



# 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  
Vincent\_Tan\_GCFW.doc.....2

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

GCFW Practical Assignment  
Version 1.6a

Track 2: Firewalls, Perimeter Protection,  
And Virtual Private Networks  
(SANS 2001 Washington DC)

By

**Vincent Tan**

**Assignment 1 – Security Architecture (15 points)**

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.

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

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes);
- GIAC Enterprises (the employees located on GIAC's internal network).

You **must** explicitly define how the business operations of GIAC Enterprises will take place. How will each of the groups listed above connect to or communicate with GIAC Enterprises? How will GIAC employees access the outside world? What services, protocols, or applications will be used?

Defining what type of access is required and why is a critical part of this assignment. If you have not thought through how this access will take place, you will not be able to adequately define your security policy and ACLs/rulesets later in the paper.

In designing your architecture, you **must** include the following components:

- filtering routers;
- firewalls;
- VPNs to business partners.

Your architecture **may** also include the following optional components if they are appropriate to your design:

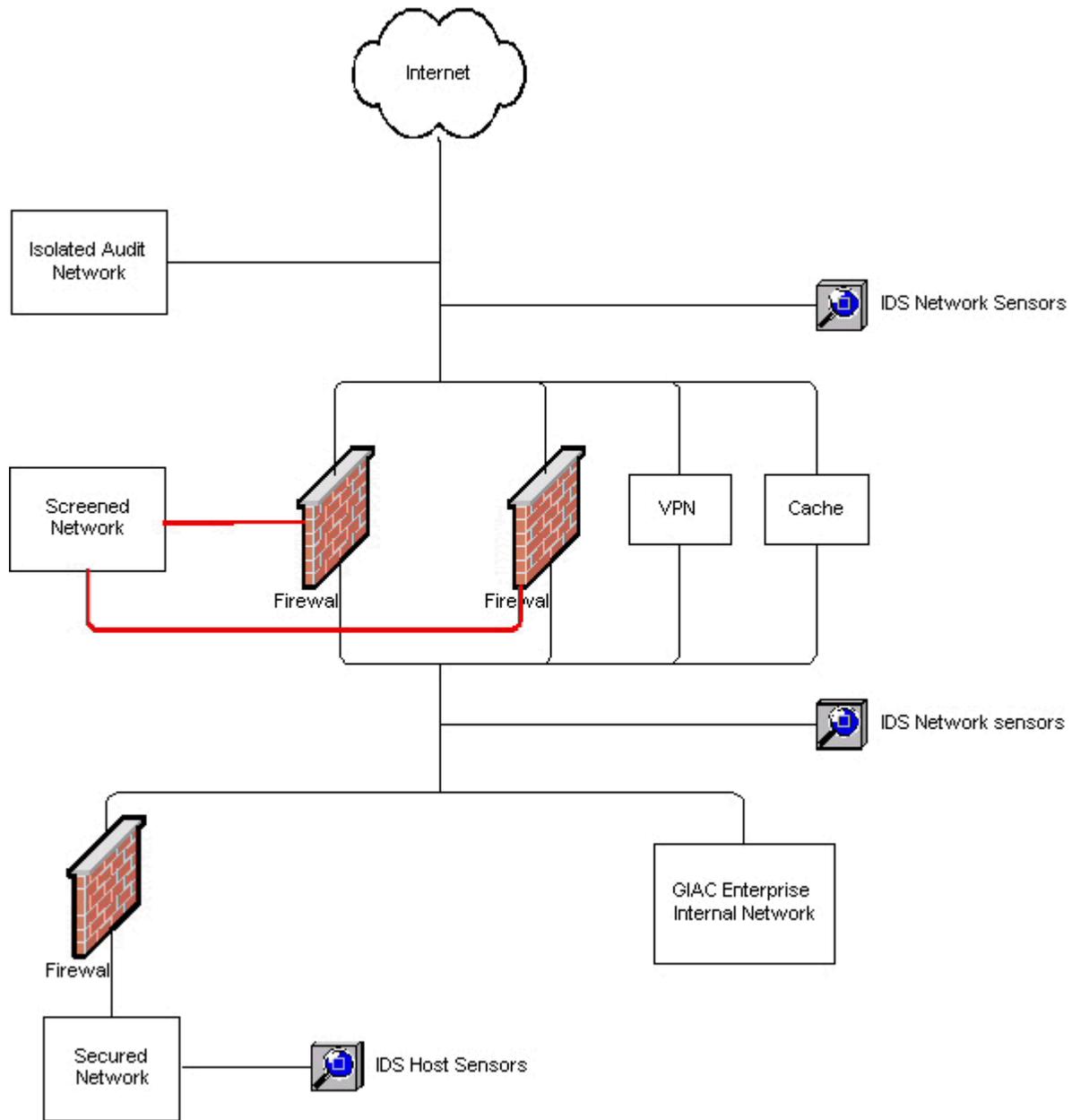
- internal firewalls (are internal firewalls appropriate for additional, layered protection; to segment internal networks...?);
- secure remote access (is additional remote access required by administrators, salespeople, telecommuters...?).

Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

The network can be as complex or as simple as you like as long as it meets the functional requirements that you define according to the guidelines given above. The important thing is not how elaborate your network is, but that your design actually works.

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

**Modular View of GIAC Enterprise's Network**



## Assignment I: Security Architecture

### 1.1 Business Description

**Giac** Enterprise is an e-business, which deals in online sale of Fortune Cookie sayings. **Giac** enterprise has expanded rapidly in the past two years, and continues to expand exponentially. The company's success is attributed to their ability to meet customers' needs on demand via the Internet. Customers are able to retrieve information such as product literature, order status and account information, while simultaneously purchasing and downloading the Fortune Cookie saying database online.

To better serve customer demand, **Giac** Enterprise has created a unique program that pools customer demand. The program analyzes and charts client's demands, and creates statistical information. These statistics are presented to suppliers for bid, thus making the supplier market competitive. **Giac** then passes the cost savings to their customer.

**Giac** also has partners around the world that translates and resells the fortune sayings to their local establishments.

### 1.2 Access Restrictions and requirements

Like a dual edged sword, **Giac**'s network engineers have to carefully factor in the access requirements and restrictions in the design of the security architecture. Too tight of a restriction will hinder the company from doing business effectively, and loosely assigning requirements will attract the wrong crowd. The engineers must provide ample access to customers, suppliers, partners and **Giac**'s employee, but not jeopardize the integrity of the overall network security.

Just like a good firewall rulebase, it is best to define a global restriction, and allow only known and needed access requirements. Using such a model on the overall architecture will help minimize unknown factors, and allow them to focus on known vulnerabilities used on protocols allowed into **Giac**'s internal network.

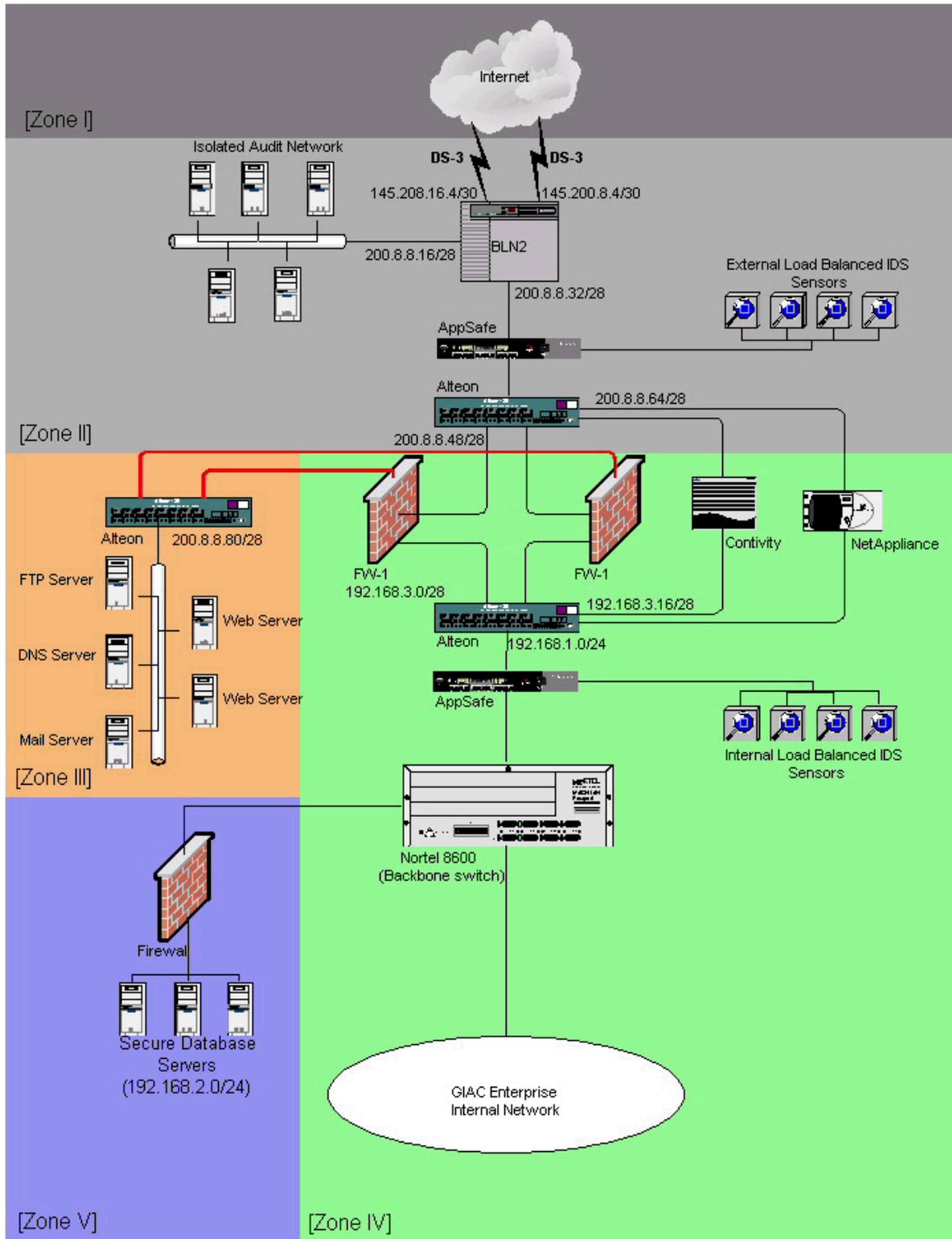
**Giac**'s network engineers have taken the zone approach in the design of the network. The zones are broken down as such:

	Color	Zone Definition
<b>Zone I</b>		Public Network
<b>Zone II</b>		External Network
<b>Zone III</b>		Screened Service Network
<b>Zone IV</b>		Internal Network
<b>Zone V</b>		Secured Network

**Zone I** is categorized as the most un-trusted network, while **Zone V** is the most trusted network. This layered approach can be compared to the water purification process. The first layer is used to filter large sediments, and as water flow past each layer, the filter gets more refined. The flow of network traffic uses the same principal.

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

**GIAC Enterprise Network Architecture**



*Note: The management interfaces on IDS and Firewall are omitted to avoid over cluttering the diagram. All management interfaces use private IP addresses.*

### **1.3 Business Operation**

For Giac Enterprise to successfully conduct its business online, access is required for the following groups:

*Potential Customers/Internet public:* GIAC is a successful global e-business enterprise that is highly exposed to the Internet. Web (HTTP) and Domain Name services (DNS) should be made available to this group.

*Customers:* GIAC customers are spread across the world (different time zones), which mean business transactions occurs 24 hours a day on GIAC's network. All customers will access non-secure information using HTTP, while secure information will use SSL.

*Suppliers:* Just like GIAC's customers, suppliers will access non-secure information via HTTP and secure information via SSL.

*Partners:* Just like anyone from the public network, the partners can access non-secure information via HTTP. However, all other access will require VPN access.

*GIAC Internal:* To enhance security, all internal hosts will use private IP addresses. All FTP and HTTP requests will be redirected to a cache box.

*GIAC External/Roaming:* GIAC has sales and support forces that constantly need access into the internal network, such as checking e-mail. All roaming employees are required to use VPN to access resources on the internal network.

### **1.4 Service, Protocol and Application definition by Zone**

**Zone I:** This is the public zone which GIAC Enterprise has no control.

**Zone II:** This is considered the External network of GIAC enterprise. The existence of such a network is to put individuals or groups who cannot comply with the ruleset of the firewall. This area is exposed to all traffic except for that which is filtered by the router.

**Zone III:** Also known as a screened service network. The only services implemented in this zone are SSH, DNS, FTP, HTTP and Mail services. Port 20, 21, 22, 25 and 53 are the only allowed egress traffic out of this zone. NTP service is only allowed from the internal network.

*Note: Only SSH version 2 is allowed for authentication. SSH1 has been disabled, as there is a well-known exploit. X-Force from Internet Security Systems informed GIAC of the [exploit](#).*

**Zone IV:** The firewall has an explicit deny rulebase. The only protocols allowed into GIAC's internal network are implicitly defined in the rulebase. Detail policy setup is available in Assignment II for firewall policy setup.

**Zone V:** The firewall is in place to protect the database server. There are no other types of services offered on the subnet. The firewall rulebase has been customized to the access requirements of these database servers. Source and destination hosts are also defined in the rulebase. All unknown sources are dropped by default.

**Note:**

*FTP services: Though there are known FTP vulnerabilities, GIAC has decided to make this service available to customers. Removing this service can be an inconvenience to the customer, which could easily translate to lost sales.*

*DNS services: GIAC Enterprise will use split DNS, by having a pair of External DNS servers for the Internet to use for resolving GIAC Enterprise's domain name, and a pair of Internal DNS servers, just for internal network name resolution. The external DNS are placed on the Service Network (Zone III), and are independent from the Internal DNS servers, which are located at the Internal network (Zone IV). Internal DNS will use NAT addresses so external host are not able to query them (in addition to DNS being blocked at firewall). Also, all external queries will be forwarded to the external DNS server for resolution.*

*NTP server: Routers, Intrusion detection sensors (IDS), TopLayer switch, and all other servers (e.g web, FTP, DNS, syslog) will be synchronized with a NTP server. The NTP server will be synchronized with the atomic clock. Synchronized time is critical in forensic investigation.*

## **1.5 Hardware specifications, version and function**

### **1.5.1 Border Router**

*Model:* Backbone Link Node 2 (BLN2)  
*Manufacturer:* Nortel Networks Inc.  
*Software Version:* BayRS version 14.0.2.2  
*Information link:* <http://www.nortelnetworks.com/products/01/ewanrs/blnr/index.html>

*Function:*

BLN2 is a rack-mountable chassis, housing four Intelligent Link Interfaces (ILI) and an additional slot for installing system resource module (SRM). In our configuration, we will use two slots for the High Speed Serial Interface (HSSI) for the redundant DS-3. Having the HSSI on two separate ILIs provide redundancy in the case of an ILI failure. The third slot has a FRE4-PPC 10/100 Mbps TX ILI for Ethernet network connectivity. The fourth slot is reserved for future expansion such as an octet FRE Ethernet slot for Point-to-Point connections. BLN2 has redundant power supply and all ILIs are independent of one another.

### **1.5.2 IDS load balancing switch**

*Model:* AppSafe 3502  
*Manufacturer:* TopLayer  
*Software Version:* 3.52.00  
*Information Link:* <http://www.toplayer.com/products/hardware/index.html>

*Function:*

The primary responsibility of the AppSafe is to provide load balancing among several Intrusion Detection Servers (IDS) network sensors. In addition to load balancing, it has found a new niche in URI filtering, and off loading the firewall's burden for packet sniffing.

### **1.5.3 IDS Network**

*Model:* RealSecure Network Sensor  
*Manufacturer:* Internet Security Systems  
*Software Version:* RealSecure version 6.0 with X-Press Update 3.4  
*Information Link:* [http://documents.iss.net/literature/RealSecure/rs\\_ps.pdf](http://documents.iss.net/literature/RealSecure/rs_ps.pdf)

*Function:*

GIAC Enterprise use RealSecure Network Sensor 6.0 for intrusion detection. All sensors report to a central management console, and a central MS SQL database. There are two sets of sensors, one outside of the firewall and one inside of the firewall. Having the sensor on both sides of the firewall enables GIAC to audit the firewall and active security features on the AppSafe. For example, if URI filtering is activated on the external AppSafe, the external sensors will see the offending mirror traffic on the ingress port of the AppSafe, however, on the internal sensor, they should not see it as the external AppSafe will not forward the offending traffic.

### 1.5.4 Isolated Audit Network

*Function:*

This lab is created to simulate attacks into GIAC Enterprise's network for intrusion auditing. This lab is isolated physically, so no accidents or confusion can stem from this network to jeopardize the Internal network infrastructure.

### 1.5.5 Load Balancer and Redirector

*Model:* Alteon 184  
*Manufacturer:* Nortel Networks  
*Software Version:* 9.00  
*Information Link:* <http://www.nortelnetworks.com/products/01/alt180/index.html>

*Function:*

The external and Internal Alteon load balances the parameter firewall. The Alteon uses a virtual IP (VIP) interface representing the firewall pair. Traffic load is then divided equally between the firewall pair. The Alteon monitors the status of the firewalls, and reacts almost instantaneously when it detects a communication failure.

The Alteons also act as traffic redirectors. The internal Alteon redirects all web request traffic to the Network Appliance cache server. VPN requests are also redirected to the Contivity server.

*Note: The latest code release added the capability of IDS load balancing, however; it still does not provide the ability to load balance the IDS by protocol.*

### 1.5.6 Parameter/Primary Firewall

*Hardware Model:* Sun Enterprise 450  
*Manufacturer:* Sun Microsystems Inc.  
*Firewall Software:* CheckPoint FW-1 4.1 with SP4  
*Information Link:* <http://www.sun.com/servers/entry/450/>  
<http://www.checkpoint.com/products/security/firewall-1.html>

*Function:*

CheckPoint FW-1 is installed on the Sun E450 platform running Solaris 2.7. All the latest patches are applied to the firewall.

### 1.5.7 VPN

*Model:* Contivity 4600  
*Manufacturer:* Network Appliance  
*Software version:* 03\_50.44  
*Information Link:* <http://www.nortelnetworks.com/products/01/contivity/#>

*Function:*

Nortel's Contivity 4600 provides VPN services, which is capable of serving up to 5000 simultaneous VPN sessions.

### 1.5.8 Cisco PIX Firewall

*Hardware Model:* Cisco PIX515

*Manufacturer:* Cisco Systems

*Firewall Software:* PIX 5.0

*Information Link:*

[http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix51\\_ds.htm](http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix51_ds.htm)

*Function:*

GIAC implemented a Cisco PIX firewall for the secure network upon the recommendation of SANS. The purpose of using a firewall different from the Primary firewall is to avoid intrusions of zero day exploits targeted at a vendor specific firewall. Therefore, if there was a zero day exploit specifically on the CheckPoint Firewall-1, the exploit could not be applied to the PIX firewall on **Zone V**.

### 1.6 Assumptions:

- i. GIAC's network engineers use the following sources to keep up with the daily security threats:
  - <http://www.sans.org>
  - <http://www.securityfocus.com>
  - <http://www.phoneboy.com>
  - <http://xforce.iss.net>
  - <http://www.hackerwhacker.com>
  - <http://www.incidents.org>
- ii. Other resources used for knowledge enhancement
  - <http://www.l0pht.com>
  - <http://www.cisco.com>
  - <http://www.nortelnetworks.com>
  - <http://www.toplayer.com>
- iii. GIAC Enterprise subscribes to premium support from the following organizations:
  - Nortel Networks
  - Checkpoint
  - Cisco
  - Sun
- iv. All application servers have the latest security patch and hot fixes installed.
- v. All GIAC Enterprise network engineer are GIFW certified by SANS.

## Assignment 2 – Security Policy (35 points)

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

- Border Router
- Primary Firewall
- VPN

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

By "security policy" we mean the specific Access Control List (ACL), firewall ruleset, IPsec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider the access requirements for internal users, customers, suppliers, and partners that you defined in Assignment 1. The policies you define should accurately reflect those business needs as well as appropriate security considerations.

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

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

In addition, for **one** of the three security policies defined above, you **must** incorporate a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information to clarify your instructions. Be certain to include the following:

1. A general explanation of the syntax or format of the ACL, filters, or rule for your device.
2. A general description of each of the parts of the ACL, filter, or rule.
3. An general explanation of how to apply a given ACL, filter, or rule.
4. For each ACL, filter, or rule in your security policy, describe:
  - the service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.
  - Any relevant information about the behavior of the service or protocol on the network.
  - If the **order** of the rules is important, include an explanation of why certain rules

must come before (or after) other rules.

5. Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

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

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

## Assignment II - Security Policy

### 2.1 Overview

The application and implementation of security policy is the essence of securing a network. The ability to assign policies at different depth of the topology allows the flexibility to meet access requirements of the overall organization. However, the engineers will have to be diligent and organized in the deployment of these policies. A disorganized implementation of these policies at multiple levels will cause administrative headache when problems arise.

Every organization has different sets of security policies. Some are not as define as others, as each organization views the value of their data/information differently. There is a linear relationship between the value of the data, and the implementation level of a security policy. GIAC Enterprise's fortune cookie saying database is highly valuable to the company. If a cracker hacks into the network, and makes the database freely available to the Internet community, GIAC Enterprise will have nothing valuable to sell.

As a large organization, the need of employees varies greatly. Having a flat security policy across the entire organization could hinder the productivity of employees, which could cause potential loss to the company as a whole. To provide flexibility to meet these requirements, we have created different levels of access by zone definition.

### 2.2 Security Considerations

According to SANS, there are four primary methods used by an attacker to gain unauthorized access to a system.

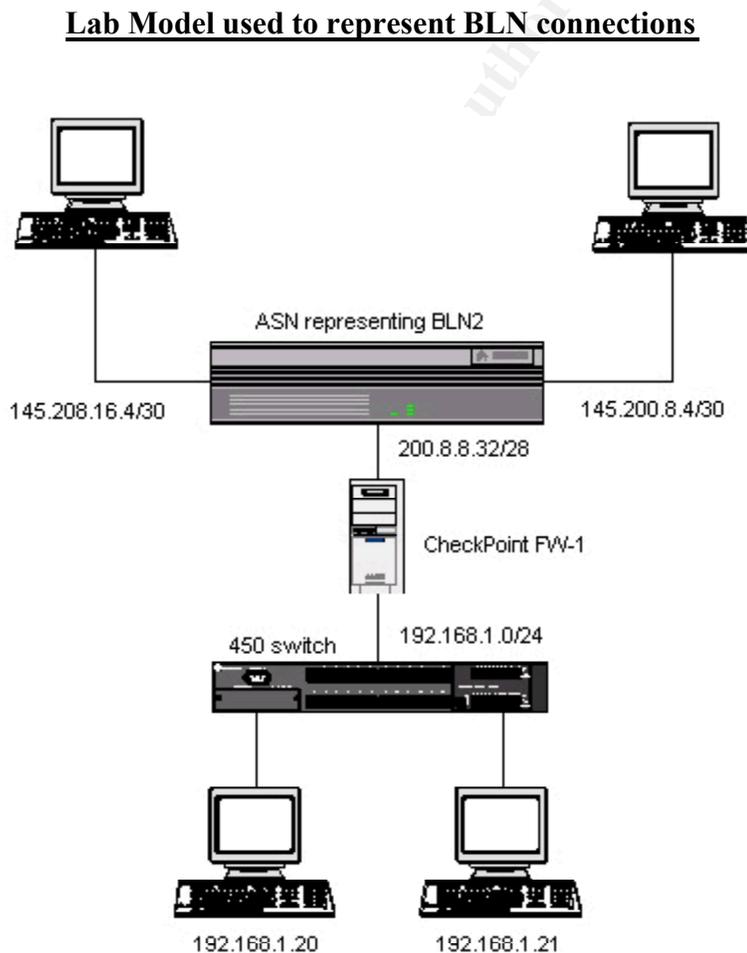
- Vulnerable services
- Insider information
- Poor Access Control
- Virus payload.

Vulnerable services are exploits discovered in application services. Generally, this refers to server application, but this vulnerability can extend to the firewall and router also. Insider information refers to someone knowing the schematics of the organization, which are usually not available to general public. The danger usually refers to disgruntle employees who seek revenge. Poor Access Control usually stems from incompetent administrators who do not understand the concept of security architecture. Finally, virus payload such as the "I Love You" virus can cause a catastrophic disaster. There should be a defined policy to warn employees not to open unknown attachments, and have a defensive mechanism in place.

From the above, we can deduce that security threats come from all angles. Therefore, it is highly important that security policies not only cover internet network access, but also physical and communication access. Equipment and building access should be secured and logged. Employees will be educated of the potential threats, and taught how to deal with possible threats.

### **2.3 Note on configuration and implementation setup:**

To illustrate GIAC Enterprise's network setup, I have setup a small-scaled model using Nortel's Access Stack Node router (ASN) to represent the BLN2. The ASN has less processing power, redundancy and expansion slots compared to BLN2; however, it will sufficiently represent the illustration of our Enterprise setup. Because both BLN2 and ARN use the same version of BayRS (Version 14.0.2.2), the setup is almost identical. Below is a modular diagram of the model used to represent GIAC Enterprise.



Nortel Network's router can be configured using Bay Command Console (bcc) or SiteManager.

Bcc is a command line interface used to configure Nortel's router. SiteManager is the GUI interface that ultimately achieves the same result as using bcc. Most administrators today use SiteManager to configure their router after the initial setup of the IP and SNMP properties on the router. However, to make this assignment more interesting, all filter configuration will be shown using bcc.

*Note: Telnet will be enabled on the router; however, access is only possible from the internal interface to specific list of hosts.*

## 2.4 Implementation of Border router policy



I will use this section to demonstrate how to use and implement a policy on GIAC's border router. In addition, I will use this section to demonstrate the required tutorial. Below is the summary of the step-by-setup guide.

- **2.4.1 Defining a security policy for border router**
- **2.4.2 Summary on using bcc**
- **2.4.3 Router setup**
- **2.4.4 Hardening the router**
- **2.4.5 Testing the policy**

### 2.4.1 Defining a security policy on the border router

As mentioned earlier, the function of a router is routing. However, we can use the router to filter traffic that we do not want in the network. Applying this filter at the border will relief the entire organization from seeing unwanted traffic. Below is the list of traffic that we do not want passing the router.

- ✓ Drop inbound private IP range(as defined in [RFC 1918](#))
- ✓ Drop inbound 169.254.0.0/16 (default subnet used by Microsoft clients when no DHCP server is present)
- ✓ Drop inbound 200.8.8.0/24 (prevents spoofing)
- ✓ Drop inbound traffic from the following ranges:
  - 127.0.0.0-172.255.255.255
  - 224.0.0.0 – 252.255.255.255
  - 255.0.0.0 – 255.255.255.255

- ✓ Drop inbound traffic with the following destination ports
  - Port 160, 161 (snmp)
  - Port 135 – 139 (netbios)
  - Port 515 (ldp)
  - Port 23 (telnet)
  - Port 111 (sunrpc)
  - Port 6000-6013 (X windows)

## 2.4.2 Summary on using BCC

Before we dwell into the creation of filters on the router, here is a brief summary of how to use BCC. There are basically two different levels when using BCC – monitor and admin. Monitor mode allows you to see router statistics in read only mode, while admin is used for making changes on the router. For monitor mode, login as “User”, and for admin privilege, login as “Manager”.

### Basic BCC

The BCC configuration hierarchy is similar to that of Unix or Windows file system. It has directories, subdirectories and files. Just like the file system, BCC has parent objects, that contain child objects, and each child object can be the parent of other child object embedded in them.

For example, here we configure port 1 on slot 4 of the router with IP address of 200.8.8.34/28.

1. Telnet/console into the router.
2. Login as Manager
3. Type “**bcc**” (this will move you from Technical Interface into BCC)
4. Type “**config**” to enter configuration mode.
5. Type “**Ethernet /1/4/1**”. This will move you to unit 1(router), slot 4 and port 1. When you are in this sub-object, all configurations will only affect this port.
6. To assign an IP address, type “**ip 200.8.8.34/28**”
7. Type “**back**” to move up one object, then type “**show config -r**”, which will show the new IP address assigned to this Ethernet interface.

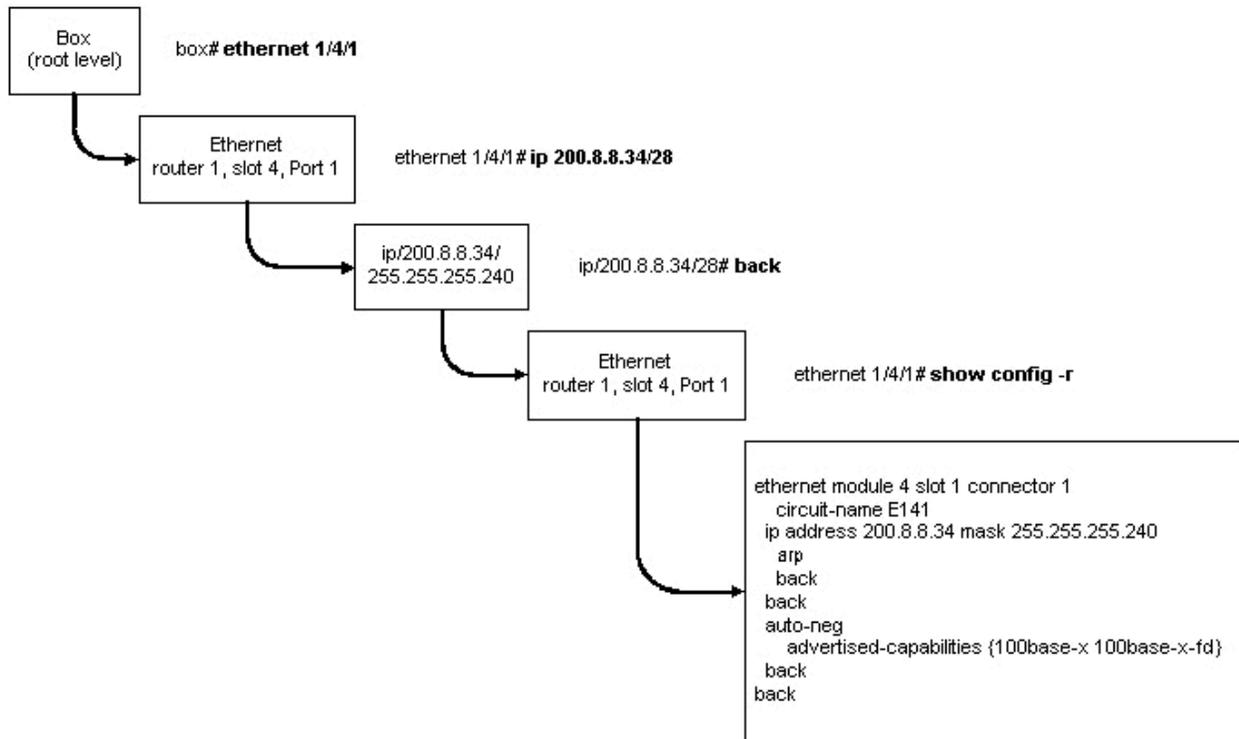
To move up the object tree, use the “back” command. It is also highly advisable to save the configuration every time a change is made. To save the configurations, use the following command:

```
Save config 1:config
```

The above command will save the current configurations to a file named “config” on volume 1.

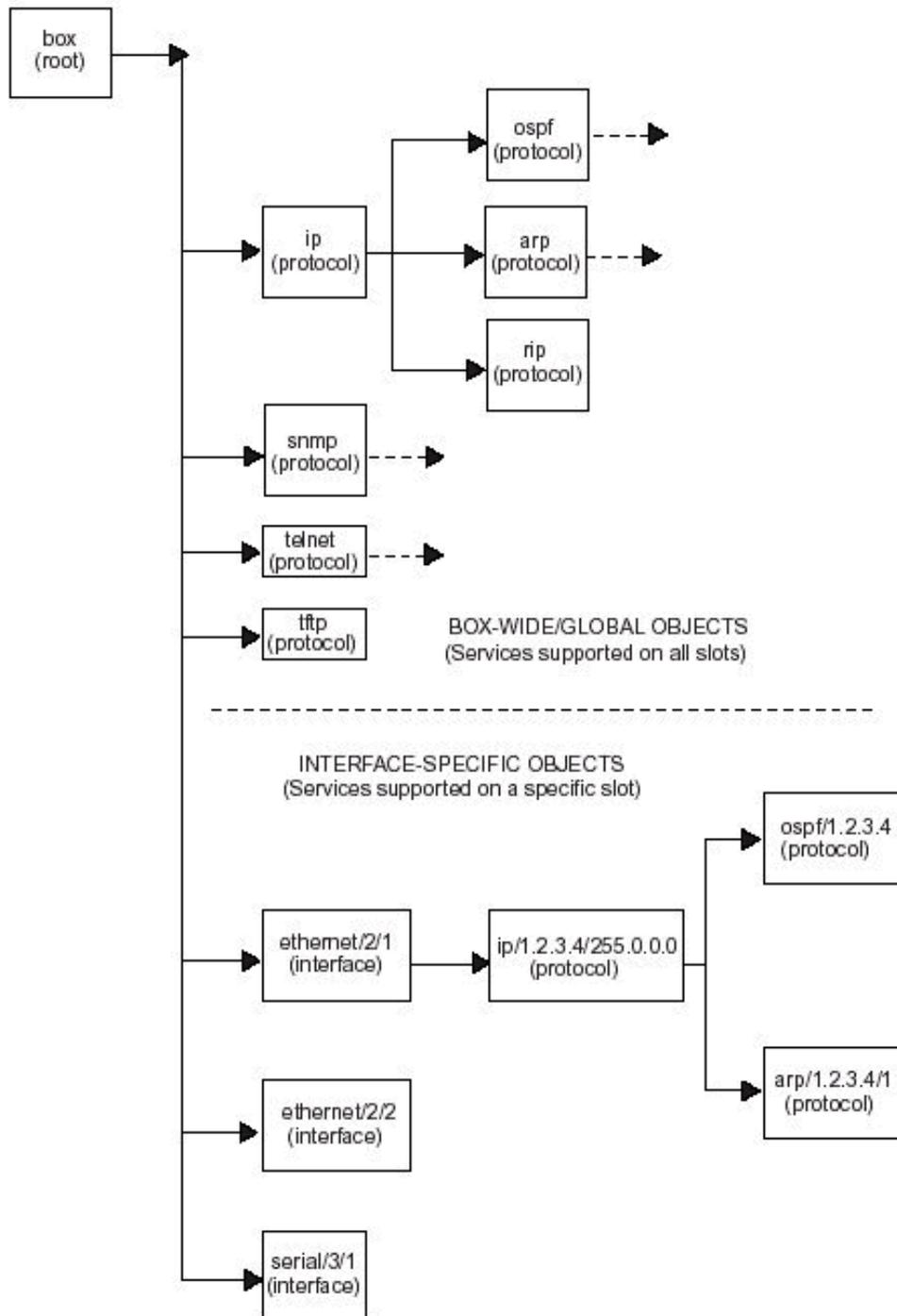
If help is needed, type “?”. BCC will show a list of available commands.

### IP Configuration diagram of BCC.



© SANS Institute 2000 -

Below is a sample of the hierarchal structure of BCC extracted from <http://support.baynetworks.com/library/tpubs/pdf/router/cns/03562A00.PDF>.



### 2.4.3 Router Setup

In this section, we will attempt to do the following:

- Connect to router
- Change default password
- Define interface properties
- Define SNMP properties
- Enable banner
- Enable logging and syslog

#### Connecting to router

Unlike Cisco routers, “out of the box” Nortel routers do not advertise any type of service. Each service has to be turned on manually. For example, to turn telnet on, it has to be enabled via the console using bcc.

Using a null modem cable, connect a PC to the router. A terminal session is established using the settings of 9600, 8, none and 1. Once the connection is established, login using the default user ID of either “Manager” or “User”, which by default has a blank password.

#### Changing default password

Manager and User are the default users on the router. To set a password, type password, then enter the old password, and specify the new password twice. Below is a screen shot on changing the password for Manager and User.

```

Welcome to the Backbone Technician Interface

SANS-Test#: password
Changing password for Manager
Old password:
New Password:
Retype new password:
Manager password changed.

SANS-Test#: password User
Changing password for User
Old password:
New Password:
Retype new password:
User password changed.

SANS-Test#: █

```

#### Defining interface properties

Referring to GIAC Enterprise’s architecture, we have to define IP properties for three interfaces.

Ethernet 1/4/1	200.8.8.34/28
Ethernet 1/2/1	145.200.8.5/30
Ethernet 1/2/2	145.208.16.5/30

The step-by-step setup for interface 1/4/1 was demonstrated in section 2.4.2. To setup the other two interfaces, “back” to the root object, then drill into each interface object, and define the IP properties.

### Defining SNMP properties

The most common way to setup/manage a Nortel router is via “SiteManager”, which is the GUI interface software. For the GUI interface to work, SNMP properties have to be defined.

List of SNMP properties to define:

- Community label
- Access type
- Manager access

Step-by-step setup:

1. At BCC root object, type “**snmp**”. This will move you into the snmp object.
2. We want to define two communities, one with “read-write” access, and the other just “read-only”. SANS community will have “read-write”, and SANSMON community will have “read-only” privilege.
3. Type “**community sans**” to create the SANS community.
4. To define access, type “**access read-write**”, which will give the SANS community “read-write” access.
5. To define management client, type “**manager 192.168.1.2**”.
6. Repeat steps 2 thru 5, except for step #4, as the default access is set to “read-only”.

### Enable Banner

The use of banner is to warn unauthorized intruders that their activities are being recorded, and give them the opportunity to retract. Legal information can be added to the banner to notify persistent unauthorized intruders of the consequence of their actions.

Two different types of banner can be displayed, one prior to login, and the other a welcome notice. To create a login banner, create a text file named “**ti\_notice.txt**”. The text file can contain warning messages about authorized use, system specific information and contact information. To create a welcome message after the logging in, create another text file named “**ti\_msg.txt**”. TFTP both files to the router. If both files are absent, the default login and welcome notices are displayed.

### Enable logging

Logging is enabled on the router itself and also configured to send logs to a central syslog server.

At root object:

1. **syslog**
2. **log-host <syslog server>**
3. **state enable**

```

stack# syslog
syslog# ?

Sub-Contexts:
  log-host
Parameters in Current Context:
  log-poll-timer  maximum-hosts  state
System Commands:
  To list all system commands, type "help commands".
  For detailed help on a specific command, type "help <command>".

syslog# state
state enabled
syslog#

```

#### 2.4.4 Hardening the router

In theory, we can define an explicit deny of all services, and only allow predefined services through the router. However, most implementations in the real world, rarely apply an explicit deny filter on the router. Furthermore, the main function of a router is to route traffic, not assume the responsibilities of the firewall. Nevertheless, the router can help filter out certain traffic that we do not want see pass **Zone 1**.

#### Building Filter Templates on BLN2/ARN

Traffic filters created on Nortel routers are similar to Access Control List (ACL) created on a Cisco router. There are two ways to create filters -- using filter templates or applying traffic filters on the interface itself. Creating filter templates is the preferred method as it consumes less space in the router's memory. Filter templates are not active until they are actually applied to the interface. When multiple templates are applied on an interface, a precedence number can be applied to each filter template on the interface. The lower the precedence number, the higher the priority.

Our plan of action is to create filter templates for each of the traffic we wish to block, as defined by our security policy for the border router. The next step is to apply the filter template to the interface that we want to block the defined traffic.

Log in to the router via the console or telnet session. Because we are creating filter templates, we will login as Manager. Once logged in, get into BCC mode by typing "bcc".

Step-by-step filter-template setup:

1. Type "**config**" to go into configuration mode.
2. Type "**ip**" to specifically define filter-template for this protocol
3. Create filter-template and give it a meaningful name for easy recognition  
**Filter-template <template-name>**

4. Type “**match**” to define the matching criteria of the filter-template
5. Define the action you want taken when criteria matches. Type “**action <value>**”.  
Example of legal values are accept, and drop.
6. Type “**action-log enable**” to enable logging.

Using the steps defined above, we create a filter-template for each of the following:

**-- Block inbound traffic with private source address as defined in [RFC1918](#).**

To create the template above, execute each of the following command, beginning at root object:

```

ii. ip
iii. filter-template "block private"
iv. match
v. source-network range 10.0.0.0-10.255.255.255
vi. source-network range 172.16.0.0-172.31.255.255
vii. source-network range 192.168.0.0-192.168.255.255
viii. action drop
ix. action-log on
x. back
xi. show config -r

```

Step x. will show the following output.

```

filter-template template-name {Block Private}
  match
    source-network range 10.0.0.0-10.255.255.255
    back
    source-network range 172.16.0.0-172.31.255.255
    back
    source-network range 192.168.0.0-192.168.255.255
    back
  back
  actions
    action drop
    action-log on
  back
back

```

We repeat the steps above for the rest of the defined security policy. Below are the built configurations with definition.

**-- Block telnet traffic**

```

filter-template template-name {Block Telnet}
  match
    dest-tcp-ports 23
    protocol 6
    source-network range 0.0.0.0-255.255.255.255
  back
back
  actions
    action drop
    action-log on
  back
back

```

When this filter is applied to the interfaces connecting to the Internet, it blocks all telnet traffic

coming into GIAC's network.

#### -- Block ICMP traffic

```
filter-template template-name {Block ICMP}
match
  protocol 1
  source-network range 0.0.0.0-255.255.255.255
back
back
actions
  action drop
  action-log detailed
back
back
```

Does not allow external source to PING internal host.

#### -- Block Netbios traffic

```
filter-template template-name {Block Netbios}
match
  dest-tcp-udp-ports 135-139
  protocol {6 17}
back
actions
  action drop
  action-log on
back
back
```

Netbios was initially built as an efficient protocol for Local Area Network (LAN). Security was not highly considered, which contributes to its appearance on SANS' Top Ten Security Threat List. Therefore, we are blocking it from GIAC's internal network.

#### -- Block SNMP traffic

```
filter-template template-name {Block SNMP}
match
  dest-udp-ports 161
  protocol 17
  source-network range 0.0.0.0-255.255.255.255
back
back
actions
  action drop
  action-log on
back
back
```

SNMP protocol is used for network management. However, if an intruder finds the correct SNMP values, he can potentially map out the network. Therefore, it is best to block SNMP access from the Internet.

#### -- Block unwanted traffic

```
filter-template template-name {Block unwanted traffic}
match
  source-network range 127.0.0.0-127.255.255.255
back
```

```

    source-network range 255.0.0.0-255.255.255.255
    back
    source-network range 224.0.0.0-252.255.255.255
    back
back
actions
    action drop
    action-log on
back
back

```

Loopback, broadcast and multicast source address ranges do not serve any purpose in GIAC's network. Therefore is also blocked at the border router.

### -- Block sunrpc

```

filter-template template-name {Block sunrpc}
match
    dest-tcp-udp-ports 111
    protocol {6 17}
back
actions
    action drop
    action-log on
back
back

```

This protocol is listed as one of the Top ten vulnerabilities at SANS (<http://www.sans.org/topten.htm>). In addition, it is not needed within the GIAC Enterprise.

### -- Block ldp

```

filter-template template-name {Block ldp}
match
    dest-tcp-ports 515
    protocol 6
back
actions
    action drop
    action-log on
back
back

```

Via CheckPoint Log viewer, we have seen a fair share of scans for ldp port 515. Obviously, it is a well-known port for vulnerabilities. CERT and FedCIRC describes the buffer overflow caused by multiple line printer daemon (LDP), which could potentially give root access to intruder. (<http://www.infosecuritymag.com/digest/2001/11-08-01.shtml>)

### -- Block X Windows

```

filter-template template-name {Block X-windows}
match
    dest-tcp-udp-ports 6000-6013
    protocol {6 17}
back
actions
    action drop
    action-log on
back
back

```

SecuriTeam at <http://www.securiteam.com/exploits/2ZUQ2QAQNU.html> describes several X windows vulnerabilities that could be a potential security issue in GIAC's network.

### **Egress Filters**

The following two filter templates are created for the ingress traffic on interface Ethernet 1/4/1. These are the traffic leaving GIAC's network for the Internet.

#### **Allow Internal**

```
filter-template template-name {allow internal}
  match
    source-network range 200.8.8.0-200.8.8.255
  back
back
actions
  action-log on
back
back
```

When this filter is applied, it specifically allows through source with IP source of 200.8.8.0 to 200.8.8.255.

#### **Deny All**

```
filter-template template-name {deny all}
  match
    source-network range 0.0.0.0-255.255.255.255
  back
back
actions
  action drop
  action-log on
back
back
back
```

When we combine the “Deny All” filter with the “Allow Internal” filter, it will stop spoofing from within GIAC Enterprise. The precedence of these rules is important. This will be elaborated when we apply these templates to the interfaces.

### **Applying Filter Templates to the Interfaces**

Now that we have successfully created all the required filter-templates, we need to apply them to the appropriate interfaces. Interface 1/2/2 (145.208.16.5/30) and 1/2/1 (145.200.8.15) are the gateways to the Internet. We apply the filter templates on the ingress traffic of these ports.

Step-by-step setup, beginning from the root object:

**i. ethernet 1/2/1**

The command above moves us into the object interface of 1/2/1

**ii. ip 145.200.8.5**

Defines the specific protocol sub-object

**iii. traffic-filter filter-name filter1**

Creates a filter on IP interface 1/2/1

- iv. **template-name "Block Private"**  
Applies template-filter "Block Private" to Filter1
- v. **back**

Repeat steps #3 thru #5, each time defining a new filter name, and applying the following filter-templates:

- Block telnet
- Block ICMP
- Block Netbios
- Block SNMP
- Block unwanted traffic
- Block sunrpc
- Block ldp
- Block X windows

Using the same procedure above, apply the same set of filter-templates to interface 1/2/2. The precedence of how these filters are applied is not critical, as none of them over-ride one another.

Upon the completion of the application above, execute "show config -r" at root object level. At the interface level, you will see the following output:

```

ethernet module 2 slot 1 connector 1
  circuit-name E121
  ip address 145.200.8.5 mask 255.255.255.252
  arp
  back
  traffic-filter filter-name filter1
    template-name {Block Private}
    precedence 1
  back
  traffic-filter filter-name filter2
    template-name {Block Telnet}
    precedence 2
  back
  traffic-filter filter-name filter3
    template-name {Block ICMP}
    precedence 3
  back
  traffic-filter filter-name filter4
    template-name {Block Netbios}
    precedence 4
  back
  traffic-filter filter-name filter5
    template-name {Block SNMP}
    precedence 5
  back
  traffic-filter filter-name filter6
    template-name {Block unwanted traffic}
    precedence 6
  back

```

```
traffic-filter filter-name filter7
  template-name {Block sunrpc}
  precedence 7
back
traffic-filter filter-name filter8
  template-name {Block ldap}
  precedence 8
back
traffic-filter filter-name filter9
  template-name {Block X-windows}
  precedence 9
back
back
back
ethernet module 2 slot 1 connector 2
  circuit-name E122
  ip address 145.208.16.5 mask 255.255.255.252
  arp
  back
  traffic-filter filter-name filter1
    template-name {Block Private}
    precedence 1
  back
  traffic-filter filter-name filter2
    template-name {Block Telnet}
    precedence 2
  back
  traffic-filter filter-name filter3
    template-name {Block ICMP}
    precedence 3
  back
  traffic-filter filter-name filter4
    template-name {Block Netbios}
    precedence 4
  back
  traffic-filter filter-name filter5
    template-name {Block SNMP}
    precedence 5
  back
  traffic-filter filter-name filter6
    template-name {Block unwanted traffic}
    precedence 6
  back
  traffic-filter filter-name filter7
    template-name {Block sunrpc}
    precedence 7
  back
  traffic-filter filter-name filter8
    template-name {Block ldap}
    precedence 8
  back
  traffic-filter filter-name filter9
    template-name {Block X-windows}
    precedence 9
  back
back
back
```

Using the same set of instructions define above, we apply the following filter-templates to interface 1/4/1.

- Allow Internal
- Deny All

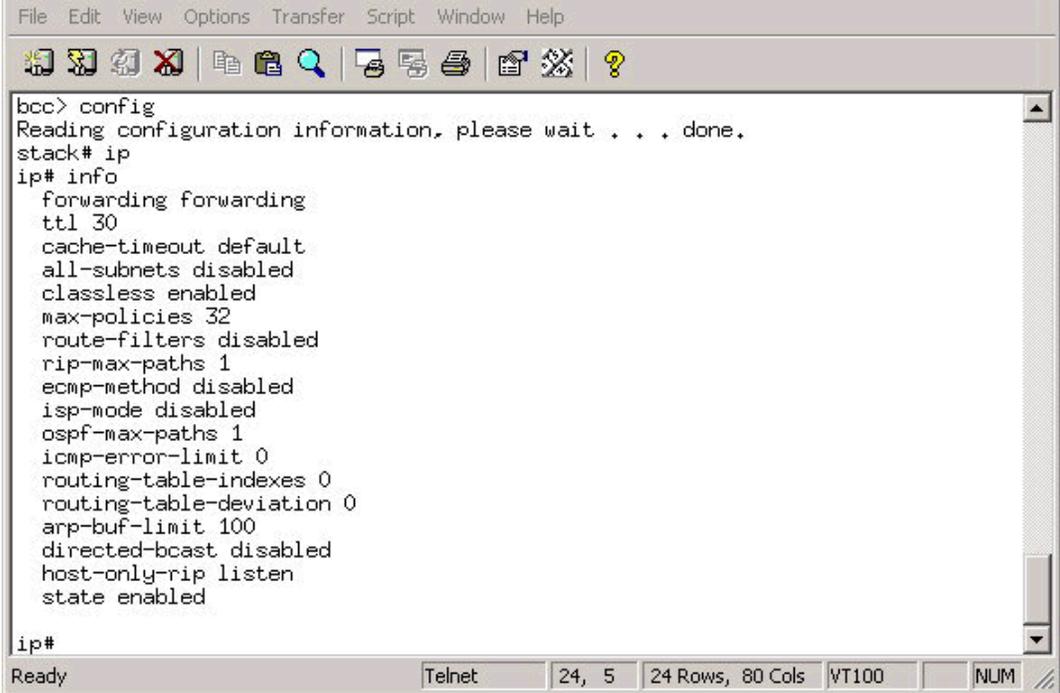
The results of our actions are as below:

```
ethernet module 4 slot 1 connector 1
  circuit-name E141
  ip address 162.114.210.86 mask 255.255.255.128
  arp
  back
  traffic-filter filter-name {filter 1}
    template-name {allow internal}
    precedence 1
  back
  traffic-filter filter-name {filter 2}
    template-name {deny all}
    precedence 2
  back
back
```

### Filter precedence

As you see, there are only two filters applied to this interface, however, the precedence of these rules are highly critical. Reversing the two rules will cause interface 1/4/1 to drop all outbound traffic to the Internet. The lower the precedence number, the higher the priority.

## Other IP properties



```

bcc> config
Reading configuration information, please wait . . . done.
stack# ip
ip# info
  forwarding forwarding
  ttl 30
  cache-timeout default
  all-subnets disabled
  classless enabled
  max-policies 32
  route-filters disabled
  rip-max-paths 1
  ecmp-method disabled
  isp-mode disabled
  ospf-max-paths 1
  icmp-error-limit 0
  routing-table-indexes 0
  routing-table-deviation 0
  arp-buf-limit 100
  directed-bcast disabled
  host-only-rip listen
  state enabled

ip#
Ready                               Telnet    24, 5    24 Rows, 80 Cols  VT100    NUM

```

[Classless](#) IP is enabled to utilize the IP addresses more efficiently, and directed broadcast has been disabled to prevent denial of service (as shown above).

Enabling Classless IP and disable directed broadcast

1. At root object of BCC, type “**ip**”
2. Type “**classless enable**” to enable classless
3. Type “**directed-bcast disable**” to disable directed-bcast
4. Typing “**info**” will show the assigned values of each child object within IP. (as shown above)

### 2.4.3 Audit Router’s security policy

#### Dropping ingress ICMP

Here we use the router’s log to view if ICMP pings are being dropped on the Ingress port. We execute “ping” from a workstation located in the 145.200.8.4 (representing a host on the Internet) network to a workstation on the 200.8.8.32 network (representing a host on the External network).

Below is the log generated by the router.

SANS-Test#: log

```

#      1: 01/22/2002 14:59:48.300  INFO      SLOT  1  TI      Code:
3
Log cleared !

```

```
# 2: 01/22/2002 14:59:48.765 INFO SLOT 1 IP Code:
141
IP Traffic Filter - Rule 3, Interface 145.200.8.5, Circuit 2 (Drop packet)
Dropped Pkt - Src: 145.200.8.6, Dst: 200.8.8.34, Prot: 1

# 3: 01/22/2002 15:00:14.800 INFO SLOT 1 IP Code:
0
The previous event on slot 1 repeated 26 time(s). [Code 141]

# 4: 01/22/2002 15:00:15.804 INFO SLOT 1 IP Code:
141
IP Traffic Filter - Rule 3, Interface 145.200.8.5, Circuit 2 (Drop packet)
Dropped Pkt - Src: 145.200.8.6, Dst: 200.8.8.34, Prot: 1
```

**Reading the log:**

# 2: 01/22/2002 14:59:48.765 INFO	Date and time information of the incident reported.
SLOT 1	The slot on the router that was reporting the incident
IP	Protocol Type
Code: 141	Nortel's Code for error reporting
IP Traffic Filter - Rule 3, Interface 145.200.8.5, Circuit 2 (Drop packet) Dropped Pkt - Src: 145.200.8.6, Dst: 200.8.8.34,	Rule 3 (Block ICMP) was used on Interface 145.200.8.5 to drop the packet, which was coming from source 145.200.8.6 going to 200.8.8.34.
Prot: 1	Refers to ICMP as defined in <a href="#">RFC 1700</a>

**Dropping ingress NetBIOS**

Again we use the log on the router to verify this test. We will use the same workstation to initiate a drive mapping to a workstation located in the 200.8.8.32 network. As defined in **Config Part III**, precedence 4 refers to the {Block Netbios} rule.

```
# 139: 01/28/2002 13:36:53.953 INFO SLOT 1 IP Code:
28
IP Traffic Filter - Rule 4, Interface 145.200.8.5, Circuit 2 (Drop packet)
```

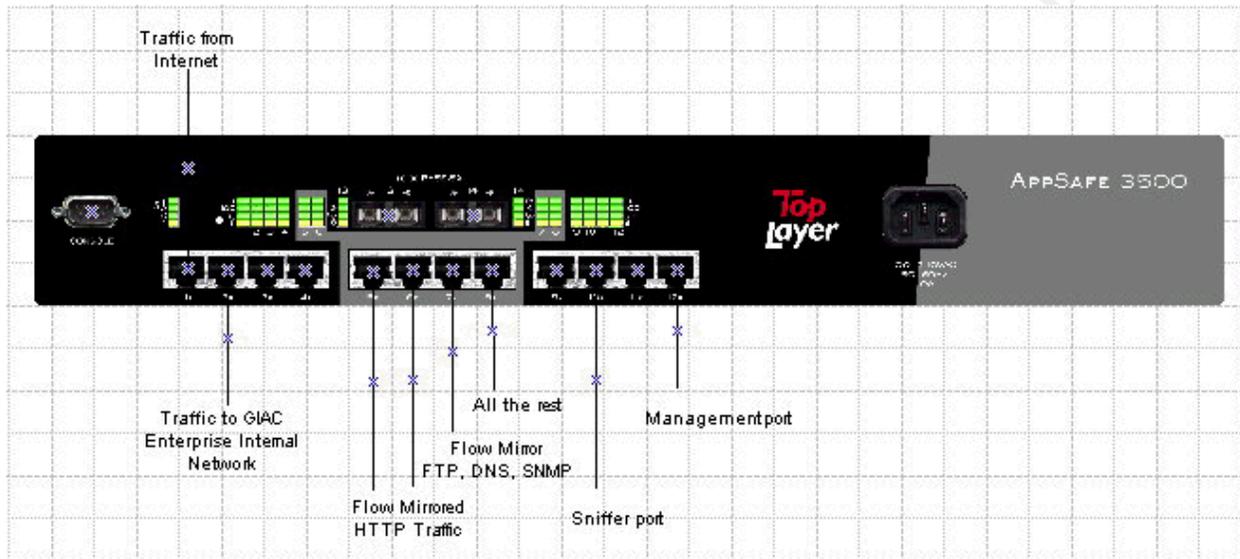
**Dropping ingress Telnet**

Telnet from 145.200.8.6 to 200.8.8.34 also fails as the log shows Rule 2 in action.

```
# 7: 01/28/2002 14:15:51.261 INFO SLOT 1 IP Code:
28
IP Traffic Filter - Rule 2, Interface 145.200.8.5, Circuit 2 (Drop packet)
```

**2.5 TopLayer AppSafe**

Intrusion detection has become an integral part of Security Architecture. Intrusion Detection Systems (IDS) have the ability to identify malicious intents, react automatically and notify appropriate authority. GIAC Enterprise has approximately 40 Mb/s of throughput traffic daily. A single IDS sensor will not have the ability to handle such throughput. The AppSafe from TopLayer was added into the network for IDS load balancing.



The AppSafe makes a carbon copy of the traffic flowing thru the bridge port (named the “**Road Bump**” zone), and flow mirror the traffic to the **IDS zone**. Policies are then applied to the traffic to remove malicious URI connections while load-balancing/filtering the mirrored traffic. For example, HTTP traffic has been assigned to port 5 and 6 while un-necessary traffic (non HTTP) is filtered completely. The IDS network sensors that connect to ports 5 and 6 see complete HTTP conversions and can be fine tuned to only detect HTTP intrusion signatures.

Just like Cisco’s Context Based Access Control (CBAC), the AppSafe also has the capability of examining traffic at the application layer, thus, enabling it to do Uniform Resource Identifier (**URI**) filtering. Recent events of “CodeRed” and “Nimda” were prime examples of the use of URI filtering.

Application	Service Class	CC Enabled	CC to (1)	CC to (2)	Redirection	TopFlow Enak
IETF ip.gre	Best Effort	Yes	FTP Only	Sniffer		Yes
IETF ip.tcp.ftp-control	Best Effort	Yes	FTP Only	Sniffer		Yes
IETF ip.tcp.ftp-data	Best Effort	Yes	FTP Only	Sniffer		Yes
IETF ip.tcp.http	Best Effort	Yes	HTTP Only	Sniffer		Yes
IETF ip.tcp.http-proxy	Best Effort	Yes	HTTP Only	Sniffer		Yes
Sun ip.rpc.rpcbind	Best Effort	Yes	All the Rest	Sniffer		Yes
Top Layer ip.tcp.http-otherURIs	Best Effort	Yes	HTTP Only	Sniffer		Yes
Top Layer unclassifiable	Best Effort	Yes	All the Rest	Sniffer		Yes
Code Red I	Denial of Service	Yes	HTTP Only	Sniffer		Yes
Code Red II	Denial of Service	Yes	HTTP Only	Sniffer		Yes
ICQ ip.udp.icq	Denial of Service	Yes	All the Rest	Sniffer		Yes
Kazaa	Denial of Service	Yes	All the Rest	Sniffer		Yes
Napster ip.tcp.napster	Denial of Service	Yes	All the Rest	Sniffer		Yes
Napster ip.tcp.napster-client	Denial of Service	Yes	All the Rest	Sniffer		Yes
Nimda-httpodbc.dll	Denial of Service	Yes	HTTP Only	Sniffer		Yes
VBS/Dismiss-A	Denial of Service	Yes	HTTP Only	Sniffer		Yes
VBS/Dismissed-B	Denial of Service	Yes	HTTP Only	Sniffer		Yes
c-CMD.EXE Exploit	Denial of Service	Yes	HTTP Only	Sniffer		Yes
d-CMD.exe Exploit	Denial of Service	Yes	HTTP Only	Sniffer		Yes
iisadmpwd	Denial of Service	Yes	HTTP Only	Sniffer		Yes
mem_bin-cmd.exe	Denial of Service	Yes	HTTP Only	Sniffer		Yes
msadc-cmd.exe	Denial of Service	Yes	HTTP Only	Sniffer		Yes
msadc-root.exe	Denial of Service	Yes	HTTP Only	Sniffer		Yes
scripts-cmd.exe	Denial of Service	Yes	HTTP Only	Sniffer		Yes
scripts-root.exe	Denial of Service	Yes	HTTP Only	Sniffer		Yes
vti_bin-cmd.exe	Denial of Service	Yes	HTTP Only	Sniffer		Yes

The policy above is applied to the “Road Bump” zone, which denies any traffic with a URI match as define in the policy. Also note the “CC(1)” and “CC(2)” columns direct flow mirroring into the predefined carbon copy groups. The external IDS network sensors will see the malicious traffic, as traffic are mirrored on the ingress port before the “Denial of Service” class is applied. Comparing the external to the internal IDS network sensors, we can see the URI filtering in action.

Application Groups: **Web Services** Total Applications: 21

Application	Profile
Code Red I	TCP:80,HttpURI:/default.ida?NNNNN
Code Red II	TCP:80,HttpURI:/default.ida?%0000%
c-CMD.EXE Exploit	TCP:80,HttpURI/c/winnt/system32/cmd.exe
d-CMD.exe Exploit	TCP:80,HttpURI/d/winnt/system32/cmd.exe
scripts-cmd.exe	TCP:80,HttpURI/scripts/.
mem_bin-cmd.exe	TCP:80,HttpURI/_mem_bin/.%
vti_bin-cmd.exe	TCP:80,HttpURI/_vti_bin/.%
msadc-cmd.exe	TCP:80,HttpURI/msadc/.
scripts-root.exe	TCP:80,HttpURI/scripts/root.exe?/c+
msadc-root.exe	TCP:80,HttpURI/msadc/root.exe?/c+
Nimda-httpodbc.dll	TCP:80,HttpURI/scripts/httpodbc.dll
iisadmpwd	TCP:80,HttpURI/iisadmpwd/.
VBS/Dismiss-A	TCP:80,HttpURI/groups/msafeverwonder.swf
VBS/Dismissed-B	TCP:80,HttpURI/Jobreee/main.htm
IETF ip.tcp.http	TCP:80
Top Layer ip.tcp.http-otherURIs	TCP:80,HttpURI/
IETF ip.tcp.ssl.http	TCP:443
IETF ip.tcp.rpc.http	TCP:593
Pointcast ip.tcp.http.pcast	TCP:80,HttpURI/FIDO
IETF ip.tcp.http-proxy	TCP:8080
ICQ ip.udp.icq	UDP:4000

Above is the screen shot of the AppSafe's Application Definition Library (ADL). Here, we define the application identification criteria, then add the custom defined application to the policy. For example, for Code Red 1, the match must use TCP port 80, and have a URI match of "/default.ida?NNNNN". As long as the characters match from left to right, it will apply the policy. In our case, the Code Red URI match will drop the packet at the AppSafe.

Before the implementation of AppSafe, GIAC's network engineers executed the "snoop" command on the firewall for troubleshooting. They would open two snoop sessions – one on the Internal interface and the other on the external, to see the ingress and egress traffic passing thru the firewall. Snoop takes away a lot of CPU cycles on the firewall, and can potentially cause problems. To offload the burden, GIAC setup a second copy of the flow mirror to a port setup for "snooping".

Port 10 on both AppSafes has been setup as a "sniffer" port. The network engineers setup a relatively inexpensive Linux workstation with three network interface cards (NIC), and loaded tcpdump. One NIC is assigned a private IP, and the other two are promiscuously plumbed. Each of the stealth interfaces is then connected to port 10, on both AppSafes. Now, the "snoop" can be done on the Linux workstation without burdening the firewall.

### 2.5.1 Security of the AppSafe

The AppSafe is transparent to the Internet, as it does not have an assigned routable interface. The management port is only visible from internal as it is assigned a private IP interface. Steps have been taken to make sure backdoor connection is not possible from the AppSafe.

*Note: One of the concerns GIAC's network engineers had was latency caused by the implementation of the AppSafe in-line. However, TopLayer assured us of no noticeable latency as the AppSafe is in place as a bridge. A [Shomiti](#) tab was proposed to mirror the traffic, but this will hinder the ability of the IDS sensor to send bi-directional RST to reset TCP sessions created by the offending host. In the case of a hardware failure on the AppSafe, BLN2 can be wired directly to the Alteon with no configuration changes.*

The configuration of the AppSafe has not been included as it is out of the scope of this presentation. For further information, please refer to <http://www.toplayer.com>.

This implementation is very safe as intruders are not able to connect to a mirrored port. In addition, the network interface cards (NICs) that are connected to these mirror port are in promiscuous mode, making them operate in stealth mode. The network sensors are physically locked with the rest of the equipment, and can only be accessed via KVM console, or via SSH-2 with ACL access.

## 2.6 Parameter Firewall (Primary)

This Firewall pair protects **Zone III** (Service Network), **Zone IV** (GIAC's Internal network) and **Zone V** (Secured Network). These firewalls are installed on Sun Enterprise 450 and have four network interface cards (NIC).

NIC I	Connected to External Network
NIC II	Connected to Internal Network
NIC III	Connected to Demilitarized Network
NIC IV	Connected to Management Network

The Solaris platforms have been bastion using the method published by Lance Spitzner, which can be found at <http://www.enteract.com/~lspitz/armoring.html> entitled "Armoring Solaris". GIAC Enterprise is currently using Checkpoint version 4.1 with SP4. Aware of the many exploits of Checkpoint, the network engineers keep a close watch on known vulnerabilities at the following sites:

<http://www.phoneboy.com>  
<http://www.checkpoint.com>  
<http://www.iss.net>  
<http://www.incidents.org>  
<http://search.securepoint.com/>

### 2.6.1 Implementation of CheckPoint FW-1

Using the fundamental concepts provided by Lance Spitzner at

<http://www.enteract.com/~lspitz/rules.html>, GIAC Enterprise has implemented a good rulebase set. Diagram below is the rulebase implemented on the parameter firewall.

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

File Edit View Manage Policy Window Help

Security Policy - GIAC - Primary Address Translation - GIAC - Primary

1	Authorized_FW_Mgmt	GIAC_FW	FireWall/ ICMP-ALL SSH	accept	Long	Gateways	Any	Allow authorized firewall
2	Any	GIAC_FW	Any	drop	Long	Gateways	Any	Drop all access to Firewall
3	Any	GIAC_webservers	http_grp	accept	Long	Gateways	Any	Web services
4	Any	GIAC_FTPserver	FTP-group	accept	Long	Gateways	Any	FTP services
5	Any	GIAC_Mail_Server	smtp	accept	Long	Gateways	Any	Mail Services
6	All_Internal_Networks	DNS-External	dns	accept	Long	Gateways	Any	Allow non internal host to
7	All_Internal_Networks	GIAC_ServiceNetwork	SSH	accept	Long	Gateways	Any	Allow SSH into Service Ne from Internal network.
8	GIAC_ServiceNetwork	Any	SSH FTP-group smtp https	accept	Long	Gateways	Any	Allowed outgoing services Network.
9	All_Internal_Networks	Any	Unauth_out	drop	Alert	Gateways	Any	drop all unauthorized servi
10	All_Internal_Networks	GIAC_ServiceNetwork	Any	accept	Long	Gateways	Any	Allow internal traffic out.
11	GIAC_ServiceNetwork	Any	Any	drop	Long	Gateways	Any	Disallow traffic from Servi Internal network.
12	Any	Any	ident NBT	drop	Long	Gateways	Any	Drop and don't log these tr
13	Any	Any	Any	drop	Long	Gateways	Any	Cleanup Rule

The table below explains the rulebase in the previous page.

Rule #	Definition
1	<p><b>Admin Access:</b></p> <p>Admin access is highly utilized for maintenance and troubleshooting. In addition, having this rule at the very top will avoid accidentally locking out management to the firewall due to another rule. For example, if we were to toggle rule 1 and 2 (below), we would have locked ourselves out of the firewall.</p>
2	<p><b>Lockdown:</b></p> <p>This rule prevents anyone from gaining access to the firewall, except for the authorized firewall administrator. All unauthorized access will be logged.</p>
3, 4, 5	<p><b>Application Access:</b></p> <p>Each of the application servers are specifically defined. HTTP, FTP and SMTP are allowed into the service network. By defining each server, it increases the performance of the rule match.</p>
6	<p><b>DNS Services:</b></p> <p>This rule has dual intent. First, it allows external queries to the DNS servers on the Service Network. Second, it prevents internal users from using the external DNS. Internal users should be using Internal DNS servers for name resolution.</p>
7	<p><b>SSH access:</b></p> <p>This rule will allow remote administration using the SSH protocol for the application servers in the service network.</p> <p><i>Note: SSH has been disabled on all SSH servers due to known exploits. There is the possibility of tightening this rule by specifying specific hosts. Assumption is made that logging is being watched tightly, and abnormal activities can be detected easily.</i></p>
8	<p><b>Outbound Traffic for Service Network:</b></p> <p>This rule controls what is being allowed out of the Service Network.</p>
9	<p><b>Drop well-known malicious activities:</b></p> <p>This rule blocks many of the well-known malicious activities from leaving the internal network. Alert is turned on to notify us of any internal host attempting to use these malicious ports, which will enable us to identify and quarantine the offending host.</p>

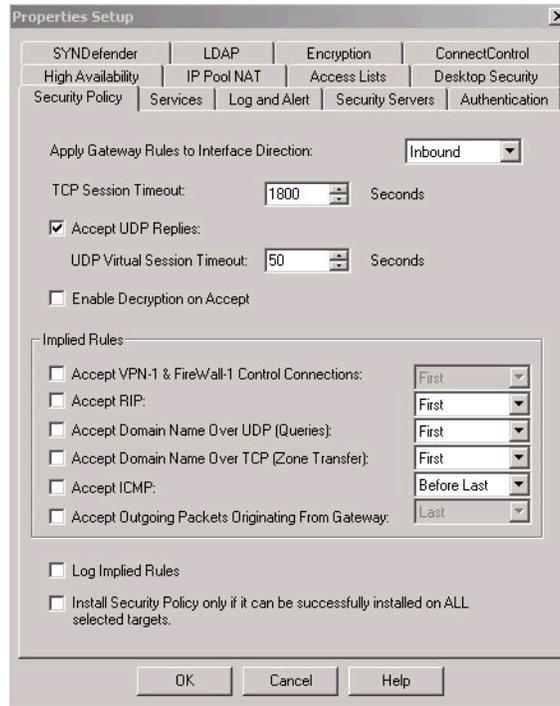
10	<p><b>Outbound Traffic:</b></p> <p>This rule allows internal hosts to connect out anywhere except for the Service Network. We do not want the internal network to have access to the service network, and vice versa. Otherwise, it defeats our purpose in separating the two networks in the first place.</p>
Rule #	Definition
11	<p><b>Service Network to Internet Network:</b></p> <p>The net effect of this rule is to disallow hosts from the service network to reach the internal network. Even though the rule explicitly drops traffic going to “any” destination, preceding rules have allowed the necessary defined traffic.</p>
12	<p><b>Cleanup logging</b></p> <p>This rule drops, and disables logging for “NetBIOS” and “Ident”, which will make the log easier to read.</p>
13	<p><b>Explicit Deny:</b></p> <p>This is the explicit deny rule, and should be the last rule defined in the rulebase. As the name implies, this rule will drop the packet if it does not match any other rules defined above this rule. The firewall tries to match the rule from top to bottom. Therefore, to improve performance, list the most frequently used rule at the top.</p>

*Note: Some of the services are bundled into a group. For example, the “HTTP\_grp” includes HTTP (80), and HTTPS (443).*

### **Other Firewall configurations**

Default implied rules are unchecked as shown below:

© SANS Institute 2000 - 2002



SYNDefender is also configured on the firewall to prevent SYN attacks, as demonstrated by [Daniel S. Martin](#) on Keith Wilcox's GCFW practical.

## 2.8 Summary:

The firewall rulebase needs to be tweaked as the need of the employees change. In addition, new exploits are discovered daily, and a change in the firewall rulebase can be used to block some of these exploits.

## 2.9 Virtual Private Network

### 2.9.1 Overview

GIAC installed Nortel's Contivity 4600 to provide **Extranet VPN** to partners, **and remote access VPN** for "roaming" corporate employees. The following definition was taken from "TCP/IP for Firewalls", a course material for the GIFW Track offered by SANS.

#### "Extranet VPN

Provides a connection between two sites where full access to the other's resources is not required (or desired). An example might be communication between two business partners, where we want incoming access to some of our systems but not all."

#### "Remote Access VPN

Provides access to a corporate network from a "roaming" user, such as a user in a hotel room with a laptop."

Ingress VPN connection will be forwarded to the External Alteon, and redirected to the Contivity

Server. To further secure the VPN connection, the Alteon has been setup to only forward protocol 50 and port 500 traffics. All other services destined for the VPN server will be redirected to a “black hole”, which just discards the traffic.

### 2.9.2 VPN server configuration

Basically, the VPN server at GIAC will provide the encrypted tunnel between remote host and the security gateway, and a LDAP or RADIUS server will be used to authenticate the remote user for network access using MS-CHAP.



From the screen capture above, we can see the Contivity server allows either Pre-Shared Key or RSA Digital Signature for the Internet Security Association and Key Management Protocol (ISAKMP) Security Association communication channel. The selected encryption options for Security Association (SA) are ESP –Triple DES with MD5 Integrity, and ESP – 56bit DES with MD5 Integrity, which uses protocol 50. If GIAC wants to enable AH encryption for legacy VPN clients, they will have to redirect protocol 51 on the External Alteon.

### 2.9.3 Step-by-step VPN client setup

The setup of Nortel’s Extranet VPN client is straightforward. The client software is stored on an FTP server for remote download. A temporary credential and password is created when the

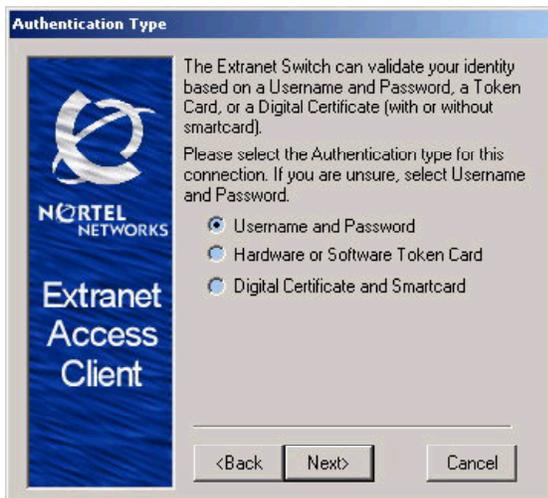
software is needed. Once the software is downloaded, just double click on the executable to install the software. After the installation, double click on “extranet.exe”, and see the setup wizard below:

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

1. Enter your profile with an identifiable description.



2. We use RAS to authenticate our session, so select the username and password option.



3. Here enter the GIAC's domain userid and password.



**User Identification**

You will need a user name and password (assigned by the Network Administrator) to connect to the remote network.

Enter your User Name:  
jdoe

Enter your Password:  
XXXXXXXXXX

Save the Password

<Back Next> Cancel

4. The Group ID and password are assigned by the VPN administrator.



**Group Authentication Information**

Besides a User name and Password, did your Network Administrator give you a Group ID and Group Password? If you are unsure, select No.

Yes, I have a Group ID and Group Password.

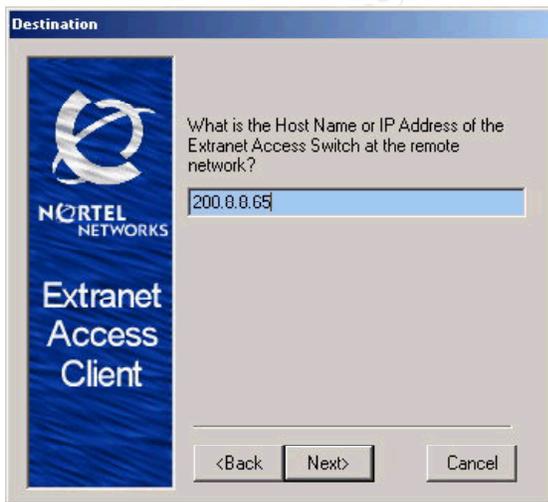
No, I do not have a Group ID and Group Password.

Enter your Group ID:  
giacvpn

Enter your Group Password:  
XXXXXXXXXX

<Back Next> Cancel

5. Enter the IP address of the VPN server that will be authenticating this session.



**Destination**

What is the Host Name or IP Address of the Extranet Access Switch at the remote network?

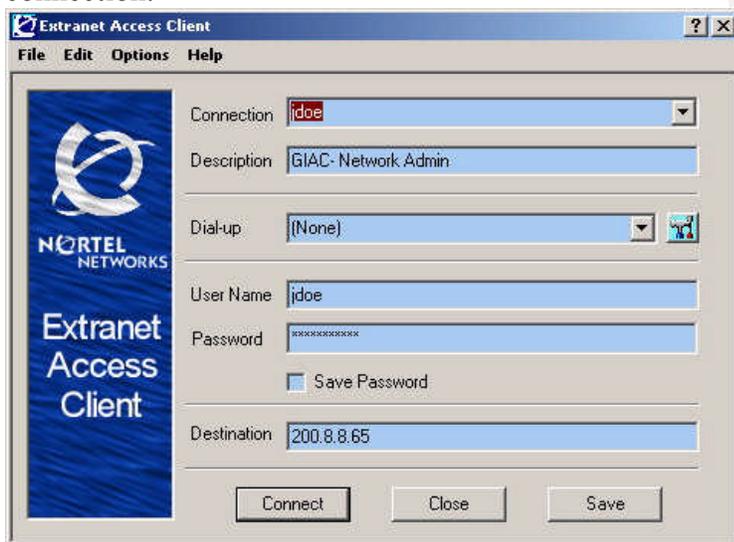
200.8.8.65

<Back Next> Cancel

6. The wizard step is completed.



The next time a connection needs to be made, a single click on connect will establish the VPN connection.



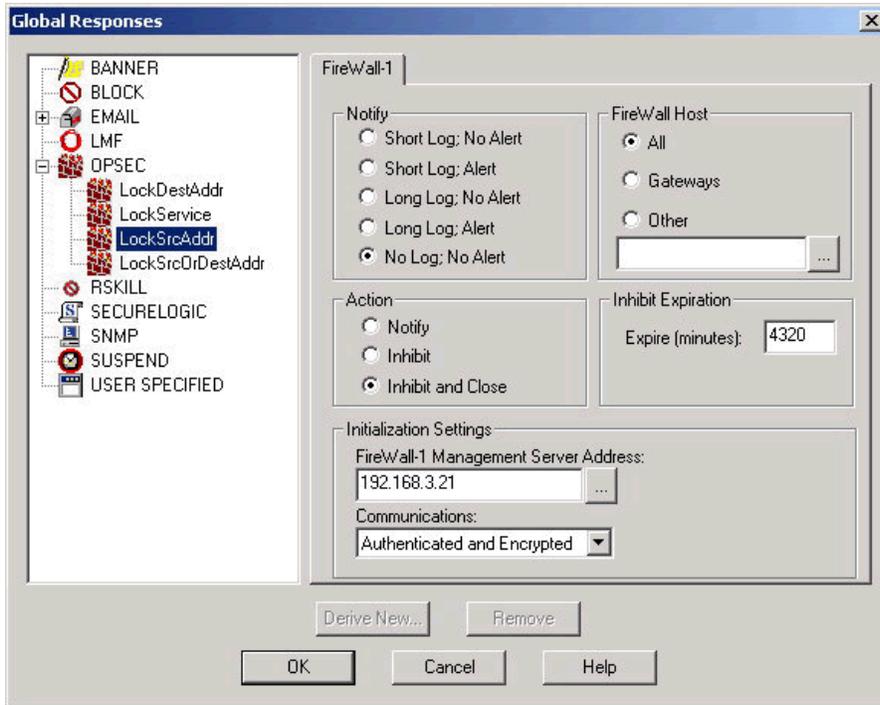
### 2.9.4 Split Tunneling

Split Tunneling has been disabled to enhance the security of the remote client. For example, the remote client had a Trojan installed on the PC, and it has established a backdoor. The remote client VPN's into the network, and establishes the VPN tunnel. With Split Tunneling turned off, the existing backdoor connection will now be re-routed via the tunnel. When the Trojan tries to connect to the master server via a known Trojan port, it will get logged and dropped on the firewall.

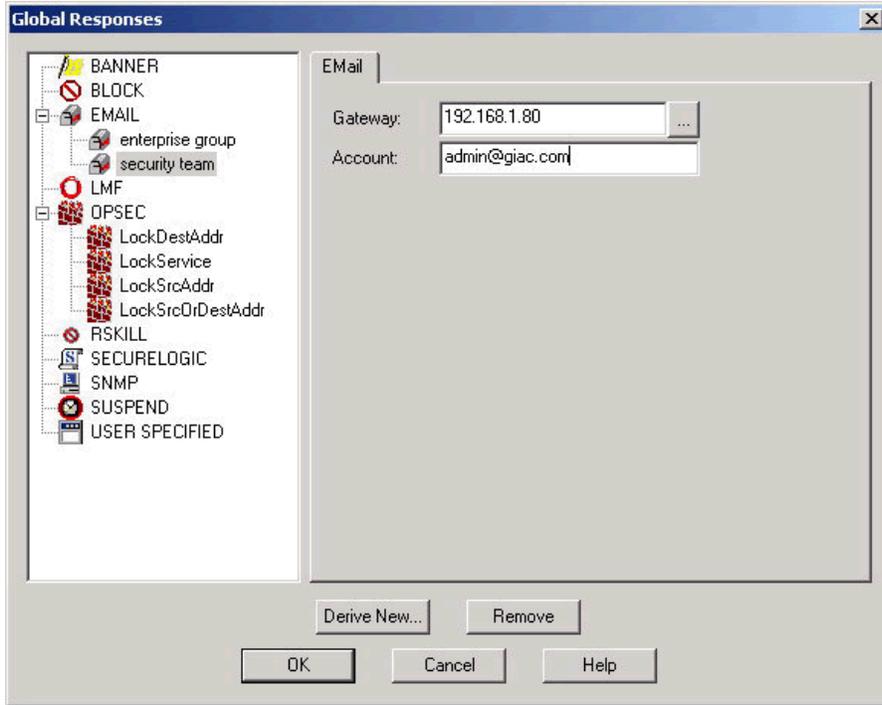
*Note: Remote VPN connections are assigned to a different subnet.*

### 2.10 Other security enhancements

Intrusion Detection Systems by RealSecure has been configured to detect malicious signatures, and to respond by sending bi-directional TCP reset. RealSecure will also send an OPSEC command to the firewall management to block the offending host.



The screen shot above shows the OPSEC configuration to lock offending source address as applied to specified signatures. When the signature is triggered, RealSecure's network sensor will issue the OPSEC command to block the offending host. An automated e-mail (illustrated below) is sent to the administrator of such event. Currently, the block is set for 4320 minutes (3 days).



### Assignment 3 – Audit Your Security Architecture (25 points)

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

1. Plan the audit. Describe the technical approach you recommend to assess the firewall. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Evaluate the audit. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

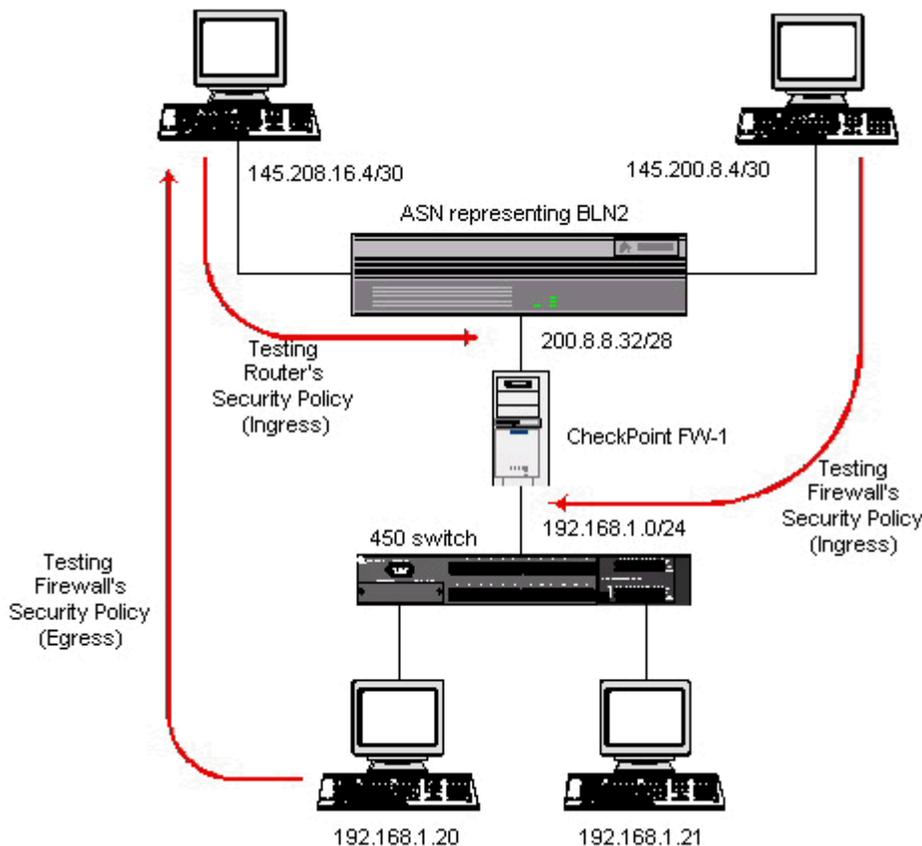
Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but you must annotate/explain the output.

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

## Assignment III - Audit Security Architecture

The technical staff at GIAC Enterprise regularly audits the network to make sure the security implementation works the way they are supposed to work. Without performing such audits, the true effects of any security implementation might not be known until it is too late.

### 3.1 Planning the Audit



One of the primary reasons why GIAC has an isolated audit network on the External network is for auditing. The audit network allows the network engineer to simulate a network attack in a controlled environment. To view the net effect of the implemented rulebase, we will compare the signatures detected between the external IDS sensors with the internal IDS sensors. In addition, we can run two sessions of tcpdump of the Linux workstation in verbose mode, using the known source IP.

#### 3.1.1 Management Approval

Anytime an audit is performed, there are associated risks involved. Therefore, it is highly critical that management is informed of the audit in advance. For example, a potential high-profile

customer may be evaluating GIAC Enterprise as a supplier. If an audit was performed during that time, and somehow cause downtime, it could affect the outcome of the business transaction. Therefore, management approval is a **pre-requisite** before any audit can be performed.

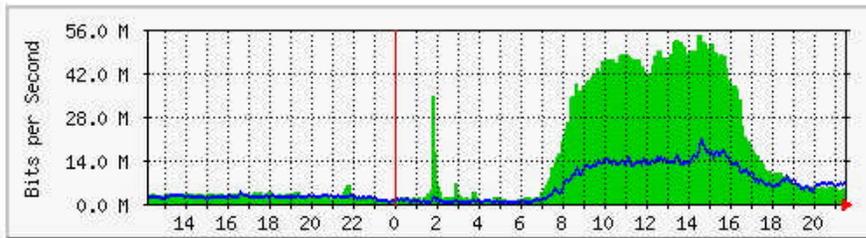
GIAC Enterprise has included audit procedures within the security policy. Such procedures are put in place to minimize confusion.

### **3.1.2 Defining the best time for an audit**

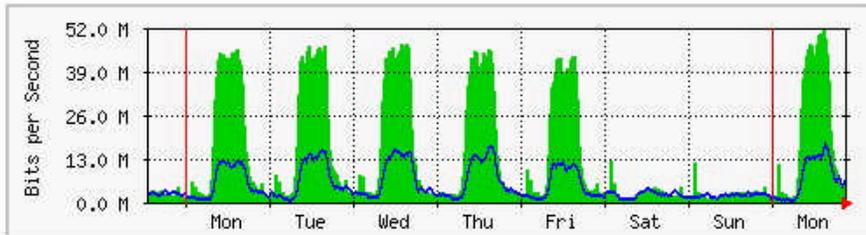
GIAC Enterprise receives the most traffic during the day, between 7am to 4pm, as most of their customers are based in the United States. Global customers are seen doing most business transaction between 4pm to 12am, and minimal transactions are seen on Sunday. Therefore, the best time to perform an audit is between 3am to 6am, or on Sunday.

Screen shot of weekly MRTG graphing to show traffic level.

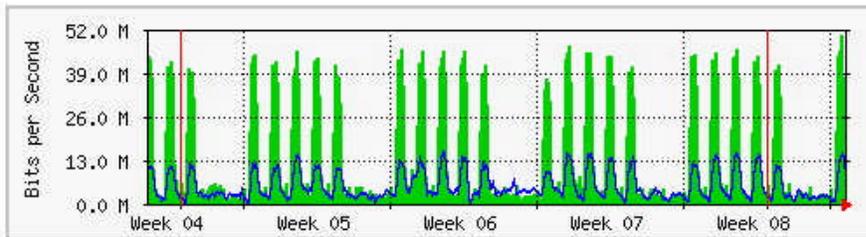
© SANS Institute 2000 - 2002, Author retains full rights.

**'Daily' Graph (5 Minute Average)**

Max In: 54.5 Mb/s (54.5%) Average In: 14.9 Mb/s (14.9%) Current In: 5441.9 kb/s (5.4%)  
 Max Out: 21.0 Mb/s (21.0%) Average Out: 5814.6 kb/s (5.8%) Current Out: 6606.8 kb/s (6.6%)

**'Weekly' Graph (30 Minute Average)**

Max In: 51.9 Mb/s (51.9%) Average In: 14.2 Mb/s (14.2%) Current In: 5441.1 kb/s (5.4%)  
 Max Out: 18.1 Mb/s (18.1%) Average Out: 5456.0 kb/s (5.5%) Current Out: 6600.1 kb/s (6.6%)

**'Monthly' Graph (2 Hour Average)**

Max In: 50.8 Mb/s (50.8%) Average In: 13.8 Mb/s (13.8%) Current In: 11.3 Mb/s (11.3%)  
 Max Out: 16.1 Mb/s (16.1%) Average Out: 5578.9 kb/s (5.6%) Current Out: 7304.0 kb/s (7.3%)

**3.1.3 Defining the cost of an audit****Personnel/Man Power**

There are four security engineers at GIAC Enterprise. Each Engineer has a specialized focus, such as firewall/Alteon, IDS/Appsafe, border router, and security analysis. However, all engineers are cross-trained for backup purposes. Therefore, when an audit is performed, it is necessary for all four engineers to be present.

**Equipment**

The AppSafe was purchased for IDS load balancing. Currently, the AppSafe has available ports that are not used for IDS load balancing. We are using one port to assist us in our audit process, however, this port will be released if it is needed for IDS load balancing. For budgetary purpose, we have decided to include the port cost.

The workstations used in the audit network are older computers obtained when employees upgraded their workstation. Most of these workstations have been depreciated to half of its initial cost. An average cost of \$500 per workstation has been allocated.

### Level of Effort

The audit network, AppSafe, Linux workstation, IDS sensors are already in place. Most of the prep work for the audit can be performed during the day, as the audit network is isolated from the rest of GIAC's internal network. Most time will be spent on researching the vulnerabilities, and the security risk associated to those vulnerabilities.

### Summary of the cost of Audit

	Unit	Cost	Total
Personnel (Average of three hours per audit)	4	30/hr	360
AppSafe (internal and external)	2	1650/port	3300
Linux workstation	1	500	500
Audit workstations	3	500	1500
Total Cost Per Audit			5660

*Note: Personnel are the only reoccurring cost for the audit. Therefore, the average cost of re-occurring audits after the initial setup should only be about \$360.*

### 3.1.4 Defining risk and consideration

No matter how prepared or controlled the environment of an audit, there is always the "X" factor, which could cause downtime to the network. We can only minimize these risks through careful planning. If something is too risky, the entire audit work should be performed in the isolated audit network. The network engineers can load the current rulebase on a [PDS2000](#), by Intrusion Inc. The PDS2000 is a Firewall Appliance using CheckPoint's FW-1. The cost of these appliances is minimal, and will simulate the current firewall environment.

### 3.2 Audit Execution

There are many tools freely available on the Internet, which can be used to audit the firewall's security policy. Some of these tools go beyond the protocol level, and are designed to attack application design flaws. Since the requirement of this assignment is to audit the primary firewall, we will use basic tools that will simply tell us if the firewall security policy is working the way it is supposed to be. Basically, we will test the rulebase from top to bottom. Details on tools and methodology will be defined in each of the subsections.

#### Auditing admin access

*Tool: checkpoint fw-1 Policy Manager*

*Methodology: Using a laptop with Policy Manager installed, we switch between a known management client IP and a non-management IP.*

Action:

For the purpose of this practical, I connected the laptop directly to the firewall. Using a randomly selected IP address of 200.8.8.83, I connected to the firewall interface of 200.8.8.81. We then executed the policy editor, and we see the failed attempts on the FW-1 log viewer as below.



Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	Us
log	drop	FWM1_mgmt	200.8.8.83	200.8.8.81	tcp	2	1059	

*Note: The illustration above was used to demonstrate the rejection of a randomly selected client to authenticate to the firewall.*

As you can see from the screen capture above, Rule #2 successfully stopped an unauthorized client from authenticating to the firewall modules.

#### Auditing Application Access

*Tools: Basic telnet, Linux server (optional)*

*Methodology: Nothing fancy, just telnet directly to the target server via the service default port number.*

Action:

The services we want to audit here are http, ftp and smtp. Using the basic telnet command, we will telnet to port 80, 21 and 25. Using tcpdump on the firewall, we look at eth0 (internal of firewall), to see if the firewall is allowing the initial request traffic through.

We setup a laptop connecting it to interface 1/2/1 of the router, and use the IP of 200.8.8.6/30. We then setup a server behind the firewall in the subnet of 200.8.8.80/28, listening on port 80, 21 and 25. The setup of this server is optional, as we only need to view the "request" traffic passing

through eth1 and forwarding it to eth0. If the session is allowed by the firewall, we should see traffic on eth0 interfaces. Otherwise, the traffic most probably got blocked on the firewall.

From the command prompt of the laptop:

```
telnet 200.8.8.85 80
```

The command above sends a telnet command through port 80 to server 200.8.8.85.

We should see the following on interface eth0:

```
Using device /dev/eth0 (promiscuous mode)
145.200.8.6 -> 200.8.8.85 HTTP C port=65097
145.200.8.6 -> 200.8.8.85 HTTP C port=65080
200.8.8.85 -> 145.200.8.6 HTTP R port=65080
145.200.8.6 -> 200.8.8.85 HTTP C port=65080
```

This tells us that port 80 traffic is allowed through the firewall. We do the same for port 21 and 25, and achieve the same result.

### Auditing the Drop well-known malicious activities

*Tool: nmapnt*

*Methodology: nmapnt was ported over from the Unix flavored of nmap, and is one of the most highly used scanning tool. Here we use nmap for a broad sweep of 65535 available ports.*

**Action:**

By default, via the rules that we have created, we have specifically defined the type of traffic we would allow into our network. However, we also want to be aware of any attacks targeted on our network. This rule is in place specifically for logging and alert. We identify these malicious activities, so we can take corrective action if the offender is persistent. Using Superscan by Foundstone Inc., we scan a server connected behind the firewall.

For the audit, we set up a laptop (running windows 2000 professional) outside of the firewall. To perform a port scan, we downloaded nmapnt from <http://www.eeye.com>, and installed it on the laptop. We will use nmapnt to do an intrusive port scan on a host on the internal network. Before executing the port scan, we activate two sessions of tcpdump on the Linux workstation, one monitoring the session outside of the firewall (External AppSafe), and the other inside of the firewall (Internal AppSafe).

*Note: For this audit, we use the IP subnet from the service network.*

We execute the following nmapnt command:

```
D:\nmapnt\nmapnt -v -sS 200.8.8.85
```

The “-v” option is to put nmapnt in verbose mode. To see more details, a “-vv” option is available. “-sS” instructs nmapnt to do a TCP SYN stealth port scan.

As soon as nmapnt starts the port scan, tcpdump on the external interface started spewing a

bunch of activities, while the internal interface detects nothing. Below is a screen shot of the two SSH sessions on the Linux workstation. This confirms the firewall rulebase is doing its job. In addition, when we look at the firewall log viewer, we see the similar dropped packets.

```

Linux - External Interface - SecureCRT
File Edit View Options Transfer Script Window Help
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.920: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.920: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.331: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.331: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.2023: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.2023: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.935: S 472253014:472253014(0) win 1024
17:13:45.588661 P 145.200.8.6.61091 > 200.8.8.85.935: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.5680: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.5680: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.889: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.889: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.762: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.762: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.702: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.702: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.sftp: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.569: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.sftp: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.569: S 472253014:472253014(0) win 1024

Ready ssh2: AES-128 1, 1 21 Rows, 110 C

Linux - Internal Interface - SecureCRT
File Edit View Options Transfer Script Window Help
[root@fwsniffer /root]# tcpdump -i eth1 -p dst host 200.8.8.85
Kernel filter, protocol ALL, TURBO mode (575 frames), datagram packet socket
tcpdump: listening on eth1

```

First, let's describe the tcpdump command line.

-i eth(x) = instructs tcpdump to listen on eth(x) interface  
 -p = Promiscuous mode  
 dst host x.x.x.x = filter to listen to IP x.x.x.x

### Reading tcpdump's Output

```

17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.sftp: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.569: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.sftp: S 472253014:472253014(0) win 1024
17:13:45.598661 P 145.200.8.6.61091 > 200.8.8.85.569: S 472253014:472253014(0) win 1024

Ready ssh2: AES-128 1, 1 21 Rows, 110 C

```

The green shaded area represents the timestamp when the event occurred. The light red area represents the source IP and source port being used. In our test, the source is 145.200.8.6, and it uses the source port of 61091. The next shade over (blue) represents the destination IP, the port target. The yellow area represents the TCP flags. In this case, they are SYN packets. Other possible options include **P**SH, **R**ST and **F**IN. The purple area is the random sequence number generated by the source, while the orange area is the ending sequence number. The ending sequence # is usually the beginning sequence number plus the data bytes. The data bytes are defined in the white area, and the gray area represents the TCP buffer size.

Below is the log from FW-1's log viewer showing ports being dropped.

200.8.8.34	 log	 drop	Sockts_de_troi-tcp2	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	47557	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	47806	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	47808	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	Back_O_2K-tcp	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	stacheldraht-handler	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	sunrpc	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	nfsd	145.200.8.6	200.8.8.85
200.8.8.34	 log	 drop	microsoft-ds-tcp	145.200.8.6	200.8.8.85

From the audit examples above, we have seen the use of tcpdump and the Log viewer to audit the traffic flow into our network. Using the same procedure, we can finish up the auditing of the rulebase of the firewall.

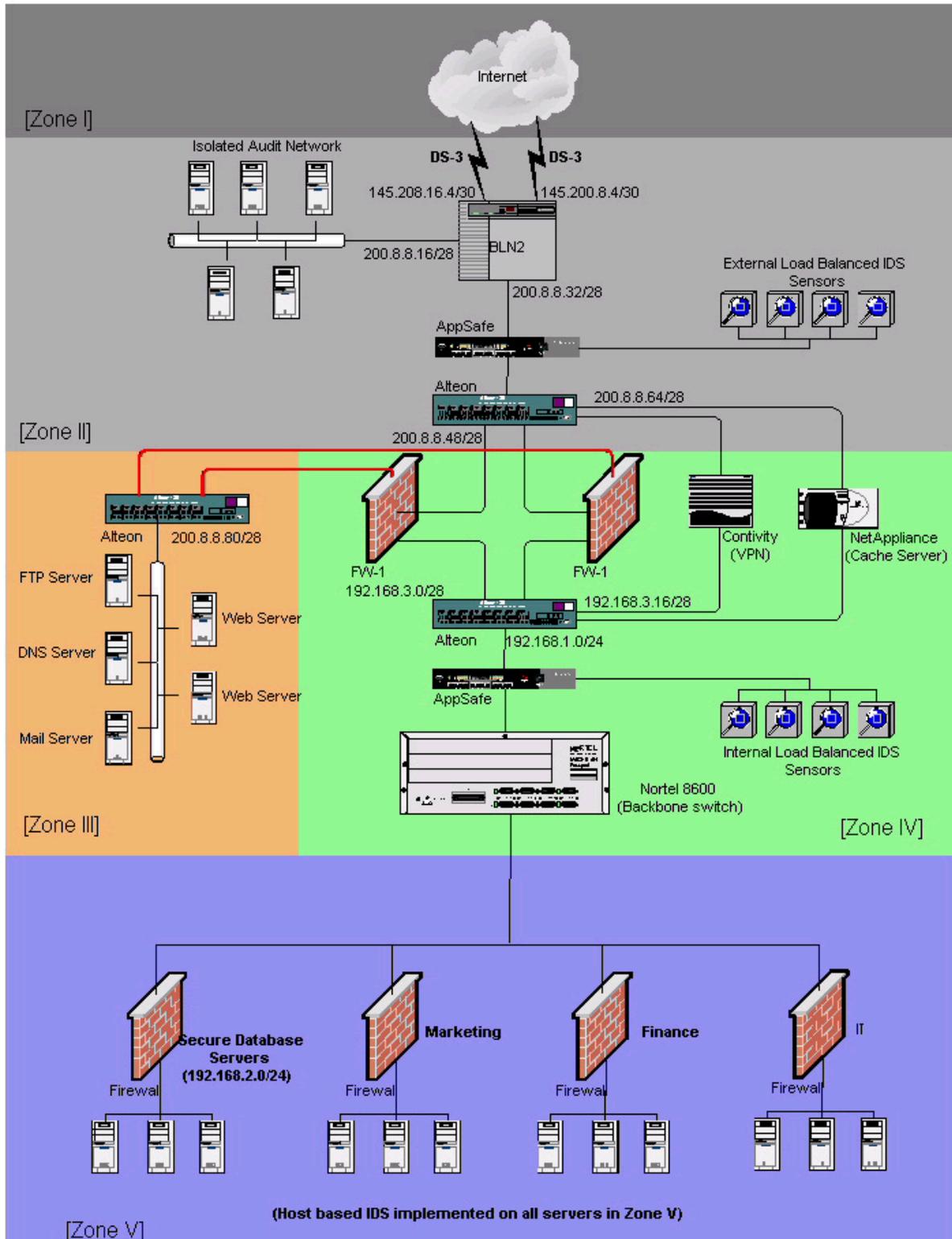
### 3.3 Audit Evaluations and Conclusion

From the audit, we saw the firewall dropping traffic from the default NetBIOS ports. We also saw the firewall dropping port 445, which is the port used for active directory. Knowing GIAC Enterprise does not use active directory, we decided to add another filter to block port 445 on the ingress port of the router.

Also during the audit, we discovered the needs of departmental security varied greatly. Some needed more security, while some need more access. To provide more granular access control, we felt it was necessary to implement departmental level firewall. In addition, the firewall implemented at this level will have a firewall different from the primary firewall. This will prevent “zero day” exploits targeted at vendor specific firewall.

Below is the suggested architecture change.

**GIAC Enterprise Network Architecture**



### Assignment 4 – Design Under Fire (25 points)

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

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

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

Your attack information should be detailed - include the specifics of how the attack would be carried out. Do not simply say "I would exploit the vulnerability described in Vendor Security Bulletin XXX". What commands would you use to carry out the attack? Are exploit tools or scripts available on the Internet? What additional steps would you need to take prior to conducting the attack (reconnaissance, determining internal network layout, determining valid account name.)? Would any of your methods be noticed (log files, IDS.)? What "stealth" techniques could you employ to avoid detection? What countermeasures would help prevent your attack from succeeding?

If it is possible to carry out the attack on a test system, include screen shots, log files, etc. as appropriate to illustrate your methods.

In designing your attacks, keep the following in mind:

- The attack should be **realistic**. The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.
- The attack should be **reasonable**. The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should not assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)

- You **must** supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

The attack does not necessarily have to succeed (though a successful attack is often the more interesting approach). If, given the perimeter and network configuration you have described above, the attack would fail you can describe this result as well.

© SANS Institute 2000 - 2002, Author retains full rights

## Assignment IV - Design Under Fire

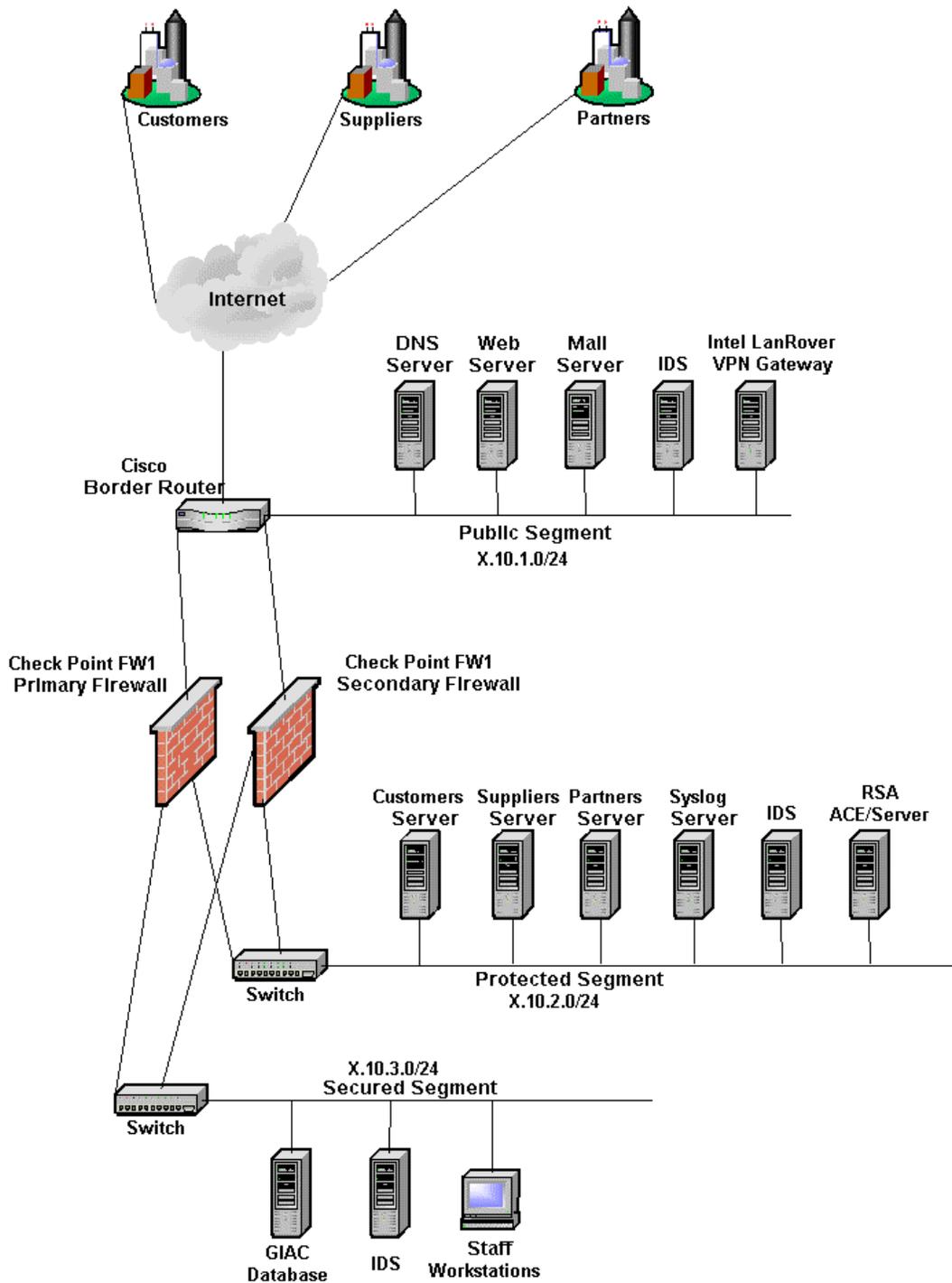
### 4.1 Introduction

The practical postings at <http://www.giac.org/GCFW.php> were well written. Bear in mind, all practical were written by currently certified GCFW! There might have been presentation flaws, however, I believe these are security conscious people who keep up with patches, hot fixes, and go the extra distance to ensure the security of their network.

Now that I have made peace, let's get on with the attack. I will be auditing and reviewing Tan Meu Huat's GCFW Practical Assignment, which is available at [http://www.giac.org/practical/MeauHuat\\_Tan\\_GCFW.doc](http://www.giac.org/practical/MeauHuat_Tan_GCFW.doc)

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

### GIAC Enterprises - Security Architecture



GIAC Enterprise Security Architecture by Tan Meau Huat

## 4.2 Overview Design Analysis

There were a few objects that caught my attention in Tan's Security Architecture.

- The Cisco router used as a firewall to protect the public segment
- Single level firewall used to protect internal network
- Single IDS on mirror port (Are the mirror port expandable?)
- Routable internal IP subnets?

Cisco's IOS has been exploited many times. Just a simple search on <http://www.google.com>, I found the following sites describing Cisco's IOS exploits.

- <http://www.netsys.com/library/hackers/hackers.2001-05-28.txt>
- <http://www.securiteam.com/securitynews/6U00U0036A.html>
- <http://www.securiteam.com/securitynews/6C00A2036Q.html>
- <http://www.cotse.com/exploits/cisco/>
- <http://packetstorm.decepticons.org/cisco/>

For example, the Cisco 3640 using IOS 12.1 in Tan's security architecture is susceptible to the ARP Table overwrite vulnerability, as mentioned by SecuriTeam.com at <http://www.securiteam.com/securitynews/6C00A2036Q.html>.

Tan also used a single pair of firewalls to protect his internal network. Even though he separated the secured network from the protected network, a single penetration on the firewall will allow complete access to the internal network.

The use of IDS in the three different segments is a good proposition, as it allows the auditing function of the firewall's rulebase. However, Tan suggested using the mirror port on the switch for the IDS. From my experience in dealing with mirror port on switches, it has very limited capabilities. I have two concerns on the way IDS is setup here.

1. Is spanning port looks at unidirectional or bi-directional traffic? If setup is unidirectional, the IDS will not see the two-way conversation.
2. This point concerns the internal IDS. If the spanning port was mirroring bi-directional traffic, it can overload if internal traffic is high. Assuming it is a 100Mbps circuit, the mirror port could potentially see up more than 100 Mbps of traffic (ingress plus egress), which could cause packet drop.

Also, Tan did not mention the use of private addresses on the internal network. Looking at the subnet scheme of the security architecture, Tan seems to be using Internet routable IP address on the internal subnets. Therefore, if the firewall was penetrable, the secured network will be immediately accessible to the Internet.

Since the focus of this section is on the primary firewall, we will ignore possible exploits from other angles of the security architecture.

### 4.3 CheckPoint Vulnerability #1

For someone to use an exploit on a firewall, they will first have to figure out what type of firewall is being used. As described by Securiteam.com at <http://www.securiteam.com/securityreviews/2SUQSQ0RPM.html>, CheckPoint FW-1 by default responds to ports 256, 257, and 258. Using tools such as **nmap**, an intruder could easily identify the type of firewall being used. The recommendation is to block the ports from all sources except for a few trusted hosts.

#### 4.3.1 CheckPoint Vulnerability #2

The infamous IP Fragmentation as discovered by Lance Spitzner. This vulnerability allows a remote attacker to cause a denial of service by sending a large number of malformed fragmented IP packets<sup>1</sup>.

Fragmentation happens when the size of the packet is larger than the local maximum transmission unit (MTU) size. The packet is chopped into multiple segments (fragments) so that it can fit into the predefined MTU size. As the packets travel across to the destination, they do not arrive in chronological order, which requires a mechanism to re-assemble the packets. Lance speculates CheckPoint FW-1 actually tries to re-assemble the fragmented packets before inspecting them. A virtual defragmentation log on the firewall is used to keep up with the re-assembly of these IP fragmentations. As the stream of fragmentation increases, the logging process takes up more system resources until a point where all resources are used up, causing the system to lockup.

I use jolt2.c (as mentioned by Lance) against Tan's firewall. It was effortless to find a copy of jolt2.c. I did a search at <http://www.google.com> using the keyword "jolt2". Google returned 643 matches in 0.15 seconds. However, it was more difficult finding the installation instructions on jolt2.c. After digging thru some online archives, I managed to put the pieces of the puzzle together. Referring to <http://archives.neohapsis.com/archives/ntbugtraq/2000-q2/0196.html>, I copied the code for jolt2.c to an ASCII text file on a Linux workstation, named "honeypot". I then proceeded to compile it using the command "`gcc jolt2.c`", and the output generated a default file called "`a.out`", which I renamed to "`jolt2`".

*Note: The test below was performed on a test network to simulate Tan's network. The firewall used in this test is equivalent to the firewall he presented, which is CheckPoint Firewall-1 with SP3.*

To make sure the code compiled correctly, I tested jolt2 on an un-patched NT server.

<sup>1</sup> <http://eve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0482>

```
./jolt2 200.8.8.86
```

The command above sends fragmented packets to host 200.8.8.86. The initial test did not yield the results I expected. Tcpcdump shows honeypot “ARP”ing for 200.8.8.86. I did a ping to 200.8.8.86 to cache its ARP, and restarted jolt2. Immediately, the CPU utilization of the targeted host jumped to 100%, and crippled it. Running tcpcdump on the Linux workstation shows the fragmented packets being sent to the host.

```
20:55:02.578835 honeypot.giac.com > 200.8.8.86: (frag 1109:9@65520)
```

I executed jolt2 again, but this time targeting the firewall’s interface of 200.8.8.33.

```
./jolt2 200.8.8.33
```

tcpcdump shows the fragmented packets being sent to the firewall.

```
22:07:53.188835 honeypot.giac.com > 200.8.8.33: (frag 1109:9@65520)
```

Using the “top” command, Tan’s firewall did not show any adverse effect to jolt2.

```
9:40pm up 3 days, 22:59, 5 users, load average: 0.06, 0.02, 0.00
68 processes: 66 sleeping, 2 running, 0 zombie, 0 stopped
CPU states: 1.3% user, 0.7% system, 0.0% nice, 97.8% idle
Mem: 126704K av, 120224K used, 6480K free, 0K shrd, 5624K buff
Swap: 257000K av, 26452K used, 230548K free

PID USER PRI NI SIZE RSS SHARE STAT %CPU %MEM TIME COMMAND
```

Doing some research on the Internet revealed Firewall-1 SP2 addressed this vulnerability (<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=solution&id=1312>).

*Note: The description above referenced SANS at [http://rr.sans.org/firewall/frag\\_attacks.php](http://rr.sans.org/firewall/frag_attacks.php) and Lance Spitzer's website at <http://www.enteract.com/~lspitz/fwtable.html>*

### 4.3.2 CheckPoint Vulnerability #3

Dameon D. Welsh posted a security alert for CheckPoint FW-1 at <http://www.phoneboy.com/homepage.html#Alerts>, which allows RDP service(UDP Port 259) through the firewall by default.

CheckPoint uses a proprietary Reliable Data Protocol (RDP) on top of the User Datagram Protocol (UDP) to establish encrypted sessions. Firewall-1 management rules allow arbitrary either bound RDP connections to traverse the firewall. Only the destination port 259 and the RDP command are verified by Firewall-1<sup>2</sup>.

Using a packet-crafting tool, we can insert a fake RDP header to the normal UDP traffic using port 259 to any remote host on either side of the firewall. Trojan horse software could use this vulnerability to pass thru the firewall and not be detected. Tan states that he was running CheckPoint Firewall-1 on a Nokia platform with SP3, which was susceptible to this exploit. CheckPoint has since released a hotfix to patch this exploit.

Workaround as suggested at <http://www.inside.security.de> before the hotfix was available were:

- Comment line 2646 of base.def (accept\_fw1\_rdp;)
- Uncheck all the implied rules and customize the rules for management connections
- Block UDP port 259 on the border router

### **4.4 Denial of Service Attack**

Recently, GIAC Enterprise was a victim of a denial of service (DOS) attack. The attack was suspected coming from 50 compromised cable/DSL systems. Looking at the sniffer trace, network engineers found out it was a TCP SYN attack. The remote attacker used the compromised system to generate multiple SYN sessions with the destination server using forged source IP addresses. The server replies with a SYN/ACK, and waits for the ACK to complete the three-way handshake. Because the source IP is forged, the server never gets an ACK reply. Each of these incomplete three-way handshakes holds up a connection in the connection queue until the timer expires. With 50 high-speed cable/DSL connections, they can quickly generate numerous forged sources TCP SYN packets, causing the connection queue to fill up. When the connection queue is maximized, the server is unable to service the normal legit connection.

<sup>2</sup> [http://www.inside-security.de/fw1\\_rdp.html](http://www.inside-security.de/fw1_rdp.html)

#### 4.4.1 Counter measure

There are a few methods to defend against SYN flood attack.

- Increasing the size of the connection queue
- Decrease the time-out handshake value to quicken the expiry time.
- Activate SYNDefender on Firewall-1

Increasing the size of the connection queue will desensitize the server from SYN Flood attacks. Hopefully, as the connection queue fills, the earlier connection queues will time out. Decreasing the time-out handshake will allow the server to clear the connection queue at a much faster rate. When the ACK is not seen after the predefined time, it will be released from the connection queue. CheckPoint Firewall-1 SYNDefender protects against the TCP SYN (requests for connection establishment) flood attacks by intercepting all SYN packets and mediating the connection attempts before they reach the operating system<sup>3</sup>.

*Note:*

*Activating SYNDefender on Firewall-1 could have adverse effect on certain type of applications that do not conform to the standard TCP three-way handshake.*

#### Attack on Internal web server

Knowing that GIAC's firewall is well protected by the firewall, we now try to attack the web servers via the default port 80. Port 80 traffic is almost always allowed through the firewall, and is usually not logged.

The first thing we want to do is determine the platform of the web server. We are hoping the web servers are unpatched NT OS, as there are abundance of vulnerabilities. Referring to SANS at <http://www.sans.org/top20.htm> we can see the IIS appears to be one of the most vulnerable web server.

To guess the platform of the webserver, we do a simple telnet via port 80. If we see the following results, we can then proceed with our attack.

```
giac# telnet 200.8.8.85 80
Trying 200.8.8.85...
Connected to 200.8.8.85
Escape character is '^]'.

```

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Wed, 13 Mar 2002 13:44:36 GMT
Content-Type: text/html

```

<sup>3</sup> <http://www.checkpoint.com/press/1996/synattack.html>

Content-Length: 87

```
<html><head><title>Error</title></head><body>The parameter is incorrect.  
</body  
></html>Connection closed by foreign host.
```

Using one of the most recent infectious worms named “Nimda”, we attempt to infect the server. Once infected, it will mass propagate the worm randomly, filling up the connection table, and thus causing a total denial of service. <http://www.incidents.org/react/nimda.pdf> has a detailed article on how the worm propagates itself.

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

## References

Mahalingam, Ragho. Nortel Networks™ Troubleshooting & Optimization. Osborne/McGraw Hill, 2001.

SANS Institute. Track 2 – Firewalls, Perimeter Protection, and Virtual Private Networks.

Stevens, W. Richard. TCP/IP Illustrated, Volume 1 The Protocols.

Nortel Networks. Bay Console Command (BCC) Supplement guide. Training material.

Martin S. Daniel. GIAC Certified Firewall Analyst Practical. March 2001.

Moe J. Alan. SANS GIAC Firewall and Perimeter Protection Practical Assignment.

Kelly M. Brian. GIAC Firewall and Perimeter Protection Curriculum Practical Assignment.

Spitzner, Lance. “Understanding The FW-1 State Table”. 29 November 2000. <http://www.enteract.com/~lspitz/fwtable.html>

Spitzner, Lance. “Building Your Firewall Rulebase”. 26 January 2000. <http://www.enteract.com/~lspitz/rules.html>

Spitzner, Lance. “Armoring Solaris”. 19 August 2000. <http://www.enteract.com/~lspitz/armoring.html>

Farrell, James. “IP Fragmentation Attacks on Checkpoint Firewalls”. 3 April 2001. [http://rr.sans.org/firewall/frag\\_attacks.php](http://rr.sans.org/firewall/frag_attacks.php)

Kargl, Frank, et al. “Protecting Web Servers from Distributed Denial of Service Attacks”. March 2001. <http://www10.org/cdrom/papers/409/>

Check Point Software Technologies. “Defining Strategies to Protect Against TCP SYN Denial of Service Attacks”. October 1996. <http://www.checkpoint.com/press/1996/synattack.html>

Secureroot computer security resources. “Firewall-1 DoS Attack”. <http://www.secureroot.com/security/advisories/9798443762.html>

## Other References

Nortel Networks. <http://www.nortelnetworks.com>

Top Layer Networks. <http://www.toplayer.com>

Cisco Systems. <http://www.cisco.com>

Network Appliance, Inc. <http://www.netapp.com>

Internet Security Systems. <http://www.iss.net>

Internet Engineering Task Force. <http://www.ietf.org>

Carnegie Mellow Software Engineering Institute. <http://www.cert.org>

Church of the Swimming Elephant. <http://www.cotse.com>

SANS Institute. <http://www.sans.org>

The SANS Institute. <http://www.incidents.org>

Packet Storm. <http://packetstorm.widexs.nl>

Securi Team. <http://www.securiteam.com>

## Acknowledgment

I would like to thank everyone who provided guidance to help me complete this assignment.