Global Information Assurance Certification Paper

GIAC Firewall and Perimeter Protection Curriculum

Practical Assignment

James McMahon

Contents

Conventions Used in this Document

1. All IP addresses have the leading two octets represented by xxx.xxx to protect the privacy of the systems used. For example, if a system's IP address is 10.20.30.40 then it would appear in this document as xxx.xxx.30.40.
2. Unless otherwise specified, all UNIX commands liste d are for the Solaris operating system and are assumed to have been run with root privilege if required.
3. Any router commands given are for Cisco routers.

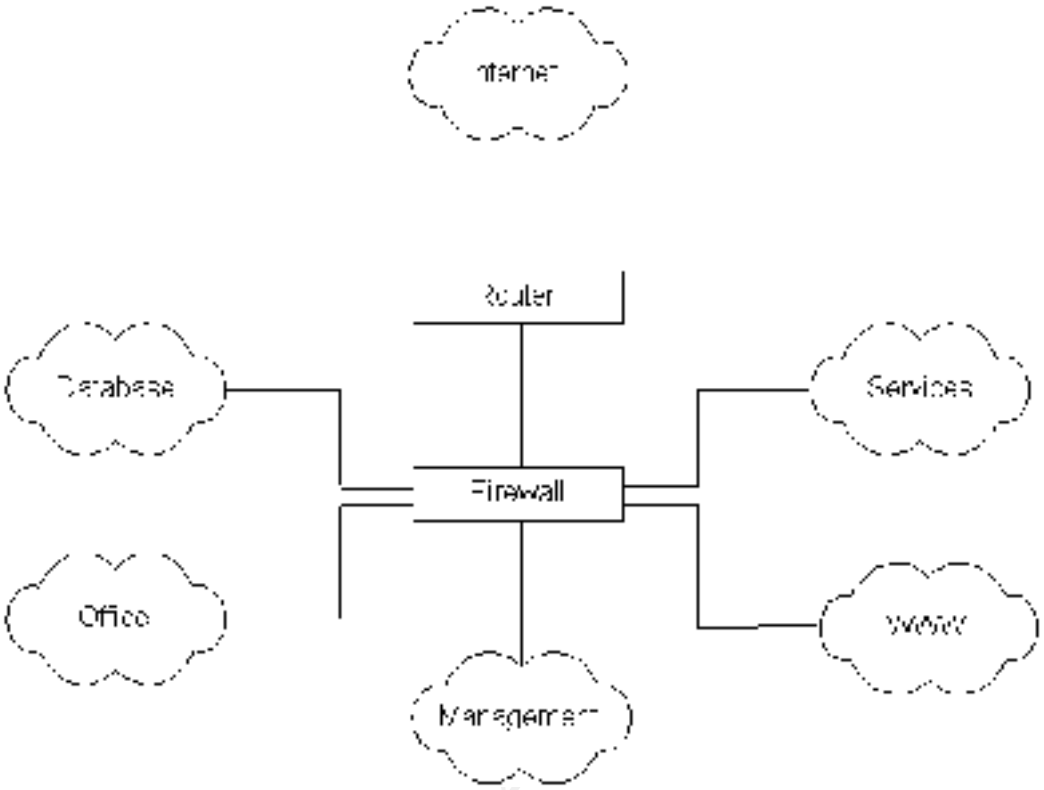
Assignment 1: Security Architecture

Define a security architecture. The goal of your policy is to use filtering routers, firewalls, VPNs and internal firewalls to rapidly implement the VISA "Ten Commandments" to the extent possible at GIAC Enterprises, a new Internet Startup that expects to earn 200 million per year in sales of online fortune cookie s ayings. The "Ten Commandments" are listed below:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up -to-date.
3. Encrypt stored data accessible from the Internet
4. Encrypt data sent across netw orks
5. Use and regularly update anti -virus software.
6. Restrict access to data by business "need to know".
7. Assign unique ID's to each person with computer access to data.
8. Track access to data by unique ID.
9. Don't use vendor supplied defaults for system password s and other security parameters.
10. Regularly test security systems and processes.

The student assignment is to produce a diagram, or set of diagrams with explanatory text defining how to us perimeter technologies to implement as many of the requirements abo ve as possible. For this assignment you are a large and growing E - business that just completed a merger/acquisition. You must consider the need for customers, suppliers, and partners.

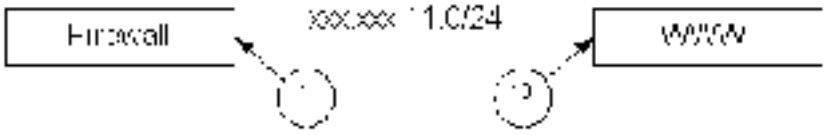
Entire Network



Notes:

1. The main components of the perimeter protecti on are the filtering router and the firewall.
2. Extra protection is provided by utilizing private address space (RFC 1918) for all services located behind the firewall except public services such as email and DNS, which are located on the Service network, an d utilizing the firewall's ability to translate addresses. This makes it harder for people to route packets to the service networks attached to the firewall in the event that the firewall service is disrupted in some way.
3. The external router is used with basic filters to block the most obvious of unwanted packets from the Internet, and also to prevent unwanted packets being transmitted to the Internet from the internal network of GIAC Enterprises. These filters include:
    a. Incoming filters to block all "spo ofed" packets arriving on the external interface. Packets are assumed to be "spoofed" if they have source addresses that are defined as private address space by RFC 1918 or source addresses that belong to GIAC Enterprises.
    b. Incoming filters to block all co nnections to the routers telnet port except those originating from the translated address range of the management network.
    c. Incoming filters to block all source routed packets.

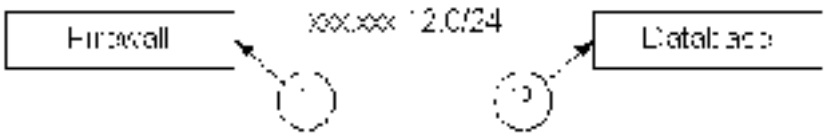
WWW Network



Notes:

1. The web server is managed using the address xxx.xxx.11. 10 as shown in the diagram above. Management is done via an SSH connection from the management network. SSH access is controlled by the firewall and also by the web servers SSH configuration. The root user is not allowed to login directly via SSH. All users must login using their personal identifiers.
2. The public web server is hosted on a separate IP address located on the same physical host.
3. The firewall is configured to accept and translate connections to the web server's virtual IP address on TCP Port 80 (HTTP) and TCP Port 443 (SSL) only.
4. Public access to the web server is via HTTP, however no information is sent to or from the web server via the Internet until a session has been established using HTTPS. This prevents potentially private information being transmitted over public networks in clear text.
5. The web server is configured to talk to the database server through the firewall. An appropriate filter rule is in place on the firewall to allow this communication that utilizes TCP Port 1521 (Oracle) .
6. The web server is running on a "hardened operating system" with the minimum packages required for execution of the web server installed, and with only required services listening on TCP or UDP ports. All other services have been removed from the server. All non-essential software has been removed from the server.
7. The web server is the only host on this subnet. This is because a web server is a high profile, and relatively easy to compromise target. If the web server is compromised, all other hosts on the subnet then have no protection from the firewall as local subnet communication is always possible, and hence no other hosts will be left on this subnet.

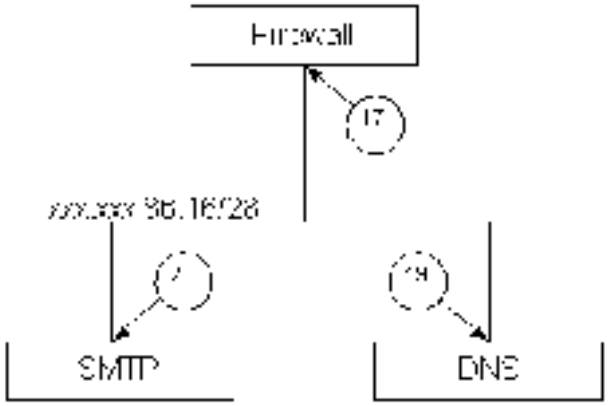
Database Network



Notes:

1. The database server is managed using an SSH session from the manageme nt network. This encrypts the session to prevent unauthorized access to data by session snooping.
2. The SSH server on the database is configured to only accept connections originating in the management network
3. The SSH server on the database is configured to deny the root user permission to login. Users must login using their unique login identifier and then use the "su" program to gain privileged access.
4. Incoming connections to the database software are accepted from the web server and from the internal off ice database server only.
5. The database server is running on a hardened operating system and is listening only on TCP Port 22 (SSH) and TCP Port 1521 (Oracle). All other unnecessary software and services have been removed from the operating system.
6. Data requested from the web server is transmitted over an unencrypted session. The sniffing of this data would require the compromising of either the firewall or the web server. If the firewall is compromised, then I expect all other boxes to be compromised. I f the web server is compromised, then queries can be directed to the database from the web server to obtain information directly. The risk of not having an encrypted session between the web server and the database server is significantly outweighed by the ability to use the firewall to control non -encrypted traffic.
7. The web server ensures that all information to be transmitted over public networks is first encrypted.

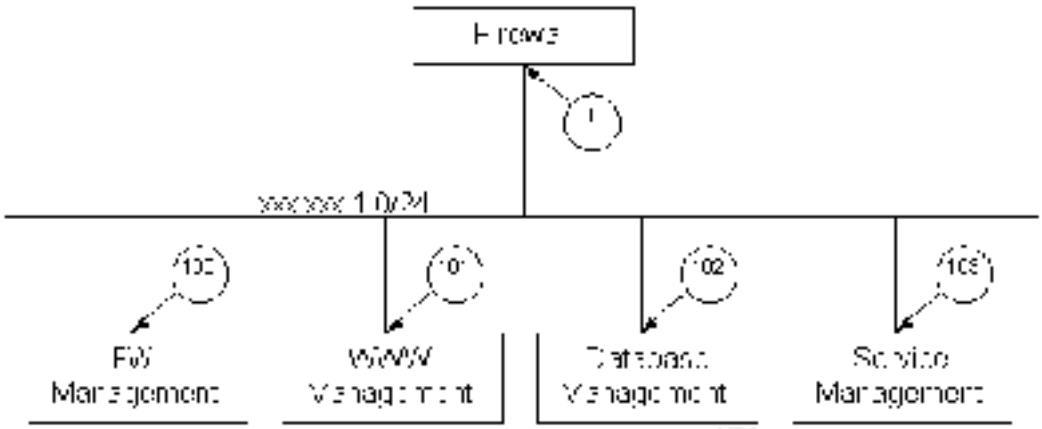
Service Network



Notes:

1. The DNS server is running bind version 8.2.2pl5. I am awar e that bind 8.2.2pl7 has been recently released and that it fixes a DOS attack that requires permission to perform a zone transfer. The DNS server is configured to allow zone transfers from the secondary DNS servers and as these are all trusted servers, a lower sense of urgency has been placed on the application of this patch.
2. The SMTP server is running sendmail version 8.9.3.
3. All boxes on this segment are running hardened operating systems with no unnecessary services or software available in order to nar row the number of possible compromises available.
4. The firewall is configured to allow management of both the DNS and SMTP servers using SSH from within the management network. All administrators must login using their unique login identifier for audit pur poses. The root user is not allowed to login directly using SSH.
5. The firewall allows incoming connections on TCP Port 25 (SMTP) to the SMTP server from any source.
6. The firewall allows incoming connections on UDP Port 53 (Domain) to the DNS server from any source, however connections on TCP Port 53 (Domain) are denied from all locations except for the secondary domain servers. This helps to prevent zone transfers for the zones hosted on the DNS servers as zone transfers are typically too large to complete using a UDP transfer.
7. The SMTP server is configured to relay mail destined for or received from internal hosts and domains only in order to prevent "spam" email.
8. Virus checking of email messages is not performed on the external mail server. This is left f or mail servers located closer to the final point of delivery.

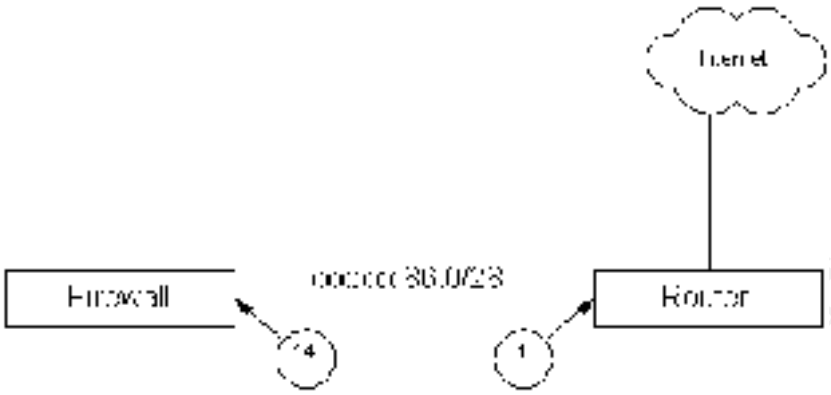
Management Network



Notes:

1. Each area of the network is managed from a separate system in the management network. This allows the restriction of access to individual systems by restricting access to the management system to those authorized to manage the external system.
2. The FW Management system is also responsible for the log management of the firewall. All other logs are stored locally.
3. In order to manage a segment, an administrator mu st first login to the relevant management system, then run the appropriate management software (SSH, FW-1 Manager), then connect to the relevant system and authenticate a second time using their unique identifier. This second authentication reduces the chance of a management system being used by an unauthorized person if it is left unattended.
4. System passwords for the obtaining of privileged access are different on all server types. ie. The root password is different on the web server and the database server.

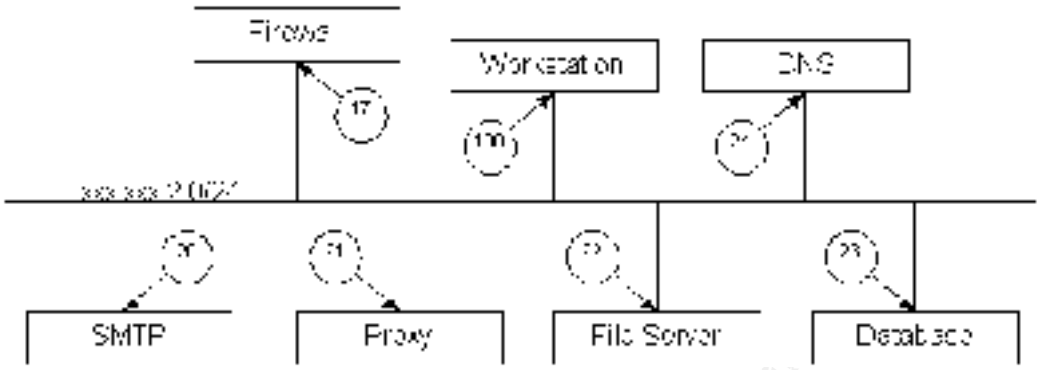
Backbone Network



Notes:

1. The router is protected from unauthorized access using the following methods:
    a. telnet connections to the router are limited to the internal interface.
    b. Ingress and Egress ACLs are in place to prevent spoofed packets from entering or leaving the protected network.
    c. Source routed packets are prevented from entering or leaving the network.
    d. Small services are disabled.
    e. Finger is disabled.
    f. Password encryption is enabled.
    g. A login banner is installed.
    h. The firewall prevents access to the routers telnet daemon from unauthorized hosts.
2. The firewall is protected as follows:
    a. The firewall is running on a hardened operating system installed with the minimum set of packages required to run the software.
    b. The firewall is using Checkpoint Fi rewall-1 Version 4.0 software.
    c. The firewall is configured to block packets on system startup until the firewall software is fully operational.
    d. The firewall is configured with IP Forwarding disabled unless the firewall software is fully operational.
    e. The firewall will accept management connections from the appropriate system on the management network only.
    f. All system access to the firewall is from the console
    g. All users must login using their unique identifier first, and then assume a privileged level of acces s if required.
    h. No services are running on the firewall except the firewall software itself. The firewall acts purely as a packet filtering device.
    i. The default fwadmin login used for Firewall -1 administration access has been removed and all administrators have their own personal identifiers to use when administering the firewall.

Office Network



Notes:

1. All office email must be relayed through the office email server. This server will provide email content scanning for viruses using Trend Micro Intersc an Virus Wall.
2. Files are able to be transferred from the office file server to the management network hosts using SSH. This transfer must be originated from the management network.
3. Office workstations are allowed access to Internet services such as web browsing and FTP but must do so using the office proxy server.
4. All office hosts utilize the office DNS server which forwards requests to the external DNS server.
5. The office Database server is required to communicate with the external database server for upda tes.

Assignment 2: Security Policy

For the purposes of this assignment, your security policy should be focused on implementation of requirement number 1 above "Install and maintain a working network firewall to protect data accessible via the Intern et". For a baseline policy, use the filtering recommendations located at www.sans.org/topten.htm . You DO NOT need to repeat that information. Instead, focus on ADDITIONAL filtering you would recommend and why. Keep in mind that you are an E -Business with customers, suppliers, and partners. You MAY NOT simply block everything! Your policy should implement your design above.

Write a tutorial on how to implement each additional recommended action in the filtering policy below on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. The base policy is taken from the recommended perimeter defense actions in the "Top Ten" document. Screenshots, network traffic traces, firewall log information and URLs to find further information should all be used. Be certain to include the following:

1. The reason these services might be considered a vulnerability
2. Relevant information about the behavior of the protocol or service on the network
3. Syntax of the filter
4. Description of each of the parts of the filter
5. Explain how to apply the filter
6. If this filter is order dependant, what other rules should this filter precede and follow
7. Explain how to test the filter
8. Be certain to point out any tips, tricks, gotcha's

Introduction

The general principal of any security policy should be to deny all services that are considered non-essential to the day to day operations of the business. The way that this question has been phrased appeared to be asking me to formulate a security policy that was based on denying specific services that could be vulnerable to attack and allowing all other services through. However on talking to Stephen Northcutt about what this part of the assignment was getting at I was informed that it was aimed at seeing if I had the knowledge to formulate a firewall rule set of medium complexity and to understand the ramifications of such a rule set.

In order to demonstrate this knowledge, I will work with an as sumed set of business requirements that would be reasonable for a company such as GIAC Enterprises. I will list the business requirements for GIAC Enterprises and implement an appropriate rule set that will enable these business requirements to be met.

Access Requirements for GIAC Enterprises

1. Public access to the GIAC web server using both HTTP and HTTPS.
2. Public access to the GIAC external mail server for sending email messages to GIAC Enterprises
3. GIAC web server able to access the GIAC database server on port TCP 1521 for oracle database access
4. Public access to the GIAC DNS server for lookups only.
5. Secondary DNS server able to access the GIAC DNS server for zone transfers of authorized zones.
6. GIAC external mail server able to deliver messages to the GIAC office mail server using SMTP
7. GIAC office mail server being able to deliver messages to the GIAC external mail server for forwarding to the Internet.
8. GIAC external mail server able to deliver SMTP messages to all public email servers.
9. GIAC management network machines able to access the appropriate servers for management via SSH.
10. GIAC office network able to browse the Internet using HTTP and HTTPS but must use the GIAC office proxy server.
11. GIAC office proxy server able to directly connect to Internet hosts for FTP, HTTP and HTTPS access.
12. GIAC management network able to access the GIAC office network file server using SSH.
13. GIAC office DNS server able to forward to the GIAC external DNS server for lookups.
14. GIAC office Mail server to scan both inbound and outbound messages for viruses.
15. GIAC office Database server able to connect to the External database server for data updates and synchronization.

Firewall Rules

Num	Source	Destination	Port	Action
1	Any	WWW	TCP 80 (http) TCP 443 (https)	Accept
2	WWW	Database	TCP 1521 (oracle/sql)	Accept
3	Any	External DNS	UDP 53 (dns)	Accept
4	Secondary DNS Servers	External DNS	TCP 53 (dns)	Accept
5	Office Email	External Mail	TCP 25 (smtp)	Accept
6	!Infrastructure	External Mail	TCP 25 (smtp)	Accept
7	Office Proxy	!Infrastructure	TCP 80 (http) TCP 443 (https)	Accept
8	Office DB	Database	TCP 1521 (oracle/sql)	Accept
9	Office DNS	External DNS	UDP 53 (dns)	Accept
10	WWW Management	WWW	TCP 22 (ssh)	Accept
11	Database Management	Database	TCP 22 (ssh)	Accept
12	Service Management	Service Network	TCP 22 (ssh)	Accept
13	Management Network	Office File Server	TCP 22 (ssh)	Accept
14	Firewall Management	Firewall	TCP 256 (fw1 control)	Accept
15	Firewall	Firewall Management	TCP 257 (fw1 logging)	Accept
16	Any	Any	Any	Drop

Group Definitions

Group	Hosts	Description
WWW	xxx.xxx.11.10	The web server
External Mail	xxx.xxx.86.20	The GIAC External mail server
External DNS	xxx.xxx.86.19	The GIAC External DNS server
Office Email	xxx.xxx.12.20	The GIAC Office mail server
Office Proxy	xxx.xxx.2.21	The GIAC Office Proxy server
Office File Server	xxx.xxx.2.22	The GIAC Office File server
Office DB	xxx.xxx.2.23	The GIAC Office Database server
Office DNS	xxx.xxx.2.24	The GIAC Office DNS server
Office Network	xxx.xxx.2.0/24	All hosts on the GIAC Office network
Secondary DNS Servers	N/A	Authorised secondary DNS servers
FW Management	xxx.xxx.1.100	Firewall Management server
WWW Management	xxx.xxx.1.101	Web Server Management server
DB Management	xxx.xxx.1.102	Database Management server
Management Network	xxx.xxx.1.0/24	All hosts on the management network
Infrastructure	xxx.xxx.1.0/24 xxx.xxx.86.0/24 xxx.xxx.11.0/24 xxx.xxx.12.0/24 xxx.xxx.2.0/24	All hosts on all local networks

Rule Ordering

Filtering firewalls perform the acti on associated with the first rule that matches the source, destination and port fields. This method of operation introduces a conflict when designing rule bases. On one hand, the most commonly matched rules should be at the top of the list so that they a re matched earlier and save on processing time. These rules are usually broad but have the disadvantage that they could "hide" some of the more specific rules that appear further down the rule base. Hence there are two alternatives: leave the specific r ules at the top of the rule base and accept the performance degradation of the firewall due to the extra comparisons made on the majority of packets, or carefully consider the influence of general rules on more specific rules that appear below them.

You can divide the rules on a filtering firewall into four types:

1. Specific to Broad – rules that allow access from a specific host to many hosts on a service. Eg. A rule to allow outbound http.
2. Broad to Specific – rules that allow access from many hosts to a specific host and service. Eg. A rule to allow inbound http access to a web server.
3. Broad to Broad – rules that allow access from many hosts to many other hosts or services. Eg. A rule that allows all services outbound from all hosts on the internal network to any hosts in the world.
4. Specific to Specific – A rule that allows a specific host access to a specific service on a specific server. Eg. A rule that allows database access from a web server to a database server.

Rules that allow access to many services or hosts often have unforeseen consequences. If a company has a requirement for all services outbound and the firewall allows this access, you will need specific rules to protect the firewall from your internal users.

In the rules that are list ed in the previous section I have attempted to put the rules that I expect to be more commonly "hit" at the top of the rule set. These include the rules that allow access to the web server, and that allow the web server access to the database server. I expect these two rules to be amongst the most heavily used rules on the firewall as it is expected that they company will have many hits on the website per day, and nearly all hits on the website will involve access to the database in some way. These rules are of type 2 (broad to specific), and will be unlikely to have any unforeseen effects on the traffic that is allowed through the firewall. It would only be in the unlikely situation that you wished to deny access to the web server from some specific internal or external hosts that rules in the form of Rule 1 and Rule 2 from my rule set could have unforeseen effects.

The next group of rules configured are the those to allow access to the GIAC external DNS server. I expect that these rules will also rece ive many "hits" as most web and email transactions to the organization will require DNS lookups. The first rule allows anyone to access the External DNS Server on UDP Port 53. This allows lookups but not zone transfers from any hosts, either external or internal. The second rule allows connections from authorized secondary name servers to the External DNS Server on TCP Port 53. This port is used for zone transfers, and although I expect that this

particular rule will not be used very often, I have located it with the other DNS rules for clarity.

The next set of rules cover SMTP or email access. The first of these rules allows specific access from the office email server in order to relay GIAC Enterprises email to the Internet. The second of these rules allows access from all boxes except the infrastructure or internal systems to the SMTP port (TCP port 25). This rule introduces the concept of "negation" which can be a useful tool to avoid unforeseen access being granted through the firewall. The intent of this rule is to allow external hosts to relay mail destined for GIAC Enterprises through the external mail server, but to deny access from the general infrastructure servers unless specifically allowed as is the case with the office email server. I have structured these rules this way as infrastructure boxes should not need to send email except in special circumstances.

The next set of rules allow the office network access to Internet services such as web browsing and FTP. These rules again utilize a negation construct to prevent unintended access being granted to servers. Access is granted to the Office Proxy Server for HTTP and HTTPS access to external boxes and from the Office Network to external boxes for FTP. This may appear to deny access from the Office Network and Proxy to the GIAC Web Server, but any requests for this site will be matched further up the rule base and hence be allowed.

The final group of rules allow access from the specific hosts on the management network to the servers that they are used to control. SSH is used to gain shell access to the servers, except for the firewall itself which allows shell access from the console only. This is achieved using the rules to allow TCP Port 22 from the management hosts to their respective servers. These rules are very specific and I would expect them to be used infrequently, hence their position at the bottom of the rule base.

The last rule is the default drop. This denies access to any services not specifically allowed previously in the rules. If the business requirements and security policy are specified correctly then this final rule will provide protection for the network from any other unwanted packets, however a firewall administrator should be aware that there are often services or requirements that are poorly specified by users and/or management, and that it could take some time for the firewall rules to reach a stable situation. It is wise to think proposed changed through carefully and to analyse them for any possible consequences on other existing rules in the network before implementation.

Assignment 3: Audit your security architecture

For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive in formation systems audit for GIAC Enterprises, an electronic commerce facility that is the largest supplier of electronic fortune cookie sayings in the world. The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly. Your assignment is:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exact ly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.
3. Perimeter analysis. Based on your assessment and referring to data from your assessment, analyze the perimeter defense and make recomm endations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Planning

Introduction

Auditing a firewall first requires an understanding of what the firewall is supposed to be protecting. Th is includes information about what actions are authorized, what risks that the organization is prepared to accept, exactly what information the firewall is supposed to be protecting and how that information is stored, and finally how you expect the firewall to work. For the purposes of this exercise this information is assumed to have been correctly defined in the security policy.

The following areas are required to be reviewed during the audit process:

1. Operational Procedures
2. Network and Security Architec ture
3. The Firewall Operating System
4. The Firewall Rules
5. Firewall Applications
6. Log and Alert Handling

Operational Procedures

The procedures that are to be followed in maintaining and modifying the firewall environment are quite possibly the most important a rea of responsibility for ensuring that the firewall environment remains as secure as possible. The procedures should include lists of tasks that need to be performed when making changes to the rules or the operating systems of the firewall environment, t he people who are required to authorize changes to rules and/or policy, the log monitoring and reviewing procedures and the patch and update procedures for all systems in the firewall environment.

Auditing procedures requires the auditor to find out wha t procedures exist for the tasks listed above and any others that may be appropriate to the environment being audited. Once the existing procedures have been discovered, it is important to find out how well the procedures are understood by the staff that actually perform the work. Most of the activity required to audit the procedures of an organization relies upon being able to talk to the members of that organization, and also to be able to review written procedures if they exist. This is best done duri ng business hours when the people who are using the procedures are available to talk to, thus making it easier to find out how well the procedures are actually followed. For an average sized firewall environment such as the one being audited I would expec t this task to take approximately one day.

As there is no physical tests involved in this phase of the audit the risk of interfering with the operation of the organization is very low. There will be some interference with the day to day activities of sta ff members as they will need to be interviewed in order to determine their understanding of the operational procedures.

Network and Security Architecture

The aim of the firewall environment's architecture is to correctly implement the security policy. The first step in auditing the architecture is to determine the authorized flow of information from the security policy. This is probably best summarized in an information flow diagram. The information flow diagram shows the directions that information is required to flow in as well as the protocols that are used for this transfer within the separate organizational areas of the network. The theoretical flow, which is derived from the security policy, needs to be matched to the actual flow that is permitte d by the firewall rules.

The existing architecture also needs to be reviewed in order to determine if it is capable of supporting the information flow required. In general, if each logical area of the network is located on a separate firewall interface, firewalls can be successfully configured to regulate the information flow.

The compilation of the information flow diagram should be a relatively short and simple task if the security policy has been defined correctly, as should the gathering of a physical network diagram. However if either of these tasks have not been done, the development of an information flow diagram and the diagramming of the physical network could take some time. I would estimate that the comparison of the physical diagram to the logical information flow diagram should take about an hour if no redesign is required, and could take up to a day if it is. This time is in addition to the time required to collect the diagrams.

The Firewall Operating System

The audit of a firewall need s to begin with the operating system that the firewall is installed on. If the operating system is not secure then neither is the firewall itself. The audit of the firewall operating system should include:

1. The packages that are installed on the firewall .
2. The services that are operating on the firewall.
3. The kernel configuration for handling ICMP requests.
4. File permissions, user accounts and trusts.

Any firewall should be installed with the minimum packages required for operation. A good checklist for th e packages required for different versions of Solaris and Checkpoint Firewall-1 is located at http://www.enteract.com/~lspitz/armoring.html . Guides such as this one and the one located at http://www.sun.com/blueprints/1299/minimization.pdf provide a good baseline for comparison against the systems are being audited.

A minimum set of commands for checking what packages are ins talled and what services are running (for Solaris) include *pkginfo*, *lsof*, and *netstat*. These system tools should be supplemented by scanning of each network interface of the firewall using a scanning tool such as *nmap* to ensure that no other ports are lis tening on the firewall. All audit tasks performed on the firewall operating system should be done with the firewall turned off to evaluate the risks to the firewall when it is not working, and also with it turned on in order to know if any changes have oc curred.

The final task for auditing your firewall at the operating system level is to verify that the patches installed are up to date. The Solaris command *patchdiag* is able to help verify which patches have been installed on the operating system.

The operating system auditing is not an overly time consuming task, and should be able to be completed within a reasonably short space of time. The main problem with the auditing of the operating system and the firewall is that some operations require disruption to the normal operation of the system, hence this should be done out of hours during a time period that is acceptable to the management and staff of the business being audited.

It should also be noted that some scanning tools will send fragmented p ackets and other "unusual" packets across the network which could possibly break the IP stack of the firewall host. Scanning the firewall in such a manner has both advantages and disadvantages. The obvious disadvantage is that it could disrupt the operat ion of a production system however the chances are high that if you can break your firewall then so can an attacker. It is better to know now and have an opportunity to fix the problem prior to it being used as an exploit. This is another reason that the se sorts of scans should only ever be done out of peak network usage times.

The Firewall Rules

The auditing of firewall rules needs to start with a manual overview of the rulebase. The goal of this is to identify any rules that will provide access that is not authorized by the organizations policy. It is quite common for temporary rules to become permanent and it should be one of the goals of the firewall rule audit to remove these temporary rules. Another goal should be to simplify the rules as much as possible. This can be done by combining rules that allow the same access to separate hosts, combining common services into groups, and removing duplicate rules.

After manually auditing the firewall rules, it is best to verify them by network scanning. Scanning should be performed from every network attached to the firewall and directed at every other network attached to the firewall. This tests both the outbound and the inbound traffic from all networks and gives a complete picture of the rules that the firewall is enforcing. Another good idea for testing these systems is to replace an authorized service system such as a DNS or SMTP server and see what it is authorized to do. Network based scanning and host replacement can usually only be done during low use periods, and always requires close coordination with the organization being audited as services will be disrupted.

The timing and resources required for this part of the audit again depends greatly on how well the organization has prepared in the first place. If the firewall environment is designed and maintained properly then the physical testing should be completed inside an hour, and the manual audit of the rulebase inside a couple of hours. However if the rulebase is long and complicated with a poor design the manual audit of the rulebase and comparison to the security policy could take a day or even more in order to ensure that no accidental faults are missed.

Firewall Applications

Firewall applications include software to provide au thentication, encryption, content filtering for both viruses and suitability for the work environment and possibly other applications. Applications should be tested to ensure that they are functioning as specified. This could include sending infected ema ils through the system and checking that they are cleaned and alerted to check a virus scanner, browsing unauthorized sites and verifying that access is denied for a content filter, and snooping network traffic inside a VPN to verify that encryption is wor king as expected.

The effort required to test firewall applications is hard to estimate. If the applications are simple and perform a single task, then it is easy to design a test that will confirm their functionality, however it is almost impossible to test every possible scenario. The development of a testing program for firewall applications is something that can be developed once and then applied in many audits, thus distributing the cost of this phase of the audit across many organizations.

Log and Alert Handling

Log and alert handling is left to the last stage of the audit because the earlier stages of the audit should make sufficient "noise" to show some interesting hits in the logs. The firewall and system logs need to be examined to see what they showed while you were scanning the networks. This is an essential task in order to assure the system owners that attempted scans and attacks will be notified in the system logs.

In the event that logging has been correctly configured it should take very little time to confirm that the correct events have been logged. However if insufficient logging has been configured it could take many hours and much consultation with the system owners in order to decide on appropriate changes. The system access required for auditing logging is minimal, and should require the attention of one of the system administrators for only a short period, and thus this auditing is best done during business hours, preferably not too long after the network and firewall audits have been performed.

Implementation

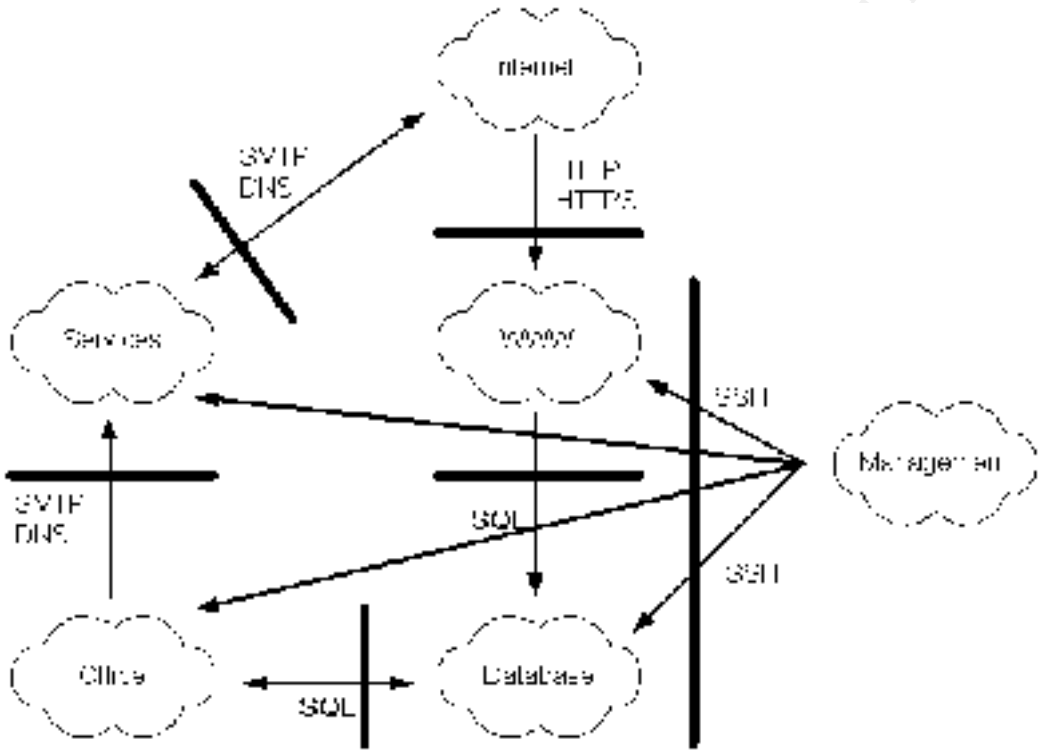
Operational Procedures

The operational procedures for GIAC Enterprises have not been covered in this assignment. It is necessary for GIAC Enterprises to have procedures that cover the following activities (and many others that I haven't listed here), however the writing of these procedures is outside the scope of this assignment.

1. Change Control
2. Patches for software and operating systems
3. Security policy change
4. Log handling
5. System access
6. Standard operating system bui ld procedures

Network and Security Architecture

The information flow diagram is shown below and the actual network diagrams for GIAC Enterprises are shown in Assignment 1. The required information flow is supported by the existing physical design. All logical elements of the network are located on a separate network interface of the firewall allowing filtering of all traffic between segments.



The firewall has six network interfaces, one for each of the logical areas represented by clouds in the abo ve diagram. The connections that require traffic needs to be regulated are indicated by the thick lines in the above diagram, and with the firewall configured as is shown in the overall network diagram (see assignment 1) this traffic can all be regulated successfully. It is now time to check the firewall to ensure that the security policy summarized in the above diagram is implemented correctly.

The Firewall Operating System

The firewall is running on the Solaris 2.6 operating system. The following pa ckages are installed:

```
# pkginfo
application CKPfw          Check Point FireWall  -1
system      SUNWaccr       System Accounting, (Root)
system      SUNWaccu       System Accounting, (Usr)
system      SUNWadmr       System & Network Administration Root
system      SUNWatfsr      AutoFS, (Root)
system      SUNWatfsu      AutoFS, (Usr)
system      SUNWcar        Core Architecture, (Root)
system      SUNWcg6        GX (cg6) Device Driver
system      SUNWcsd        Core Solaris Devices
system      SUNWcsr         Core Solaris, (Root)
system      SUNWcsu        Core Solaris, (Usr)
system      SUNWdfb        Dumb Frame Buffer Device Drivers
system      SUNWdtcor      Solaris Desktop /usr/dt filesystem anchor
system      SUNWesu        Extended System Utilities
system      SUNWhmd        SunSwift SBus Adapter Drivers
system      SUNWide        IDE device drivers
system      SUNWkey        Keyboard configuration tables
system      SUNWkvm        Core Architecture, (Kvm)
system      SUNWlibC       SPARCompilers Bundled  libC
system      SUNWlibms      Sun WorkShop Bundled shared libm
system      SUNWloc        System Localization
system      SUNWnisr       Network Information System, (Root)
system      SUNWnisu       Network Information System, (Usr)
system      SUNWos86u       Platform Support, OS Functionality (Usr)
system      SUNWpcelx      3COM EtherLink III PCMCIA Ethernet Driver
system      SUNWpci        PCI Simba device drivers
system      SUNWpcmci      PCMCIA Card Services, (Root)
system      SUNWpcmcu      PCMCI  A Card Services, (Usr)
system      SUNWpcmem      PCMCIA memory card driver
system      SUNWpcser      PCMCIA serial card driver
system      SUNWpd         PCI Drivers
system      SUNWploc       Partial Locales
system      SUNWpsdpr      PCMCIA ATA card dr  iver
system      SUNWqfed       Sun Quad FastEthernet Adapter Driver
system      SUNWsolnm      Solaris Naming Enabler
system      SUNWswmt       Patch Utilities
system      SUNWter        Terminal Information
system      SUNWtoo        Programming Tools
system      SUNWvplr       SMCC sun4u new platform links
system      SUNWvplu       SMCC sun4u new usr/platform links
system      SUNWxwdv       X Windows System Window Drivers
system      SUNWxwmod      OpenWindows kernel modules
```

There are far more packag es installed on this system than are strictly required, and I will discuss these packages in the analysis section.

Netstat reveals that the following services are listening. Note that this is with the firewall running, as I am unable to stop the firewall s in our production environment and I didn't have a test server available.

```
# netstat -na | egrep "Idle|LISTEN"
```

```
      *.259                              Idle
      *.514                              Idle
      *.56161                            Idle
      *.56162                            Idle
      *.22                *.*              0      0     0      0 LISTEN
      *.256               *.*              0      0     0      0 LISTEN
      *.50346             *.*              0      0     0      0 LISTEN
      *.50347             *.*              0      0     0      0 LISTEN
      *.50348             *.*              0      0     0      0 LISTEN
      *.50349             *.*              0      0     0      0 LISTEN
      *.50350             *.*              0      0     0      0 LISTEN
      *.259               *.*              0      0     0      0 LISTEN
      *.50351             *.*              0      0     0      0 LISTEN
      *.900               *.*              0      0     0      0 LISTEN
      *.18183             *.*              0      0     0      0 LISTEN
      *.18184             *.*              0      0     0      0 LISTEN
127.0.0.1.262             *.*              0      0     0      0 LISTEN
```

The behaviour of the firewall when the firewall is not running is governed by variables controlled by the *ndd* command. The values of the more important variables are shown. The general format of the command to obtain these values is:

ndd –get <device name> <variable name>

I wrote a short script that queried the values of all variables for a device and wrote them to a file. The script is shown below:

```
#!/bin/ksh
for var in `ndd -get /dev/tcp ? | cut -f1 -d' '``
do
      tmp=`ndd -get /dev/tcp $var`
      echo "$var   $tmp" >> nddtcpvalues
done
```

The script was run with the /dev/tcp and the /dev/ip devices and the results were then edited to just show the appropriate variable settings:

```
tcp_smallest_nonpriv_port   2050
tcp_strong_iss   2
ip_forwarding   1
ip_respond_to_address_mask_broadcast   0
ip_respond_to_echo_broadcast   0
ip_respond_to_timestamp   1
ip_respond_to_timestamp_broadcast   1
ip_send_redirects   0
ip_forward_directed_broadcasts   0
ip_forward_src_routed   0
ip_icmp_return_data_bytes   64
ip_send_source_quench   0
ip_ignore_redirect   1
```

In these results ip_forwarding is set to 1 which is not desirable without the firewall running, however the firewall was running so this is expected. The tcp_strong_iss variable allows the Solaris operating syste m to use strong sequence numbers for sessions making it much more difficult to "hijack" sessions. The firewall is set to not respond to address mask broadcasts or echo broadcasts. It is also set to not forward source routed packets or directed broadcasts and to ignore any ICMP redirects that it receives. The firewall is set to respond to timestamp requests, and this should possibly be turned off.

The Firewall Rules

A manual examination of the firewall rules reveals that they enforce the documented policy for GIAC enterprises with few exceptions. The only obvious problem is that the policy states that the Office DNS server can talk to the External DNS server for domain lookups. This is enforced by rule 9, but rule 3 allows all hosts to communicate with the External DNS server for lookups. I would recommend changing the policy to allow the Office hosts to talk directly to the external DNS server as I see little benefit in restricting this. The consequences of the office hosts talking directly to the Ex ternal DNS server would only affect the operation of those hosts, for example if the internal DNS server was part of a split DNS configuration, then office hosts would not correctly resolve internal host to IP address combinations. It is possible to enforce the policy as written by changing the rule base as follows:

1. Move rule 9 to a position above rule 3.
2. Insert a rule below the newly positioned rule 9 to deny access from the entire Office network to the DNS server on Port UDP 53.

There is some room for improvement and consolidation of rules, but only if the security policy is slightly modified. If all hosts on the management network were allowed to SSH to the infrastructure, then rules 10 to 13 could be consolidated. I would recommend allowing this cha nge as the risk in allowing this access is minimal. All users of hosts on the management network should be trusted, and in the event of a compromise of hosts on this network it is likely that all other locations in the network will already be compromised. The benefits that result from the simpler rulebase that would result from this change are greater than the benefits of having the slightly better security on management access.

Unfortunately I was unable to obtain permission to scan production systems f or this assignment, and I was not in possession of sufficient infrastructure to produce a test site. If I was able to scan these networks I would have used the following command:

```
#  nmap -v -sA -T Aggressive -P0 -o nmap_<source_net>2<dest_net>.txt
<network>
```

where <network> is the nmap form of the network. Eg. xxx.xxx.2.0/24 would be xxx.xxx.2.* and <source_net> and <dest_net> are the logical names assigned to the networks being scanned from and to for this assignment. Eg. Office for xxx.xxx.2.0/24.

The results I would expect are shown in the table on the next page.

Source Net	Destination Net	Ports Open	Protocol's Open
Database	WWW	80/tcp 443/tcp	HTTP HTTPS
	Office	-	-
	Service	25/tcp 53/udp	SMTP DNS
	Management	-	-
WWW	Office	-	-
	Service	25/tcp 53/udp	SMTP DNS
	Management	-	-
	Database	1521/tcp	Oracle/SQL
Office	Service	-	-
	Management	-	-
	Database	1521/tcp	Oracle/SQL
	WWW	80/tcp 443/tcp	HTTP HTTPS
Office DNS	Service	53/udp	DNS
Office Email	Service	25/tcp	SMTP
Service	Management	-	-
	Database	-	-
	WWW	80/tcp 443/tcp	HTTP HTTPS
	Office	-	-
Management	Database	22/tcp 1521/tcp	SSH Oracle/SQL
	WWW	22/tcp 80/tcp 443/tcp	SSH HTTP HTTPS
	Office	-	-
	Office File Server	22/tcp	SSH
	Service	22/tcp 25/tcp 53/udp	SSH SMTP DNS

Again, I am unable to scan our external firewall while it is in production. I would expect that no ports are listening on the external interface of the firewall, and that on the internal interfaces that only the firewall management ports would be accessible while the firewall was in operation, and that these would only be available from the management station.

Firewall Applications

The only firewall application in use by GIAC enterprises is the virus scanner on the Office Email server. A file containing the KA KWORM virus was sent to my account to test the scanner. The scanner logs show the following:

Date:	11/20/2000 14:40:15
Method:	SMTP
From:	<my from address>
To:	<my to address>
File:	noname
Action:	The file virNOtF1Z is moved to the configured virus directory.
Virus:	VBS_KAKWORM.A

The email that actually arrived at my account contained a message that indicated that a virus had been removed from it and the attached file was in quarantine. The account that I sent the email from received a notificatio n message informing me that I had attempted to send a file containing a virus to my internal account and that the file had been quarantined.

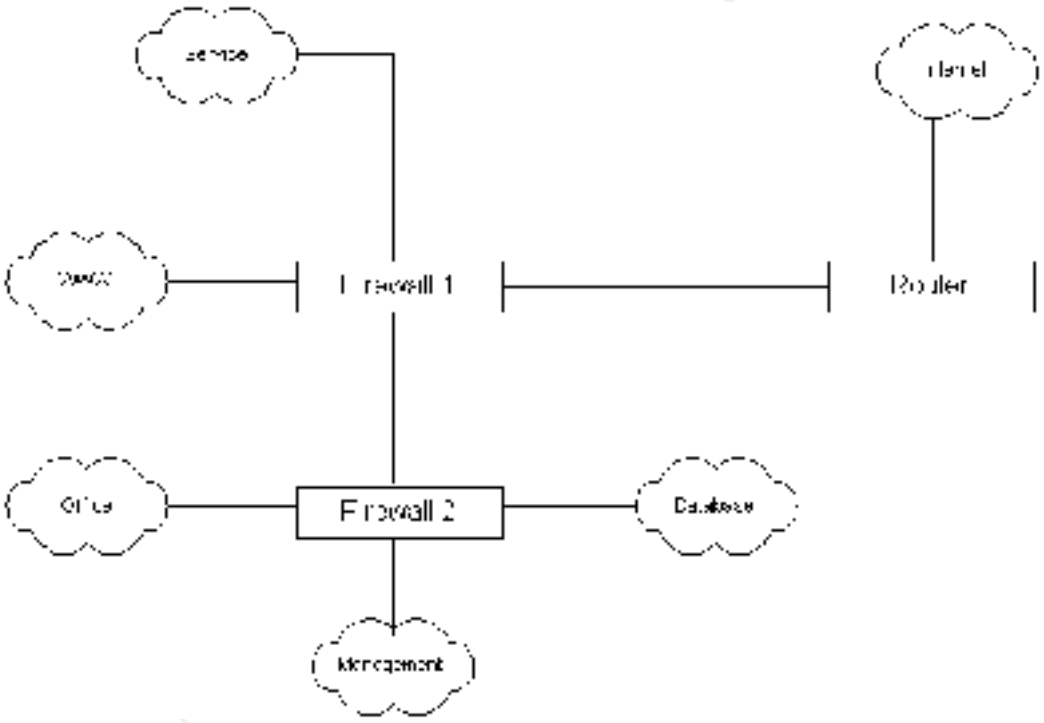
Perimeter Analysis

Operational Procedures

The operational procedures were considered to be outside the scope of this assignment.

Network and Security Architecture

The network and security architecture was considered to be adequate for the purpose that it was designed, however certain enhancements could improve the security and manageability of the architecture. Th e recommended enhancements are shown in the diagram below.



The advantages given by this alternative network architecture is an extra layer of separation between the areas that are allowed privileged access to networks and the Internet. These advantag es can be even greater if an alternative operating system and firewall combination is used on the second firewall. An excellent choice could be to use Solaris and Checkpoint Firewall -1 for Firewall 1 and Solaris and Gauntlet on Firewall 2. This combinati on also gives the advantage of using two different types of firewall – Gauntlet is a proxy based firewall as opposed to the filtering firewall implementation used by Checkpoint Firewall -1.

I would also recommend the addition of a dedicated syslog host to centralize the log management for the system. This would make it far easier to correlate all activities that are occurring to hosts in the system and hence to manage and monitor unusual

activities. The use of a utility such as *swatch* to automate the monitoring of logs would make the monitoring of the overall system far easier for the system administrators.

The Firewall Operating System

The main problem that showed up on the firewall operating system audit was that there were unnecessary packages installed. While these packages themselves do not actively create a security problem, the addition of extra software opens up the possibility for the exploit of as yet unknown security holes. I would recommend removing at least the following packages from the firewall system:

```
system      SUNWnisr       Network Information System, (Root)
system      SUNWnisu       Network Information System, (Usr)
system      SUNWpcelx      3COM EtherLink III PCMCIA Ethernet Driver
system      SUNWpci        PCI Simba device drivers
system      SUNWpcmci      PCMCIA Card Services, (Root)
system      SUNWpcmcu      PCMCIA Card Services, (Usr)
system      SUNWpcmem      PCMCIA memory card driver
system      SUNWpcser      PCMCIA serial card driver
system      SUNWpsdpr      PCMCIA  ATA card driver
system      SUNWtoo        Programming Tools
system      SUNWxwdv       X Windows System Window Drivers
system      SUNWxwmod      OpenWindows kernel modules
```

These packages are not required on the firewall and could possibly provide further means of compromising the firewall's security.

I would also recommend setting the firewall so that it does not respond to ICMP timestamp requests and or broadcasts. This can be done using the following commands.

```
# ndd -set /dev/ip ip_respond_to_timestamp 0
# ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The Firewall Rules

I would recommend that the firewall rules are changed only slightly from the listed configuration. The rulebase should be modified as specified below to enforce the security policy as written:

1. Move rule 9 to a position above rule 3.
2. Insert a rule below the newly positioned rule 9 to deny access from the entire Office network to the DNS server on Port UDP 53.

I would also recommend the addition of a further rule that rejects any "ident" connections that pass through the firewall. Several applications including *telnet* use the Identification protocol as part of their auditing techniques. This protocol provides information about the remote systems User ID and operating system and could possibly allow information gathering about the network. Although this protocol is

already denied by the default drop rule, a "Reject" (sending a RST packet) is better in this case as there can be significant performance degradation caused by con nections waiting for an "ident" connection to time out. The ideal place for this rule would be between the existing rules 9 and 10.

I would also recommend the consolidation of the management access rules (rules 10 - 13) into a single rule. However this co uld only be done if management were willing to change the security policy regarding the access of the management network to servers.

Firewall Applications

The virus scanner appears to be performing its job correctly. It is essential that the virus scanner engine and data files are kept up to date and it should be part of the procedures for this to be checked.

The use of a second firewall such as gauntlet would allow database and internal email access to be handled by a proxy – reducing the opportunity for individual packet attacks on the systems thus protected – individual packets wouldn't be considered valid by the proxy and would thus be rejected. Any attacks would have to be based on vulnerabilities in the end service which should be handled if vend or patches are kept up to date.

Log and Alert Handling Analysis

Centralizing the handling of logs would provide an easier method of management. The addition of an IDS system at a point both external and internal to the firewalls would provide a greater chance of detecting both network scans and inappropriate network activity or attacks. I recommend that an IDS be placed internally to the firewall to provide a monitor on what intrusion or scanning attempts have been successful. I would also recommend t he addition of a central log server running *syslog* and allowing all hosts on the network to send their logs to this server. This would require opening up port 514/udp from all networks to the designated syslog host.