

Cisco Systems Inc. “Configuring PIX to PIX and VPN Client 3.X”
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b5.html (February 10, 2003)

FreeRADIUS.org “Cisco IOS and RADIUS”
http://www.freeradius.org/radiusd/doc/cisco (February 10, 2003)

FreeRADIUS.org “FreeRADIUS Frequently Asked Questions & Answers”
FAQ.freeradius,v 1.10 2002/05/10 15:54:11)
http://www.freeradius.org/faq/ (February 10, 2003)

Inforexpress Inc. (CyberArmor data sheet)
http://www.infoexpress.com/current/doc/ca-data.pdf (February 10, 2003)

Jonathan Hassell “RADIUS Securing Public Access to Private Resources”
(Chapter 5 Getting Started with FreeRADIUS) OReily October 2002
http://www.oreilly.com/catalog/radius/chapter/ch05.html (February 10, 2003)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.