



# 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 Contents .....	1
Todd_Greenlaw_v2_GCFW.doc.....	2

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

GIAC Enterprises  
Security Architecture, Design and Detail  
SANS Network Security 2001 San Diego, CA Oct 15th - October 22nd

Submitted by: Todd William Greenlaw  
Submitted to: SANS GIAC - Firewalls, Perimeter Protection, and VPNs  
Submitted for: GCFW Practical Assignment version 1.6a  
Due Date: Dec 27, 2001  
Document name: Todd\_Greenlaw\_v2\_GCFW.doc

## Table of Contents

<a href="#"><u>Introduction</u></a>	4
<a href="#"><u>Design Principles</u></a>	4
<a href="#"><u>Assignment 1.0</u></a>	5
<a href="#"><u>1.1 GIAC Enterprises Business Plan</u></a>	5
<a href="#"><u>Sales and distribution Web Site</u></a>	5
<a href="#"><u>Manufacturing Portal</u></a>	5
<a href="#"><u>'Back Office' Infrastructure</u></a>	6
<a href="#"><u>1.2 Security Architecture - Core and Layers</u></a>	7
<a href="#"><u>1.3 Gateway Security Layer - High Available Filtering Routers</u></a>	8
<a href="#"><u>Purpose</u></a>	8
<a href="#"><u>Security Provided</u></a>	8
<a href="#"><u>Attack Prevention</u></a>	8
<a href="#"><u>Attack Detection - Logging</u></a>	9
<a href="#"><u>1.4 Core Security Layer - High Available (HA) Stateful Inspection Firewalls</u></a>	10
<a href="#"><u>Software Components</u></a>	10
<a href="#"><u>Hardware Components</u></a>	10
<a href="#"><u>Purpose</u></a>	10
<a href="#"><u>Security Provided</u></a>	10
<a href="#"><u>Attack Prevention – ACLs and Security Policy</u></a>	11
<a href="#"><u>Attack Detection – Detailed Logging and Alerting</u></a>	11
<a href="#"><u>1.5 Logical &amp; Physical Security Layer - Separate LANs</u></a>	12
<a href="#"><u>Hardware Components</u></a>	12
<a href="#"><u>Logical Components</u></a>	12
<a href="#"><u>Purpose</u></a>	12
<a href="#"><u>Security Provided</u></a>	12
<a href="#"><u>Service LAN</u></a>	12
<a href="#"><u>Management LAN</u></a>	13
<a href="#"><u>Office LAN</u></a>	14
<a href="#"><u>1.6 VPN Security Layer - IPSEC compliant VPN</u></a>	14
<a href="#"><u>1.7 Best Practices Security Layer</u></a>	15
<a href="#"><u>Assignment 2.0</u></a>	16
<a href="#"><u>2.1 Security Policy for the Internet Gateway Routers</u></a>	16
<a href="#"><u>Logging</u></a>	16
<a href="#"><u>Passwords</u></a>	16
<a href="#"><u>Source routing</u></a>	17
<a href="#"><u>Unnecessary Services</u></a>	18
<a href="#"><u>Directed broadcasts</u></a>	18
<a href="#"><u>Ingress and Egress Filters</u></a>	19
<a href="#"><u>Egress List</u></a>	19
<a href="#"><u>Ingress List</u></a>	19
<a href="#"><u>Login Banners</u></a>	22
<a href="#"><u>Restrict Access to Router</u></a>	23
<a href="#"><u>Allow only ssh into router</u></a>	23
<a href="#"><u>Test three rules</u></a>	24

<a href="#"><u>2.2 Firewall Security Policy</u></a>	27
<a href="#"><u>Firewall Properties – Security Policy Properties:</u></a>	28
<a href="#"><u>Security Policy Editor – Rule Base:</u></a>	31
<a href="#"><u>2.3 VPN Security Policy</u></a>	34
<a href="#"><u>Assignment 3.0</u></a>	35
<a href="#"><u>3.1 Audit of GIAC Enterprises Security Architecture</u></a>	35
<a href="#"><u>Phase 1 Technical Review</u></a>	35
<a href="#"><u>Phase 2 – Technical Audit</u></a>	37
<a href="#"><u>3.2 Security Audit</u></a>	37
<a href="#"><u>Firewall Audit Results</u></a>	38
<a href="#"><u>Audit Evaluation</u></a>	46
<a href="#"><u>Assignment 4.0</u></a>	47
<a href="#"><u>4.1 Design under fire</u></a>	47
<a href="#"><u>Vulnerability 1</u></a>	48
<a href="#"><u>Vulnerability 2</u></a>	48
<a href="#"><u>Vulnerability 3</u></a>	49
<a href="#"><u>Attack 1 – Attack on Firewall</u></a>	49
<a href="#"><u>Attack Defense</u></a>	50
<a href="#"><u>Attack 2 - Denial of Service Attack</u></a>	50
<a href="#"><u>Attack Defense</u></a>	51
<a href="#"><u>5.0 List of References</u></a>	52

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

## Introduction

Network architecture designed for a 'for profit organization' in most cases must be cost-effective, scalable, reliable and secure in order to ensure reliable efficient delivery of goods and services. The network design phase uses an iterative process and must focus on all aspects of the business model. The technology must support the business model and provide consistency throughout the organization.

The author of this document agrees with using a "Defenses in Depth" strategy; however the assumptions made for GIAC Enterprises places it into the medium to small business category. Having said that many businesses of this size do not have access to the expertise or capital required to build and maintain a network with complex design.

## Design Principles

The technology design decisions have been made with the following underlying principles and doctrine:

- 1) 'Design decisions made today will impact all aspects of GIAC Enterprises organization for many years to come'. The design must scale. Vendors that use open standards are preferred however products and vendors are chosen based on a best of breed approach.
- 2) 'Security and ease of use are polar opposites' GIAC Enterprises will attempt to use a common sense methodology as well as stay inbounds of the KIS (Keep It Simple) principle as much as practically possible. Redundancy will be used on core gateways, and core security enforcement points.
- 3) 'Protect against the SANS top 20'. GIAC Enterprises network security will strive to protect against the top network security threats as listed on the SANS Institutes "The 20 Most Critical Internet Security Vulnerabilities" list  
<http://www.sans.org/top20.htm>.

## **Assignment 1.0**

### **1.1 GIAC Enterprises Business Plan**

The business plan of GIAC Enterprises is the creation of an e-business that securely and profitably sells fortune cookie sayings online. GIAC Enterprises network is designed and deployed using technology in order to execute this business plan. The execution of this business plan is the creation of a secure online manufacturing, sales, production and distribution network. The foundation of this network includes the following components:

#### **Sales and distribution Web Site**

An e-commerce enabled web site for the sales and marketing of fortune cookie sayings to customers and business partners. The site also provides general company related information to the public. The GIAC secure web site is a secure online market place for the sales and distribution of fortune cookie sayings directly to customers and to business partners. The online market place web site is enabled with a VeriSign 128-bit SSL (Secure Sockets Layer) Global Server ID. This digital server certificate guarantee's the web sites authenticity and enables customers and business partners to connect to the secure web site using an SSL enabled web browser. The communications between the web browser and the web server are encrypted. The partners and clients authenticate to the site with a unique user ID and password. This authentication is passed on to separate directory server infrastructure located in the backend management network as will be detailed in following sections. The user ID and password uniquely identifies the company and individual purchaser. The purchasers have the ability to place bulk orders online from anywhere in the world. The order is verified and passed into the backend management LAN for accounting and fulfillment purposes.

For further information on Secure Server Digital Certificates and Certificate Authorities please refer to the following web site; <http://www.verisign.com>.

#### **Manufacturing Portal**

A Virtual Private Network (VPN) will facilitate the manufacturing of fortune cookie sayings by providing a secure online workspace for the authors of fortune cookie sayings. This workspace will consist of an IPSEC host to site (GIAC Network) VPN. The remote suppliers access the fortune-maker application located on the GIAC backend management LAN. The remote hosts use an IPSEC compliant VPN client that is used to establish an encrypted tunnel with the IPSEC VPN gateway. Once connected the remote user is authenticated by passing logon credentials to the backend directory server infrastructure. The remote user is then able to launch the fortune-maker application.

### 'Back Office' Infrastructure

The 'back office' network infrastructure consists of the office network infrastructure and applications that enable GIAC Enterprises business functions. The infrastructure includes: desktops, printers, servers, applications, fulfillment and accounting systems.

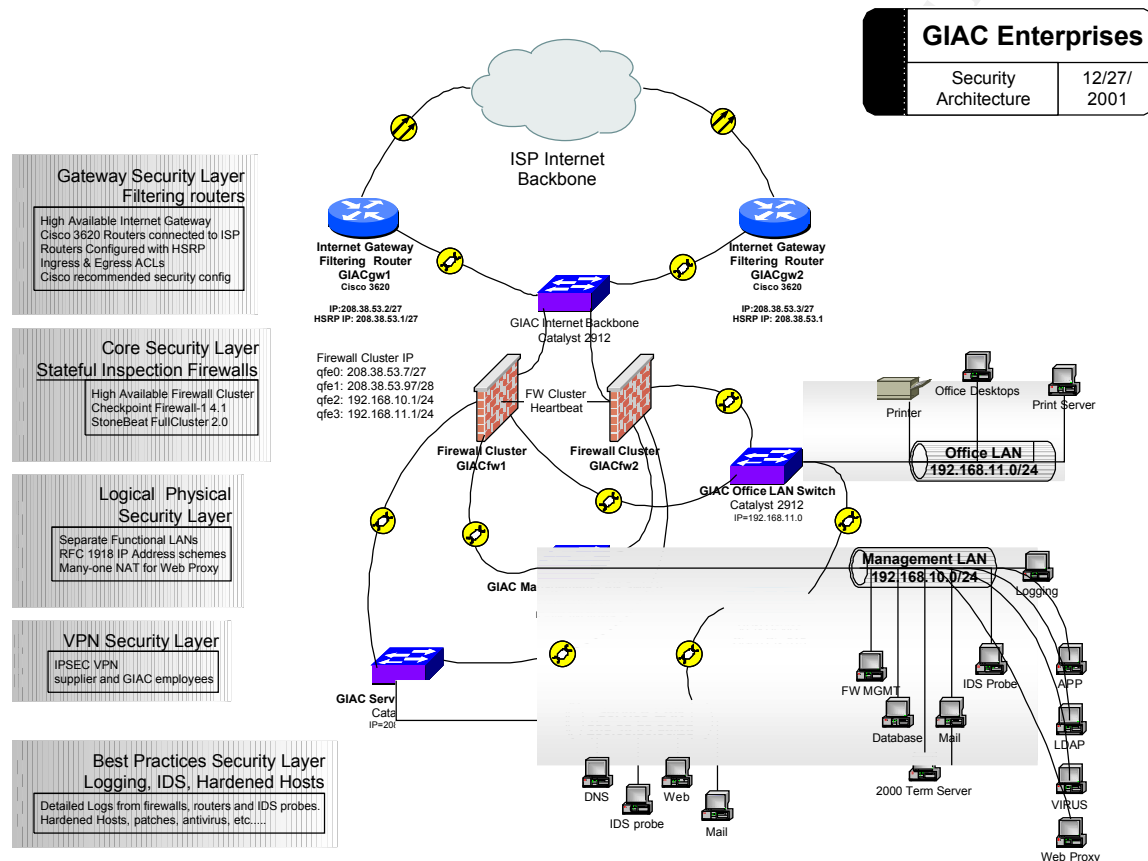
The back office network supports remote GIAC employees using the host to site VPN infrastructure. Remote GIAC employees connect to the VPN gateway using an IPSEC VPN client. Once authenticated to the backend directory server infrastructure the remote workers access all GIAC applications by launching a Windows 2000 Terminal server client and connecting to the Windows 2000 Terminal Server farm located on the GIAC management LAN.

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



## 1.2 Security Architecture - Core and Layers

In order to achieve the goals of the business plan deliverables as stated previously, the technology security roadmap uses a layered approach. The goal is to create several security layers around the infrastructure. The core layer of this design is stateful inspection firewalls. The core is surrounded with additional layers as indicated in the following diagram:



	Service Net	Management Net	Office Net	Address Translation
Address Scheme	208.38.53.96/28	192.168.10.0/24	192.168.11.0/24	
GIACfw1	208.38.53.98	192.168.10.2	192.168.11.2	
GIACfw2	208.38.53.99	192.168.10.3	192.168.11.3	
Firewall-Cluster	208.38.53.97	192.168.10.1	192.168.11.1	
GIAC Web	208.38.53.100			
GIAC Mail External	208.38.53.101			
GIAC DNS	208.38.53.102	192.168.10.21		
GIAC VPN	208.38.53.103		192.168.11.10	
Database Server		192.168.10.20		
Internal Mail Server		192.168.10.21		
Log server		192.168.10.22		
Directory Server		192.168.10.23		
LDAP				
Data backup Server		192.168.10.24		
Web Proxy Server		192.168.10.25		Hide NAT 205.233.109.65
Win 2000 Terminal Server		192.168.10.26		

--	--	--	--	--

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

### 1.3 Gateway Security Layer - High Available Filtering Routers

#### Hardware Components

Two - Cisco 3620 routers, each configured with two Fast Ethernet Interfaces.

<http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm>

#### Software Components

IOS - c3620-is-mz.120-16 IP Plus

Hot Standby Configuration (HSRP)

#### Purpose

GIAC Enterprises hosts all major components of the e-business infrastructure at GIAC premises therefore; high-speed reliable Internet connectivity is essential. The gateway routers connect GIAC Enterprises core firewalls to the Internet backbone through a tier one Canadian telecommunication provider. These gateway routers are critical to the delivery of services to the major stakeholders of GIAC Enterprises. The gateway routers also provide routing enabling GIAC Enterprises to conduct online business.

#### Security Provided

The security provided by the gateway routers can be broken into two areas; attack prevention (defense) and attack detection (offence). Attack prevention is a properly configured and hardened router with static filters at the ingress and egress interfaces. Attack detection is a router properly configured to provide detailed logging.

#### Attack Prevention

The gateway routers use static packet filters as the first layer of perimeter security. These static packet filters take the form of extended access lists on the gateway routers. The access lists are: Ingress/inbound filtering of traffic entering GIAC Enterprises from the Internet and Egress/outbound filtering of traffic leaving GIAC Enterprises to Internet. The static packet filters; ingress/egress combined with internet router security recommendations from Cisco provide a layer of protection against several security threats such as anti-spoofing and denial of service. The gateway router configurations address some of the SANS Institutes "The 20 Most Critical Internet Security Vulnerabilities" list <http://www.sans.org/top20.htm>. These recommended security configuration enhancements and the ingress and egress access lists are detailed in section two of this paper. For information pertaining to securing Cisco router please refer to the following web page; <http://www.cisco.com/warp/public/707/21.html>.

The redundant architecture provides a further level of protection against Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS).

### Attack Detection - Logging

The gateway routers provide detailed logging information as the first layer of intelligence gathering on the state of traffic behavior. The routers log to a syslog server on the management network. Scripts will search the logs for suspicious events. The logging server is configured for alerting via email and paging.

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

## 1.4 Core Security Layer - High Available (HA) Stateful Inspection Firewalls

### Software Components

Two Checkpoint Firewall-1 Version 4.1 Firewalls, Service pack 5

<http://www.checkpoint.com/products/security/firewall-1.html>

StoneBeat FullCluster for Firewall-1 2.0 service pack 5

<http://www.stonesoft.com/products/stonebeat/fullcluster.html>

### Hardware Components

Two Sun Microsystems NetraT105 servers, Solaris 5.6 Operating System, and patch cluster Generic\_105181-29.

### Purpose

The stateful inspection firewalls act as the security core of GIAC Enterprises. As with the filtering routers high throughput and reliability are required for the proper execution of the GIAC business plan. Stateful inspection firewalls were chosen for the purposes of performance while still maintaining a relatively high security standard. Checkpoint Firewall-1 will be configured in a high available firewall cluster using StoneBeat's FullCluster for Firewall-1 software. The high available cluster provides stateful inspection filtering for all GIAC networks. The firewall cluster is configured in a hot-standby (active-standby) configuration but can be reconfigured for load balancing (active-active) if required.

### Security Provided

As with the gateway routers the security provided by the firewall cluster is a combination of attack prevention and attack detection. Attack prevention is a combination of the firewall clusters properly configured global security properties and the security policy rule base (access control list). These two areas control what traffic is allowed to traverse the firewall interfaces. Attack detection is provided by the firewall clusters logging and alerting features.

### Attack Prevention – ACLs and Security Policy

The firewall cluster provides all security policy enforcement for GIAC. This enforcement includes access control at the perimeter and access control between the various GIAC networks. The HA firewalls connect the trusted GIAC networks to un-trusted networks namely the Internet via the gateway routers. The firewall cluster rule base and the security policy are concerned with but not limited to the protecting GIAC network resources from common attacks, hostile intent and unintentional abuse within GIAC and from the Internet. The firewall rule base and security policy have several core areas of responsibility they are indicated below:

- 1) Denying all access to all unnecessary services or unused ports and permitting access only to those specific services and ports required to communicate with applications. This may sound obvious but it must be stated and addresses several of the SANS Institutes “The 20 Most Critical Internet Security Vulnerabilities” <http://www.sans.org/top20.htm> list. These are detailed further in section 2 of this document.
- 2) Protection from common attacks such as denial of service and SYN flooding. The redundant architecture allows for a level of protection against Denial of Service (DoS) and Distributed DDoS attacks.

### Attack Detection – Detailed Logging and Alerting

Detailed logging at the firewall provides another source of intelligence on normal versus abnormal network traffic behavior. The logging and alerting features will be used to send a combination of pages and email on events of interest. Checkpoint Firewall-1 has a feature known as MAD - Malicious Activity Detection. MAD will look for predefined patterns in the log file and send alerts based on these patterns. This is not a full-blown IDS as the predefined alerts are relatively static. MAD will be used as an additional layer to alert when abnormal traffic patterns are detected.

## 1.5 Logical & Physical Security Layer - Separate LANs

### Hardware Components

Cisco 2900 Switches

<http://www.cisco.com/univercd/cc/td/doc/pcat/2900.htm>

### Logical Components

RFC 1918 IP Addressing

Network Design – Separating networks

### Purpose

GIAC consists of four functional networks providing distinct services to facilitate the execution of the business plan. Each functional LAN uses a separate IP address scheme. Each network terminates on a separate interface at the firewall cluster. Each LAN aggregates on separate Cisco 10/100 Mb switches. The functions of each LAN are described in following sections.

### Security Provided

Separating the LANs into functional areas and terminating each LAN at the firewall will control what traffic is allowed to traverse what interface. Separating functional areas creates the desired layered effect at the security core. If a host is compromised the damage may be contained in one area. Another area of risk mitigation is the use of non-routable RFC 1918 address space for internal networks and the many-to-one network address translation (NAT) used for the outgoing web proxy.

### Service LAN

The services LAN uses a routable (legal) IP address scheme and hosts the major e-business infrastructure namely the; corporate web server (HTTP, HTTPS), mail server (SMTP), a domain name resolution server (DNS-udp-53), IDS probe, and the site VPN termination device (IPSEC protocols). All IP traffic in and out of the service LAN is processed by the firewall cluster. The security policy is defined in section 2 of this document however; the service LAN is the only network accepting in-bound stateful traffic from the Internet. Traffic from the Internet into the service LAN is primarily concerned with providing Internet and VPN services to customers, business partners, suppliers and employees.

### Traffic Flow

- Stateful Communication to Internet  
Services: Mail, DNS
- Stateful communications to management network  
Services: Database, Data backup, Mail, Logging

- Stateful Communication to office LAN  
Services: None
- Stateful communication from Internet  
Services: Web, Secure Web, DNS udp-53, Mail, IPSEC
- Stateful communication from Management LAN  
Services: Mail, FTP, SSH, DNS
- Stateful communication from Office LAN  
Services: None

### Management LAN

The management LAN uses an RFC 1918 <http://www.ietf.org/rfc/rfc1918.txt> compliant address scheme. The Management LAN hosts the major network infrastructure of the "Back Office" administrative and operations data network required to support a combination of billing, client relationship, order fulfillment and service management for GIAC Enterprises. The management LAN hosts the following services; database server, firewall management server, internal mail server, IDS probe, data backup server, Windows 2000 terminal servers, logging servers, the fortune-maker application server, a virus server, and a web proxy server configured with many-one NAT.

### Traffic Flow

- Stateful Communication to Service Network  
Services: Mail, SSH, DNS
- Stateful Communications to Internet  
Services: Web, secure Web
- Stateful Communication to Office LAN  
Services: None
- Stateful Communication flows from Internet  
Services: None
- Stateful Communication from Service Network  
Services: Mail, Database, Logging, Data backup
- Stateful Communication from Office LAN  
Services: Windows 2000 Terminal Server remote desktop protocol



### Office LAN

The office LAN uses an RFC 1918 compliant address scheme and hosts the GIAC employee's workstations, printers, and print servers. GIAC employees access all desktop and company applications including the internet using a windows 2000 terminal server client that connects to a Windows 2000 Terminal server farm located on the management LAN. All applications reside on the management LAN. This concept uses a centralized computing model that GIAC systems administrators can control from a single point.

### Traffic Flow

- Stateful Communication to service LAN  
Services: IPSEC via VPN Gateway
- Stateful Communication to Internet  
Services: None
- Stateful Communications to Management LAN  
Services: Windows 2000 Terminal Server Client, TCP-3389
- Stateful Communication from service LAN  
Services: IPSEC via VPN Gateway
- Stateful Communication from Internet  
Services: None
- Stateful Communication from Management LAN  
Services: None

### 1.6 VPN Security Layer - IPSEC compliant VPN

Components: Cisco Pix 515

The site VPN device will connect the service LAN to the office LAN. This device provide an IPSEC tunnel from the remote client device through the firewall cluster to specific services on the office LAN. The IPSEC VPN provides client-site secure, encrypted, and authenticated remote communication. Once authenticated through the VPN users run a Windows 2000 terminal client to access the required internal applications. The VPN allows authors of fortune cookie sayings access to the fortune-maker application on the management LAN and GIAC remote employees access to office apps on the Management LAN.

### 1.7 Best Practices Security Layer

I have included 'Best Practices' as a security layer because it may be one of the most important aspects of perimeter protection security. 'Best Practices' is a term banded about in many fields including network security. This term at the most basic level refers to 'how we do our jobs'. A person concerned about perimeter protection should adopt a set of procedures, policies, and day-to-day practices that help in the mitigation of risk. This can include but is not limited to ensuring that whenever a host or user is inserted onto a trusted network a validation process has been followed. This validation process is to mitigated risk for: applications, hosts, networks, and network devices. Best practices ensures the following items have been addresses prior to network insertion:

Hardened Operating Systems  
Intrusion Detection & Alerting  
Detailed Logging  
Daily backups  
Screen Savers  
Disaster Recovery Plan  
Minimum Password Policies  
Acceptable use policy  
Remote user policy

Threats can attack a network from several areas. Cisco has several white papers on this subject and I have included some excerpts about types of threats and threat mitigation from the following white paper:

[http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm)

#### Types of Threats

- ❑ Unauthorized access—Mitigated through filtering at the firewall
- ❑ Application layer attacks—Mitigated through HIDS on the public servers
- ❑ Virus and Trojan-horse attacks—Mitigated through virus scanning at the host level
- ❑ Password attacks—Limited services available to brute force; OS and IDS can detect the threat
- ❑ Denial of service—Committed access rate (CAR) at ISP edge and TCP setup controls at firewall to limit exposure
- ❑ IP spoofing—RFC 2827 and 1918 filtering at ISP edge and local firewall

#### Best Practices Threat Mitigation

- ❑ Packet sniffers—Switched infrastructure and host IDS to limit exposure
- ❑ Network reconnaissance—HIDS detects recon; protocols filtered to limit effectiveness
- ❑ Trust exploitation—Restrictive trust model and private VLANs to limit trust-based attacks
- ❑ Port redirection—Restrictive filtering and host IDS to limit attack

## Assignment 2.0

### 2.1 Security Policy for the Internet Gateway Routers

The security policy of the gateway routers are detailed in the following section of this document. The underlying goal of the security policy is to protect GIAC from the SANS Institutes “The 20 Most Critical Internet Security Vulnerabilities” list <http://www.sans.org/top20.htm>. The SANS “Top 20” is a consensus document detailing the current top 20 critical Internet security vulnerabilities. The gateway routers are configured with Cisco recommended security enhancements that help in the prevention of; denial of service attacks, route hijacking, and exploitation of unneeded router services.

This section details the gateway router security configuration. For readability the entire router configuration is not included. Included are the areas deemed to be critical to the security policy. The syntax below was used with the purpose of allowing someone the ability to cut and past into a router configuration if desired.

#### Logging

Logging should be enabled to provide an audit trail. The following commands enable detailed logging.

GIACgw1# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# **Logging buffered 10000**

**Logging trap debugging**

**Logging facility local2**

! log to syslog server located on management LAN

**Logging 192.168.10.22**

! turn on log message time stamping

**Service timestamps debug datetime localtime show timezone msec**

#### Passwords

Encrypt the exec user password using the stronger encryption of the ‘enable secret’ command. Do not use the ‘enable password’ command. The ‘service password encryption’ command should still be used to encrypt all other passwords. These commands are performed in the global configuration mode.

GIACgw1# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# **service password-encryption**

**enable secret**

**no enable password**

### Source routing

The IP protocol has options that allow the sender of a packet to control its route to the destination. This can be used legitimately for troubleshooting but in most cases is used by those with hostile intent for session hijacking. This is disabled with the following command in global configuration mode.

GIACgw1# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# **no ip source-route**

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

### Unnecessary Services

As stated previously all unnecessary services pose a security risk and must be disabled. The following services are global services on the router that should be disabled as part of this philosophy. These services are disabled from the routers global configuration mode.

GIACgw1# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
GIACgw1(config)#  no ip finger
                  no service tcp-small-servers
                  no service udp-small-servers
                  no ip bootp server
                  no cdp run
                  no service pad
                  no ip bootp server
```

### Interface Services not required for a router connected to the Internet

Cisco has certain services that when connected to the Internet are vulnerable and should be disabled. Commands below will disable these vulnerable services when performed in the router interface configuration mode.

GIACgw1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# Interface FastEthernet0/0

```
GIACgw1(config-i)# ip address 205.233.109.2 255.255.255.0
                  ip access-group Ingress in
                  no ip redirects
                  no ip proxy-arp
                  ntp disable
                  no cdp enable
```

### Directed broadcasts

A directed broadcast is a feature that allows a request to be sent to all hosts on a network. A person with hostile intent can use it for intelligence gathering purposes and denial of service attacks such as the well-known 'Smurf attack'. The command below is performed in the router interface configuration mode.

GIACgw1#conf terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# Interface FastEthernet0/0

```
GIACgw1(config-i)# no ip directed-broadcast
```

### Ingress and Egress Filters

This section of the router configuration includes the ingress and egress static packet filters. Ingress and Egress filters protect against several of the SANS "Top 20". The access lists refer to specific vulnerabilities however these filters may not be practical in every situation. The routers are directly connected to the Internet, which is the border between GIAC and the largest un-trusted network in the world. The main point is that you must prevent as much as you can at this layer. This includes; spoofed addresses, vulnerable services, denial of service, and services that should not be running anyway. The filters are detailed and explained in this section of the document. The specific vulnerability each filter is protecting against is also included next to the filter.

Access lists have to be enabled per router interface. The Egress and Ingress Filters are applied to the router interfaces as shown below.

GIACgw1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# Interface FastEthernet0/1

GIACgw1(config-i)# **ip access-group egress in**

GIACgw1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)# Interface FastEthernet0/0

GIACgw1(config-i)# **ip access-group ingress in**

Named - access lists are created by starting in global configuration mode, naming the access list and then building the access list as indicated below with the ingress and egress access lists.

### Egress List

GIACgw1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)#**ip access-list extended Egress**

!

! Anti Spoofing from inside GIAC - Permit only my routable address space outbound.

! Top 20 Ref # - G5 Not filtering packets for correct incoming and outgoing addresses.

permit ip 208.38.53.96 0.0.0.7 any

permit ip 205.233.109.65 0.0.0.0 any

!

! Deny all other Traffic outbound.

deny ip any any

!

### Ingress List

GIACgw1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

GIACgw1(config)#**ip access-list extended Ingress**

! Anti Spoofing from outside GIAC - Deny all RFC 1918 Address Space inbound.

! Top 20 Ref # - G5 Not filtering packets for correct incoming and outgoing addresses.

! Ref RFC 2827 Network Ingress Filtering <http://www.ietf.org/rfc/rfc2827.txt>

! RFC 3013 Recommended Internet Service Provider Security Services and Procedures.

! Ref <http://www.ietf.org/rfc/rfc3013.txt>

deny ip 10.0.0.0 0.255.255.255 any log

deny ip 172.0.0.0 0.240.255.255 any log

deny ip 192.168.0.0 0.0.255.255 any log

!

! Anti Spoofing from outside GIAC - Deny My routable Address Space.

! Top 20 Ref # - G5 Not filtering packets for correct incoming and outgoing addresses.

deny ip 208.38.53.96 0.0.0.7 any log

deny ip 205.233.109.65 0.0.0.0 any log

!

! Anti Spoofing from outside GIAC - Deny IANA Reserved Address Space

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

! Top 20 Ref # - G5 Not filtering packets for correct incoming and outgoing addresses.

deny ip host 0.0.0.0 any log

deny ip 1.0.0.0 0.255.255.255 any log

deny ip 2.0.0.0 0.255.255.255 any log

deny ip 5.0.0.0 0.255.255.255 any log

deny ip 7.0.0.0 0.255.255.255 any log

deny ip 23.0.0.0 0.255.255.255 any log

deny ip 27.0.0.0 0.255.255.255 any log

deny ip 31.0.0.0 0.255.255.255 any log

deny ip 37.0.0.0 0.255.255.255 any log

deny ip 39.0.0.0 0.255.255.255 any log

deny ip 41.0.0.0 0.255.255.255 any log

deny ip 42.0.0.0 0.255.255.255 any log

deny ip 58.0.0.0 1.255.255.255 any log

deny ip 58.0.0.0 1.255.255.255 any log

deny ip 59.0.0.0 1.255.255.255 any log

deny ip 60.0.0.0 0.255.255.255 any log

deny ip 69.0.0.0 0.255.255.255 any log

deny ip 70.0.0.0 0.255.255.255 any log

deny ip 71.0.0.0 0.255.255.255 any log

deny ip 79.0.0.0 7.255.255.255 any log

deny ip 82.0.0.0 1.255.255.255 any log

deny ip 84.0.0.0 3.255.255.255 any log

deny ip 88.0.0.0 7.255.255.255 any log

deny ip 96.0.0.0 31.255.255.255 any log

!

! Deny Netbios Traffic  
 ! Information Leakage. Deny traffic from services that are not needed.  
 ! Top 20 Ref - W4 NETBIOS - unprotected Windows networking shares.  
 ! Top 20 Ref - W5-Information leakage via null session connections.  
 ! Top 20 Ref - Appendix A Common Vulnerable Ports.  
 deny tcp any any range 135 139 log  
 deny udp any any range 135 netbios-ss log  
 !  
 ! Deny TFTP Traffic  
 ! Information Leakage. Deny traffic from services that are not needed.  
 ! Top 20 Ref - Appendix A Common Vulnerable Ports.  
 deny udp any any eq tftp log  
 !  
 ! Deny syslog Traffic  
 ! Information Leakage. Deny traffic from services that are not needed.  
 ! Top 20 Ref - Appendix A Common Vulnerable Ports.  
 deny udp any any eq syslog log  
 !  
 ! Deny SNMP Traffic  
 ! Information Leakage. Deny traffic from services that are not needed.  
 ! Top 20 Ref - Appendix A Common Vulnerable Ports.  
 ! U7-Default SNMP Strings  
 deny udp any any range snmp snmptrap log  
 !  
 ! Deny RPC  
 Top 20 Ref # - U1 Buffer Overflows in RPC.  
 deny tcp any any 111 log  
 !  
 ! Deny LPD  
 To 20 Ref # - U5 Buffer Overflow LPD.  
 deny tcp any any 515 log  
 !  
 ! Deny ICMP Redirects  
 ! An ICMP redirect message instructs an end node to use a specific router as its path to a !  
 particular destination.  
 deny icmp any any redirect log  
 !  
 ! Deny Multicast Addresses  
 ! Top 20 Ref # - G5 Not filtering packets for correct incoming and outgoing addresses.  
 deny ip 224.0.0.0 31.255.255.255 any log  
 !  
 ! Deny DHCP Auto Configuration Addresses  
 ! Top 20 Ref # - G5 Not filtering packets for correct incoming and outgoing addresses.  
 deny ip 169.254.0.0 0.0.255.255 any log  
 deny ip 192.0.2.0 0.0.0.255 any log





### Restrict Access to Router

Enable ACLs on vty Ports by creating access lists and then applying the access lists to the console and auxiliary ports as shown below.

!

```
GIACgw1(config)# access-list 15 permit 192.168.10.0 0.0.0.255
                  access-list 15 deny any
```

!

```
GIACgw1(config)# line con 0
                  transport input none
                  line aux 0
                  access-class 15 in
                  transport input all
                  line vty 0 4
                  access-class 15 in
                  password 7 1451045318007D
```

!

!

### Allow only ssh into router

!

```
GIACgw1(config)# transport input ssh
```

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

### Test three rules

Rule: Ingress Anti-spoofing

deny ip 208.38.53.96 0.0.0.7 any log (210 matches)

Test: Attempt to connect through router with a spoofed address. Verify router logs to ensure spoofed address is blocked.

Nmap:

nmap -S 208.38.53.98 -e0 -sS -P0 208.38.53.97

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security ( <http://www.eEye.com> )

based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Router Logs:

\*Dec 1 03:57:31 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.98(45721) -> 208.38.53.97(760), 1 packet

\*Dec 1 03:57:37 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.98(45719) -> 208.38.53.97(259), 1 packet

\*Dec 1 03:57:43 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.98(45720) -> 208.38.53.97(259), 1 packet

\*Dec 1 03:57:49 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.98(45721) -> 208.38.53.97(259), 1 packet

Rule: Deny Access to router (Access list on vty ports)

```
permit 192.168.10.0, wildcard bits 0.0.0.255
deny any log
```

Test: Attempt a telnet connection to the router from a source address that is not permitted.  
Insert a sniffer between attacking host and the router. Verify sniffer trace with results from nmap to ensure address is blocked.

Nmap:  
nmap -sT -p23 -P0 208.38.53.1

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com  
eEye Digital Security ( <http://www.eEye.com> )  
based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

The 1 scanned port on (208.38.53.1) is: closed  
Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds

Tcpdump Results:

```
tcpdump host 208.38.53.1
tcpdump: listening on \Device\NPF_{5B975FCB-FBBD-46F3-B3DE-8743159B09D2}
23:19:34.442209 208.38.53.10.1436 > 208.38.53.1.23: S 3600425395:3600425395(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
23:19:34.443318 208.38.53.10.1436 > 208.38.53.1.23: S 3600425395:3600425395(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
23:19:34.446229 208.38.53.1.23 > 208.38.53.10.1436: R 0:0(0) ack 3600425396 win
0
23:19:34.867345 208.38.53.10.1436 > 208.38.53.1.23: S 3600425395:3600425395(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
23:19:34.868159 208.38.53.10.1436 > 208.38.53.1.23: S 3600425395:3600425395(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
23:19:34.871087 208.38.53.1.23 > 208.38.53.10.1436: R 0:0(0) ack 1 win 0
23:19:35.368039 208.38.53.10.1436 > 208.38.53.1.23: S 3600425395:3600425395(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
23:19:35.368885 208.38.53.10.1436 > 208.38.53.1.23: S 3600425395:3600425395(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
23:19:35.371804 208.38.53.1.23 > 208.38.53.10.1436: R 0:0(0) ack 1 win 0
```

Rule: Ingress Deny Netbios ports

deny tcp any any range 135 139 log (108 matches)

deny udp any any range 135 netbios-ss log (8 matches)

Test: Attempt a connection through the router on a netbios port. Verify results from nmap against router logs.

Nmap:

nmap -p137-139 -P0 208.38.53.97

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security ( <http://www.eEye.com> )

based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Interesting ports on (208.38.53.97):

Port	State	Service
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 41 seconds

Router Logs:

Dec 1 04:16:11 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1234) -> 208.38.53.97(137), 1 packet

\*Dec 1 04:16:12 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1267) -> 208.38.53.97(137), 1 packet

\*Dec 1 04:16:14 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1303) -> 208.38.53.97(137), 1 packet

\*Dec 1 04:16:29 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1385) -> 208.38.53.97(137), 1 packet

\*Dec 1 04:16:35 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1388) -> 208.38.53.97(137), 1 packet

\*Dec 1 04:16:41 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1391) -> 208.38.53.97(137), 1 packet

\*Dec 1 04:16:47 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1394) -> 208.38.53.97(138), 1 packet

\*Dec 1 04:16:53 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1397) -> 208.38.53.97(138), 1 packet

\*Dec 1 04:16:59 MST: %SEC-6-IPACCESSLOGP: list Ingress denied tcp 208.38.53.10(1267) -> 208.38.53.97(137), 1 packet

## 2.2 Firewall Security Policy

The goal of the stateful inspection firewall cluster is to defend GIAC from exploits and from those with malicious intent. As stated previously GIAC intends to build a security policy that defends against the SANS Institutes 'Top 20'. Many of these vulnerabilities are covered with a properly configure firewall and have been included in the list

From the SANS "Top 20" (with specific reference number):

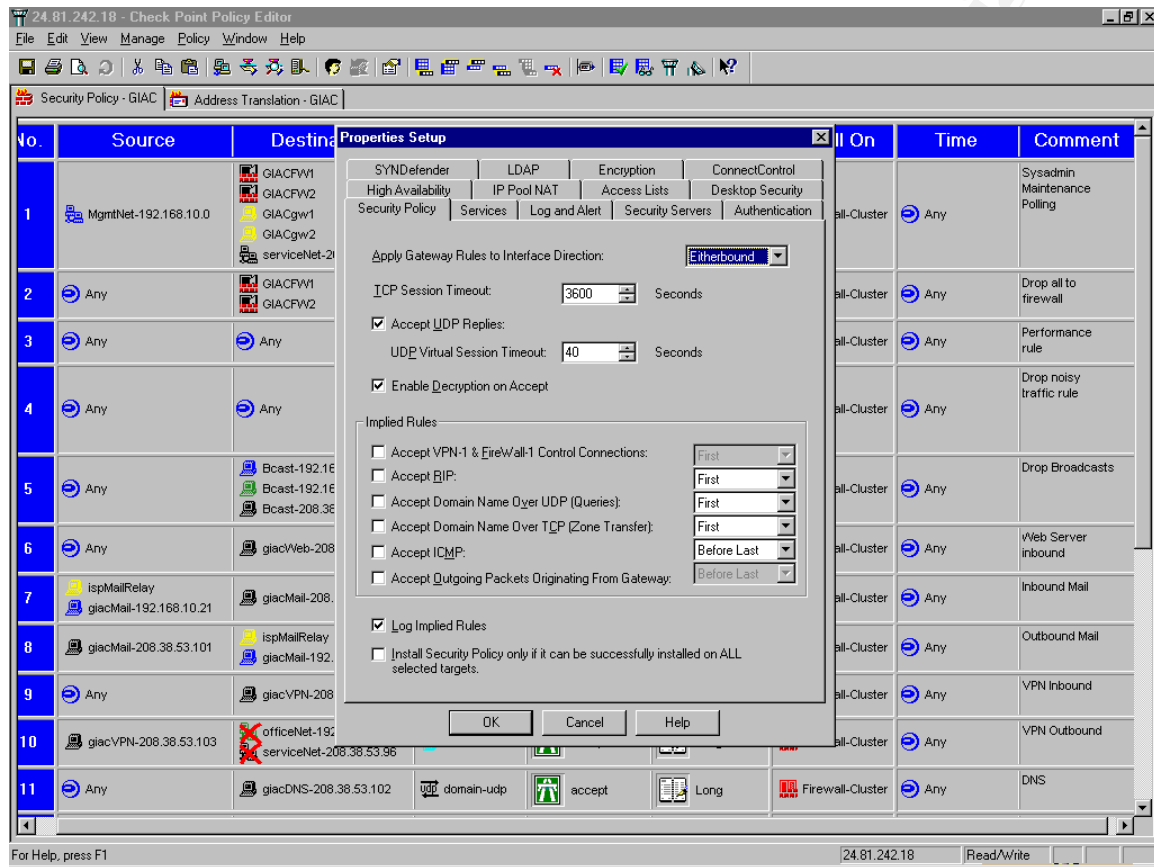
- ✓ G1 - Default installs of operating systems and applications
- ✓ G4 - Large number of open ports
- ✓ W4 - NETBIOS - unprotected Windows networking shares
- ✓ W5 - Information leakage via null session connections
- ✓ U1 - Buffer Overflows in RPC Services
- ✓ U3 - Bind Weaknesses
- ✓ U5 - LPD (remote print protocol daemon)
- ✓ U6 – sadmind and mountd
- ✓ U7 - Default SNMP Strings
- ✓ G6 - Non-existent or incomplete logging
- ✓ Appendix A - Deny access to common vulnerable ports

The table below details the intended security policy for GIAC. The actual security policy is included in the next section of this document:

Rule	Source	Destination	Service	Action	Track	Comment
1	Mgmt-Net	Firewalls Routers Service-net	ssh fw-mgm ping	Accept	Long	Systems Administration Rule Polling and alerting
2	any	Firewalls	any	drop	Long	Drop all traffic to the firewalls
3	Any	Any	Ident	Reject		Performance rule reject any ident traffic.
4	Any	Any	Netbios Tftp snmp	drop		Noisy traffic, drop vulnerable ports
5	Any	Broadcast	Any	drop		Drop all traffic to broadcast address of GIAC networks
6	Any	Web Server	HTTP HTTPS	Accept	Long	Accept traffic to web servers
7	ISP mail Internal mail	External mail	SMTP	Accept	Long	ISP is Mail relay for GIAC. Allows ISP mail server and GIAC internal mail server to send mail to GIAC external mail server.
8	External mail	ISP mail Internal mail	SMTP	Accept	Long	Allows GIAC External Mail server to send to ISP mail server and GIAC internal mail server.
9	Any	GIAC VPN	IPSEC	Accept	Long	VPN in Rule
10	GIAC VPN	Any	IPSEC	Accept	Long	VPN out Rule
11	Any	GIAC DNS	Udp-53	Accept	Short	Inbound DNS Rule to GIAC DNS
12	GIAC DNS	ISPDNS	Udp-53	Accept	Short	Outbound DNS Rule to ISP DSN server.
13	GIAC Web	GIAC DB	Sql	Accept	Long	Web server Database
14	Service-Net Routers	Log Server	syslog	Accept	Long	Logging Rule
15	Web Server	LDAP Server	LDAP	Accept	Long	Authentication Rule
16	Service-Net	Mgmt-Net	Backup	Accept		Data Backup (only allow during backup window)
17	Web proxy	Negate	HTTP HTTPS	Accept	Long	GIAC Internal office can surf internet outbound
18	Office-net	Windows2000 Term Server	Tcp-3389	Accept	Long	Office and Remote VPN Users access applications
19	Service-net	Any	Any	Drop	Alert	Alert on any other traffic initiated from service net
20	Any	Any	Any	Drop	Long	Catch all rule

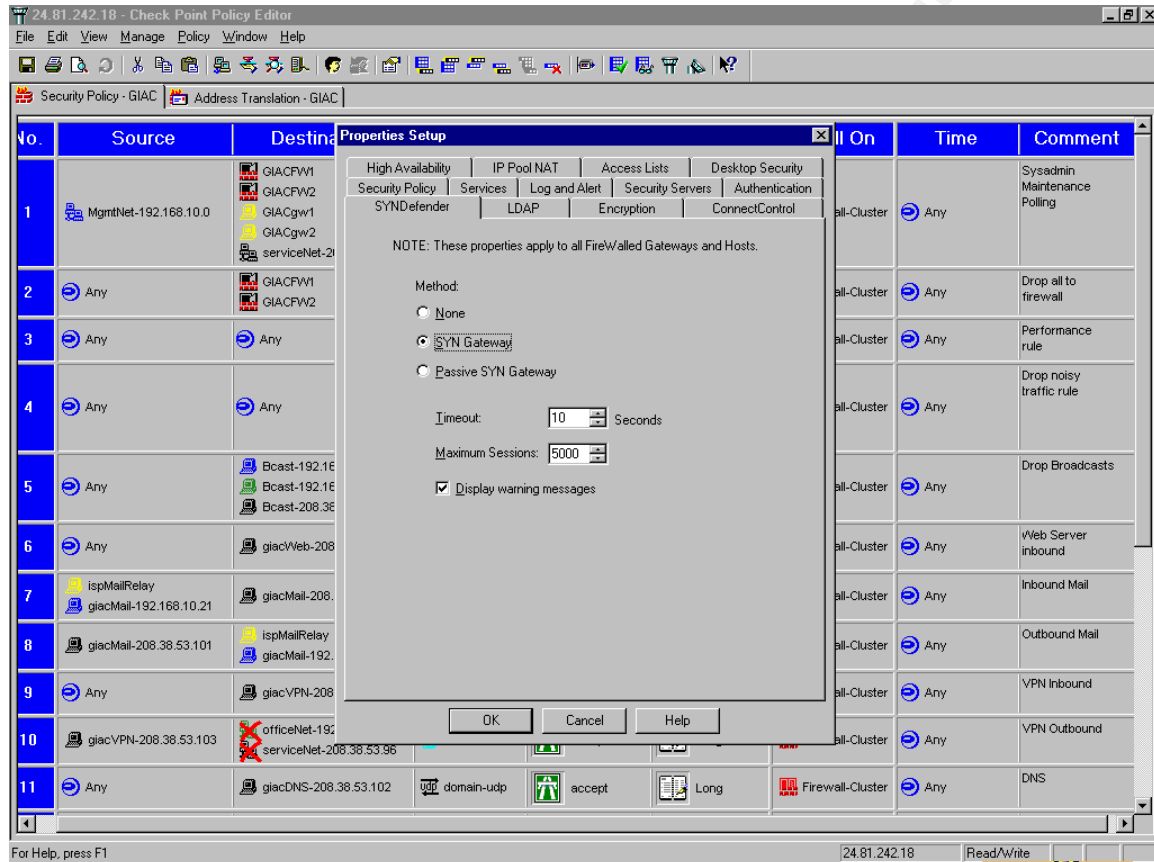
### Firewall Properties – Security Policy Properties:

Detailed below is the global properties page of the Checkpoint Firewall-1 security policy. The default selections in the security policy allow certain traffic. The goal is to remove the default selections and start with a clean ‘deny all’ policy. This is shown in the screen capture below:



### SYN Gateway:

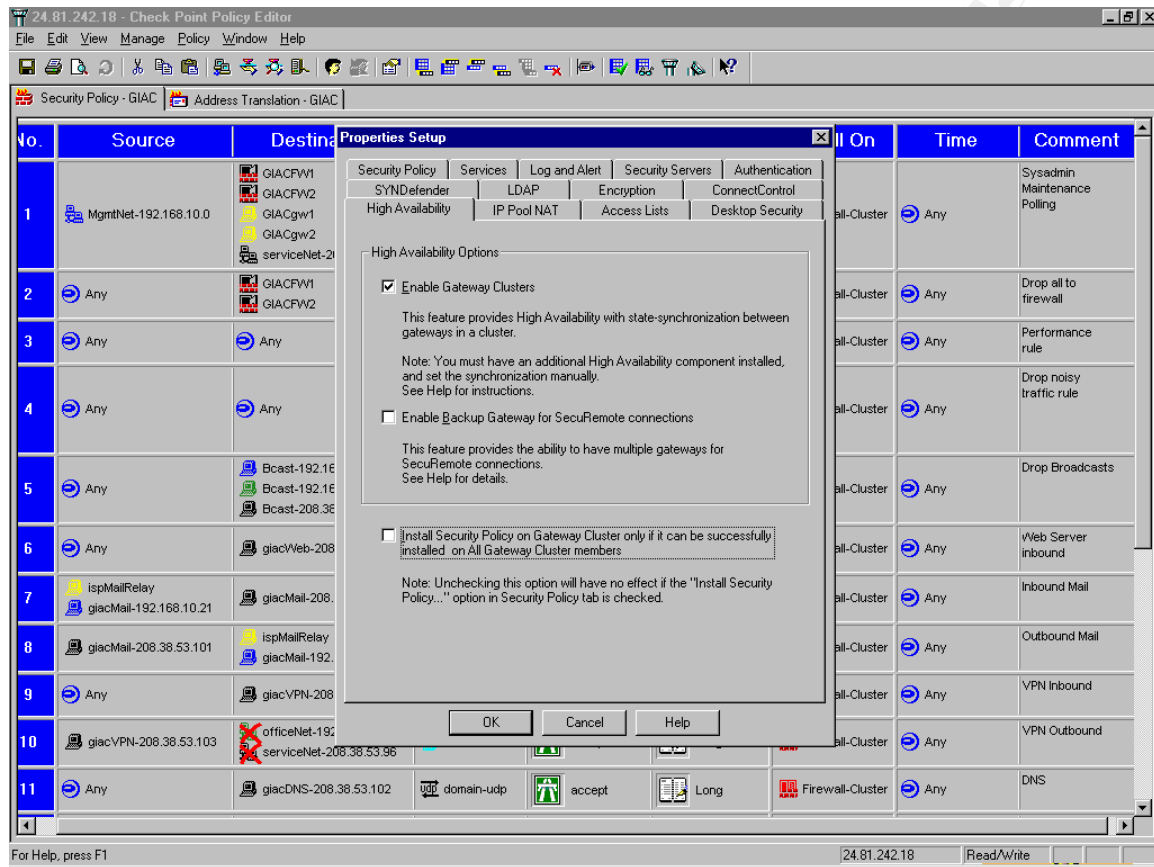
The SYN gateway feature of the global properties is a Checkpoint feature that defends against possible SYN attacks. This feature is disabled by default but it is enabled for GIAC as part of the 'security layer' philosophy. The jury is out on its effectiveness but it may provide the level of protection required in certain situations. This configuration is shown in the screen capture below:





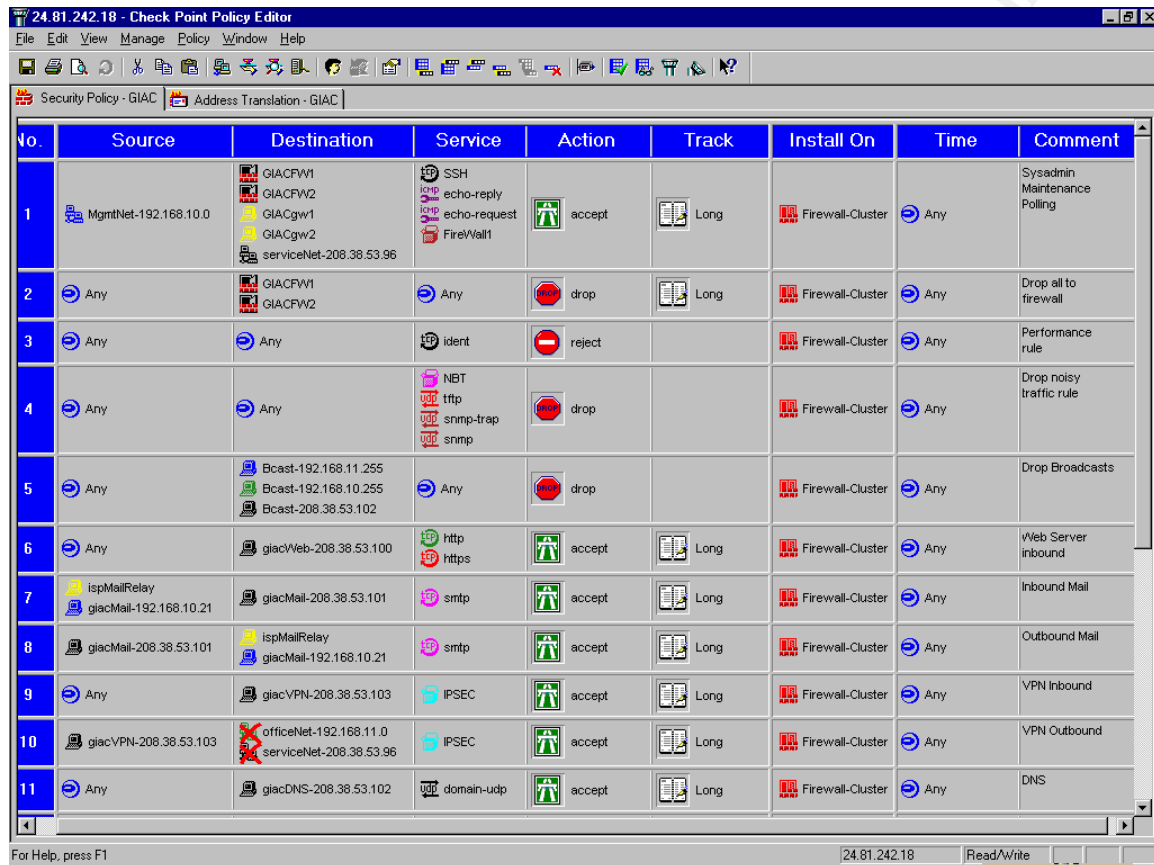
### High Availability:

The GIAC firewalls are configured as a high available cluster. The third party add on that provides this functionality is StoneBeat FullCluster. The High Availability properties page enables this functionality. The functionality has to be turned on in the Firewall-1 properties setup as shown in the screen capture below:



### Security Policy Editor – Rule Base:

The firewall cluster's security policy or ACL has been described in the previous sections of this document are defined in the visual rule base editor (GUI). The security policy is compiled and installed on the firewall cluster. After this is compiled and installed it becomes the security policy for the firewall cluster as indicated in the graphic below:



No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	MgmtNet-192.168.10.0	GIACFW1 GIACFW2 GIACgw1 GIACgw2 serviceNet-208.38.53.96	SSH echo-reply echo-request FireWall1	accept	Long	Firewall-Cluster	Any	Sysadmin Maintenance Polling
2	Any	GIACFW1 GIACFW2	Any	drop	Long	Firewall-Cluster	Any	Drop all to firewall
3	Any	Any	ident	reject		Firewall-Cluster	Any	Performance rule
4	Any	Any	NBT tftp snmp-trap snmp	drop		Firewall-Cluster	Any	Drop noisy traffic rule
5	Any	Bcast-192.168.11.255 Bcast-192.168.10.255 Bcast-208.38.53.102	Any	drop		Firewall-Cluster	Any	Drop Broadcasts
6	Any	giacWeb-208.38.53.100	http https	accept	Long	Firewall-Cluster	Any	Web Server inbound
7	IspMailRelay giacMail-192.168.10.21	giacMail-208.38.53.101	smtp	accept	Long	Firewall-Cluster	Any	Inbound Mail
8	giacMail-208.38.53.101	IspMailRelay giacMail-192.168.10.21	smtp	accept	Long	Firewall-Cluster	Any	Outbound Mail
9	Any	giacVPN-208.38.53.103	IPSEC	accept	Long	Firewall-Cluster	Any	VPN Inbound
10	giacVPN-208.38.53.103	officeNet-192.168.11.0 serviceNet-208.38.53.96	IPSEC	accept	Long	Firewall-Cluster	Any	VPN Outbound
11	Any	giacDNS-208.38.53.102	domain-udp	accept	Long	Firewall-Cluster	Any	DNS

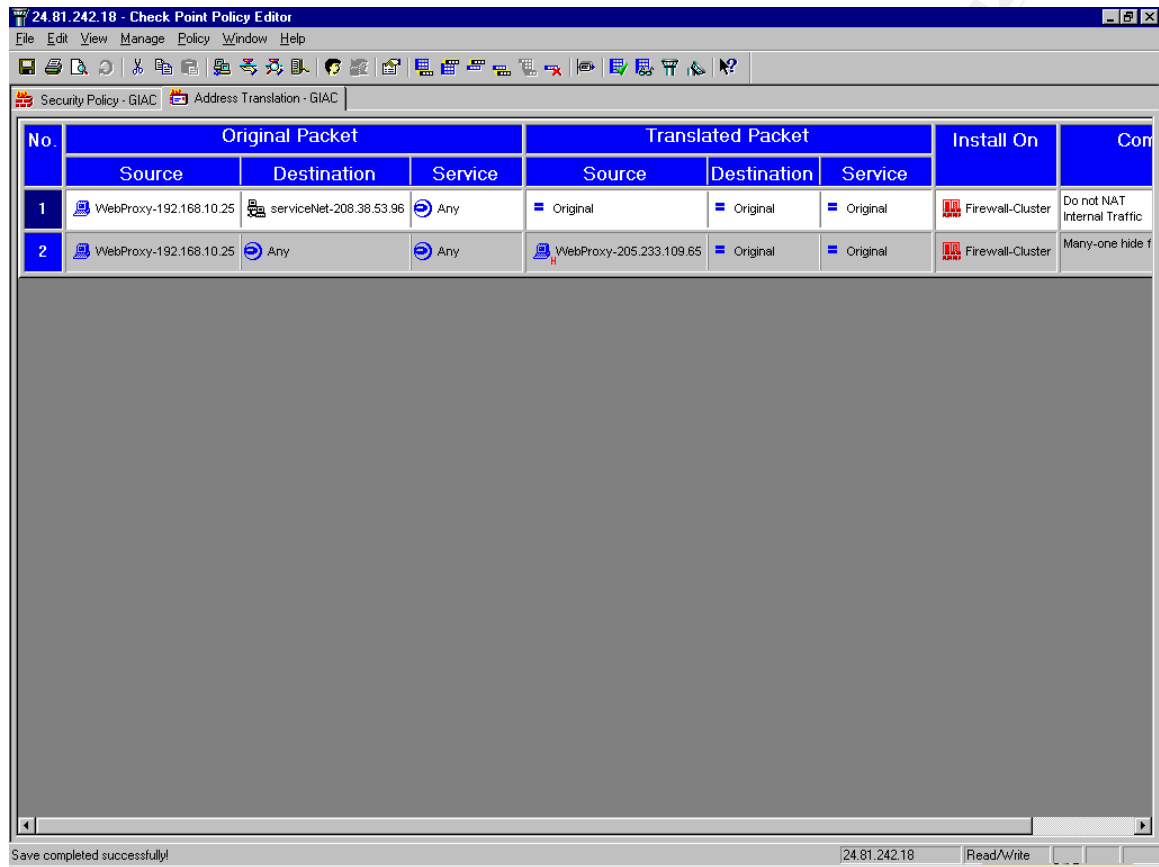
Security policy continued....

24.81.242.18 - Check Point Policy Editor									
File Edit View Manage Policy Window Help									
Security Policy - GIAC Address Translation - GIAC									
7	ispMailRelay giacMail-192.168.10.21	giacMail-208.38.53.101	smtp	accept	Long	Firewall-Cluster	Any	Inbound Mail	
8	giacMail-208.38.53.101 ispMailRelay giacMail-192.168.10.21		smtp	accept	Long	Firewall-Cluster	Any	Outbound Mail	
9	Any	giacVPN-208.38.53.101	IPSEC	accept	Long	Firewall-Cluster	Any	VPN Inbound	
10	giacVPN-208.38.53.101 officeNet-192.168.11.0 serviceNet-208.38.53.96		IPSEC	accept	Long	Firewall-Cluster	Any	VPN Outbound	
11	Any	giacDNS-208.38.53.102	domain-udp	accept	Short	Firewall-Cluster	Any	Inbound DNS	
12	giacDNS-208.38.53.102 ispDNS-205.233.109.39		domain-udp	accept	Short	Firewall-Cluster	Any	Outbound DNS	
13	giacWeb-208.38.53.100 giacDB-192.168.10.20		sqlnet1	accept	Long	Firewall-Cluster	Any	Web - Database queries	
14	serviceNet-208.38.53.96 GIACgw1-208.38.53.2 GIACgw2-208.38.53.3	giacLog-192.168.10.22	syslog	accept	Long	Firewall-Cluster	Any	Logging Rule	
15	giacWeb-208.38.53.100 giacLDAP-192.168.10.23		ldap	accept	Long	Firewall-Cluster	Any	User Authentication Rule	
16	serviceNet-208.38.53.96 giacBackup-192.168.10.24		Net-backup	accept	Long	Firewall-Cluster	Any	Data Backup	
17	WebProxy-192.168.10.25 officeNet-192.168.11.0 MgmtNet-192.168.10.0		http https	accept	Long	Firewall-Cluster	Any	Office web proxy	
18	officeNet-192.168.11.0 giacTerm-192.168.10.26		tcp-3389	accept	Long	Firewall-Cluster	Any	Windows Terminal Server Access	
19	serviceNet-208.38.53.96	Any	Any	drop	Alert	Firewall-Cluster	Any	Alert if service LAN attempt's outbound	
20	Any	Any	Any	drop	Long	Firewall-Cluster	Any	Clean up Rule all Drop rule	

Save completed successfully! 24.81.242.18 Read/Write

### Address Translation for Web Proxy:

The web proxy server is used by the internal office users as well as the VPN users who requiring Internet access. In order to facilitate this, a many-to-one hide network address translation (hide NAT) was configured for the web proxy server. An additional rule had to be added above the NAT rule to prevent translating internal traffic as shown below:



No.	Original Packet			Translated Packet			Install On	Comments
	Source	Destination	Service	Source	Destination	Service		
1	WebProxy-192.168.10.25	serviceNet-208.38.53.96	Any	Original	Original	Original	Firewall-Cluster	Do not NAT Internal Traffic
2	WebProxy-192.168.10.25	Any	Any	WebProxy-205.233.109.65	Original	Original	Firewall-Cluster	Many-one hide f

Save completed successfully! [24.81.242.18] Read/Write

### 2.3 VPN Security Policy

The primary focus of the VPN is to provide connectivity from the remote site to the corporate GIAC headquarters. The remote user will connect to the Internet through a broadband connection such as DSL or a Cable modem. The remote users will either be GIAC employees or GIAC suppliers. The assumption is that both groups are trusted and have read and signed the GIAC Corporate acceptable use policy. The remote device i.e. desktop is configured with an IPSEC VPN software client such as the Cisco Secure VPN Client. The remote desktop will also have a personal firewall and anti virus software. The IPSEC VPN software client will establish a tunnel to the GIAC corporate VPN. Once the authentication occurs and the tunnel is established ACLs will determine what services the remote user can access in the GIAC corporate network. In this case the remote user will only be able to access A Microsoft Windows 2000 Terminal server farm. The remote user will have to authenticate at three access points; the remote desktop (operating system), the IPSEC VPN Client to IPSEC VPN termination point (Cisco Pix), and the internal access point (Windows 2000 terminal server).

The IPSEC VPN client establishes a secure encrypted tunnel to the VPN termination point, which in this case is the GIAC VPN device. The VPN termination device has a routable interface on the service LAN and a non-routable interface on the office LAN. The remote user is authenticated at the VPN termination point, receives a local virtual IP address and name resolution parameters. The VPN access control list determines where in the GIAC network the remote user can access.

The security policy parameters for the IPSEC VPN are as follows:

- ❑ Split tunneling is not enabled as this is considered to be a security violation. Split tunneling may allow an outside threat into the VPN tunnel. If remote workers require Internet access at the same time as they are using the VPN tunnel they can access Internet services through the corporate Internet gateway.
- ❑ Phase 1 of the IKE setup process will use “Main Mode”. Aggressive mode was not selected, as it does not provide identity protection. The assumption is that all remote workers will have broadband access so bandwidth is not a concern. A pre-shared key will be used to establish the authentication. Triple DES (3DES) will be used for the encryption algorithm, and the Hash algorithm will use MD5.
- ❑ Phase 2 of the IKE process will use Encapsulating Security Payload (ESP) for the security protocol of the VPN tunnel. ESP was selected over Authentication Header (AH) because AH breaks NAT implementations and ESP uses Triple DES (3DES) encryption. MD5 will be used for the Hash algorithm. Tunnel mode will be used between the host and the VPN termination point. The VPN will encapsulate the original packet hiding the real source and destination addresses. This will support the use of RFC 1918 addresses behind the GIAC VPN gateway as well as remote workers whose source address is NAT’ed.

## Assignment 3.0

### 3.1 Audit of GIAC Enterprises Security Architecture

The technical security audit of the GIAC firewall cluster will be completed in several phases. This starts with a holistic view of GIAC enterprise and then drills down into testing enforcement points with penetration tools. The investigation phase or technical review will be conducted during normal business hours, as the auditors need access to GIAC staff and technical drawings. The testing phase will be conducted during off prime hours as negotiated with the GIAC staff and GIAC's ISP. Security testing poses a risk to GIAC Enterprises as it introduces elements and change in the GIAC network environment. Anytime change is introduced into an environment there is an associated risk. The risk can take many forms such as; an outage caused by the introduction of elements, extra stress on network infrastructure due to penetration testing. Alarms can be triggered at the ISP or at GIAC's NOC. Unskilled auditors can wreak havoc on infrastructure they know nothing about. The technical audit plan is detailed in the steps below.

#### Phase 1 Technical Review

The level of effort required to complete phase one is:

8 hours onsite – Research, Plan and Review at a billing rate of \$100.00 per hour.

Phase one will be completed in the following sequence:

##### 1) Review of the GIAC business plan.

Auditors will interview a representative of GIAC Enterprises to gain an understanding of what GIAC does. It is important auditors have an overview of the business and in turn what the goals of the network infrastructure are.

##### 2) Review overall security policy of GIAC.

Auditors will review the corporate security policy of GIAC Enterprises. This will include the corporate acceptable use policy as well as any stated network security policy.

ected. The NAMP scans will

<b>GIAC Enterprises</b>	
Security Architecture	12/27/ 2001



## Phase 2 – Technical Audit

The level of effort to complete phase two is:

- 8 hours onsite – Setup and Testing at a billing rate of \$200.00 per hour
- 8 hours offsite – Analyzing the Data at a billing rate of \$200.00 per hour
- 4 hours offsite – Report Documentation at a billing rate of \$100.00 per hour

Phase two will be complete in the following sequence:

1) Audit the firewall server operating system configuration.

Ensure servers are hardened using the 'Best Practices' approach of disabling all services not needed. Audit operating system patch level and password policy.

2) Audit the firewall software.

Determine if the firewall software has gaping security holes in its code. Audit firewall software to determine if patch level is acceptable.

The following sites can be used to research exploits:

<http://www.incidents.org>

<http://www.cert.org>

<http://msgsg.securepoint.com/bugtraq/>

<http://www.securityfocus.com/>

[http://www.checkpoint.com/techsupport/alerts/list\\_vun.html](http://www.checkpoint.com/techsupport/alerts/list_vun.html)

3) Testing firewall security policy.

As stated previously testing will be conducted by placing an attack probe on each of the security enforcement points. The attack probe will run a series of NMAP scans against the firewall and against the three network segments protected by the firewall. A network traffic capture host running TCPDUMP will be placed on the other side of the security point being tested. The results of the NMAP scans will be compared against the firewall logs and the network traces from TCPDUMP to determine if each security enforcement point is performing as expected.

## 3.2 Security Audit

### Nmap

The primary audit tool used to test the security policy is NMAP. NMAP is a network-mapping tool written by Fyodor. NMAP will help determine what ports are listening and with this knowledge we can determine if the security policy is working. The essence of the security policy is to block everything by default and only allow those services required to operate the business. NMAP will indicate whether they are doing a good job at this.

### Firewall Logs

The Checkpoint Firewall logs are to correlate the data from the nmap scan. The logs should indicate accepts on traffic allowed and drop/reject/alert on all other traffic.



## Tcpdump

The second audit tool used to test the security policy is Tcpdump. Tcpdump is a network packet capture utility. It will be used to passively sniff the network while NMAP is being run looking for traffic that should not pass the firewall's security policy. Tcpdump provides detailed packet capture information and will allow us to determine if the security policy is not acting as expected.

## Firewall Audit Results

The audit results shown in the document below are excerpts from the security tools used. The information is included to demonstrate the methods of the security audit of the GIAC firewall cluster. The results shown are scans against the GIAC service LAN and the GIAC firewall cluster. The results indicate the firewall cluster's security policy is performing as expected.

### **Nmap TCP SYN Scan of web server IP 208.38.53.100 test rule 6**

The following NMAP TCP SYN scan was performed against the web server to determine whether the security policy is working. Please note the web server on the host was not running. The audit test demonstrates the firewall allowed ports 80 and 443 to 208.38.53.100 and rejected ident port 113. The security policy performed as expected.

```
nmap -sS -P0 -O 208.38.53.100
```

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com  
eEye Digital Security ( <http://www.eEye.com> )  
based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Warning: No TCP ports found open on this machine, OS detection will be MUCH less rel  
Interesting ports on (208.38.53.100):

(The 1520 ports scanned but not shown below are in state: filtered)

Port	State	Service
80/tcp	closed	http
113/tcp	closed	auth
443/tcp	closed	https

Too many fingerprints match this host for me to give an accurate OS guess  
Nmap run completed -- 1 IP address (1 host up) scanned in 691 seconds

### Firewall Logs filtered for web server as destination IP 208.38.53.100

The corresponding firewall log file was too large (allot of drops due to scan) to include the entire file. The portion of the log file corresponding to the nmap scan above is shown below:

Note: The indent service indicated in the nmap scan does not show in the firewall logs as we have chosen not to log this service.

```
"8208" "22Dec2001" "15:10:38" "SBIF2" "24.81.242.18" "log" "accept" "https"
"24.81.242.19" "208.38.53.100" "tcp" "6" "42816" "" "" "" "" "" "" "" "" ""
"firewall" " len 40"
"8230" "22Dec2001" "15:10:39" "SBIF2" "24.81.242.18" "log" "accept" "http"
"24.81.242.19" "208.38.53.100" "tcp" "6" "42816" "" "" "" "" "" "" "" "" ""
"firewall" " len 40"
```

```
"12523" "22Dec2001" "15:13:37" "SBIF2" "24.81.242.18" "log" "accept" "http"
"24.81.242.19" "208.38.53.100" "tcp" "6" "42827" "" "" "" "" "" "" "" "" ""
"firewall" " len 60"
"12524" "22Dec2001" "15:13:37" "SBIF2" "24.81.242.18" "log" "accept" "http"
"24.81.242.19" "208.38.53.100" "tcp" "6" "42828" "" "" "" "" "" "" "" "" ""
"firewall" " len 60"
"12525" "22Dec200" "15:13:37" "SBIF2" "24.81.242.18" "log" "accept" "http"
"24.81.242.19" "208.38.53.100" "tcp" "6" "42829" "" "" "" "" "" "" "" "" ""
"firewall" " len 60"
```

### Tcpdump trace on web server IP 208.38.53.100

The tcpdump trace is included to show the traffic that made it through the firewall's security policy to the web server. As you can see from the trace the only traffic to make it through the firewall was http tcp-80 and https tcp-443. This verifies the security firewall security policy.

tcpdump host 208.38.53.100

tcpdump: listening on \Device\Packet\_{5B975FCB-FBBD-46F3-B3DE-8743159B09D2}

```
15:10:19.470328 24.81.242.19.42816 > 208.38.53.100.443: S 2083472418:2083472418(0)
win1024
15:10:19.470487 208.38.53.100.443 > 24.81.242.19.42816: R 0:0(0) ack 2083472419 win 0
15:10:19.470904 208.38.53.100.443 > 24.81.242.19.42816: R 0:0(0) ack 1 win 0
15:10:20.469718 24.81.242.19.42816 > 208.38.53.100.80: S 2083472418:2083472418(0)
win 1024
15:10:20.469872 208.38.53.100.80 > 24.81.242.19.42816: R 0:0(0) ack 2083472419 win 0
15:10:20.470293 208.38.53.100.80 > 24.81.242.19.42816: R 0:0(0) ack 1 win 0
15:13:18.442567 24.81.242.19.42829 > 208.38.53.100.80: FP 1293025768:1293025768(0)
win
1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
15:13:18.442715 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1293025769 win 0
15:13:18.443410 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0
15:13:20.537493 24.81.242.19.42827 > 208.38.53.100.80: S 1293025768:1293025768(0)
win 1
024 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
15:13:20.537659 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 1293025769 win 0
15:13:20.538088 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 1 win 0
15:13:20.538569 24.81.242.19.42828 > 208.38.53.100.80: . ack 0 win 1024 <wscale 10,nop,
mss 265,timestamp 1061109567 0,eol>
15:13:20.538658 208.38.53.100.80 > 24.81.242.19.42828: R 0:0(0) win 0
15:13:20.539051 208.38.53.100.80 > 24.81.242.19.42828: R 0:0(0) win 0
15:13:20.541272 24.81.242.19.42829 > 208.38.53.100.80: FP 1293025768:1293025768(0)
win
1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
15:13:20.541362 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0
15:13:20.542017 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0
15:13:22.651640 24.81.242.19.42827 > 208.38.53.100.80: S 1293025768:1293025768(0)
win 1
024 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
15:13:22.651812 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 1 win 0
15:13:22.652232 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 1 win 0
15:13:22.654331 24.81.242.19.42829 > 208.38.53.100.80: FP 1293025768:1293025768(0)
win
1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
15:13:22.654419 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0
```

15:13:22.655078 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0  
 15:13:24.463692 24.81.242.19.42829 > 208.38.53.100.80: FP 1293025768:1293025768(0)  
 win1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:24.463833 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0  
 15:13:24.464528 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 1 win 0  
 15:13:28.590079 24.81.242.19.42827 > 208.38.53.100.80: S 1566183696:1566183696(0)  
 win 1024 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:28.590258 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 273157929 win 0  
 15:13:28.590710 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 273157929 win 0  
 15:13:28.591002 24.81.242.19.42828 > 208.38.53.100.80: . ack 1 win 1024 <wscale  
 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:28.591081 208.38.53.100.80 > 24.81.242.19.42828: R 0:0(0) win 0  
 15:13:28.591442 208.38.53.100.80 > 24.81.242.19.42828: R 0:0(0) win 0  
 15:13:28.593871 24.81.242.19.42829 > 208.38.53.100.80: FP 1566183696:1566183696(0)  
 win1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:28.593960 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 273157929 win 0  
 15:13:28.594620 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 273157929 win 0  
 15:13:30.702623 24.81.242.19.42829 > 208.38.53.100.80: FP 1566183696:1566183696(0)  
 win1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:30.702783 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 273157929 win 0  
 15:13:30.703488 208.38.53.100.80 > 24.81.242.19.42829: R 0:0(0) ack 273157929 win 0  
 15:13:34.528971 24.81.242.19.42827 > 208.38.53.100.80: S 1757896112:1757896112(0)  
 win 1024 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:34.529168 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 464870345 win 0  
 15:13:34.529623 208.38.53.100.80 > 24.81.242.19.42827: R 0:0(0) ack 464870345 win 0  
 15:13:34.529920 24.81.242.19.42828 > 208.38.53.100.80: . ack 1 win 1024 <wscale  
 10,nop,mss 265,timestamp 1061109567 0,eol>  
 15:13:34.530000 208.38.53.100.80 > 24.81.242.19.42828: R 0:0(0) win 0

**Nmap UDP Scan of the Web Server IP 208.38.53.100 overall test of firewall ACL**  
 nmap -sU -P0 -O 208.38.53.100

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com  
 eEye Digital Security ( <http://www.eEye.com> )  
 based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Warning: No TCP ports found open on this machine, OS detection will be MUCH less  
 reliable  
 All 1448 scanned ports on (208.38.53.100) are: filtered  
 Too many fingerprints match this host for me to give an accurate OS guess  
 Nmap run completed -- 1 IP address (1 host up) scanned in 1929 seconds

**Nmap TCP SYN Scan of the Firewall Cluster IP 208.38.53.7 test Rule 2**  
 nmap -sS -P0 208.38.53.7

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com  
eEye Digital Security ( <http://www.eEye.com> )  
based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

All 1523 scanned ports on (24.81.242.18) are: filtered  
Nmap run completed -- 1 IP address (1 host up) scanned in 1654 seconds

### Corresponding Firewall Logs

Below is a portion of the firewall logs indicating the results of the nmap scan above. The entire log file was not included. Results indicate firewall ACL working as expected. As per rule 2.

```
"2" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "1600"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"3" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "917"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"4" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "1996"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"5" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "820"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"6" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "75" "24.81.242.19"
"208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall" " len 40"
"7" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "773"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"8" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "635"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"9" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "1471"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"10" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "559"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"11" "22Dec2001" "18:10:14" "SBIF2" "208.38.53.7" "log" "drop" "812"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54834" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"12" "22Dec2001" "18:10:19" "SBIF2" "208.38.53.7" "log" "drop" "1600"
"24.81.242.19" "208.38.53.7" "tcp" "2" "54835" "" "" "" "" "" "" "" "" "" "firewall"
" len 40"
"13" "22Dec2001" "18:10:19" "SBIF2" "208.38.53.7" "log" "drop" "917"
```

```
"24.81.242.19" "208.38.53.7" "tcp" "2" "54835" "" "" "" "" "" "" "" "" "" "firewall"  
" len 40"  
"14" "22Dec2001" "18:10:19" "SBIF2" "208.38.53.7" "log" "drop" "1996"  
"24.81.242.19" "208.38.53.7" "tcp" "2" "54835" "" "" "" "" "" "" "" "" "" "firewall"  
" len 40"
```

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

## **Nmap TCP SYN Scans on the rest of the Service Network**

The nmap scans results show firewall ACL rules working as expected.

Nmap scan of all other host on service net

nmap -sS -P0 208.38.53.101-103

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security ( <http://www.eEye.com> )

based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

### **Mail server show no ports open as only ISP mail server is allowed inbound on port 25 as per rule 7**

Interesting ports on (208.38.53.101):

(The 1522 ports scanned but not shown below are in state: filtered)

Port	State	Service
113/tcp	closed	auth

Interesting ports on (208.38.53.102):

(The 1522 ports scanned but not shown below are in state: filtered)

Port	State	Service
113/tcp	closed	auth

### **DNS server shows no open ports as this is a tcp scan and DNS is only allowed in on UDP-53 as per rule 11**

Interesting ports on (208.38.53.103):

(The 1522 ports scanned but not shown below are in state: filtered)

Port	State	Service
113/tcp	closed	auth

Nmap run completed -- 4 IP addresses (4 hosts up) scanned in 3081 second

### **Nmap UDP Scan of DNS Server shows UDP-53 open as per firewall rule 11**

nmap -sU -p53 -P0 208.38.53.103

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security ( <http://www.eEye.com> )

based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Interesting ports on (208.38.53.103):

Port	State	Service
53/udp	open	domain

Nmap run completed -- 1 IP address (1 host up) scanned in 16 seconds

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



### **Test rule 18 - outgoing alert rule from Service LAN**

Generate outgoing traffic from web server command line to an Internet address. This demonstrates the outgoing alert rule. Any other traffic originating from the service network that is not explicitly allowed is dropped and an alert is generated. This will alert to possible host compromises on the service net.

Telnet to outside address using port 80

```
telnet 24.81.242.19 80
```

Connecting To 24.81.242.19...Could not open a connection to host on port 80: Connect failed

### **Corresponding Firewall Log show drop and alerts**

```
"25007" "22Dec2001" "20:47:55" "Sbif3" "208.38.53.97" "alert" "drop" "http"
"208.38.53.100" "24.81.242.19" "tcp" "18" "1033" "" "" "" "" "" "" "" "" ""
"firewall" " len 48"
"25008" "22Dec2001" "20:48:50" "Sbif3" "208.38.53.97" "alert" "drop" "http"
"208.38.53.100" "24.81.242.19" "tcp" "18" "1034" "" "" "" "" "" "" "" "" ""
"firewall" " len 48"
```

### **Tcpdump results show outbound traffic from web server**

```
20:50:51.827127 208.38.53.100.1034 > 24.81.242.19.80: S 2433493110:2433493110(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
20:50:51.828114 208.38.53.100.1034 > 24.81.242.19.80: S 2433493110:2433493110(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
20:50:54.775436 208.38.53.100.1034 > 24.81.242.19.80: S 2433493110:2433493110(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
20:50:54.776322 208.38.53.100.1034 > 24.81.242.19.80: S 2433493110:2433493110(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
20:51:00.784068 208.38.53.100.1034 > 24.81.242.19.80: S 2433493110:2433493110(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
20:51:00.784964 208.38.53.100.1034 > 24.81.242.19.80: S 2433493110:2433493110(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
```

### Audit Evaluation

The information gathered from the security audit concludes the overall security design of the firewall cluster is sound and complies with the GIAC security policy and business plan. The entire audit test results are not included in this document however; results stated in the previous section of this document are indicative of the consistent methodology used during the audit and of the thorough testing of the firewall cluster. Results of the audit indicate enhancements can be made to the security design with the use of an internal firewall to protect the management LAN. The management LAN has valuable resources and if it were compromised would create havoc from a business perspective. The use of an internal firewall would create another layer of security and would move GIAC towards a more comprehensive 'Defense in Depth' than the current perimeter security model deployed today.

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



## Section 1: Research Vulnerabilities and plan an attack with one.

### Vulnerability 1

The following vulnerability was posted on the SecurityFocus Vulnerability list:

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1890>

bugtraq id: 1890

Class: Design Error

CVE-2000-1032

Published: Nov 1, 2000

Vulnerable: Checkpoint Firewall-1 3.0, 4.0

This attack is described as follows:

Vulnerability exists in Firewall-1 whereby an attacker can determine a valid username by the response given by the firewall to authentication requests (port 259 on the firewall) from a remote client.

Upon connecting to the firewall, the attacker enters a username and password. If the username and password are invalid, the firewall will respond with "<username> not found". If the username is valid, and the password is invalid, the firewall will respond with "Access denied by Firewall-1 authentication".

Upon successfully determining a valid username, a remote attacker could then attempt a brute force or password grinding attack to determine the password for the valid username. If successful, an attacker could then gain access to the firewall based on that user's privileges.

### Vulnerability 2

The following vulnerability was posted on the SecurityFocus Vulnerability list:

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1419>

Bugtrac id: 1419

Class: Configuration Error

Published: Jul 5, 2000

Vulnerable: Checkpoint Firewall-1 3.0, 4.0, 4.1

This attack is described as follows:

If Checkpoint Firewall-1 receives a number of spoofed UDP packets with Source IP = Destination IP, the firewall (and likely the machine hosting it) crashes.

### Vulnerability 3

The following vulnerability is posted on the SecurityFocus Vulnerability list:

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1419>

Bugtrac Id: 1312

Class: Failure to handle Exceptional Conditions

Published: June 6, 2000

Vulnerable: Checkpoint Firewall-1 4.0, 4.1

This attack is described as follows:

By sending illegally fragmented packets directly to or routed through Check Point FireWall-1, it is possible to force the firewall to use 100% of available processor time logging these packets. The FireWall-1 rulebase cannot prevent his attack and it is not logged in the firewall logs.

#### Attack 1 – Attack on Firewall

I have chosen to use vulnerability 2 above for the attack on the firewall.

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1419>

IP spoofing involves changing your source address so the target thinks the packet came from someone else. The essence of this attack is to generating spoofed udp packets using the firewalls outside interface address as the source and destination address. There are a variety of tools that can be used to modify the source IP address to fool target systems. Nmap was used to demonstrate spoofed udp traffic to a test firewall using the source address of the firewall. The results of this test are include below:

The following scan was run using Nmap:

```
nmap -S 208.38.53.7 -e0 -sU -P0 208.38.53.7
```

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com

eEye Digital Security ( <http://www.eEye.com> )

based on nmap by fyodor@insecure.org ( [www.insecure.org/nmap/](http://www.insecure.org/nmap/) )

Firewall log results from running the above scan

```
"1" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "1465"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"2" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "391"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"3" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "5001"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"4" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "1451"
```

```

"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"5" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "3457"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"6" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "765"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"7" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "522"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"8" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "1440"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"9" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "5190"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"
"10" "18Dec2001" "13:59:30" "RTL80291" "208.38.53.7" "log" "drop" "1512"
"25.81.242.18" "208.38.53.7" "udp" "2" "45832" "" "" "" "" "" "" "" "" "" "" "firewall"
" len 28"

```

### Attack Defense

This type of attack would be defeated with proper ingress anti-spoofing filters on the gateway routers in front of the firewall along with proper anti-spoofing configuration on the firewall itself. I ran this test on a Checkpoint Firewall-1 4.1 firewall with service pack 5 and did not crash the firewall. The firewall logged and dropped the traffic.

### Attack 2 - Denial of Service Attack

DoS Attack from 50 compromised systems connected to broadband Internet access. The attack target is the corporate web server.

A denial of service attack is an attempt by an attacker to consume and exhaust all system resources of a target system or network and deny access by anyone else. In the case of 50 compromised systems connected to broadband Internet access I chose to use a packet flood attack. The goal of a packet flood attack is to send more packets to a machine than it can handle. This may be an attempt to exhaust all processing power or bandwidth the target has available.

The attack tool used on the 50 compromised hosts is called the "Tribe Flood Network 2000" (TFN2K). <http://www.cert.org/advisories/CA-1999-17.html>. This distributed DoS (DDoS) tool uses a client server architecture, which allows a single client to control many servers. The TFN2K server will be installed on 49 compromised hosts. The TFN2K client will be installed on the 50<sup>th</sup> compromised host and is used to communicate with all of the TFN2K servers. The client can be used to direct all of the servers into utilizing an entire menu of attacks against the target network. The menu of DDoS attacks the TFN2K servers can launch at the target include: Targa; UDP flood; SYN flood; ICMP flood; Smurf

attack; and a mixture of these attacks.

### Attack Defense

The main defenses against this and all DoS attacks are properly configured ingress/egress anti-spoof filters on the gateway routers, patched operating systems, redundant Internet gateway routers, redundant Internet gateway firewalls, and a good ISP.

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

## 5.0 List of References

The SANS Institutes Firewall's Perimeter Protection, and VPNs  
All course material from Track 2 - SANS Network Security 2001 Oct 15-22  
Including Chris Benton's course notes and insight.

The SANS Institutes "The 20 Most Critical Internet Security Vulnerabilities" list  
<http://www.sans.org/top20.htm>.

Improving Security on Cisco Routers  
<http://www.cisco.com/warp/public/707/21.html>

Extending the Security Blueprint to Small, Midsize, and Remote-User Networks  
[http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm)

RFC's:  
Address Allocation for Private Internets  
<http://www.ietf.org/rfc/rfc1918.txt>

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing  
<http://www.ietf.org/rfc/rfc2827.txt>

Recommended Internet Service Provider Security Services and Procedures  
<http://www.ietf.org/rfc/rfc3013.txt>

INTERNET PROTOCOL V4 ADDRESS SPACE  
<http://www.iana.org/assignments/ipv4-address-space>

Auditing Tools used:  
Nmap  
[www.insecure.org/nmap/](http://www.insecure.org/nmap/)

Tcpdump  
<http://www.tcpdump.org/>

Exploit Research web sites used:  
<http://www.incidents.org>  
<http://www.cert.org>  
<http://msgs.securepoint.com/bugtraq/>  
<http://www.securityfocus.com/>  
[http://www.checkpoint.com/techsupport/alerts/list\\_vun.html](http://www.checkpoint.com/techsupport/alerts/list_vun.html)



Books:

Northcutt, Stephen; Cooper, Mark; Fearnow Matt; Karen Frederick  
Intrusion Signatures and Analysis, New Riders Jan 2001

Spitzner, Lance; Founder of the Honeynet Project  
Know Your Enemy – The Honeynet Project, Addison Wesley Sept 2001

Cole, Eric & Skoudis, Edward  
SANS Institutes Course Book - Computer and Network Hacker Exploits

Stewart, Judy  
SANS Institutes Course Book - Cisco's Security Features: What, Where to use and How

Firewall Web Sites:

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

<http://www.phoneboy.com/>

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