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

Jeremy Covey
GSEC practical
Assignment V 1.2f

Securing Your VPN

How to address key security concerns in deploying VPN's

Virtual Private Networks are emerging as a viable cost-effective answer for companies wishing to connect employees, remote locations and other businesses to their existing information assets. With the tragic events of September 11th fresh in our nation's mind many organizations are in a rush to set up a VPN system that will allow many of their employees to telecommute to the workplace or travel less to other branch locations. With minimal amount of capital, companies can create a secure connection to their employee's home, a remote office or another business by tunneling through the Internet infrastructure. There are many different kinds of VPN implementations such as, an extranet VPN (an external party to your company's intranet), intranet VPN (multiple company sites interconnected via the Internet), and remote access VPN (dial-up or broadband user using VPN to access corporate intranet). The cost and return on investment make it a very appealing option to management, but what about it's functionality?

In this paper I will discuss the basic components that make up a VPN system and how each component plays a role in providing connection to an existing network. Special emphasis will be placed on how to secure each component of the VPN system to ensure safe data communication form one location to another. Although there are many solutions for deploying VPN's, I have chosen to look at remote access IPSec VPN products that aid in aggregating the complicated process of securing a VPN, in an effort to clearly depict the basic underlying concepts.

COMPONENTS

Let's begin by identifying the key components in a secure VPN environment. It should be first noted that the majority of the hardware and services that I will discuss can usually be run on existing infrastructure, although new equipment is often implemented for security or other reasons. The following is list of common components found in VPN systems:

- Servers
- Client machines
- Routers
- Filtering devices, such as firewalls or viruswalls
- Key management agents

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Public key infrastructure
- Encryption
- Digital certificates

The following is a sample diagram that illustrates how components fit into the VPN system as a whole:

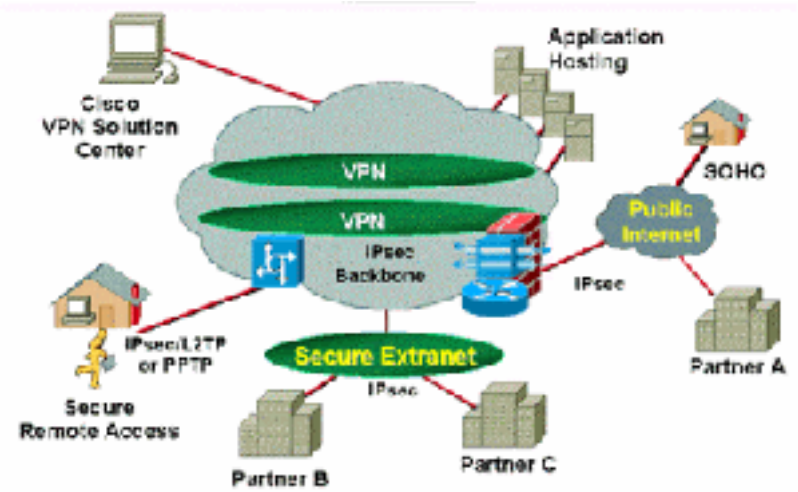


Figure 1-A [1]

As I have stated already, there are many ways to set up VPN and it really depends on the need of the organization. However there are three main components to a VPN system that are essential to security and ultimately the functionality of a system. These three security components, which will be the main focus of the paper, are host systems, tunneling methods and company-side systems. All three of these areas are very broad topics that need to be further discussed in order to get a good sense of their role in a VPN.

HOSTS

Host systems can be a multitude of different systems ranging from an employee's home pc to sever in a remote office location. Host systems are as much a critical part of security to a VPN as the encryption method used to protect the data traveling on the net. One must remember that a system is only a strong as its weakest link and there are many considerations that must be scrutinized when configuring host systems with regards to the VPN connection. The IT staff will play an integral role in creating a secure host computer by implementing key security software hardware components to that system. Key components, such as: firewalls, antivirus software, IDS (intrusion detection systems) software and remote manageability software. Administrators need to have the ability to watch this computer at all times. This will ensure that the system is configured properly and cannot be comprised by any unauthorized people. This can be achieved with VPN client software such as Checkpoint's VPN-1 Secureclient. Secureclient has mechanism built in that, upon authentication, will automatically connect to a companies VPN security policy server and check the configuration to ensure that it is in line with the company's security objectives. This way you can configure firewall, antivirus and other software settings of

[1] Coutesy of How stuff Works inc. URL: http://www.howstuffworks.com/gif/vpn-diagram2.gif

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

many remote machines via a checkpoint VPN-1 gateway and policy server residing at the office. If the security conditions are not met, the sever will not allow the connection to be established and then log the refusal for the administrators to review. In addition to these features, it might also be a good idea to install some other types of host-based IDS that will be accessible and configurable from the company office. This added feature will allow the administrators to analyze traffic patterns and detect any possible intrusion attempts.

In addition to employing security features on the host computer it also may be necessary to install a hardware solution to the network the host is connected to. With most VPN remote hosts physical connections' today being broadband this is a must. The solution would most likely entail a router, firewall, or a combination of the two. For most SOHO (small office/home office) a properly configured router/switch will suffice. Proper configuration will entail crafting the access control list to drop all traffic except to the ports that are needed by the VPN and other essential services for your system. This will provide yet another hurdle for potential hackers. The major thing to remember when configuring on the host side is that you VPN can only be as secure as the host that are connected to it.

What I have discusses in the previous paragraph is somewhat geared towards remote access VPN set up. The scenario is going to be a bit different if you are implementing and intranet or extranet VPN. One will still need the proper perimeter defenses such as firewalls, viruswalls, and routers with the appropriate ACL (Access Control List) configuration. The major differences are how you will tie the VPN hardware into the existing LAN and what software you are going to use on a server as opposed to client machine. For this am going to refer you to the section a bit later in my paper that is labeled "company-side systems"

Once the host is set up properly and tested enough to be given the seal of approval by IT it's time to discuss how the data will be transmitted over the Internet infrastructure. This has always been looked upon as the most important aspect of the VPN because it's responsible for the tunneling of data across the Internet. There are some fundamental concepts in this area that need to be discussed.

AUTHENTICATION

Authentication is the first thing that needs to be completed before any connection can be made. ISAKMP is the method by which security associations (SA) are formed and the process is independent of the manner in which any keys are passed. The Internet Key Exchange (IKE) defines the manner in which keys are passed. A security association (SA) is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. Secure remote VPN authentications, in the most secure form, are conducted by using X.509 digital certificates under IPSec Internet Key Exchange (IKE) specification. Collectively Digital certificates and other key management services are called a PKI (public Key Infrastructure). Encryption is also added to the mix during authentication as well as the rest of the communications there after to uphold their trust created through cryptic key exchanges. There are a couple different encryption algorithms that can use, with the most secure being triple DES and Rijndael AES. Algorithms will be responsible for encrypting data that will be "tunneled" through the Internet infrastructure. Now it is important to understand that this is merely one method of conducting authentication. There are also many other considerations to take into account when choosing you method of authentication.

One of the biggest problems accrued from changing from traditional password authentication methods to secure ID's, such as digital certificates is user acceptance. Change is a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

difficult thing, especially in an enterprise environment and users may have problems with the role over to new authentication methods. You had better plan on spending a little money on educating your employees so that security methods do not compromise productivity. There are other options available but they do not fall into the scope of this paper. To get a better feel for the various methods I suggest going to Network Fusion magazines website. They have a great little section on VPN's located at http://www.nwfusion.com/research/vpn.html . I would also recommend looking at the SANS Institute reading room located at http://www.sans.org/infosecFAQ/.

There are volumes of material to be read about authentication and encryption and although it is important I will argue that there are greater risks waiting at the ends of the tunnel then in the middle. With host security issues already covered at the one end, it is time to take a look at what is being done on the company side.

COMPANY-SIDE SYSTEMS

The correct configuration of the company side VPN components is essential for protecting valuable company data that resides on your network. There has to be a barrier between you network and where the tunnel ends. Most companies (depending on the size) connection to the net will have some sort of firewall and or viruswall followed by routers. The barrier, also known as a DMZ(de-militarized Zone) is in between the routers and the rest of the network backbone and will house the VPN equipment such as gateways and servers. VPN gateways are little more then encrypted routers that can aid in some of the authentication and encryption services. There are quite a few products on the market these days that aggregate many of the services in to one piece of equipment to ease management. Again, Checkpoint is a company that provides such a software product to take care of these various services. Their VPN-1 SecureServer is an integrated VPN/firewall application for servers that adds VPN capabilities to secure confidential client-server communications. Now I must emphasis again that there are many ways to configure you VPN components with regards to it's connection to your network and different businesses have different needs. It is, however, extremely important to separate you VPN traffic from you network traffic. Jim Metzler, founder of Ashton, Metzler and associates speaks from real world experience, "Data can be greatly compromised if an IP tunnel dumps off into an insecure part of another company's network, he says. For instance, if you connect to a partner that passes your traffic straight through to its network without holding the traffic in a "demilitarized zone," then your information could be in jeopardy."

His comments bring up another interesting point that should be discussed. If you plan to establish a Extranet VPN connecting your company to another network, will you know where your VPN traffic will end up on their network? I am willing to wager money that not many administrators of VPN's could answer that question in any depth. It is in your best interest to do some homework when planning a B2B (business to business) Extranet VPN. Many companies are taking up a step further and requiring an audit of the other companies network to ensure their potentially sensitive data is safe. I suggest creating a document outlining key security practices and have both groups sign off on it. One can never forget the legality involved in sharing important and sensitive business ideas or products with other companies. For a business, new products and ideas are future sources of revenue and need to be protected as such.

With that being said, I would like to offer my opinion on how to set up the perimeter security for you VPN. My best practice would entail having a router filtering all VPN traffic leading to a VPN gateway located in the DMZ. The rest of the incoming and outgoing traffic

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

would pass through the router and be carried to the companies network backbone. As for the VPN traffic, it will go through the VPN gateway and head to a server running the VPN server software responsible for delivering the appropriate services to remote users. It should be noted that there might be more than one server running the VPN software in the DMZ. It really depends on the size an scope of the organization. There may be an extra server or servers solely running security policy server software for remote users. For my example solution, the system should have two NIC's, (Network Interface Cards) one taking in traffic from the VPN gateway and the other sending data to a router protecting the edge of your network infrastructure. Again this is merely one option, but it should provide an understanding as to how to lock down and differentiate you VPN from the rest of you network. This solution provides a good home for the end of you VPN tunnel without any direct contact to the rest of your LAN (Local Area Network).

CONCLUSION

In closing I would like to reiterate that VPN's are much like chains, they are only as strong as their weakest link. Much focus has been placed on ensuring encrypted tunneled VPN data cannot be obtained over the Internet infrastructure. It is essential not to over look the role that host and server-side systems play with regards to VPN security. Whether it is an Intranet, Extranet, or Remote access VPN, information managers need understand the basic steps to keep their VPN, as well as LAN's safe. Many IT professionals fail to research these critical methodologies and thus run the risk of security breaches of their entire network. VPN systems are currently in a state of evolution, changing almost daily. A good implementation will entail standardized yet customizable components that satisfy you business needs. There are many products out there now that can ease deployment and manageability of both VPN client and server configurations, which can ease the burden of deploying such a network at the enterprise level. The key is doing your homework about what your VPN is connected to and making sure proper documents regarding VPN security policy is in place. This will ensure everyone is operating a secure manner.

Lastly, as with anything you plan to implement test, test and test again before implementation into the production environment. Putting VPN into a production environment without any form of testing is not only poor practice, but also a potentially open door for possible intruders. Imagine having to explain to you B2B (Business to Business) partner that some of their business ideas have been accessed by others outside your company. Not exactly the situation any company would want to be in, not to mention the potential loss of revenue that could occur.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

BIBLOGRAPHY

Check Point Software technologies Ltd. " VPN-1/ Firewall-1 secure server URL: http://www.checkpoint.com/products/security/whitepapers/firewall-1_integrated.pdf (11/4/01)

Check Point Software technologies Ltd. " VPN-1 gateway URL: http://www.checkpoint.com/products/security/datasheets/vpn-1_gateway_datasheet.pdf (11/13/01)

Ciolek Gregory J "Virtual Private Network (VPN) Security" SANS Institute information security reading room January 4, 2001 URL: http://www.sans.org/infosecFAQ/encryption/VPN_sec.htm (11/5/01)

Cisco Systems. " Remote Access VPN Design" URL: http://www.cisco.com/warp/public/779/largeent/design/remote_vpn.html (10/29/01)

Harkins, Dan "CRACK: The new VPN authenticator" Network World, 05/28/01 URL: http://www.nwfusion.com/news/tech/2001/0528tech.html (11/4/01)

Gittlen, Sandra "VPN security requirements debated" Network World, 09/17/01 URL: http://www.nwfusion.com/columnists/2001/0917gittlen.html (11/2/01)

SANS Institute Information security reading room URL: http://www.sans.org/infosecFAQ/encryption/encryption_list.htm (11/5/01)

RFC 2408 URL: http://www.faqs.org/rfcs/ (10/15/01)

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.