



# 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.

**SANS GIAC Certification  
Level 2 GCFW  
Firewalls, Perimeter Protection, and VPNs**

**Practical Assignment  
For  
Baltimore SANS 2001**

**Submitted By:**

**Kurt Koenigsknecht  
August 3, 2001**

## Table of Contents

<u>Assignment 1 – Design the Security Architecture</u>	3
<u>GIAC Enterprise Security Design</u>	4
<u>Security Architecture Planning Checklist</u>	5
<u>External Access Requirements</u>	5
<u>Other Services Requirements</u>	7
<u>Firewall and Network Infrastructure Requirements</u>	9
<u>Defense In Depth</u>	9
<u>Systems to Provide External Services</u>	12
<u>Systems to Provide Internal Services</u>	13
<u>Security Architecture Summary</u>	13
<u>Assignment 2 - Security Policy</u>	14
<u>Laboratory Environment Restrictions</u>	15
<u>Border router policy</u>	15
<u>Border Router Policy</u>	17
<u>Border Router Policy Overview</u>	17
<u>Entire Border Router Rule Base</u>	17
<u>Breakdown of Router Rulebase</u>	19
<u>Perimeter Firewall Policy:</u>	24
<u>Primary Firewall Rule Base Overview</u>	28
<u>Perimeter Firewall Entire Rule Base</u>	29
<u>Breakdown of Rulebase</u>	29
<u>NAT Rule Base</u>	35
<u>Assignment 3 - Audit Your Security Architecture</u>	37
<u>Overview of Assessment Purpose</u>	38
<u>Planning Phase</u>	38
<u>Technical Approach</u>	38
<u>Estimated Assessment Costs</u>	39
<u>Implement the Assessment</u>	40
<u>Perform Analysis</u>	54
<u>Assignment 4 - Design Under Fire</u>	55
<u>Firewall Attack</u>	56
<u>Denial of Service Attack and Counter Measures</u>	58
<u>Denial of Service Attack</u>	58
<u>Counter Measures</u>	59
<u>Other Counter Measures</u>	59
<u>Compromise of Internal System</u>	61
<u>References</u>	63

## Assignment 1 – Design the Security Architecture

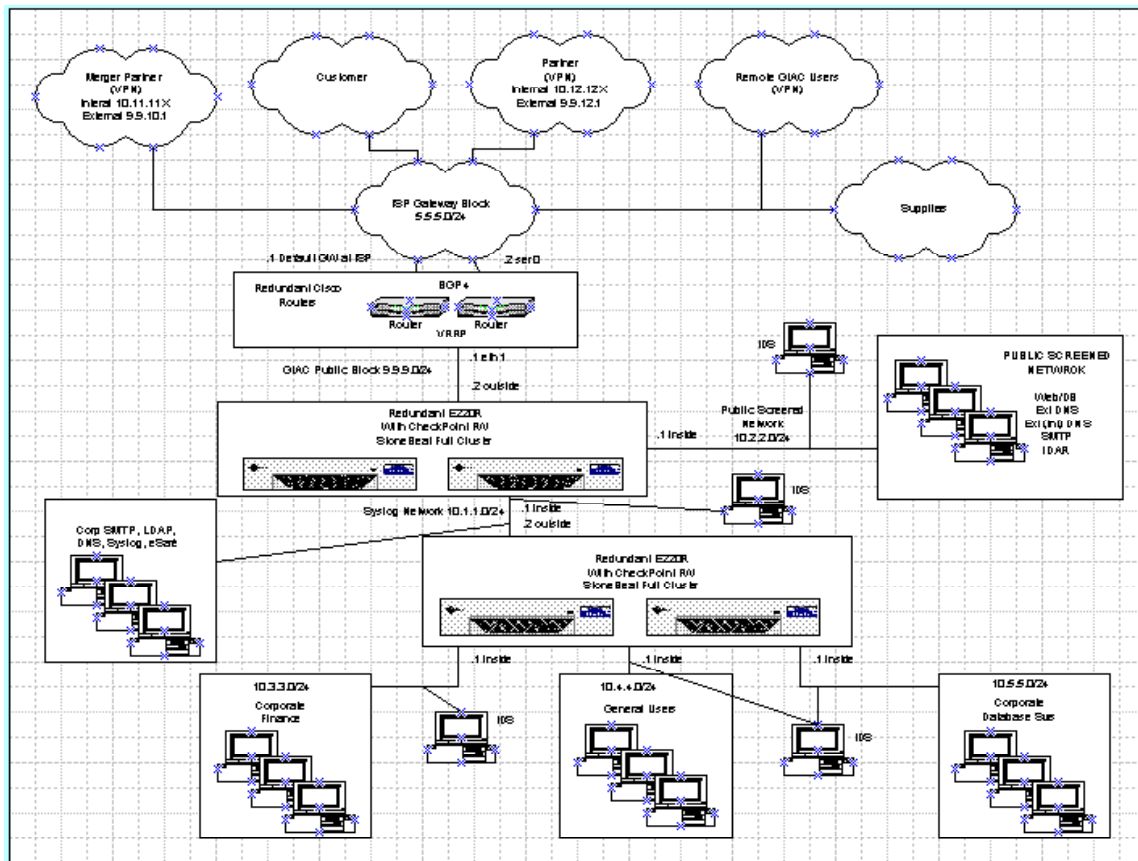
Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn \$200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access 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).

© SANS Institute 2000 - 2005, Author retains full rights.

## GIAC Enterprise Security Design



GIAC Enterprise Security Design  
Figure 1.

## Security Architecture Planning Checklist

The following information was gathered from GIAC Enterprises to assist in the development of the security architecture. The security architecture, see Figure 1, will be built around the business and technical requirements developed as a result of the planning checklist below.

### **External Access Requirements**

**Customers-** Will require inbound access via the Internet to purchase bulk online fortunes. Authentication will require each customer to establish a unique ID at the site. All orders will be placed electronically via a secure external Web server utilizing SSL. The orders will be processed and confirmation of each will follow with a reply encrypted electronic mail message. Those services that will be required are:

- TCP Port 80 To External Web
- TCP Port 443 to External Web
- TCP/UDP Port 53 to External DNS
- SMTP Port 25 to External SMTP (Encrypted with commercial PGP)

**Suppliers-** Will require inbound services via the Internet in order to supply the fortune cookie sayings to GIAC Enterprises. The expected deliveries are not large enough to justify using secure FTP services, thus encrypted electronic mail will be used. Using encrypted electronic mail provides the additional benefit of not opening FTP services through the firewall. Authentication will require each supplier to establish a unique ID at the site. Each supplier will complete delivery forms, via a secure external Web server utilizing SSL. The order process will generate an electronic ticket number, which will be used as a “delivery identifier”, for both parties to track the shipment from order to final delivery. All deliveries will be made via encrypted electronic mail. Those services that will be required are:

- TCP Port 80 to External Web
- TCP Port 443 to External Web
- TCP/UDP Port 53 to External DNS
- SMTP Port 25 to External SMTP (Encrypted with commercial PGP)

**Partners-** Who translate and resell the fortune cookie sayings will require access to the data stored in the corporate SQL database and secure external Web. SQL replication will be used to supply the partners with only the required database data needed rather than provide full access, by numerous systems, to the database. This allows GIAC to limit SQL traffic to just one DB server on

each end of the encrypted VPN. The secure Web access will be used to enter sales forecasts, complete sales orders, check inventory, track shipments, as well as, obtain other information. Authentication will require each partner to establish a unique ID at the site. Those services that will be required are:

- TCP Port 80 to External Web
- TCP Port 443 to External Web
- TCP/UDP Port 53 to External DNS
- SMTP Port 25 to External SMTP (Encrypted with commercial PGP)
- SQL replication between Partner and GIAC DB Svrs (Encrypted VPN)

**The Merger Partner-** The merger has been completed and the site will be considered an extension of the corporate LAN. An encrypted VPN will be established to allow only those services that are required. Those services that will be required are:

- TCP/UDP Port 53 to Corporate DNS Server (Encrypted VPN)
- SMTP Port 25 to Corporate Mail Server (Encrypted VPN)
- SQL Port to Corporate SQL Server (Encrypted VPN)

**Remote GIAC Users-** Will require services as if attached to the local LAN. An encrypted VPN will be created to allow those services that are required. Those services that will be required are:

- TCP/UDP Port 53 to Corporate DNS Server (Encrypted VPN)
- SMTP Port 25 to Corporate SMTP Server (Encrypted VPN)
- SQL to Corporate SQL Server (Encrypted VPN)

### ***Other Services Requirements***

**Border Router-** Will require services inbound to send data to the Syslog server. Those services that will be required are:

Syslog Port 514 to internal syslog server

**External DNS-** Will require outbound DNS services. DNS Zone transfers will be limited by configuration at the server level. Those services that will be required are:

TCP/UDP Port 53 to World

**External (Internal) DNS-** Will require outbound DNS services. DNS Zone transfers will be limited by configuration at the server level. The Corporate DNS server will require inbound DNS. Those services that will be required are:

TCP/UDP Port 53 to World

TCP/UDP Port 53 from Corporate DNS Server

**External SMTP-** Will require inbound services to the corporate mail server. Those services that will be required are:

SMTP port 25 from World

SMTP Port 25 to Corporate Mail Server

**Corporate SQL Server-** Will require inbound and outbound services to Merger Partner, Partners and Remote users. The Corporate SQL server will replicate read/only data to the Ext Web Server. Those services that will be required are:

SQL traffic to/from Merger Partner

SQL replication to/from Partner Site

SQL Traffic to/from Remote users

SQL replication to the Ext Web Server

**Internal DNS Server-** Will require services outbound to the external (Internal) DNS servers. DNS Zone transfers will be limited by configuration at the server level. Those services that will be required are:

TCP/UDP Port 53 to External Internal DNS

**Corporate E-mail Server-** Will require outbound SMTP services to the world and SMTP to/from the Merger Partner. Those services that will be required are:

SMTP Port 25 to World



SMTP Port 25 to Merger Partner

**Corporate Web/FTP Proxy-** Will require outbound HTTP, HTTPS and FTP services to the world. Those services that will be required are:

TCP Port 80 to World  
TCP Port 443 to World  
FTP Port 21 to World

**Syslog Server:** Will require logging from the border router to the syslog server. Those services that will be required are:

Syslog Port 514 Services from the Border Router

**Corporate LDAP Server:** LDAP authentication will be required for any corporate services that will be made available. The firewall will access the LDAP server via built in SSL connection of the Account Management Client. The Public Screened Network (PSN) will require LDAP authentication for the Web server. This will be done via the iPlanet Directory Access Router (IDAR) that contains only the required LDAP information for external authentication. The Corporate LDAP server will supply the data via a one-way SSL connection. Those services that will be required are:

LDAP-SSL Port 636 to iDAR

**PSN LDAP Server:** LDAP authentication will be required for any PSN services that will be made available. Those services that will be required are:

TCP Port 636 inbound from Corporate LDAP server.

## Firewall and Network Infrastructure Requirements

### *Defense In Depth*

The GIAC Enterprise security architecture will utilize what is commonly referred to as “Defense In Depth” or successive layers of defense for the entire enterprise, so that if one layer fails, others layers are still providing defenses. As each level of security is accessed a higher degree of access and authorization is enforced. These rights are granted through a combination of hardware and software defenses (i.e. router, firewalls etc...), as well as, a centralized directory architecture used for authentication.

The directory is leveraged by a challenge response system, which will be initiated by the firewall, application or web servers depending on the destination of the service. Digital certificates, as well as, two-part authentication can easily be integrated into the architecture should non-repudiation become a business requirement.

To ensure the integrity of what has been built and to reduce the risk that an attacker could disrupt network communications a complete architecture requires the use of an IDS (Intrusion Detection System) as an early warning and response mechanism. The IDS designated to provide for these capabilities covers the networks and server.

Every critical component in the path between service delivery and the Internet has been enhanced with redundancy to ensure that systems will have continuous availability.

Most systems can be configured to be highly available without clustering or HA software. All servers are built with the maximum hardware redundancy (i.e. power supplies, raid controllers) available by the system vendors. For the most critical systems that do require extremely high availability (i.e. Firewalls and Database servers) clustering and HA software will be implemented.

Providing reliable secure services, both external and internal, will require a combination of hardware and software products. The following systems and devices will be used in the security architecture:

**Border Router:** Cisco 4700 IOS 12.1, The Internet pathway is fronted with dual routers for Internet communications. This design provides the flexibility should GIAC Enterprise desire multi-homing functionality with two ISP's in the future.

**Internet Firewall:** Check Point Firewall-1/VPN-1, version 4.1 strong (3DES), service pack 4 (and sp4 hotfix-released July 9, 2001 for RDP Communication Vulnerability <http://www.checkpoint.com/techsupport/alerts/rdp.html> hosted on two Sun

Microsystems E220R's, HA and load balanced with Stonesoft Stonebeat FullCluster 2.0 Build 20, patched and hardened Solaris 7. Check Point Account Management Client to provide the connection to LDAP-SSL for authentication.

**Internal Firewall:** Check Point Firewall-1/VPN-1, version 4.1 strong (3DES), service pack 4 (and sp4 hotfix-released July 9, 2001 for RDP Communication Vulnerability), hosted on two Sun Microsystems E220R's, HA and load balanced with Stonesoft Stonebeat FullCluster 2.0 Build 20, patched and hardened Solaris 7. Check Point Account Management Client to provide the connection to LDAP-SSL for authentication.

**VPN:** Each site being considered for VPN access must first pass a GIAC Enterprises security audit before being granted permission to attach. The VPN's are then subject to reassessment quarterly. GIAC Enterprises reserves the right to perform audits on a more frequent intervals. Partners will provide GIAC Enterprises at least 30 days notice of any additional VPN connections that will be attached. All GIAC Enterprise VPN's require 3DES encryption.

**Firewall Management/IDS Console:** Check Point Firewall-1 Management Console Version 4.1 service pack 4 (and sp4 hotfix-released July 9, 2001 for RDP Communication Vulnerability), ISS Real Secure Console, hosted on Compaq DL580, patched and hardened Windows 2000.

**Content Scanning:** Three tiered approach will be used with each tier utilizing a different manufacture. This will help minimize any product vulnerabilities or lag time by any one manufacture in updating its tables.

- Aladdin Knowledge Systems, eSafe Mail Version 3.02
  - This system will act as the External SMTP relay and content scan inbound mail.
- Aladdin Knowledge Systems, eSafe Protect Gateway, Version 3.02, hosted on Compaq DL580, patched and hardened Windows 2000.
  - This will be used for scanning FTP and HTTP downloads
- Trend Micro AntiVirus on all Windows Servers
- Network Associates, Inc on all Windows Desktops

**Roaming User VPN Access:** Check Point SecureClient/SecuRemote, Version 4.1 Build 4185 will provide encrypted VPN, as well as Personal Firewall protection. All roaming users will utilize Windows 2000 Professional which will minimize administration and provide improved security over Windows98/WindowsNT 4.0.

**Cisco Systems Catalyst 3500 series XL:** The switches that will be used

throughout the enterprise are the Cisco Catalyst 3500 XL. The use of switches for the infrastructure will also reduce exposure to packet sniffers.

**IDS System:** The network IDS system will be ISS Real Secure Network Sensor 6.0 <http://www.iss.net> located on each of the internal subnets. The host based IDS, for critical servers, will be Tripwire for Servers 2.4 <http://www.tripwire.com> for both the Solaris and Windows environment.

**Syslog Server:** Windows 2000 server, host on Compaq DL580, patched and hardened.

**TCP/IP Scheme:** The private address range of 10.X.X.X will be used for the entire internal addressing scheme at GIAC Enterprises. Private address ranges are not routable over the Internet thus; utilizing the private addressing scheme along with Network Address Translation reduces the likelihood of successful spoofing of the network schema.

**Segmented Networks:** The use of a segmented network provides boundaries between disparate services, as well as, added protection for systems from other subnets by minimizing the types and amount of traffic flows. The segmented networks are as follows:

- Public Screened Network
  - External WEB/DB
  - External DNS
  - External Internal DNS
  - External SMTP
  - IDAR
- Buffer Zone Network
  - Corporate SMTP
  - Corporate LDAP
  - Corporate DNS
  - Corporate Syslog
  - Corporate eSafe
- Corporate Finance Network
  - Financial Systems
  - Finance Users
- General Users Network
  - General Users
- Corporate Database Server Network
  - Corporate Database Servers
  - Database Users

### **Systems to Provide External Services**

Providing services outside the corporate LAN will require the following systems and the associated services to be hosted and made available:

#### **External DNS**

ISC's BIND 9.1.2, hosted on two (primary and secondary) Sun Microsystems Netra t 1120's, Solaris 8, patched and hardened. DNS Zone transfers only allowed to secondary servers.

#### **External (Internal) DNS**

ISC's BIND 9.1.2, hosted on a Sun Microsystems Netra t 1120, Solaris 8, patched and hardened.

#### **External SMTP**

Aladdin eSafe Mail 3.0.2 build 71, hosted on a Compaq DL580, Windows2000 patched and hardened. The eSafe Mail software will provide content scanning at the Internet gateway, thus reducing the exposure to harmful content before it enters the enterprise network. Scanned mail is then relayed to the Corporate SMTP server.

#### **iDAR—PSN LDAP Server**

iPlanet Directory Access Router 2.1, hosted on Sun Microsystems E220R, Solaris 8, patched and hardened.

## **Systems to Provide Internal Services**

Providing services to the corporate LAN will require the following systems and the associated services to be hosted and made available:

### **Corporate Database Server**

Oracle 8.16, hosted on Veritas Clustered Sun Microsystems E220R's with each dual Fiber attached to a Hitachi 9200 Storage Array, Solaris 8, patched and hardened.

### **Internal DNS Server**

ISC's BIND 9.1.2, hosted on two (primary and secondary) Sun Microsystems Netra t 1120's, Solaris 8, patched and hardened. DNS Zone transfers only allowed to secondary servers.

### **Corporate E-mail Server**

iPlanet Messaging 4.15 sp6, hosted on Solaris 2.6 (Messaging 4.15 does not support Solaris 8), patched and hardened.

**Note:** When GIAC Enterprises migrates to iPlanet Messaging 5.X, Solaris 8 will be used.

### **Corporate Web/FTP Proxy**

iPlanet Web Proxy Server 3.6, hosted on Solaris 8, patched and hardened.

### **Corporate LDAP Server(s)**

iPlanet Directory Server 5.0, hosted on two (master and master replica) Sun Microsystems E220R's, Solaris 8, patched and hardened.

## **Security Architecture Summary**

The information provided was utilized to develop the security architecture. Each of the services required, inbound and outbound, will require specific hardware and software. The combined hardware and software will be used to create a security architecture based on two common conceptual designs.

- Defense in depth (i.e. layered security approach)
- The concept of least privilege (i.e. deny all, then allow only what is

required)

© SANS Institute 2000 - 2005, Author retains full rights.

## Assignment 2 - Security Policy

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 ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note 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.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.



Be certain to point out any tips, tricks, or "gotchas".

### **Laboratory Environment Restrictions**

Before the policies of the architecture designed are discussed, the author would like to make a few comments about the limitations in the lab environment.

GIAC Enterprises is a hypothetical company thus, the large amounts of equipment used in the design are as well. The lab environment used will duplicate as close as possible the architecture described in the previous section. Fortunately, the primary components, Cisco IOS and Check Point Firewall-1/VPN-1 products operate very similar regardless of the model of equipment they are implemented on. The lab environment was still able to duplicate the security policies with very minimal disconnect from the actual design. Although this is not ideal, the equipment limitations dictated the need to do this. Lab environment restrictions that require mentioning are as follows:

- The Cisco router used was a 1601R IOS version 12.0.
  - The policies will still reflect the technical and business requirements stated, just implemented to reflect the hardware available.
- The Perimeter and Internal firewall systems where collapsed into a single system. The Check Point Firewall-1/VPN-1 4.1 sp4 with RDP hotifx, host was a Sun Ultra5 running Solaris7 with a quad Ethernet card installed. The configuration provided only 5 Ethernet connections, thus the Buffer Zone Network equipment had to be moved to an alternate subnet. The equipment was moved to the "General Users" network for the purpose of demonstrating the buffer zone server polices that needed to be implemented<sup>1</sup>.
  - The policies will still reflect the technical and business requirements stated, just implemented in the collapsed environment to reflect the hardware available.

### **Border router policy**

The border router is the first line of defense for any access point to the Internet. Cisco provides routers that have a host of security features built into the IOS that should be utilized to the fullest extent possible. The router should be used not as a firewall but as a way to reduce the "noisy" traffic that attempts to enter the perimeter. This provides two benefits; the firewall will not have to reject known garbage traffic, the firewall will not have to log this activity, both of which should increase overall performance at the firewall.

---

<sup>1</sup> This does minimize the authors' view of the importance of having the Buffer Zone network, and its servers, segregated in the original design.

The Syslog feature will be enabled to log traffic to a centralized server. Logging and monitoring the logs is extremely important and must be used. Logs will be used first to provide proactive alerting to current activity and second to record activity should it be required for forensics at some later date.

The base line used for the Border router was recommendations for perimeter protection posted in the SANS Institute (<http://www.sans.org/>) Top 10 Most Critical Internet Security Threats (<http://www.sans.org/topten.htm>). The "Top Ten" list includes a section on Perimeter protection for an added layer of defense in depth. It is as follows:

1. Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
2. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
3. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
4. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 -- earlier ports plus 445(tcp and udp)
5. X Windows -- 6000/tcp through 6255/tcp
6. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
7. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
8. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
9. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
10. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

## ***Border Router Policy***

### ***Border Router Policy Overview***

The border router will be used to terminate “dirty” traffic before it reaches the perimeter firewall. It is important that the configuration be carefully implemented as to avoid denying services that are needed. Not all of the border router recommendations from the “Perimeter Protection” section posted in the SANS Institute Top 10 Most Critical Internet Security Threats (<http://www.sans.org/topten.htm>) will be implemented. Some of the recommendations will be implemented in the firewall policy rather than at the border router, these will be noted.

A complete snapshot of the entire rule base is shown below, the following text will provide a detailed breakdown.

#### ***Entire Border Router Rule Base***

```
service password-encryption

hostname Router

enable secret 5 $1$c/jK$RNMWB0JxW2TY/Lson2m5e.
enable password 7 030752180500

no ip finger
no ip bootp server
no ip source-route
no service tcp-small-servers
no service udp-small-servers
no snmp
no cdp enable

interface Ethernet0
 ip address 9.9.9.1 255.255.255.0
 ip access-group 16 in

interface Serial0
 ip address 5.5.5.2 255.255.255.0
 ip access-group 101 in

no ip classless

logging trap debugging
logging 10.1.1.3
```

```
ip route 0.0.0.0 0.0.0.0 5.5.5.1
ip route 10.1.1.0 255.255.255.0 9.9.9.2
ip route 10.2.2.0 255.255.255.0 9.9.9.2
ip route 10.3.3.0 255.255.255.0 9.9.9.2
ip route 10.4.4.0 255.255.255.0 9.9.9.2
ip route 10.5.5.0 255.255.255.0 9.9.9.2
```

```
access-list 16 permit 9.9.9.0 0.0.0.255
access-list 16 permit 10.1.1.0 0.0.0.255
access-list 16 permit 10.2.2.0 0.0.0.255
access-list 16 permit 10.3.3.0 0.0.0.255
access-list 16 permit 10.4.4.0 0.0.0.255
access-list 16 permit 10.5.5.0 0.0.0.255
access-list 16 deny any log
```

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny udp any any range 512 514 log
access-list 101 deny tcp any any range 512 514 log
access-list 101 deny udp any any eq 111 log
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 2049 log
access-list 101 deny tcp any any eq 2049 log
access-list 101 deny udp any any eq 4045 log
access-list 101 deny tcp any any eq 4045 log
access-list 101 deny udp any any range 135 139 log
access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any 445 log
access-list 101 deny tcp any any 445 log
access-list 101 deny udp any any range 6000 6255 log
access-list 101 deny tcp any any range 6000 6255 log
access-list 101 deny udp any any eq 69 log
access-list 101 deny tcp any any eq 117 log
access-list 101 deny tcp any any eq 514 log
access-list 101 deny tcp any any eq 515 log
access-list 101 deny tcp any any eq 1080 log
access-list 101 deny ip any host 10.1.1.3 log
access-list 101 deny udp any any eq 37 log
access-list 101 deny tcp any any eq 37 log
access-list 101 deny ip host 0.0.0.0 any log
access-list 101 permit ip any any
```

banner login / Warning: Authorized access only All violators are subject to

prosecution /

### **Breakdown of Router Rulebase**

**Recommendation 1**, Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses and block classless routes. Also block source routed packets. (**Please note:** Other sections of access-list 101 will be discussed later in the configuration.) This was accomplished with the following:

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log
no ip classless
no ip source-route
```

**Recommendation 2**, Block unused login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp). The NetBIOS port 139 will be addressed with recommendation 4. These services are highly exploitable therefore; if they are not used block them here or at the Internet firewall to prevent any occurrence of them. FTP, Telnet and SSH will be blocked at the Internet firewall. Under those conditions that require administration with services that are blocked, those services will be made available by the on staff security personnel in the 7 x 24hr operations center. This was accomplished with the following:

```
access-list 101 deny udp any any range 512 514 log
access-list 101 deny tcp any any range 512 514 log
```

**Recommendation 3**, Block RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp). Remote Procedure Call (RPC) and NFS are susceptible to exploits from RPC calls, so again since they are not used block them. This was accomplished with the following:

```
access-list 101 deny udp any any eq 111 log
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 2049 log
access-list 101 deny tcp any any eq 2049 log
access-list 101 deny udp any any eq 4045 log
access-list 101 deny tcp any any eq 4045 log
```

**Recommendation 4**, Block NetBIOS in Windows NT -- 135 (tcp and udp), 137

(udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445(tcp and udp). Yes, NetBIOS is NOT a secure service, under no circumstances will GIAC Enterprises allow NetBIOS services over the Internet connection. Due to the many default sharing configuration of the Windows platform, it is just too great a risk. This was accomplished with the following:

```
access-list 101 deny udp any any range 135 139 log
access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any 445 log
access-list 101 deny tcp any any 445 log
```

**Recommendation 5**, Block X Windows -- 6000/tcp through 6255/tcp. These services have been proven to have many vulnerabilities and again they will not be used so block them. This was accomplished with the following:

```
access-list 101 deny  udp any any range 6000 6255 log
access-list 101 deny  tcp any any range 6000 6255 log
```

**Recommendation 6**, Block Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp). This was accomplished with the following:

GIAC Enterprises will limit zone transfers to secondary servers via DNS configuration. External access to LDAP services will be blocked at the firewall. The firewall account management module will utilize SSL port 636 for secure authentication via LDAP.

**Recommendation 7**, Block Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp). This was accomplished with the following:

GIAC Enterprises will block these services at the Internet Firewall by limiting the public to the mail relay system only.

**Recommendation 8**, Block Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.) This was accomplished with the following:

GIAC Enterprises will block these services at the Internet Firewall by limiting Web—HTTP to the web servers TCP/IP addresses only.

**Recommendation 9**, Block "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp). This was accomplished with the following:

```
no service tcp-small-servers
no service udp-small-servers
access-list 101 deny  udp any any eq 37 log
access-list 101 deny  tcp any any eq 37 log
```

**Recommendation 10**, Block Miscellaneous-- TFTP (69/udp), finger (79/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), SOCKS (1080/tcp) and others. Many of these services are vulnerable to exploits and since they are not used they will be blocked. This was accomplished with the following:

```
access-list 101 deny udp any any eq 69 log
access-list 101 deny  tcp any any eq 117 log
access-list 101 deny  tcp any any eq 514 log
access-list 101 deny  tcp any any eq 515 log
access-list 101 deny  tcp any any eq 1080 log
no ip finger
no snmp
no cdp enable
no ip bootp server
```

#### **Other Border Router configuration settings:**

**Ethernet 0** is the inside address of the Border router and is configured as follows:

```
interface Ethernet0
ip address 9.9.9.1 255.255.255.0
ip access-group 16 in
```

**Serial Interface 0** is the external interface of the Border router and is configured as follows:

```
interface Serial0
ip address 5.5.5.2 255.255.255.0
ip access-group 101 in
```

**The Syslog Server.** This configuration setting enables and sends syslogs to 10.1.1.3. No external system is permitted access to the syslog server.

**Note:** Limitations in the lab environment require the syslog server to be moved to the 10.4.4.X network and be assigned the address of 10.4.4.3 for the audit phase of the practical.

```
logging trap debugging
logging 10.1.1.3
```

```
access-list 101 deny ip any host 10.1.1.3 log
```

Routing is completed with static routes only. The following configuration sets the default route to the ISP and creates static routes to all internal networks within GIAC Enterprises. Not using routing protocols greatly reduces the risk of having an unexpected route. By only statically creating routes, routing behavior can easily be determined.

```
ip route 0.0.0.0 0.0.0.0 5.5.5.1
ip route 10.1.1.0 255.255.255.0 9.9.9.2
ip route 10.2.2.0 255.255.255.0 9.9.9.2
ip route 10.3.3.0 255.255.255.0 9.9.9.2
ip route 10.4.4.0 255.255.255.0 9.9.9.2
ip route 10.5.5.0 255.255.255.0 9.9.9.2
```

**Access-list 16** permits only the GIAC Enterprise utilized TCP/IP ranges in to the Border router. This will prevent any unknown segments from being inserted into the network without the proper approval. Again, the behavior can easily be determined through this explicit deny of all networks other than those specified.

```
access-list 16 permit 9.9.9.0 0.0.0.255
access-list 16 permit 10.1.1.0 0.0.0.255
access-list 16 permit 10.2.2.0 0.0.0.255
access-list 16 permit 10.3.3.0 0.0.0.255
access-list 16 permit 10.4.4.0 0.0.0.255
access-list 16 permit 10.5.5.0 0.0.0.255
access-list 16 deny any log
```

**Access-list 101**, is used to implement the ACL recommendations discussed above. The last line is to permit anything not denied above.

**Note:** By default the Cisco access-list has an implied deny at the end of each list.

```
access-list 101 permit ip any any
```

**Banner login**, To provide warning and deterrent to those undesirables from entering the network, a warning message has been implemented. In reality GIAC Enterprises does not expect this to keep anyone from intruding on its network, its more of a legal formality to prove warning was given to anyone that might be prosecuted.

```
banner login / Warning: Authorized access only All violators are subject to
```



prosecution /

**Password protection**, The perimeter router is the most vulnerable component in the security architecture, limiting access to this device is critical. That has been done by using enable-secret passwords and passwords on the console and tcp ports.

© SANS Institute 2000 - 2005, Author retains full rights.

**Perimeter Firewall Policy:****Listing of applicable addresses used in the Firewall rulebase**

<b>Device Description</b>	<b>Private Address</b>	<b>Public Address</b>
Perimeter Router Ethernet	N/A	9.9.9.1/ 255.255.255.0
Firewall External Interface	N/A	9.9.9.2/ 255.255.255.0
PSN Network	10.2.2.0/ 255.255.255.0	N/A
Corp Fin Network	10.3.3.0/ 255.255.255.0	N/A
General Users Network	10.4.4.0/ 255.255.255.0	N/A
Corporate DB Network	10.5.5.0/255.255.255.0	N/A
Merger Partner Firewall	N/A	9.9.10.1/ 255.255.255.0
Merger Partner Subnet	10.11.11.0/ 255.255.255.0	N/A
Merger Partner DB Svr	10.11.11.3/255.255.255.0	N/A
Partner Firewall	N/A	9.9.12.1/ 255.255.255.0
Partner Subnet	10.12.12.0/ 255.255.255.0	N/A
Partner DB Server	10.12.12.3/255.255.255.0	N/A
All GIAC Subnets Hidden Address	N/A	9.9.9.2/ 255.255.255.0
Corporate Syslog Server	10.4.4.3/ 255.255.255.0	N/A
Corporate SMTP Server	10.4.4.4/ 255.255.255.0	N/A
Corporate DNS Server	10.4.4.5/ 255.255.255.0	N/A
Corporate DB Server	10.5.5.3/ 255.255.255.0	N/A
Corporate LDAP Server	10.4.4.6/ 255.255.255.0	N/A
Corporate eSafe Server	10.4.4.14/ 255.255.255.0	N/A
Web/FTP Proxy Server	10.4.4.15/ 255.255.255.0	9.9.9.15/ 255.255.255.0
External SMTP Server	10.2.2.4/ 255.255.255.0	9.9.9.4/ 255.255.255.0
External (Internal) DNS Svr	10.2.2.5/ 255.255.255.0	9.9.9.5/ 255.255.255.0
External IDAR	10.2.2.6/ 255.255.255.0	N/A

External Web Server	10.2.2.10/ 255.255.255.0	9.9.9.10/ 255.255.255.0
External DNS Server	10.2.2.11/ 255.255.255.0	9.9.9.11/ 255.255.255.0

When installing the firewall a few basic precautions should be taken during the installation of Check Point Firewall-1. While installing the software configure the system to:

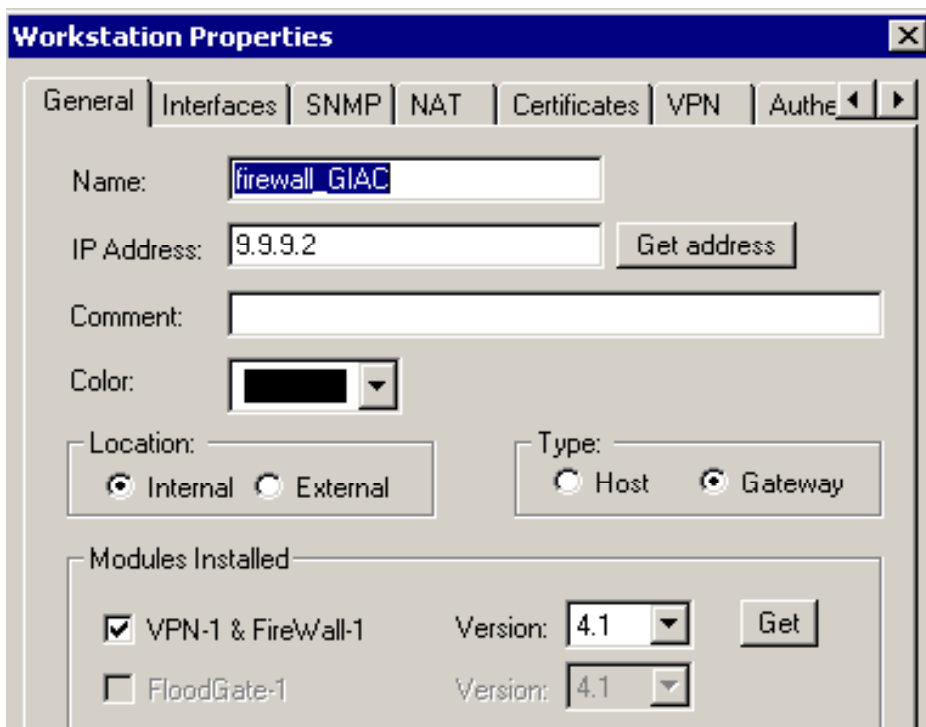
- Harden Solaris
  - The system was installed using the posting on SANS Information Security Reading Room, for Securing a Solaris Check Point Firewall located at [http://www.sans.org/infosecFAQ/firewall/solaris\\_check.htm](http://www.sans.org/infosecFAQ/firewall/solaris_check.htm) Title and author listed below:
    - **Securing a Solaris Check Point Firewall**  
Lee R. Baker  
March 11, 2001
  - Use only static routes, configure the system to NOT be router.
    - Configure /etc/defaultrouter, this will prevent the system from becoming a router. All additional routes will be done with static route.
    - “touch” /etc/notrouter
- Install CheckPoint 2000 Firewall-1 sp4 with hotfix-released July 9, 2001 for RDP Vulnerability, <http://www.checkpoint.com/techsupport/alerts/rdp.html>. Install the Account Management Client to enable LDAP-SSL connectivity. A few notes worth mentioning while installing the firewall software:
  - When Configuring IP Forwarding disable it at boot time.
    - This causes the firewall to fail closed. If the firewall software is not running the system will NOT forward packets. Failing closed is always the rule of thumb.
  - Confirm that “Accept ICMP” is not enabled.
    - This will help with disabling “PINGING” through the firewall.
  - No Configuring for SNMP Extension
    - The SNMP protocol was never designed to be a secure protocol and thus should not be used on the firewall. The risks far out way any benefits that SNMP could bring to the enterprise.
  - Enable SYN Defender “SYN Gateway” in the Firewall properties
    - This will protect against SYN attacks

- Install the Account Management Client (LDAP module)
  - Enable LDAP account management in the Firewall properties
  - Allows LDAP to be used for secure (SSL port 636) authentication at the firewall.
- Log implied rules
  - Check Point recently has done a much better job with not “enabling” functions such as “Accept ICMP” and “Accept Domain Name queries” by default. Always check what is enabled with the “implicit rules” and log them to avoid confusion.
- View the implied rules now and after any changes made to the rule base.
  - This will help avoid the unexpected.
- Automate “logswitch” to keep logs manageable.
  - Create cron scripts to logswitch
  - Create cron script to comma delimited format the file.
    - This will provide an excel ready file for review.
    - This will also keep the log size manageable.

The Internet firewall gateway configuration and implemented security policy are as follows:

**Workstation Properties**, defines the system name, External TCP/IP address and the software and version of the firewall installed.

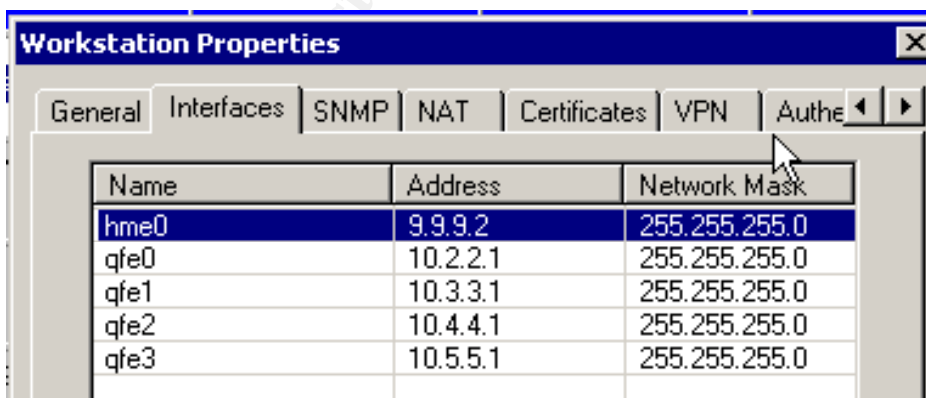
**Note:** It is very important that the external address of the firewall be defined as the primary firewall object. The Check Point license is linked to this address and according to Check Point secure remote functionality will fail should the external address not be the license holder.



Interfaces Tab, defines the systems interfaces, TCP/IP address and netmasks.

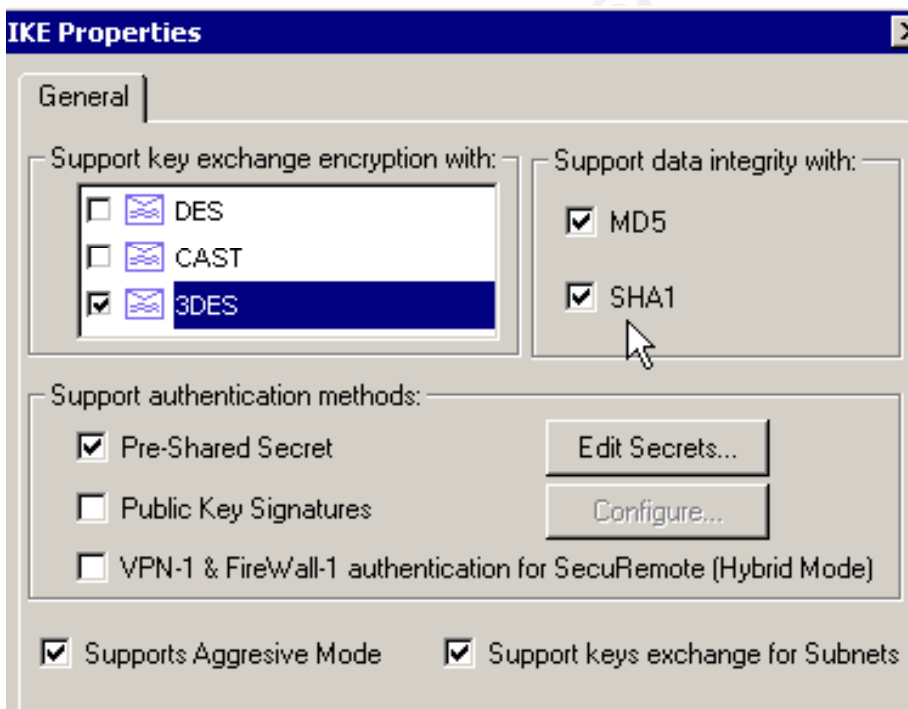
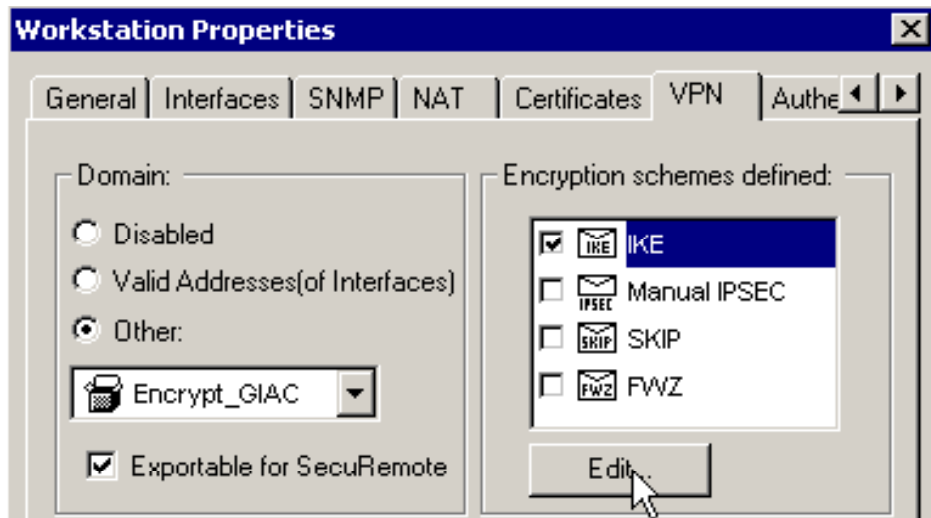
**Note:** The Primary and Internal Firewalls have been collapsed into a single unit for the Security Policy phase of this paper.

**Note:** GIAC Enterprise has implemented anti-spoofing at the perimeter router. Another option would have been to implement it at the Internet Firewall interfaces. Check Point does provide anti-spoofing capabilities at this level of the configuration.



VPN Tab, defines the Encryption domain that will be used for the VPN connections to the Merger Partner, Partner and SecuRemote user networks. The Isakamp/Oakley (IKE)

encryption scheme with 3DES with a MD5 was chosen for the site-to-site VPN's. This Check Point "supported" yet publicly available encryption provides a very secure robust algorithm. This is in sharp contrast to FWZ, which is Check Points proprietary offering. GIAC Enterprises believes IT security needs are better served by not using proprietary offerings that cannot be fully reviewed/tested by outside expertise.



### **Primary Firewall Rule Base Overview**

The rule base has been implemented to reflect two primary criteria. First, implement the rules in the most secure manor possible (i.e. Place the "Stealth" rule as close to the top as possible and not using "Any" for the source and destinations. Second, place rules in a

descending order with the most widely used rules first. Check Point utilizes a sequential methodology for matching rules, performance will be best if the most actively used rules are closer to the top.

It is recommended that comments be included on each rule. Documentation, although sometimes tedious to create, will help avoid possible confusion at some later date.

A complete snapshot of the entire rule base is shown below, the following text will detail the purpose of each rule.

### Perimeter Firewall Entire Rule Base

No.	Source	Destination	Service	Action	Track	Install On	Time	
1	firewall_Merger_Partner firewall_Partner	firewall_GIAC	ISAKMP	accept	Long	Gateways	Any	Key Exch
2	firewall_GIAC	firewall_Merger_Partner firewall_Partner	ISAKMP	accept	Long	Gateways	Any	Key Exch
3	GIAC_Corp_DB Partner_Corp_DD	GIAC_Corp_DB Partner_Corp_DD	sqlnet1 sqlnet2	Encrypt	Long	Gateways	Any	Encrypt S
4	Encrypt_Merger_Partner Encrypt_GIAC	Encrypt_GIAC Encrypt_Merger_Partner	sqlnet1 sqlnet2 smtp dns	Encrypt	Long	Gateways	Any	Encrypt S Allow DN
5	GIAC_Remote_Users@Any	GIAC_Corp_DB GIAC_Corp_DNS GIAC_Corp_SMTP	sqlnet1 sqlnet2 dns smtp	Client Encrypt	Long	Gateways	Any	Allow GIA Need to m
6	Any	firewall_GIAC	Any	drop	Long	Gateways	Any	Stealth th
7	Ext_SMTP Net_10_3_3_0 Net_10_4_4_0 Net_10_5_5_0	GIAC_Corp_SMTP	smtp	accept	Long	Gateways	Any	Allow SM Allow cle
8	Net_10_3_3_0 Net_10_5_5_0	GIAC_Corp_Proxy	ftp http https	accept		Gateways	Any	Client acc Logging is
9	GIAC_Corp_Proxy	GIAC_Internal_Nets	https http->HTTP_esafe ftp->FTP_esafe	accept		Gateways	Any	Outbound HTTP Outbound HTTP
10	GIAC_Corp_SMTP	GIAC_Internal_Nets	smtp	accept	Long	Gateways	Any	Allow Corp SM
11	GIAC_Internal_Nets	Ext_SMTP	smtp	accept	Long	Gateways	Any	Outside world :
12	GIAC_Internal_Nets	Ext_DNS	domain-udp	accept	Long	Gateways	Any	Outside world : with DNS serve
13	GIAC_Internal_Nets	Ext_Web	http https	accept	Long	Gateways	Any	Outside acces
14	Ext_DNS Ext_Int_DNS	GIAC_Internal_Nets	dns	accept		Gateways	Any	Allow external No need to log
15	GIAC_Corp_DNS	Ext_Int_DNS	dns	accept		Gateways	Any	Allow internal No need to log
16	GIAC_Brdr_Rtr	GIAC_Corp_Syslog	udp_syslog	accept	Long	Gateways	Any	Allow Syslog tr
17	GIAC_Corp_LDAP	PSN_LDAP_IDAR	ldap-ssl	accept	Long	Gateways	Any	Allow Corp LD
18	Net_10_3_3_0 Net_10_5_5_0	GIAC_Corp_LDAP	ldap-ssl	accept	Long	Gateways	Any	Allow corp cle
19	GIAC_Corp_DB	Ext_Web	sqlnet1 sqlnet2	accept	Long	Gateways	Any	
20	Any	Any	Any	drop	Long	Gateways	Any	Anything not e

### Breakdown of Rulebase

## Rule 1 & 2

The following two rules are used to allow for the key exchanges among the VPN's. The rules could have been combined into one rule but was decided against to avoid any possibility that the Merger Partner and Partner might have data communications between them through our channels.

firewall_Merger_Partner firewall_Partner	firewall_GIAC	ISAKMP	accept	Long	Gateways	Any	Key Exchange
firewall_GIAC	firewall_Merger_Partner firewall_Partner	ISAKMP	accept	Long	Gateways	Any	Key Exchange

## Rule 3

This following rule allows the VPN replication to/from the Partner DB server and the GIAC Corporate DB Server. This method, one to one replication, was chosen over allowing multiple clients (i.e. multiple IP addresses) access to the GIAC Corporate DB server. Replication will also provide control over which data will be replicated instead of exposing the entire database system.

GIAC_Corp_DB Partner_Corp_DB	GIAC_Corp_DB Partner_Corp_DB	sqlnet1 sqlnet2	Encrypt	Long	Gateways	Any	Encrypt SQL
---------------------------------	---------------------------------	--------------------	---------	------	----------	-----	-------------

## Rule 4

The following rule provides the Merger Partner with VPN access to only those services necessary to perform day-to-day business with GIAC Enterprises. Although GIAC Enterprises does consider the Merger Partner completely friendly the policy of providing only those service necessary is applicable. The required services will be reviewed on regular intervals, as well as, case by case as necessary to determine a modification of this policy. This rule provides the Merger Partner with SQL, SMTP and DNS services.

Encrypt_Merger_Partner Encrypt_GIAC	Encrypt_GIAC Encrypt_Merger_Partner	sqlnet1 sqlnet2 smtp dns	Encrypt	Long	Gateways	Any	Encrypt SQL Allow DNS a
----------------------------------------	----------------------------------------	-----------------------------------	---------	------	----------	-----	----------------------------

## Rule 5

The following rule provides GIAC Enterprise roaming users with VPN access to those services that are necessary. Again, although these users are considered to be friendly the policy of providing only those services necessary is applicable. The users will also have access to the PSN services like the general public. The required services will be reviewed on regular intervals, as well as, case by case as necessary to determine a modification of this policy. This rule provides the roaming users with SQL, SMTP and DNS services.

GIAC_Remote_Users@Any	GIAC_Corp_DB GIAC_Corp_DNS GIAC_Corp_SMTP	sqlnet1 sqlnet2 dns smtp	Client Encrypt	Long	Gateways	Any	Allow GIAC Need to moc
-----------------------	-------------------------------------------------	-----------------------------------	----------------	------	----------	-----	---------------------------



## Rule 6

The following rule is known as the “Stealth Rule”. The firewall gateway will be hidden from the outside world. The ISAKMP and Encryption rules must come before the Stealth rule to allow for encryption and key exchanges to take place. The Stealth rule drops all connectivity attempts without reply. This rule should be as close to the top of the rule base as possible to prevent unwanted access to the firewall gateway.



## Rule 7

The following rule provides SMTP access to the Corporate SMTP server from the PSN network, as well as, the local subnets so clients can retrieve mail. Not exposing the primary SMTP gateway to the outside world significantly reduces the risk of exploitation.



## Rule 8

The following rule provides the GIAC clients with access to the Corporate Proxy server. The Proxy Server resides on the 10.4.4.0 network, thus including that network was not necessary. The Proxy server then provides access to the Internet for those requesting clients.



## Rule 9

The following rule provides the GIAC Corporate Proxy with HTTP/HTTPS and FTP to the outside world (i.e. Not the GIAC subnets). This as opposed to having “Any” as a destination that unnecessarily provides internal GIAC subnets access. This follows the policy of providing only those services that are needed. The Proxy server is the mechanism used by all GIAC users to gain access to the Internet for those services. The HTTP and FTP downloads are scanned for harmful content by the eSafe Protect Gateway. Logging is done at the Proxy server, thus logging is not necessary.



## Rule 10

The following rule provides SMTP outbound only for the Corporate SMTP mail sever. Providing outbound SMTP services are a necessity yet poses very little risk to the server.



## Rule 11

The following rule provides those not part of GIAC Enterprise SMTP access to the external SMTP gateway. This as opposed to having “Any” as a source that unnecessarily provides internal GIAC subnets access. This follows the policy of providing only those services that are needed.



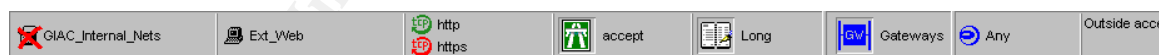
## Rule 12

The following rule provides those not part of GIAC Enterprise DNS access to the external DNS server. This as opposed to having “Any” as a source that unnecessarily provides internal GIAC subnets access. This follows the policy of providing only those services that are needed. Zone transfers are limited to secondary servers by DNS server configuration.



## Rule 13

The following rule provides those not part of GIAC Enterprise HTTP/HTTPS access to the external WEB server. This as opposed to having “Any” as a source that unnecessarily provides internal GIAC subnets access. This follows the policy of providing only those services that are needed.



## Rule 14

The following rule provides the external/external internal DNS servers DNS access to the outside world. This as opposed to having “Any” as a destination that unnecessarily provides access to internal GIAC subnets. This follows the policy of providing only those services that are needed. Logging is not necessary for simple DNS queries.



## Rule 15

The following rule provides the Corporate DNS server DNS access to the External Internal DNS server. This rule provides the Corporate DNS server the ability to fulfill

those DNS queries it directly wasn't able to. Logging is not necessary for simple DNS queries. Zone transfers are limited to secondary servers with DNS server configuration.

 GIAC_Corp_DNS	 Ext_Int_DNS	 dns	 accept		 Gateways	 Any	Allow interne No need to lo
-------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------	--	----------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------	--------------------------------

## Rule 16

The following rule provides the border router with the ability to send its Syslog data to the Corporate Syslog server. The Syslog server contains vital data and should be protected by limiting access from only the border router.

**Note:** The amount of traffic generated by syslog will be monitored to determine if its placement in the rulebase is appropriate.

 GIAC_BrdR_Rtr	 GIAC_Corp_Syslog	 syslog	 accept	 Long	 Gateways	 Any	Allow Syslog
-------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------	--------------





## Rule 17

The following rule provides the Corporate LDAP server SSL services to the PSN LDAP IDAR server. The Corporate LDAP server feeds the IDAR server with only the required LDAP data necessary for authentication. The IDAR server then provides that data to the PSN servers via SSL as needed. This secures the Corporate LDAP server while allowing for a unified user database for all GIAC users, as well as, those doing business with GIAC.

 GIAC_Corp_LDAP	 PSN_LDAP_IDAR	 ldap-ssl	 accept	 Long	 Gateways	 Any	Allow Corp t
----------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------	--------------

## Rule 18

The following rule provides the GIAC subnets with LDAP services over SSL for authentication. This again, protects the Corporate LDAP server while providing the necessary services to the unified user database.

 Net_10_3_3_0	 Net_10_5_5_0	 GIAC_Corp_LDAP	 ldap-ssl	 accept	 Long	 Gateways	 Any	Allow corp clie
--------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------	-----------------

## Rule 19

The following rule provides the GIAC Corporate Database server, address 10.5.5.3, the ability to replicate a read/only copy of the database to the External Web Server.



## Rule 20

Finally, the “Clean Up” rule. This rule is used to deny all services that are not specifically allowed in the above rule base. Logging this rule is especially important as it becomes a record that will show unauthorized attempts made. In addition this can become a valuable trouble shooting tool when services don’t perform as expected.



**Note:** Don’t forget to intermittently review the implied rule base for those rules that aren’t so obvious.

© SANS Institute 2000 - 2005, Author retains full rights.

## NAT Rule Base

No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	GIAC_Internal_Nets	GIAC_Internal_Nets	Any	Original	Original	Original
2	Ext_DNS	Any	Any	Ext_DNS (Valid Address)	Original	Original
3	Any	Ext_DNS (Valid Address)	Any	Original	Ext_DNS	Original
4	Ext_Int_DNS	Any	Any	Ext_Int_DNS (Valid Address)	Original	Original
5	Any	Ext_Int_DNS (Valid Address)	Any	Original	Ext_Int_DNS	Original
6	Ext_SMTP	Any	Any	Ext_SMTP (Valid Address)	Original	Original
7	Any	Ext_SMTP (Valid Address)	Any	Original	Ext_SMTP	Original
8	Ext_Web	Any	Any	Ext_Web (Valid Address)	Original	Original
9	Any	Ext_Web (Valid Address)	Any	Original	Ext_Web	Original

**Note:** By default Firewall-1 will NAT all networks, with NAT enabled, anytime packets pass through firewall interface. This can cause problems with servers that limit access by client IP addresses. The NAT configuration has been manually modified to reflect NO NAT from internal nets to internal nets (see NAT rule one).

The firewall OS requires that static routes and arp's be created to allow the static NAT rules to work as expected.

### Routes and arp's

The Routes and arp's used in this Solaris implementation are as follows:

```
route add 9.9.9.4 10.2.2.4 1
```

```
arp -s 9.9.9.4 8:0:20:b5:7b:0e pub
```

```
route add 9.9.9.5 10.2.2.5 1
```

```
arp -s 9.9.9.5 8:0:20:b5:7b:0e pub
```

```
route add 9.9.9.10 10.2.2.10 1
```

```
arp -s 9.9.9.10 8:0:20:b5:7b:0e pub
```

```
route add 9.9.9.11 10.2.2.11 1
```

```
arp -s 9.9.9.11 8:0:20:b5:7b:0e pub
```

© SANS Institute 2000 - 2005, Author retains full rights.