# Global Information Assurance Certification Paper

## Copyright SANS Institute
## Author Retains Full Rights

# GIAC Certified Firewall Analyst (GCFW)
## Practical Assignment Version 1.8
**Craig L. Duerr**
December 12, 2002

# Table Of Contents

Assignment 1

# *Security Architecture for GIAC Enterprises*

GIAC Enterprises is a small e-commerce concern dedicated to providing quality fortune cookie fortunes to American dessert companies. Recently, management decided to expand its offerings to the emerging Chinese market by partnering with a Hong Kong firm.

Management's aggressive growth plan called for a more integrated workflow approach that would link all departmental systems to each other. They recognized the increased dependence on electronic workflows increases GIAC Enterprises' exposure to potential attacks, both internal and external.

Management was interested in a security solution that utilizes existing equipment where possible, existing IT expertise for maintenance and expansion, and free software and operating systems when security and performance are not at risk.

Among the IT staff are strong Linux administrators. Linux was already a strong part of the network, and new components using Linux have always been welcome.

## Connectivity

GIAC Enterprises has several different groups with specific connectivity requirements. The groups' requirements are detailed below.

### Customers
Customers need to access the WWW server for placing orders as well as order fulfillment. They need to access the Web server via an SSL connection for account creation, access, order submission and product delivery. They are restricted to http, https protocols access only. Credit cards and purchase orders are available payment options.

### Remote Teleworkers and Mobile Salespeople
GIAC offers a work-at-home program as an employee perk and cost savings measure. Sales personnel also work out of their home offices when not on the road. Remote access for these employees ranges from accessing email and placing orders to requiring full IT administrative access. One Internet service provider (ISP) was selected to best meet the needs of all mobile personnel. The ISP was selected for its nationwide local access availability.

Remote workers accessing the network via the *Secure Client* software and *VPN-1* virtual private network (VPN) are limited to server network access for *Lotus Notes*, internal DNS access for queries, ftp proxy access and http proxy access.

### GIAC International, LLC Hong Kong

GIAC's international partner, GIAC International, LLC, requires Gateway-to-Gateway VPN access to the accounting database as well as the production database.  Access is restricted to accounting and production servers during database replication hours only.  GIAC International business databases are replicated daily at 6am for two hours and again at 9pm for two hours each day.

### Suppliers

GIAC's suppliers are writers, who may supply Chinese fortunes in bulk or a few at a time.  All suppliers access the production Web site via an SSL connection to a Web application that connects them to the production and accounting databases.

Suppliers will communicate with the Web application over a SSL connection.

### Local Employees

GIAC office-based employees access the accounting, production and sales databases in support of all departments.  In addition, they share printers and files through a common server located on the LAN.

Local employees access the Internet via a WWW proxy as well as a SMTP server.  The SMTP server will connect to a proxy for outbound and inbound email delivery.

### IP Addressing

The internal network will use 6 private subnets and 8 legal IP addresses.  The subnets are 192.168.9.0 - 192.168.14.0.  The legal addresses are assigned by the ISP.  GIAC uses 1.100.215.0/24 for pool of addresses in lieu of a real subnet.  The Internet Assigned Numbers Authority (IANA) reserved network address list normally includes this subnet; however, adjustments were made accordingly throughout this document since it is being referred to as "legal" address space.

**Figure 1 - GIAC Network Diagram**
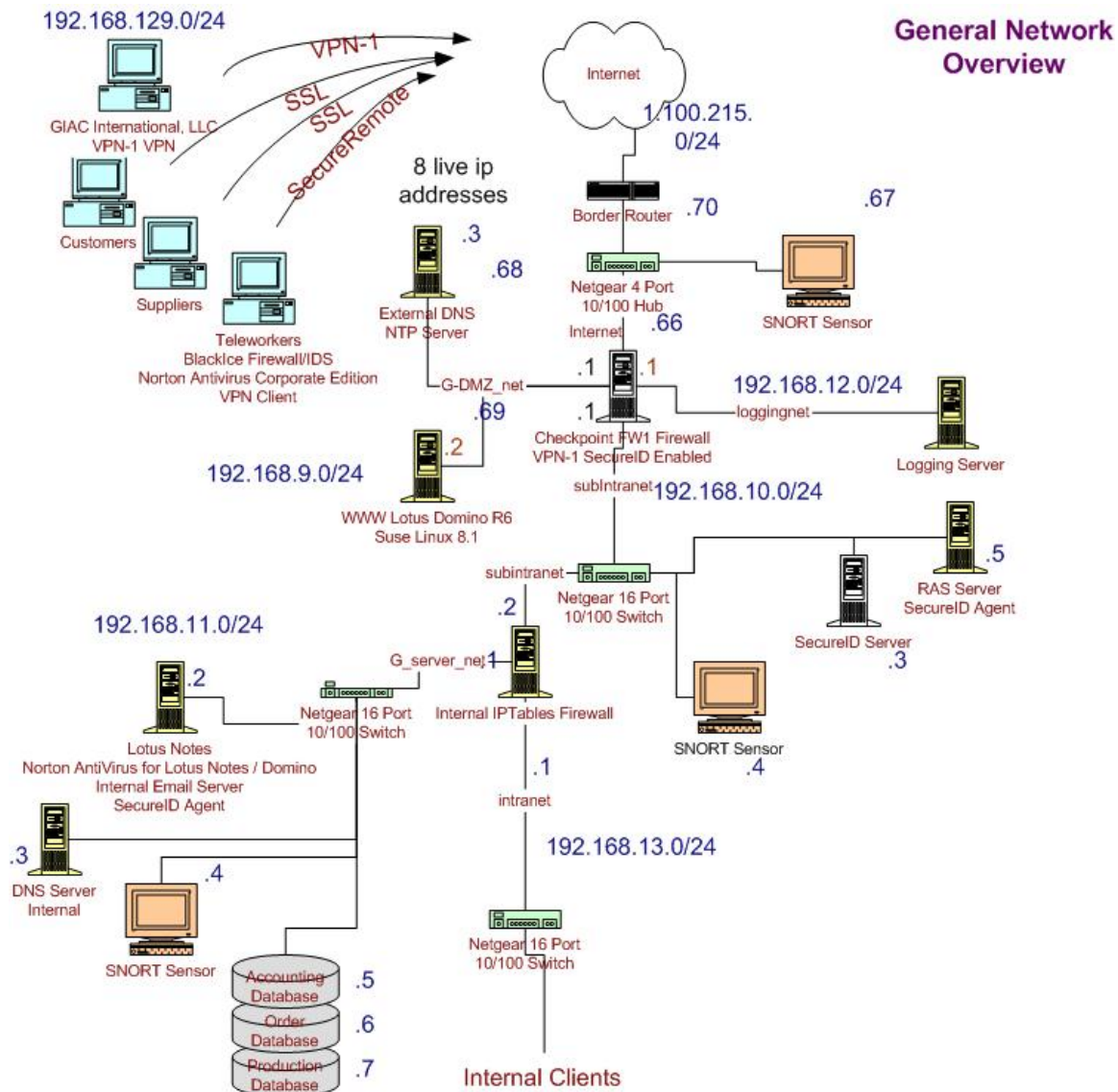


# The Components (From Exterior to Interior)

### Border Router

There is a Cisco 2600 with IOS Version 11.3 with Access Control List (ACL) software at the Internet border. The border router was positioned as a bastion router equipped to filter out the "noise" traffic. By stopping traffic at that point, the primary firewall will be relieved of inspecting packets that are not even remotely required.

It was configured to allow specific protocols only; those not specifically permitted are denied.

The router was configured with static routes.

### Hub

A Netgear 4 port 10/100 Hub was selected for placement between the primary firewall and bastion router. Placing the hub here allows the Snort IDS sensor to sniff all traffic to and from the Internet.

### Primary Firewall

Checkpoint's Firewall-1 4.1 SP6 was selected as the primary firewall. It is licensed with VPN-1 for the VPN component of the network. It functions as a gateway-to-gateway and client-to-gateway VPN utilizing Secure Client 4.1 SP56 (build 4200) for Windows 9x/NT/2k/XP. The operating system is Windows 2000 Server, service pack 3.

The firewall management module is licensed to run on the firewall only.

The Checkpoint product selected provides quite a bit of GIAC's required functionality on one box. Its "Security Servers" proxy popular services, such as SMTP and HTTP, transparently ties in user authentication where desired. The inbound SMTP proxy allows the company to adjust the banners easily as well as provides an additional queue for the occasional email server reboot.

Placement in the legal subnet allows the firewall to answer Address Resolution Protocol requests for the hosts for which it is translating. The firewall provides address translation services for the WWW server and the VPN to the Internet; thus, it must be placed on the Internet to function correctly.

The firewall also serves as a router at the center of the network creating additional subnet spaces for logging and the demilitarized zone (DMZ).

### IDS Sensor

Snort version 1.9.0 intrusion detection system (IDS) was selected for its ease of use, low cost, great documentation, large user base and network performance. Snort relies heavily on "rules" that provide it with attack-specific information. This means that administrators will have to regularly update these rules for the sensor to remain effective. Snorts' ability to mark suspect traffic with user configured tags in logs is key to our alerting infrastructure.

Snort was configured to add specific strings to certain alerts sent to logs. Those strings are used later to trigger alerts to key staff when necessary. Snort was

configured to send its logs to a remote logging host and can also perform local logging.

The sensor was placed on the legal subnet connected to a hub so that it may see all traffic directed to and from the GIAC network and the Internet.

### Devices located on the Primary Firewall's Interface "G-logging_net"

### Logging Server

Syslog running on Suse 8.1,equipped with OpenSSH 3.5 was selected as the logging server for the network. It was placed on a subnetwork off the primary firewall, thereby minimizing network penetration in the event syslogd is compromised. Syslog records all log entries for syslog-capable devices (the router, IDS sensors, Linux systems). The sensors are configured to log locally in addition to sending their logs to this system. The two log destinations will aid investigations of intrusions by providing corroborating information. A system breech of two different boxes in two different networks is much more difficult to hide than one.

The logging server is also the alerting server. It is equipped with Swatch 3.0.4. Swatch software scans logs for administrator-set keywords. Once a keyword appears, key personnel can be informed of the problem via email, pager or cell phone.

### Primary Firewall Interface "G-DMZ_Net"

This interface is to allow for a DMZ network to house the Web, DNS and NTP servers. If something should become compromised, the damage is limited by allowing only the absolutely required protocols out of this network.

### Primary Firewall Interface "G-Subintra_Net"

This interface was named "Subintra_Net" because it is located in the network on the firewall where the intranet would typically go. There is a secondary firewall blocking access to the actual intranet.

### IDS Sensor –

Snort sensor was placed to detect attack signatures in traffic to and from the VPN. Attacks coming from the VPN that get past the firewall need to be checked for known attack signatures. VPN clients, including the remote gateway to the GIAC International network, are a significant risk.

The IDS sensor was configured to send logs to the logging host.

### Switch

Netgear Model JFS516 16 Port 10/100 Fast Ethernet Switch was placed to reduce risk of multi-point network traffic sniffing.  It was configured to mirror the firewall port to the Snort IDS port enabling the IDS sensor to watch firewall traffic.

### Secondary Firewall, Internal

4 Network Interface Cards, Suse Linux 8.0, IPTables was selected as the secondary firewall to provide additional layering.  The additional layer of control in the network allows the administrator better control of traffic and better enforcement of the "deny all not explicitly allowed" rule.  IPTables' extensive logging will also aid in troubleshooting of network issues involving the primary firewall.

### Secondary Firewall Interface "G-Sever_net"

### Switch

Netgear Model JFS516 16 Port 10/100 Fast Ethernet Switch was chosen as the switch.  It was placed here to reduce risk of multi-point network traffic sniffing.  It was configured to mirror the firewall port to the Snort IDS port enabling the IDS to watch firewall traffic.

### IDS Sensor

Snort IDS sensor was placed to detect attack signatures in traffic to and from server network; it catches traffic from the Intranet and Server net.  The IDS sensor was configured to send logs to logging host.

### Secondary FW I/F Intranet

This network was created to house the in-house users.  File and print servers used by in-house users were placed here.

### All Employees

NAV Corporate Edition 7.6 for Small Business was selected for use by all employees because of its ease of use and deployment of initial software and virus definitions.  The NAV solution provides virus scanning for email via Lotus Notes.

### Teleworkers, Mobile Sales

BlackIce PC Protection, Version 3.5 was selected for the mobile sales force.  The BlackIce personal firewall augments the overall design by blocking unauthorized access to Teleworkers and Mobile Salesperson's computers.  Those systems are vulnerable because they provide a connection back into the network.

### Backup Connectivity

A modem pool equipped remote access server was included for emergency access requirements.  The server provides network access for Teleworkers,

Mobile Sales people, and IT administrators in the event of VPN access failures. The RAS server authenticates users using the SecureID server.

## Assignment 2

Host hardening is an extremely important part of any security plan. It has not been explicitly defined in this practical because it is not required by the 1.8 assignment instructions. Vendor software updates, physical security for the network, and eliminating non-essential services are required of a complete security policy. If neglected, those areas will quickly become the focus of an attack.

### Border Router

The Cisco border router software includes ACL. What follows is a list of Cisco ACLs in use and their function.

These ACLS apply to ingress traffic.

<u>Block ICMP redirects</u> – This ACL allows the company to block incoming ICMP redirects, which can be used to reconfigure a host's routing table.

```
deny icmp any any redirect
```

<u>Private address space per RFC 1918</u> – Traffic coming from these addresses is forged or coming from a misconfigured device, so it is dropped.

```
deny ip 10.0.0.0 0.255.255.255 any

deny ip 172.16.0.0 0.15.255.255 any

deny ip 192.168.0.0 0.0.255.255 any
```

Deny incoming multicast address space per
(http://www.iana.org/assignments/multicast-addresses)

```
deny ip 224.0.0.0 15.255.255.255 any
```

Deny incoming traffic with an address in the loopback space

```
deny ip 127.0.0.0 0.255.255.255 any
```

Deny incoming reserved address space per IANA
(http://www.iana.org/assignments/ipv4-address-space)

```
deny ip 0.0.0.0 0.255.255.255 any
```

```
deny ip 2.0.0.0 0.255.255.255 any

deny ip 5.0.0.0 0.255.255.255 any

deny ip 7.0.0.0 0.255.255.255 any

deny ip 23.0.0.0 0.255.255.255 any

deny ip 27.0.0.0 0.255.255.255 any

deny ip 31.0.0.0 0.255.255.255 any

deny ip 36.0.0.0 0.255.255.255 any

deny ip 37.0.0.0 0.255.255.255 any

deny ip 39.0.0.0 0.255.255.255 any

deny ip 41.0.0.0 0.255.255.255 any

deny ip 42.0.0.0 0.255.255.255 any

deny ip 58.0.0.0 0.255.255.255 any

deny ip 59.0.0.0 0.255.255.255 any

deny ip 60.0.0.0 0.255.255.255 any

deny ip 70.0.0.0 0.255.255.255 any

deny ip 71.0.0.0 0.255.255.255 any

deny ip 72.0.0.0 0.255.255.255 any

deny ip 73.0.0.0 0.255.255.255 any

deny ip 74.0.0.0 0.255.255.255 any

deny ip 75.0.0.0 0.255.255.255 any

deny ip 76.0.0.0 0.255.255.255 any

deny ip 77.0.0.0 0.255.255.255 any

deny ip 78.0.0.0 0.255.255.255 any
```

```
deny ip 79.0.0.0 0.255.255.255 any

deny ip 82.0.0.0 0.255.255.255 any

deny ip 83.0.0.0 0.255.255.255 any

deny ip 84.0.0.0 0.255.255.255  any

deny ip 85.0.0.0 0.255.255.255  any

deny ip 86.0.0.0 0.255.255.255  any

deny ip 87.0.0.0 0.255.255.255  any

deny ip 88.0.0.0 0.255.255.255  any

deny ip 89.0.0.0 0.255.255.255  any

deny ip 90.0.0.0 0.255.255.255  any

deny ip 91.0.0.0 0.255.255.255  any

deny ip 92.0.0.0 0.255.255.255  any

deny ip 93.0.0.0 0.255.255.255  any

deny ip 94.0.0.0 0.255.255.255  any

deny ip 95.0.0.0 0.255.255.255  any

deny ip 96.0.0.0 0.255.255.255  any

deny ip 97.0.0.0 0.255.255.255  any

deny ip 98.0.0.0 0.255.255.255  any

deny ip 99.0.0.0 0.255.255.255  any

deny ip 100.0.0.0 0.255.255.255   any

deny ip 101.0.0.0 0.255.255.255   any

deny ip 102.0.0.0 0.255.255.255   any

deny ip 103.0.0.0 0.255.255.255   any
```

```
deny ip 104.0.0.0 0.255.255.255   any

deny ip 105.0.0.0 0.255.255.255   any

deny ip 106.0.0.0 0.255.255.255   any

deny ip 107.0.0.0 0.255.255.255   any

deny ip 108.0.0.0 0.255.255.255   any

deny ip 109.0.0.0 0.255.255.255   any

deny ip 110.0.0.0 0.255.255.255   any

deny ip 111.0.0.0 0.255.255.255   any

deny ip 112.0.0.0 0.255.255.255   any

deny ip 113.0.0.0 0.255.255.255   any

deny ip 114.0.0.0 0.255.255.255   any

deny ip 115.0.0.0 0.255.255.255   any

deny ip 116.0.0.0 0.255.255.255   any

deny ip 117.0.0.0 0.255.255.255   any

deny ip 118.0.0.0 0.255.255.255   any

deny ip 119.0.0.0 0.255.255.255   any

deny ip 120.0.0.0 0.255.255.255   any

deny ip 121.0.0.0 0.255.255.255   any

deny ip 122.0.0.0 0.255.255.255   any

deny ip 123.0.0.0 0.255.255.255   any

deny ip 124.0.0.0 0.255.255.255   any

deny ip 125.0.0.0 0.255.255.255   any

deny ip 126.0.0.0 0.255.255.255   any
```

```
        deny ip 127.0.0.0 0.255.255.255   any

        deny ip 197.0.0.0 0.255.255.255   any

        deny ip 220.0.0.0 0.255.255.255   any

        deny ip 240.0.0.0 0.255.255.255   any

        deny ip 241.0.0.0 0.255.255.255   any

        deny ip 242.0.0.0 0.255.255.255   any

        deny ip 243.0.0.0 0.255.255.255   any

        deny ip 244.0.0.0 0.255.255.255   any

        deny ip 245.0.0.0 0.255.255.255   any

        deny ip 246.0.0.0 0.255.255.255   any

        deny ip 247.0.0.0 0.255.255.255   any

        deny ip 248.0.0.0 0.255.255.255   any

        deny ip 249.0.0.0 0.255.255.255   any

        deny ip 250.0.0.0 0.255.255.255   any

        deny ip 251.0.0.0 0.255.255.255   any

        deny ip 252.0.0.0 0.255.255.255   any

        deny ip 253.0.0.0 0.255.255.255   any

        deny ip 254.0.0.0 0.255.255.255   any

        deny ip 255.0.0.0 0.255.255.255   any
```

Allows FTP in

```
        permit tcp any any eq 20

        permit tcp any any eq 21
```

Allows SSH in

```
         permit tcp any any eq 22
```

## Allows Telnet in

```
         permit tcp any any eq 23
```

## Allows SMTP in

```
         permit tcp any any eq 25
```

## Allows IMAP in

```
         permit tcp any any eq 143

         permit udp any any eq 143
```

## Allows SecureRemote and VPN-1 in

```
         permit tcp any any eq 264

         permit tcp any any eq 18207

         permit udp any any eq 259

         permit udp any any eq 500

         permit 94 any 1.100.215.1 0.0.0.0

         permit 50 any 1.100.215.1 0.0.0.0

         permit 51 any 1.100.215.1 0.0.0.0
```

## Allows HTTP in
```
         permit tcp any any eq 80
```

## Allows HTTPS (SSL) in
permit tcp any any eq 443

## Allows DNS in
```
         permit tcp any any eq 53

         permit udp any any eq 53
```

## Allows established connections
```
         permit tcp any any established
```

Explicit drop rule (here for notation only).  This rule reminds the administrator that everything not explicitly allowed is denied.

```
deny ip any any
```

The following ACLs are for egress traffic.
Allows traffic out if it originates from the legal network

```
permit ip 1.100.215.0 0.0.0.255 any
```

Denies traffic going out that may have leaked or was maliciously sent

```
deny ip 192.168.9.0 0.0.0.255 any log-input

deny ip 192.168.10.0 0.0.0.255 any log-input

deny ip 192.168.11.0 0.0.0.255 any log-input

deny ip 192.168.12.0 0.0.0.255 any log-input

deny ip 192.168.13.0 0.0.0.255 any log-input

deny ip 192.168.14.0 0.0.0.255 any log-input

deny ip 192.168.15.0 0.0.0.255 any log-input
```

Block Traceroute probe responses - OUT

```
Deny icmp any any time-exceeded
```

The order of rules in the list is important because the router compares each incoming packet to the rule set from top to bottom.  The most-often used rules should go highest in the list for performance optimization.  When the router reaches a rule for which the packet is a match, it allows the packet to continue on and then handles the next packet.

If you place a rule that generally allows all packets at the top of the rule set and get more specific at the bottom, the top rule "shadows" the other rules.  Rules that are shadowed by other rules never get used, because a packet filtering through the rule set gets sent on its way before the critical ACL is reached.
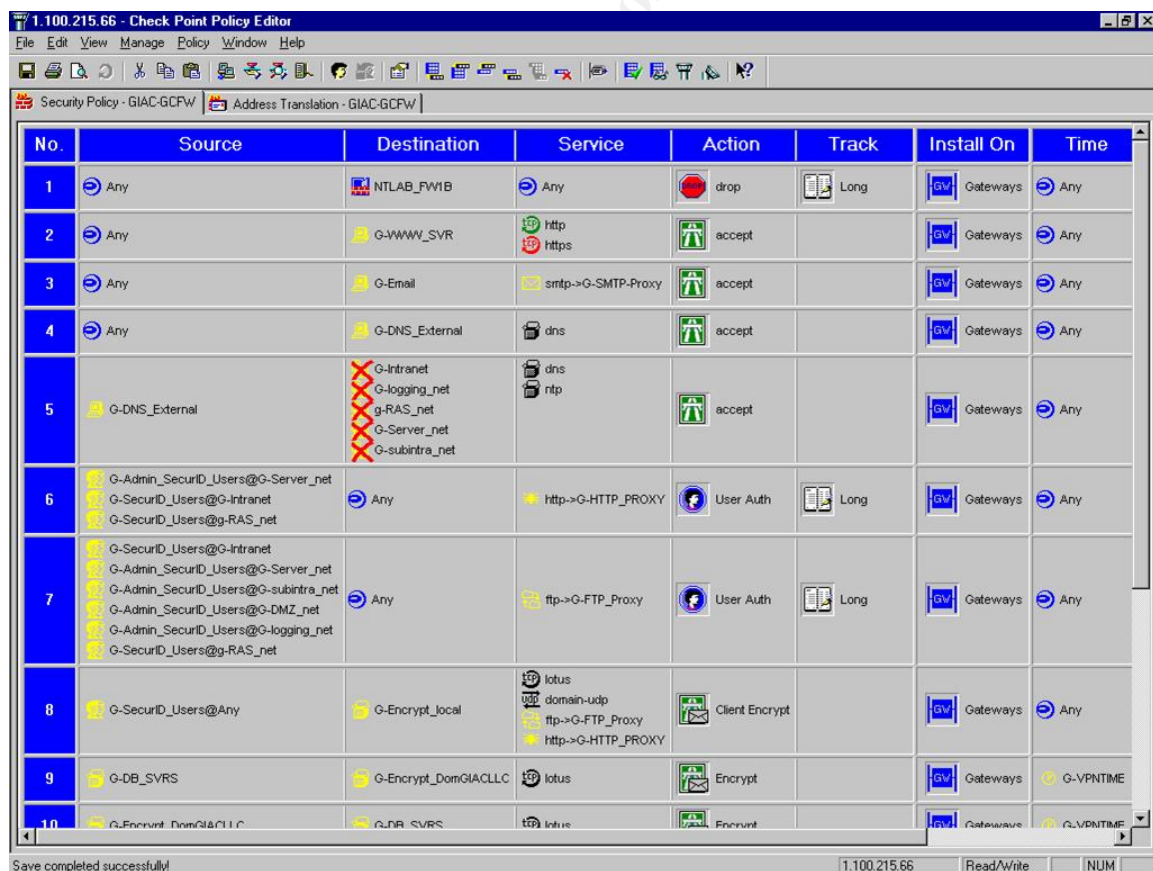
### Tips, tricks, **potential problems**

- Don't forget the implicit deny everything rule!
- Don't save the running config until all services are tested
- Check IANA regularly to insure "reserved" list is up-to-date and is not blocking legitimate access
- Consider setting the logging on all rules to "long" at the start of a rule base rollout so that troubleshooting is easier. The first few days of new access restrictions tends to bring many complaints that can be verified through log entries.

### Primary Firewall

Figures 2 and 3 show the rules in place on the firewall.

### Figure 2 - Firewall-1 Rule Set, part 1

Figure 3 - Firewall Rule Set, part 2

**Figure 4 - Firewall Rule Set, part 3**

**Figure 4 – Firewall-1 Rule Set, part 4**



As part of GIAC practical repository.
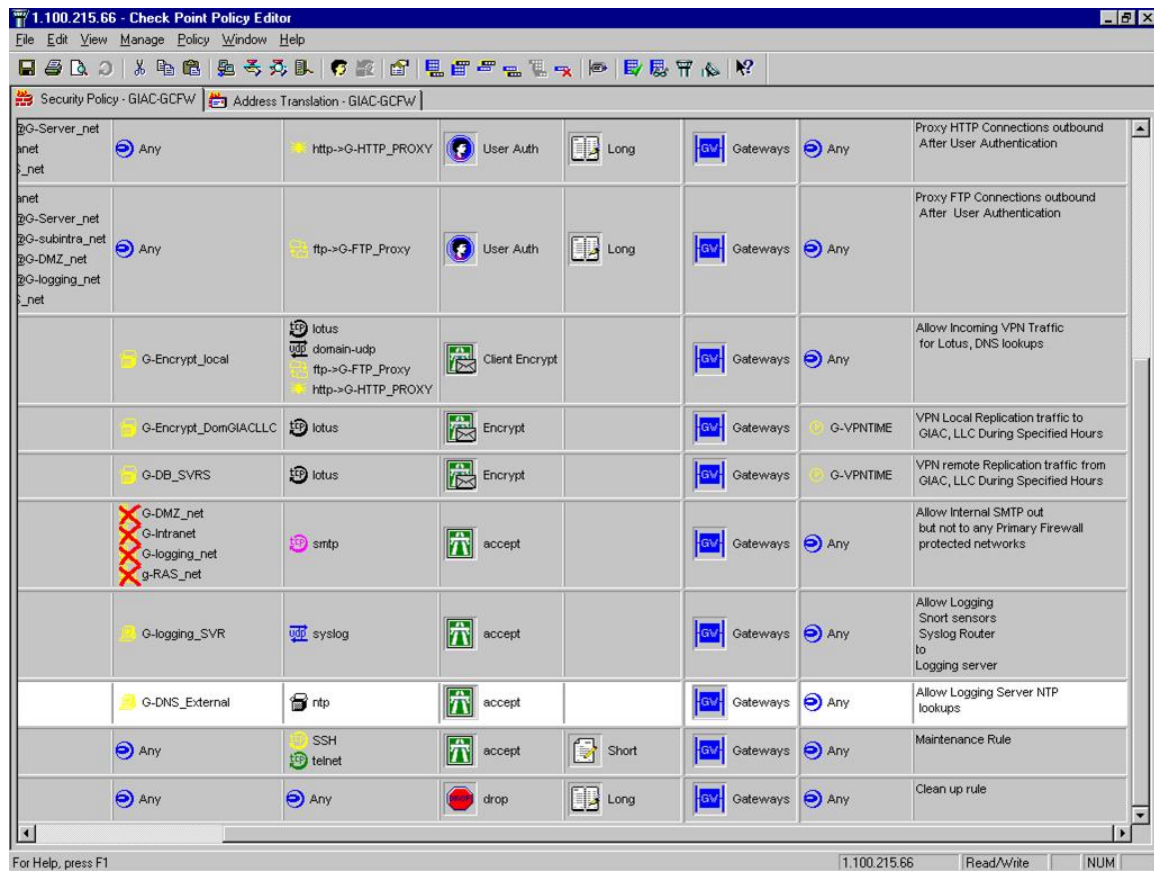
The following is a listing of each rule and its purpose.

1) This is the stealth rule. It puts the firewall in "stealth" mode. Any access to the server is dropped, making the firewall "invisible."
2) This rule allows clients from the Internet access the WWW server. It also is responsible for network address translation for the WWW server.
3) This rule allows Internet email servers to access the SMTP proxy on the firewall. The firewall acts as the SMTP server for the email domain and accepts incoming email. This "security server" allows for a safer interface between the Internet and the internal email server. The banners on the SMTP proxy were changed so it does not give away any information about the server, network or firewall.
4) This rule allows everyone access to the external DNS server on the DMZ.
5) This rule allows the external DNS server located on the DMZ network DNS and NTP protocol access out to any destination except the house networks. The red Xs through the networks denote that the "negate" command (e.g., "any but" the listed objects) was selected.
6) This is the HTTP proxy authentication rule. This rule allows the company to tie a user to his/her WWW activity through the firewall.
7) This is the FTP proxy authentication rule. Like the HTTP proxy authentication rule, this rule authenticates users attempting to use the FTP proxy on the firewall.
8) VPN rule (explained later in this document)
9) VPN rule (explained later in this document)
10) VPN rule (explained later in this document)
11) This rule allows the Internal email server to send mail using the SMTP protocol to any network but the house networks.
12) This rule provides access for syslog devices sending syslog protocol traffic to the logging server.
13) This rule enables the logging server to connect to the DNS external server for NTP time updates.
14) This administrative rule provides the technical staff access to all systems on the network from their own workstations. It is restricted to SSH and telnet to accommodate both Linux systems (SSH) and the router (telnet).
15) This rule server as the "Clean-Up Rule." As a "deny all" rule, it enforces the company's basic security premise of "deny all unless explicitly allowed." Logging is enabled to aid in troubleshooting by capturing a record of packets that are denied by the firewall. This is helpful when applying restrictive security rules; the administrator may be unaware of all protocols in use.

**Rule Order**

Rules placement is integral to the Firewall-1 rule set. When determining rule placement, function is the primary consideration. Packets traversing the firewall are evaluated against the rulebase from top (Rule 1) to bottom (Rule 2). Once a packet reaches a rule that matches the rule's criteria, that packet is acted upon. If rules are improperly ordered, a rule that is too general could allow (or deny) a packet before your more specific rule.

A good guideline for order placement is to place specific rules at the top of the rule base. Rules used more often should be placed highest in the list, with least-often used rules going lower.

Rule 1 is placed at the top for "Stealth." This rule makes the firewall mostly invisible to network users. It must always go at the top of the rule base to perform this function. Rule 2 is at the top of the rule base because the majority of traffic traversing the firewall is expected to be HTTP and HTTPS in nature. This allows the firewall to let the high-volume traffic through the firewall soon in the rule base, thus reducing firewall-processing time of the packet. Internal users will be able to access the G-WWW_SVR server without authenticating; users bound for the destination will be allowed through the firewall without getting to the "User Authentication" object. This is acceptable, as the G-WWW_SVR server itself will authenticate users accessing its applications. Internal users heading off to other WWW destinations will be stopped for authentication at Rule 4.

**Tips, tricks, potential problems**

- Time restrictions can be tricky. Administrators in charge of the database servers must be consulted about replication times and duration. Replications can be cut off if the time duration is too short. Database administrators should be aware that lengthy replication times may be the cause of communication errors during replication.
- Logging is vital during a new rule base rollout. When the rules are in place, it is likely that end users and even IT staff will blame the firewall out of hand as the cause of the problem. It is the firewall administrator's job to know how to read the log as well as to have the appropriate logging in place for troubleshooting.
- Logging is slow. It is a good idea to turn off name resolution on logs. Display will be significantly faster without involving DNS.
- Network address translation is tricky. A frequent Firewall-1 administrator problem is to enable translation on the object without doing anything else. Don't forget to add a route to the appropriate host as well as an Address Resolution Protocol (ARP) entry appropriate for the operating system in use.
- Comment, comment, comment. A brief description of rules' goals should be included in the rule base. A comment field is provided.

Good use of the comments will help ensure that troubleshooting efforts will not result in a weaker rule base.

**Virtual Private Network**

The Virtual Private Network is integrated with the Firewall-1 software. The rules that represent the Virtual Private network are detailed below.

Rule 6) This rule provides for client virtual private networking using the Secure Client VPN client. Clients in the G_SecurID_Users@Any group are authenticated using the SecurID ACE card and the SecurID server through the firewall. This rule allows Lotus and DNS Query traffic only.

Rule 7) This rule provides for encryption of database replication taking place from the server network to the remote site, GIAC International, LLC. A time component has been added to restrict replication traffic to predetermined times.

Rule 8) This rule provides for encryption and decryption of database replication traffic from GIAC International, LLC heading for the server network. Again, a time component has been added to restrict replication traffic to predetermined times.

**Figure 5 Encrypt Action Properties for Rules 7 and 8**
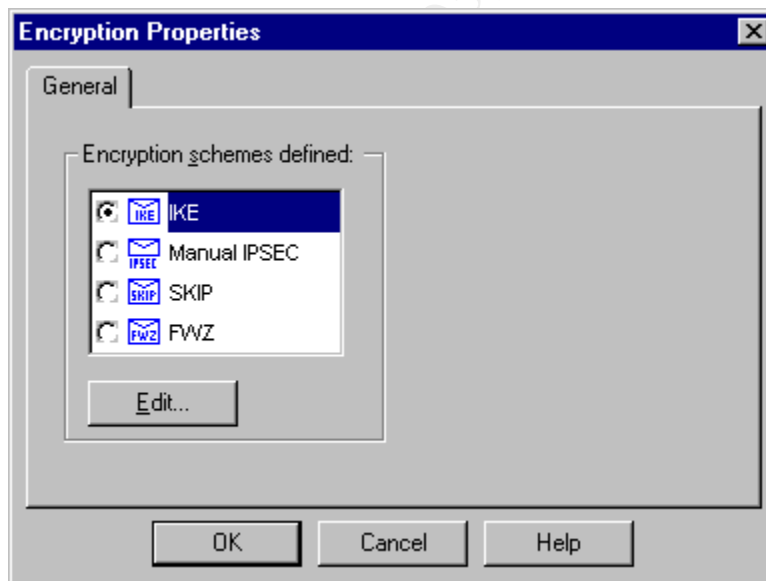


**Figure 6 IKE Properties for Rules 7 and 8**
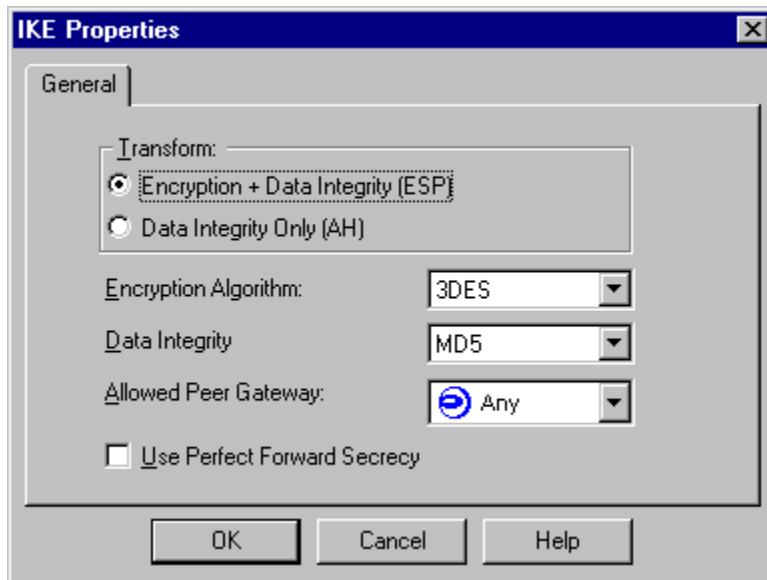
**Rule Order**

Rules for encrypting traffic between a host or another gateway must be placed properly to ensure encryption and optimal performance. Rule 6 is the client encryption rule. It is placed lower in the rule base than customer traffic and internal users because they will likely generate less traffic. Rules coming later in the rule base are not expected to generate as much traffic.

Rule 7 is the G-DB_SVRS side of the gateway-to-gateway virtual private network. It is placed above the rule that encrypts traffic initiated from the GIAC International network, because more traffic will be initiated from the server network to GIAC International than initiated remotely.

**Tips, tricks, potential problems**

1) When configuring VPN on the remote firewall, it is wise to have the remote administrator on the telephone. Both administrators should have their policy editors open and ready. Proper functionality is dependent on both systems' settings being consistent.
2) The times in the time object in Rules 7 and 8 should be relayed to the database administrators on both sides of the VPN as well as the Firewall-1 administrators. This will help ensure that technical staff don't get caught up trying to resolve communications issues when off-schedule replication attempts fail.

# Assignment 2 - Tutorial

# *Tutorial For Implementing Access Control Lists on Cisco 2600 IOS 11.3 Border Router*

This tutorial will walk you through applying Access Control Lists (ACLs) on the Cisco 2600 IOS v.11.3 Border Router for GIAC Enterprises.  Following the step-by-step instructions will result in full implementation of the ACLs detailed in the first half of this assignment.

Implementing ACLs without affecting legitimate traffic is a difficult task at best.  We will approach this task cautiously, and will only make changes permanent after a "test-drive" period.

Begin your task by starting your favorite telnet client from an administrative workstation.  You will telnet to the IP address of the Ethernet port 1.100.215.70.  Once you become connected, you will be presented with a password prompt as follows.

```
User Access Verification

Password:
```

Once the access password is properly entered, you will be presented with the router name and prompt.

```
NLRT06>
```

From this prompt you have limited access to the router.  This level of access is provided for informational access only.  This level of access can be used by general IT personnel to gather information in the event of network difficulty.

A few words about Cisco's operating system IOS are in order before we can proceed.

IOS offers extensive help at each prompt by simply typing '?'.  If you need help on a particular keyword, you simply type a '?' after the word, and a list of possible parameters will follow.

For example, type 'systat ?' at the prompt.

```
NLRT06>systat ?
```

```
        all  Include information about inactive ports

        <cr>
```

This tells us that the command expects either the keyword "all"—which will give information about inactive ports (and, presumably, active ports)—or a carriage return "<cr>" (enter key).

Instead of typing a full command, at any prompt you can use IOS' "auto complete" feature as a shortcut. Simply hit the "tab" key after entering a few of the commands' first characters. If there is more than one command available starting with the characters you have entered, your terminal will "beep" and the router prompt will return a clean line. If you are unsure of the next characters needed to auto-complete the command, you can type a '?' to get a list of available commands that match your characters.

It is important to note that all commands are not always available at all prompts in IOS. For instance, if you are trying to configure a route using the 'IP' command, the IP command won't be available to you until you enter config mode. There is more information on config mode later in this tutorial.

Here's another important note on the IOS operating system: IOS 11.3 represents the oldest, most common version of IOS found on the Internet after Year 2000 upgrades. While IOS versions among router hardware differ very little (if you know IOS 11.3 on a low end Cisco router you will be comfortable with IOS 11.3 on a high end Cisco router), commands and syntax can vary slightly between versions. If you encounter problems with a command's syntax, check the context sensitive help by pressing "?" at each step of the command entry.

Also, all changes made to the router are made to it's "running-config," the configuration currently loaded in memory and not the memory on the router's flash card. This allows for instant changes as well as recovery in case of mistakes. Since the commands aren't written to storage until you explicitly tell the router to do so (which is covered at the end of this tutorial), you can cycle the router's power to recover from mistakes.

The next level of access, "administrator" level, is reached by typing "enable" at the prompt. Administrator level is used for making such changes to the router as applying ACLs or bringing network interfaces up or down. You are then presented with another password prompt.

```
        NLRT06>enable

        Password:
```

Once the password is entered correctly, the router prompt changes. Notice the pound sign after the router's name.

        NLRT06#

Enter configuration mode by typing "conf t," which is short for "configure terminal." The router prompt will change to include the word "config."

        NLRT06#conf t

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

        NLRT06(config)#

Now we are ready to enter the ACLs. We begin with the ingress ACLs. The command we are going to use will build a list of ACLs to be applied all at once. The syntax of the command is as follows:

ip access-list extended <name_of_the_list>

The ACL is created using the global IP command. The keyword "access-list" tells the router that we are going to create a list. The "extended" keyword indicates that the type of access controls will be extended. Only standard and extended types are available here. "Extended type" is more resource-intensive than "standard," with the router comparing source, destination and port information for each packet instead of just source information. We are going to call our first list "ingress_acls" because it will be applied to inbound traffic on the Internet interface (serial 0/0).

        NLRT06(config)#ip access-list extended ingress_acls

Notice again that the router prompt has changed. The new prompt indicates that you are in extended ACL entry mode.

        NLRT06(config-ext-nacl)#

The first access control we will enter is one that will block ICMP redirects. ICMP redirects coming from the Internet are not to be trusted. If allowed, they could reconfigure a host's routing table. We will turn the ICMP redirects off here.

The command we will be using is "deny." Its syntax is as follows: deny <protocol or protocol number> <source address or keyword "Any" or source "Host"> <destination address or keyword "Any" or destination "Host"> <icmp message type>.

We could append the "log" command to send messages when the rule is enforced, if desired. We will focus on logging only those rules that represent possible security breach to cut down on the "noise."

```
NLRT06(config-ext-nacl)#deny icmp any any redirect
```

Once this (the very first ACL) command has been entered and applied, the router enforces an "implicit deny all" rule. This rule says that if there isn't a rule explicitly permitting a packet through the router, it should be denied. This rule has the effect of disconnecting anyone and everyone from configuring the router, and will even disconnect you if you are not careful. If that should happen, simply go to the router and cycle the power. Your original settings will be reinstated, and you will have to re-start this process at the beginning.

It is good practice to use a text editor to create these next commands. Once you are happy with the commands that you have created, use cut and paste to enter them. This will also help prevent typos. In this mode of ACL list creation (named-list mode), you are allowed to add and remove ACLS as needed. However, you are unable to place them in specific positions.

Rule order is important because packets are applied to this filter from top to bottom. Your most frequently used rules should be placed at the top of the list. Once a packet is matched against a rule, the router allows it to continue onto its destination. The sooner in the ACL that the router can release its packets, the less time it spends processing, the better it will perform.

The first rules are "permit' rules allowing traffic we explicitly desire.

The "permit" command syntax is as follows: permit <protocol, or protocol number> <source address or keyword "any" or "host" > <destination address or keyword "any" or "host"> <keyword "eq" or established" (among many others)> <well-known service name or number>.

There is one on each line.

Allows SSH incoming

```
permit tcp any any eq 22
```

Allows SMTP incoming

```
permit tcp any any eq 25
```

Allows SecureRemote and VPN-1 access to the firewall only

Here, we have used a specific destination address. This permit command syntax is slightly different and has an important twist—"destination wild-card bits": permit <protocol, or protocol number> <source address or keyword "any" or "host" > <destination address> <destination wild-card bits> <keyword "eq" for equals> <well-known service name or number>. Rather than provide the standard binary bit mask to indicate host and network portions of an address, Cisco requires you to invert the 1's and 0's.

For instance, the network 192.168.13.0 with a net mask of 255.255.255.0 would have a bit mask of 11111111.11111111.11111111.00000000. The Cisco wild card inverts the 0s and 1s to 00000000.00000000.00000000.11111111 or 0.0.0.255. If you omit the wild card, 0.0.0.0 is assumed.

```
permit tcp any 1.100.215.66 0.0.0.0 eq 264

permit tcp any 1.100.215.66 0.0.0.0 eq 18207

permit udp any 1.100.215.66 0.0.0.0 eq 259

permit udp any 1.100.215.66 0.0.0.0 eq 500

permit 94 any 1.100.215.66 0.0.0.0

permit 50 any 1.100.215.66 0.0.0.0

permit 51 any 1.100.215.66 0.0.0.0
```

Allows HTTP incoming

```
permit tcp any 1.100.215.69 0.0.0.0 eq 80
```

Allows HTTPS (SSL) incoming

```
permit tcp any 1.100.215.69 0.0.0.0 eq 443
```

Allows DNS

```
permit tcp any 1.100.215.68 0.0.0.0 eq 53

permit udp any 1.100.215.68 0.0.0.0 eq 53
```

Allows established connections incoming

```
permit tcp any any established
```

We continue the access list creation process by adding those networks that IANA has listed as reserved. The list can be found at http://www.iana.org/assignments/ipv4-address-space and should be checked regularly for changes.

The command used here is "deny." We will be denying traffic from the following list of networks because their use is either a mistake or malicious. The syntax of this command is as follows: deny <protocol, or protocol number> <source address > <Source wildcard bits> <destination address or keyword "Any" or "Host">.

One command is entered on each line.

You should still be at this prompt:

    NLRT06(config-ext-nacl)#

Enter the following ACLs, one per line.

    deny ip 0.0.0.0 0.255.255.255 any

("deny ip 1.0.0.0 0.255.255.255 any" is removed because we are using the address space as our "live" allocation)

    deny ip 2.0.0.0 0.255.255.255 any

    deny ip 5.0.0.0 0.255.255.255 any

    deny ip 7.0.0.0 0.255.255.255 any

    deny ip 23.0.0.0 0.255.255.255 any

    deny ip 27.0.0.0 0.255.255.255 any

    deny ip 31.0.0.0 0.255.255.255 any

    deny ip 36.0.0.0 0.255.255.255 any

    deny ip 37.0.0.0 0.255.255.255 any

    deny ip 39.0.0.0 0.255.255.255 any

    deny ip 41.0.0.0 0.255.255.255 any

    deny ip 42.0.0.0 0.255.255.255 any

```
deny ip 58.0.0.0 0.255.255.255 any

deny ip 59.0.0.0 0.255.255.255 any

deny ip 60.0.0.0 0.255.255.255 any

deny ip 70.0.0.0 0.255.255.255 any

deny ip 71.0.0.0 0.255.255.255 any

deny ip 72.0.0.0 0.255.255.255 any

deny ip 73.0.0.0 0.255.255.255 any

deny ip 74.0.0.0 0.255.255.255 any

deny ip 75.0.0.0 0.255.255.255 any

deny ip 76.0.0.0 0.255.255.255 any

deny ip 77.0.0.0 0.255.255.255 any

deny ip 78.0.0.0 0.255.255.255 any

deny ip 79.0.0.0 0.255.255.255 any

deny ip 82.0.0.0 0.255.255.255 any

deny ip 83.0.0.0 0.255.255.255 any

deny ip 84.0.0.0 0.255.255.255   any

deny ip 85.0.0.0 0.255.255.255   any

deny ip 86.0.0.0 0.255.255.255   any

deny ip 87.0.0.0 0.255.255.255   any

deny ip 88.0.0.0 0.255.255.255   any

deny ip 89.0.0.0 0.255.255.255   any

deny ip 90.0.0.0 0.255.255.255   any

deny ip 91.0.0.0 0.255.255.255   any
```

```
deny ip 92.0.0.0 0.255.255.255    any

deny ip 93.0.0.0 0.255.255.255    any

deny ip 94.0.0.0 0.255.255.255    any

deny ip 95.0.0.0 0.255.255.255    any

deny ip 96.0.0.0 0.255.255.255    any

deny ip 97.0.0.0 0.255.255.255    any

deny ip 98.0.0.0 0.255.255.255    any

deny ip 99.0.0.0 0.255.255.255    any

deny ip 100.0.0.0 0.255.255.255    any

deny ip 101.0.0.0 0.255.255.255    any

deny ip 102.0.0.0 0.255.255.255    any

deny ip 103.0.0.0 0.255.255.255    any

deny ip 104.0.0.0 0.255.255.255    any

deny ip 105.0.0.0 0.255.255.255    any

deny ip 106.0.0.0 0.255.255.255    any

deny ip 107.0.0.0 0.255.255.255    any

deny ip 108.0.0.0 0.255.255.255    any

deny ip 109.0.0.0 0.255.255.255    any

deny ip 110.0.0.0 0.255.255.255    any

deny ip 111.0.0.0 0.255.255.255    any

deny ip 112.0.0.0 0.255.255.255    any

deny ip 113.0.0.0 0.255.255.255    any

deny ip 114.0.0.0 0.255.255.255    any
```

```
deny ip 115.0.0.0 0.255.255.255   any

deny ip 116.0.0.0 0.255.255.255   any

deny ip 117.0.0.0 0.255.255.255   any

deny ip 118.0.0.0 0.255.255.255   any

deny ip 119.0.0.0 0.255.255.255   any

deny ip 120.0.0.0 0.255.255.255   any

deny ip 121.0.0.0 0.255.255.255   any

deny ip 122.0.0.0 0.255.255.255   any

deny ip 123.0.0.0 0.255.255.255   any

deny ip 124.0.0.0 0.255.255.255   any

deny ip 125.0.0.0 0.255.255.255   any

deny ip 126.0.0.0 0.255.255.255   any

deny ip 127.0.0.0 0.255.255.255   any

deny ip 197.0.0.0 0.255.255.255   any

deny ip 220.0.0.0 0.255.255.255   any

deny ip 240.0.0.0 0.255.255.255   any

deny ip 241.0.0.0 0.255.255.255   any

deny ip 242.0.0.0 0.255.255.255   any

deny ip 243.0.0.0 0.255.255.255   any

deny ip 244.0.0.0 0.255.255.255   any

deny ip 245.0.0.0 0.255.255.255   any

deny ip 246.0.0.0 0.255.255.255   any

deny ip 247.0.0.0 0.255.255.255   any
```

```
deny ip 248.0.0.0 0.255.255.255   any

deny ip 249.0.0.0 0.255.255.255   any

deny ip 250.0.0.0 0.255.255.255   any

deny ip 251.0.0.0 0.255.255.255   any

deny ip 252.0.0.0 0.255.255.255   any

deny ip 253.0.0.0 0.255.255.255   any

deny ip 254.0.0.0 0.255.255.255   any

deny ip 255.0.0.0 0.255.255.255   any
```

The next addresses are designated "private address space" per RFC 1918.
Again, any traffic coming from the Internet with a source of these networks is a
misconfigured device or is malicious in nature.

```
deny ip 10.0.0.0 0.255.255.255 any

deny ip 172.16.0.0 0.15.255.255 any

deny ip 192.168.0.0 0.0.255.255 any
```

Multicast address space per RFC 3330

```
deny ip 224.0.0.0 0.255.255.255 any
```

Loopback address space per RFC 3330, 1700

```
deny ip 127.0.0.0 0.255.255.255 any
```

The last rule is the "implicit deny all" rule previously discussed. It is included
here for clarity and documentation purposes. It's nice to have the visual
reminder should troubleshooting become necessary.

```
deny ip any any
```

Ingress rules are complete. You will now exit the ACL group edit mode by typing
"exit" once.

```
Exit
```

You will get the following prompt:

```
NLRT06(config)#
```

We now need to apply the access group ACLs to a specific interface in a specific direction. Direction is "in" or "out" (bound). The "ingress_acls list" was designed to block or permit packets coming in from the Internet, so we will block them "in." The mode needed to apply the access list is "interface." The interface command is used to configure interfaces, Ethernet, serial, etc. The command syntax for Interface is as follows: interface <interface type, serial, Ethernet, Token Ring, etc.> <serial Interface number/serial interface number>.

```
NLRT06(config)#interface serial 0/0

NLRT06(config-if)#
```

Notice the prompt change indicates that you are in interface config mode. From here, we use the IP command again with the following syntax: IP <access-group> <access-group name> <direction in or out>.

```
NLRT06(config-if)#ip access-group ingress_acls in

NLRT06(config-if)#exit

NLRT06(config)#
```

From here your ingress_acls access-list is in effect. Now we turn to egress filters.

Egress filters are important for many reasons. For instance, it is useful if one of our systems should fall prey to an attack and be turned into a worm propagator or denial of service zombie. While it is most difficult to keep patches and configurations so completely up-to-date that you can avoid **every** attack that exists, it is quite easy to put some outbound restrictions in place that will deny an attacker complete success in the event of a security breach. Also, egress filters help ensure a misconfigured router or network device doesn't "leak" traffic meant for the internal network only.

Implementing egress ACLs takes place in the same manner as our ingress_acls list. You should still be at the config prompt. If not, follow the first steps listed above to get back to the following prompt.

```
NLRT06(config)#
```

Again, we are using the IP command. In this case we are calling the list "egress_acls."

```
NLRT06(config)# ip access-list extended egress_acls

NLRT06(config-ext-nacl)#
```

From the "nacl" prompt, we don't start our egress ACLs list with the most-often used rule. Instead, we are blocking certain ports and services. The most-used rule comes after the blocking rules because if it were placed at the start of the list, the services that we want to block would be allowed through before the packet got to the rule that it matches.

Denies Windows file sharing services

```
deny tcp any any range 135 139

deny udp any any range 135 139
```

Denies SNMP traffic

```
deny tcp any any range 161 162
```

Denies X-windows traffic

```
deny tcp any any range 6000 6255
```

Denies Tftp traffic

```
deny tcp any any eq 69
```

Denies Syslog traffic

```
deny tcp any any eq 514
```

This rule permits traffic originating from legal network(s) out

```
permit ip 1.100.215.0 0.0.0.255 any
```

The next rule adds an element that we have not used previously. Log-input sends the MAC address to the logging facility. If the rules are tripped, this will help in investigating the cause.

Denies traffic going out that may have leaked or was maliciously sent

```
deny ip 192.168.9.0 0.0.0.255 any log-input

deny ip 192.168.10.0 0.0.0.255 any log-input
```

```
        deny ip 192.168.11.0 0.0.0.255 any log-input

        deny ip 192.168.12.0 0.0.0.255 any log-input

        deny ip 192.168.13.0 0.0.0.255 any log-input

        deny ip 192.168.14.0 0.0.0.255 any log-input

        deny ip 192.168.15.0 0.0.0.255 any log-input
```

The next rule is unique in that it blocks traceroute probe responses on their way
out.  We can't be certain of the program, protocol or port of the incoming
response, so we block the outgoing response.

```
        Deny icmp any any time-exceeded
```

Here, again, we are explicitly creating the drop all rule to remind us of its
existence.

```
        deny ip any any
```

From here we can exit and apply our list to the appropriate interface.

```
        Exit

        NLRT06(config)#

        NLRT06(config)#interface serial 0/0

        NLRT06(config-if)#ip access-group ingress_acls in

        NLRT06(config-if)#exit

        NLRT06(config)#exit

        NLRT06#exit
```

Exits the terminal.

Your ACLs are now in force.  You haven't saved the running configuration yet—
and for good reason.  If connectivity problems should arise after applying these
ACLs, you can simply cycle the router's power to get back on online.

If you determine there is a protocol in use that is needed but restricted by these
ACLs, you can enable that security by creating an explicit permit rule (ingress or
egress) or negating an existing rule.  This is done by going into edit mode on the

list holding the offending rule and inserting "no" in front of the "deny" command that is the problem.

After running the router for a day or two without problems, you are ready to make the changes permanent. The procedure is as follows: Telnet to the router, enter your password, type enable, enter your password again to get to the enable prompt:

```
NLRT06#
```

From here, you need to instruct the router to copy the running-config to the startup-config. The command for that is:

```
Copy running-config startup-config
```

The result of this command should be:

```
Building configuration...

[OK]

NLRT06#
```

Type "exit", and you are done.

**Assignment 3**

# *Audit Your Design*

**Plan the Audit**

The audit will be performed with a laptop equipped with Linux and nmap. Linux was chosen for the wide range of available network tools. Nmap was chosen for its powerful scanning features.

Nmap allows the auditor to send with ease both TCP and UDP packets to any host required. Nmap's OS fingerprinting feature will help identify the actual host responding in situations where network address translation may be employed. Nmap will not search for vulnerabilities—it simply provides information about the actual ports open on a target and, from that, information about the target itself.

The auditor probes the firewall from each network to get a more complete idea of the rules in effect. From each network, a series of nmap scans will take place, a TCP SYN scan, and a UDP scan.

| Protocol | ports | destination | source |
|----------|-------|-------------|--------|
| Tcp SYN | all | firewall NAT hosts | each net |
| Udp | all | Firewall NAT hosts | each net |
| ICMP | | All hosts | each net |

Firewall-1 is capable of performing address translation for multiple hosts, and it does so for the WWW server. After the ICMP scan, the ARP cache will be examined to determine the hosts for which address translatation is being performed. Multiple firewall MAC address entries in the ARP cache for multiple hosts indicates address translation is in use. It will also indicate which hosts are affected.

A "TCP SYN" scan of the firewall and the IP addresses for which it is performing one-to-one address translation will reveal if the firewall is enforcing its service rules. Performing that scan from each network will tell the auditor what services are allowed and from which networks they are allowed.

A "UDP scan" is less reliable than the SYN scan above but helps flesh out the data needed by the auditor to provide a complete picture of rules in effect.

The audit should begin with only the most basic information about the network configuration. The audit is a test of the rulebase in effect on the firewall. Anything could have changed since the policy was put in place, and so

everything should be checked. Because the rulebase can be modified in any way, including the removal and addition of objects and rules, we can assume very little at the start. A general scan for services on all hosts on all networks should be performed. Hosts that are accessible should have ports scanned for both UDP and TCP protocols.

**Costs and Level of Effort**

> Network scans –TCP x 4 networks = 16 hours
> > 1500 ports – 10 mins
> > 65k ports – 4hours, 45mins each
> Network scans – UDP x 4 networks = 4 hours
> Analysis and follow-up of scan results = 4 hours
> Total Time = 24 hours
>
> Hardware and software required
> 1 Laptop with Network Interface Card
> Linux with Nmap 3.0
> 1 IP Address for the "legal" network
> Cat 5 Network Cable
> Approx $1,500

The level of effort on the initial audit should be high, as the first audit will provide the baseline for subsequent audits. All anomalous results should be followed up as best as possible. Level of effort in this area can range from hours to months. A new installation will require more effort in documentation of all rules, ACLs and open ports.

**Time Considerations**

Except for the specific timed rule tests listed above, the audit should be performed during the regular day shift. An audit performed during regular business hours will provide the auditor with a look at the network as it is used. No IT personnel are expected on duty after hours.

**Risks and Considerations**

During the audit, it is likely that the IDS sensors will generate large amounts of logging. In fact, the audit will generate much more traffic than would be typically faced in everyday situations. Those systems could become overwhelmed and could fail. The IDS systems should be checked for functionality immediately following the audit.

Similarly, alerting systems could become overwhelmed and fail. The Swatch alerting systems should be checked immediately following the audit.

Once the audit period has begun (but before network traffic is generated), personnel should be notified to track alerts received but to hold response. Notifying staff that the audit is taking place could lead to changes in the firewall. Therefore, access to the firewall should be restricted during the audit. This firewall is not equipped with a remote management station but, if it were, that station should be restricted as well. The Firewall-1 license application will explain which licenses are in effect and which workstations (if any) are authorized for Management GUI access.

The audit traffic could mask real attack/recon/DOS traffic. Because general user access will continue during the audit, it is important that security is not shut down. Alarms sent out by the IDS should be tracked and all log entries at the logging server should be checked as usual. Scans from the auditor's laptop can be identified by IP address specifically assigned to the device for the task.

Alerts and log entries not coming from the auditor's laptop IP address should be noted and reconciled by the staff as usual.

Audit results could be skewed by anyone with knowledge of the audit and access to the firewall. Audit subject, date and time pre-knowledge should be limited as much as possible to mitigate this problem. The Chief Technical Officer or Chief Security Officer and the auditor should be the only people aware of the audit plans.


**Conduct the Audit**

The audit will be performed from each network connected to the primary firewall.

On each network, an nmap scan is performed against the firewall itself, using OS fingerprinting and a SYN scan; it scans all ports (1-65227). This tells us if a stealth rule is in effect for all networks. IT personnel commonly open up access to the firewall to make support of the firewall easier.

Verify Rule 1
From the Internet
nmap –sS –O –p1-65535 1.100.215.66 -P0

```
     25/tcp      open          smtp
     264/tcp     open          bgmp
     265/tcp     open          unknown
     500/tcp     closed        isakmp
```

From the DMZ network
nmap –sS –O –p1-65535 192.168.9.1 -P0

```
25/tcp      open         smtp
264/tcp     open         bgmp
265/tcp     open         unknown
500/tcp     closed       isakmp
80/tcp      open         http
443/tcp     open         https
443/udp     open         https
20/udp      open      ftp-data
20/tcp      open      ftp-data
21/tcp      open      ftp
```

From the SubIntranet
nmap –sS –O –p1-65535 192.168.10.1 -P0

```
25/tcp      open         smtp
264/tcp     open         bgmp
265/tcp     open         unknown
500/tcp     closed       isakmp
80/tcp      open         http
443/tcp     open         https
443/udp     open         https
20/udp      open      ftp-data
20/tcp      open      ftp-data
21/tcp      open      ftp
```

From the Logging network
nmap –sS –O –p1-65535 192.168.12.1 -P0

```
25/tcp      open         smtp
264/tcp     open         bgmp
265/tcp     open         unknown
500/tcp     closed       isakmp
```

From the Internet network, with the firewall as the default gateway, scan all hosts
on the "legal" network.  This shows what systems are available to the world.

```
nmap -sP 1.100.215.0/24 -n
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Host  (1.100.215.67) appears to be up.
Host  (1.100.215.70) appears to be up.
Nmap run completed -- 256 IP addresses (2 hosts up)
scanned in 5 seconds
```

Check the laptop's ARP tables for firewall MAC address entries and compare
them against MAC addresses for systems for which the firewall should be
translating.

```
Arp -vn
Address                  HWtype  HWaddress
Flags Mask               Iface
1.100.215.34             ether   08:00:03:22:2A:8A   C
eth0
1.100.215.35             ether   00:02:FD:2A:69:80   C
eth0
1.100.215.33             ether   08:00:03:22:83:38   C
eth0
1.100.215.36             ether   00:01:96:AC:4E:80   C
eth0
1.100.215.42             ether   00:02:A5:0C:14:25   C
eth0
Entries: 5      Skipped: 0       Found: 5
```

From the Internet network, scan all of the IP addresses for which the firewall is responsible with a SYN scan (scan all ports).

```
Nmap -sS -p1-65535 1.100.215.66 -P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Interesting ports on  (1.100.215.66):
(The 65532 ports scanned but not shown below are in
state: filtered)
Port         State        Service

25/tcp      open         smtp
264/tcp     open         bgmp
265/tcp     open         unknown
500/tcp     closed       isakmp


Nmap -sS -p1-65535 1.100.215.68 -P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Interesting ports on  (1.100.215.68):
(The 65532 ports scanned but not shown below are in
state: filtered)
Port         State        Service

53/tcp      open         domain


Nmap -sU -p1-65535 1.100.215.68 -P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
```

(The 65532 ports scanned but not shown below are in
state: filtered)
Port        State        Service

53/udp      open         domain


Nmap –sS –p1-65535 1.100.215.69 –P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Interesting ports on  (1.100.215.69):
(The 65532 ports scanned but not shown below are in
state: filtered)
Port        State        Service

80/tcp    open         http
443/tcp   open         https


Nmap –sU –p1-65535 1.100.215.69 –P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Interesting ports on  (1.100.215.69):
(The 65532 ports scanned but not shown below are in
state: filtered)
Port        State        Service

443/udp   open         https


Nmap –sS –p1-65535 1.100.215.71 –P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Interesting ports on  (1.100.215.71):
(The 65532 ports scanned but not shown below are in
state: filtered)
Port        State        Service


Nmap –sU –p1-65535 1.100.215.71 –P0
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)
Interesting ports on  (1.100.215.71):
(The 65532 ports scanned but not shown below are in
state: filtered)
Port        State        Service

```
514/udp          open          syslog
```

These scans tells us what ports are open for the servers that we host, verifying Rules 2, 3, 9 and 10. Did SSH or telnet show up? If so, Rule 10 is open too wide. If not, it can be assumed to be in place or assumed that it was removed. (It would be better if it were removed.) Consider Rule 11 not in effect if basic services are open on systems (across subnets) that should otherwise be restricted.

On the Subintranet, DMZ and Logging networks, open a browser and connect to a random Web site on the Internet. The firewall should require authentication for each attempted connection. Verify Rule 4

On the Subintranet, DMZ and Logging networks, an ftp client is used to connect to a random ftp site on the Internet. The firewall should require authentication for each attempted connection. Verify Rule 5

From the Internet, use the Secure Client software to access the database servers (email, production and accounting), WWW and DNS. *(Note: I was unable to perform this scan, as I did not have proper licensing to recreate the VPN in my lab. I am providing the commands required to perform the scans as well as the expected results.)*

An nmap scan of all networks while connected with Secure Client should be performed. This help determines if any "leaks" are occurring via Secure Client connections. Verify Rule 6.

    Nmap –Ss 192.168.9.0/24
    Nmap –Ss 192.168.10.0/24

These scans should not get through.

    Nmap –Ss 192.168.11.0/24

This scan should report the following:

    For host 192.168.11.3:
    DNS UDP 53
    DNS TCP 53
    Lotus TCP 1352

    For host 192.168.11.2:
    FTP-Data TCP 20
    FTP TCP 21

    Nmap –Ss 192.168.12.0/24

Nmap –Ss 192.168.13.0/24

These scans should not get through.

Nmap –Ss 1.100.215.0/24

This scan should report the following:

For host 1.100.215.1:
FTP-Data UDP 20
FTP TCP 21
HTTP TCP 80
HTTPS TCP 443
VPN Topology TCP 264
VPN Key TCP 265
ISAKMP TCP 500

For host 1.100.215.68:
DNS TCP 53
DNS UDP 53
NTP TCP 123
NTP UDP 123

For host 1.100.215.69:
HTTP TCP 80 1.100.215.1
HTTPS TCP 443 1.100.215.1

During regular hours, perform an nmap scan of the GIAC, LLC, remote subnet.
Try the same scan during off hours. Lotus port should be open and available
during on-hours only (Firewall-1 VPN ports will be open at all times.) This
verifies Rules 7 and 8 including the time component.

Nmap –Ss 192.168.129.0/24


**Evaluate the Audit**

While performing the audit, I noticed the firewall rules did not allow for NTP or
DNS protocols properly. I made adjustments to the rulebase accordingly.

The following improvements could be made to improve security of the firewall.

The firewall is a single point of failure—a second firewall configured for high
availability mitigates the risk of the entire network going down due to a firewall
failure.

Also, a black box VPN could be added for improved performance and less reliance on single firewall.

A second logging server placed on a different network would improve logging reliability.

# Figure 9 - Network Diagram Based on Audit Results
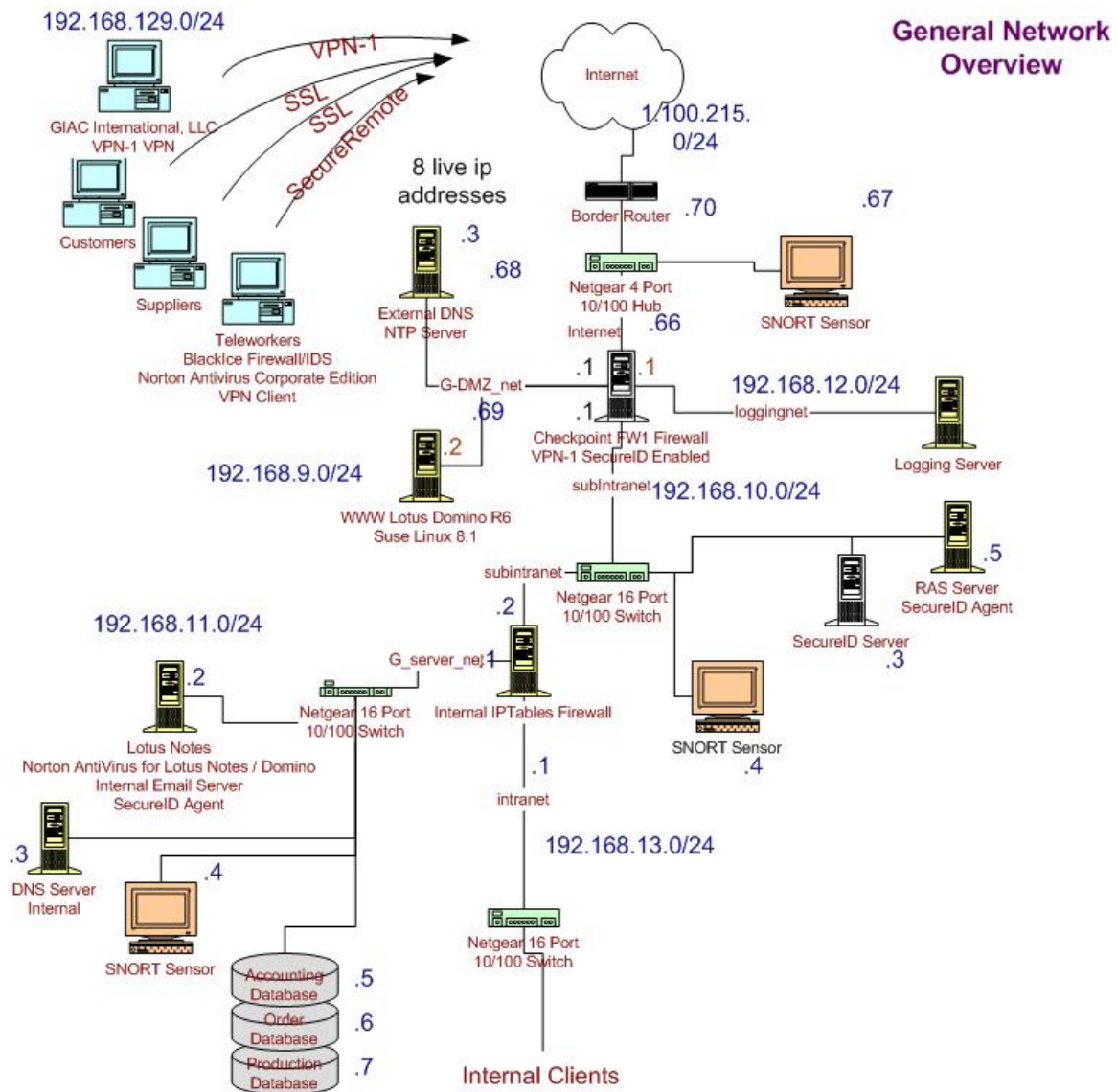
## Assignment 4

**Research and Design an Attack Against the Firewall**

Several steps are required to mount an attack against a firewall in a target network.  I will discuss the steps necessary detailing the attack itself.  Also, I will explain why it may or may not be successful.  The target network I have chosen belongs to Mike Bell. I have included a copy of his GIAC Enterprises network diagram here [Figure 9].  It can be found at the GIAC Web site at http://www.giac.org/practical/Mike_Bell_GCFW.doc .

**Figure 10 - Network Diagram from Mike Bell's GIAC Network Design**
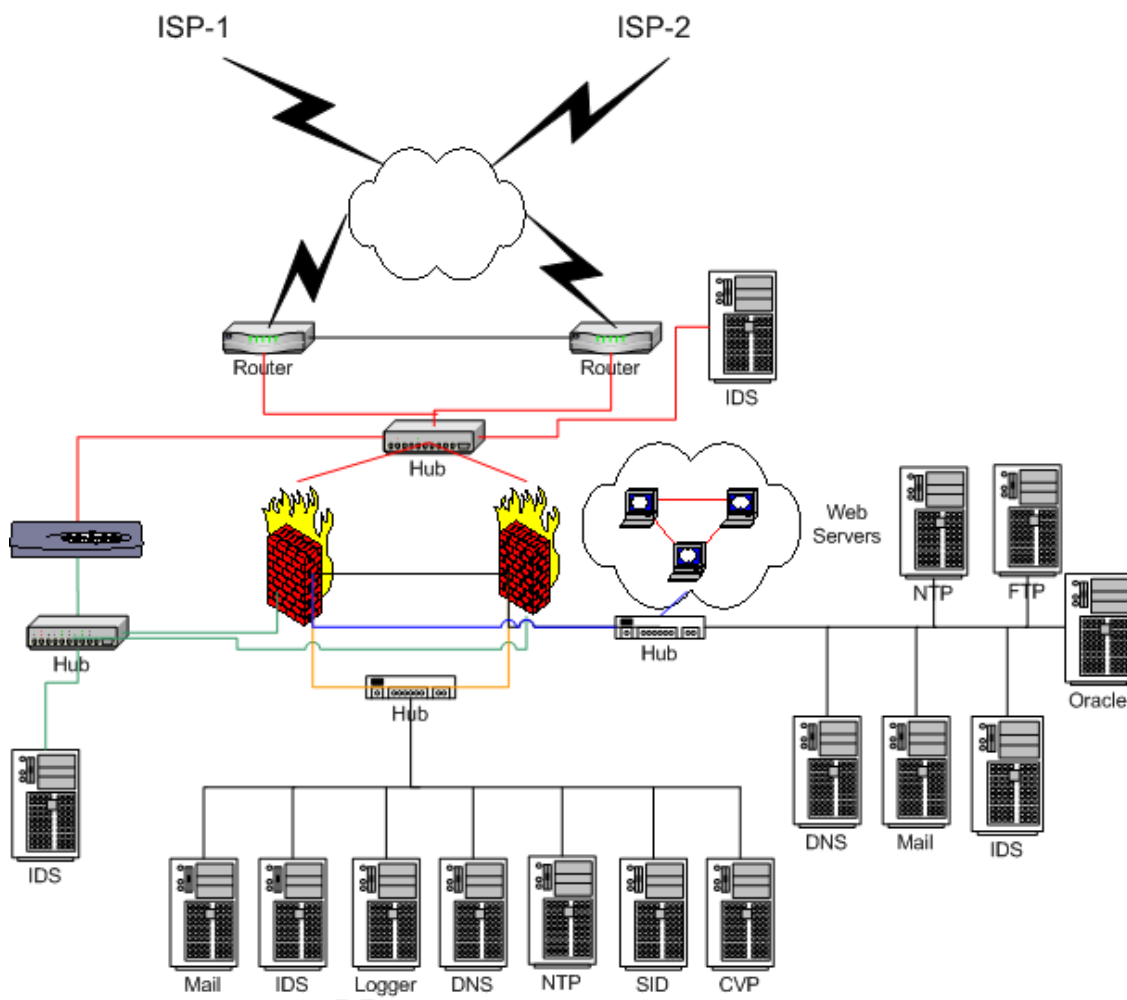


Due to lack of appropriate resources, I was unable to recreate the network as described in the diagram. Therefore, I have described likely scenarios based on analysis of his paper.

Once the target is identified, the first step in an attack is to get an idea of the target network's remote exposure. This can be achieved in many different ways. For instance, a modem program called a "War Dialer" can be used to determine if remote access servers are in use in the company's telephone number blocks. The dialer program simply calls each number in the list and logs the number if a computer answers. A phone call to the company receptionist posing as a new remote employee may yield some information regarding remote access telephone numbers or software in use, or at least lead the caller to a help desk or IT person.

On the other hand, the easiest and least risky method is likely a network scan of the target from the Internet. A tool like nmap can be used to determine the network address block in use, services available and hosts online.

In this case, an nmap network scan would reveal live hosts serving http and https but would not reveal the type of the firewall. The firewall is configured to implicitly drop all control connections coming from the Internet interface, then explicitly allow those connections required on the internal interfaces. Firewall-1 address translation (for assigning a legal IP address to a server behind the firewall) can be used as a fingerprint for remote firewall identification. It would not work here, as it requires ICMP echo replies for identification.

The most likely method for determining the firewall make and version information would be a phone call. A call to someone in the IT department posing as a vendor support person gathering some "groundwork" information might be all that's needed.

Once the firewall version and platform information is obtained, a search of the Internet should produce a number of exploits as well as code to actually perform the exploit. Exploit code is often provided under the pretense that a system administrator would want to determine if his/her own system is vulnerable.

The target firewall chosen for this portion of the practical is a Checkpoint Firewall-1 Version 4.1 Service Pack 6 running on a Sun Solaris High Availability Cluster. Available remote attacks against the Checkpoint Firewall 4.1 SP6 are few.

However, there are many attacks designed for the Checkpoint Firewall-1 product. As a market leader, it is the premiere target for exploit developers.

I have selected the Checkpoint Firewall-1 Valid Username vulnerability. .The vulnerability can be found at Securityfocus, bugtraq ID 1890, Common Vulnerabilities and Exposures (http://online.securityfocus.com/bid/1890/info/).

The Firewall-1 product responds to IKE Aggressive Mode login requests, regardless of how it was configured to respond. The vendor has issued a hot fix as of October 2002. The recentness of the hot fix release makes the attack a possibility. Many system administrators don't apply patches until they are thoroughly vetted or at least released in an office service pack roll-up.

This vulnerability provides the attacker with a positive response if a correct username has been guessed. Correctly identifying a user name provides us with 50% of the puzzle needed to authenticate to the firewall's VPN. Password guessing is typically quite easy once an avenue of attack is found. Once a valid

username (or set of usernames) is found, a password-guessing attack can be employed.

Success in the password-guessing attack depends largely on the use of strong passwords on accounts set up on the firewall used for VPN access.

A Google search of the Internet for exploit code yielded the following information from http://www.securitytracker.com/alerts/2002/Sep/1005175.html :

> To exploit the flaw, a remote user can send an IKE Phase-1 aggressive mode packet with the following payloads:
>
> a) ISAKMP Header
> b) SA - Containing one proposal with four transforms
> c) Key Exchange - DH Group 2
> d) Nonce
> e) Identification - Type ID_USER_FQDN, Value is Secure Client username

This provides us with all the information needed to craft our own tool. Perl would be a good candidate scripting language to use for the tool. It is highly portable, installed on virtually all Unix and Linux variations, and has many modules for use with network communications.

Considering that 50% of the attack depends on weak passwords and that I may be attempting to guess a password for the majority of the time spent on this avenue of attack, I decided to search a bit further for ready-made exploit code. Another Google search yielded more information about the selected exploit, including the name of a tool called "fw1-ike-userguess." This tool was used in the verification of the flaw but doesn't seem to be available.
http://www.securiteam.com/securitynews/5TP040U8AW.html

Once a tool has been created (or located), the discovery phase of the attack proceeds to account name recovery. The tool would likely need some sort of list of possible names to use to determine if they are valid usernames on the firewall. A review of the company's Web site should yield a few email names that can be traced to actual names. That information should provide the naming convention used for creating accounts. It is likely that email accounts are created with the same convention used on for the Firewall-1 accounts used for VPN access. For instance, if c.duerr@giac.com reaches Craig Duerr, we can surmise that Firewall-1 accounts for Craig Duerr are c.duerr also.

Once a positive list of valid accounts is gathered, the "tool" we have created or selected would then be employed to try to "guess" the password of those accounts.

There are some limiting factors involved in the attack. First, the firewall would need to employ IKE Aggressive Mode. Second, accounts created on the firewall would need to have fairly simple passwords. Third, the speed at which the brute force password-guessing attack can proceed is limited to the bandwidth and CPU power available.

The primary information gathering steps used in this attack can be fairly quiet. If account guessing is performed in a slow manner, it could be difficult to ascertain that an attack is underway. The password-guessing portion of this attack is extremely noisy. It would not take long to notice this attack is underway if firewall logs are reviewed regularly. The IDS would not likely pick up the attack.

### Conclusion

This attack would fail most likely because two-part authentication is being used. Hope rests in the possibility that accounts were created on the firewall for administrative use when the SecureID server was not in use.

### Denial Of Service Attack

The Distributed Denial Of Service (DDOS) attack chosen for this portion of the assignment was Tribe Flood Network (TFN). TFN operates using two separately installed components. The client program is tribe.c and the tribe daeom, td.c. The attacker remotely controls the client programs which, in turn, control the remote daemon programs.

The command line needed to start the attack is:

./tfn ip_list_of_tribe_daemons 2 www.giac.com 80

(Usage Information taken from http://www.defcon.tv/distributed/tfn.analysis.txt. )

This command tells Tfn to connect to the list of Tribe daemons using attack type 2 (for this particular binary attack, two is SYN flood) directed at www.giac.com on port 80. The results of this attack are a SYN flood overwhelming the target network as described by Mike Bell in his practical.

The firewall in the target network is configured with Checkpoint's "SYNDefender" option set for "SYN Gateway." This option allows the firewall administrator to limit sessions and reduce the timeout, thus protecting the server that is being attacked from exhausting its resources as it responds to the SYN flood. The firewall itself monitors the connection attempts and, once it determines the timeout value has been exceeded for a given connection, it sends a RST packet to the target server enabling it to immediately release its resources and go on servicing other requests.

The SYN Gateway configuration option comes at the slight cost of increased connection time to legitimate users. It won't prevent the upstream Internet gateway from becoming overloaded with traffic from the attackers. It also consumes some additional overhead on the firewall itself. Given a large enough pipeline from the Internet, the firewall can become overwhelmed with the SYN flood while still protecting the WWW server. Once all firewall resources are consumed with traffic (unlikely in this network based on Mr. Bell's estimate of bandwidth versus the firewall hardware in use), legitimate packets will be dropped.

A user monitoring the firewall's logs would notice the numbers indicating log entries are no longer contiguous and that the log entries are skipping (if the logging module responds at all).

SYN Defender is a good countermeasure to employ for general everyday use. Additional steps could be taken at the upstream ISPs to block the traffic.


**Attack an Internal System**

I selected the WWW servers as the target of my attack. I chose to attack the WWW server because exploits are numerous and typically pretty easy to find. Also, it is typically quite easy to get version information from a WWW server.

The first step in the attack is to gather information about the target. A search of Netcraft (at http://www.netcraft.com ) should show the operating system and http software version running on the site. I found Apache 1.3.27 running on the site's Web servers.

A search of Bugtraq (http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl ) for Apache, Version 1.3.27 yielded 5 possibilities.

Additionally, Whisker by Rain Forest Puppy (www.wiretrip.net/rfp/ ) could be used to provide information regarding scripts and directories accidentally left in place. Whisker gives specific vulnerability information where available. The command I ran was:

        whisker.pl -h www.giac.com 80 -l whisker.log –I 123456789

This command will crawl the Web site and report back any interesting details it finds. The "–h switch" indicates the host and port to scan, the "–l switch" ("l" as in log) indicates the log file name, the "–I switch" ("I" capital "I" as in Intrusion) indicates which IDS evasion techniques to use. I chose all the possible choices.

A likely exploit choice would be the "Multiple Apache HTDigest Buffer Overflow Vulnerabilities" found at http://online.securityfocus.com/bid/5993/info/.  No exploit code could be found for this problem at this time. To exploit this problem, a similar system would be set up using the same version operating system and Web server software. The development of a buffer overflow problem is well documented on the Internet.

Shell code is code that, once appended to the end of the data used to overflow a buffer in an attack, executes to provide some sort of entry into a compromised system.  For instance, shell code can be used to cause an Xterm window to open on the attackers computer from the compromised host.  Shell code for use in the exploit is also freely available.  One such source for both shell code and buffer overflow exploit development is http://www.shellcode.com.ar/en/docz.html ..


References

"RSA SecureID:RSA ACE/Agent for Lotus Domino." RSA Security | RSA ACE/Agent for Lotus Domino Technical Specs. http://www.rsasecurity.com/products/securid/techspecs/lotusnotes.html (October 10, 2002).

Rudenko, Innokenty. Cisco Routers for IP Routing. Scottsdale: The Coriolis Group, 1999.

Securiteam. "Checkpoint FW-1 VPN Security Flaw (updated)." http://www.securiteam.com/securitynews/5TP040U8AW.html (December 8, 2002).

SecurityFocus Online. "Vulnerabilities." SecurityFocus Home Vulns Archive. http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl (December 4, 2002).

SecurityTracker.com. "(Vendor Disputes Claim and Provides a Response) Re: Checkpoint." http://www.securitytracker.com/alerts/2002/Sep/1005175.html (December 8, 2002).

Sedalo, Matias. "Heap. Stack & Buffer Overflow." January 1, 2003. http://www.shellcode.com.ar/en/docz.html (December 9, 2002).

Stanislawski, David. "Firewalls, perimeter protection and VPN's Security Permiter Figure 1." SANS GCFW Practical assignment. Version 1.5E. http://www.giac.org/practical/David_Stanislawski_GCFW.zip (October 10, 2002).

Stout, Kent. "GIAC Certified Analyst (GCFW) Practical Assignment." Version 1.7. http://www.giac.org/practical/Kent_Stout_GCFW.doc (December 11, 2002).

Surla, Greg. "GIAC Certified Firewall Analyst Practical." Version 1.7.
http://www.giac.org/practical/Greg_Surla_GCFW.doc
(December 11, 2002).

Wagner, David. "Multiple Apache HTDigest Buffer Overflow Vulnerabilities."
SecurityFocus Home vulns. October 17, 2002.
http://online.securityfocus.com/bid/5993/info/ (December 4, 2002).

Welch-Abernathy, Dameon. "Ports used by FireWall-1 4.1 and earlier."
PhoneBoy's FireWall-1 FAQs. December 06, 2002.  http://www.phoneboy.com/
(December 12, 2002).