Global Information Assurance Certification Paper

SANS GIAC Certification
Level 2 GCFW
Firewall and Perimeter Protection Curriculum

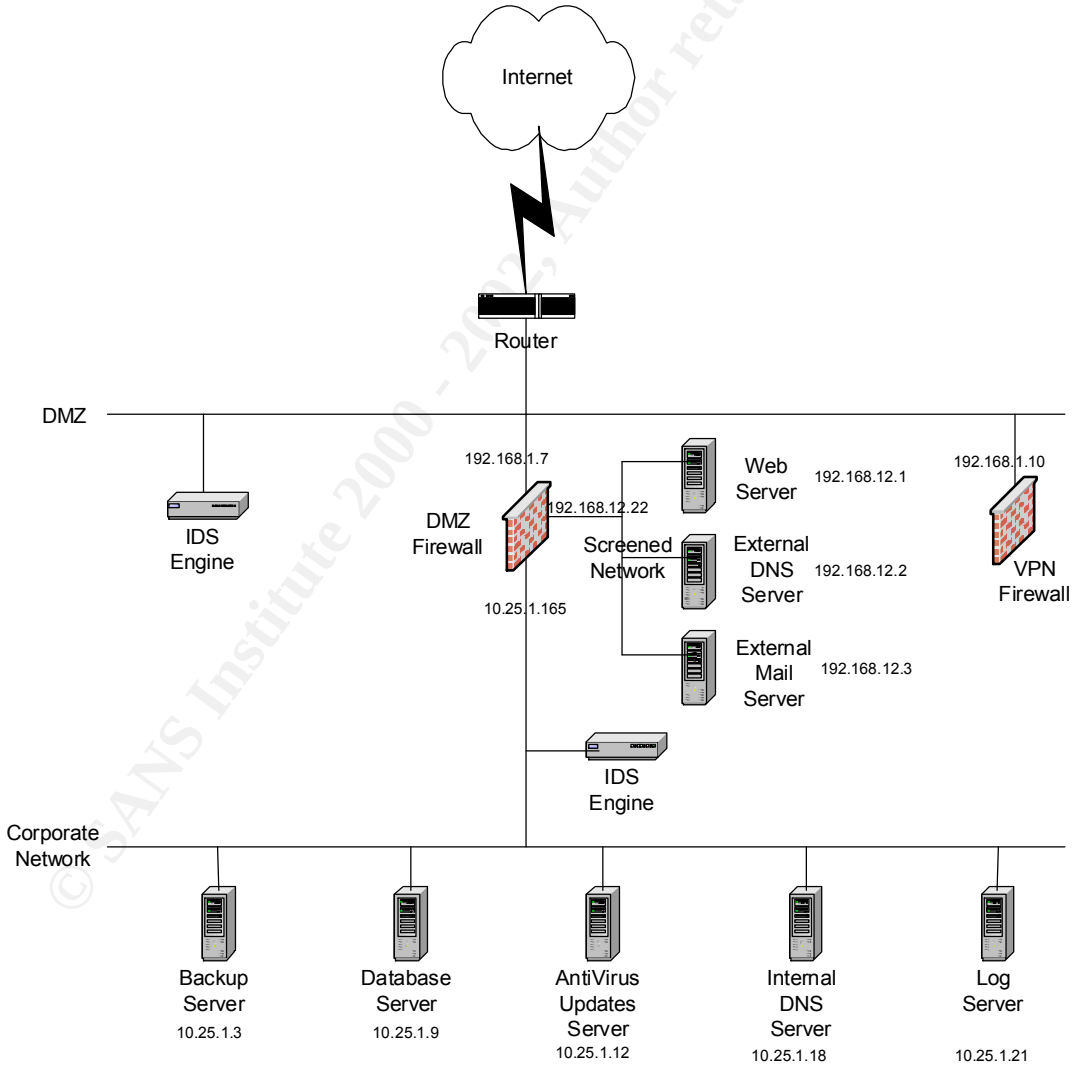
Practical Assignment
for
SANS NS2000 Monterey

Janice Southerland
November 21, 2000

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 sayings.

The student assignment is to produce a diagram, or set of diagrams, with explanatory text defining how to use perimeter technologies to implement as many of the requirements above 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.



GIAC Enterprises
Nework Diagram

Security Architecture for GIAC Enterprises

Please refer to the network diagram on the previous page for a visual of the architecture. Also, please note that the specific IP addresses selected are used for illustrative purposes only.

1. Install and maintain a working firewall to protect data accessible via the Internet.

The following components are used by GIAC Enterprises in order to build a solid security infrastructure, with the primary objective being defense in depth. Visa's requirements are basic guidelines that should be adopted and supported by all organizations. However, these guidelines are just a baseline and should be enhanced as feasible.

* Cicso 7206 border router running IOS 12.0 with ACLs implemented for the following:
    * Ingress filtering
    * Egress filtering
    * Allow only absolute minimal ICMP traffic that is deemed necessary
    * All other services as outlined in SANS Top Ten Blocking Recommendations

    The strategy to block this traffic at the router versus the firewall is based upon a recommendation by our emergency response partner. The idea is to block as much unwanted traffic as far away from our corporate resources as possible. We plan to monitor this closely. If it's determined that blocking this much traffic at the router blinds us in investigating suspicious activity, then at that time we will move the blocking rules to the firewall instead.

* Checkpoint Firewall-1 4.1 between the unprotected network and the trusted internal network. This DMZ firewall is also used to implement a screened network containing the webservers, the external DNS server, and the mailserver. Additionally, the firewall is performing NAT services for outward-bound Internet traffic, in order to prevent exposure of our internal IP addresses.

* Split DNS structure. External DNS server resolves queries for the few hosts in the screened network only. Internal DNS server resolves internal queries only.

* Intrusion detection systems, both network-based and host-based, have been implemented.

    The network IDS is ISS RealSecure, with an engine placed between the border router and the DMZ firewall, and another placed behind this same firewall to monitor traffic which has been accepted through the firewall.

    The host-based IDS is a complementary combination of Axent Intruder Alert and Tripwire. It is installed on all servers with an Internet exposure, as well as on all internal servers with mission critical or sensitive data.

Maintenance of all of these components includes monitoring of traffic, alerting where feasible, and reporting. WebTrends has been implemented to assist with reporting. This product gives us the capability to report on data from both the Cisco IOS and the Checkpoint firewalls. It allows us to correlate information from both sources, thus providing a bigger picture than single points of reporting.

2. Keep security patches up-to-date.

All third party host, network, and application software has been inventoried, and versions of the same have been identified. Various security mailing lists are subscribed to by the company's CERT members, and are monitored for new vulnerabilities as they are identified. Also, the company has partnered with an emergency response vendor that offers a tailored mechanism for distribution of alerts and patch information.

An internal application has been developed to log these alerts, along with the severity, person assigned, applicability of patch, estimated completion date, and final completion date. This helps to assure that the alert does not go into a black hole without followed up.

3. Encrypt stored data accessible from the Internet.

Corporate security policy states that no critical data will be stored on any server that is exposed to the Internet. A tiered architecture is the standard model for Internet web applications, with a firewall between the web/application servers and the database servers.

A third party web application may have the customer registration database stored within its own architecture. Where this is the case, customers' passwords are stored in an encrypted format.

4. Encrypt data sent across networks.

* Business-to-business communications are encrypted via Checkpoint's VPN-1 Gateway solution.
* Business-to-customer web traffic is encrypted using SSL.
* Remote access traffic is encrypted by means of the Checkpoint VPN-1 Gateway and the Checkpoint VPN-1 SecureClient.
* Email traffic is encrypted using PGP.

5. Use and regularly update anti-virus software.

Norton AntiVirus is deployed for workstations and servers. When new signatures become available, a process is initiated to pull the signature files down, and they are then distributed to servers and workstations throughout the organization. Norton AntiVirus is also implemented for remote users.

McAffee VirusScan is used in conjunction with Content Technology's MailSweeper to scan incoming emails and attachments for viruses as they enter the environment, before they are delivered to the user's mailbox.

6. Restrict access to data by business "need to know".

Corporate security policy states that access to data will be authorized on a "need to know" basis. Approval by the data owner is required for access authorization. Access to applications and data is based upon the user's role(s) within the organization. Access to sensitive data (payroll, sales, customer information, etc.) is audited, and the data owners review the audit reports for compliance.

Internet access is also restricted, and is to be used for business purposes only. WebSense, a URL filtering software package, has been implemented to restrict sites that are in violation of the company's respect policy.

7. Assign unique IDs to each person with computer access to data.

Corporate security policy states that each employee is issued a unique ID with the level of access that his/her job requires, and that he/she is responsible for all activity while that ID is logged on to any system. Shared IDs are not acceptable and will not be issued. Third parties with access to extranet applications (vendors, partners, etc.) are issued unique IDs as well. These third parties are required to sign a legal access agreement before the IDs are issued.

Privileged system accounts, such as root, are not allowed direct login. The user must login with his/her own account and switch user to the privileged account, based upon an access list of authorized users.

Password management guidelines are as follows:

* Idle accounts expire after 30 days of inactivity
* Account locks after 3 invalid password attempts
* Password expiration interval of 30 days
* Password history of 6 passwords
* Minimum password length of 8 characters
* Dictionary words are not allowed for passwords; quality is checked during password selection process by a password quality utility

Password resets are performed in an automated manner in order to prevent social engineering. If the user forgets his/her password, he/she is prompted with a challenge. If the challenge is met, the password is set to a default value known only by the user.

8. Track access to data by unique ID.

Tracking access to data by unique ID is accomplished by both application and system logs. System logs for servers residing in the screened network are consolidated on a protected log server. Server times are synchronized in order to facilitate the research of suspicious incidents. WebSense provides logging and reporting of web access by corporate users.

9. Don't use vendor-supplied defaults for system passwords and other security parameters.

A standard baseline for securely configuring all devices and applications has been developed and is maintained and implemented by the responsible team. Default passwords are changed, and any unnecessary default accounts are either removed or disabled. Sample scripts and programs are removed. Default parameters are modified to reflect the organization's security policy, as in the case with the defaults in Checkpoint's properties page.

10. Regularly test security systems and processes.

The corporate Internal Audit team conducts periodic audits of applications and operating system security. Network-based audits are scheduled quarterly using tools such as nmap and Nessus. Audits of our perimeter security and external web applications are also performed periodically by contracted third parties to validate findings of our internal audits. Password cracking programs such as John the Ripper or Crack are run periodically to test compliance with password policies.

Assignment 2: Security Policy

Develop a security policy (implemented as a firewall filtering policy) that focuses on requirement #1, above: "Install and maintain a working network firewall to protect data accessible via the Internet". Use the Base Security Policy listed below as a starting point; you DO NOT need to repeat this information. Instead, focus on what 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 security architecture design from Assignment 1, above.

For each ADDITIONAL filtering recommendation in your policy, write a tutorial on how to implement that recommendation on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. Screen shots, network traffic traces, firewall log information, and URLs to find further information should all be used.

Be certain to point out any tips, tricks, or "gotchas".

The Base Security Policy contains the filtering recommendations from Appendix B of the SANS Top Ten document located at http://www.sans.org/topten.htm. Please note, we are NOT asking you to write a tutorial to explain how to block the services from the Top Ten, only for the ADDITIONAL filters you recommend. Student practicals from July - August 2000 focused on how to block the services described below; you may wish to reference one of these practicals in your work. They can be found at http://www.sans.org/giactc/gcfw.htm.

In this section, we list the Base Security Policy so you know what additional services to recommend blocking. This Policy lists ports that are commonly probed and attacked.

Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts.

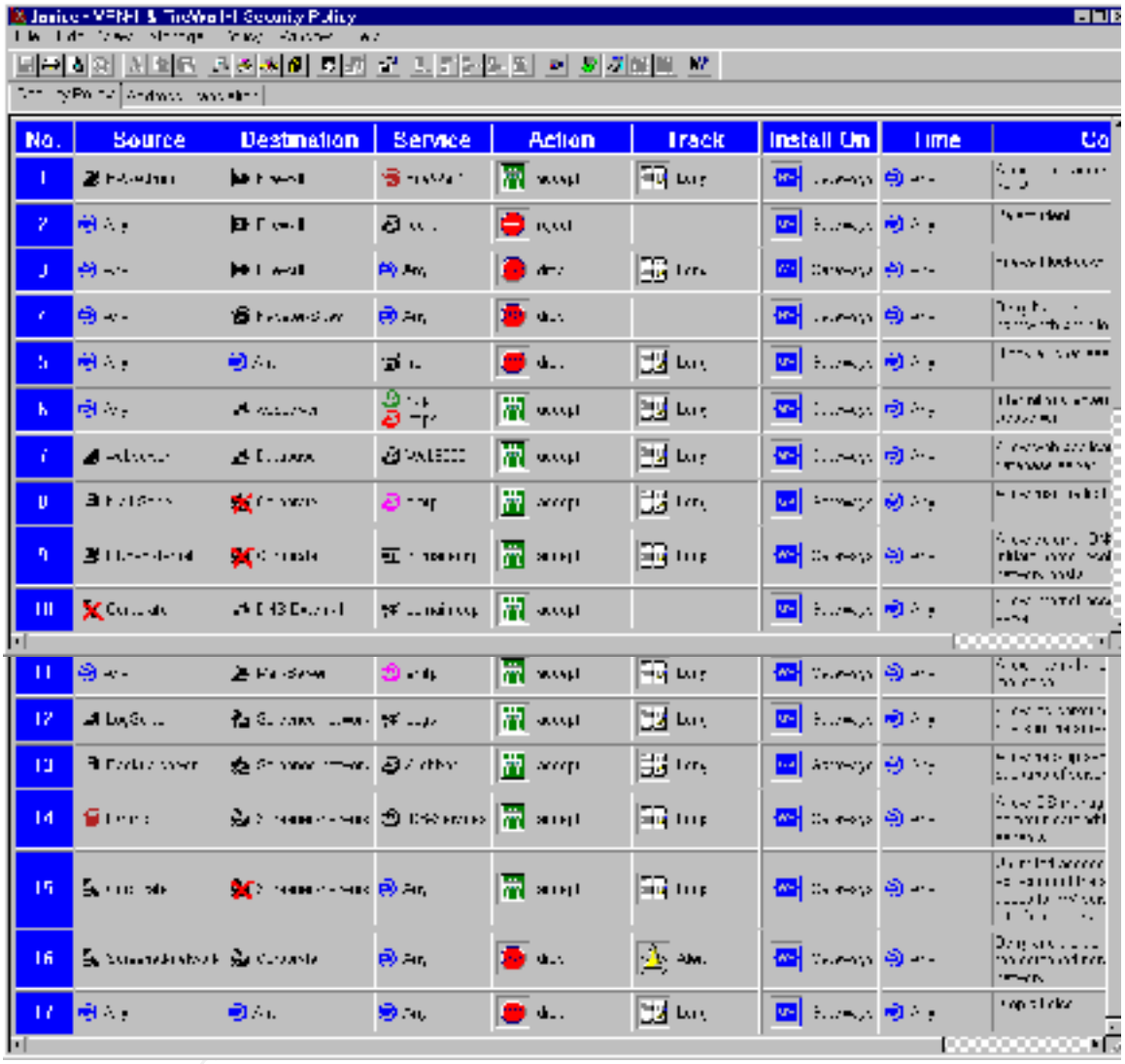
Security Policy for GIAC Enterprises

The following firewall policy assumes for the purpose of this exercise that the base policy referenced in the assignment instructions has been implemented via a combination of filters on the border router and firewall rules on the DMZ firewall. In addition to the blocking of these ports, ingress and egress filtering has been implemented on the Cisco 7206 border router. For further information on blocking the top ten ports on a Cisco router, please refer to http://pasadena.net/cisco/secure.html and http://www.sans.org/infosecFAQ/blocking_cisco.htm.

The first step in setting up a secure rulebase on the Checkpoint Firewall-1 4.1 firewall is to review the default properties page and turn off the default properties. If it's found that any of these properties are actually required, it is recommended to turn them back on in the firewall rulebase. For more details, please see an excellent whitepaper, Building Your Firewall Rulebase by Lance Spitzer, at http://www.enteract.com/~spitz/rules.html.

As with any packet filtering device, rule order within the Firewall-1 policy is critical. When a packet is received, the firewall compares it against the rulebase and when it finds the first rule that matches, it applies that rule. Therefore it is important to keep the more specific rules first and the more general rules last.

For the policy shown below, the rule "clusters" are ordered by firewall-related rules first, screened network rules next, and finally internal rules. An exception to this ordering is the rule for both internal and external access to the webserver. Even though this is a general rule, because it will be accessed frequently, it appears towards the top after the firewall-related rules.



Rule 1: Firewall administration access to the firewall.

This rule allows firewall administrators to access the firewall, and limits them to only the predefined Firewall-1 services. Access is limited based upon IP address. The rule must appear in order above the firewall lockdown rule (Rule 3).

Rule 2: Reject ident protocol from any source

The ident protocol is sometimes used by pop mail, ftp, and http servers to identify the sending user. This rule is designed to deny ident for security and performance reasons. Ident may allow an attacker to gain knowledge of your network, such as user information, objects, or processes considered private. Poor performance or an inability to establish a connection to a server may occur as the connection times out. This rule rejects the packet so that a RST is issued to quickly close the connection instead of waiting for a timeout, thus improving response.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	01:16:26	eth-s1p1c0	Firewall	reject	ident	169.254.92.3	192.168.12.1	tcp	2
17Nov2000	01:21:33	eth-s1p1c0	Firewall	reject	ident	169.254.92.3	10.25.1.9	tcp	2

For more detail:
Pix Performance Issues Caused by IDENT Protocol
http://cio.cisco.com/warp/public/110/2.html

Phoneboy Productions
http://www.phoneboy.com/

Rule 3: Firewall lockdown rule

The lockdown rule is placed at the beginning of the rule base with the purpose of protecting the firewall from the rest of the world. Placing it here insures that regardless of what rules may be added later, the firewall is still protected. It ensures that the firewall isn't accidentally exposed to unauthorized users.

Fore more detail:
Auditing Your Firewall
http://forbidden.net-security.org/txt/audit.htm

Rule 4: Deny access to Napster networks from any source

Napster is a client-server system that allows individuals to download MP3 music files. This rule denies access to known Napster server websites in order to prevent abuse of corporate Internet bandwidth and file server diskspace by users. The rule is placed at the top of the rulebase, just after the firewall-related rules, because it is a very specific blocking rule.

Gotcha:
This rule will need to be audited periodically due to the volatility of the Napster server network addresses.

64.124.41.0/255.255.255.0
208.178.163.56/255.255.255.248
208.178.175.128/255.255.255.248
208.49.239.240/255.255.255.240
208.49.228.0/255.255.255.0
208.184.216.0/255.255.255.0

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	14:25:31	eth-s1p2c0	Firewall	drop	8888	10.25.1.43	64.124.41.227	tcp	4

For more detail:
Napster - Should You Be Worried About It?
http://www.sans.org/infosecFAQ/napster.htm

Rule 5: Deny IRC for any source any destination

Internet chat applications such IRC (Internet Relay Chat) provides a means for information to be transmitted between our network and remote networks in both directions. There are multiple security risks associated with the use of IRC, including attacks involving Trojan horse programs. This rule denies IRC traffic both inbound and outbound, and is placed at the top of the rulebase, just after the firewall-related rules, because it is a very specific blocking rule.

Tips:
It is difficult to identify all the ports that IRC may use. Block the commonly used ports as a best attempt. Ports 6665-6670, 6680.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	14:42:11	eth-s1p2c0	Firewall	drop	6667	10.25.1.43	195.40.6.1	tcp	5
17Nov2000	2:04:19	eth-s1p1c0	Firewall	drop	6667	169.254.92.3	10.25.1.72	tcp	5

For more detail:
CERT Incident Note IN-2000-08 Chat Clients and Network Security
http://www.cert.org/incident_notes/IN-2000-08.html

Rule 6: Allow access to the webserver for any source any destination

This rule allows both http and https access to the webserver from inside and outside our network. It is placed in the upper section of the rulebase due to the frequency that this traffic will occur.

Tips:
There are many exploits documented for a variety of webserver application software, including CGI. "Homegrown" applications should be subjected to intense security scrutiny before going into production on an Internet-exposed webserver. It's extremely important to ensure that security advisories are monitored and acted upon in this environment.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	15:09:21	eth-s1p2c0	Firewall	accept	http	10.25.1.43	192.168.12.1	tcp	6
17Nov2000	15:10:19	eth-s1p2c0	Firewall	accept	https	10.25.1.43	192.168.12.1	tcp	6
17Nov2000	1:57:44	eth-s1p1c0	Firewall	accept	http	169.254.92.3	192.168.12.1	tcp	6
17Nov2000	1:59:51	eth-s1p1c0	Firewall	accept	https	169.254.92.3	192.168.12.1	tcp	6

For more detail:
How to Eliminate the Ten Most Critical Internet Security Threats
http://www.sans.org/topten.htm

Rule 7: Allow access from the webserver to the database

Corporate security policy mandates that no database information will be stored on servers with an exposure to the Internet. Access from the webserver in the screened network to the database in the corporate network is limited to the tcp service associated with the third party web application. The rules for the screened network are clustered together beginning with this one. This rule is placed well above the more generic rule that denies access from the screened network to the corporate network.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	2:17:44	eth-s1p3c0	Firewall	accept	web8000	192.168.12.22	10.25.1.9	tcp	7

Rule 8: Allow smtp traffic to the Internet

Smtp traffic is allowed from the mailserver in the screened network out to the Internet. The rule is placed with the cluster of screened network rules.

Tips:
Make sure that smtp relay has been disabled on the mailserver. Configure sendmail to prevent someone from directly connecting to the smtp port to send spoofed email to other sites. Sendmail has been called the "buggiest daemon on Earth", as there have been numerous vulnerabilities documented throughout the years. Keeping up to date on patches and upgrades to secure versions of sendmail are basic requirements.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	15:32:29	eth-s1p3c0	Firewall	accept	smtp	192.168.12.3	1.2.3.4	tcp	8

For more detail:
Spoofed/Forged Email
http://www.cert.org/tech_tips/email_spoofing.html

An Elementary Introduction to Sendmail
http://www.sans.org/infosecFAQ/sendmail.htm

How to Eliminate the Ten Most Critical Internet Security Threats
http://www.sans.org/topten.htm

Rule 9: Allow the external DNS server access to initiate name resolution for the hosts in the screened network.

The external DNS server is allowed to initiate name resolution for the screened network hosts. The server is not, however, allowed a connection to the corporate network. This DNS server should only have entries for publicly available servers. The rule is placed with the cluster of screened network rules.

Tips:
There have been a large number of problems with BIND because of the complexity of the functions it performs. Because of this, the number of attacks to target the host running the BIND service has increased dramatically. BIND is number one on the SANS list of the ten most exploited Internet security flaws! The basics to securing BIND include updating to the latest version and patch level; run bind as a non-privileged user; and run BIND in a chrooted environment.

For more detail:
How to Eliminate the Ten Most Critical Internet Security Threats
http://www.sans.org/topten.htm

Foiling DNS Attacks
http://www.securityportal.com/cover/coverstory20001113.html

Rule 10: Allow Internet access to external DNS server for DNS lookups

This rule allows Internet access to the external DNS server. Access from the corporate network is denied; they will use the internal DNS server. This traffic will not be logged; otherwise the logs will fill up in a short time. The rule is placed in the cluster of rules that have sources including the Internet.

Tips:
Refer to rule 9 above for more information. Ensure that the external DNS server in configured to only resolve for those domain names for which it is authoritative. Failing to do so may result in a DoS situation.

Rule 11: Allow internal and external smtp access to the mailserver

This rule allows internal and external smtp access to the mailserver. The rule is placed in the cluster of rules that have sources including the Internet.

See Rule 8 for tips and reference articles.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	15:23:03	eth-s1p3c0	Firewall	accept	smtp	10.25.1.43	192.168.12.3	tcp	11
17Nov2000	15:27:39	eth-s1p1c0	Firewall	accept	smtp	1.2.3.4	192.168.12.3	tcp	11

Rule 12: Allow log server to access the hosts in the screened network

The log server in the corporate network is allowed access to retrieve the logs from the hosts in the screened network. In order to trust the integrity of your system logs, it's recommended to consolidate the logs on a dedicated remote log server. The log server always initiates this connection on UDP port 514. This rule is placed with the rule cluster having the corporate network has the source.

Tips:
Consolidating logs on a dedicated remote log server is recommended in order to maintain the integrity of the log data. A variety of rootkits are available which can either delete or alter logs. UDP port 514 should be blocked to protect the log server from receiving unauthorized logging information from the Internet. This port is blocked in this rulebase by virtue of the "drop all else" rule. Use a tool such as swatch for automated filtering and notification.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	4:17:55	eth-s1p2c0	Firewall	accept	Logs	10.25.1.21	192.168.12.1	udp	12

For more detail:
Know Your Enemy: II
http://www.enteract.com/~lspitz/enemy2.html

Rule 13: Allow the backup server access to initiate backups of the screened network hosts

Corporate policy states that all production servers are backed up to a central backup server on a routine basis. This rule allows the backup server in the corporate network to access the hosts in the screened network via the application-specific service. The backup server always initiates this connection. This rule is placed with the rule cluster having the corporate network has the source.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	5:11:09	eth-s1p2c0	Firewall	accept	Archiver	10.25.1.3	192.168.12.1	tcp	13

Rule 14: Allow IDS management stations to communicate with host and network sensors

IDS management stations must communicate with their host and network sensors in order to consolidate the data gathered. This data should be consolidated on stations inside the corporate network in order to secure it. Only those ports specific to each application are opened, and the management stations always initiate the connection. This rule is placed with the rule cluster having the corporate network has the source.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	4:43:11	eth-s1p2c0	Firewall	accept	IDS-Services	10.25.1.113	192.168.12.1	tcp	14

Rule 15: Unlimited Internet access for the corporate network, excluding access to the screened network

This rule allows unlimited Internet access for corporate users, with the exception of denied access to the screened network. This will prevent the users from accidentally bringing in something from the screened network if were to become compromised. It is an untrusted network, and no access will be allowed from the trusted network. This rule will also allow the requirement for the anti-virus server to access the vendor site for signature updates. This rule is placed at the bottom of the rule cluster having the corporate network has the source.

Tips:
This rule should be reviewed and further limitation of services should be implemented. The majority of users will only need http and https access.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	16:17:06	eth-s1p2c0	Firewall	accept	http	10.25.1.43	167.216.133.33	tcp	15
17Nov2000	16:19:31	eth-s1p2c0	Firewall	drop	http	10.25.1.43	192.168.12.1	tcp	15

Rule 16: Deny access from the screened network

The DMZ should never initiate traffic to the corporate network. Evidence of such traffic may suggest a compromise within the screened network. The only exception to this is the access allowed from the webserver to the database server. Any other traffic should be considered suspicious. Alerting for this rule is turned on for quick notification.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	16:29:17	eth-s1p3c0	Firewall	drop	ftp	192.168.12.22	10.25.1.12	tcp	16

For more detail:
Building Your Firewall Rulebase
http://www.enteract.com/~lspitz/rules.html

Rule 17: Deny all else

Firewall-1 will drop all packets that don't match any rules; however, by default the traffic will not be logged. This rule in included at the bottom of the rulebase in order to log all events that are denied as a result of no rule matches.

Tips:
In order to keep the rulebase short and simple, this rule is used to block known threats such as Trojan horses, worms, and backdoors. Otherwise, the rulebase could become extremely complicated, resulting in greater opportunity for human error.

Filter test results:

Date	Time	Interface	Origination	Action	Service	Source	Destination	Prot	Rule
17Nov2000	0:13:55	eth-s1p1c0	Firewall	drop	netbus	1.3.5.7	10.25.1.43	tcp	17

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 information systems audit for GIAC Enterprises, a 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:

- 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.
- Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.
- Perimeter analysis. Based on your assessment and referring to data from your assessment, analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: Assignment 3 should be primarily focused on VISA requirement number 1, "Install and maintain a working network firewall to protect data accessible via the Internet." and your base + recommended security policy. Credit towards honors status will be given to students that are able to design an audit that can test all or a good deal of the VISA requirements.

Security Assessment for GIAC Enterprises

Planning the Assessment

Overview

The GIAC Enterprises security staff understands that a firewall is only as strong as its implementation. Even though this particular rule base is relatively simple, mistakes can happen. It has been determined that an audit of the perimeter defense is prudent before the company goes live with online sales of fortune cookie sayings.

Because staffing resources are limited, the company investigated contracting the audit out to a third party Internet security firm. However, after weighing out the costs of outsourcing the audit (average quote was $15,000) versus conducting the audit internally, it was determined that the most cost effective solution was to perform the audit ourselves.

The pilot for online sales is just a few weeks away, so there is not enough time to review commercial audit tools, make the selection, negotiate pricing, get the contract through Legal, and actually perform the audit. The security team requested an exception to corporate policy and gained approval to use freeware audit tools available on the web. Aside from the time limitation and costing savings aspects, it's a good idea to use the same tools to audit your network that the attackers are using.

In planning the assessment with the Web Support team, it was determined that after hours on a weekend would be the optimal time to perform the assessment. Their concerns focused around the fact that with the short time frame before go-live, the users will be crunching every day and into the evenings in order to get their application and data certified in time to make their launch deadline. They could not afford to experience an outage if the audit tools were to cause adverse effects to the site.

Tests that are non-intrusive and non-threatening to performance will be executed during daytime hours. Some tests will be based on normal traffic flow and will simply be a review of log activity.

The network audit will require the efforts of two security analysts for several hours over the course of two nights. Conducting the audit "after hours" translates to executing in a window between the hours of midnight and 5 am. There may not be a real need for two analysts; however, it's a good opportunity for a junior analyst to receive training in using these tools. Additional hours, approximately 16 hours or less will be required to analyze the results and make recommendations for improvement.

In an effort to prove compliance with Visa's standards for security readiness so that we may begin accepting Visa credit cards, additional manual audits will be performed with the assistance of the Desktop Support team, the Internal Audit team, and the Data Security team.

Audit Methodology

1. Audit the firewall itself (Visa Commandment #1)

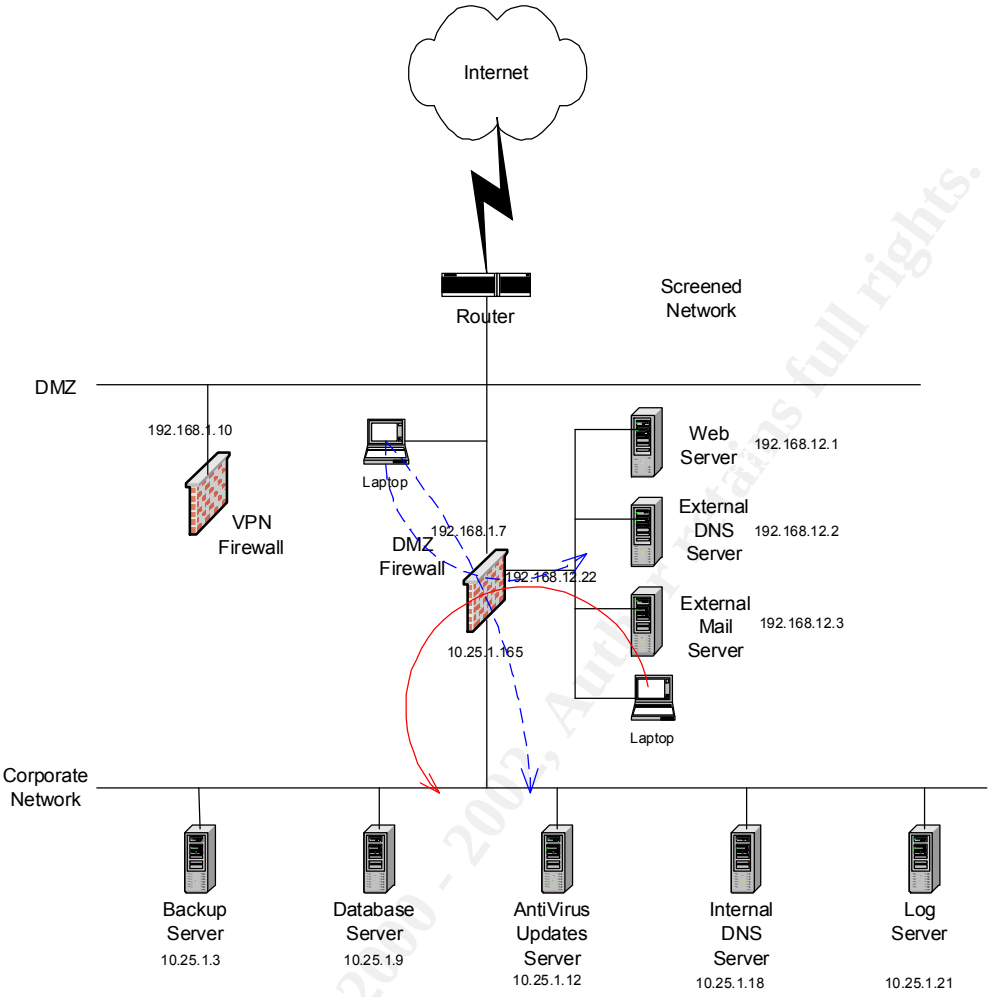
The firewall itself should be reviewed. You need to ensure that it is physically secured with controlled access. Then, the operating system itself should be fully "armored". Finally, port scan the firewall, scanning for icmp, udp, and tcp, in order to identify if there are any open ports. You should find no open ports, and you shouldn't be able to ping it.

2. Audit the firewall rulebase (Visa Commandment #1)

Next you want to ensure that the firewall is enforcing what you intended it to enforce. To do this, it's necessary to scan every network segment from every other network segment to see what is allowed and what is denied through the firewall. The preferred result is that the firewall is only allowing the traffic you expected when you designed the firewall policy. In order to accomplish this, place your auditing system on one side of the firewall and scan a system on the other side of the firewall.

Please refer to the diagram on the following page. Notice that the audit system will be placed outside the firewall and will attempt to penetrate through to both the screened network and to the corporate network, designated by the broken blue lines. Next the audit system will be placed on the screened network and will attempt to penetrate to the corporate network, designated by the solid red line. The intention of the second scan is meant to simulate a scenario where a host on the screened network has been compromised.

The scanning tool of choice for this step is Fyoder's nmap. Nmap has been described as "the premier port scanning tool available". Nmap is designed to allow the user the ability to scan large networks to determine what hosts are up and what services are running. It provides a list of services that are active on the target system. Nmap will also provide a best guess as to the O/S and version number running on it. Also, it tells the attacker how difficult tcp sequence prediction is for the remote host, which can be used to target hosts with a good potential for session hijacking.



GIAC Enterprises
Audit Strategy

3. Check for version numbers of DNS and Sendmail (Visa Commandment 2)

As mentioned earlier in the Security Policy section of this document, both DNS and Sendmail are subject to a number of vulnerabilities if software versions and patches are not kept up to date.

The 'dig' command will be used to attempt to determine the version of BIND being run on the External DNS Server. The command is as follows:

'dig -t txt -c chaos VERSION.BIND @giacenterprises.com' will query the version number of the BIND software running on giacenterprises.com.

In order to attempt to determine the version of sendmail on the MailServer, we will try to telnet to port 25 . If the line referencing the version number of sendmail was not commented out or falsified in /etc/mail/sendmail.conf, then we will be able to find what version of Sendmail the mail server is running.

4. Validate that data sent across networks is being encrypted (Visa Commandment #4)

Test resources on the web server that should only be accessed while encrypted by accessing web pages, which should be SSL encrypted. Run tcpdump while performing the test to ensure the data is actually being encrypted. As a separate test, monitor traffic from our hosts to partner hosts using tcpdump to validate that business to business traffic is being encrypted as expected.

5. Validate that anti-virus scans are running on a scheduled basis and signatures are current (Visa commandment #5)

This will require a manual audit of a random sampling of workstations throughout the organization. The assistance of the Desktop Support team will be required. Identify the sample group, and verify the datestamp of the last signature update as well as the datestamp of the last completed scan.

6. Ensure that access is limited on a "need to know" basis (Visa commandment #6)

Solicit the assistance of Internal Audit and Data Security to review the ACL's of each user community in regards to the web application. Levels of access and specific data should be restricted based upon the user's role in the organization.

7. Ensure that no shared accounts exist for accessing the web application (Visa commandment #7)

As an extension of the audit performed in Item 7 above, Internal Audit should verify that only individual accounts are authorized to access the web application.

8. Audit the log server data (Visa commandment #8)

Review the log data stored on the log server, ensuring that the log collection process is working properly, and that the logs are reflecting individual IDs and their activity.

9. Test for default password values for Cisco gear, SNMP community strings, and any NT servers on the corporate network (Visa commandment #9)

Ensure that the default values for Cisco gear passwords have been changed, and that the enable password has been set. Verify that default SNMP community strings have been changed. Although there are no NT servers exposed to the Internet, there are several in the corporate network running turnkey applications. Verify that default passwords have been changed, and that unnecessary default accounts have either been renamed or removed. Also ensure that any privileged accounts in use on Internet-exposed hosts have a different password value than the equivalents inside the corporate network.

10. Run cracking program on various password files to ensure that the password quality utility is effective (Visa commandment #10)

Select several mission critical servers and use the John the Ripper cracking tool to attempt to crack the password file. Verify that the password quality program is performing as expected.

Implement the Assessment

Nmap Scan

Nmap was run in all scenarios as described in the planning phase above. Below is sample output of the scans from outside the firewall, with the webserver and the mailserver as targets. It's interesting to note that nmaps O/S scan was not accurate. These are not AIX, IBM RS/+, or Solaris servers.

```
laptop# nmap -sS -v -v -n -O -P0 -p 21,22,23,24,25,80,111,6000 192.168.12.1
```

Where the command line instruction for nmap is detailed as follows:
-sS: SYN scan, aka stealth scan (SYN, RST or SYN/ACK, then RST)
-v: verbose
-n: don't resolve IPs to hostnames via DNS
-O: fingerprint target OS
-P0: don't PING first (scan even if unPINGable)
-p: target port number listing; FTP, SSH, telnet, etc.
192.168.12.1: target IP

```
laptop# nmap -sS -v -v -n -O -P0 -p 21,22,23,24,25,80,111,6000 192.168.12.1
Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Initiating SYN half-open stealth scan against  (192.168.12.1)
Adding TCP port 23 (state Firewalled).
Adding TCP port 25 (state Open).
The SYN scan took 2 seconds to scan 7 ports.
For OSScan assuming that port 25 is open and port 36242 is closed and
neither are firewalled
Interesting ports on  (192.168.12.1):
Port    State       Protocol  Service
21      filtered    tcp       ftp
22      filtered    tcp       ssh
23      filtered    tcp       telnet
25      filtered    tcp       smtp
80      open        tcp       http
111     filtered    tcp       sunrpc
```

```
6000    filtered    tcp       X11
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
Sequence numbers: 877E27B7 D88339E3 DDDF492F CD973A9D A40E8D36 9A1411BF
Remote OS guesses: AIX 4.02.0001.0000, AIX v4.2, AIX 4.2, AIX 4.3.2.0 on an
IBM RS/*, Solaris 2.6 - 2.7 with tcp_strong_iss=2
OS Fingerprint:
TSeq(Class=TR)
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
Nmap run completed -- 1 IP address (1 hosts up) scanned in 6 seconds
```

```
laptop# nmap -sS -v -v -n -O -P0 -p 21,22,23,24,25,80,111,6000 192.168.12.3
Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Initiating SYN half-open stealth scan against  (192.168.12.3)
Adding TCP port 23 (state Firewalled).
Adding TCP port 25 (state Open).
The SYN scan took 2 seconds to scan 7 ports.
For OSScan assuming that port 25 is open and port 30251 is closed and
neither are firewalled
Interesting ports on  (192.168.12.3):
Port    State       Protocol  Service
21      filtered    tcp       ftp
22      filtered    tcp       ssh
23      filtered    tcp       telnet
25      open        tcp       smtp
80      filtered    tcp       http
111     filtered    tcp       sunrpc
6000    filtered    tcp       X11
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
Sequence numbers: 4A7F90DD 62F29D15 A660F374 92D94DA7 B5BEFAE3 8AC269E1
Remote OS guesses: AIX 4.02.0001.0000, AIX v4.2, AIX 4.2, AIX 4.3.2.0 on an
IBM RS/*, Solaris 2.6 - 2.7 with tcp_strong_iss=2
OS Fingerprint:
TSeq(Class=TR)
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
Nmap run completed -- 1 IP address (1 hosts up) scanned in 6 seconds
```

In reference to Audit Methodology Item #1, the firewall is physically secured in the organization's data center behind doors with a combination of cardkey and palm scan method of authentication for entry. The firewall is running on a Nokia appliance, which is shipped from the factory with a hardened version of the BSD O/S named IPSO, and is considered an "armored" system. Nmap scans of the firewall interface were performed as outlined in the Methodology; nmap failed to guess the O/S accurately.

In reference to Audit Methodology Item #3, we were unable to successfully determine the version numbers for BIND or sendmail. Version numbers were manually verified for current versions.

In reference to Audit Methodology Item #4, based upon tcpdump output, all traffic that was expected to be encrypted was found to be encrypted.

In reference to Audit Methodology Item #10, it appears that the password quality program is doing an adequate job. Few passwords were actually cracked, but the program can be tweaked to better match the intelligence of the cracking program.

In reference to Audit Methodology Items #5,6,7,8,9, these manual audits are still in process. Some resources from other areas are scheduled but are not currently available. Projected completion time is two weeks.

Perimeter Analysis

No high risk issues were found during the course of this assessment. However, with new exploits coming out daily, GIAC Enterprises should continue to work at making their web presence and enterprise environment as secure as possible.

The greatest exposure detected during this initial assessment is the unrestricted Internet access for corporate hosts. Ultimately you will want to limit outbound traffic to only what is absolutely required, such as limiting outbound traffic to http and DNS queries. If possible, you should also proxy all outbound traffic.

GIAC Enterprises should continue to strive towards developing a unified application security architecture that addresses end-to-end security in terms of distributed applications that span multiple security domains. The architecture should address security in each tier in the n-tier architecture.

The company policy regarding restricted access to the corporate network by its recent acquisition, 'Fortunes R Us', is right on target. A complete security assessment should be executed, and compliance to GIAC Enterprise's security policies should be required before making the acquired organization an extension of the company's corporate network.

Recommendations for accomplishing this challenge and improving the enterprise security architecture is as follows:

* Consider using digital certificates for VPN authentication versus shared secrets.
* Consider using digital certificates for strong authentication of vendors to extranet applications.
* Implement internal firewalls between business units to help protect critical data from insider threats.
* Consider the purchase of the AppScan product to review homegrown web applications while they're still in certification.

Recommendations (continued from previous page)

* Schedule an audit of the third party web application before launch if possible. Tools such as Whisker may be used, or it might be more appropriate to outsource the penetration test in sake of time.
* During the next scheduled audit, use the Nessus vulnerability scanner to dig a little deeper as a follow up to this initial scan.
* Consider the purchase of the Finjan SurfinShield product to defend against malicious code that may be downloaded by naïve users browsing the web.
* Limit Internet access for the corporate network to http and https as feasible. Follow up by adding very specific rules for exceptions. For example, you would want to create a policy to restrict the port and destination for allowing the anti-virus server to download signature updates from the vendor.
* Consider complementing the RealSecure IDS with another product like Snort for a more complete view of suspicious traffic. RealSecure does not seem to pick up most of the popular horizontal scans.
* Continue performing network scans quarterly, with additional scans if major modifications are made to the network design.
* Treat the CERT plan as a "cyber disaster recovery plan"; have practice scenarios to enforce methods learned in incident management training.

References for Assignment 3

Top 50 Security Tools
http://www.insecure.org/tools.html

Nmap Network Security Man Page
http://www.insecure.org/nmap/nmap_manpage.html

Nessus
http://www.nessus.org

DNS Security
http://www.sans.org/infosecFAQ/DNS_sec.htm

What Is nmap and What Can It Do?
http://www.sans.org/newlook/resources/IDFAQ/What_is_nmap.htm

Auditing Your Firewall Setup
http://www.enteract.com/~lspitz/audit.html

Hacking Exposed, Stuart McClure, Joel Scambray, George Kurtz, Osborne/McGraw-Hill, 1999