



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.

GIAC Firewall and Perimeter Protection Curriculum Practical Assignment Version 1.3

**SANS Network Security
Monterey CA
October 15-19, 2000**

Prepared by Tomas Alex

November 22, 2000

Table of Contents

1. Assignment 1: Security Architecture.....	3
1.1. Scope.....	3
1.2. Assumptions.....	3
1.3. Security Architecture.....	4
1.3.1. Install and maintain a working network firewall to protect data accessible via the Internet.....	6
1.3.2. Keep security patches up-to-date.....	7
1.3.3. Encrypt stored data accessible from the Internet.....	8
1.3.4. Encrypt data sent across networks.....	8
1.3.5. Use and regularly update anti-virus software.....	8
1.3.6. Restrict access to data by business "need to know".....	9
1.3.7. Assign unique IDs to each person with computer access to data.....	9
1.3.8. Track access to data by unique ID.....	9
1.3.9. Don't use vendor-supplied defaults for system passwords and other security parameters.....	9
1.3.10. Regularly test security systems and processes.....	10
2. Assignment 2: Security Policy	11
2.1. Scope.....	11
2.2. Border Router Policy.....	12
2.2.1. Ingress ACLs.....	12
2.2.2. Egress ACLs	13
2.2.3. Armoring the Router.....	14
2.3. Perimeter Firewall Policy Baseline.....	15
2.4. E-Commerce Perimeter Firewall Policy.....	16
2.5. Corporate Perimeter Firewall Policy.....	19
3. Audit Your Security Architecture.....	25
3.1. Planning the Assessment.....	25
3.1.1. Preliminary Meeting.....	25
3.1.2. Scope	25
3.2. Implementing the Assessment.....	27
3.2.1. Install and maintain a working network firewall to protect data accessible via the Internet.....	27
3.2.2. Keep security patches up-to-date.....	31
3.2.3. Encrypt stored data accessible from the Internet.....	31
3.2.4. Encrypt data sent across networks.....	31
3.2.5. Use and regularly update anti-virus software.....	32
3.2.6. Restrict access to data by business "need to know."	32
3.2.7. Assign unique IDs to each person with computer access to data.....	32
3.2.8. Track access to data by unique ID.....	33
3.2.9. Don't use vendor-supplied defaults for system passwords and other security parameters.....	33
3.2.10. Regularly test security systems and processes.....	33
3.3. Perimeter Analysis	33

1. Assignment 1: Security Architecture

1.1. Scope

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

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

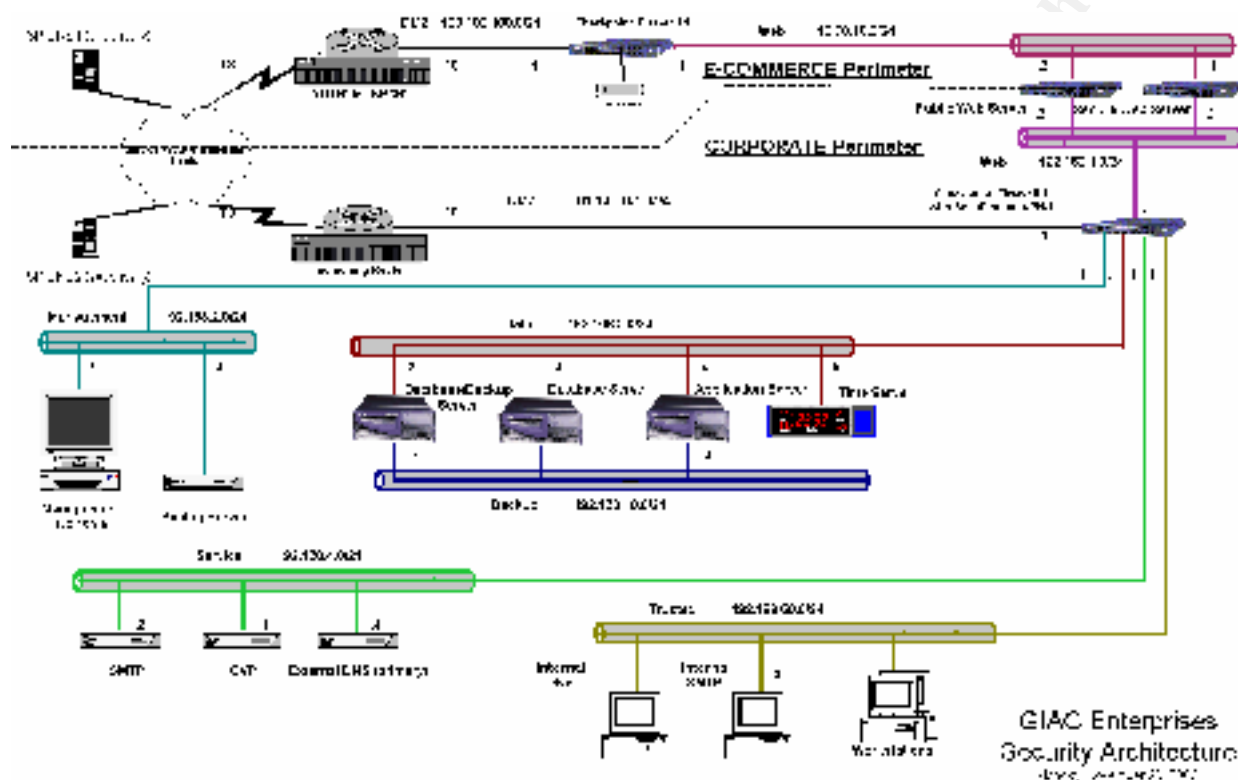
The student assignment is to produce a diagram, or set of diagrams with explanatory text defining how to use perimeter technologies to implement as many of the requirements above as possible. For this assignment you are a large and growing E-business that just completed a merger/acquisition you must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

1.2. Assumptions

- The expected number of online fortune cookie customers and transactions was not mentioned.
- Size, functionality, and complexity of the application being used was not mentioned.
- Expected growth was not mentioned.
- The number of internal GIAC Enterprise users, supplier users, and partner users was not mentioned.
- Unlimited budget.

Due to these assumptions, specific machine sizing in terms of CPU, disk, clustering, and load balancing were not taken into account. This proposal explains which perimeter technologies to implement the VISA 10 commandments.

The security architecture (figure 1) is comprised of two components: network infrastructure and perimeter design.



The network fabric is implemented with switching technologies to obtain a high level of network performance and efficiency with each segment having its own dedicated switch(s). This is useful for preventing sniffing from an untrustworthy host and also prevents possible VLAN exploits across a shared switch. The physical network is divided into two distinct perimeters: E-Commerce and Corporate (i.e. head office). The E-Commerce perimeter is dedicated to service GIAC Enterprise's online fortune cookie business (i.e. web servers) while the Corporate perimeter services all other internet services the company requires to do the rest of its day-to-day business. Both E-Commerce and Corporate each have their own dedicated T1/T3 internet connections. The benefits of this separation are discussed below. Ensure Quality of service (QOS) is configured for both internet pipes from the ISP

The DMZ - includes the border router and firewall, the first layer of defence from the internet
The Web Service Network – public and secure web servers, limited access to/from the internet

Corporate is divided into 7 network segments:

The DMZ - includes the border router and firewall, the first layer of defence from the internet

The Web Service Network – public and secure web servers connecting to Corporate Perimeter firewall, limited access to/from Corporate service networks

The Management Service Network – includes management console for managing Corporate firewall and any firewalls at other office locations and central syslog server that logs all system events from hosts on all service networks (explained below), limited access to/from internet and other service networks

The Data Service Network – includes database and application servers, a time server (i.e. radio or satellite device), limited access to/from Corporate service networks

The Backup Network – includes database and application servers, a backup server, separate network who's sole purpose is it to backup these servers thereby leaving the Database Service Network to process only online business transactions only, no connection to the Corporate firewall

The Service Network – includes external SMTP, CVP (Content Vectoring Protocol) server, and external DNS (primary) server, limited access to/from internet and to/from Internal Network

The Trusted Network – includes internal SMTP and DNS servers with limited access to Service Network, the entire corporate community with limited access to/from internet based on business use only

Since GIAC Enterprises has just completed a merger/acquisition and will probably have more in its lifetime, consideration of interconnecting these newly acquired companies (along with their customers, suppliers, and vendors) with the existing security architecture is critical. All data sent between GIAC Enterprises networks and these acquired companies will be done over VPN links across the internet. The VPN will be established from gateway to gateway (i.e. Checkpoint FW1 to Checkpoint FW1) between the different locations which will ensure that the networks are seen as one (see figure 2).



Figure 2.

Existing remote office, partner, and supplier access to the corporate perimeter will be granted across and Internet connections using VPNs. Mobile users (road warriors) and users from home will be granted access via the VPN also. No VPN access is permitted to the E-Commerce perimeter. It is dedicated to service the online fortune cookie business.

The perimeter design is based on the VISA "Ten Commandments" below.

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

In the big picture, the perimeter defence is made up of multiple layers where each layer sees to it's own part. The E-Commerce border router and firewall pair protect the web servers from internet. The firewall's routing tables only contain routes to the web servers. The web servers themselves have ip forwarding disabled so they cannot forward packets from the E-Commerce perimeter to the Corporate perimeter. The Corporate border router and firewall protect and segment the Service Networks (including web servers) and the Trusted Network from the internet.

Perimeter security for E-Commerce, Corporate, and the field offices is implemented with stateful filtering firewalls and border routers with ACLs:

Function	Product
Border Routers (all)	Cisco 3600, IOS 12.1.3 (i.e. SSH capable)
E-Commerce Firewall	Sun Netra T1, Checkpoint Firewall-1 4.1 + SP2
Corporate Firewall	Sun Netra T1, Checkpoint Firewall-1 4.1 with VPN-1+ SP2
Field Office Firewall(s)	Sun Netra T1, Checkpoint Firewall-1 4.1 with VPN-1+ SP2

The perimeter defence has been designed with multiple layered technologies where each layer provides additional protection with overlap to the previous layer.

Border Routers

Deny RFC 1918 addresses.
Deny packets with localhost, broadcast, and multicast addresses.
Deny packets without ip addresses.
Anti-spoofing for both inbound and outbound ip addresses.
Log ingress and egress significant events.
Disable all non-essential services.

E-Commerce Firewall

Deny packets with localhost, broadcast, and multicast addresses.
Anti-spoofing for both inbound and outbound ip addresses.
Static network address translation (NAT) for web servers.
Restrict access management access.
Log ingress and egress significant events (including border router).

Corporate (head office) Firewall

Deny packets with localhost, broadcast, and multicast addresses.
Anti-spoofing for both inbound and outbound ip addresses.
Static network address translation (NAT) for DNS and CVP servers.
Dynamic NAT for Trusted Network access to internet.
Restrict access management access.
Restrict access to Web, Management, Database, Other, and Trusted Network zones.
Log ingress and egress significant events (including border router).

All host based systems in both the E-Commerce and Corporate perimeters are secured as if there were no perimeter defence. Sun Microsystems hardware platforms have been selected to be used solely in all network segments except the Trusted segment and have a minimum security configuration as follows:

- Solaris 2.6 + Recommended (includes security) patches
- Redundant mirrored root disk (using Solstice DiskSuite)
- The OS security has been hardened by an open source tool called Titan (<http://www.fish.com/titan>)
- All syslog data sent to syslog server
- Tripwire (<http://www.tripwire.com>) is configured to monitor binary file signatures for any unexpected change.

In order to bind the layers together we must incorporate system clock synchronisation, centralised logging, and backup & recovery.

All system clocks in the Corporate (excluding Trusted) perimeter must be synchronised with NTP (Network Time Protocol) from the same accurate time source, the Time Server, in order to better understand what is happening and when reviewing system logs and alerts. We're assuming the Trusted Network has its own internal Time Server.

The central dedicated Log Server on the Management Network segment receives logs from other systems excluding those the E-Commerce border router and firewall and the Trusted Network. Syslogd is the only service that is run on it. Swatch, "The Simple WATCHer" (<http://www.stanford.edu/~atkins/swatch>) and filter" is also installed to monitor log files in real time and send out alerts when required. The E-Commerce firewall collects logs from both the border router and itself. These are backed up to a local tape drive attached to the firewall. The Trusted Network has its own central log server.

Backup and recovery is an integral part of the perimeter defence since it provides protection from data that gets corrupted because of a malicious hacker and when a system has a hardware error and fails. It is implemented on a dedicated server located in the Corporate/Data Network and across a dedicated Backup Network. Commercial grade backup software (e.g. Veritas NetBackup) is used and installed on all systems in the Corporate/Data Networks. Backup of systems outside of the Corporate/Data Network will be done remote backup commands (i.e. ufsdump) on those systems tunneled through (Secure Shell) SSH to ensure that the data is encrypted when sent across networks.

Also note that the external SMTP server runs the latest version of Sendmail and the external DNS (primary) server runs the latest version of BIND.

1.3.2. Keep security patches up-to-date.

Regularly monitor all vendor and open source web sites for patches:

Sun	http://sunsolve.sun.com
Cisco	http://www.cisco.com
Checkpoint	http://www.checkpoint.com
Veritas NetBackup	http://www.veritas.com

Tripwire	http://www.tripwire.com
Titan	http://www.fish.com/titan
Solaris Fingerprint Database	http://sunsolve.Sun.COM/pub-cgi/show.pl?target=content/content7
Swatch	http://www.stanford.edu/~atkins/swatch
Sendmail	http://www.sendmail.org
BIND	http://www.isc.org/products/BIND

Regularly monitor and subscribe to the following mailing lists (there are more) to keep informed about the latest exploits and security vulnerabilities:

SANS	http://www.sans.org
CERT	http://www.cert.org
SecurityFocus	http://www.securityfocus.com
FIRST	http://www.first.org

1.3.3. Encrypt stored data accessible from the Internet.

Any sensitive data on any systems in the E-Commerce and Corporate Service Networks can be encrypted using PGP (<http://www.pgp.com>). Solaris 2.6 does not have any mechanism to do filesystems encryption itself. However, data within the database (i.e. Oracle, SyBase, etc.) located on the database servers can be encrypted when stored and decrypted via the application when accessed from the internet. Note that this will probably incur performance and compatibility issues.

The secure web server SSL certificates cannot be encrypted since the product, iPlanet, (<http://www.iplanet.com>) does not have that capability. Also, the web server itself will be started manually since the automated start script would need to include the SSL password in plain text. A definite security weakness.

Note that the need for an external FTP server was not deemed required so that removes a potential direct internet access point to corporate data.

1.3.4. Encrypt data sent across networks.

Data traversing networks is encrypted in three fashions:

VPN – Access to data on internal Corporate perimeter systems by administrators, remote offices, partners, suppliers, and remote travelling and work from home users is encrypted.

SSL – Access to data on the web servers from the internet by customers is encrypted via Secure Sockets Layer (SSL). Provision has been taken into account for the purchase of 128-bit SSL (Global Server) Ids from Verisign (<http://www.verisign.com>) for the secure web servers.

SSH – Access to data on both the E-Commerce and Corporate perimeter firewalls by administrators is encrypted via SSH. As mentioned above, data on the Corporate service networks is sent to the Data network via SSH for backup purposes.

1.3.5. Use and regularly update anti-virus software.

Three mechanisms are put in place to provide anti-virus protection across service network servers and desktop (and road warrior) machines:

CVP – A CVP server exists for scanning all SMTP traffic, inbound and outbound. All outbound HTTP and FTP traffic are also relayed through this server.

Anti-Virus on Desktop (includes road warriors) – Filesystem monitoring and scanning on all MS Windows/NT systems Norton Anti-Virus (<http://www.norton.com>). Note that GIAC Enterprises only has Microsoft OS based non-server systems.

Anti-Virus on Servers – Filesystem monitoring and scanning on all Solaris service network servers with Tripwire.

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

Restricting access to data by business "need to know" must ultimately be done where the level of granularity is the individual user since business requirements may vary.

Access to data for customers to the online fortune cookie application (i.e. web servers) is restricted by unique ID. Each customer will have restricted access to their data, via a secure https connection, based on the appropriate business requirements.

Mobile personnel (and home users), field offices, suppliers, and partners have restricted VPN access to data by business requirement to specified services (i.e. applications) on specified servers.

Internal users (i.e. trusted network) also have unique IDs that allow access to internal applications, internal data, and internet data. IDs have also been grouped based on departmental and business requirements whether they are unix or NT based.

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

As mentioned in section 1.3.6, all GIAC Enterprises employees, suppliers, partners, and customers have a unique ID already due to specific business needs.

A central corporate internal LDAP server is single management and administration point for all internal and VPN user IDs. Enforced password policy restrictions are in effect.

Online fortune cookie customers' user IDs are stored on the secure web server and also have enforced password policy restrictions in effect.

1.3.8. Track access to data by unique ID.

Any access to data is tracked and logged by unique ID. This will include all system logs (e.g. syslog), mail logs, Oracle database logs, application logs, firewall logs, and web server logs. A log maintenance policy has been enforced which dictates that all log files be rotated and inspected on a daily basis. Tracking by unique ID's key advantage is that all activity can be tracked to a particular individual and two or more individuals using the same ID. This is especially useful when the activity appears to be malicious or suspicious in nature.

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

All hosts in both the E-Commerce and Corporate perimeters follow the corporate host security hardening policy which includes:

- Changing of all system (i.e. unix/root and NT/administrator) passwords to be complex and hard
- Lockdown file permissions on key system and device files
- Unused services and ports
- IP kernel variables

The open source tool called Titan, <http://www.fish.com/titan>, is used to harden security parameters and lockdown vendor vulnerabilities on the Solaris platforms.

The following key Checkpoint Firewall-1 vendor properties have been disabled:

- Enable Decryption on Accept
- Accept RIP
- Accept Domain Name over UDP (Queries)
- Accept Domain Name over TCP (Zone Transfer)
- Accept ICMP

See section 2.3 for further details.

The following key Cisco border router vendor parameters have also been disabled:

- ip directed-broadcast
- ip proxy-arp
- ntp
- finger
- ip source-route
- bootp server
- http server
- snmp

See section 2.2.3 for further details.

1.3.10. Regularly test security systems and processes.

All security systems and processes in each layer of defence in the E-Commerce and Corporate perimeters are regularly tested by the following means:

- Network port scans are performed with Nmap (<http://www.nmap.org>) from all network segments to ensure no unknown services are listening (i.e. trojan horse).
- Mail with an attachment containing a virus is sent inbound and outbound to ensure scanning and detection occurs.
- Run unix Crack against all user password databases and files.
- Run Titan to audit Solaris system security.
- All relevant system logs and alerts are checked to ensure the test events have been detected.

The results are reviewed and any security failures will be corrected.

2. Assignment 2: Security Policy

2.1. Scope

For the purpose of this assignment, your security policy should be focused on implementation of requirement number 1 above "Install and maintain a working network firewall to protect data accessible via the Internet". For a baseline policy, use the filtering recommendations located at www.sans.org/top10.htm. You DO NOT need to repeat that information. Instead, focus on ADDITIONAL filtering you would recommend and why. Keep in mind that you are an E-Business with customers, suppliers, and partners, you MAY NOT simply block everything! Your policy should implement your design above.

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

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

** You may find it easier to create a section of your practical that describes the order in which you would apply all of the rules rather than trying to do it with each policy cluster. Be certain to explain your reasons for the order you choose, we cannot read your mind.

Base Security Policy

Please note, we are NOT asking you to write a tutorial to explain how to block the services from the "top ten" security vulnerabilities. You may wish to reference one of the later practicals in your work since they were focused on blocking the "top ten" they can be found: <http://www.sans.org/giac/gcfw.htm>.

In this section, we list the base security policy so you know what additional services to recommend blocking. These are ports that are commonly probed and attacked.

Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order. Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

- 1) Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
- 2) Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
- 3) RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

4) NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

5) X Windows -- 6000/tcp through 6255/tcp

6) Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)

7) Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

8) Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

9) "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

10) Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

11) ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages.

2.2. Border Router Policy

The primary focus of the all GIAC Enterprises's border routers is to reduce the level of internet noise by providing anti-spoofing, blocking private addressing, controlling ICMP traffic, and blocking source routing. All routes are static.

2.2.1. Ingress ACLs

Interface Ethernet1 is the dirty (i.e. connected to the internet) interface. Access-list 110 is applied to inbound packets on interface Ethernet1:

```
interface Ethernet1
ip address x.x.x.x 255.255.255.0
ip access-group 110 in
```

Deny any packets with source addresses from the private addressing space (i.e. RFC 1918). These packets should never come from the internet since there are no routes back to these networks. Either they are leaking from another network or it is malicious 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
```

Deny packets with broadcast and multicast addresses. These packets either noise from other networks or a denial of service attack.

```
access-list 110 deny ip 255.0.0.0 0.255.255.255 any log
access-list 110 deny ip 224.0.0.0 7.255.255.255 any log
```

Deny packets no source ip address or localhost address. They are probably a denial of service attack:

```
access-list 110 deny ip host 0.0.0.0 any log
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
```

Prevent spoofing. Deny incoming packets that have our DMZ address space. This example uses the E-Commerce address space:

```
access-list 110 deny ip 100.100.100.0 0.0.0.255 any log
```

Continued spoofing prevention. Deny packets with the external router interface ip address:

```
access-list 110 deny ip host xxx.xxx.xxx.xxx any log
```

Deny ident traffic since it's an unreliable protocol used by SMTP servers to identify the user sending mail. No logging done to prevent log file from filling up:

```
access-list 110 deny tcp any any eq 113
```

And finally, log everything that does not meet the above rules.

```
access-list 110 deny ip any any log
```

After this initial noise filter, allow all remaining traffic and apply access list to external interface:

```
ip access-group 110 in
```

2.2.2. Egress ACLs

Interface Ethernet0 is the internal (i.e. connected to the DMZ segment) interface. Access-list 120 is applied to inbound packets on interface Ethernet0:

```
interface Ethernet0
ip address x.x.x.x 255.255.255.0
ip access-group 120 in
```

Deny any packets with source addresses from the private addressing space (i.e. RFC 1918). These packets should never come from the internet since there are no routes back to these networks. Either they are leaking from another network or it is malicious activity.

```
access-list 120 deny ip 192.168.0.0 0.0.255.255 any log
access-list 120 deny ip 172.16.0.0 0.15.255.255 any log
access-list 120 deny ip 10.0.0.0 0.255.255.255 any log
```

Don't allow internal hosts to send icmp outbound.

```
access-list 120 deny icmp any any log
```

Only allow packets from our network from our network outbound. This prevents spoofing of other network ip addresses.

```
access-list 120 permit ip xxx.xxx.xxx.xxx 0.0.0.255 any
```

Log everything else.

```
access-list 120 deny ip any any log
```

2.2.3. Armoring the Router

The router's security is hardened in the following manner:

Add this to external interface of screening router for secure encrypted administrative access purposes:

```
administrative access
access-list 120 permit 100.100.100.2 0.0.0.128
  line vty 0 4
    transport input ssh
    access-class 120
    login
```

The following services are disabled.

```
no ip proxy-arp
no ntp enable
no service finger
no ip source-route
no ip bootp server
no ip http server
no cdp run
no snmp
```

Protect the enable password with encryption.

```
service password-encryption
enable secret
```

Limit ICMP functionality.

```
no ip unreachable
no ip direct broadcast
no ip directed-broadcast
```

Limit these IP parameters:

```
no service udp-small-servers
no service tcp-small-servers
```

Save cpu cycles by disabling.

```
no logging console
```

Everything is logged to the syslog server

```
logging xxx.xxx.xxx.xxx
```

Change the banner

```
banner /WARNING : Authorized Access Only /
```

For additional information on securing Cisco routers see:

<http://pasadena.net/cisco/secure.html>

<http://www.cisco.com/warp/public/707/21.html>

<http://www.attrition.org/~modify/texts/phrack/Phrack55/P55-10>

2.3. Perimeter Firewall Policy Baseline

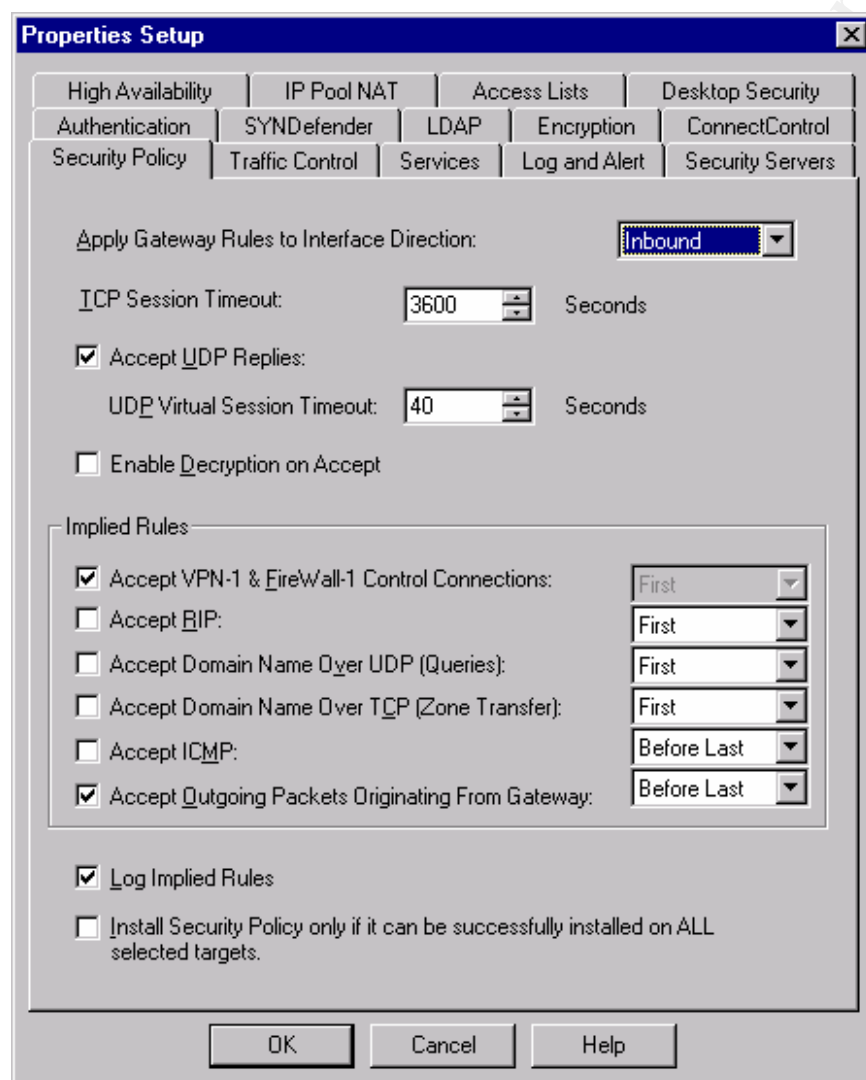
This tutorial assumes a basic working knowledge of the Checkpoint Firewall-1 product. It also assumes the reader has installed and licensed the product and its required modules (i.e. VPN).

The following configuration will be used on both the E-Commerce and Corporate firewalls.

Lockdown (disable) the Checkpoint Firewall-1 properties enabled by default:

Disable "Enable Decryption on Accept"
Disable "Accept RIP"
Disable "Accept Domain Name over UDP (Queries)"
Disable "Accept Domain Name over TCP (Zone Transfer)"
Disable "Accept ICMP"

These properties are disabled because they enable those services for the entire perimeter (something we do not want). The rulebases below will activate them at a more granular level specific to a source, destination, and service.



Configure the following:

Ensure that SYNDefender (in the Properties Setup), a Firewall-1 property that protects against SYN floods, is also activated.

Configure anti-spoofing on all firewall network interfaces.

Firewall-1 Rulebase Format

No.	Rule number
Source	Source objects: workstations, firewalls, networks, groups
Destintation	Destination objects: workstations, firewalls, networks, groups
Service	Protocol objects: tcp, udp, both, or groups
Action	accept – accept packets drop – drop packets reject – drop packet and reply with RST encrypt – encrypt VPN packets Client Encrypt – authenticate user and encrypt VPN packets
Track	Logging used: none, along, alert
Install on	Rule applied to this firewall
Time	Time the rule is active
Comment	Description

Note: Several excellent Firewall-1 papers should can be referenced at <http://www.enteract.com/~lspitz> that cover building firewall rulebases, auditing your firewall setup, understanding the Firewall-1 state table, and Firewall-1 troubleshooting tips.

Rulebase Design Caveats

The following rulebases have been designed with performance and, above all, simplicity. The fewer rules in the rulebase, the easier it is to understand and maintain. The most commonly used rules have been moved to the top to improve performance since there are fewer rules to parse (i.e. rules relating to the web, database, and application servers). Generally, more specific rules are placed ahead of more general rules. This prevents the general rules being matched prior to specific ones. Also, logging is turned on for all rules unless explicitly defined.

2.4. E-Commerce Perimeter Firewall Policy

Defined Objects

Object	Address	Description
econ_fw	100.100.100.1	e-commerce firewall
Border_router	100.100.100.10	border router
dns_svr	100.100.100.4	GIAC primary dns server
isp_dns1	xxx.xxx.xxx.xxx	ISP secondary dns server
isp_dns2	yyy.yyy.yyy.yyy	ISP secondary dns server

Groups

Group	Description
web_grp	web servers (public and secure)
Admin	administrator workstation (ip addresses)

NAT Implementation

Host	Private Address	Internet Address
Public Web Server	10.70.10.2	100.100.100.2
Secure Web Server	10.70.10.3	100.100.100.3

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	web_grp	http https	accept	log	ecm_fw	Any
2	Any	dns_srv isp_dns1 isp_dns2	domain-udp	accept	log	ecm_fw	Any
3	border_router	ecm_fw	syslog	accept	log	ecm_fw	Any
4	admin	ecm_fw	FireWall1 ssh	accept	log	ecm_fw	Any
5	admin	border_router	ssh	accept	log	ecm_fw	Any
6	Any	ecm_fw	ident knt	reject		ecm_fw	Any
7	Any	ecm_fw	Any	drop	log	ecm_fw	Any
8	web	Any	Any	drop	Alert	ecm_fw	Any
9	Any	Any	Any	drop	log	ecm_fw	Any

Rule 1

Description

Allow anyone access to the public and secure web servers on ports 80 and 443.

Test

Generate web (http and https) traffic from external site.

Rule 2

Description

Allow anyone in the E-Commerce perimeter to do nslookups (53/udp) to the specified name servers. Note that a policy property is to accept all udp replies initiated. Zone transfers (53/tcp) are not required here (they are also a security risk).

Test

Launch nslookup on one of the web servers to generate 53/udp traffic.

Rule 3

Description

Allow the border router to send syslog traffic to firewall. Centralized log management on the firewall is more secure. Syslog traffic from the web servers is sent to the other firewall (see Corporate Perimeter Firewall Policy).

Test

Generate traffic which will generate syslog traffic on the border router.

Rule 4

Description

Allow administrator workstations (i.e. specific ip addresses) SSH (port 22) access to the firewall and to connect to the firewall management server (i.e. the firewall) for remote administrative purposes.

Test

The administrators connect from these specific ip addresses with SSH and the Firewall-1 Gui. Verify the connectivity.

Rule 5

Description

Allow administrators workstations (i.e. specific ip addresses) to SSH (port 22) to the border router.

Test

The administrators connect from these specific ip addresses with SSH and the connectivity is verified.

Rule 6

Description

Reject all noisy traffic (i.e. NetBIOS and ident) to the firewall. Ident is an unreliable protocol used by mail servers. The traffic is rejected instead of dropped since reject closes the connection quickly by sending an RST packet. Logging has been disabled for this noisy traffic.

Test

Generate noisy traffic and ensure it is not logged by the firewall.

Rule 7

Description

Drop any other traffic to the firewall (i.e. firewall lockdown). This is logged because to determine if the firewall is being maliciously attacked.

Test

Generate traffic to the firewall and ensure it is being logged.

Rule 8

Description

Drop any traffic generated from the web network. The web network should never initiate traffic destined outbound through the firewall. This may mean that the web network is compromised and the traffic logged and an alert is generated. Note that it will generate traffic outbound through its network interface connected to the Corporate perimeter firewall to communicate with the application server.

Test

Generate traffic initiating from the web network to activate rule and ensure alert occurs.

Rule 9

Description

Drop all traffic that does not match the rules. This rule is ALWAYS the last rule and discards any unwanted traffic.

Test

Generate traffic that does not match any of the above 8 rules.

2.5. Corporate Perimeter Firewall Policy

Defined Objects

Object	Address	Description
corp_fw	101.101.101.1	corporate firewall
border_router	101.101.101.10	border router
isp_dns1	xxx.xxx.xxx.xxx	isp dns secondary server
isp_dns2	yyy.yyy.yyy.yyy	isp dns secondary server
backup_svr	192.168.3.2	backup server
db_svr	192.168.3.3	database server
app_svr	192.168.3.4	application server
time_svr	192.168.3.5	ntp server
manage_svr	192.168.2.2	management console
syslog_svr	192.168.2.3	syslog server
smtp_svr	192.168.4.2	external smtp server
dns_svr	192.168.4.3	external dns primary server
int_dns	192.168.50.2	internal primary dns server
int_smtp	192.168.50.3	internal smtp server













































































Groups/Networks

Group/Network	Description
admin	administrator workstation (ip addresses)
mobile_users	remote VPN users
field_offices	field VPN offices
supplier	supplier VPN offices
partner	partner VPN offices
internal_svrs	internal VPN accessed servers
partner_svrs	partner VPN accessed servers
supplier_svrs	supplier VPN accessed servers
mobile_srvcs	mobile VPN accessed services
internal_srvcs	internal VPN accessed services
supplier_srvcs	supplier VPN accessed services
partner_srvcs	partner VPN accessed services
web_grp	web servers (public and secure)
data_grp	database, application, and backup servers
manage_grp	management console and syslog server
service_grp	smtp, cvp, and external primary dns server
internal	trusted network

NAT Translation

Host	Private Address	Internet Address
External SMTP Server	192.168.4.2	101.101.101.2

External Server	Primary	DNS	192.168.4.4	101.101.101.4
-----------------	---------	-----	-------------	---------------

No.	Source	Destination	Service	Action	Track	Install On
1	 web_grp	 app_svr	 app_ports	 accept	 Long	 corp_fw
2	 app_svr	 web_grp	 app_ports	 accept	 Long	 corp_fw
3	 app_svr	 db_svr	 app_ports	 accept	 Long	 corp_fw
4	 border_router  corp_fw  web_grp  data_grp  manage_svr  service_grp	 syslog_svr	 syslog	 accept	 Long	 corp_fw
5	 Any	 corp_fw	 ident  NBT	 reject		 corp_fw
6	 int_smtp	 smtp_svr	 smtp	 accept	 Long	 corp_fw
7	 internal	 smtp_svr	 smtp->smtp_cvp	 accept	 Long	 corp_fw
8	 smtp_svr	 internal	 smtp->smtp_cvp	 accept	 Long	 corp_fw
9	 int_dns	 dns_svr  isp_dns1  isp_dns2	 domain-udp	 accept	 Long	 corp_fw
10	 internal	 dns_svr  isp_dns1  isp_dns2	 domain-udp	 accept	 Long	 corp_fw
11	 isp_dns1  isp_dns2	 dns_svr	 domain-tcp	 accept	 Long	 corp_fw

Rule 1

Description

Allow the web servers (public and secure) access to the application server via the defined application ports.

Test

Generate traffic to the web servers which should send traffic to the application server.

Rule 2

Description

All the application server access to the web servers (public and secure) via the defined application ports.

Test

Generate traffic to the web servers which send traffic to the application server which in turn will send traffic back to the web servers. The application itself is really tested here.

Rule 3

Description

Allow the application server access to the database server on the defined application ports.

Test

Generate traffic to the web servers (public and secure) and perform a data retrieval query. The application server should access the database server. Note that only the application server can access the database server.

Rule 4

Description

Allow syslog log traffic from the specified systems to syslog server. Centralized log management to one host is more secure and easier for review of all logs.

Test

Generate traffic to the various hosts which will generate syslog traffic to the syslog server.

Rule 5

Description

Reject all noisy traffic (i.e. NetBIOS and ident) to the firewall. Ident is an unreliable protocol used by mail servers. The traffic is rejected instead of dropped since reject closes the connection quickly by sending an RST packet. Logging has been disabled for this noisy traffic.

Test

Generate noisy traffic and ensure it is not logged by the firewall.

Rules 6, 7, 8

Description

Allow the internal smtp server access to the service smtp server to retrieve mail (port 25). Allow smtp traffic inbound and outbound to the service smtp server except from the internal network.

Test

Send and retrieve mail from the internal mail clients. Send email with virus attachment to test CVP server for detection.

Rules 9,10,11

Description

Allow the internal DNS server to do name lookups (port 53/udp) only. Allow all networks (except internal) to perform nslookups. Allow ISP secondary dns servers access to perform zone transfers (53/tcp).

Test

Generate internal and service nslookup traffic. Modify the service primary DNS server configuration file so the ISP perform a zone transfer during the next opportunity. Only the serial number in the main BIND configuration file needs to be changed, not any production entries.

12	internal	web manage data service	http->http_cvp ftp->ftp_cvp https	accept	Long	corp_fw
13	admin	web_grp data_grp manage_grp service	ssh	accept	Long	corp_fw
14	admin	corp_fw	FireWall1 ssh	accept	Long	corp_fw
15	admin	border_router	ssh	accept	Long	corp_fw
16	Any	corp_fw	Any	drop	Long	corp_fw
17	backup_svr	web_grp manage_grp service_grp	ssh	accept	Long	corp_fw
18	corp_fw	backup_svr	ssh	accept	Long	corp_fw
19	corp_fw web_grp manage_svr service_grp app_svr backup_svr db_svr	time_svr	ntp	accept	Long	corp_fw

Rule 12

Description

Allow internal http (port 80), https (443), and ftp (ports 20 & 21) outbound access to everything except the service networks.

Test

Launch an internal web browser to access external http and ftp sites. Attempt to download a file containing a virus and ensure CVP server performs scanning and detection.

Rule 13, 14, 15

Description

Allow administrators workstations (i.e. specific ip addresses) SSH (port 22) access to the specified service machines for remote administrative purposes.

Test

The administrators connect from these specific ip addresses with SSH and the connectivity is verified.

Rule 16

Description

Drop any other traffic to the firewall (i.e. firewall lockdown). This is logged because to determine if the firewall is being maliciously attacked.

Test

Generate traffic to the firewall and ensure it is being logged.

Rule 17, 18

Description

Allow the SSH (port 22) access to the web, management, and service hosts to tunnel ufsdump backups through. Note that the more secure machine always initiates the SSH. Thus the firewall initiates a SSH to the backups server.

Test

Initiate a SSH to the specified hosts and execute a remote ufsdump through the SSH tunnel.

Rule 19

Description

Allow ntp (port 123/tcp) access from the service networks to the service time server.

Test

Execute the ntp time synchronization script running via cron the hosts in the service networks.

20	mobile_users@Any	internal_svrs	mobile_srvc	Client Encrypt	Long	corp_fw
21	internal	field_offices	office_srvc	Encrypt	Long	corp_fw
22	field_offices	internal_svrs	office_srvc	Encrypt	Long	corp_fw
23	internal	supplier	supplier_srvc	Encrypt	Long	corp_fw
24	supplier	supplier_svrs	supplier_srvc	Encrypt	Long	corp_fw
25	internal	partner	partner_srvc	Encrypt	Long	corp_fw
26	partner	partner_svrs	partner_srvc	Encrypt	Long	corp_fw
27	web manage data service	internal	Any	drop	Alert	corp_fw
28	Any	Any	Any	drop	Long	corp_fw

Rule 20

Description

Allow any remote users VPN access through SecuRemote (Checkpoint mobile office VPN software) to the specified services on the specified servers.

Test

Initiate a SecuRemote VPN connection and ensure connectivity to specified services on specified servers is established.

Rule 21, 22, 23,24, 25, 26

Description

Allow internal network to VPN access field, supplier, and partner specified services on the specified servers. Allow field offices, suppliers, and partners VPN access to the specified services on the specified internal servers.

Test

Initiate VPN access to and from field offices, suppliers, and partners and ensure connectivity to specified services on specified servers is established.

Rule 27

Description

Drop any traffic generated from the web, management, data, and service networks to the internal network. These networks should never initiate traffic destined to the internal network. This may mean that these networks have been compromised so the traffic is logged and an alert is generated.

Test

Generate traffic initiating from these networks to activate rule and ensure alert occurs.

Rule 28

Description

Drop all traffic that does not match the rules. This rule is ALWAYS the last rule and discards any unwanted traffic.

Test

Generate traffic that does not match any of the above 27 rules.

3. Audit Your Security Architecture

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

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

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

3.1. Planning the Assessment

3.1.1. Preliminary Meeting

- Sign Non-Disclosure Agreements (NDA) to protect the client's corporate assets. Show client that audit firm has appropriate insurance coverage for any damage caused by perimeter assessment.
- Recommend the client consider running a background check for each member of the audit team to ensure authenticity.
- Inform the ISPs of perimeter audit since they may have IDS tools in place.
- Obtain a list of emergency (7x24) contact numbers in case the audit takes a production host down.

3.1.2. Scope

The perimeter assessment includes:

- I. The testing of both the E-Commerce and Corporate perimeters from the internet and from within each network segment. This includes a review of the firewall and router rulebases. Any denial of service or concentrated brute force tests will be completed during a maintenance period or during an inactive time during the day (or night) to minimize the possibility of host failure. All other parts of the audit can be completed during prearranged times.

- Network Mapping

Network mapping is the starting point of the audit whose purpose is to gather as much information about GIAC Enterprises internet accessible hosts and services.

First the whois database (i.e. <http://whois.networksolutions.com>) is queried to gather any domain contacts, DNS servers, etc.

Secondly, the DNS servers themselves are queried to gather data about the external network(s), email gateways, versions of BIND running, source of authority detail, and any available hosts. A zone transfer will also be attempted to obtain all the DNS information. Tools such as nslookup, dig, and Sam Spade will be used. Sam Spade (<http://samspade.org/ssw>) will be used in this audit.

Traceroute, tracert or Sam Spade will then gather information about the various hops and between the audit testing machine and the GIAC Enterprises nodes or their ISP. This provides detail on the intervening routers and firewalls that are seen.

Commence port scanning on each host accessible to the internet to determine which (if any) ports and services are active. A tool called Retina (<http://www.eeye.com/html/Products/Retina/overview.html>) will be employed although several other good tools exist (e.g. Nmap, <http://www.insecure.com/nmap>). Retina's Scanner module initiates the port scanning but also utilizes other modules to deal with specific ports and services.

Initiate port scanning from the other service networks including the trusted network to simulate first line systems being compromised. This will test the other layers of defence.

- **Gaining Access and Denial of Service (DoS)**

After the active ports and services have been identified by the Retina:Scanner module, the other modules are initiated.

The Retina:Scanner module itself initiates an Audit on those active ports and services looking for explicit security flaws and any vulnerabilities. These include but are not limited to: DNS, FTP servers, Mail Servers, other IP services, and Remote Access tools. The Audit also initiates various DoS attacks.

The Retina:Miner module is the run against the web servers to gather data about web site and run such operations as guessing passwords or locating hidden web pages.

- **Detection**

Did the logs and alerts detect our audit? In order for a the perimeter defence to be complete, intrusion and port scanning attempts like those performed during this audit must be logged and alerted.

- II. Audit of host (including border routers) security. Titan (<http://www.fish.com/titan>) will be used to audit all Solaris hosts located in the screened networks.

Estimated Level of Effort and Costs

Task	Estimate Time	Cost
E-Commerce and Corporate Perimeter Audit	2 days	\$3000
Host Security Audit	1 day	\$1500
Security Architecture and Rulebase Review	1 day	\$1500
Generate Perimeter Analysis Findings	1 day	\$1500

This is an estimate only and is subject to availability of resources, access to GIAC Enterprises perimeter infrastructure and speed of any required internet connections.

3.2. Implementing the Assessment

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

The investigation commences with a query to the whois database at <http://whois.networksolutions.com> which would look something like this:

Registrant:

GIAC Enterprises Ltd. (GIACENTER-DOM)
555 Wall Street
Parsipanny, NJ 123456
US

Domain Name: GIACENTER.COM

Administrative Contact, Technical Contact, Billing Contact:
Alex, Tomas (TA1111) tomas.alex@GIACENTER.COM
Giac Enterprises Ltd.
555 Wall Street
Parsipanny, NJ 123456

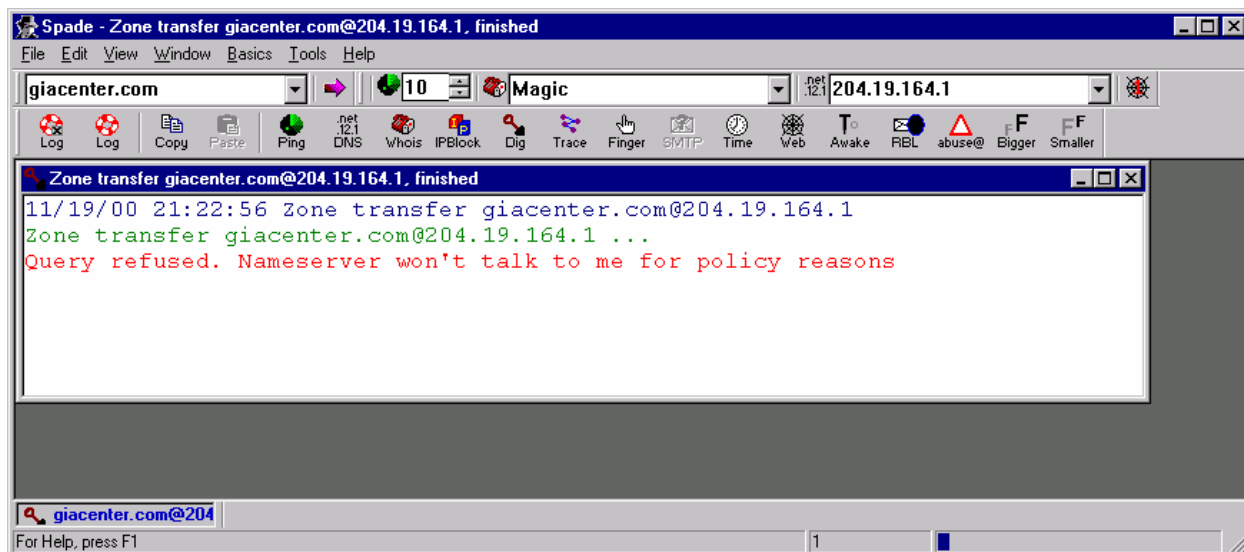
US
973-555-5555 (FAX) 973-555-5554

Record last updated on 01-Apr-1998.
Record expires on 01-Apr-2001.
Record created on 01-Apr-1998.
Database last updated on 19-Nov-2000 10:58:47 EST.

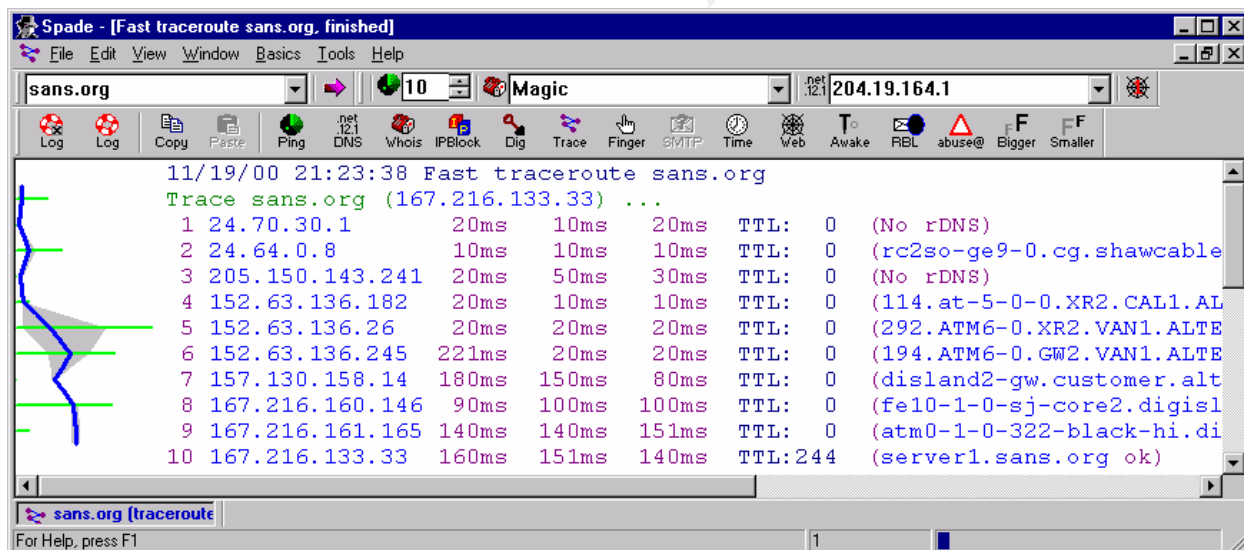
Domain servers in listed order:

NS.GIACENTER.COM 198.161.236.4
DNS.ISP.COM 198.161.236.2

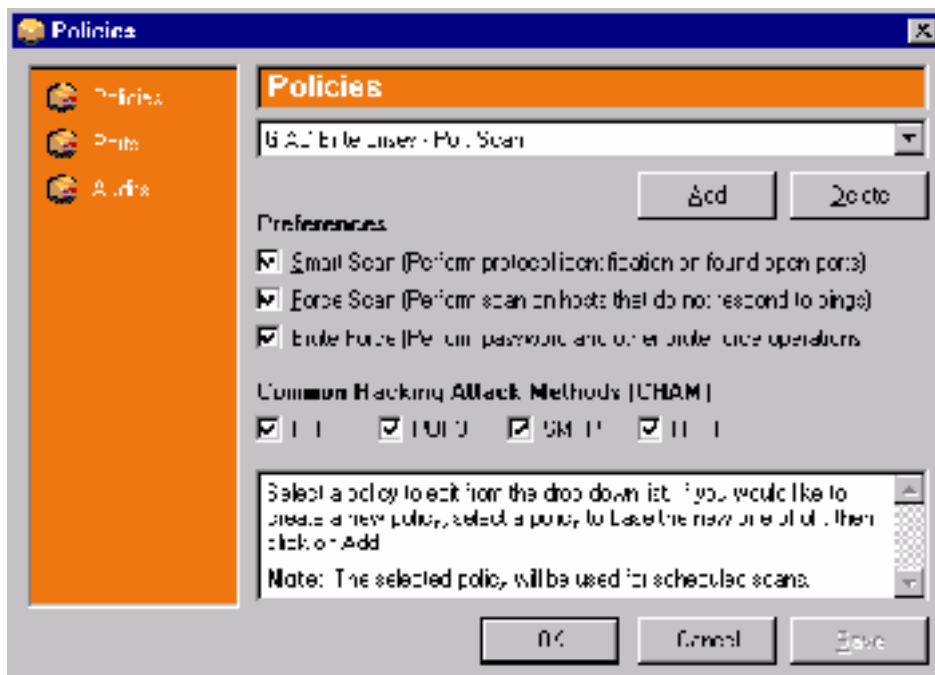
Next a zone transfer is attempted. The results should appear similar to this. The GIAC Enterprises name server should not allow zone transfers to the anything but its secondary name servers.



We can continue with Sam Spade and execute a trace (i.e. traceroute) to determine the route packets take between our auditing host and a selected GIAC Enterprises address. The actual trace would look similar to this:

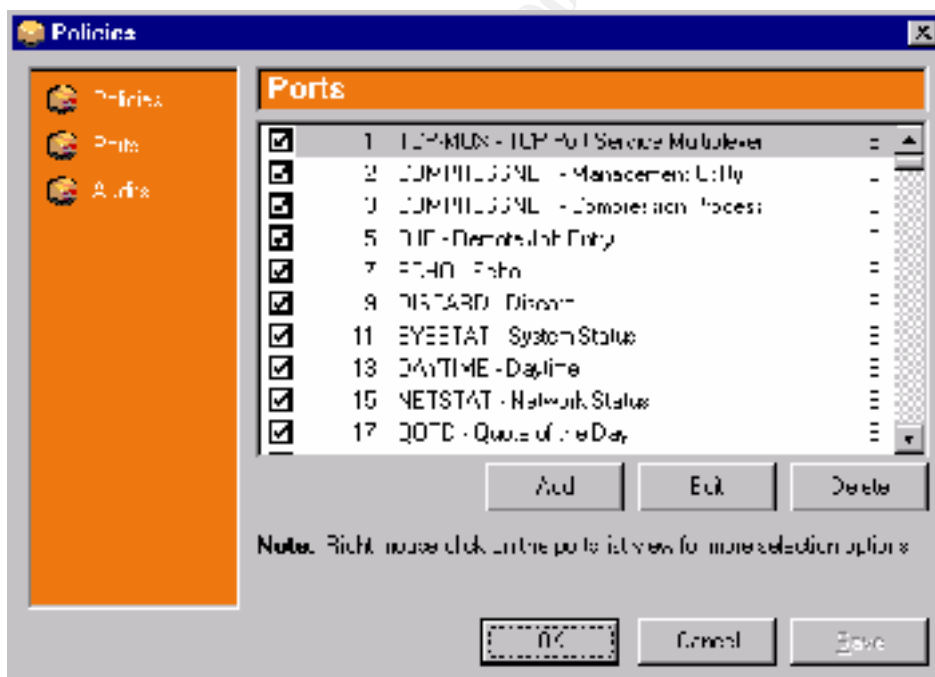


The port scanning commences to determine which ports and services are active from the internet on the GIAC Enterprises internet address space. The internet address space consists two separate address ranges: one for the online fortune cookie web servers and one for the other internet required services.



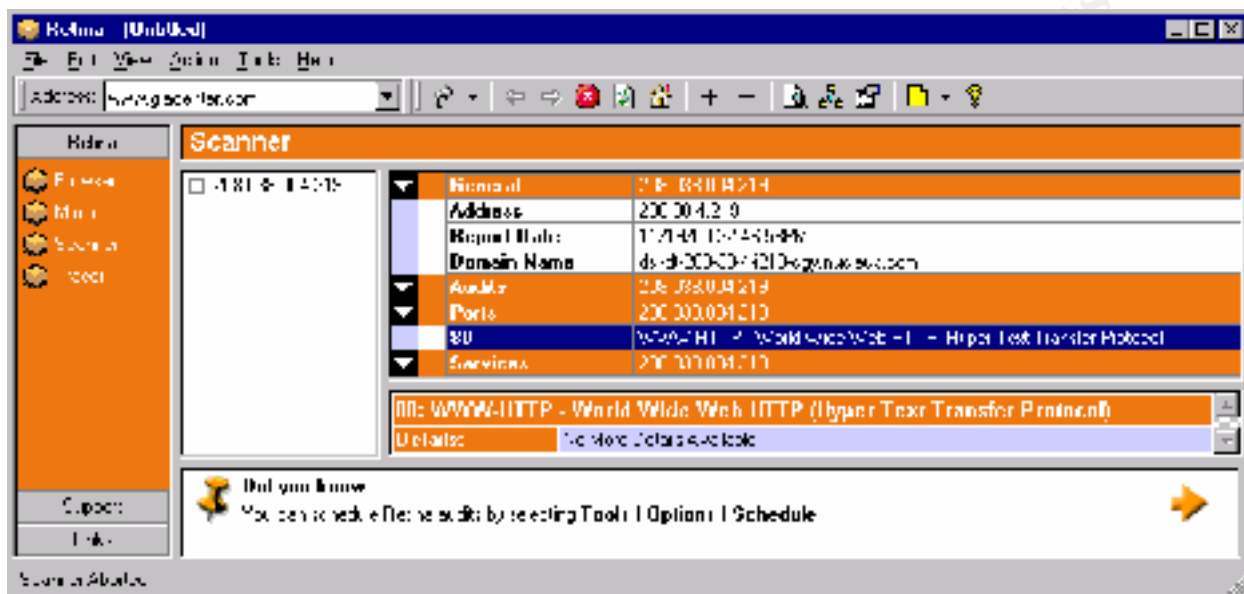
A policy in Retina:Scanner is configured to perform the following types of scans:

And all of the ports available to Retina:Scanner are selected:



Note that this initial port scan (tcp and udp) of both networks will take an excessive amount of time (due to the timeout period) since there a lot of ports (most ports between 1-1024 and other well known ports/services) on several hosts to be scanned.

The following is an example of the Retina front end:



Based on the security policy, we should expect to see the following ports to be detected. Note that there are no visible ports or services on the border routers or firewall. Also, if there was any deviation from this list, the firewall rulebases and router filters would need to be corrected.

Host	Port	Service
Public Web Server	80/tcp	http
Secure Web Server	443/tcp	https
SMTP Server	25/tcp	smtp
Primary DNS Server	53/udp	domain

Next, the Retina:Scanner audit component (includes DoS tests) can be run against any visible (open) ports listed above to discover any known vulnerabilities or exploits. If any vulnerabilities or exploits are detected, GIAC Enterprises will immediately be contacted and advised on corrective measures.

Finally, the web servers are now audited with Retina:Miner to gauge their response to a series of tests including such operations as guessing passwords or locating hidden web pages. Again, if any anomalies are detected, GIAC Enterprises personnel are contacted.

The auditor host should now be positioned on the other network segments in both the E-Commerce and Corporate perimeters and the series of scans repeated. This will check the firewall inbound and outbound rulebase between all of these network segments. This audit may reveal the presence of active ports or services which should not be running which could also indicate the presence of trojan horses.

All system log files will also be checked to ensure that the port scanning, vulnerability and exploit mapping, DoS attacks, and brute force attacks on the web servers was detected (i.e. logged or alerts). For example, the DoS and brute force attacks should activate the Checkpoint MAD (Malicious Activity Detection) script to generate an alert which monitors for such activity.

3.2.2. Keep security patches up-to-date.

The current policy for keeping security patches up-to-date is reviewed. Each host in both perimeters is manually logged on to and checked to ensure they are up-to-date with the latest security patches for all OSES and applications (e.g. backup software, web server software, database, etc.). Review current subscriptions to security mailing lists and add any that are missing (e.g. securityalert@sun.com). Verify Tripwire is functioning correctly and Solaris Fingerprint Database is being used.

3.2.3. Encrypt stored data accessible from the Internet.

Review all corporate data located on the perimeter to ensure that it has been stored in an encrypted manner. Identify any data that cannot be encrypted due to application functionality and review the file security.

Test any non-database encrypted data with the unix strings command to validate:

```
strings -a <encrypted-file>
```

No strings should be found in this file since it has been encrypted.

For the database, run SQL queries against the database to determine if returned data is encrypted.

3.2.4. Encrypt data sent across networks.

Tcpdump (<http://www.tcpdump.org>) will be used to audit the VPN link between offices, the SSL connection to the secure web server, and the SSH access to the perimeter for administrators. An audit host with tcpdump installed will be positioned on a shared hub with the appropriate perimeter firewall to capture the packets. We capture all the packets between the source and destination to ensure that all traffic is captured is valid.

- VPN Audit

```
tcpdump -n host testhost and host firewall > output.log
```

Where testhost is the remote office initiating the connection to a host within the perimeter through the firewall. Ensure all traffic encrypted specifically looking for ip protocol 50 and 51 packets (encapsulating security payload and authentication header).

- SSL Audit

```
tcpdump -n host testhost and host secure_web_server > output.log
```

Where testhost is an outside host with a browser initiating a connection to the secure web server. Ensure all traffic encrypted looking for destination tcp port 443 (SSL). Also verify the authenticity of the Verisign certificate on the secure web server by checking the detail on it within a web browser.

- SSH Audit

`tcpdump -n host testhost and host adminhost > output.log`

Where testhost represents the host initiating the connection and adminhost is the host to be administered. Verify that packets are encrypted looking for tcp port 22 (SSH).

3.2.5. Use and regularly update anti-virus software.

Verify procedures to monitor and update anti-virus lists in the CVP Server and Norton Anti-Virus software. Also ensure that Tripwire on the Solaris hosts is functioning correctly. This software should be configured for automatic anti-virus updates every few days.

Verifying anti-virus CVP server scanning:

Send mail to an internal GIAC Enterprises recipient with a relatively new virus to ensure the CVP Server detects and handles it. Verify web browsing and ftp outbound attempting download of virus are also detected and handled.

Verifying anti-virus on desktop (including road warriors)

Copy a relatively new virus on the desktop or mobile host and ensure anti-virus software detects and handles it.

Verifying anti-virus on Servers:

Modify a key system binary file (e.g. ls) and see if the Tripwire software detects if the MD5 checksum has changed during its next run.

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

In section 3.2.1, the auditing of the perimeters with the port scans on all network segments produced a map available port and services on the hosts. This map should directly correspond to the security policy which is based on restricted access to data by business "need to know".

Verification of the VPN access to data between the head office, remote offices, and partners will need to be conducted on each VPN for their specific servers and services they allow. Again, access to data must correspond to the security policy.

Verify that each individual user has a unique ID since business access to data may vary from user to user.

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

Ensure all personnel that require computer access to data on the perimeters have unique IDs.

Administrators

Verify by examining all Solaris host /etc/passwd and /etc/shadow files to ensure ID uniqueness. Also verify perimeter firewall user databases and SSH files for

Customers

Verify by examining application (i.e. web server) user database to ensure appropriate customer access to data is configured.

VPN

Review perimeter firewall VPN user databases to ensure ID uniqueness for remote office, partner, and mobile personnel.

3.2.8. Track access to data by unique ID.

Review all system and application log files to ensure all accessed data can be connected back to a unique ID. Ensure that the log files exist and are rotated on a daily basis in order to be more manageable for review. The log files to be inspected: all firewall log files, syslog server syslog file, Oracle log files, iPlanet web server log files, and any other application log files.

The log files will also be inspected for any unusual or suspicious activity and will be brought to the attention of the administrators.

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

Verify that all hosts in both perimeters have all appropriate system passwords changed or that those particular IDs have been disabled. Other security parameters to inspect would be: services and ports, file permissions, ip kernel variables, eeprom password, banners for services that are used, etc. Titan (<http://www.fish.com/titan>), a collection of modules that inspect and, optionally, lockdown a Solaris host, will be used to audit the systems.

The border routers will be checked against a known secure border router configuration.

3.2.10. Regularly test security systems and processes.

All of the processes mentioned in the prior VISA requirements, 3.2.1 through 3.2.9, should be routinely completed by GIAC Enterprises administrators since the perimeters (especially the security policy) and systems will always be changing due to business and technology themselves changing. Some products, like the anti-virus software and Retina, can be automatically scheduled. Other processes, patch updates, application changes, etc. will still require the manual approach in order to complete a security review.

3.3. Perimeter Analysis

The current GIAC Enterprises security architecture is a robust design and follows the VISA requirements to a good degree.

To improve the current design, the following recommendations have been made:

1. Install an IDS (Intrusion Detection System) on the perimeter-network segments.

Even though a host based IDS exists (Swatch) and an Integrity Checker IDS (Tripwire) already exist, the addition of a Network base IDS can add additional detection mechanism at a network level. They can analyze every packet for attack signatures and take the appropriate action. They should be installed at each network segment: E-Commerce/Corporate Perimeter-Web, Corporate-Management, Corporate-Data, Corporate-Service, and Corporate-Trusted (Figure 3). Several Network IDS products are available such as NFR (<http://www.nfr.com>).

2. Install an additional firewall between the Trusted network and the Corporate Perimeter firewall.

This adds another layer of defence between the Trusted network and the Corporate Perimeter firewall. The Corporate firewall's routing tables only contain routes to the Trusted network's firewall so the Trusted hosts cannot be reached directly from there in case of a compromise (Figure 3).

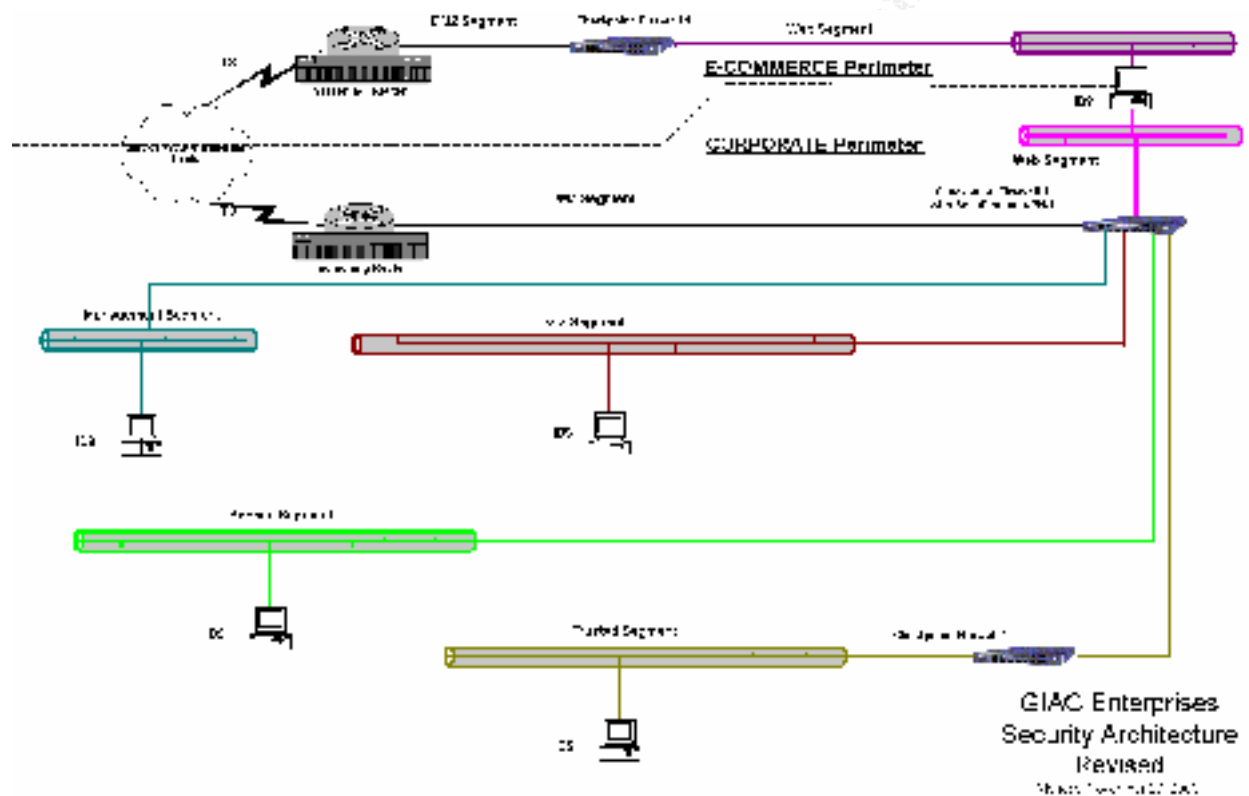


Figure 3.

3. Create high-availability clustered firewalls at the perimeters start.

A product such as RainWall (<http://www.rainfinity.com>) can improve the perimeter defence protecting against downtime due to unplanned or planned outages (Figure 4).

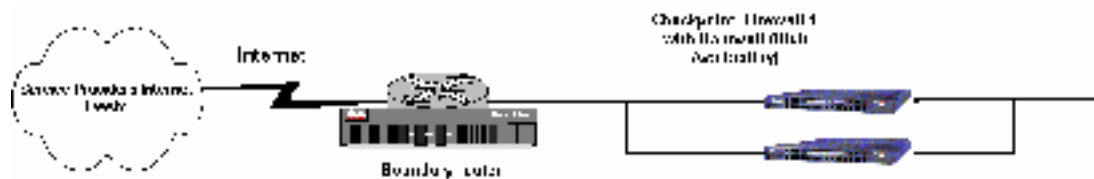


Figure 4.

4. Upgrade all personnel access to the perimeters with certificate authentication.

The use of certificates for all user authentication into the system (i.e. all users accessing the secured application server to carry out transactions) is recommended. Without certificate authentication (i.e. just userid and password), a user is only weakly authenticated because the authentication information can be entered from any browser. With strong authentication (such as certificates or Tokens), a user has to have a copy of the certificate database issued for that specific user, together with the database password – this information should never have been made publicly available, so is not easily obtainable by any hacker.

Administrative level users have access to additional functionality on the system. A physical token such as SecurID is recommend for these users.

5. Install Modular Syslog on the syslog server.

Improve the security of the syslog server with Modular Syslog (<http://www.core-sdi.com/english/freesoft.html>). All syslog data will can is now encrypted on the syslog server.