Global Information Assurance Certification Paper

GCFW Practical v4.0

Niksun Appliance 2005 as a Perimeter Defense
and
GIAC Enterprises Security Architecture

Matthew P. Steiniger
Submitted December 28, 2004

Matthew P. Steiniger
GCFW Practical v4.0
December 28, 2004

Abstract
The purpose of this paper is twofold. The first purpose is to inform the reader about how Niksun NetVCR and NetDetector 2005 can be used as valuable tools for monitoring network perimeters. The second purpose is to define a secure network infrastructure for the fictitious company, GIAC Enterprises.

Ironically, I have chosen not to use Niksun NetVCR and NetDetector in the security architecture for GIAC Enterprises. This was done because it did not seem cost-effective to use this solution for such a small organization. After reading this paper, the reader should be able to decide for whether or not Niksun NetVCR and NetDetector could be of use to his or her organization.

Assignment 1

Niksun NetVCR/NetDetector 2005 as a Network Perimeter Defense

1) What is the problem?

Perimeter security is one of the most important concerns in the Information Security Industry today. The network perimeter is the first line of defense against malicious activity from outside of your network, as well as the last line of defense in controlling the flow of data out of your network. On the Information Technology Security playing field an organization needs a defense that can see all of the data moving in and out of a network at all times. Unfortunately security personnel are not always capable of seeing everything that occurs every second of the day on a network, and they may not catch malicious activity the moment that it occurs.

What an organization needs is a network recording device capable of recording multiple network connections, at speeds of up to a gigabit per second. On top of being able to record such a large amount of data, the device needs to be able to perform real-time analysis for possible intrusions, as well as allow security personnel to replay and perform manual analysis of the collected data. The solutions are Niksun NetVCR and NetDetector 2005.

2) What are Niksun NetVCR and NetDetector 2005?

What are Niksun NetVCR and NetDetector 2005? These are the latest software versions of two of Niksun's most effective network monitoring solutions. Niksun NetVCR is a network recording appliance capable of recording all of the network traffic on two gigabit Ethernet connections, four 100 megabit connections, or many combinations of network links. The collected data can then be analyzed to

identify network problems, and show network trends. Niksun NetDetector is much like NetVCR, however there are a few significant differences. Rather than focusing on network troubleshooting, NetDetector employs a fully functional Intrusion Detection System.

Until this latest version, NetVCR and NetDetector could not be housed on the same appliance. This meant that an organization would have to purchase two appliances, both of which were very similar and involved running analysis on the exact same data sets. Fortunately, Niksun has continued to work hard to improve their products. Now you can have the functionality of both appliances on one system.

3) Why record all of that data?

But why mention NetVCR/NetDetector appliance as a perimeter security device? What is so important about logging a bunch of data? The importance becomes clear when a malicious attack occurs on a server on your network. As you look through the logs on the server and your Intrusion Detection System you find that the attacker was clever enough to erase any possible evidence that they were there.

If properly installed and configured you can go back and replay all of the network traffic to and from the affected system. This can allow you to find out important information like; the attackers IP address, how the attacker got in to your network, what other machines did the attacker "talk" to on your network, etc. You can also use this appliance to monitor LAN user's Internet activity and walk through websites that they visited, rebuilt from the same packets used in the actual transmission.

Another important reason to collect all of this data is for it's usefulness in the event that an attacker does gather important data from your network. If you have recorded all of the data leaving your network you will not be left guessing exactly "what" an attacker made off with. Wouldn't it be nice to be able to say that an attacker did not steal your organizations sensitive data? This would be preferable compared to picking up the pieces after a network intrusion and hoping that the attacker did not get anything important, without really being sure.

4) What else can this appliance really do?

So what else can the Niksun NetVCR and NetDetector appliance do? Below is a list of the major features of the combined appliance:

1. Support for 10/100 Ethernet, Gigabit Ethernet, T1/E1, ATM, POS, and ATM OC-3/OC-12 interfaces. (Niksun, "Niksun Appliance User's Guide")
2. Accessible via a web management interface using HTTP or HTTPS. (Niksun, "Niksun Appliance User's Guide")

3. Capable of recording partial or full data packets on a network, filtered by network address, port, or any through the use of any number of many other optional filters. (Niksun, "Niksun Appliance User's Guide")
4. Configurable user accounts for granting or limiting user access to the appliance. (Niksun, "Niksun Appliance User's Guide")
5. Support for TACACS+ and RADIUS external authentication.
6. Able to be secured using an integrated firewall. (Niksun, "Niksun Appliance User's Guide")
7. On demand traffic analysis of collected data based on host, subnet, or protocol over a user-specified period of time. Analysis can be performed in a "drill-down" fashion. (Niksun, "Niksun Appliance User's Guide")
8. Allows the user to view decoded packet information and dumps from collected packet, and search the data for specific string data. This data can also be exported to pcap for analysis. (Niksun, "Niksun Appliance User's Guide")
9. Generate IP host pairs tables. (Niksun, "Niksun Appliance User's Guide")
10. Generate lists of TCP connection statistics, including communication time, retransmits, TCP flags, and applications used. (Niksun, "Niksun Appliance User's Guide")
11. Perform TCP reconstruction of HTTP, SMTP, FTP, chats (MSN Messenger, AOL Instant Messenger, Yahoo), and Telnet traffic sessions. This feature also allows searching reconstructed data for user-specified strings. (Niksun, "Niksun Appliance User's Guide")
12. Create charts showing network traffic over time periods from seconds to months. (Niksun, "Niksun Appliance User's Guide")
13. Generate reports identifying top network talkers, applications/ports being used on a network, network utilization, packet rate, and network problems. (Niksun, "Niksun Appliance User's Guide")
14. Generate alarms based on anomalous network traffic, network performance thresholds, port scanning, Snort signatures, and other intrusion detection capabilities. Alerts can be sent to the user's screen, pager, e-mail, or via an SMTP trap. (Niksun, "Niksun Appliance User's Guide")

5) How does this appliance work?

So how does the NetVCR/NetDetector appliance work exactly? First, raw data is collected from one or more network interfaces that are connected in carefully selected areas of your LAN (Niksun, "Niksun Appliance User's Guide"). This data is passed to the Traffic Recorder which does exactly that, records the network traffic to disk storage in "Datasets" (Niksun, "Niksun Appliance User's Guide"). The Query Processor then allows the data to be analyzed in one of two ways; through the Alerter, which runs in the background and generates alarms based on anomalies and pre-set thresholds, or through queries passed on through the Web GUI (Niksun, "Niksun Appliance User's Guide"). Connections to the NetVCR/NetDetector appliance are controlled through a user-configurable

integrated firewall (Niksun, “Niksun Appliance User’s Guide”). All of this occurs on a hardened FreeBSD platform.

The hardware platform can be ordered to fit your organizations needs. A high-end appliance would typically be a dual Pentium 4 processor system with four gigabytes of memory and a half Terabyte of SCSI hard disk storage in a 2U rack-mountable chassis.

6) How do you deploy it?

This solution could be deployed in many ways. First, you will need to be able to capture network traffic that is moving through your network. This can be accomplished by; placing a hub in-line where you would like to collect traffic, using a switch span port, or preferably through using more efficient network “taps”. There are advantages and disadvantages to using any of these methods.

A hub is a less-costly alternative which will allow you to connect the NetVCR/NetDetector appliance, as well as other Intrusion Detection Systems. Why does this work? Because a hub is merely a multi-port repeater that pushes traffic that it receives out to all of the ports on the hub. This option is cost effective, but it could cause latency issues and collisions if used on a high-traffic network link. Another concern using this solution compared to a passive network “tap” is if a hub loses power, you lose that network link.

A switch span port can be used to duplicate traffic on a switched port. I do not recommend this option. I have seen instances where a switch is unable to adequately duplicate the traffic to the span port, leaving me with incomplete network conversations. There is an advantage to this option though. If you have a NetVCR/NetDetector interface monitoring a switch span port you can reconfigure the span port quickly to monitor any device connected to that switch, without unplugging any network links.

Lastly, you can use a network “tap” which will allow you to gather all of the data without adding additional latency like using a hub. A network “tap” can allow you to monitor a network line, without participating in any of the conversations. The best choice is a passive “tap” that will still pass network traffic if the unit loses power. Unfortunately network taps typically split the “tapped” traffic into two separate interfaces, one for each side of the conversation. Normally this would tie up two interfaces on your NetVCR/NetDetector appliance. This leaves you with three options:

1) Use two interfaces and merge the datasets on the NetVCR/NetDetector appliance.
2) Use an expensive solution, such as a TopLayer Switch to aggregate the network traffic into a single interface for monitoring. This solution will

provide you with up to four aggregated ports for monitoring with this solution, as well as other Intrusion Detection Systems.

3) "Tap" the line with a Net Optics aggregator tap. The Net Optics aggregator "tap" provides you with a monitoring port that has already combined both sides of the conversation. Unfortunately this solution comes at a higher cost than a normal network "tap" (Net Optics, "10/100BaseT Port Aggregator Tap").

Ok, so now you have the equipment you need to monitor the network. The next important step is determining the proper place to monitor your network from. Here is a list of some important areas you should consider monitoring on your network:

1) Between your firewall and the Internet. This will allow you to see failed attempts to penetrate your firewall.
2) Between your firewall and your DMZ. This is particularly useful if the DMZ network is running Network Address Translation. If you are running Network Address Translation you will be unable to see the real addresses of these systems by monitoring outside of your firewall.
3) Between your firewall and you internal LAN. The same as the DMS, this is useful is you are running Network Address Translation.
4) Between a high-importance server, such as a web server, and the system's connection to your LAN.
5) On the link between remote office locations and your organization headquarters.

7) But are there drawbacks?

As with any security solution, there are drawbacks and weaknesses. The main drawback is that although you will be able to record encrypted data, such as SSL, the data collected will be pretty much useless. A clever attacker could use encrypted connections to enter your network, or worse yet, use an encrypted connection to steal your sensitive data. You will still be able to gather important information, but an attacker could still hide their payload.

8) Summing it all up.

As you can see, the Niksun NetVCR/NetDetector appliance is a potentially valuable tool for network perimeter security personnel. The appliance features a fully-functional Intrusion Detection System, which can be used to complement, or possibly replace, existing Intrusion Detection Systems. This appliance will provide you with a set of eyes watching the perimeter of your network at all times, alerting capabilities, and on-demand access to all of the data entering and exiting your network perimeter.

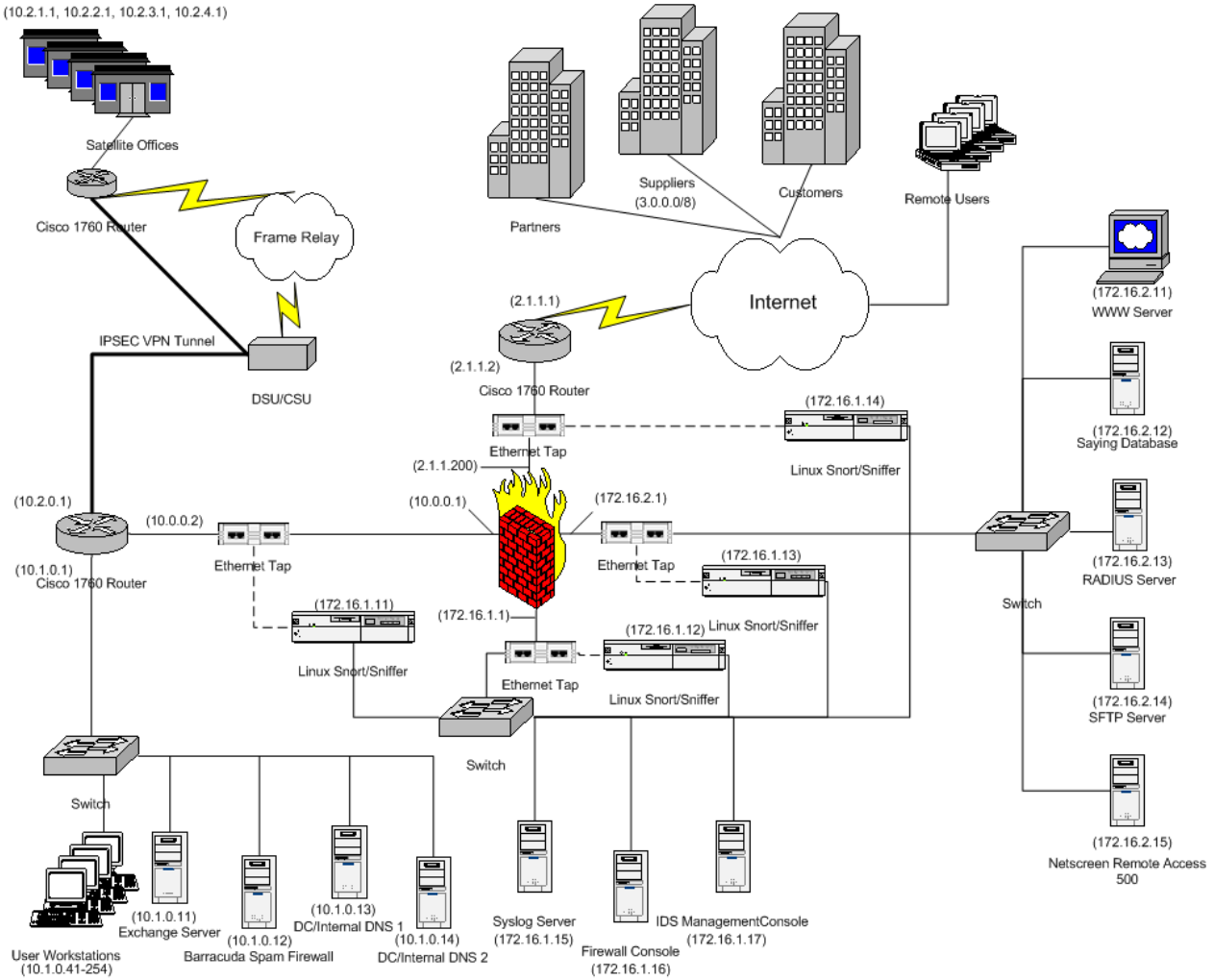
This appliance does come with a hefty price, depending on your configuration. With licensing and support, a high-end appliance could cost upwards of $50k. But if you can afford the hefty price tag, can you afford to not have such a useful network monitoring tool?

Assignment 2 – Security Architecture for GIAC Enterprises

GIAC Enterprises is a small business that markets fortune cookie sayings worldwide. The organization employs 50 people. Most of GIAC Enterprises' employees work at their home office, while the remainder of GIAC Enterprises' employees works out of four regional satellite offices around the world. All of GIAC Enterprises' sales are done via the Internet.

All server and workstation systems connected to the GIAC Enterprises network that are running Microsoft Windows operating systems run a copy of Symantec Antivirus with current virus definitions acquired from the Internet. All servers running Linux operating systems will run McAfee Antivirus. Wireless connectivity is restricted on the GIAC Enterprises network. All network switches will run "port security" to help ensure that no unauthorized computer or network devices are connected to the GIAC Enterprises network.

Network Diagram for GIAC Enterprises:



I) Network Access Requirements by Group:

1) Customers
GIAC Enterprises' customers need to be able to access the GIAC Enterprises website. The customers connect to the GIAC Enterprises website through HTTPS and select the product that they would like to purchase. Access to the HTTPS website is restricted to customers using a username and password provided by GIAC Enterprises. The customer is able to create the required username and password from the initial login page. Password resets are performed by emailing the customer a "one-time use" password, which allows them to create a new password. The customer is able to use a secure form over HTTPS to purchase products. After a customers order is processed and verified, the user is notified via email that they can now login to the HTTPS website and download the product. Use of the HTTPS website requires that TCP port 443 is open to the Internet.

2) Suppliers
Suppliers for GIAC Enterprises make deliveries of fortune cookie sayings via secure transactions to the GIAC Enterprises SFTP server. Access to the SFTP server is restricted by requiring a username and password that is provided the supplier by certified mail, and activated upon confirmed receipt. Password resets can be performed by certified mail or by phone after confirmation using the caller's date of birth, and mother's maiden name. Access to the SFTP server is access controlled at the border router and the firewall to only allow the specific IP addresses of GIAC Enterprises' suppliers. Use of the SFTP server requires that TCP port 22 is open to specific supplier IP addresses.

3) Partners
GIAC Enterprises business partners access GIAC Enterprises network resources through a Netscreen Remote Access 500 SSL appliance. This appliance allows GIAC Enterprises partners to review information provided to business partners in a secure manner. Access to the Netscreen Remote Access 500 appliance is controlled by RADIUS authentication, using a username and password that is provided to business partners by certified mail, and activated upon confirmed receipt. Password resets can be performed by certified mail or by phone after confirmation using the caller's date of birth, and mother's maiden name. Accessing the Netscreen Remote Access 500 SSL appliance requires TCP port 443 is open to the Internet.

4) GIAC Enterprises employees on the User LAN
GIAC employees are able to access internal LAN resources. Local access to servers is limited to server administrators, and is controlled

through Active Directory authentication. Access to workstations is limited to authorized GIAC Enterprises personnel authenticated through Active Directory. GIAC Enterprises employees are allowed access to the Sayings Database server in the DMZ through the firewall. Personnel are issues usernames and passwords in person at headquarters. Password resets can be performed in person or by phone after confirmation using the caller's date of birth, and employee number. Internal LAN users require access to the Internet using HTTP, HTTPS, and FTP, through TCP port 80, TCP port 443, TCP port 20, and TCP port 21. The Internal DNS server will need to forward DNS lookup requests to the Firewall on UDP port 53. The Barracuda Spam Firewall will need to be able to send and receive SMTP email messages on TCP port 25 through the Firewall. Internal LAN users will require access to the SFTP server through the Firewall using TCP port 22. Internal LAN users will also need access to the Saying Database server using TCP port 1433 and UDP port 1434. The Internal Domain Controllers will require access to NTP through TCP port 123.

5) GIAC remote users (sales force)
GIAC Enterprises remote users access GIAC Enterprises network resources through a Netscreen Remote Access 500 SSL appliance. This appliance allows GIAC Enterprises remote users to access email and other required resources in a secure manner. Access to the Netscreen Remote Access 500 appliance is controlled by RADIUS authentication, using username and password provided at headquarters, or through certified mail, and activated upon receipt. Password resets can be performed by certified mail or by phone after confirmation using the caller's date of birth, and employee number. GIAC Enterprises remote users will require access to the Netscreen Remote Access 500 SSL appliance using TCP port 443. GIAC remote user computer systems will be secured using a "personal firewall" allowing users to access only HTTP, HTTPS, and FTP, through TCP port 80, TCP port 443, TCP port 20, and TCP port 21.

6) General Public
The general public is allowed to access the public WWW server using HTTP. No other access is required, or allowed to the general public. The general public will have access over the Internet to TCP port 80 on the WWW server.

7) GIAC Enterprises Security Personnel
GIAC Enterprises Security personnel will require access from the Security LAN using HTTP, HTTPS, FTP, and NTP. These services are required to update software and apply security patches. NTP is required so that time can be synchronized on all of the Security LAN servers to ensure that the time and date is correct on all security logs. This will require access

through TCP port 80, TCP port 443, TCP port 20, TCP port 21, and TCP port 123.

II) Network Component List

Perimeter Network Components

1) Cisco 1760 Router, Border
The Cisco 1760 Router on the edge of the GIAC Enterprises perimeter is used to route traffic to and from the GIAC Enterprises LAN, as well as to screen out any unnecessary network traffic. It is required at the edge of the network perimeter to perform routing functions. All passwords to access the device are encrypted, and all access via SNMP, Telnet, HTTP, and HTTPS are disabled. The only method of accessing the router for management is using a physically connected console, or from the Firewall Console IP address, using only SSH. IP source routing, IP redirects, IP unreachables, IP proxy-arp, and CDP are disabled. The router has been configured to reject packets coming in from the Internet from private IP addresses, and IANA unassigned/reserved IP addresses. The router's main weaknesses are vulnerabilities found in the Cisco IOS. To mitigate this risk, all available patches are installed when they are available. This device was chose because of the large amount of available support for Cisco products. The specific model was selected because it is a cost-effective, rack-mount router. Cisco 1760 routers offer excellent screening capabilities, and strong encryption for remote access (Cisco Systems, Inc., "Cisco 1760 Modular Access Router Data Sheet"). This router adheres to the principal of defense in depth because it is used in conjunction with a firewall to screen out unwanted network traffic.

2) Symantec Gateway Security 400 Appliance (Primary Firewall)
The Symantec Firewall appliance is used to shield the GIAC Enterprises LAN from malicious attacks. It is placed directly behind the perimeter router as a second-line of defense. Management of the firewall is restricted to the Firewall Console on the Security LAN. This firewall was selected for ease of use and configuration, strength as a firewall, and being sized properly for the organization. This firewall offers stateful packet inspection, detailed logging, intrusion prevention, content filtering, and automatic updates (Symantec Corporation, "Symantec Gateway 400 Series"). This firewall adheres to the principal of defense in depth because it is used in conjunction with a screening router to screen out unwanted network traffic. The 400 model was selected because it is sized to meet the needs of this organization (Symantec Corporation, "Symantec Gateway 400 Series").

3) Ethernet Tap, Outside
The Outside Ethernet Tap is located between the perimeter router and the firewall. The tap selected is the Net Optics 10/100 Port Aggregator Tap. The Net Optics tap allows passive monitoring of network links, without the risk of adding another point of failure to your network (Net Optics, Inc., "10/100BaseT Port Aggregator Tap"). This device allows monitoring of all data passing in and out of the GIAC Enterprises network. There are no known weaknesses associated with a passive Ethernet Tap. This device was chosen based on cost, and proven effectiveness for monitoring Ethernet. This tap adheres to defense in depth because it is used in conjunction with three other taps to monitor traffic flowing across the GIAC Enterprises' network.

4) Ethernet Tap, DMZ
The DMS Ethernet Tap is located between the firewall and the DMZ. This device allows monitoring of all data passing in and out of the DMZ. The tap selected is the Net Optics 10/100 Port Aggregator Tap. The Net Optics tap allows passive monitoring of network links, without the risk of adding another point of failure to your network (Net Optics, Inc., "10/100BaseT Port Aggregator Tap"). There are no known weaknesses associated with a passive Ethernet Tap. This device was chosen based on cost, and proven effectiveness for monitoring Ethernet. This tap adheres to defense in depth because it is used in conjunction with three other taps to monitor traffic flowing across the GIAC Enterprises' network.

5) Ethernet Tap, Security LAN
The Security LAN Ethernet Tap is located between the firewall and the Security LAN. The tap selected is the Net Optics 10/100 Port Aggregator Tap. The Net Optics tap allows passive monitoring of network links, without the risk of adding another point of failure to your network (Net Optics, Inc., "10/100BaseT Port Aggregator Tap"). This device allows monitoring of all data passing in and out of the Security LAN. There are no known weaknesses associated with a passive Ethernet Tap. This device was chosen based on cost, and proven effectiveness for monitoring Ethernet. . This tap adheres to defense in depth because it is used in conjunction with three other taps to monitor traffic flowing across the GIAC Enterprises' network.

6) Ethernet Tap, User LAN
The User LAN Ethernet Tap is located between the firewall and the GIAC Enterprises user LAN. The tap selected is the Net Optics 10/100 Port Aggregator Tap. The Net Optics tap allows passive monitoring of network links, without the risk of adding another point of failure to your network (Net Optics, Inc., "10/100BaseT Port Aggregator Tap"). This device allows monitoring of all data passing in and out of headquarters, including the unencrypted network traffic from the remote offices that is moving to and

from the firewall. There are no known weaknesses associated with a passive Ethernet Tap. This device was chosen based on cost, and proven effectiveness for monitoring Ethernet. This tap adheres to defense in depth because it is used in conjunction with three other taps to monitor traffic flowing across the GIAC Enterprises' network.

DMZ Network Components

7) WWW Server
The public WWW Server, running Microsoft IIS on Microsoft Windows 2003, is placed in the GIAC Enterprises DMZ. This device is placed in the DMZ, because this is the only area of the GIAC Enterprises network that incoming HTTP port 80 requests will be allowed. This device has no specific strengths since it is an HTTP server. The WWW Server will require access to the IDS Management Console to synchronize time using NTP on TCP port 123. The WWW Server is blocked from accepting any traffic from ports other than port 80, however it is still susceptible to IIS exploits. To mitigate the risk of IIS exploits being used on the system, all default IIS data structures have been removed, and all of the current patches have been applied. Microsoft Windows 2003 running IIS was chosen due to ease of installation and management.

8) Saying Database
The Saying Database is a server running Microsoft Windows 2003 with SQL 2000. The device has been placed in the DMZ to allow fast communications with the web servers that will be accessing the Saying Database. The Saying Database will require access to the IDS Management Console to synchronize time using NTP on TCP port 123. This server is vulnerable to Microsoft SQL 2000 vulnerabilities. To help mitigate the risk of SQL 2000 attacks, only the GIAC Enterprises internal LAN users can access the Saying Database through the firewall. All other communications with the server occur behind the firewall. Additionally, all current patches have been applied to this server for both Microsoft SQL 2000 and Microsoft Windows 2003.

9) RADIUS Server
The RADIUS Server is placed in the DMZ for user authentication. This authentication information is passed on to the Netscreen Remote Access 500 device. The RADIUS Server will require access to the IDS Management Console to synchronize time using NTP on TCP port 123. The RADIUS Server is running Microsoft Windows 2003 with Steel-Belted Radius software in Stand-Alone mode. To mitigate any weaknesses all patches and hotfixes have been applied to this server.

10) SFTP Server
The SFTP Server is a Windows 2003 server running SFTP, which is encrypted FTP running over SSH. This requires TCP port 22 to be allowed incoming from the Internet, as well as from the User LAN. The SFTP Server will require access to the IDS Management Console to synchronize time using NTP on TCP port 123. To mitigate the risk of attacks, all current patches and hotfixes are applied to this server.

11) Netscreen Remote Access 500
The Netscreen Remote Access 500 appliance is placed in the DMZ to allow remote access to resources on the GIAC Enterprises network. This appliance allows remote users to connect to GIAC Enterprises LAN resources through a secure SSL VPN connection. The Netscreen Remote Access 500 appliance will require access to the IDS Management Console to synchronize time using NTP on TCP port 123. To mitigate the risk of attacks to this system, only incoming HTTPS connections are allowed to this server from the Internet. This appliance was chosen because it affords remote users a simple method to connect to GIAC Enterprises, while still encrypting all data over the Internet. The model 500 was selected because it is sized to the needs of the organization.

Security LAN Network Components

12) Outside Linux Snort/Sniffer
The Outside Linux Snort/Sniffer server is running Redhat Linux, Snort Intrusion Detection System, and Ethereal Sniffer. Snort Intrusion Detection System (IDS) gives security personnel the capability to monitor network activities using s signature-based system. Ethereal allows security personnel to monitor and record network traffic for malicious activity. This server has been placed in the Security LAN, to ensure that it is isolated from the rest of the GIAC Enterprises network. The Security LAN is used to protect network monitoring and management systems from being tampered with. To mitigate the risks of attacks against the Linux operating system, or tampering with IDS logs, the only traffic allowed from the Outside Linux Snort/Sniffer server is HTTP, HTTPS, FTP, and NTP. This traffic is allowed solely for the purposes of obtaining security patches and hotfixes, and maintaining accurate system time for IDS and firewall logs. Additionally, all current patches have been applies to this server. The software packages on this server were chosen because they are proven in the security field, and because the software is available with no initial or recurring cost.

13) DMZ Linux Snort/Sniffer
The DMZ Linux Snort/Sniffer server is running Redhat Linux, Snort Intrusion Detection System, and Ethereal Sniffer. Snort Intrusion Detection System (IDS) gives security personnel the capability to monitor

network activities using s signature-based system. Ethereal allows security personnel to monitor and record network traffic for malicious activity. This server has been placed in the Security LAN, to ensure that it is isolated from the rest of the GIAC Enterprises network. The Security LAN is used to protect network monitoring and management systems from being tampered with. To mitigate the risks of attacks against the Linux operating system, or tampering with IDS logs, the only traffic allowed from the DMZ Linux Snort/Sniffer server is HTTP, HTTPS, FTP, and NTP. This traffic is allowed solely for the purposes of obtaining security patches and hotfixes, and maintaining accurate system time for IDS and firewall logs. Additionally, all current patches have been applies to this server. The software packages on this server were chosen because they are proven in the security field, and because the software is available with no initial or recurring cost.

14) Security LAN Linux Snort/Sniffer
The Security LAN Linux Snort/Sniffer server is running Redhat Linux, Snort Intrusion Detection System, and Ethereal Sniffer. Snort Intrusion Detection System (IDS) gives security personnel the capability to monitor network activities using s signature-based system. Ethereal allows security personnel to monitor and record network traffic for malicious activity. This server has been placed in the Security LAN, to ensure that it is isolated from the rest of the GIAC Enterprises network. The Security LAN is used to protect network monitoring and management systems from being tampered with. To mitigate the risks of attacks against the Linux operating system, or tampering with IDS logs, the only traffic allowed from the Security LAN Linux Snort/Sniffer server is HTTP, HTTPS, FTP, and NTP. This traffic is allowed solely for the purposes of obtaining security patches and hotfixes, and maintaining accurate system time for IDS and firewall logs. Additionally, all current patches have been applies to this server. The software packages on this server were chosen because they are proven in the security field, and because the software is available with no initial or recurring cost.

15) User LAN Linux Snort/Sniffer
The User LAN Linux Snort/Sniffer server is running Redhat Linux, Snort Intrusion Detection System, and Ethereal Sniffer. Snort Intrusion Detection System (IDS) gives security personnel the capability to monitor network activities using s signature-based system. Ethereal allows security personnel to monitor and record network traffic for malicious activity. This server has been placed in the Security LAN, to ensure that it is isolated from the rest of the GIAC Enterprises network. The Security LAN is used to protect network monitoring and management systems from being tampered with. To mitigate the risks of attacks against the Linux operating system, or tampering with IDS logs, the only traffic allowed from the User LAN Linux Snort/Sniffer server is HTTP, HTTPS, FTP, and NTP.

This traffic is allowed solely for the purposes of obtaining security patches and hotfixes, and maintaining accurate system time for IDS and firewall logs. Additionally, all current patches have been applies to this server. The software packages on this server were chosen because they are proven in the security field, and because the software is available with no initial or recurring cost.

16) Syslog Server
The Syslog Server is running on Redhat Linux. This server has been placed on the Security LAN to ensure that all stored data stays within one secure area on the GIAC Enterprises LAN. The Security LAN is used to protect network monitoring and management systems from being tampered with. To mitigate the risks of attacks against the Linux operating system, or tampering with IDS logs, the only traffic allowed from the User LAN Linux Snort/Sniffer server is HTTP, HTTPS, FTP, and NTP. This traffic is allowed solely for the purposes of obtaining security patches and hotfixes, and maintaining accurate system time for IDS and firewall logs. Additionally, all current patches have been applies to this server. The software packages on this server were chosen because the software is available with no initial or recurring cost.

17) Firewall Console
The Firewall Console is running on Windows 2003 Server. The Firewall Console is a central point of management for the main firewall. This server has been placed on the Security LAN to ensure that only authorized users on the Security LAN are able to access and maintain the GIAC Enterprises firewall. To mitigate the risks of attacks to this system, it has had all of the latest security patches and hotfixes applied. Windows 2003 Server was selected as the operating system for ease of use by security personnel.

18) IDS Management Console
The IDS Management Console is running on Redhat Linux. The IDS Management Console is a central point of management for all of the IDS systems on the GIAC Enterprises network. This server has been placed in the Security LAN to ensure that only authorized users on the Security LAN are able to access and maintain the IDS systems. The IDS Management Console system is also running as an NTP server to allow time synchronization queries from the DMZ. This will require TCP port 123 to be open from the DMZ to this system. To mitigate the risks of attacks to this system, it has had all of the latest security patches and hotfixes applied. Redhat Linux was selected as the operating system for the IDS Management console because there is no cost associated with the software, and because Analysis Console for Intrusion Databases (ACID) Console for Snort runs on Redhat Linux.

User LAN Network Components

19) Cisco 1760 Router, Internal and Cisco 1760 Routers, Remote Offices
The Cisco 1760 Router on the inside of the GIAC Enterprises perimeter is used to route traffic to and from the GIAC Enterprises remote offices, as well as to screen out any unnecessary network traffic. Connectivity between headquarters and the remote offices is established through IPSEC VPN tunnels running over frame relay lines to each office. Each office also has a Cisco 1760 Router to route traffic to headquarters, and establish connectivity. All passwords to access the device are encrypted, and all access via SNMP, Telnet, HTTP, and HTTPS are disabled. The only method of accessing the router for management is using a physically connected console, or from the Firewall Console IP address using only SSH. IP source routing, IP redirects, IP unreachables, IP proxy-arp, and CDP are disabled. The router has been configured to reject packets coming in from the Internet from private IP addresses, and IANA unassigned/reserved IP addresses. The router's main weaknesses are vulnerabilities found in the Cisco IOS. To mitigate this risk, all available patches are installed when they are available. This device was chose because of the large amount of available support for Cisco products. The specific model was selected because it is a cost-effective, rack-mount router. Cisco 1760 routers offer excellent screening capabilities, and strong encryption for remote access (Cisco Systems, Inc., "Cisco 1760 Modular Access Router Data Sheet"). This router adheres to the principal of defense in depth because it is used in conjunction with a firewall to screen out unwanted network traffic.

20) User Workstations
User Workstations on the GIAC Enterprises network are separated from computer systems in the DMZ to prevent malicious attacks initiated from the User LAN to reach the DMZ, as well as to prevent attacks initiated in the DMZ to reach user workstations. Additionally, the user workstations are separated from the Security LAN to prevent tampering with security systems and logs by unauthorized individuals. Users Workstations are only allowed to access HTTP, HTTPS, and FTP on the Internet. Additionally, User Workstations are allowed access to the WWW Server using HTTP, the Saying Database server using TCP port 1433 and UDP port 1434, and the SFTP Server using TCP port 22. The user workstations run Windows XP software for ease of use. All of the latest service packs, patches, and hotfixes are applied.

21) Exchange Server
The Exchange Server is running Microsoft Exchange 2003 and Microsoft Windows 2003 Server. The Exchange server is placed inside the User LAN to allow users to access the server to receive email messages. The Exchange server is running Symantec Antivirus to scan email messages

for malicious content. The Exchange server is allowed to access HTTP, HTTPS, and FTP through the firewall. This traffic is allowed solely for the purposes of obtaining security patches and hotfixes. No SMTP traffic moves through the firewall directly to the Exchange Server. This helps mitigate the risk of Exchange-specific attacks being made against the GIAC Enterprises email system. Microsoft Exchange 2003 was chosen because of ease of use and malicious file blocking capabilities when used with Microsoft Outlook 2003 on the user workstations. This server helps contribute to defense in depth because it is being used in conjunction with the Barracuda Spam Firewall and user workstations to block viruses and malicious content.

22) Barracuda Spam Firewall 400
The Barracuda Spam Firewall 400 is located on the User LAN to allow it to communicate with the Exchange Server. The Barracuda Spam Firewall 400 is used to filter malicious content and file attachments that could contain executable code. This server uses three virus scanners to scan incoming emails. These additional layers of protection, in addition to virus scanning on the Exchange Server and user workstations contribute to defense-in-depth. The Barracuda Spam Firewall is allowed to send and receive SMTP email messages on TCP port 25 through the firewall. Additionally, the Barracuda Spam Firewall will need access to TCP port 7 outgoing, HTTP TCP port 80 outgoing, NTP TCP port 123 outgoing, TCP port 2703 incoming and outgoing, and TCP port 6277 incoming and outgoing (Barracuda Networks, “Barracuda Spam Firewall Quickstart Guide”). These additional ports are required for connectivity to Barracuda Networks for performing updates. The Barracuda Spam Firewall 400 was selected because of ease of use, user-manageable message quarantine areas, and RAID redundancy in the event of disk failure (Barracuda Networks, “Reclaim Your Email, Barracuda Spam Firewall”).

23) DC/Internal DNS 1
The DC/Internal DNS 1 Server is a Windows 2003 domain controller running Active Directory and DNS. This server is located on the User LAN for authenticating users. This server also runs DNS to answer user queries, as well as to support Active Directory. This server is allowed access to HTTP, HTTPS, and FTP for performing updates. Additionally, this server is allowed to access UDP port 53 for the purpose of forwarding DNS queries to external DNS servers. To help mitigate the risk of attacks against this server, all of the latest service packs, patches, and hotfixes have been applied. Windows 2003 Server was selected because of ease of administration, and the ability to create Windows domains for use with Windows XP workstations.

24) DC/Internal DNS 2

The DC/Internal DNS 2 Server is a Windows 2003 domain controller running Active Directory and DNS. This server is a redundant server for the GIAC Enterprises Active Directory domain, and for DNS name resolution. This server is located on the User LAN for authenticating users. This server also runs DNS to answer user queries, as well as to support Active Directory. This server is allowed access to HTTP, HTTPS, and FTP for performing updates. Additionally, this server is allowed to access UDP port 53 for the purpose of forwarding DNS queries to external DNS servers. To help mitigate the risk of attacks against this server, all of the latest service packs, patches, and hotfixes have been applied. Windows 2003 Server was selected because of ease of administration, and the ability to create Windows domains for use with Windows XP workstations.

Assignment 3 – Firewall Policy

This is the rulebase for the Symantec Gateway Security 400, the primary firewall for GIAC Enterprises. The specific appliance model being used is the Symantec Gateway Security 420, which has four 10/100BaseT interfaces. The interfaces are connected as follows; WAN1 is connected to the Internet, WAN2 is connected to the DMZ, WAN3 is connected to the Security LAN, and WAN4 is connected to the User LAN.

Firewall Rules:

1) Allow HTTPS/TCP port 443 from the Internet on WAN1 incoming to the WWW Server (172.16.2.1) on WAN2. This rule allows customers to access the organization's secure web server.

2) Allow SFTP/TCP port 22 from the 3.0.0.0/8 network incoming on WAN1 to the SFTP Server (172.16.2.14) on WAN2. This rule allows specific suppliers to access the organization's secure FTP server.

3) Allow HTTPS/TCP port 443 from the Internet on WAN1 to the Netscreen Remote Access 500 Appliance (172.16.2.15) on WAN2. This rule allows GIAC Enterprises Partners to access the SSL VPN appliance.

4) Allow HTTP/TCP port 80 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the Internet on WAN1. This rule allows users on the internal LAN to access websites on the Internet.

5) Allow HTTPS/TCP port 443 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the Internet on WAN1. This rule allows users on the internal LAN to access SSL websites on the Internet.

6) Allow FTP/TCP port 20 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the Internet on WAN1. This rule allows users on the internal LAN to access FTP on the Internet.

7) Allow FTP/TCP port 21 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the Internet on WAN1. This rule allows users on the internal LAN to access FTP on the Internet.

8) Allow DNS/UDP port 53 from DC1 (10.1.0.13) on WAN4 outgoing to the Internet on WAN1. This rule allows the primary DNS server on the internal LAN to forward DNS requests to the Internet.

9) Allow DNS/UDP port 53 from DC2 (10.1.0.14) on WAN4 outgoing to the Internet on WAN1. This rule allows the secondary DNS server on the internal LAN to forward DNS requests to the Internet.

10) Allow SMTP/TCP port 25 from the Barracuda Spam Firewall (10.1.0.12) on WAN4 incoming and outgoing to the Internet on WAN1. This rule allows incoming and outgoing email messages to pass between the Barracuda Spam Firewall and the Internet.

11) Allow TCP port 1433 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the Saying Database (172.16.2.12) on WAN2. This rule allows internal LAN users to access the Saying Database in the DMZ.

12) Allow UDP port 1434 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the Saying Database (172.16.2.12) on WAN2. This rule allows internal LAN users to access the Saying Database in the DMZ.

13) Allow SFTP/TCP port 22 from the User LAN (10.0.0.0/8) on WAN4 outgoing to the SFTP Server (172.16.2.14) on WAN2. This rule allows internal LAN users to access the data stored on the secure FTP server in the DMZ.

14) Allow NTP/TCP port 123 from DC/Internal DNS 1 (10.1.0.13) on WAN4 outgoing to the Internet on WAN1. This rule allows this Domain Controller to synchronize time with NTP servers on the Internet.

15) Allow NTP/TCP port 123 from DC/Internal DNS 2 (10.1.0.14) on WAN4 outgoing to the Internet on WAN1. This rule allows this Domain Controller to synchronize time with NTP servers on the Internet.

16) Allow HTTP/TCP port 80 from the Internet on WAN1 incoming to the WWW Server (172.16.2.11) on WAN2. This rule allows the general public to access GIAC Enterprises public web server.

17) Allow HTTP/TCP port 80 from the Security LAN (172.16.1.0/24) on WAN3 outgoing to the Internet on WAN1. This rule allows computer systems on the Security LAN to access websites on the Internet to perform software updates.

18) Allow HTTPS/TCP port 443 from the Security LAN (172.16.1.0/24) on WAN3 outgoing to the Internet on WAN1. This rule allows computer systems on the Security LAN to access secure websites on the Internet to perform software updates.

19) Allow FTP/TCP port 20 from the Security LAN (172.16.1.0/24) on WAN3 outgoing to the Internet on WAN1. This rule allows computer systems on the Security LAN to access FTP servers on the Internet to perform software updates.

20) Allow FTP/TCP port 21 from the Security LAN (172.16.1.0/24) on WAN3 outgoing to the Internet on WAN1. This rule allows computer systems on the Security LAN to access FTP servers on the Internet to perform software updates.

21) Allow NTP/TCP port 123 from the Security LAN (172.16.1.0/24) on WAN3 outgoing to the Internet on WAN1. This rule allows computer systems on the Security LAN to synchronize their time with NTP servers on the Internet, to ensure that all logs have accurate time.

22) Allow NTP/TCP port 123 from the DMZ on WAN2 outgoing to the Security LAN (172.16.1.17) WAN3. This rule allows computer systems in the DMZ to synchronize time with the NTP server setup on the IDS Management Console on the Security LAN.

23) Allow TCP port 7 from the Barracuda Spam Firewall (10.1.0.12) on WAN4 outgoing to the Internet on WAN1. This rule allows the Barracuda Spam Firewall to perform software updates over the Internet.

24) Allow NTP/TCP port 123 from the Barracuda Spam Firewall (10.1.0.12) on WAN4 outgoing to the Internet on WAN1. This rule allows the Barracuda Spam Firewall to synchronize time with NTP servers on the Internet.

25) Allow TCP port 2703 from the Barracuda Spam Firewall (10.1.0.12) on WAN4 incoming and outgoing to the Internet on WAN1. This rule allows the Barracuda Spam Firewall to perform software updates over the Internet.

26) Allow TCP port 6277 from the Barracuda Spam Firewall (10.1.0.12) on WAN4 incoming and outgoing to the Internet on WAN1. This rule allows the Barracuda Spam Firewall to perform software updates over the Internet.

27) Deny any traffic not explicitly allowed in the firewall rulebase. This rule is not actually configured on the firewall. This is the default "deny" rule for all network traffic that is not explicitly allowed in any of the rulebase.

The order of the rulebase is not important on this appliance because there are no explicit deny rules other than the default deny rule. The default behavior of the firewall is to deny and log any inbound packets not explicitly allowed in the rulebase. The default behavior of the firewall is to deny and log any outbound packets, once outbound rules are defined for protected systems and you select to use those rules (Symantec Corporation, "Symantec Gateway 400 Series Administrator's Guide"). All of the protected network segments have explicit outbound rules. Additionally, there are no "loose" rules which would allow network traffic through the firewall that was not intended to be allowed. Overall, this tight rulebase contributes to a strong security posture. Any risks to computer

systems on the GIAC Enterprises network are mitigated through the use of antivirus software, and the application of regular software patches and updates.

References

1) “10/100BaseT Port Aggregator Tap.” Net Optics. 2004. Net Optics, Inc. 19 Dec. 2004 <http://www.netoptics.com/pdf/datasheet/DSNET96443.pdf>.

2) “Barracuda Spam Firewall Quickstart Guide.” Barracuda Networks. 2004. Barracuda Networks. 19 Dec. 2004 < http://www.barracudanetworks.com/support/docs/Manuals/BarracudaQuickStart Guide.pdf>.

3) “Cisco 1760 Modular Access Router Data Sheet.” Cisco Systems. 2003. Cisco Systems, Inc. 19 Dec. 2004 < http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1760e_ds.pdf>.

4) “Niksun Appliance User’s Guide, Version 3.1.” Niksun. 2004. Niksun, Inc. 19 Dec. 2004 <access to this document online requires being a Niksun support customer able to login at http://supportnet.niksun.com/>.

5) “Reclaim Your Email, Barracuda Spam Firewall.” Barracuda Networks. 2004. Barracuda Networks. 19 Dec. 2004 <http://www.barracudanetworks.com/news_and_events/docs/Barracuda_Datash eet.pdf>.

6) “Symantec Gateway 400 Series.” Symantec Corporation. 2004. Symantec Corporation. 19 Dec. 2004 < http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=1063>.

7) “Symantec Gateway 400 Series Administrator’s Guide.” Symantec Corporation. 2004. Symantec Corporation. 19 Dec. 2004 < ftp://ftp.symantec.com/public/english_us_canada/products/symantec_gateway_s ecurity/2-400-Series/manuals/SGS400_AdminGuide.pdf>.