Network Security Architecture Plan for GIAC Enterprises

Drew Timmerman
GCFW Practical
Version 4.0

January 10, 2005

1 Abstract

This document begins by exploring a new technology: Host-Based Intrusion Prevention. This technology has the potential to vastly improve network security and greatly aid a well-planned defense-in-depth strategy.

The next section describes the network security architecture for an online retailer. GIAC Enterprises is a fortune cookie saying reseller. It purchases sayings from several suppliers and resells them online. Because all of the revenue generated for GIAC Enterprises comes from online sales, the survival of this company depends on having an efficient, reliable computer network. Communication between the GIAC Enterprises headquarters, branch offices, business partners, and customers absolutely must be easy to use and always available.

The final section presents specific configuration of packet routing and filtering for GIAC Enterprises. These are the actual commands and settings that need to be set up based on the hardware that GIAC Enterprises will employ.

2 Assignment 1: Future State Of Security Technology

2.1 Introduction To Host-Based Intrusion Prevention

In the world of network security, there is a lot of focus on perimeter protection. There is a good reason for that. If you can prevent unauthorized access to your network at the perimeter, then you do not have to worry about each system defending itself. Unfortunately, if your perimeter defense is compromised, you stand the risk that an intruder could easily cause problems to many systems.

Defending a network perimeter will keep out the majority of evil-doers. But if you incorporate host-based intrusion prevention, you are making good use of defense-in-depth. The following sections will explore all relevant aspects of host-based intrusion prevention.

2.2 A Smart IDS?

So, what is a host-based intrusion prevention system (HIPS)? It sounds like an intrusion detection system (IDS) with brains to react to a situation. In a nutshell, that is exactly what it is. An IDS recognizes behavior that looks suspicious and determines if that is expected for a given system. A HIPS takes this idea a step further.

For instance, if you have an email server that typically communicates via TCP port 25 and all of a sudden one night it begins communicating through port 80, an IDS will try to determine if that is expected. If you set up a web-based front end for users to check email, that may be communication that you are expecting and welcoming. If you did not modify your IDS so that it knows that you are expecting such behavior, it might notify you via email or a pager that a port is communicating that previously was not. If you did not set up that web server for users to check their email, you will want to react to this situation as soon as possible. This may take a while to happen with an IDS, since there may be nobody around that can do anything about it. A HIPS attempts to react immediately by already having an idea of how to deal with a given situation. It may simply try to close TCP port 80; it may shut down the whole system; or do something completely different.

2.3 What's The Problem?

A host-based intrusion prevention system can do many things that are impossible to accomplish any other way. For instance, what good is a firewall if you have a system that is being attacked from the inside? An article by Network Magazine states that, "According to InterGov (www.intergov.org), an international organization that works with police agencies to combat cyber crime, insiders commit about 80 percent of all computer and Internet related crime, and these crimes cause an average loss of about $110,000 per corporate victim."

An attack can also be unintentional. If an employee has a virus or worm on their home computer and they bring a disk into the office that contains vacation photos, they could inadvertently spread malicious software which completely circumvents your firewall. Another problem lies with Virtual Private Network (VPN) users. A VPN will typically bypass your firewall and connect directly to systems on your network. There is no way to guarantee that a user's home system is secured as well as the systems you have control over. There is a need for systems to be able to defend themselves in this situation.

2.4 How It Works

Because host-based intrusion prevention is a new technology, it seems that implementation could take many different forms. According to the SANS Institute, intrusion prevention works in the following manner: "Similar to adaptive IDS, this is done by defining policies that describe how our applications work and what system calls they typically make. Anything that falls outside of this policy is prevented and generates an alert." ("SANS GCFW training". Defense In-Depth, module 2.4. Page 1-12.) They go on to say that a HIPS will typically run at the operating system's kernel level so that it can monitor all applications and processes.

In general, a HIPS utilizes IDS and adds reactionary measures. The IDS portion begins with a baseline audit. This is the process of determining what a given system should be doing. Once the baseline is established, the IDS portion detects behavior that seems suspicious. This can include new programs or services running that previously were not. It will look for new user accounts. It will look for new, modified, or missing files. Once the IDS triggers an alert, the prevention portion of the HIPS will attempt to react.

As operating systems become more sophisticated, I believe that HIPS will be built into the operating system. That could work better since no third party vendor should understand the operating system as well as the one who created the system in the first place. However, it often times is easy to overlook problems with your own creation if you are buried in the details; and it may take an outside party to discover such problems.

One thing to note is that placing the intrusion prevention system on the host rather than the network is that the host can fully monitor itself instead of just being able to see what is transmitted across the network. This nullifies the issue of how effective the intrusion prevention system is on a switched network environment.

2.5 Effects On Information Security Industry

One of the best things I see about a HIPS is that a system can be more self-reliant. If you have a mobile web server that you move from office to office for demonstration purposes, you do not have to count on the perimeter protection from the network you are currently connected to. This could also help protect notebook systems when they are not connected to your network.

A host-based intrusion protection system can be smart enough to learn what seems wrong. Unlike a network-based intrusion prevention system, which typically uses signatures to detect malicious behavior, a HIPS reacts based on what is normal for that system. It is also easy for a HIPS to include signature based detection so that you have the best of both worlds. But, because a HIPS is proactive instead of solely reactionary, you get a system that is ready to deal with a new attack immediately.

2.6 Effects On Information Systems Personnel

Unfortunately, there are many negative aspects related to HIPS that contribute to the reason that we do not see widespread use of this technology today.

To begin with, this technology is both complex and expensive. You have to deploy HIPS software to every system that you want to have protected. A network-based intrusion prevention system does not need to be installed on every system. Furthermore, a network-based solution typically does not care how many systems it is protecting. As long as it can keep up with the traffic, it can protect many, many systems. This can affect the cost of host-based versus network-based intrusion prevention systems as well. If you have to purchase a license for every system you want to protect, the HIPS could get very expensive.

Besides the burden of deployment, one would have to deal with the issues of maintaining a wide scale deployment of HIPS. It would be necessary to update individual systems on a regular basis. Unless there was a well-designed central management system, this would take a lot of time from information systems personnel. Additionally, centralized logging would be crucial. Not only would you have to configure this, but consideration would have to be taken to the additional network traffic if all logs are being sent across the wire to a central location. Finally, information systems personnel would have to deal with false positives. This is inevitable with any immature technology. Information systems personnel would need to become familiar with the type of problems false positives from the HIPS can cause and how to fix an overzealous HIPS system. This would be the situation from the example where the information systems department deploys a web-based front end to a mail server. This is new behavior to the mail server, and it may simply block TCP port 80, but it may also shut down mail services. Either way, the information systems personnel would need to realize that it is the HIPS that is preventing users from being able to check email remotely rather than the firewall or something else.

Then there are the problems associated with the individual systems being protected. A HIPS would need to closely monitor all system activity. This can bog down a system significantly. Another problem which is pointed out by Chris Brenton in his Track 2 SANS presentation, this could be a potential entry point for an attacker to launch a denial of service attack. If the attacker can cause a system to shut down because it is reacting to what it sees as an intrusion, the system may suspend services necessary to continue its normal operation.

A host-based intrusion prevention system cannot be the only line of defense in a well planned defense-in-depth strategy. If you rely solely on the HIPS and the system is compromised, then it stands to reason that the HIPS could be compromised as well. If HIPS is circumvented as well as the security built into the system, you have no other way to detect or prevent an attack.

2.7 Effects On Design Of Network Architecture

A HIPS deployment should not have much effect on the design of network architecture. It is certainly no replacement for patch management, virus protection, or perimeter protection. It will simply augment a well designed network that makes use of defense-in-depth. It is another layer of protection, so there is less reliance on the perimeter for protection.

A network-based intrusion prevention system monitors traffic on the network. Because of that, it is platform independent for the most part. As long as systems follow the standards for best practices, a network based solution can work with any type of operating system. For example a network based intrusion prevention system does not care if it is monitoring HTTP traffic from an Apache system running on a Linux server or an Internet Information Services (IIS) system running on Windows 2003. Conversely, a host-based intrusion prevention system must be able to run on the servers you are trying to protect. If you choose to run a HIPS package in a mixed environment, you may have trouble finding one solution that can adapt to heterogeneous systems. This could be a factor in planning what type of systems you expect to deploy in your environment.

2.8 Conclusion

To conclude, there are many aspects to a well designed network. Perimeter protection should take care of most external attacks. For the host, patch management is important, but it is signature based and detects problems after they are discovered. A HIPS will potentially protect systems against new vulnerabilities as well as internal attacks. This technology has may hurdles to clear, but has the potential to be an extremely important piece of a network that makes good use of defense-in-depth.

3 Assignment 2: Security Architecture

3.1 Introduction

This section discusses the network security architecture that will be implemented for GIAC Enterprises. GIAC Enterprises is an online reseller of fortune cookie sayings. The headquarters for GIAC Enterprises is located in Durango, Colorado. The majority of its fifty employees work at the headquarters office. GIAC Enterprises has four branch offices located in Auckland (New Zealand), Paris (France), Tokyo (Japan), and Buenos Aries (Argentina). There are only a few employees at each branch office.

The following document was produced in order to define a well thought out network that meets the GIAC Enterprises' business needs as well as provide adequate security and reliability to ensure the company is always able to do business. In order to attain this goal, careful planning must be put into this network design. Because the public Internet is involved, there is no guarantee that malicious activity can always be averted. Chris Brenton put it well in a System Administration, Network Security (SANS) conference for Track 2, “Business [security] is about accepting some levels of risk.” (FW_22_1303.mp3). GIAC Enterprises must accept this risk as offering public network services and traversing the public Internet is the bread and butter for GIAC Enterprises.

This section will first explore the business needs of GIAC Enterprises. Forget the technical aspects; what does GIAC need in order to have the capability to generate revenue?

Next, we explore the actual requirements to get the job done. Additionally, we will define what restrictions must be in place in order to ensure security as best can be done. As previously stated, there are no guarantees that the GIAC Enterprises’ network will be completely safe all the time. But, there is a lot that can be done to mitigate problems.

Finally, the hardware and configuration will be provided. This will include a networking scheme and specific hardware necessary to complete the project of designing and implementing a reliable network that utilizes defense-in-depth. Price comparisons came from Computer Discount Warehouse (http://www.cdw.com). David D. Scribner’s web site, (http://pages.prodigy.net/dscribner/pub/ip_address_classes.pdf) was very useful in determining the addressing scheme that would best suit GIAC Enterprises.

3.2 Business Requirements And Access Methods

3.2.1 Customers

GIAC Enterprises is an online retailer. Therefore, customers must have access to systems which allow them to view inventory, make secure purchases, and communicate with GIAC Enterprises Personnel.

Web browsers will be supported via HTTP and HTTPS. The ports used for this are TCP ports 80 and 443, respectively. Customers will browse products using HTTP; they will place orders and use the support features of ‘live chat’ using HTTPS. HTTPS will allow for secure transactions when placing orders and receiving technical support.

Email will be supported via SMTP using TCP port 25. This allows customers to contact GIAC Enterprises via email. It also allows GIAC Enterprises to email customers who have signed up to receive news and specials announcements.

3.2.2 Suppliers

GIAC Enterprises must purchase fortune cookie sayings from wholesalers in order to comprise the inventory for resale. This process is exactly like the relationship with its customers as in the section above, but it is in the opposite direction. GIAC Enterprises purchasing personnel must be able to access web servers hosted by wholesale fortune cookie saying providers.

Web browsers will be supported via HTTP and HTTPS. GIAC Enterprises employees must have outbound TCP ports 80 and 443 open in order to support this traffic.

Email will be supported for communication with suppliers as well. This requires that TCP port 25 be available for SMTP traffic.

3.2.3 Partners

GIAC Enterprises has several international business partners. These partners translate fortune cookie sayings and resell them. These business partners have a special relationship with GIAC Enterprises. In addition to HTTP, HTTPS, and SMTP traffic, these partners require the ability to query each other's databases and access each other's internal intranets.

Web browsers will be supported by HTTP and HTTPS. The ports again are 80 and 443.

Email will be supported by SMTP via TCP port 25.

A Virtual Private Network connection will be available for the business partners of GIAC Enterprises. This solution will allow business partners to query the company's inventory and translation system. Partners will be able to view the GIAC company intranet which is located on the company LAN by sending HTTP traffic across the established VPN connection.

3.2.4 GIAC Enterprises Employees on the Internal Network

Because GIAC Enterprises has limited resources for maintaining access control, most every protocol will be allowed for outbound traffic from employees on the internal network. If outbound traffic was completely locked down and exceptions made on an as needed and per protocol basis, it would take up too much time from the information systems personnel. There are some types of traffic, including specific protocols and specific IP address ranges which will be blocked at the border. These will be discussed in a later section as they will affect all traffic, not just traffic generated by employees on the internal network.

3.2.5 GIAC Enterprises Remote Offices

Connectivity to and from the GIAC Enterprises remote offices must be as seamless as possible. Basically, users in remote offices will need to have the same interfaces to the same systems as employees in the headquarters office. In order to achieve this, GIAC will take measures to provide high availability and high speed access to the core systems. Each branch office will have its own server for authentication, DNS, and DHCP. Additionally, they will have a server to provide file storage and the sales database system. Both servers will set up with RAID 5 configurations and contain dual power supplies. They will be backed up daily by a local tape backup. All domain controller information, DNS, DHCP, files, and databases will be replicated between the headquarters and branch offices in order to have synchronized information.

3.2.6 GIAC Enterprises Mobile Users

Mobile users will require access to information systems through several different means. Frequently, these employees are on the road and need to correspond with business partners and clients via email and phone conversations. In order to make this as convenient as possible, GIAC Enterprises will provide Exchange information via Outlook Web Access. This provides all employees with email, contacts, to-do lists, and all collaborative folders. In addition to this, there are times when mobile users require access to their sales system. This will require virtual private network (VPN) access, which will grant access to all systems as if the employee was logged into a computer which is directly connected to the company LAN.

Outlook Web Access will be provided by an Internet Security and Acceleration (ISA) server. This traffic will run via HTTPS over TCP port 443.

VPN access will be available for mobile users. This will allow mobile users to get information from the sales database server, the company intranet, all personal files, and anything else they would have while at the office.

3.2.7 The General Public

The general public will have very limited access to the system. Information regarding products and services as well as contact information will be available through the GIAC Enterprises web server. All other traffic will be prohibited until a member of the general public becomes a customer. In that case, they are granted a few more means for communication (see above).

Web traffic will be allowed from anywhere to the GIAC Enterprises' HTTP Proxy Server via TCP port 80.

3.3 Security Requirements And Restrictions

The following section details what security precautions will be necessary. The goal is to protect the GIAC Enterprises network as much as possible without being so restrictive that it imposes any problems with the flow of business.

Domain Name Service (DNS) is a concern that affects all categories defined in the security requirements. Each office will run an internal DNS server. This server will be the means for nodes in the LAN to locate each other. The DNS servers will also lookup Internet addresses by querying the upstream ISP's DNS server. However, GIAC Enterprises will not service DNS queries to anyone on the Internet. DNS is a big point of vulnerability, and GIAC will therefore not take the chance of hosting any public DNS servers. DNS entries will be left on the upstream ISP's server for the few services that are publicly available at GIAC Enterprises. The only pointers necessary are host (A) records and mail exchange (MX) pointing to the ISA server in order to allow Outlook Web Access and Email traffic. Additionally, there will be a host (A) record pointing to the HTTP proxy server for web service. The upstream ISP will have no other knowledge of the GIAC Enterprises LAN addressing.

3.3.1 Customers

Customers will be provided HTTP and HTTPS traffic from the HTTP proxy server. This server is placed in the Service Network. It relays web pages from the internal HTTP web server.

Email will be provided via SMTP from the Microsoft Internet Security and Acceleration Server. This server is placed in the Service Network. It relays all email traffic from the internal Exchange server.

3.3.2 Suppliers

Suppliers will provide access to their systems via HTTP and HTTPS traffic. Therefore, outbound traffic to web servers must be permitted for the GIAC Enterprises employees. For security, the firewall will provide a many-to-one network address translation (NAT) and stateful inspection services. This will cause all outbound web traffic to appear to come from one device and verify that the communication originated from within the GIAC Enterprises LAN.

Email will also be provided for communication with suppliers. Again, email will be routed from the internal MS Exchange server through the ISA server.

3.3.3 Partners

Business partners will need access to the GIAC Enterprises web server. This traffic will be provided by the HTTP Proxy Server in the service network.

Email will be provided through the ISA server as it is for everyone else.

VPN access will be granted by the SonicWall Firewall. The user account will be a GIAC Enterprises domain user which has limited permissions. These permissions will be fully restrictive, only granting access to necessary systems. This is because GIAC Enterprises will not be able to verify the security of the business partner's systems. It is up to the business partners to secure their own computer systems.

3.3.4 GIAC Enterprises Employees on the Internal Network

All outbound traffic which originates from a workstation within the GIAC Enterprises LAN and is destined for some machine on the Internet will have the address headers replaced by the address of the SonicWall Firewall. This is done by using a many-to-one NAT.

The firewall will also provide stateful inspection of all outbound traffic in order to verify that any traffic bound for an internal workstation is due to a request by that workstation.

There will be some global filtering which will affect traffic from employees on the internal network as well as all other types of traffic. Some of these filters will be placed on specific IP address and some will be placed on specific protocols.

Other than that, all outbound traffic which is generated by a workstation on the LAN will be permitted. It would be nice to set up the outbound permit rules on an as-needed basis, but GIAC Enterprises does not have the information systems manpower to maintain this. It will be left up to the firewall and router to filter any malicious traffic.

GIAC Enterprises will not be able to personally grant and deny all outbound traffic; this is why the GIAC Enterprises network will utilize defense in depth. Of course there will be maintenance necessary to ensure the perimeter is kept secure (reviewing logs, tweaking settings), but GIAC information systems employees cannot open a port for every time an employee needs a new type of access to an outside system.

3.3.5 GIAC Enterprises Remote Offices

For the branch offices to be fully connected to the headquarters office, a full-time VPN connection will be established. If one branch or headquarters loses its Internet connection, employees at the branch office can still work since they have everything they need replicated to local servers. Most of the time, full connectivity will be established. This will allow headquarters to gather all syslog and IDS entries from all office locations.

3.3.6 GIAC Enterprises Mobile Users

The Exchange Server located in the GIAC LAN will run Outlook Web Access. Defense in depth dictates that Exchange servers should not be directly accessible from the Internet. Therefore, a Microsoft ISA Server will publish OWA and will be located in the service network.

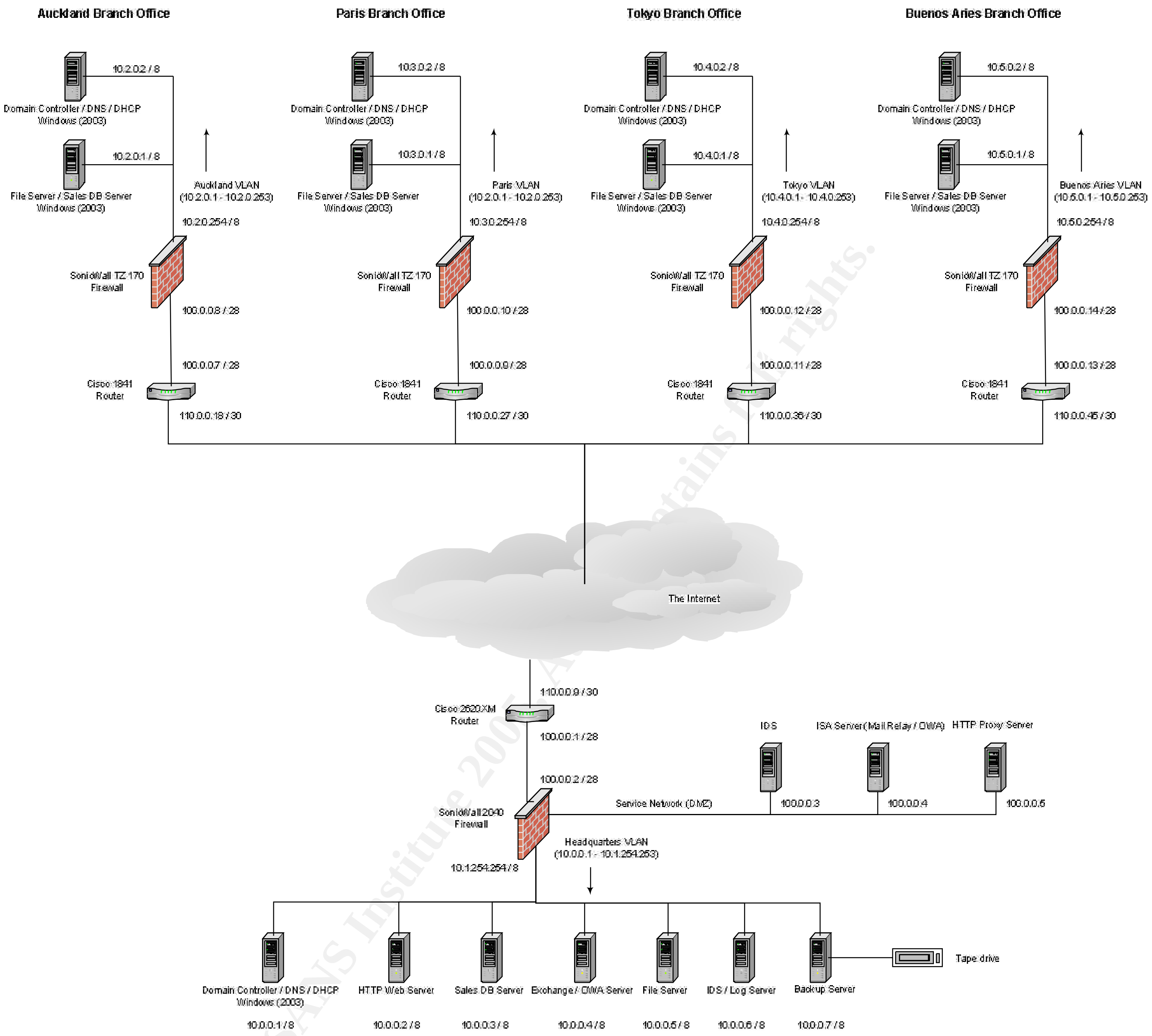
VPN access will be granted by the SonicWall Firewall. Mobile users will have full access to anything that they would have if they were directly connected to the LAN. Care must be taken to ensure that the mobile user's computer is secure. Therefore, GIAC Enterprises' policy will dictate that the only computers acceptable for VPN access are notebook computers that are issued by GIAC Enterprises. These notebook computers have the operating system, virus protection, personal firewall, and all other software loaded by GIAC Enterprises Information Systems personnel. Any notebook computer which has not been inspected by Information Systems personnel for more than a one month period of time will be revoked access to the GIAC network. This is to ensure that the notebook has the latest security patches and all other security measures are still functional. Strong passwords are required for all users, and this is enforced using Microsoft Group Policy. However, all employees which are granted VPN access will have their passwords regularly tested for strength using l0ftcrack (http://www.atstake.com/products/lc/).

3.3.7 The General Public

GIAC Enterprises does not allow direct access to any internal system from the Internet. Therefore, all web server communications will be routed through the HTTP proxy server. This server is located in the service network. In addition to the HTTP proxy server having its own security precautions, all traffic will first have to pass through the static filtering of the router and the stateful inspection system located on the SonicWall Firewall.

3.4 Network Architecture

3.4.1 IP Addressing Scheme



3.4.1.1 GIAC Headquarters

The GIAC Enterprises' headquarters in Durango, Colorado has a fairly simple addressing scheme. As with many aspects of its network design, it follows the 'keep it simple' format. It has been allocated the following public addresses: 100.0.0.0 / 28. This gives GIAC Enterprises 14 usable public IP addresses. For internal addressing, GIAC Enterprises has decided to use the following class A addressing scheme: 10.0.0.0 / 8. That allows for plenty of nodes on the LAN. The next hop to GIAC Enterprises headquarters' ISP is 110.0.0.2 and the external IP address of GIAC's router is 110.0.0.9 / 30.

110.0.0.9 / 30	Outside address of headquarters router
100.0.0.1 / 28	Inside address of headquarters router
100.0.0.2 / 28	Outside address of headquarters firewall
100.0.0.3 / 28	Intrusion Detection System
100.0.0.4 / 28	ISA Server (Publish OWA and mail relay)
100.0.0.5 / 28	HTTP Proxy Server
10.1.254.254 / 8	Inside address of headquarters firewall
10.0.0.1 – 10.1.254.253 / 8	Headquarters LAN Nodes

3.4.1.2 GIAC Enterprises Remote Offices

GIAC has four remote offices, each connecting to a different ISP. The IP addressing is distributed as follows:

3.4.1.2.1 Auckland, New Zealand Branch Office

This office uses the IP address assigned by its ISP for the external address of its router. It uses two of the public addresses from the GIAC class C subnet. For internal addressing, it is allocated 10.2.0.1 through 10.2.0.254. Note that the Auckland branch office has a different ISP than the headquarters office. This means that the outside address of the Auckland router uses a different IP/subnet than headquarters.

110.0.0.18 / 30	Outside address of Auckland router
100.0.0.7 / 28	Inside address of Auckland router
100.0.0.8 / 28	Outside address of Auckland firewall
10.2.0.254 / 8	Inside address of Auckland firewall
10.2.0.1 – 10.2.0.253 / 8	Auckland LAN Nodes

3.4.1.2.2 Paris, France Branch Office

This office uses the IP address assigned by its ISP for the external address of its router. It uses two of the public addresses from the GIAC class C subnet. For internal addressing, it is allocated 10.3.0.1 through 10.3.0.254.

110.0.0.27 / 30	Outside address of Paris router
100.0.0.9 / 28	Inside address of Paris router
100.0.0.10 / 28	Outside address of Paris firewall
10.3.0.254 / 8	Inside address of Paris firewall
10.3.0.1 – 10.3.0.253 / 8	Paris LAN Nodes

3.4.1.2.3 Tokyo, Japan Branch Office

This office uses the IP address assigned by its ISP for the external address of its router. It uses two of the public addresses from the GIAC class C subnet. For internal addressing, it is allocated 10.4.0.1 through 10.4.0.254.

110.0.0.36 / 30	Outside address of Tokyo router
100.0.0.11 / 28	Inside address of Tokyo router
100.0.0.12 / 28	Outside address of Tokyo firewall
10.4.0.254 / 8	Inside address of Tokyo firewall
10.4.0.1 – 10.4.0.253 / 8	Tokyo LAN Nodes

3.4.1.2.4 Buenos Aries, Argentina Office

This office uses the IP address assigned by its ISP for the external address of its router. It uses two of the public addresses from the GIAC class C subnet. For internal addressing, it is allocated 10.5.0.1 through 10.5.0.254.

110.0.0.45 / 30	Outside address of Buenos Aries router
100.0.0.13 / 28	Inside address of Buenos Aries router
100.0.0.14 / 28	Outside address of Buenos Aries firewall
10.5.0.254 / 8	Inside address of Buenos Aries firewall
10.5.0.1 – 10.5.0.253 / 8	Buenos Aries LAN Nodes

3.4.2 Filtering Routers

3.4.2.1 GIAC Enterprises Headquarters

There will be only one router for the Durango, Colorado headquarters. It will be used for basic packet filtering and Internet routing. It is a Cisco 2620XM. This router will give high performance and is designed for flexibility.

If GIAC Enterprises decides in the future to set up a different or alternate route to the Internet, this router can easily add that functionality by simply adding a card and modifying the router's configuration. The cost of the router is $1,538.44.

This filter will perform static packet filtering. It will perform egress filtering by only permitting the 100.0.0.0 / 28 address space to leave the perimeter. Keep in mind that the private addresses (10.0.0.0 / 8) will use NAT at the firewall to obtain a public address before leaving the network. For ingress filtering, this filter will block all incoming private IP addresses as well as the loopback address. Additionally, it will block source routed packets, telnet, SSH, NetBIOS, SMB, DNS, syslog, TFTP, and SNMP traffic. GIAC will not be able to block specific countries from having access to the service network as it is a global online enterprise.

3.4.2.2 GIAC Enterprises Remote Offices

All branch offices will utilize a Cisco 1841 router. These cost $1,099.00 each. According to Cisco, the "Cisco 1800 Series Integrated Services Router is optimized for data-access applications, providing small-to-medium sized businesses and small branch offices with the complete functionality and flexibility to deliver secure Internet and Intranet access." (http://www.cisco.com/en/US/products/ps5853/index.html) The border routers at CIAC branch offices will have the same static packet filtering configuration as the headquarters router. This includes both ingress and egress filtering.

3.4.3 Firewalls

3.4.3.1 GIAC Enterprises Headquarters

Which firewall will support the GIAC headquarters is an important decision. Cost is a factor, but much more important than that is coming up with a firewall that is easy to install, configure, and maintain. Providing robust security is also very important. Furthermore, GIAC has decided to use a different vendor for its firewalls than the provider of other networking equipment. This reduces the chance that an attacker can use the flaw in one vendor's implementation in order to traverse multiple layers of defense.

In order to require the least burden on GIAC Information Systems staff, a hardware solution is the most desirable. A stateful packet inspection SonicWall 2040 has been chosen for this solution. It costs $1,488.49. SonicWall has a good track record for security and has an easy to manage interface. The configuration of this firewall will be discussed in a future section.

3.4.3.2 GIAC Enterprises Remote Offices

In order for consistent management, GIAC will also implement SonicWall firewalls at each branch office. The chosen model is the $399.54 SonicWall TZ 170. This is a stateful packet inspection firewall that will work fine for branch offices. Again, it leverages the fact that the static packet filtering router is provided by a different vendor than the firewall. This makes good practice for defense-in-depth.

3.4.4 VPN

Virtual private networking will be provided by the GIAC headquarters firewall (SonicWall 2040). This solution is simple and effective. It does not present the problem of a 'back door' into the network without going through the firewall.

3.4.4.1 Business Partners

VPN connectivity will be granted to business partners. Because there is no way to enforce the security of business partners, the domain account used by business partners will be very restrictive, only granting access to required systems as described in sections 3.2.3 (Business Requirements and Access Methods – Partners) and 3.3.3 (Security Requirements and Restrictions – Partners).

3.4.4.2 GIAC Enterprises Mobile Users

All GIAC employees which use the available VPN connection will do so by using a GIAC issued notebook computer. GIAC Policy stipulates that VPN enabled notebook computers will be securely configured as described in section 3.2.6 (Security Requirements and Restrictions – GIAC Enterprises Mobile Users).

3.4.4.3 GIAC Enterprises Remote Offices

All communication between branch offices and headquarters will be sent over the Internet. Therefore, VPN connections are required for secure communication.

3.4.5 Intrusion Detection System

Network based intrusion detection systems (IDS) will be set up on the headquarters service network and the headquarters LAN. These systems will monitor traffic and alert GIAC Enterprises information systems personnel when it detects network traffic anomalies. The brand chosen for this is Snort (www.snort.org).

3.4.5.1 GIAC Enterprises Headquarters' Service Network

The service network IDS will be concerned with monitoring the GIAC Enterprises' public servers, namely the mail relay / Outlook Web Access proxy, and the HTTP proxy server. Since these systems have a very small variety of tasks, training Snort what is 'normal' will be easy.

3.4.5.2 GIAC Enterprises LAN

There will be a second Snort IDS placed as a node on the headquarters LAN. Because the remote offices are also part of the same LAN (thanks to VPN), it will only be necessary to have one IDS for all four offices.

3.5 Conclusion

As previously mentioned, there is no way to guarantee complete security of a network short of 'pulling the wire'. The network security architecture outlined in this section meets the goals as best possible. It is as simple as possible, while providing all the functionality that is required. It utilizes defense-in-depth and will hold up to many types of attacks.

4 Assignment 3: Firewall Policy

4.1 Introduction

This section lists specific commands and configuration options for the perimeter security hardware that will be used by GIAC Enterprises. The company will have one border router and one firewall at its headquarters location and at each branch office. High security and high performance are the two goals of this configuration.

Many of the concepts came from multiple sources. One of the sources that provided valuable assistance was an education and research group in the United Kingdom called JANET (http://www.ja.net/CERT/JANET-CERT/prevention/cisco/private_addresses.html).

4.2 Routers

The Cisco routers at the headquarters and branch offices will perform much of the firewall duties by means of static packet filtering. Because this technology is simple, it is less likely to have accidental mis-configuration or filter incorrectly. The headquarters router and all branch office routers will use the exact same configuration.

To begin with, there are some global configuration settings to be made. We must block source routed packets and disable the finger protocol.

```
no ip source-route
no ip finger
```

A warning will be issued to anyone who logs into one of the routers in order to view or modify its configuration.

```
banner motd #
************************************************************
               !!!!Notice!!!!
************************************************************

This system is restricted to authorized individuals.

Unauthorized access is a criminal violation of the law and is subject to
prosecution.
```

```
All connections and changes will be logged.

************************************************************
              !!!!Notice!!!!
************************************************************
#
```

Additionally, the password used to log into the routers will be encrypted.

```
service password-encryption
```

4.2.1 Egress (Outbound traffic)

The first rule to be applied to the internal interface of the router is to block specific protocols. These are traffic types which are not allowed in any direction. They are NetBIOS, SMB, syslog, POP-3, TFTP, and SNMP. Thanks to Arne Vidstrom (http://ntsecurity.nu/papers/port445) for input on port assignments for SMB.

```
access-list 101 deny tcp any any range 135-139
access-list 101 deny udp any any range 135-139
access-list 101 deny tcp any any 445
access-list 101 deny udp any any 514
access-list 101 deny tcp any any 110
access-list 101 deny udp any any 69
access-list 101 deny udp any any 161
access-list 101 deny udp any any 162
```

The next outbound filter will block echo replies and destination unreachables. This will assist with thwarting attempts to map the GIAC Enterprises' network. Unfortunately, an attacker can map the border router by using traceroute or firewalk; but the good thing is they can not map any farther than the router itself. They will not make it to the firewall or beyond.

```
access-list 101 deny icmp any any echo-reply unreachable
```

The next filter will be applied to the internal interface of the router which only permits the source IP address space of 100.0.0.0 / 28 to pass. This will prevent any traffic from getting out which has a source IP address of an internal host that was not successfully NAT'd at the firewall. It will also prevent any traffic with a spoofed address from leaving the network.

```
access-list 101 permit 100.0.0.0 0.0.0.15
```

Finally, we block all other traffic. We will log any packets that match this and will record the media access control (MAC) address since any rule that makes it to the explicit deny will probably have a spoofed or otherwise incorrect address.

access-list 101 deny any log-input

This type of traffic is very suspect, and therefore all egress filtering will be logged. The order of these rules is important. The first few rules will block specific types of traffic no matter which device is sending them. Following that, access is granted from approved internal nodes. All other traffic is explicitly denied. Rearrangement of these rules would definitely compromise the strength of this rule base. For instance, if the permit statement preceded the rule to block NetBIOS traffic, any internal node could potentially leak out information that would be very valuable to a malicious entity on the Internet.

4.2.2 Ingress (Inbound Traffic)

A filter will be applied to the external interface of the router which will first block all incoming private IP addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). It will also block the loopback address (127.0.0.1). This access control list will be checked first as it is the simplest for the router. This will help to prevent traffic from other routers that are configured incorrectly. In addition, it will help prevent DoS attacks.

access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 172.16.0.0 0.15.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 deny ip 127.0.0.0 0.255.255.255 any

The next rule is one of the few that is different for the different GIAC Enterprises locations. This rule blocks incoming traffic with a source address of a node 'inside' of the router. So, the headquarters router will filter any packets with a source address of 100.0.0.1/28 through 100.0.0.5/28. The Auckland branch office router will filter 100.0.0.7 and 100.0.0.8. The other branch offices will follow the Auckland model. This prevents an attacker from spoofing the public address of any of the GIAC Enterprises' servers, routers, or firewalls.

Headquarters (this could be done with fewer commands, but it is harder to read)
access-list 102 deny host 100.0.0.1 any
access-list 102 deny host 100.0.0.2 any
access-list 102 deny host 100.0.0.3 any
access-list 102 deny host 100.0.0.4 any
access-list 102 deny host 100.0.0.5 any

Auckland branch
access-list 102 deny host 100.0.0.7 any

```
access-list 102 deny host 100.0.0.8 any
```

Paris branch

```
access-list 102 deny host 100.0.0.9 any
access-list 102 deny host 100.0.0.10 any
```

Tokyo branch

```
access-list 102 deny host 100.0.0.11 any
access-list 102 deny host 100.0.0.12 any
```

Buenos Aries branch

```
access-list 102 deny host 100.0.0.13 any
access-list 102 deny host 100.0.0.14 any
```

The next rule to be applied to the external interface of the router is to block specific protocols. These are traffic types which are not allowed in any direction. They are NetBIOS, SMB, syslog, POP-3, TFTP, and SNMP.

```
access-list 102 deny tcp any any range 135-139
access-list 102 deny udp any any range 135-139
access-list 102 deny tcp any any 445
access-list 102 deny udp any any 514
access-list 102 deny tcp any any 110
access-list 102 deny udp any any 69
access-list 102 deny udp any any 161
access-list 102 deny udp any any 162
```

Finally, telnet and SSH coming into the router will be blocked to keep people on the Internet from attempting to log into the router. Then, everything else is permitted. This is only allowed since the router is only the first line of defense and is not the only filtering device.

```
access-list 102 deny tcp any any 23
access-list 102 deny tcp any any 22

access-list 102 permit any any
```

It is important that this rule set be applied to the external interface of the router. This is because we want the router to be able to send logs to the log server in GIAC headquarters. If it was applied to the internal interface, it would filter out its own logs.

The order of the ingress rules is not important, with the exception of the last rule. It needs to be at the end; otherwise any subsequent deny statements would never be processed.

4.3 Firewalls

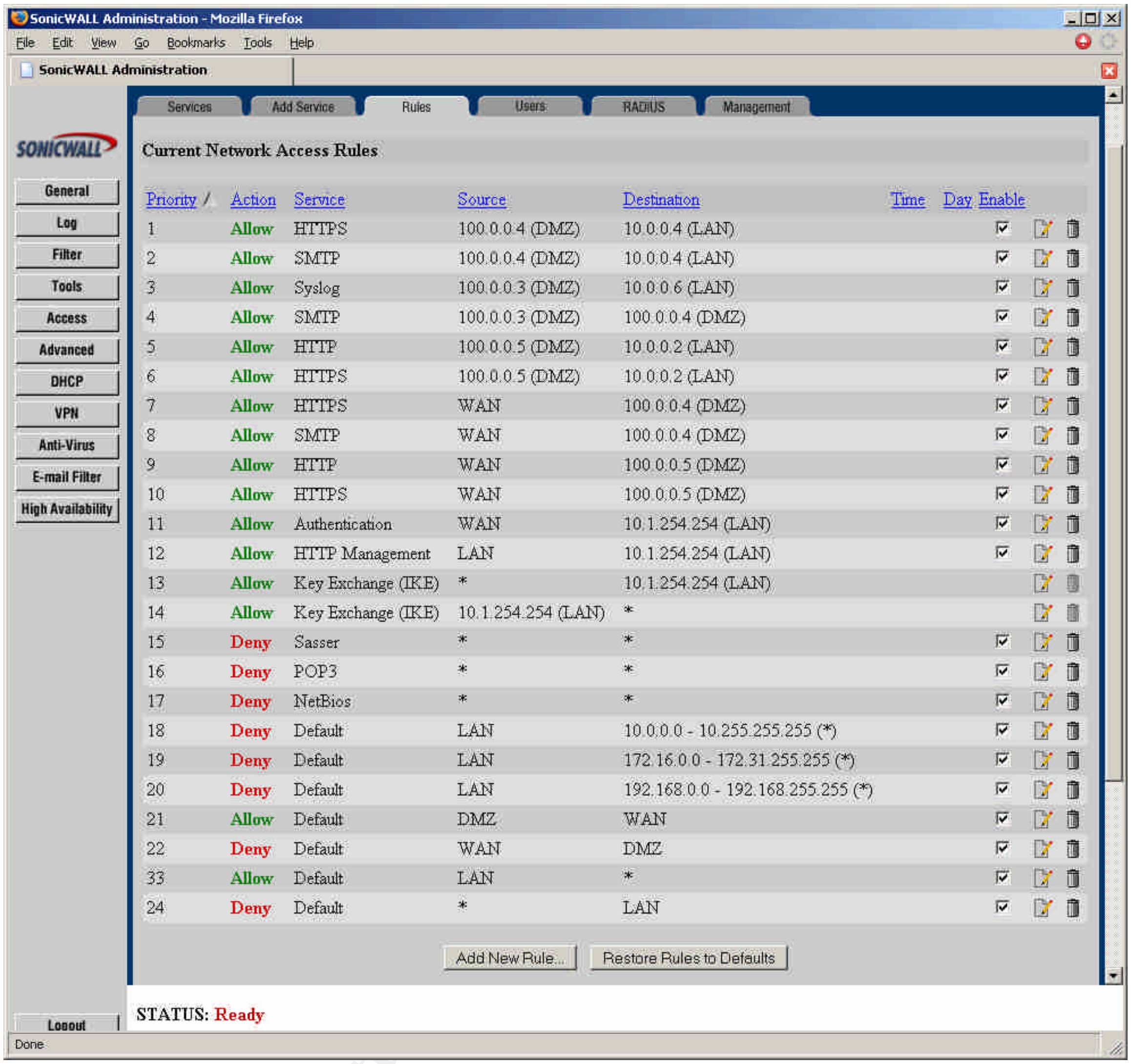
The SonicWall firewalls provide stateful inspection packet filtering. This technology will be utilized to lock down traffic on a more advanced level than the static filter that the routers provide. Both types are necessary, and compliment each other. One of the features of the SonicWall as a brand is its ease of installation and configuration. From the factory, the SonicWall firewalls will block and log the following: Syn flood, Ping of death, IP Spoofing, Land attack, Smurf amplification, and sequence number prediction. It will also use 'stealth mode' which will make reconnaissance more difficult for attackers.

In addition to the default security measures, POP-3, Sasser, and NetBIOS are all explicitly denied on the firewalls in all directions. The configuration will also explicitly block all incoming private IP addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) and the loopback address (127.0.0.1).

Finally, the implicit deny will be added explicitly to the end of the firewall rule base. This denies all traffic that has not matched another rule coming into the DMZ or LAN.

A view of the actual firewall configuration will be shown in each of the following sections. Some of the entries are the same for the headquarters firewall and branch offices, and some are different.

4.3.1 Headquarters Firewall Configuration



Current Network Access Rules

Priority /	Action	Service	Source	Destination	Time	Day	Enable
1	Allow	HTTPS	100.0.0.4 (DMZ)	10.0.0.4 (LAN)			☑
2	Allow	SMTP	100.0.0.4 (DMZ)	10.0.0.4 (LAN)			☑
3	Allow	Syslog	100.0.0.3 (DMZ)	10.0.0.6 (LAN)			☑
4	Allow	SMTP	100.0.0.3 (DMZ)	100.0.0.4 (DMZ)			☑
5	Allow	HTTP	100.0.0.5 (DMZ)	10.0.0.2 (LAN)			☑
6	Allow	HTTPS	100.0.0.5 (DMZ)	10.0.0.2 (LAN)			☑
7	Allow	HTTPS	WAN	100.0.0.4 (DMZ)			☑
8	Allow	SMTP	WAN	100.0.0.4 (DMZ)			☑
9	Allow	HTTP	WAN	100.0.0.5 (DMZ)			☑
10	Allow	HTTPS	WAN	100.0.0.5 (DMZ)			☑
11	Allow	Authentication	WAN	10.1.254.254 (LAN)			☑
12	Allow	HTTP Management	LAN	10.1.254.254 (LAN)			☑
13	Allow	Key Exchange (IKE)	*	10.1.254.254 (LAN)			
14	Allow	Key Exchange (IKE)	10.1.254.254 (LAN)	*			
15	Deny	Sasser	*	*			☑
16	Deny	POP3	*	*			☑
17	Deny	NetBios	*	*			☑
18	Deny	Default	LAN	10.0.0.0 - 10.255.255.255 (*)			☑
19	Deny	Default	LAN	172.16.0.0 - 172.31.255.255 (*)			☑
20	Deny	Default	LAN	192.168.0.0 - 192.168.255.255 (*)			☑
21	Allow	Default	DMZ	WAN			☑
22	Deny	Default	WAN	DMZ			☑
33	Allow	Default	LAN	*			☑
24	Deny	Default	*	LAN			☑

STATUS: Ready

At the headquarters office, there are rules to be applied to the interface which supports the service network. These are rules 1 through 10 as shown above.

Rules 1, 7: HTTPS will be allowed from the WAN to the DMZ IP address 100.0.0.4. HTTPS will be allowed from the DMZ IP address 100.0.0.4 to the Exchange Server on the LAN. This will allow GIAC Enterprises employees to interface with Outlook from anywhere in the world via Outlook Web Access.

Rules 2, 8: SMTP will be allowed from the WAN to the DMZ IP address 100.0.0.4. SMTP will be allowed from the DMZ IP address 100.0.0.4 to the Exchange Server on the LAN. This will allow sending and receiving email. Because the email is run through this proxy, it will protect the Exchange server which houses the actual email and other Outlook information.

Rules 3 - 4: Syslog will be allowed from the DMZ IP address 100.0.0.3 to the IDS / Log server on the LAN. SMTP will be allowed from the DMZ IP address

100.0.0.3 to the DMZ IP address 100.0.0.4. This will allow log entries from the IDS system on the service network to be sent to the central logging system on the GIAC Enterprises LAN. Additionally, alerts will be relayed from the service network IDS through the service network mail relay. That way, alerts can be emailed immediately to the network administrator.

Rules 5, 6, 9, 10: HTTP and HTTPS will be allowed from the WAN to the DMZ IP address 100.0.0.5. HTTP and HTTPS will be allowed from the DMZ IP address 100.0.0.5 to the HTTP Web Server on the LAN. This sets up a proxy for web traffic in order to support the GIAC Enterprises web site, which includes the SSL sales system.

Rules 11 - 14: These allow authentication and management via web browser. The firewall can only be configured from a machine with a private internal IP address. This also facilitates VPN connections from anywhere by using IKE.

Rules 15 - 17: This explicitly denies traffic generated by the Sasser worm (TCP 5554 and 9996), POP-3 email (TCP 110), and NetBIOS (TCP and UDP 135-139) from moving anywhere across the firewall.

Rules 18 - 20: This explicitly prevents any local traffic bound for a private IP addresses.

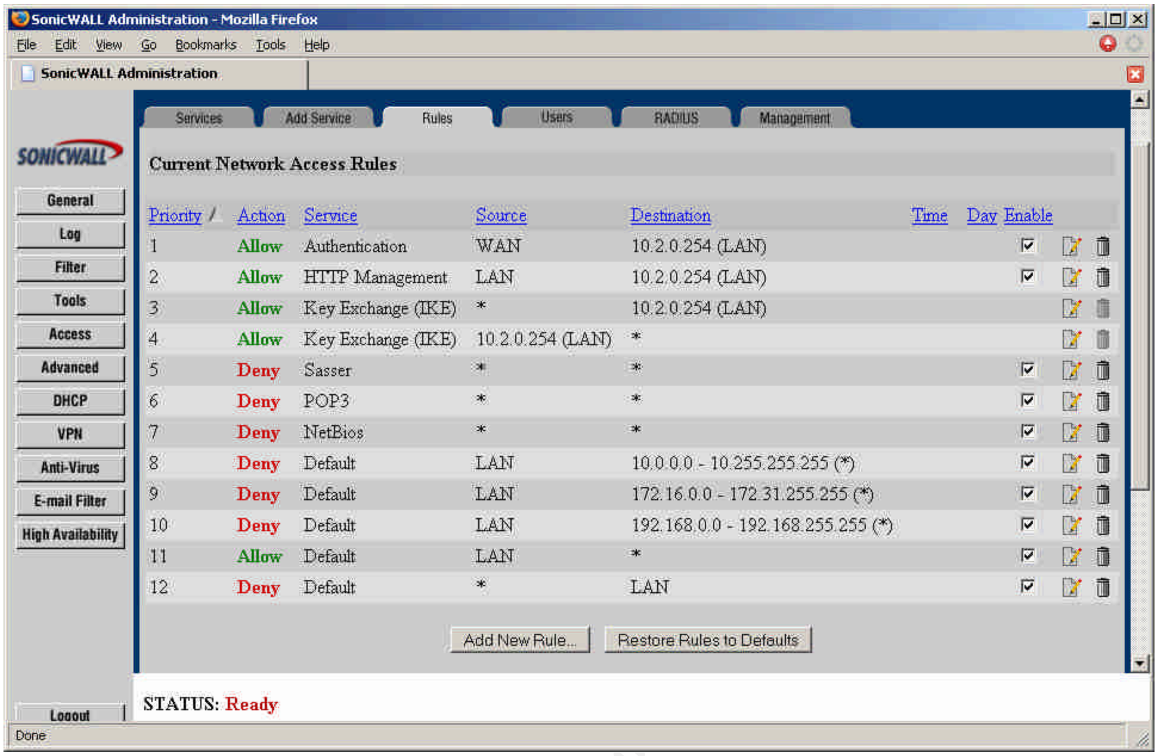
Rules 21: This allows any other traffic generated by a system in the DMZ to access other nodes on the Internet. This will save the trouble of reconfiguring the firewall if, for instance, a machine on the DMZ needs to get to the Internet for a software update.

Rule 22: All traffic from the Internet which is bound for a server in the service network is blocked once it reaches this rule. Any legitimate traffic bound for the service network is permitted in a prior rule.

Rule 23: This allows all other types of traffic out to the Internet. If a particular type of traffic causes problems, it will be added to a rule which will block it, similar to rules 15 – 17.

Rule 24: This is the explicit deny, which blocks all inbound traffic that was not requested by a machine inside the GIAC Enterprises LAN.

4.3.2 GIAC Enterprises Remote Offices



Current Network Access Rules

Priority	Action	Service	Source	Destination	Time	Day	Enable
1	Allow	Authentication	WAN	10.2.0.254 (LAN)			☑
2	Allow	HTTP Management	LAN	10.2.0.254 (LAN)			☑
3	Allow	Key Exchange (IKE)	*	10.2.0.254 (LAN)			
4	Allow	Key Exchange (IKE)	10.2.0.254 (LAN)	*			
5	Deny	Sasser	*	*			☑
6	Deny	POP3	*	*			☑
7	Deny	NetBios	*	*			☑
8	Deny	Default	LAN	10.0.0.0 - 10.255.255.255 (*)			☑
9	Deny	Default	LAN	172.16.0.0 - 172.31.255.255 (*)			☑
10	Deny	Default	LAN	192.168.0.0 - 192.168.255.255 (*)			☑
11	Allow	Default	LAN	*			☑
12	Deny	Default	*	LAN			☑

STATUS: Ready

Rules 1 - 4: These allow authentication and management via web browser. The firewall can only be configured from a machine with a private internal IP address. This also facilitates VPN connections from anywhere by using IKE.

Rules 5 - 7: This explicitly denies traffic generated by the Sasser worm (TCP 5554 and 9996), POP-3 email (TCP 110), and NetBIOS (TCP and UDP 135-139) from moving anywhere across the firewall.

Rules 8 - 10: This explicitly prevents any local traffic bound for a private IP addresses.

Rule 11: This allows all other types of traffic out to the Internet. If a particular type of traffic causes problems, it will be added to a rule which will block it, similar to rules 15 – 17.

Rule 12: This is the explicit deny, which blocks all inbound traffic that was not requested by a machine inside the GIAC Enterprises LAN.

4.4 Conclusion

With multiple layers of perimeter protection as provided by the Cisco routers and SonicWall firewalls, GIAC Enterprises will maintain a robust outer defense. Besides high security and high performance, the configuration also allows for ease of use and high availability.

5 References

Network Magazine. “Strategies & Issues: Thwarting Insider Attacks”. URL:http://www.networkmagazine.com/article/NMG20020826S0011 (4 September, 2002)

Brenton, Chris and The SANS Institute. (http://www.sans.org). “SANS GCFW training”. Defense In-Depth, module 2.4.

Scribner, David. “IP Address Classifications”. URL:http://pages.prodigy.net/dscribner/pub/ip_address_classes.pdf (21 September, 2003)

Cormack, A with JANET (http://www.ukerna.ac.uk/). “Traffic which should be blocked by routers”. URL:http://www.ja.net/CERT/JANET-CERT/prevention/cisco/private_addresses.html (17 July 2001)

Vidstrom, Arne. “The use of TCP port 445 in Windows 2000”. URL:http://ntsecurity.nu/papers/port445. (20 November, 2000)

Computer Discount Warehouse. Power over Ethernet. LAN/WAN, pages 10-24. Security, pages 28-33. November, 2004 Issue.

Cisco Systems. “Cisco 1800 Series Routers”. URL: http://www.cisco.com/en/US/products/ps5853/index.html. (16 September, 2004)

Roesch, Marty. “Snort.org” URL:http://www.snort.org/ (20 November, 2004)

Lammle, Todd. Cisco Certified Network Associate Study Guide. Alameda, CA: Sybex, Inc, 2002. 464 - 477.