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

Symantec Enterprise VPN Solution: Extending our Network through the Internet

Robin Duffy

GSEC v1.4b (August 2002) OptionA

04/14/03

Abstract

This paper will discuss an organizations attempt to secure their network and extend resources by way of the Internet utilizing a Symantec Enterprise Firewall and Symantec Enterprise VPN Server for NT v6.5. Our goal with this project was to give Internet access to all regions, provide security to the networks, and provide access to a database kept at a central site.

A vpn solution over the public Internet was a cost effective way to provide this statewide organization with a way to collect and store client-tracking data at a central site, provide all locations with access to valuable resources on the Internet, as well as communication via email. In the initial stages of this project we were faced with questions concerning the security of our data and our networks connected to the Internet. Why should we care about security over the Internet? At what point do we consider our networks secure? And how much shall we spend on securing our systems?

We care about security because we are expected to maintain privacy for our clients and because we value our resources. By defining our threat we can determine our level of security. Our perceived threat is private information exposed on the public Internet. How much we spend will depend on management's determination of the risk they are willing to accept. Management is willing to accept that the Internet may be inaccessible from time-to-time and that we are dependent on the ISP vendor for service.

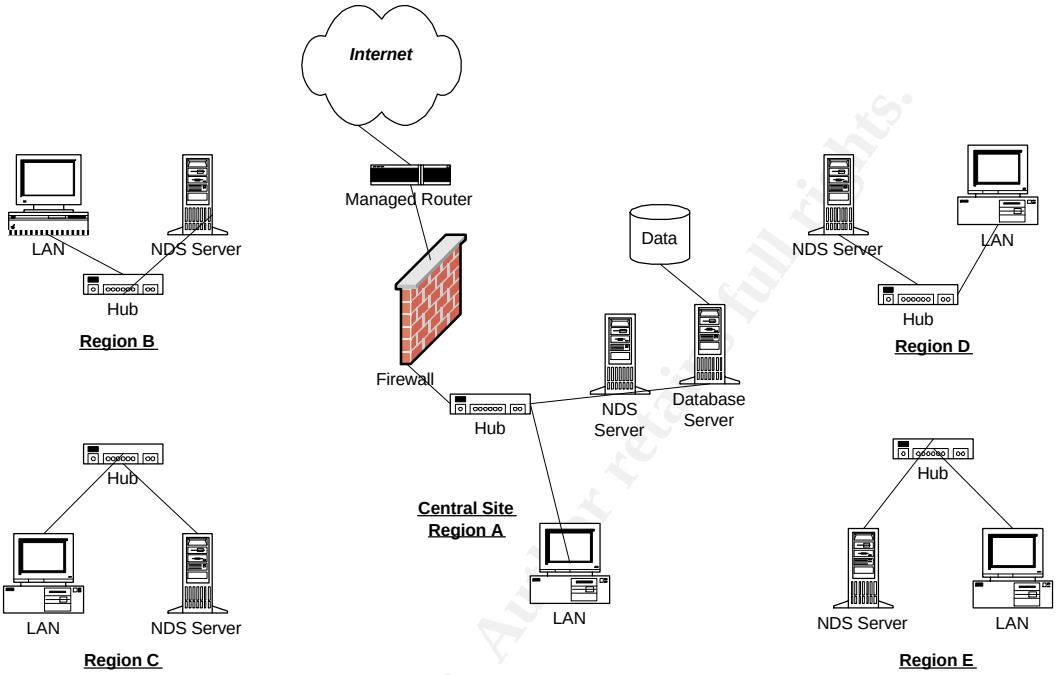
This paper assumes the reader has a base knowledge of TCP/IP, routing, as well as the concept of a Virtual Private Network.

The Network before the project

This is a statewide organization with 5 regions. The 4 remote locations each had their own Novell file and print server and only a few dial up accounts to the Internet. Access to these remote regions was through dial up over a Shiva/Lanrover/E device. Dial up rights to the regional LAN was through membership in a group in NDS. The Central Site had a fractional T1 connection to the Internet through a major ISP, a Symantec Raptor Firewall NT v6.0, one NT4 PDC (Primary Domain Controller) and a BDC (Backup Domain Controller), an application server, database server, and NT4 Terminal Server with Citrix MetaFrame1.8 that provided the central WAN with access to the database over Frame Relay. This Central Site was also equipped with a Shiva/Lanrover/E that

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

also provided some access to the regions to the database for a select few users. This solution did not provide adequate access to the number of users needing access to this database.



Project Outline

- Write a Site Security Policy & Plan. Get management approval on policy.
- Investigate software, hardware, and connectivity issues necessary for vpn solution.
- Acquire equipment and contracts with ISP to provide connections to the Internet.
- Install firewall/vpn servers. Initiate vpn tunnels to central location that will house the database server and hide the IP addressing of the network.
- Create rules to pass traffic and test vpn access.
- Backup Procedures for Disaster Recovery.
- Monitor firewall logs and enable audit features on servers.

Security Policy

Symantec's Installation Guide states that "*before configuring your security gateway, it is important to understand exactly what network resources and services you want to protect.*"[1] They go on to further stress the importance of support from top management and anyone responsible for administering the site.

[1] SEF/SEVPN v6.5 Installation Guide (p.2-1)

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

Without the support of top management, the policy carries little weight. The use of the vpn solution would initially be used for passing information to the database at the Central Site, so the Site Security Policy was written based on this planned usage of the vpn solution. The organization currently had no such policy concerning the Internet or company network resources. The SANS Institute provides access to templates on different information security policies. The development team researched these policies and did an audit of files to make sure there was no existing policy. A policy is described as the document that will list our specific requirements and rules that will be enforced. SANS strongly recommends standards and guidelines to help make your policy more effective by outlining what is best practice or what is "standard" for your organization.[2] In this instance, an "acceptable use" policy was all that management requested. This policy would define the acceptable use of equipment and services provided to our users. It included usage of email, equipment, and use of the Internet. The policy was presented to top management and administrators for approval. Upon approval the Site Security Policy was included in the Employee Handbook.

Choosing the product and connectivity

We contracted with an ISP for Internet connections at sites where it did not exist. Vendors were considered based on their regional availability, as well as their support, and reliability. Several ISP's were going through bankruptcy at the time and so careful consideration was given to this choice. Cost was at issue as well as service, technical support, and whether or not that company would even be there in a year. Because of the limits of staffing and resources at our own organization, a vendor that would configure and manage the Internet routers was chosen. The ISP's policy provided that a circuit would be installed in 45 to 60 days, so the circuits were ordered for all regions before hardware or software for the vpn solution.

During the next phase of the project, an inventory was taken of equipment already possessed by the organization. Software and licensing issues were addressed. It is important to have the requirements of your solution defined prior to looking at product.[3] The firewall/vpn solution would need to be easily deployed. It would allow us to add additional vpn site-to-site tunnels, it would provide us with auditing features, remote management of regional firewalls, and would secure our resources at the application level. We would also need the ability for a few select users to vpn over mobile tunnels. A proxy that could hide the topology of our internal network was highly desired. The flexibility and speed of packet filters (or circuit gateways) verses the security of application gateways (proxy servers) were discussed and researched by the development team. Each of these types of firewalls has their disadvantages as well. Packet filtering can not stop worms such as Code Red or Nimda and application gateways tend to be

[2] SANS Institute, The Sans Institute Security Policy Project
[3] Taylor, Laura, "Firewall Shopping 101"

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

inflexible. A hybrid firewall with vpn capabilities was desired.[4] The team did an audit of users that would need access to the database, peak usage times, and the number of users accessing the Internet was addressed.

The organization already has an Axent (Axent was acquired by Symantec) Raptor Firewall NT v6.0. *Requirements as listed by Symantec's Installation Guide: ([1]SEF Installation Guide p.3-4) a minimum of two Network Interface Cards; Intel Pentium II, 233 MHX or better; sites with less than 200 users require at least 128 MB RAM and a 200-300 MB paging file, and 2GB disk with at least 200 MB free disk space; sites with more than 200 users require at least 256 MB RAM with 250-500 MB paging file and 4 GB disk with at least 2 GB free disk space.* This organization had two NT servers that could be utilized at the sites with only 25-50 users. Symantec Enterprise Firewall (SEF) provides inspection of packets at the application level as well as proxy services. This product is described as a hybrid firewall. The product provides remote management, logging capabilities, and ease of use through GUI interfaces. The currently installed version v6.0 had Power VPN capabilities but the organization was not licensed for that option. Cost issues also played a role in the decision process. Symantec's cost was estimated at $99.95 per user at the 100 user level in a "Buyer's Guide" published by Network World in October 2002.[5] This cost was middle of the road, but Symantec offered all that we wanted in a hybrid firewall. We would have to upgrade the existing firewall at the Central Site, two existing servers that would fit the requirements for sites with less than 200 users that could be utilized as firewall/vpn servers for regional sites; we would then have two more NT servers to be purchased.

Installation

You can install Symantec Enterprise Firewall (SEF) or Symantec Enterprise VPN Server (SEVPN) on Win2K Pro, Win2K Server, or WinNT. Before you install the firewall/vpn software you should take the following steps: ([1] SEF Installation Guide p.3-6, 3-7)

- Format the drive as NTFS. After the drive is formatted as NTFS, use the volume ID to acquire the licensing from the Symantec Support Site.
- Make sure your O/S is patched to the latest service pack supported by the software.
- Install the TCP/IP protocol ONLY. Address the inside and outside Network Interface Cards. Only the outside interface will have a default gateway.
- Add permanent routes to your inside networks on the routing table.
- Do NOT enter any DNS.
- Set the computer's Windows NT name to match its TCP/IP name.
- Use the pre-install checklists provided by the vendor.

[4] Smith, Rick, "Hybrid firewalls can dig up worms"
[5] Network World, "Buyer's Guide: VPN's, The Bottom line on per-user pricing"

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

We have found that it is helpful in troubleshooting if your NIC's are different vendors. Check the Symantec Knowledgebase for supported network adapters. SEF does not perform as a router. If you need routing functions for your inside clients, point them to an internal router and add the firewall as the default gateway on that router. Install the SEF and SEVPN, as well as the Symantec Raptor Management Console. The media in the United States is available as 3DES or DES. If you install 3DES, all of the Symantec Raptor Management Consoles (SRMCs) used to manage the security gateway must also be 3DES. 3DES was the install chosen by this organization. Install the SEF and SEVPN server, as well as the Symantec Raptor Management Console. Once the install is complete, you will select the 'Raptor Firewall Setup' icon on the desktop, you will indicate which network adapter is the inside interface and which is the outside interface. You will also create the local management password at this time. A reboot of the system is required at this point. The system then goes through a lockdown of services that are not needed for the firewall. Run 'rempass' from the command prompt to create the password for the remote firewalls you will manage. Rempass is the host, password, service, and port configuration tool. You are presented with a menu and will select (a) to add a new host, enter the IP address of the host, and then select the service to add. In this case select (1) for Firewall Management Console. You are now asked to enter the password or pass phrase and then confirm it. It is also important to note that there is software that should never be installed on a firewall. [6] Any software that that would allow remote access to a firewall could degrade the security of your firewall. The following is a list of software you should NOT install to a firewall:

- Any software package that permits a user to view a remote desktop.
- Backup agent software.
- UPS software.
- Web server software.
- Antivirus software.

You should also know what ports some software will open on the firewall. The software does not have to be designed for remote access to open dangerous ports and start services which can create a hole for an attacker to take advantage and gain control of the system. You should carefully consider what is installed to the firewall. Installing any additional software could leave your firewall open to an exploit or attack. Attackers could compromise the entire network once they have control of the firewall or change the way the firewall passes traffic. Firewalls should be in a locked room with a locked screen saver as well.

Virtual Private Networks

[6] Symantec Knowledgebase: Software that should not be loaded on the SEF/SEVPN

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

The main security feature of a vpn tunnel is that the ends are trusted systems. They are connected by an encrypted and authenticated path. Symantec's solution provided the option for IPsec IKE tunnels. IPsec stands for IP security. It is a set of protocols (standards) designed by the IETF (Internet Engineering Task Force) to secure communications over both public and private networks. IPsec operates at layer 3(Network Layer) of the OSI reference model.[7] It provides the security in the site-to-site vpn tunnels we will create. Only the gateways need to be aware of the IPsec settings. IKE stands for Internet Key Exchange. IKE is defined as a hybrid protocol for exchanging SA's (security associations). A security association (SA) is the shared policy of key(s) used to protect information.[8]

Open the SRMC and select 'Connect to localhost'. You will begin to configure the firewall by setting a global IKE policy that is the same on all gateways. Open the folder called 'Virtual Private Networks'. Under 'Virtual Private Networks' are the 'Secure Tunnels', 'VPN Policies', and the 'IKE Policy'. You can edit the global IKE policy here. On the SEF/SEVPN server, the global IKE policy works in conjunction with the IPSec/IKE vpn policy, functioning as phase 1 negotiations for the secure tunnel. The IKE policy (vpn policy) configured and selected for the 'Secure Tunnels' functions as Phase 2. In short, phase 1 will set up the secure channel in which to do the phase 2 setup. Phase 2 is the set up of the tunnels. The keys exchanged in phase 2 will determine how the data will be encrypted and then decrypted between the two end points. What you really need to know is that both peers must be configured with the same global IKE policy for phase 1 and that the vpn tunnels are using the same IKE policy for phase 2. The 'VPN Policy' section contains pre-configured policies that you may edit to suit your needs. We would select to pass the traffic through the 'Secure Tunnels' to the Proxy Services and the IKE feature would be utilized with pre-shared keys to authenticate the peer. The defaults were left in regards to 'Tunnel Mode' and ESP. 'Tunnel Mode' encrypts the header and the payload. ESP stands for 'Encapsulated Security Payloads'.[9] ESP is a protocol within IPsec that provides confidentiality and integrity to an IP datagram. And PFS, which stands for 'Perfect Forward Secrecy' and requires that you specify the Diffe-Hellman Group1 or Group 2. PFS adds additional security with the shared secret value. We configured our policy as follows: 'Data Integrity Preferences' (authentication) MD5, and 'Data Privacy Preference' (encryption/decryption at end points) 3DES. 'PFS' was selected and the Diffe-Hellman Preference used was Group 1 which is 768 bits long. Group 2 uses more CPU power at 1024 bits. The settings of data, tunnel lifetime and inactivity timeouts were all left at the defaults. Again, it is important to note that your tunnels must be configured exactly the same on each peer.

[7] Webopedia, IPsec
[8] RFC2409, The Internet Key Exchange, Request for Comments 2409
[9] RFC1827, IP Encapsulating Security Payload (ESP), Request for Comments

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

Before we create our 'Secure Tunnels', we must first address the other components needed for the tunnels. Under 'Base Components' you will find 'DNS', 'Network Interfaces', 'Network Entities', 'User Groups', 'Users', 'Authentication', 'Times', 'Protocols',' Raptor Services', and 'Filters'. The 'Network Interfaces' contained the inside and outside interface of the firewall. We started with the 'Security Gateway' under 'Network Entities'. We entered the name, the IP address (outside of firewall), selected to enable IKE, and entered a shared secret. This was done for the local gateway and all remote end points. 'Network Entities' can be individual hosts such as mail servers, subnets, mobile users, or groups. These entities are used to pass traffic through the firewall and the vpn tunnels. We also configured the trusted networks and a host for the firewall (outside interface).

We have deemed our regional networks as trusted and will use the networks as remote entities, the Central Site Firewall as the local entity when configuring the Central Site tunnels. The regional SEF/SEVPN will use the same settings for their tunnels, however the local trusted network is the local entity and the Central Site Firewall is the remote entity. Your tunnels must be the same on each side or they will not function. We chose to pass traffic to the 'Proxy Services' so rules are applied to traffic through the tunnel. The entities configured are also used when we configured rules under the 'Access Controls' folder. You may also configure individual users to gain access to the network through the 'Users' section as well as 'Groups' such as Raptor Mobile Users. The 'Times' folder can be edited and applied to rules to restrict access in to or out of the protected network based on time. Traffic passing through the tunnels to the Central Site would pass through the Proxy services. And services flowing out to the regional sites would do the same. This would require a GSP (Generic Service Passer) service for the traffic that would enter the tunnels. The GSPD (Generic Service Passer Daemon) is listed under 'Proxy Services' in the 'Access Controls' folder and will need to be enabled to use this service. From our pre-install checklist we are aware of the protocols that would need to be configured through the GSP service. Protocols that did not pre-exist on the firewall would be added in the 'Protocols' folder under 'Base Components'. 'Service Redirection' is also necessary at the Central Site for servers that would be accessed via the vpn tunnels. Requests at the 'Security Gateway' for the application would be passed to the Citrix Server if it meets the criteria of the rules configured. Rules are configured under the 'Access Controls' folder. Rules for browsing the Internet and email going out and coming in to the mail server were configured, as well as a 'Service Redirection' for SMTP to the mail server and to the Citrix Server for the client-tracking application. We also configured rules to allow our vpn clients to pass the client-tracking application through the vpn tunnels.

DNS can be a complicated subject with regards to a firewall and how you configure it can affect the performance of your firewall. The Domain Name Service is used to translate Internet names. SEF uses a proxy that is installed called "DNSd". It is installed by default and is a secure, fully functional, caching

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

DNS name server and proxy. This proxy can provide name resolution for computers inside and outside the network while keeping the inside network private. The requests that arrive on the private interface are resolved from the hosts file, if that fails; it looks to the hosts.pub file, if no record is found the request is resolved through DNS recursion from the Internet. From the properties page of the DNSd proxy under 'Proxy Services' in the SRMC, you will see the entry for the loopback and one for the inside interface. These entries correspond to the hosts file which are your private network. The hosts.pub file is empty until public records are entered. These records will correspond to your public hosts that are perhaps on your service network. Queries to the public interface will not use the hosts (private) file. This was a very basic configuration and network with no service network. There are no internal name servers. The Internet root name servers are hard coded into the DNSd proxy. DNSd will deliver and cache the response. The private reverse zones will need to be added when the firewall is authoritative. You will see an entry for 127.0.0.1 localhost, the loopback interface, the inside and outside adapters, a host entry for the IP address of the internal firewall, and the reverse zone for the localhost. We also entered private host records for servers. If you do not want the firewall to act as a caching server, you can configure 'forwarders' under the 'DNS' folder under 'Base Components'. It is not necessary to configure forwarders on the SEF unless you have an internal firewall that does not have access to the Internet root hint servers. You can use forwarders to direct your hosts to the ISP name servers if you wish. In this scenario you would "trust" the ISP records. By using forwarders on SEF you will make private name server entries ineffective and prevent the proxy from using the built in list of root hint servers. "Cache poisoning" is an exploit where the DNS cache table is manipulated with false information. By using forwarders, you are trusting that the ISP name servers have not been corrupted.[10]

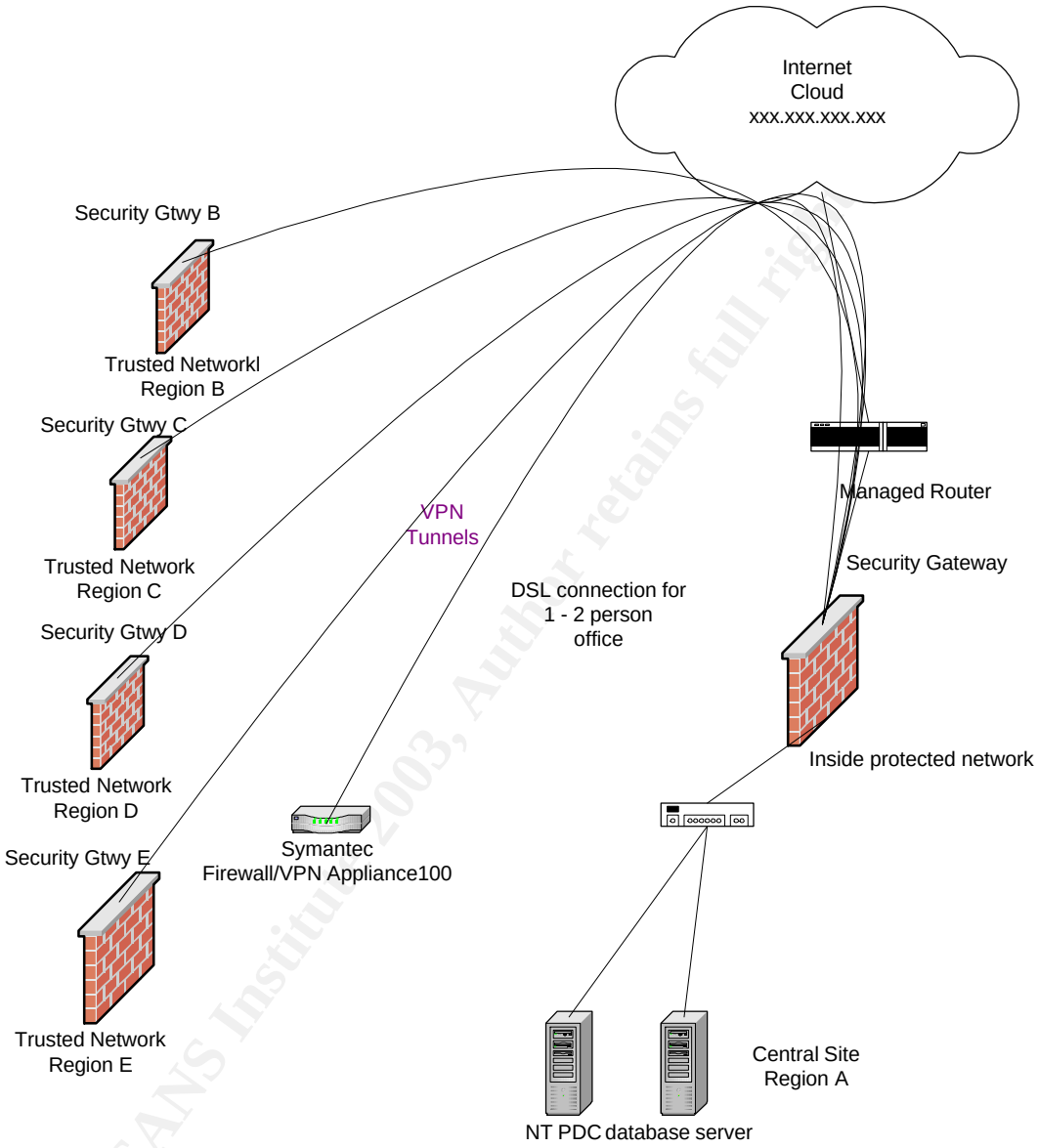
The Extended Network

Users are required to authenticate to their network. These networks were behind firewalls and considered trusted by the central location. The site-to-site vpns would pass the traffic from the trusted networks to the Central Site 'Security Gateway' – which is then redirected to the internal server in the protected network if the traffic adheres to the configured rule. It is also important to note that if you are using DHCP on your networks, that you take care with regards to the 'lease' of the addresses. The SEF counts each new IP as a license and if your leases expire quickly, you could have users being counted multiple times and using up your licensing. By default, SEF uses the outside address on traffic passing out to the Internet and the default transforms for tunnels is to use the original client address. 'Address Transforms' under 'Access Controls', can be configured to change this behavior. Our application does not require the IP address of the client, so all traffic on this firewall will utilize the outside interface address.

[10] DNSd Tutorial, Firetower.com

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

The firewalls and vpn servers are in place; secure tunnels initiated, and rules configured. We have now extended our network over the Internet.



Protecting the VPN

To keep the vpn safe from hackers/attackers we need to maintain security at our trusted networks, keep our rules specific to services and users that need to pass the traffic, and monitor the firewalls. We maintain security at the trusted networks with password policies, network usage policies, and educating the end-users to exploits used by attackers. You need to know that just installing a firewall is not enough to protect the network. Knowing how to read the logs is a

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

vital part of the system. In an article by Laura Taylor[11], titled Read your Firewall Logs, she advises us "*read the log files every day, you'll get a feel for what is normal and abnormal connection behavior."* While this is helpful, we have found several web sites that can be useful as well. A FAQ: Firewall Forensics (What am I seeing?)[12] is a wonderful resource for the administrator. Knowledge of ports used in exploits can be your first defense against attacks. Under the 'Monitoring Controls' folder you will find the log files. You can filter through the day's messages using IP address, text, message numbers, and components. This is a very useful feature when troubleshooting traffic. The 'Active Connections' folder will list the source, destination, and type of service, duration and the internally-used ID of each connection. The SEF also can be configured to protect for 'IP Spoofing'. Select the outside interface and select all inside addresses to protect. This way, if an inside address comes from the outside interface, the packet is dropped. You can also protect for DOS (Denial of Service) attacks. You should only enable this feature when you know you are under attack. If complaints about service come in for the firewall, the command 'netstat –a' will list TCP connections, if there are many in a SYN_RCVD state, then you are under attack. When you find that you are being attacked, calling the owner of the IP address may not be enough. Most ISP's will want to see log files providing proof of the attacks. Symantec offers a program called remotelogfile.exe. This program allows you to keep logs on a remote pc/server, have the option to filter, and to save to another file.

Disaster Recovery

Backup procedures for the firewall would include configuration files, the routing table, the hosts and hosts.pub files. These files are copied to a backup directory and password protected and can be kept on a floppy. If there is an attempt to recover the firewall on a system with a volume ID other than the current one, the password is required. If the firewall needs to be rebuilt or a new hard drive installed, the volume ID will change and you will need to send to Symantec for a license key based on the new volume ID.

Backup and disaster recovery documents were updated for the vpn system.

Conclusion

The SEF/SEVPN solution was cost effective, easily deployed, and can now be centrally managed by staff. The organization was also able to eliminate dialup into the regional sites improving security and access speeds for users and administrators. And where do we go from here? Penetration testing can be done to test the firewalls external security. We would like to convince top management that writing security policies is not intended to restrict our own users as much as it is to ensure the safe environments to accomplish their work.

[11] Taylor, Laura, "Read your firewall logs"
[12] A FAQ: Firewall Forensics (What am I seeing?)

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

Testing of backups and recovery procedures should continually be done. Education of users and the constant mantra of what is safe to do and what is not so safe will always be the challenge this department will face.

References

[1] Symantec Enterprise Firewall and Symantec Enterprise VPN Server, Installation Guide, Version 6.5, April 2001

[2] SANS Institute, The Sans Institute Security Policy Project
URL: http://www.sans.org/resources/policies/

[3] Taylor, Laura, "Firewall Shopping 101", 21 February, 2002
URL: http://www.smallbusinesscomputing.com/buyersguide/print.php/978221

[4] Smith, Rick, Network World "Hybrid firewalls can dig up worms", 01 April, 2002
URL: http://www.nwfusion.com/news/tech/2002/0401tech.html

[5] Network World, "Buyer's Guide: The bottom line on per-user pricing" 20 October, 2002
URL: http://www.nwfusion.com/reviews/2002/1028bgchart.html

[6] Symantec Knowledgebase, Software that should not be loaded on the SEF/SEVPN
URL: http://service1.symantec.com/SUPPORT/ent-gate.nsf/50fd411fcbe7755a88256bc1005cd7c8/1ba8af595d94addb88256bd0007f9493?OpenDocument&prod=Symantec%20Enterprise%20Firewall&ver=6.5.2%20for%20Windows%20NT/2000&src=ent&pcode=sym_ent_firewall&dtype=corp&svy=&prev=&miniver=sym_ent_firewall_65_nt

[7] Webopedia, IPsec
URL: http://www.webopedia.com/TERM/I/IPsec.html

[8] RFC2409, The Internet Key Exchange, Request for Comments 2409, D. Harkins & D. Carrel, Cisco Systems, November 1998
URL: http://ietf.org/rfc/rfc2409.txt?number=2409

[9] RFC1827, IP Encapsulating Security Payload, Request for Comments 1827, R. Atkinson, August 1995
URL: http://www.faqs.org/rfcs/rfc1827.html

[10] DNSd Tutorial
URL: http://www.firetower.com/faqs/dns/

[11] Taylor, Laura, "Read your firewall logs!" 10 July, 2002
URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2782699,00.html

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

[12] A FAQ: Firewall Forensics (What am I seeing?), version 1.2.0, January 200
URL: http://www.linuxsecurity.com/resource_files/firewalls/firewall-seen.html

© SANS Institute 2003, Author retains full rights.