Global Information Assurance Certification Paper

SCOTT BAKER -SANS –GCFW-TRACK 2 – PERIMETER PROTECTION AND VIRTUAL PRIVATE NETWORKS PRACTICAL ASSIGNMENT VERSION 1.6a

Prepared by Scott Baker
11-13-2001

ASSIGNMENT ONE:

ASSIGNMENT # 1 - Scott Baker - Security Architecture Assumptions:

GIAC Enterprises is not under any budget constraints. They have outgrown their current network, which sets behind one firewall on a 10 Megabit flat network. This design is lacking in performance and security and they want a new secure design that will accommodate growth.

BUSINESS NEEDS:
GIAC has provided the following access requirements for their business.

- Customers who purchase bulk online fortunes. These customers will use HTTPS/SSL over the Internet to connect to a transactional database in the Secure Net.

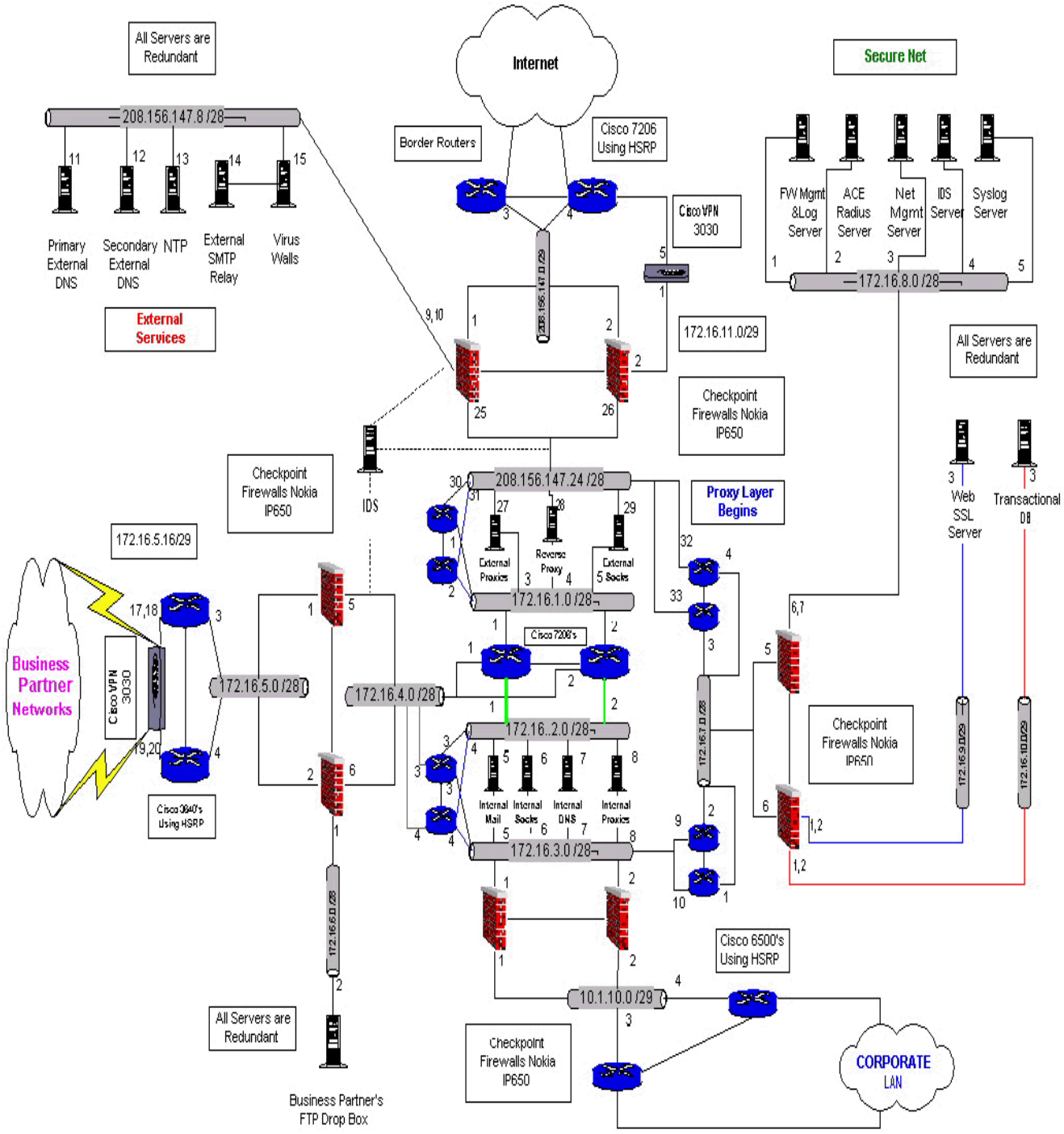
- Suppliers who supply the fortune sayings. These suppliers/ business partners will use a VPN to connect to GIAC and SFTP to transmit the bulk data to a FTP Drop Box, which will be monitored by the Transactional Database and automatically be transferred over via SFTP following an electronic receipt to the supplier.

- International partners who translate and resell fortunes will use a VPN to connect to GIAC. They will pick up their data from the business partner FTP server using SFTP and the transaction will be recorded by Business Partner name, time, filename, and file size. The transaction will then be recorded in the transactional database for billing.

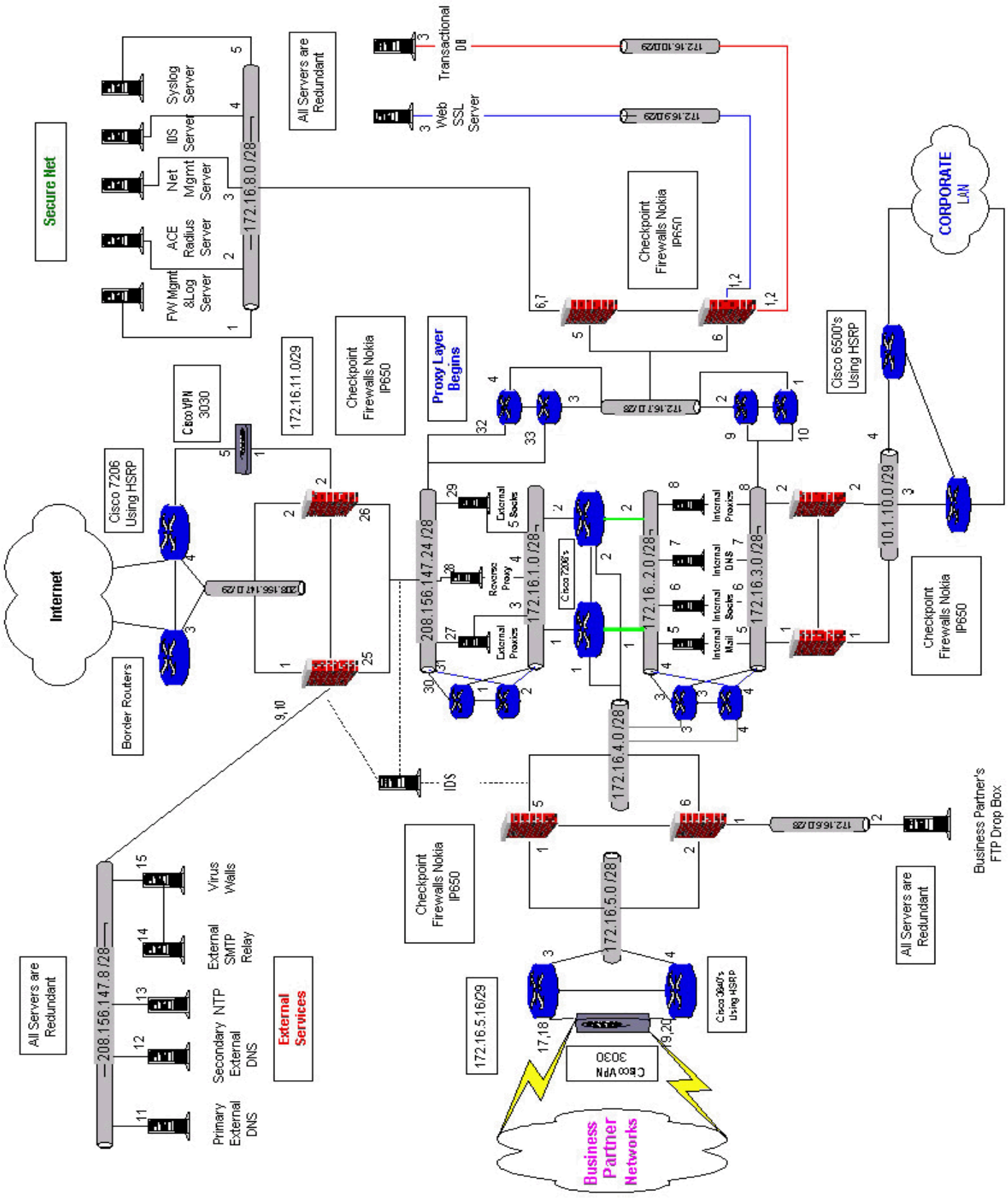
- GIAC Employees located on GIAC's internal network will use the secure proxy layer to connect externally. When connecting internally from home or another ISP a Cisco 3030 VPN concentrator will be used. The customer will run client software to connect to the network using IPSec. These devices and methods will be described below.

DIAGRAM OF GIAC ENTERPRISES SHOWN ON NEXT PAGE

Two drawings are provided. One 8 ½ x `11 and a smaller image 8 x 8 for easier viewing within the document.

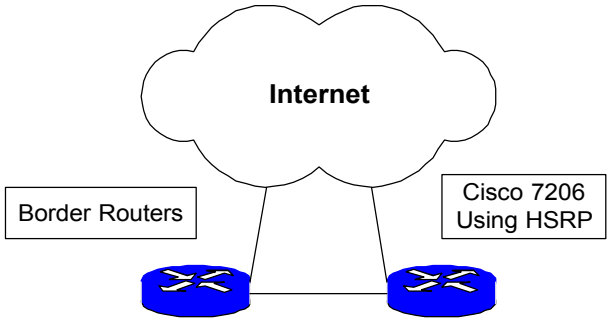


GIAC CORPORATE NETWORK DIAGRAMS



DEVICE DESCRIPTIONS

BORDER ROUTER:



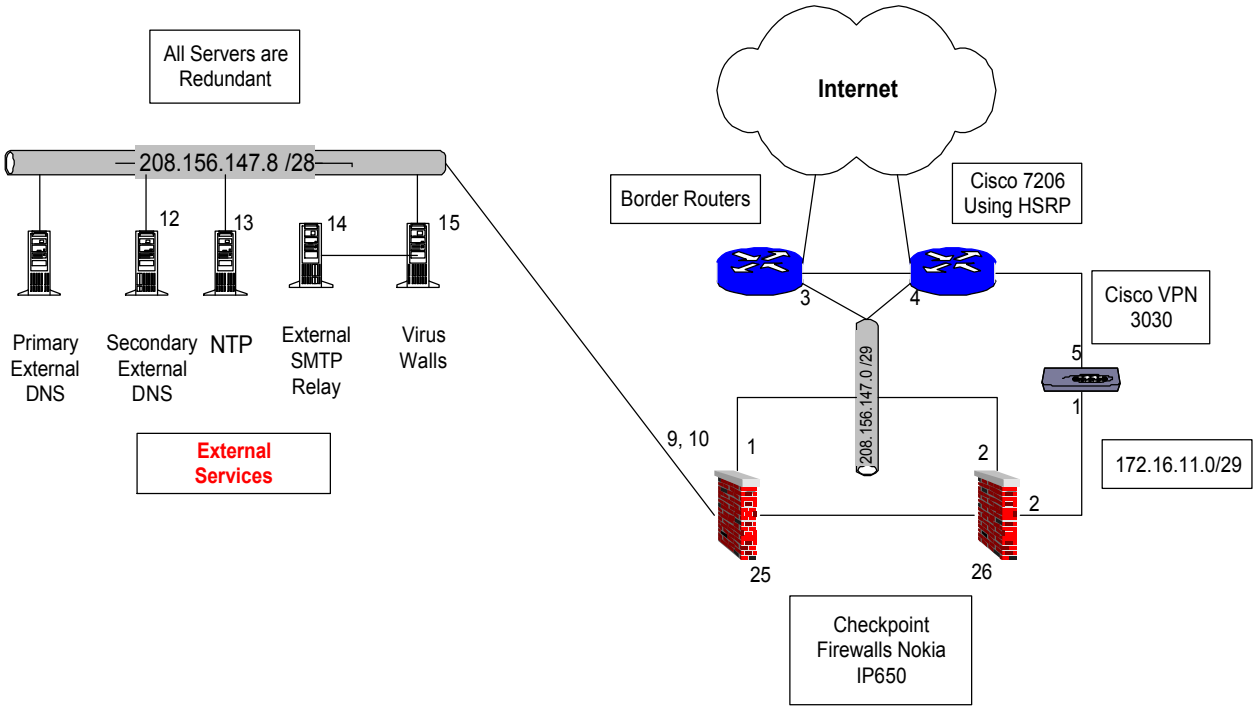
The border router will be a pair of Cisco 7206's for fail over HSRP will be used. configured with a minimal amount of rules. This is a high performance router and was chosen because of the high volume of internet traffic within the company. Because the internet portion of the business is growing rapidly, this router was chosen to incorporate the growth of the company. They key features and benefits taken from Cisco's site at http://www.cisco.com/warp/public/cc/pd/rt/7400rt/ are listed below.

Key Features and Benefits

Feature	Benefit
1 rack unit (RU) form factor with front-to-back airflow and single port adaptor slot	Dramatically reduces the needed amount of costly rack space and increases processing performance per rack unit
2 fixed 10/100/1000 Mbps ports (RJ-45 for Fast Ethernet and Ethernet, and Gigabit Interface Converter (GBIC) for Gigabit Ethernet)	Maximizes LAN connectivity without extra rack space
Single AC, double DC power supply with 50W power consumption	Lowers power consumption and increases operational efficiency
Up to 300-kpps processing capability	Provides high-performance routing and processing performance
NSE-1 processor with Parallel Express Forwarding (PXF) technology	Delivers high-performance, hardware-accelerated, high-touch IP services

Cisco IOS Software	Supports IP network services including quality of service, security, compression, and IPSec 3DES encryption at high speed
Broad range of WAN media interfaces from DS0 to OC3 (40+ port adapters)	Allows flexible network configurations
Service Selection Gateway (SSG)	Creates value-added revenue by providing Web-based self-provisioning services
Common port adapters with Cisco 7500 and Cisco 7200 routers	Simplifies stocking spares and protects customer investment in interfaces
Cisco Element Manager Framework (CEMF) and Service Connection Manager (SCM)	Simplifies and accelerates the deployment and management of new services and elements across the network

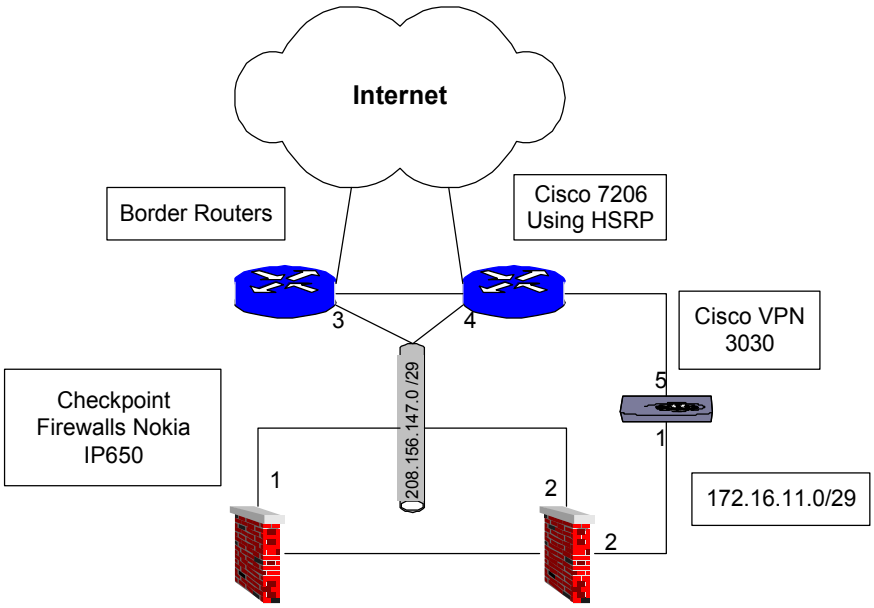
BORDER FIREWALL



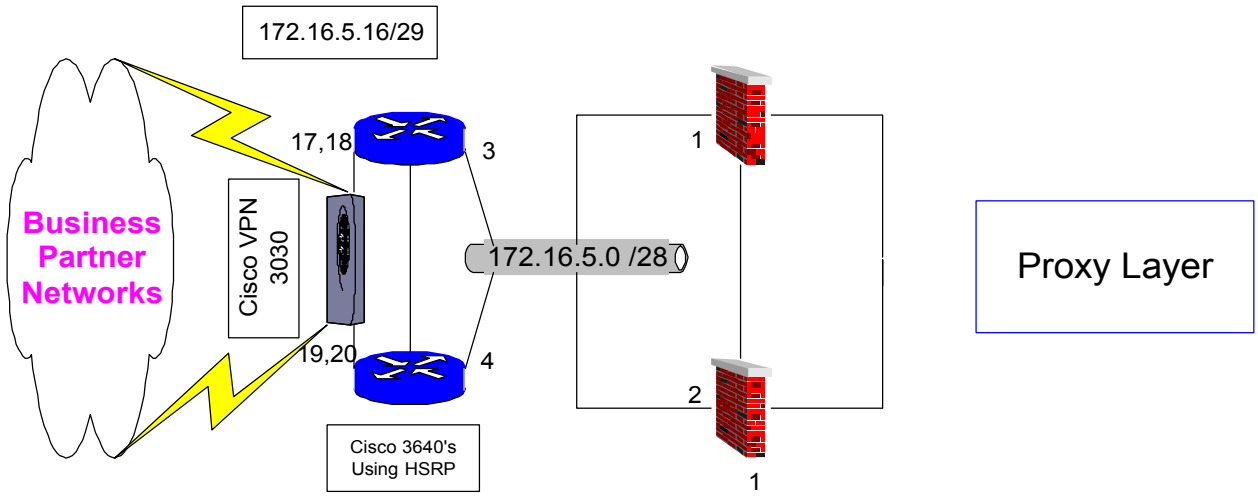
The Border Firewall will be a pair of Nokia IP650 boxes with redundant dual power supplies running Checkpoint 4.1 with the latest security fixes applied. The features and benefits for the Nokia IP650 are covered in assignment three. These boxes will be running in monitored circuit mode with Checkpoint configured for stateful fail over. This firewall will do all the natting for internal devices and will allow the needed services for internal and external traffic flow. A separate firewall interface is used for the VPN traffic, which is on the unencrypted side of the VPN concentrator. It's also a good place to log and secure the unencrypted Employee and any Business Partner VPN traffic.

BORDER AND BUSINESS PARTNER VPN

VPN DIAGRAMS



INTERNET BORDER VPN DIAGRAM SHOWN ABOVE AND BUSINESS PARTNER VPN DIAGRAM SHOWN BELOW



Cisco VPN 3030 Concentrator

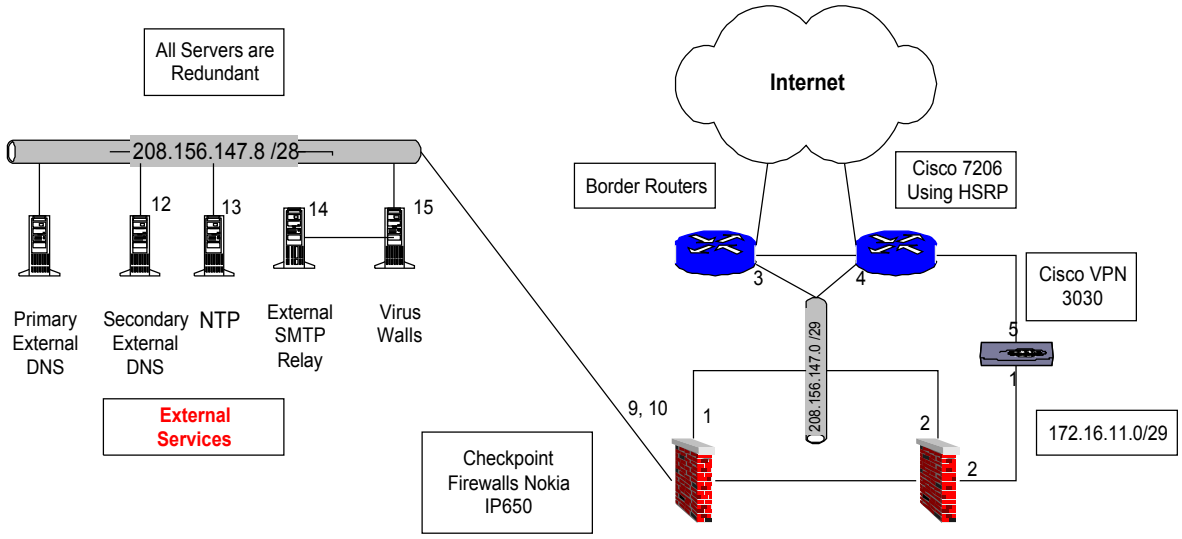
The 3030 Concentrator VPN platform is the chosen model. It is designed for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through fractional T3 (50 Mbps maximum performance) and up to 1500 simultaneous sessions. GIAC will have dual T1's and this model will fit that range with plenty of scalability for growth. Specialized SEP modules perform hardware-based acceleration. The 3030 is field-upgradeable to the 3060. Redundant configurations are available. This VPN device will be used for secure remote access and will be used by administrators, salespeople, and telecommuters who need access to internal services. Site to site VPN will be used for business partners. Current border VPN design terminates at the firewall to allow log and tcpdump monitoring of the unencrypted traffic. The key benefits and features are listed below and were found at: http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm

Key Features and Benefits

Table 20-16: Feature Summary for the Cisco VPN 3000 Series

Feature	Cisco 3005	Cisco 3015	Cisco 3030	Cisco 3060	Cisco 3080
Simultaneous Users	100	100	1500	5000	10000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	N/A	N/A	Option	Option	Yes
Available Expansion Slots	0	4	3	2	N/A
Upgrade Capability	No	Yes	Yes	N/A	N/A
System Memory	32 MB (fixed)	64 MB	128 MB	256 MB	256 MB
T1 WAN Module	Fixed option	Option	Option	Option	Option
Hardware	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Dual Power Supply	Single	Option	Option	Option	Yes

EXTERNAL SERVICES NETWORK DEVICES



Primary and Secondary external DNS servers

Shown in the graphic above, will fetch DNS queries for the internal Primary and Secondary DNS servers. They will also be authoritative for the GIAC.com domain. They will have external addresses and be located in the External Services portion of the DMZ.

The Virus Walls and External SMTP relay

Shown in the graphic above, will also have external addresses and reside in the External Services portion of the DMZ. The External mail server will send and receive SMTP traffic to and from the Internet. It will forward it to the internal proxies in the proxy layer when the traffic is destined for the internal network. Trend Micro InterScan® VirusWall for Solaris will be used to scan the e-mail. The VirusWall will scan inbound and outbound SMTP e-mail and attachments for viruses and has content checking capabilities. SMTP Traffic must go thru the VirusWall first to be scanned. VirusWall currently has a Web based interface for easy administration. The key features for Trend Micro's VirusWall are Real-time virus detection and clean up for all SMTP, HTTP, and FTP Internet traffic at the gateway. It also blocks malicious mobile code (Java and ActiveX) at the gateway, 100% compatible with FireWall-1 and most major firewalls, and configures remotely using a Web browser or locally via Windows interface.
http://www.antivirus.com/products/isvw/

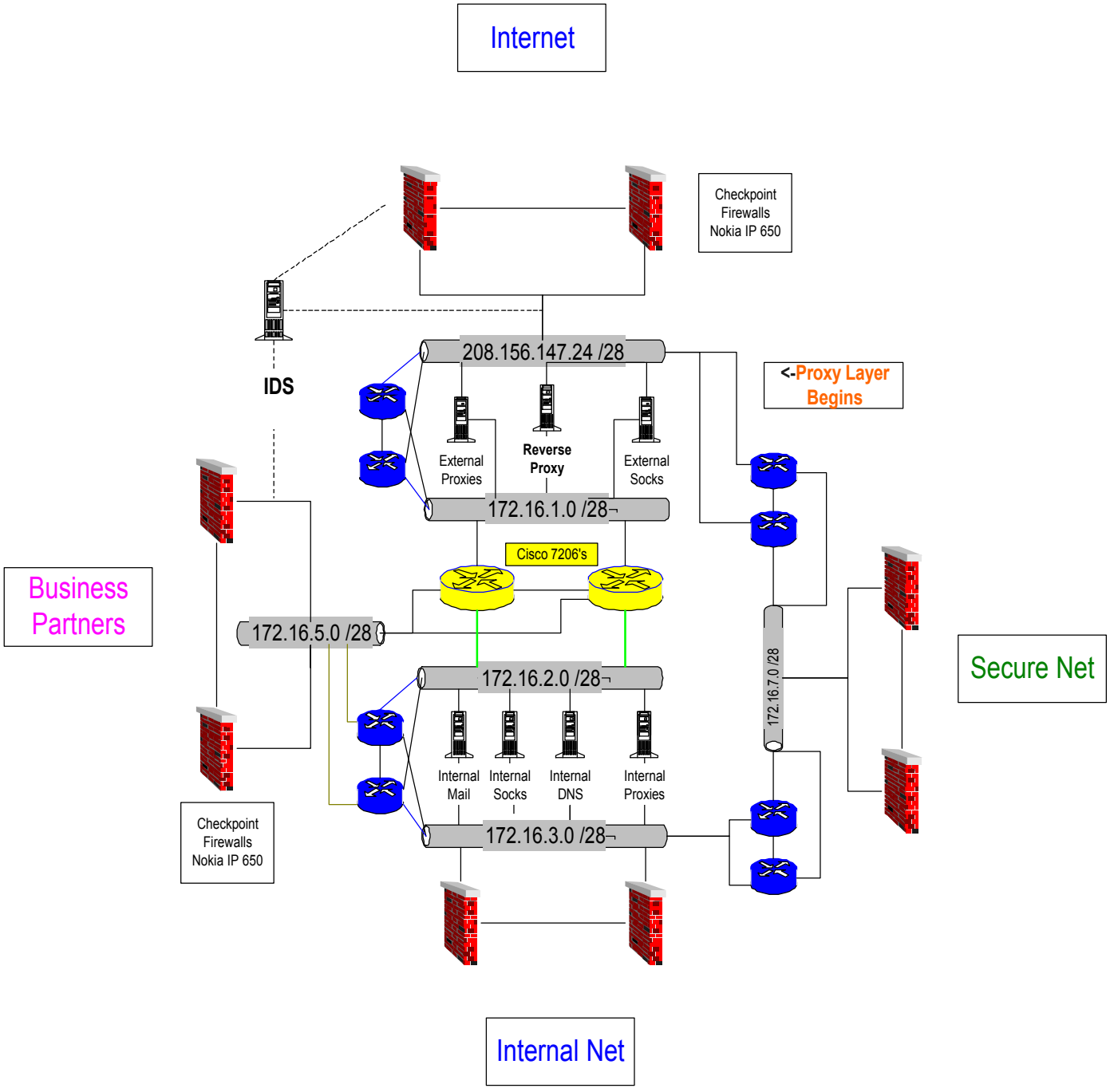
NTP Server

An NTP server will be installed in the external services portion of the DMZ for time synchronization of the network, log files, and database transactions. This server will get its time from internet time servers.

THE PROXY LAYER DEVICES

PERIMETER ROUTER (CISCO 7206)

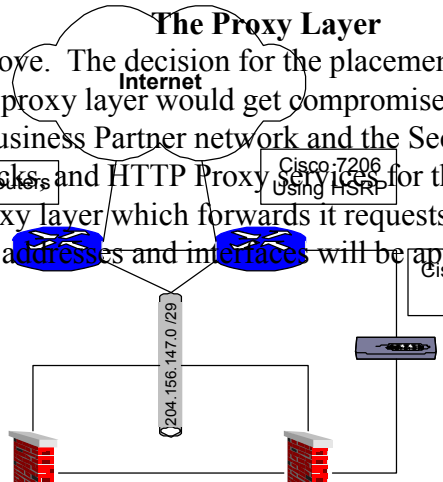
Highlighted in yellow below in the graphic. The perimeter router's purpose will route internal DMZ traffic where it needs to go. Total redundancy has been created for entire network but since the perimeter router (Cisco 7206) was the heart of the network and a single point of failure for all traffic, it was decided to design total redundancy around the perimeter router and the internal and external proxy services layer which proved to be well worth it. This design not only produces total fail over redundancy but in the event that a pair of routers would die, The Business Partners and Web SSL Transaction Database portion of the business would not be affected nor would the internal network. All routers in the proxy layer are 7206's. This is by design because the redundant routers between the 208.156.147.24 and 172.16.1.0 networks and the redundant routers between 172.16.2.0 and 172.16.3.0 networks must be able to handle the load in the event of a router pair failure. This design also gave several ways to take some load off the 7206. The SSL Web traffic can route around the top leg of the proxy layer network. Then route traffic for the Business Partners through the lower leg of the proxy layer network while internal web, VPN, and ftp traffic will use the 7206 center path straight out to the internet.



Perimeter Router Shown Above in Yellow

The Proxy Layer

is shown highlighted in the graphic above. The decision for the placement of these services was a secure one. If any of the boxes in the proxy layer would get compromised there is still a firewall protecting the Corporate LAN, The Business Partner network and the Secure Net portions of the DMZ. All requests for Mail, DNS, Socks, and HTTP Proxy services for the internal LAN will point to the Internal portion of the proxy layer which forwards it requests to the External portion of the proxy layer. Public and private addresses and interfaces will be applied to the External



proxy layer devices that are routed to the internet.

Internal SMTP Mail Servers

Running on a Solaris 8 OS, are used to handle requests from and delivery to the internal LAN. They send their requests outbound from the internal LAN to the External Mail Servers and Virus Walls, also running on a Solaris OS in the External Services portion of the DMZ. After the mail gets scanned for viruses, it gets sent to its destination. Incoming mail gets scanned by the Virus Walls then forwarded to the SMTP relay. The SMTP relay forwards the mail to the internal mail servers. The internal mail servers deliver the mail to the client on the internal LAN.

Internal Primary and Secondary DNS servers

Running on a Solaris 8 OS and located in the proxy layer, will cache and forward all requests coming from the internal LAN that they do not have locally, to the Primary and Secondary external DNS servers located in the External Services portion of the DMZ. The Primary and Secondary External DNS servers will also be authoritative for the GIAC.com domain.

Cache Flow Reverse Proxy SA-745 Series

The Cache Flow 700 series is designed for reverse proxy solutions. Internet requests destined to the GIAC.com web SSL application in the Secure Net will be intercepted by the redundant SA-745 Reverse proxy which will have public addresses. This server will also be a certificate server for the corporate network for the purposes of signing SSL certificates. This server contains the corporate private key, and is used as the root authority for their environment. The 700 series Features are listed below.

http://www.cacheflow.com/products/700/features.cfm

The SA-700 Series is the industry's only solution specifically engineered to accelerate and scale Web sites. The SA-700 is designed to seamlessly integrate with a site's existing systems and networks, delivering an immediate performance impact. The following capabilities of the SA-700 will help high-traffic Web sites to serve more customers through a lower cost infrastructure.

Key Platform Features

Optimized Configuration for Web Server Acceleration

- High RAM-to-disk ratio
- Specialized system architecture

Superior Price/Performance

- Generates 100Mbps of data throughput

Optimized Power Utilization

- Only outputs 100 Watts

Space-Friendly 1U (<1.75") Form Factor

- Delivers real estate cost savings

Integrated SSL Cryptographic Processor

- Processes 200 key negotiations per second, ~10 times the power of a standard Web server

Simple to Manage Appliance

- Installs in minutes; little ongoing maintenance required

Key Software Features

CacheOSTM Server Edition

- Industry's only system software that is tuned for the workload of a high-traffic Web site

CacheFlow Content Manager (optional)

- Intelligent synchronization and management of content across a distributed network of server accelerators
- Content Manager datasheet

CacheFlow Intelligent Akamaizer

- Automatically readies content for the Akamai FreeFlow service
- Combined CacheFlow/Akamai solution allows sites to scale globally and gracefully handle peak events
- CacheFlow Akamaizer White Paper
- Akamaizer General FAQ or Akamaizer Technical FAQ

Secure Content Acceleration

- Can accelerate both public (HTTP) and private (HTTPS) content through integrated SSL functionality
- Technical Note: SSL Primer (link to new PDF, attached to this email)

Dynamic Content Acceleration

- Accelerates all content that is not unique to a user, including dynamically generated pages
- Accelerates all images within user-specific pages

Denial of Service (DoS) Protection

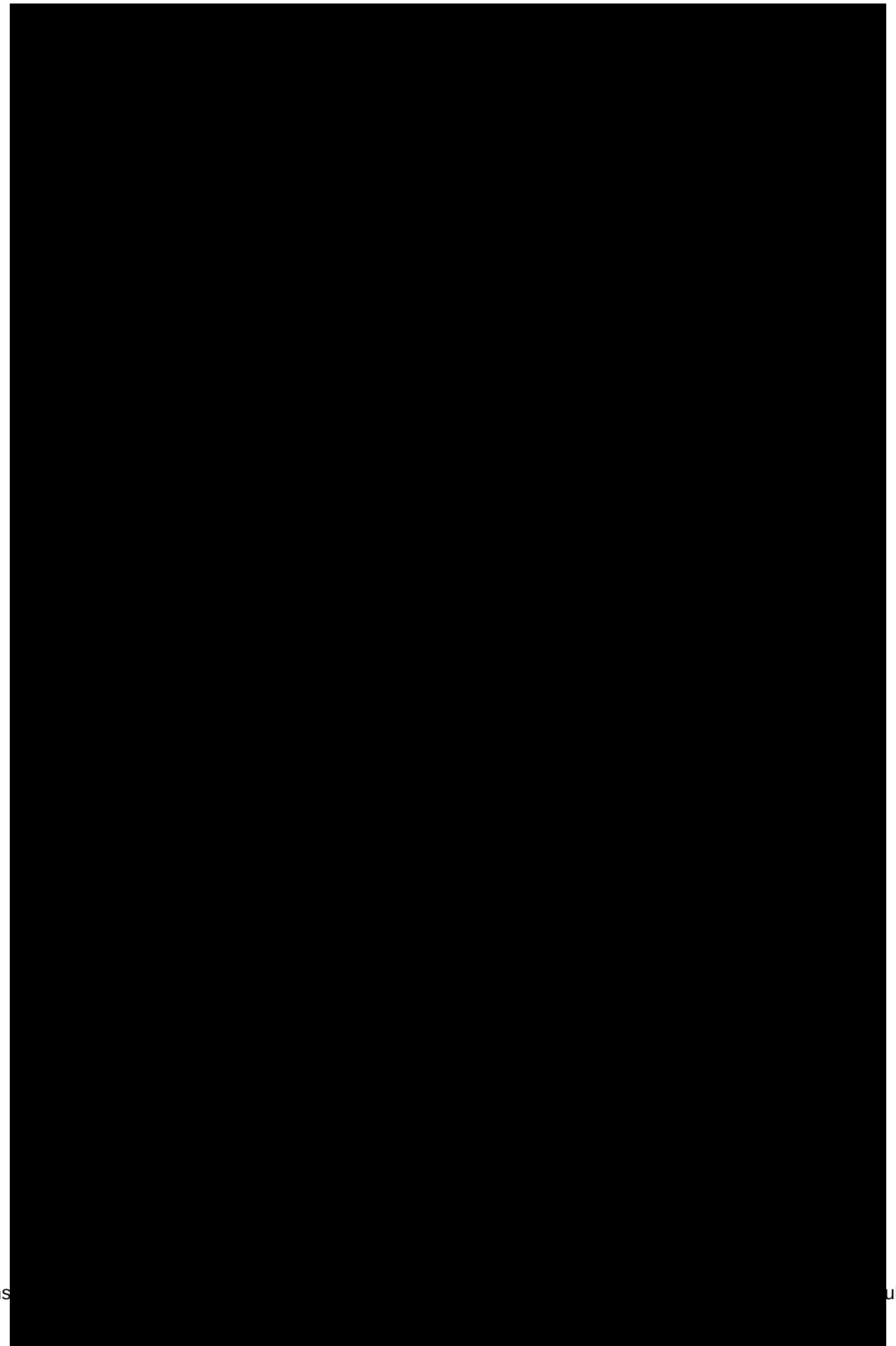
- Prevents sites from crashing during hacker-initiated DoS attacks
- Server accelerator distinguishes between valid and malicious connections, servicing users while resisting the attack

Robust security

- Certified by a leading security audit firm for safe placement outside the firewall

Specifications for the different 700 series models are listed on the next page.

700 Series



[1]Server accelerators are sized according to the amount of throughput required and the working set size. The working set is defined as the amount of unique content served over the course of a day. A server accelerator will deliver maximum performance when working set content is served directly from RAM.
[2]The SA-745 is optimized for Web sites with a high degree of large-file content types. The size of these sites dictates that all content will not fit into RAM, and the majority must therefore be served from disk (which has throughput implications). The SA-745 is built with a large storage capacity to fit the data characteristics of these rich content Web sites.

Cache Flow Forward Proxy SA-645 Series

The Cache Flow 600 series is designed for forward proxy solutions. Dual redundant SA-645's will be used in the Internal and External proxy layers for Internal LAN http and https requests. Internal LAN users will point to the Internal proxies in the Internal proxy layer. The Internal proxies will forward any requests from the internal LAN that they do not have cached to the External proxies who will make their requests to the root servers if they don't have the request in their cache. The External proxies will have public and private addresses. Its features and specifications are listed below.
http://www.cacheflow.com/products/600/

Key Platform Features

Optimized Configuration for Client Acceleration

- Large disk capacity to efficiently manage Internet content

Space Friendly 1U (<1.75") Form Factor

- Delivers real estate cost savings

Front Panel LCD and Joystick Device

- Provides a quick and easy method for setting the Content Accelerator's initial network configuration
- Eliminates the need to connect terminal interface for initial configuration

Configuration Restoration

- Allows system configuration to be archived, including all system settings, filtering and access control policies
- Archive can be loaded to the Client Accelerator from an HTTP, FTP, or TFTP server in the rare case of system failure.
- Simple to Manage Appliance Installs in minutes; little ongoing maintenance required

Key Software Features

Standards-based Proxy Authentication and Policy Control - Enables administrators to manage which users can access the Internet using LDAP, RADIUS and NTLM and provides exportable reporting and logging information.

Content filtering - Allows organizations to implement Internet policies to manage, restrict and log user access to web content through integrated, subscription-based solutions from Websense™ and Secure Computing.
Multimedia Services - Certified support for major streaming media formats which optimize live and on-demand streaming content for improved viewing and listening quality. Multimedia support includes RealProxy™, Microsoft Windows Media, Apple QuickTime, MP3 and Flash.
Adaptive Refresh - Patent-pending technology that ensures users always receive "fresh" and up-to-date content by intelligently communicating with origin web servers and proactively updating cached content based on usage patterns, frequency of requests, and time required to retrieve web objects.
Rules-Based Filtering and Forwarding - Powerful rules library that makes it easy to create sophisticated filtering and forwarding policies applied to individuals or an entire organization.
Real-time Logging and Event Notification - Enables the logging of system events, and allows administrators to specify events to be logged, size of event log, and email alerts for occurring events.
DNS Caching - Enables caching of DNS entries to boost overall performance by eliminating latencies inherent in contacting a DNS server.
Transparent Caching - Allows all HTTP requests to be transparently redirected to the CacheFlow appliance from any Layer 4 switch or WCCP enabled router, and simplifies deployment by eliminating the need to configure individual browsers.
Management - Available both in a web-based graphical user interface and command line interface for managing, configuring, monitoring and upgrading the client accelerator remotely.
Content Manager - Allows administrators to view, distribute, monitor and purge content from as network of distributed caches on a scheduled or dynamic basis.
Web Object Pipelining - Allows parallel requests to the host server, thus reducing wait time even when the data is not available in the cache. Results in 50% wait time on first requests to web sites.

600 Series Specifications:

[redacted]

Model CA-610

Model CA-615

Model CA-625

Model CA-645

System

Disk Drives

1x4GB IDE

1x18GB Ultra-Wide SCSI

2x18GB Ultra-Wide SCSI

4x18GB Ultra-Wide SCSI

RAM

128MB

384MB

768MB

1GB

Network Interfaces

(2) 10/100 Base-T Ethernet

(2) 10/100 Base-T Ethernet

(2) 10/100 Base-T Ethernet

(2) 10/100 Base-T Ethernet

Client Accelerator Sizing

Maximum WAN Throughput

9.5-10.5 Mbps

12.5-26 Mbps

26-52 Mbps

52-104 Mbps

Operating System

CacheOS™

Internal and External socks

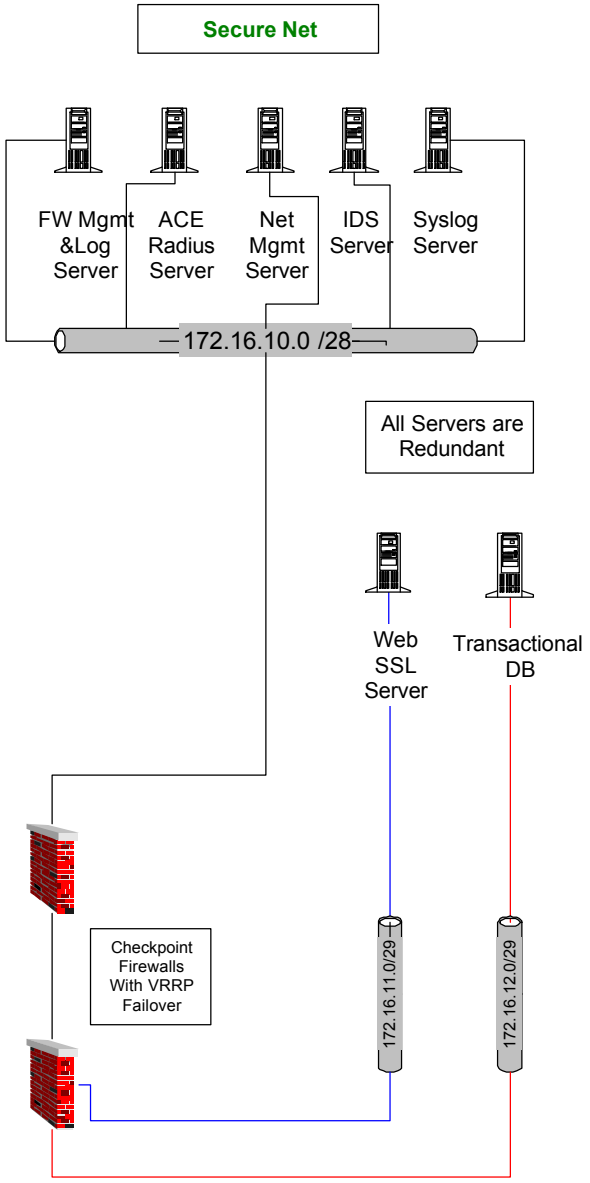
Any Non HTTP and HTTPS traffic will use the latest socks ver.5 service running on a hardened Solaris OS. Socks Internal LAN clients will point to the internal socks servers in the proxy layer. The internal socks servers will forward their requests to the external sock servers which will make the external connection. The external socks servers will be hidden behind a hide NAT from the Internet. Some connections may require static nats.

Intrusion Detection

Snort will be running on a hardened Solaris OS in the DMZ as the IDS detection system. Snort sensors will be installed on the internal side of the border firewall, on the internal side of the external services network, and on the internal side of the business partner network for malicious activity monitoring. Logs will be exported to the IDS server in the Secure Net for analysis.

SECURE NET DEVICES

SECURE NET DIAGRAM



Syslog Server

All devices with logging capabilities will push their logs to the syslog server. The syslog server will have very large capacity drives to store the log data. Logs will be pushed nightly to a larger capacity centralized log storage server and stored for eight months. After eight months the logs will be deleted sequentially by the oldest time and date.

ACE Server

An ACE server will be used for RSA SecurID two-factor VPN Authentication for administrators, salespeople, and telecommuters. RSA ACE/Server includes Livingston 2.0 RADIUS server, so

you can manage user accounts from a single database for both RADIUS and RSA SecurID authentication. RSA ACE/Server is also compatible with other leading authentication technologies, such as Kerberos and TACACS+ which will be used in this design.

The Secure Net Firewall

Will be a pair of Nokia IP650 boxes with redundant dual power supplies running Checkpoint 4.1 with the latest security fixes applied. These boxes will be running in monitored circuit mode with Checkpoint configured for stateful fail over.

Checkpoint Firewall Management Server

The management server will run Solaris 2.8 on a hardened OS and will manage all Checkpoint firewalls including collecting the logs for each Firewall. All access to the management servers will use the SSH secure protocol. Only the management servers will be allowed to SSH to the firewalls. The primary management server will have a backup server. Both servers will be backed up nightly to tape. Also the /etc/fw/conf directory will be copied to a backup directory on the primary in case GIAC needs to get back to the previous rule changes quickly. The /etc/fw/conf directory will be rsynced from the primary management server to the backup server after the nightly rule pushes to ensure the backup server has the latest changes in the event of a failure.

IDS Server

An IDS server will be located in the Secure Net for log storing and analysis of Snort logs. Traps will be configured to notify administrators of critical events.

Network Management Server

HP Openview and Cisco Works will be used as the Network device management tool. The servers will reside in the Secure Net.

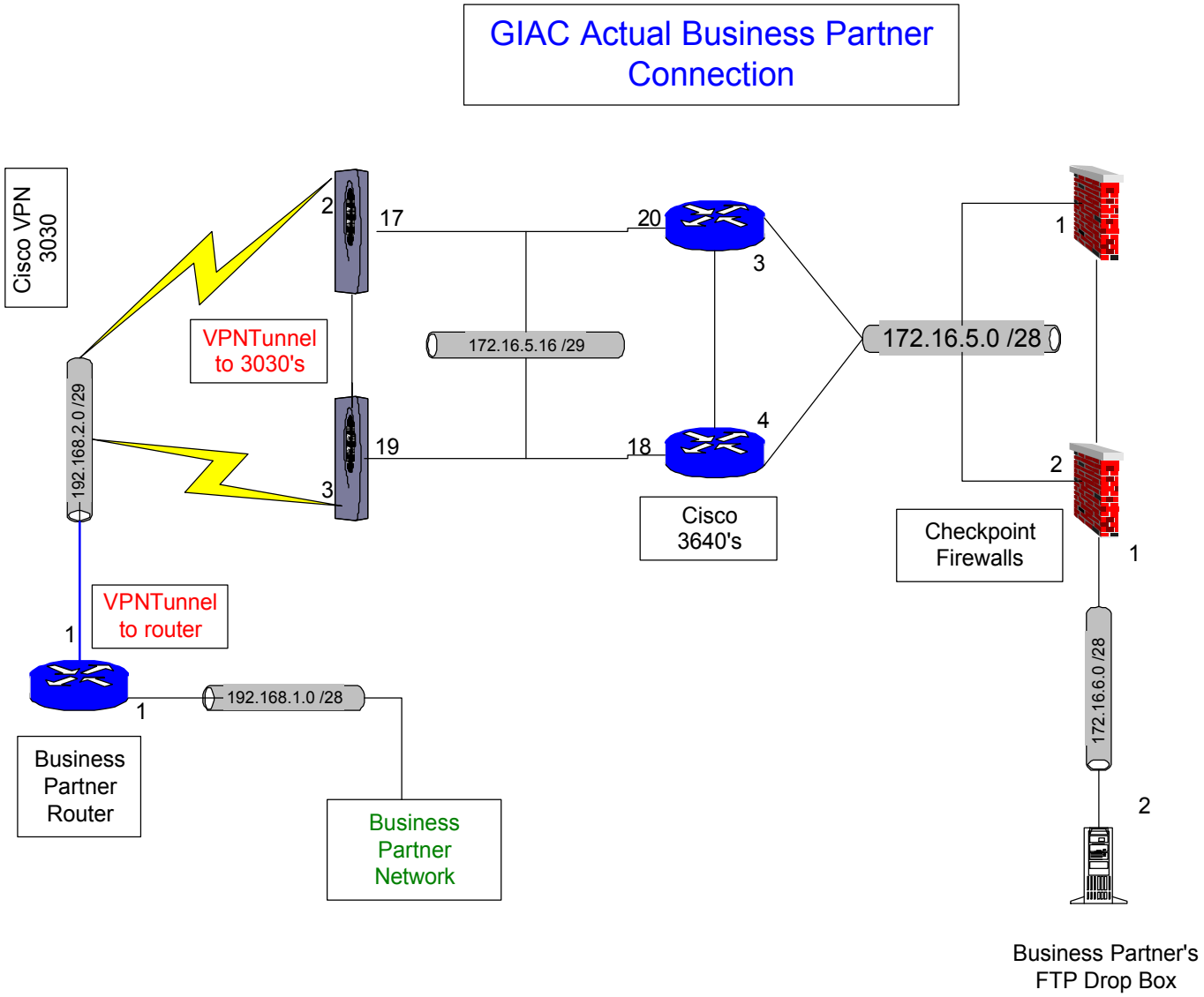
Web SSL Server

Customers who purchase bulk online fortunes will use this server to connect via HTTPS/SSL over the internet to make online purchases.

Transactional Database

The customer's transactions will be recorded to a transactional database in the Secure Net for billing and tracking purposes.

BUSINESS PARTNER NETWORK DEVICES



The Business Partner Firewall

Will be a pair of Nokia IP650 boxes with redundant dual power supplies running Checkpoint 4.1 with the latest security fixes applied. These boxes will be running in monitored circuit mode with Checkpoint configured for stateful fail over.

Cisco VPN 3030 Concentrator

The 3030 Concentrator VPN platform is the chosen business partner model. It is designed for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through fractional T3 (50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The 3030 is field-upgradeable to the 3060. Redundant configurations are available.
http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm

Site to site VPN will be used for business partners. Current Business Partner VPN design terminates at the 3640 router to allow logging and tcpdump monitoring of the unencrypted traffic as it enters the GIAC network. The key benefits and features are listed above on page 8.

FTP Server

- Suppliers who supply the fortune sayings will use a VPN to connect to GIAC and SFTP to transmit the bulk data to a FTP Drop Box which will be monitored by the Transactional Database and automatically be transferred over via SFTP following an electronic receipt to the supplier.

- International partners who translate and resell fortunes will use a VPN to connect to GIAC. They will pick up their data from the business partner FTP server using SFTP and the transaction will be recorded by Business Partner name, time, filename, and file size. The transaction will then be recorded in the transactional database for billing

Cisco 3640 Router

A Cisco 3640 router was chosen for the Business Partner router. Its features and benefits are listed below.

Key Features and Benefits

The 3600 Series Modular Access routers provide value added end-to-end networking solutions with the following benefits:

Multiservice Integration—Complementing the Cisco 2600 Series, the Cisco 3600 Series extends the versatility, integration, and power to larger remote branch offices. The Cisco 3600 Series leads the way in Cisco's commitment to add multiservice voice/data integration capabilities to its product portfolio, enabling corporate customers to control costs and allowing service providers to offer broader managed service options.

Investment Protection—The ability of the Cisco 3600 series to support field-upgradable modular components, customers can easily change network interfaces without a "forklift upgrade" of the entire remote branch office solution.

Lower Cost of Ownership—Integrating the functions of CSU/DSUs, ISDN Network Termination (NTI) devices, and other equipment found in branch office wiring closets in a single, compact unit provides a space-saving solution that can be managed remotely using network management applications such as CiscoWorks and CiscoView.

Part of the Cisco end-to-end solution—As a key part in the Cisco comprehensive end-to-end solution, the 3600 series allows businesses to extend a cost- effective, seamless network infrastructure to the remote branch office location

Table 1: Cisco 3600 series Features and Benefits	**Benefit**
Versatility	
Modular Architecture	Network Interfaces are field-upgradable to accommodate future technologies while providing solutions for today Additional Interfaces can be added on a "pay as you grow" basis to allow network growth LAN and WAN interface configuration is easily customized for individual needs
WAN Interface cards and Network Modules Shared with Cisco 1600 and 2600 Series Routers	Reduced cost of maintaining inventory of Cisco 1600, 2600, and 3600 Series modular components Lower training costs for support personnel
DC Power Supply Option	Allows deployment of DC power environments such as telecommunications carrier central offices
Power	
High-Performance RISC Architecture	Support for advanced QoS features such as RSVP, WFQ, CAR, and IP Precedence to reduce recurring WAN costs Enables security features such as data encryption, tunneling, and Radius, TACACS, and AAA to protect data assets Integration of legacy networks via data link switching plus (DLSW+) and Advanced Peer-to-Peer Networking (APPN) High-speed Fast Ethernet to Fast Ethernet routing (50-70kpps) for maximum scalability
Full Cisco IOS Support	Provides the widest array of networking and routing protocol support in the industry for large-scale end-to-end network solutions
Manageability	
Integrated DSU/CSUs and NT1 Options	Enables remote management of all CPE elements for higher network availability and lower operational costs
Modem Management, Including Modem Statistics, Real-Time Call in Progress, Monitoring Modem Activity Log and Modem Hard/Soft Busy Out.	Enhanced monitoring of modem call progress and statistics in real time to reduce problem detection and resolution time
Support for CiscoWorks, CiscoWorks2000, and CiscoView	Allows simplified management of all integrated and stackable components
Support for Cisco Voice Manager (CVM)	Reduces the costs of deploying and managing integrated voice/data solutions

Enhanced Setup Feature	Context-sensitive questions guide the user through the router configuration process, allowing faster deployment
Autoinstall	Configures remote routers automatically across a WAN connection to save the cost of sending technical staff to remote sites
Reliability	
Redundant Power Supply Options	RPS unit can be shared with other network components such as the Cisco Catalyst 1900, 2500, 2600, and 4000 Series to protect the network from downtime due to power failures
Dial-on-Demand Routing	Allows automatic backup of WAN connections in case of a primary link failure. Supported over ISDN, or low and high speed asynchronous/synchronous lines
Dual Bank Flash memory	Backup copy of Cisco IOS can be stored in Flash memory
Ergonomic Design	
LED Status Indicators	Provides at-a-glance indications for power, RPS status, network activity, and interface status
All Network Interfaces Located on Back of Unit	Simplifies installation and cable management for maximum uptime
Easy-to-Open Chassis Design	Allows fast and easy access for installation or upgrading of Flash or DRAM memory

Switches

Cisco Catalyst 2950 series switches were chosen for the entire DMZ network. A 5509 RSM device will be used for the internal LAN which has route switch modules for routing and switching. These devices support Gigabit speeds and the Key Features for these devices are listed below**.**

Key 2950 Series Features

Wire-speed performance in connecting end-stations to the LAN
Powerful migration path to Gigabit speeds while leveraging existing copper infrastructure
Sophisticated quality of service
Multicast Management via IGMP Snooping
Cisco Cluster Management Suite (CMS) Software offers ease-of-use and ease-of-deployment
Superior manageability
Security and high availability
Enhanced Cisco IOS Services
Support for Cisco Redundant Power System 300 (RPS 300)

Key 5509 Series Features:

System Features
This section describes the Catalyst 5000 family hardware features. For software feature descriptions, refer to the *Software Configuration Guide* for your switch. For supervisor engine descriptions and installation procedures, refer to the *Catalyst 5000 Family Supervisor Engine Installation Guide*.

Fault Tolerance and Redundancy
The Catalyst 5000 family switches have the following features:

- Catalyst 5002 switch
    - The chassis contains two fully redundant AC-input or DC-input, load-sharing power supplies. Each power supply has a separate power input.
- Catalyst 5000 switch
    - The chassis can house two fully redundant, hot-swappable, AC-input or DC-input, load-sharing power supplies. Each power supply has a separate power input.
    - The fan assembly is hot-swappable.
- Catalyst 5505 switch, Catalyst 5509 switch, and Catalyst 5500 switch
    - The chassis can house two hot-swappable supervisor engines.
    - The chassis can house two fully redundant, hot-swappable, AC-input or DC-input, load-sharing power supplies. Each power supply has a separate power input.
    - The fan assembly is hot-swappable.
    - The clock modules are redundant.

Assignment #2 - Scott Baker - Security Policies

Configuring the Cisco VPN 3000 Concentrator to a Cisco Router over the Internet using IPSec

Introduction

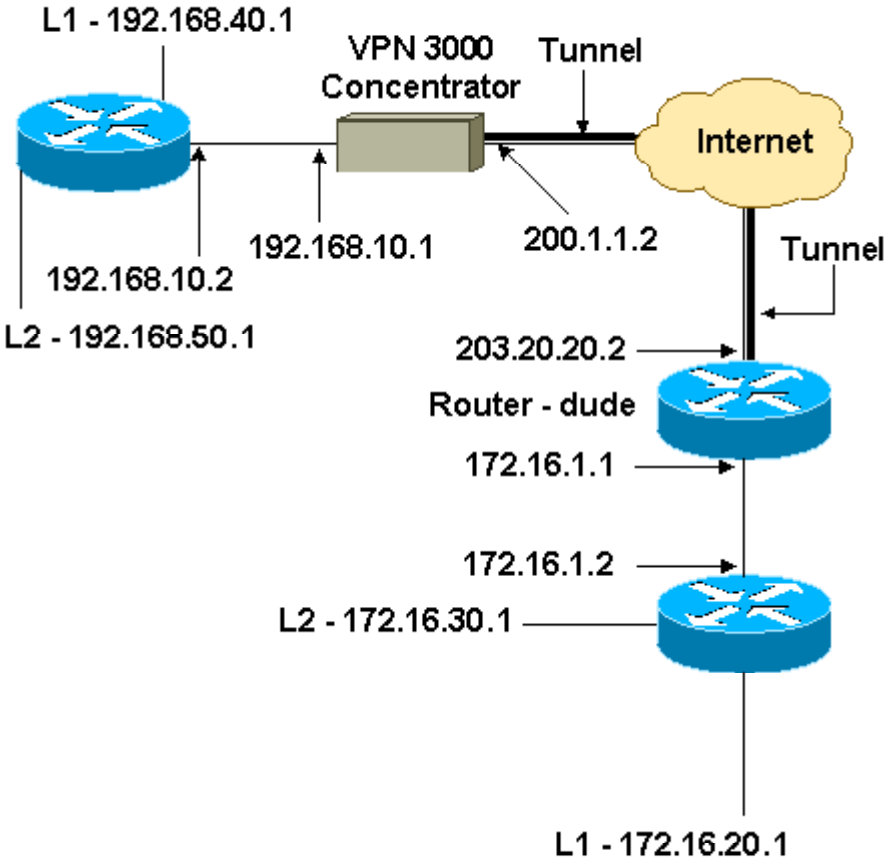
The goal of this sample configuration is to connect a private network behind a router running Cisco IOS® software to a private network behind the Cisco VPN 3000 Concentrator. The devices on the networks know each other by their private addresses.

Hardware and Software Versions

This configuration was developed and tested using the software and hardware versions below.

- Cisco 7100 router with Cisco IOS Software Release c7100-ik2s-mz.121-5.T7.bin
- Cisco VPN 3000 Concentrator with 3.0.3

Network Diagram



Assumptions:

To avoid confusion it will be assumed that the router dude router in the above graphic is the business partner router and addresses. The 192.168.x.x addresses will reflect that of the GIAC network. Since a Cisco VPN 3000 series model was not available to configure, a sample configuration of a similar network was provided below found on Cisco's site at http://www.cisco.com/warp/public/471/ALTIGAR.shtml. The difference in the sample configuration below is that the VPN is configured over the Internet, which may be a possibility for GIAC in the future since we already have a VPN 3030 at the Border for employee and admin access over the Internet. The configuration below would fit a sample business partner connection over the Internet. We would just substitute our IP addresses and access lists. We would mostly use the business partner private connection network shown above for the business partner suppliers who need faster connections for their large data transfers or a more private connection for better security. IPSec, Triple DES, and ESP will be the choice for the Encryption tunnel. The sample configuration starts below. The choices in the sample may not be the choices for the GIAC network and I will try to note where the changes are.

Router VPN Configuration

Router Configuration

```
dude#wr t
Building configuration...

Current configuration : 2673 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dude
!
boot system flash:c7100-ik2s-mz.121-5.T7.bin
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
!--- IKE policies
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 200.1.1.2
!
!--- IPSec policies
crypto ipsec transform-set to_vpn esp-des esp-md5-
hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
 !--- Traffic to encrypt
 match address 101
!
call rsvp-sync
!
interface FastEthernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
 crypto map to_vpn
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 fair-queue
 framing g751
 dsu bandwidth 34010
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
```

VPN Concentrator Configuration

As this was a lab setting, we first accessed the VPN Concentrator through the console port and added a minimal configuration so that the further configuration could be done through the graphical user interface (GUI).

To ensure that there was no existing configuration in the concentrator, we selected:

Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration.

After rebooting, the VPN Concentrator came up in Quick Configuration, and the following items were configured:

- Time/Date
- Interfaces/Masks in **Configuration > Interfaces** (public=200.1.1.2/24, private=192.168.10.1/24)
- Default Gateway in **Configuration > System > IP routing > Default_Gateway** (200.1.1.1)

At this point, the VPN Concentrator was accessible through HTML from the inside network.

Note: Because we were managing our Concentrator from *outside*, we also had to select:

- **Configuration > Interfaces > 2-public > Select IP Filter > 1. Private (Default)**
- **Administration > Access Rights > Access Control List > Add Manager Workstation** to add the IP address of the *external* manager.

This is not necessary unless you are managing the the VPN Concentrator from *outside*.

1. After bringing up the GUI, select **Configuration > Interfaces** to re-check the interfaces:

Configuraton | Interfaces — Friday, 15 June 2001 15:19:56

Save Refresh

This section lets you configure the **VPN 3000 Concentrator Series** network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.90.A4.00.0A.94	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.90.A4.00.0A.95	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				

- Power Supplies

2. Select **Configuration > System > IP Routing > Default Gateways** to configure the **Default** (Internet) **Gateway** and the **Tunnel Default** (inside) **Gateway** for IPSec to reach the other subnets in the private network:

Configuration | System | IP Routing | Default Gateways

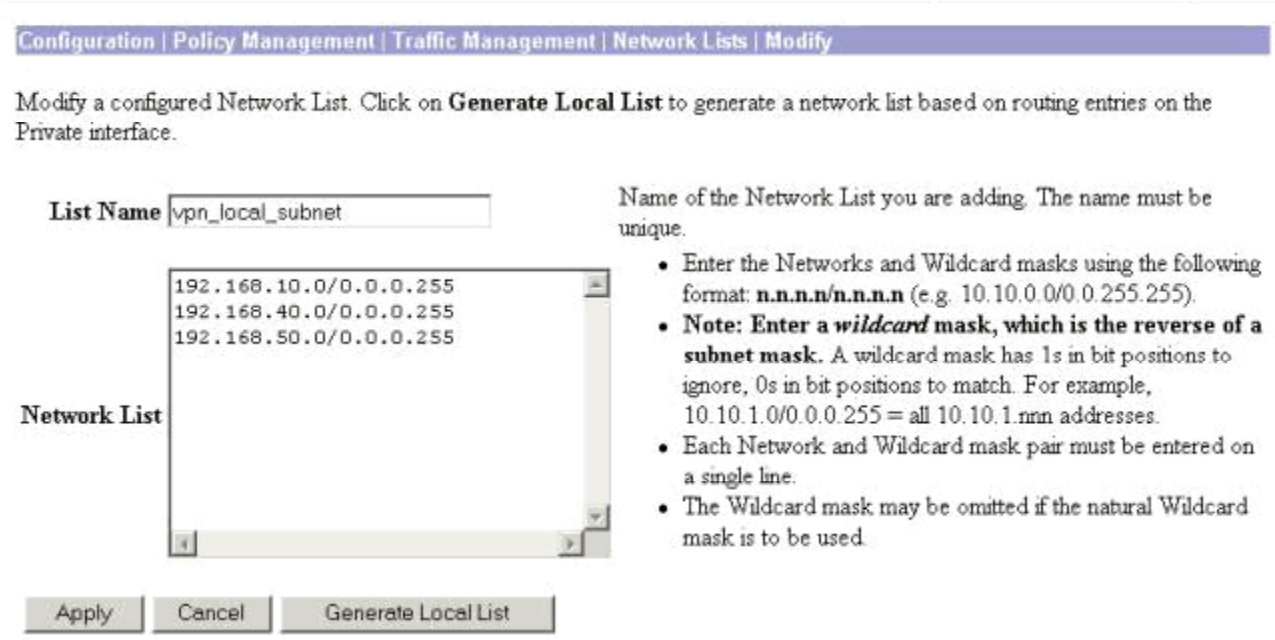
Configure the default gateways for your system.

Default Gateway	200.1.1.1	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Metric	1	Enter the metric, from 1 to 16.
Tunnel Default Gateway	192.168.10.2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.
Override Default Gateway	☑	Check to allow learned default gateways to override the configured default gateway.

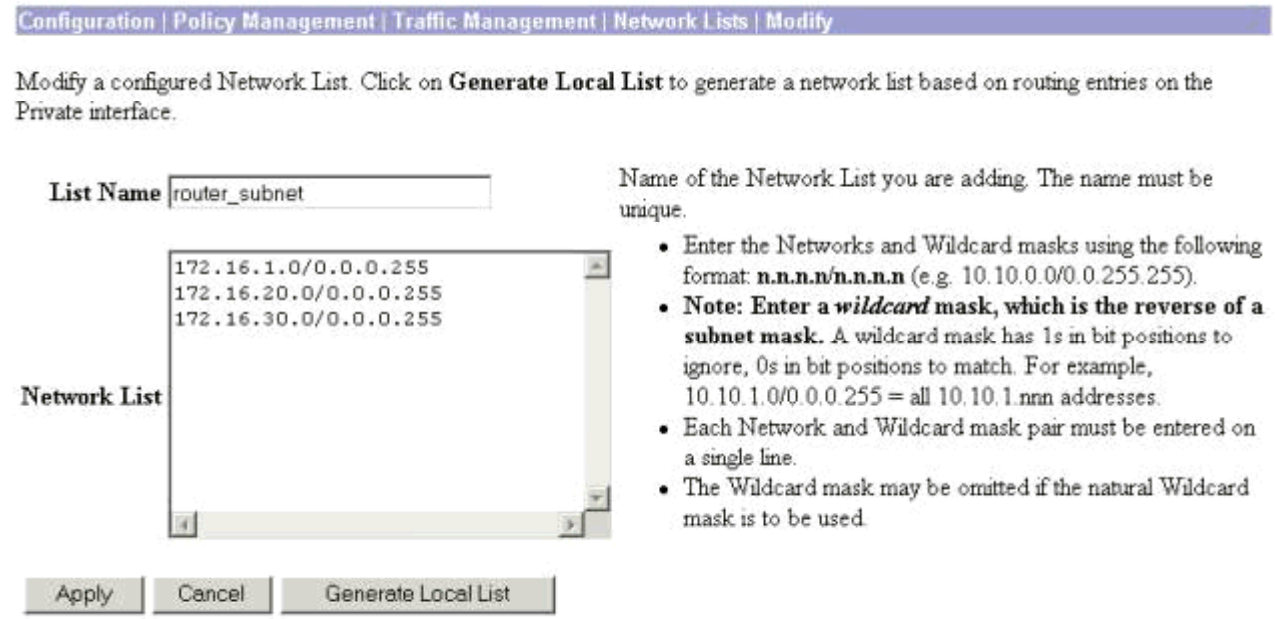
Apply Cancel

3. Select **Configuration > Policy Management > Network Lists** to create the network lists defining the traffic to be encrypted.

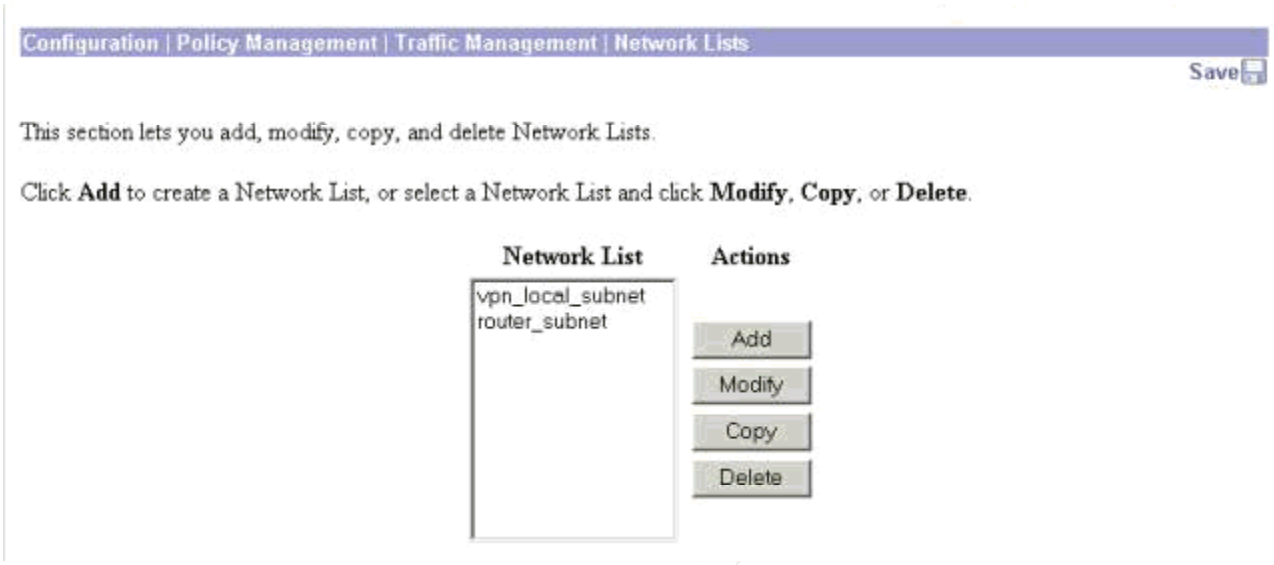
The local networks:



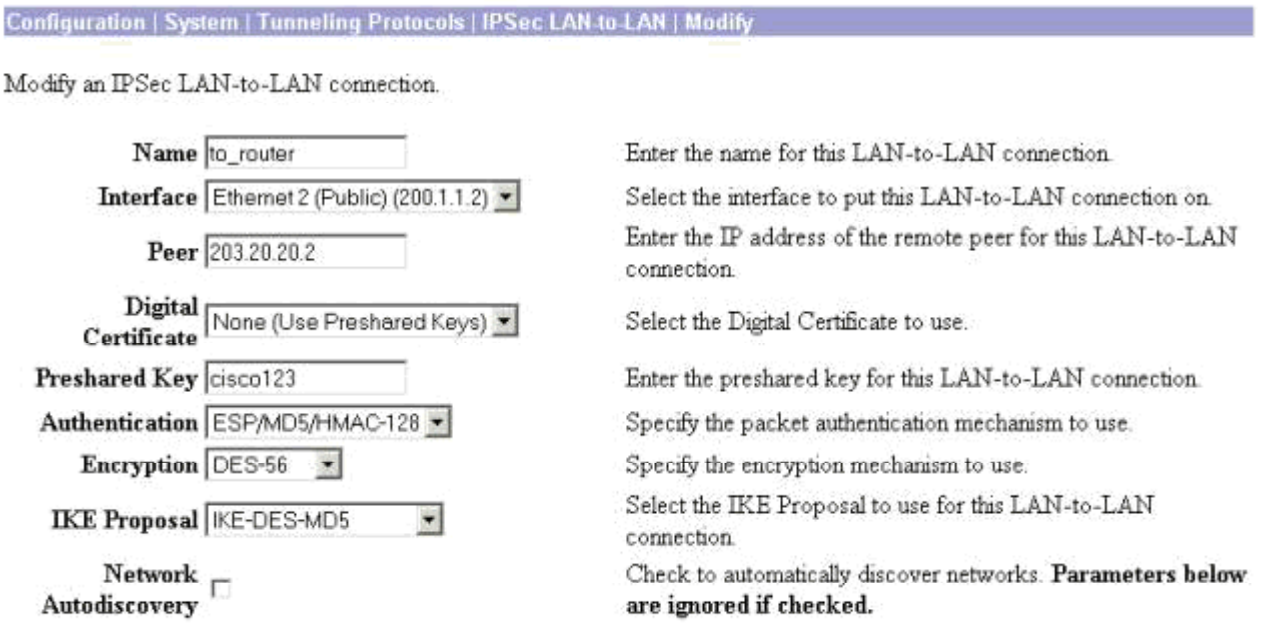
The remote networks:

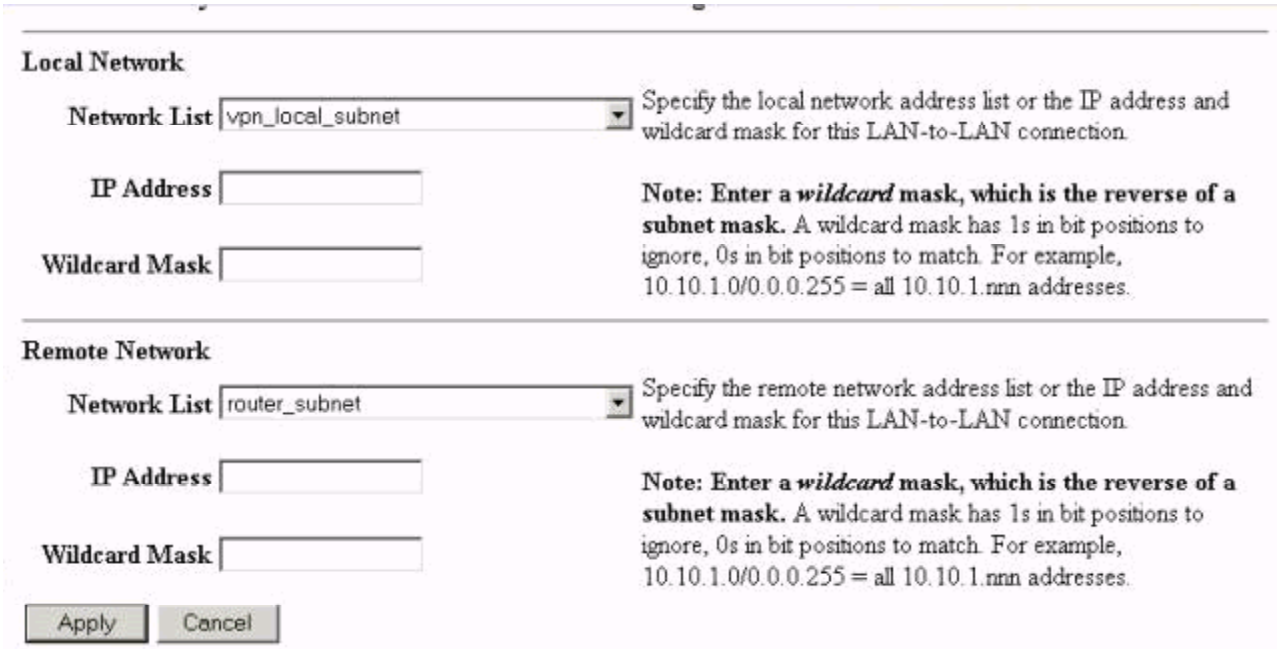


4. When completed, these are the two network lists:



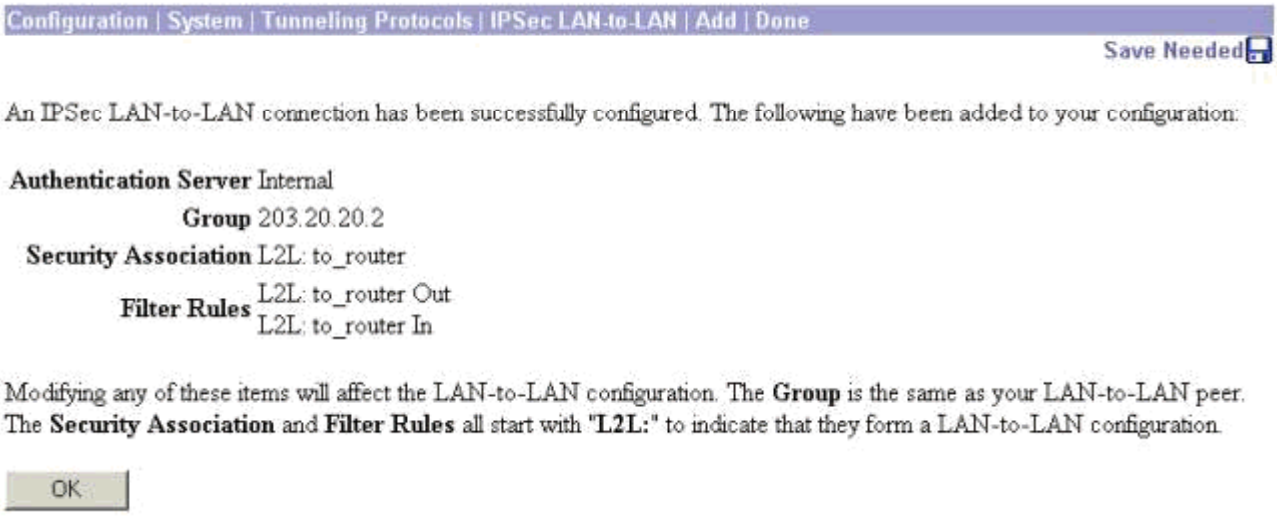
5. Select **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** and define the LAN-to-LAN tunnel:



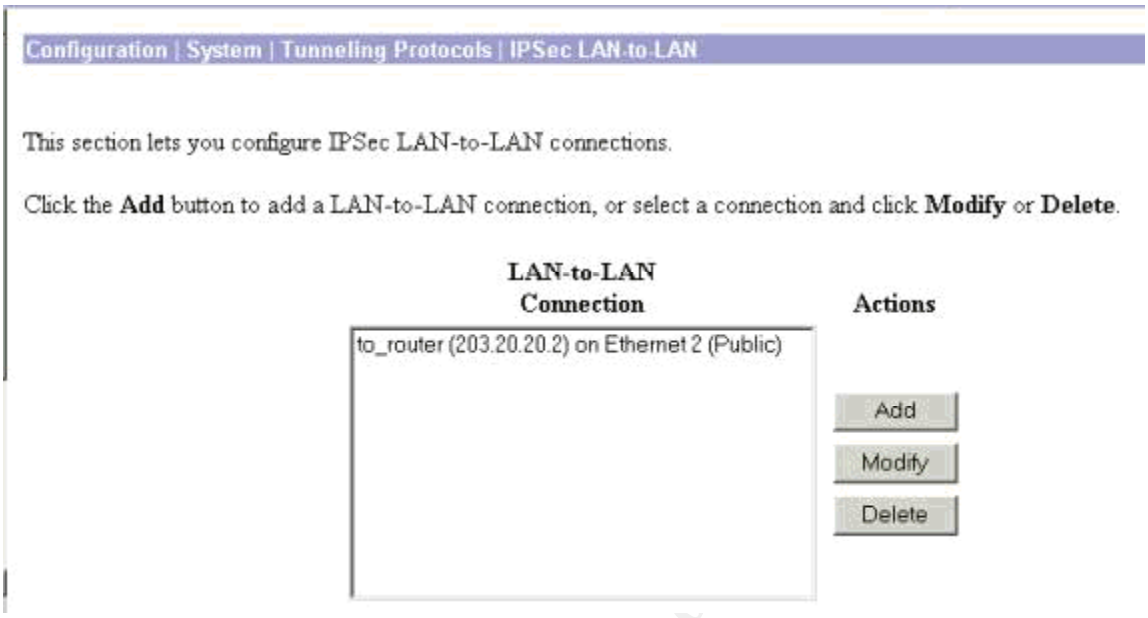


6. After you click **Apply**, the following screen is displayed with the other configuration that is automatically created as a result of the LAN-to-LAN tunnel configuration:

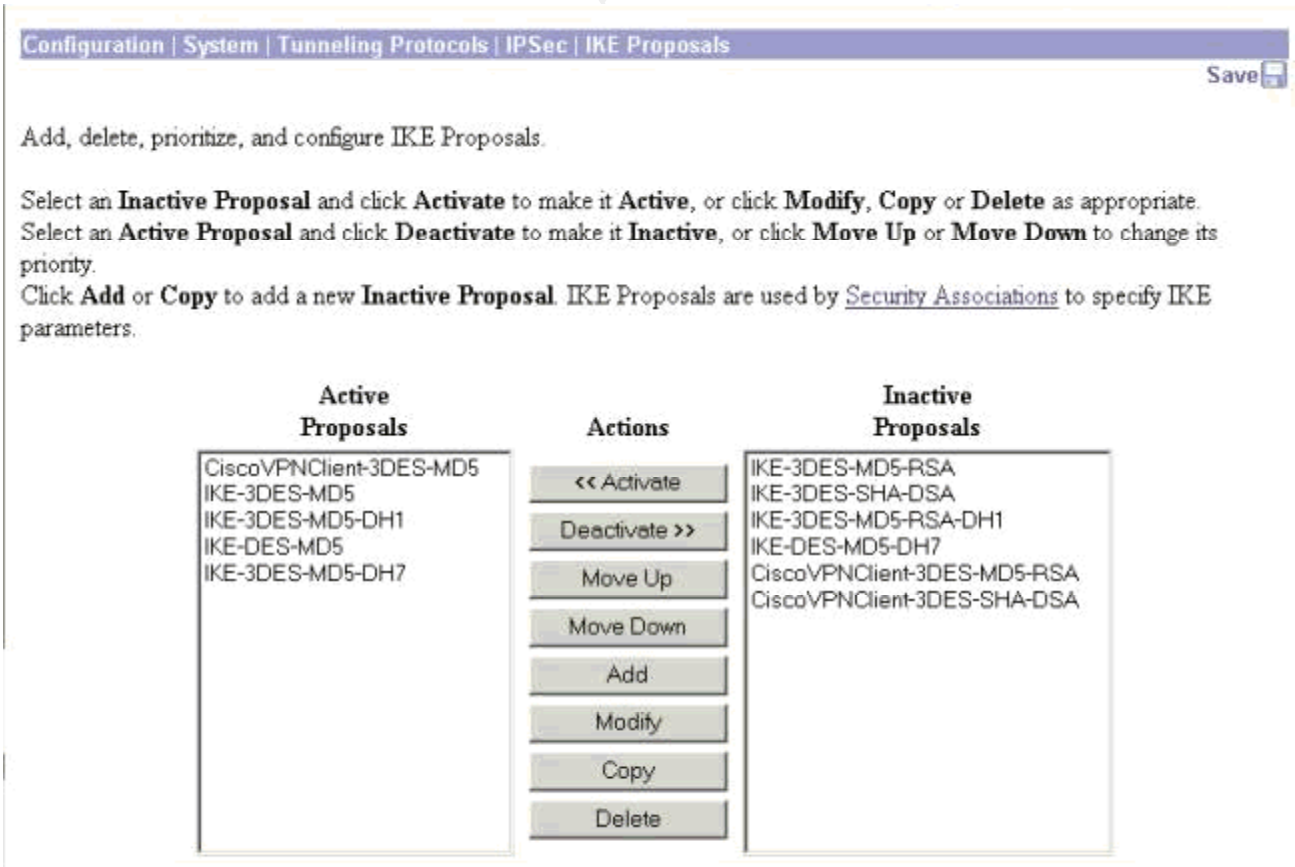
Under **Encryption we change it to 3DES and Under **IKE Proposal** above we change it to IKE-3DES-MD5 to reflect the GIAC requirements***



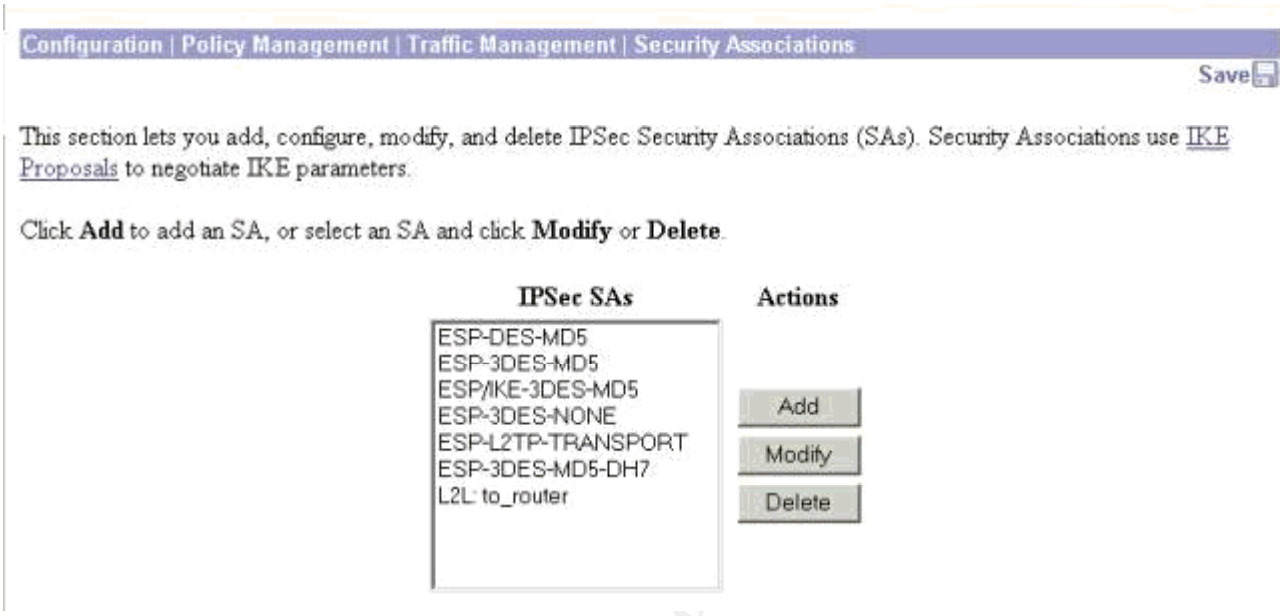
The previously created LAN-to-LAN IPSec parameters can be viewed or modified in **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN**.



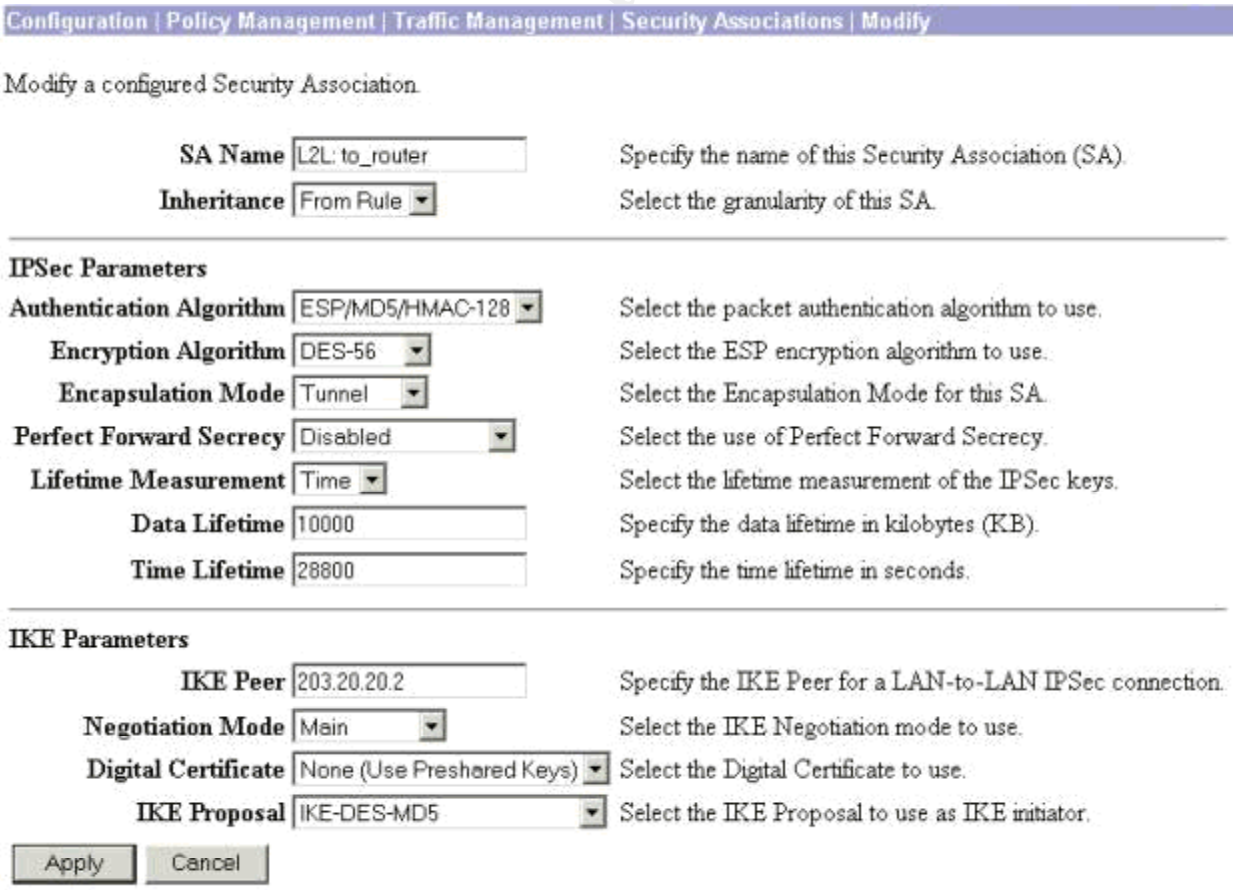
7. Select **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** to confirm the active IKE Proposal.



8. Select **Configuration > Policy Management > Traffic Management > Security Associations** to view the list of Security Associations.



9. To verify the Security Associations, click the Security Association name, and then click **Modify**.



****Under** Encryption Algorithm **we change it to 3DES and Under** IKE Proposal **above we change it to IKE-3DES-MD5 to reflect the GIAC requirements*****

`debug` and `show` Commands

On the Router

Before attempting any **debug** commands, please see Important Information on Debug Commands.

- **debug crypto engine** - Shows the traffic that is encrypted.
- **debug crypto ipsec** - To see the IPSec negotiations of phase 2.
- **debug crypto isakmp** - To see the ISAKMP negotiations of phase 1.
- **show crypto ipsec sa** - To view the settings used by current security associations.
- **show crypto isakmp sa** - To view all current Internet Key Exchange security associations (SAs) at a peer.
- **show crypto engine connection active** - To view the current active encrypted session connections for all crypto engines.

You can use the IOS Command Lookup Tool to see more information about particular commands. To use this tool, you must be a registered user and you must be logged in.

IOS Command Lookup

On the VPN Concentrator

To turn on logging, select **Configuration > System > Events > Classes > Modify**. The following options are available:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Severity to Log = 1-13

Severity to Console = 1-3

You can retrieve the event log by selecting **Monitoring > Event Log**.

GIAC Border Router Cisco 7206 ACL Policy

When anti-spoofing access lists exist, they should always reject datagrams with broadcast or multicast source addresses, and datagrams with the reserved "loopback" address as a source address. It's usually also appropriate for an anti-spoofing access list to filter out all ICMP redirects, regardless of source or destination address.

A mixture of Ingress and Egress filtering will be used. It has been decided to use **Standard and Extended Access Lists** on the Border Router.

!Global Configuration Commands

ip verify unicast rpf
no ip source-route
no ip bootp server
no cdp enable
no service finger
ip route 0.0.0.0 0.0.0.0 null 0 255
service tcp-keepalives-in
no service tcp-small-servers
no service udp-small-servers
no snmp
banner login
service password-encryption
enable secret *****

!Configure Internal Ethernet Interface

interface ethernet0

ip address 208.156.147.3 255.255.255.248
no ip directed-broadcast
no ip proxy-arp
no ip redirects

!Configure VPN Ethernet Interface

interface ethernet1
ip address 208.156.147.42 255.255.255.252
no ip directed-broadcast
no ip proxy-arp
no ip redirects
ip access-group 103 in
access-list 103 permit tcp any host 208.156.147.42 eq isakmp log
access-list 103 permit ip host 208.156.147.42 any log
access-list 103 permit eq ip-proto-50 host 208.156.147.42 any log

!Configure External Serial Interface

interface serial0
permit bgp any any
no ip redirects
no ip unreachables
no ip directed-broadcast
no ip proxy-arp
ip access-group 101 in
ip access-group 102 out

!Ingress and Egress Filters

!Block inbound ICMP.
access-list 101 deny any any eq icmp

!Deny outbound ICMP
access-list 102 deny any any eq icmp

!Block Direct Attacks Against the Firewall Interface
access-list 101 deny ip any host 208.156.147.1 log

! Block Private Net packets you should never see as a inbound source
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log

! Block Public Net packets you should never see as an inbound source
access-list 101 deny ip 208.156.147.0 0.0.0.255 any log

!Deny Loopback and Multicast Addresses you should never see as a inbound source
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 224.0.0.0 7.255.255.255 any log

!Deny any packets without a source address
access-list 101 deny ip host 0.0.0.0 any

Deny other unwanted inbound services like SSH, Telnet, FTP command port, and rlogin services.
access-list 101 deny tcp any any eq 22
access-list 101 deny tcp any any eq 23
access-list 101 deny tcp any any eq 21
access-list 101 deny tcp any any range 512 514

!VPN Traffic on serial interface
access-list 103 permit tcp any host 208.156.147.42 eq isakmp log
access-list 103 permit eq ip-proto-50 any host 208.156.147.42 log
access-list 103 deny ip any host 208.156.147.42 log
!Allow remaining systems to run and reply to TCP based services
access-list 101 permit ip any 208.156.147.0 0.0.0.255
access-list 102 permit ip 208.156.147.0 0.0.0.255 any

ACL descriptions

ACL descriptions -The following security ACL descriptions already applied in the above configuration, were found at http://www.cisco.com/warp/public/707/21.html.
Anti-spoofing with RPF checks
With Cisco Express Forwarding, it's possible to have the router check the source address of any packet against the interface through which the packet entered the router. If the input interface isn't a feasible path to the source address according to the routing table, the packet will be dropped. Since Symmetric Routing will be used, Cisco Express Forwarding will be enabled on the router in order to use this feature. This feature is known as a reverse path forwarding (RPF) check, and is enabled with the command
ip verify unicast rpf. It is available in Cisco IOS software 11.1CC, 11.1CT, 11.2GS, and all 12.0 and later versions, but requires that CEF be enabled in order to be effective.
This command will be enabled.

ip verify unicast rpf

In a "smurf" attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By using the **no ip directed-broadcast** command, command directed broadcasts that would cause link-layer broadcasts at that interface are dropped instead. This

command will be enabled.
no ip directed-broadcast

IP Source Routing - The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in real networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options. A Cisco router with the no ip source-route set will never forward an IP packet which carries a source routing option. You should use this command unless you know that your network needs source routing. This command will be enabled.

no ip source-route

Cisco Discovery Protocol (CDP) is used for some network management functions, but is dangerous in that it allows any system on a directly-connected segment to learn that the router is a Cisco device, and to determine the model number and the Cisco IOS software version being run. This information may in turn be used to design attacks against the

router. CDP information is accessible only to directly connected systems. The CDP protocol may be disabled with the global configuration command **no cdp running**. CDP may be disabled on a particular interface with **no cdp enable**. This command will be enabled.

no cdp enable

Might not want your border router to serve as a bootp server

no ip bootp server

Cisco routers provide an implementation of the "finger" service, which is used to find out which users are logged into a network device. Although this information isn't usually tremendously sensitive, it can sometimes be useful to an attacker. The "finger" service may be disabled with the command **no service finger.** This command will be enabled.

no service finger

Rapidly discard packets with invalid destination addresses. This command will be enabled

ip route 0.0.0.0 0.0.0.0 null 0 255

Detect and delete "dead" interactive sessions, preventing them from tying up VTYs**.** Can help to guard against both malicious attacks and "orphaned" sessions caused by remote system crashes. This command will be enabled

service tcp-keepalives-in

If the router receives a datagram in which it is unable to deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP Host Unreachable message. Use the ip unreachables interface subcommand to enable or

disable the sending of these messages. This command will be enabled

no ip unreachables

Provide a minimum of protection for configured passwords.

service password-encryption

Configure a password for privileged router access. This command will be enabled

enable secret password

By default, Cisco devices up through IOS version 11.3 offer the "small services": echo, chargen, and discard. These services, especially their UDP versions, are infrequently used for legitimate purposes, but can be used to launch denial of service and other attacks that would otherwise be prevented by packet filtering The small services are disabled by default in Cisco IOS 12.0 and later software. In earlier software, they may be disabled using the commands **no service tcp-small-servers** and **no service udp-small-servers.**
no service tcp-small-servers
no service udp-small-servers.

SNMP management stations often have large databases of authentication information, such as community strings. This information may provide access to many routers and other network devices. This concentration of information makes the SNMP management station a natural target for attack, and it should be secured accordingly.

SNMP version 2 will be used for GIAC devices, which supports an MD5-based digest authentication scheme, and allows for restricted access to various management data.
For SNMP version 2, configure digest authentication with the authentication and md5 keywords of the snmp-server party configuration command. If possible, use a different MD5 secret value for each router. Do *not* use the snmp-server community command for any purpose in a pure SNMP version 2 environment; this command implicitly enables SNMP version 1.

Warning Banners

Warning Banners - In some jurisdictions, civil and/or criminal prosecution of crackers who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. One way of providing this notification is to put it into a banner message configured with the Cisco IOS **banner login** command.

The following notice information will be put in the GIAC banner and written by the Legal Team.

- A notice that any use of the system may be logged or monitored without further notice, and that the resulting logs may be used as evidence in court.

- Specific notices required by specific local laws.

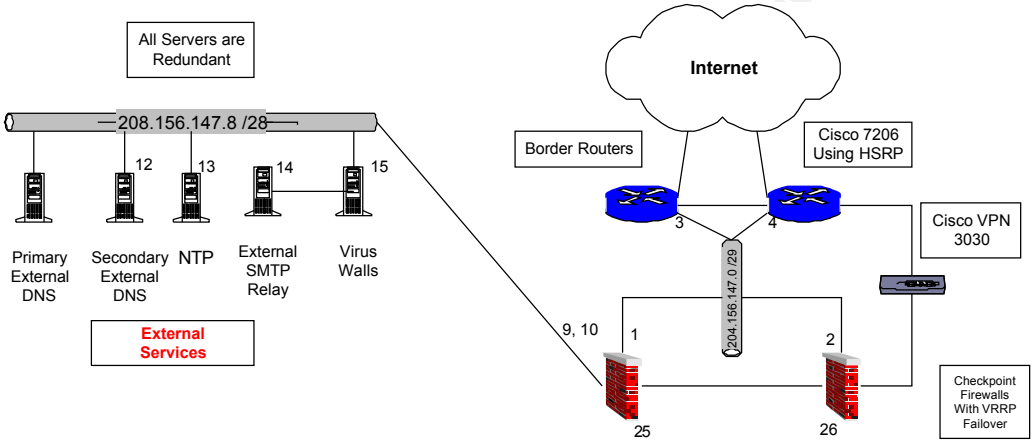
From a security, rather than a legal, point of view, your login banner usually should *not* contain any specific information about your router, its name, its model, what software it's running, or who owns it; crackers may abuse such information.

Establish a warning banner to be displayed to users who try to log into the router.

banner login

!!END of Border Router config….

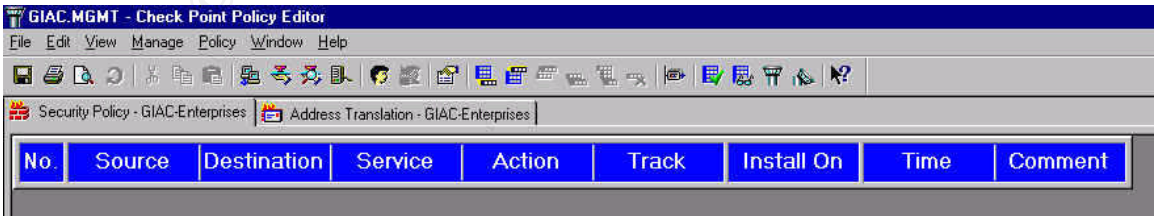
*****Checkpoint Border Firewall Policy Starting on Next Page*****



GIAC Checkpoint Border Firewall Security Policy

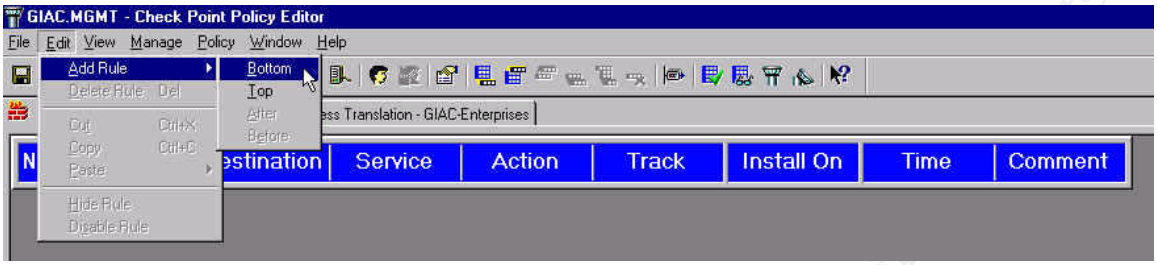
Using The Policy Editor:

The Border Firewall Sits behind the Border Routers and it is the main entry point for all GIAC Internet bound traffic. For the Border Checkpoint Firewall Policy, all traffic is dropped unless there is a rule for it. The graphic shown below shows a blank Checkpoint GUI Policy. A description of each column in the rulebase will follow the graphic.

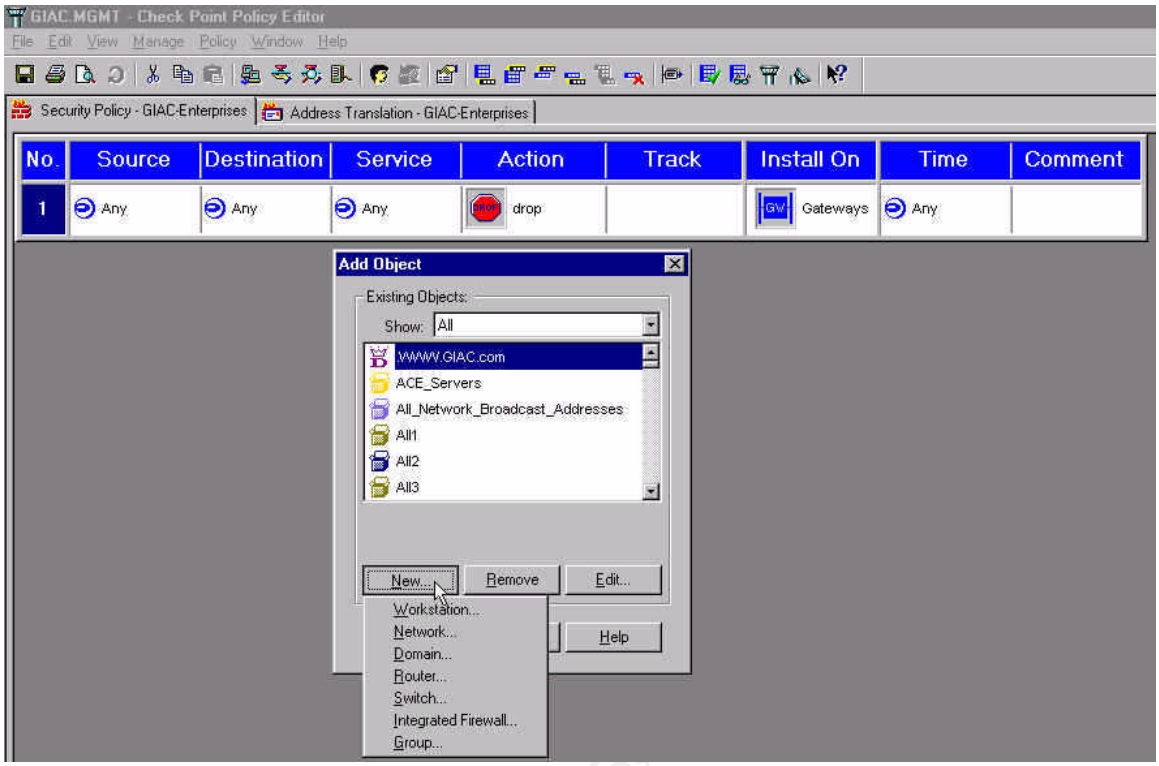


When you first run the client and connect to the management Server you will need to create a

new rulebase by choosing File - New. A dialog box comes up. Choose Empty Rulebase. It will prompt you to give the policy a name such as GIAC Enterprises. The result is shown above. The first time you add a rule you will do it by choosing Edit-Add Rule-Bottom shown below.



Your first rule pops up shown above. Theses are the default rule settings when creating a new rule, which are any any any drop. Notice the columns above in the blank rule. You have Source, Destination, Service, Action, Track, Install On, Time, and the Comment section. The Source, Destination, and Service fields are self-explanitory which, would be Source IP address Destination IP address and Services used. If you right click on the any box under Source and choose add, you will get a dialog box of objects to choose from shown in the graphic below. If your object is already created, choose it. If not choose new and notice the selections you can create below in the graphic.



Choose or create your Source, Destination and Service objects for your rule. The Next tab next to services is the Action tab. By right clicking in the white box under Action, will get the selections shown in the graphic below.

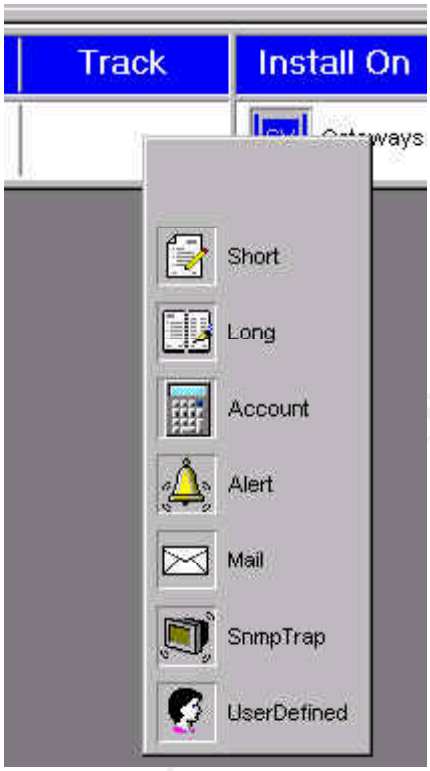
Here you can choose what to do with the packet or rule. You can choose whether to Accept, Drop, or Reject the packet along different forms of authentication methods. The difference between the Drop and Reject is that the reject sends back an ICMP message where the Drop drops the packet.

To Modify a Rule's Action:

1. Right-click on the rule's current value.
2. Choose one of the following options from the menu:
3.

Edit Properties - Edit the properties of the rule's Action.
Adds Encryption - Add Encryption to the Action for this rule.
Edit Encryption – This choice is available if the rule's existing Action is User, Client or Session Authentication, and encryption has been added.
Remove Encryption - Remove Encryption from the Action for this rule.
Accept the connection – Drop the connection and do not notify the sender – Reject the connection – Invoke User Authentication for the connection – Invoke Client Authentication for the connection – Invoke Session Authentication for the connection– Encrypt outgoing packets, accept and decrypt incoming packets – Client Encrypt – Accept only SecuRemote communications.

Next we have the **Track** Column shown below in the Graphic.



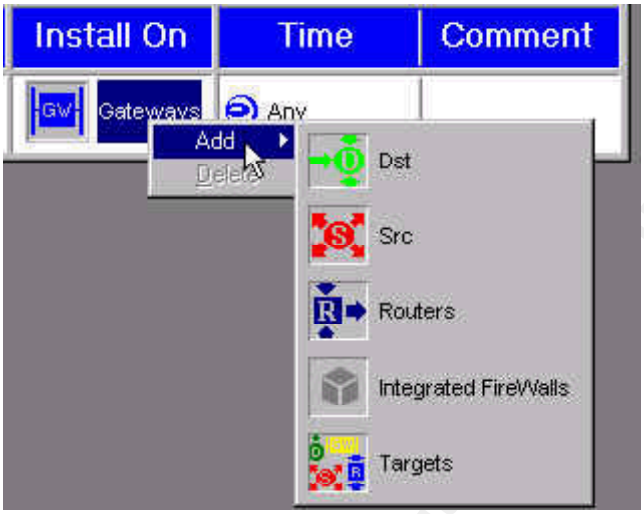
When you right click on the Tracking tab you get the choices shown above. Their descriptions are below.

To Modify a Rule's Track:

1. Right click on the value in Track.
2. Choose one of the following options from the menu:

Blank - No logging or alerting for this communication.
Short Log - Log in short format.
Long Log - Log in long format.
Account - Log in accounting format.
Alert - Issue an alert (as defined in the Popup Alert Command field in the Log and Alert tab of the Properties Setup window.
Mail - Send a mail alert (as defined in the Mail Alert Command field in the Log and Alert tab of the Properties Setup window.
SNMP Trap - Issue an SNMP trap (as defined in the SNMP Trap Alert Command field in the Log and Alert tab of the Properties Setup window.
User Defined - Issue a User Defined Alert (as defined in the User Defined Alert Command field in the Log and Alert tab of the Properties Setup window.

Next is the **Install On** column and its choices and descriptions are shown below**.**



The GIAC default Install On column setting is Gateways. Gateway means that it will install the policy on whatever firewall module the policy is pushed to. By Choosing Gateways it will filter traffic according to the setting in the policy properties tab, which is set to "inbound only". If you a specific firewall object for "Install On", it will filter traffic "Inbound" and "Outbound" which may cause overhead on the firewall. The only reason you would need that is if you had Internet connections on both sides of the firewall. The descriptions for the different settings are listed below.

The Install On field specifies which FireWalled objects will enforce the rule. The Install On object is not necessarily the packet's destination. For instance, a packet from the Internet destined for a local host must pass through the gateway. You may, therefore, choose to enforce your security policy on the gateway, even though the gateway is neither the source nor the destination. The entire security policy is installed on all the Install On objects, but each object enforces only that part of the security policy that is relevant to it.

To Modify the Install On Field:

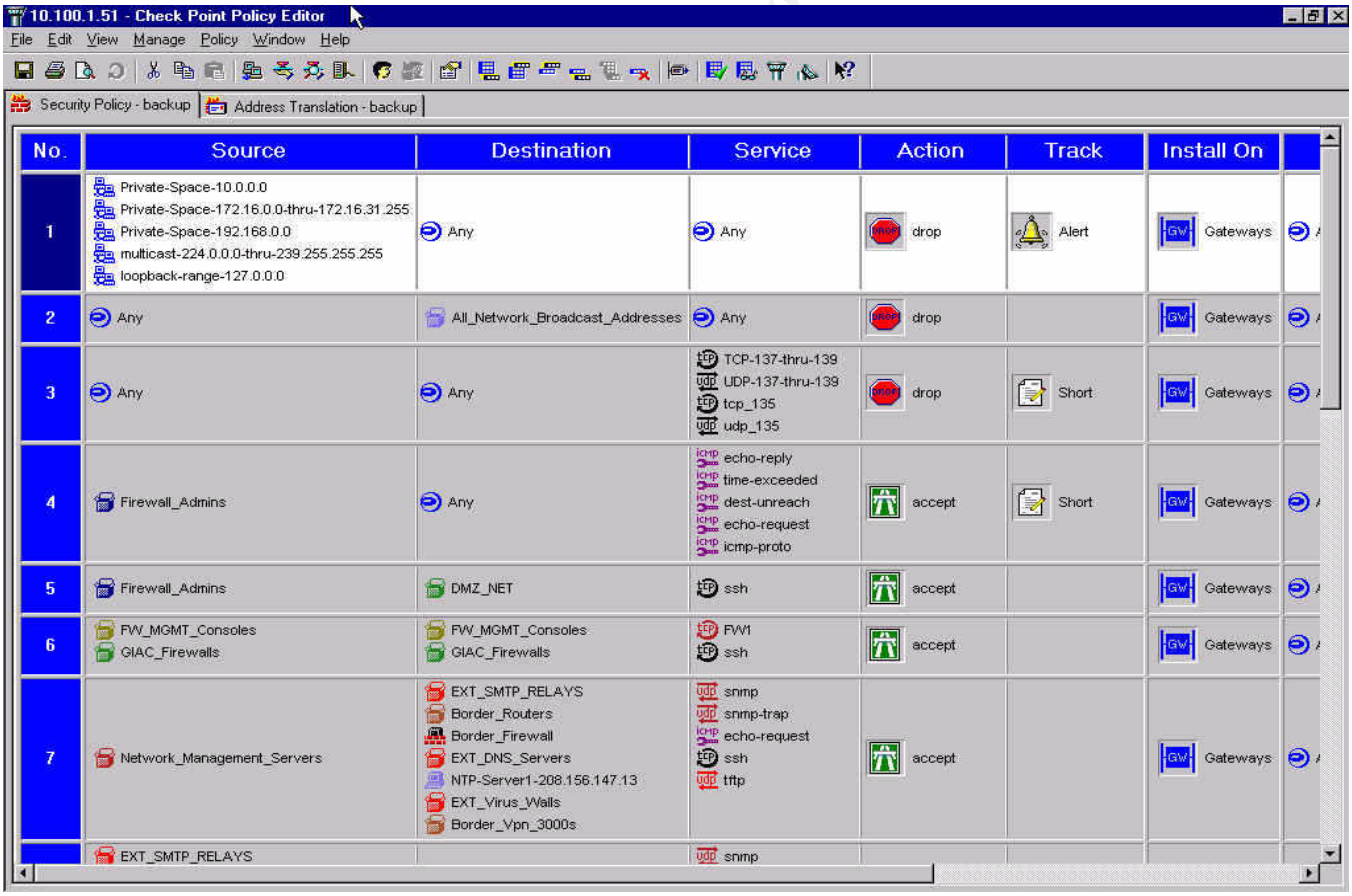
1. Right-click on the current value. You can only specify one value in the Install On field.
2. From the drop-down menu, choose one of the following:

Gateways - Enforce on all network objects defined as gateways, in the direction specified in the Apply Gateway Rules to Interface Direction property in the Security Policy tab of the Properties Setup window.
Destination - Enforce in the inbound direction on the FireWalled network objects defined as Destination (typically servers) in this rule.
Source - Enforce in the outbound direction on the FireWalled network objects defined as Source

(typically clients -initiators of traffic) in this rule.
Routers - Enforce on all routers
Integrated Firewalls - Enforce on all Integrated Firewalls
Targets – The Select Target window is displayed. Choose one or more objects. The rule is enforced on the specified target object(s) only, in the inbound and outbound (eitherbound) directions.

GIAC Policy Rules Described:

Now that we have had a basic tutorial in the Checkpoint GUI Policy Editor, the GIAC rulebase for the Border firewall can be analyzed. There are a total of four firewalls in the GIAC DMZ and each one will have its own separate policy similar to this one. Because of time and study constraints, only the primary firewall policy is submitted The Border firewall policy currently has 23 rules. Each one will be described below.



Rule #1 Rule one says that any private address space, multicast traffic, and loop back traffic will be dropped. A little anti-spoofing protection here since the border firewall should never see these private addresses as a source coming from the Internet.

Rule #2 Rule two says that any source destined for any of our network broadcast addresses,

drop the traffic. This will help to protect against smurf attacks to broadcast addresses from the Internet in case the border router gets compromised.
Rule #3 Rule three **shown above** will Drop Unwanted Microsoft/NetBios Traffic on ports 135, 137, 138, and 139. Don't need any unneeded Microsoft vulnerabilities.

Rule #4 Rule four **shown above** will allow the security admins to ping and traceroute within the DMZ network for troubleshooting. Notice the **source** field of rule four there is a Firewall_Admin group, groups can be used for grouping alike objects.
Destination is any using a few ICMP services for troubleshooting DMZ devices.

Rule #5 Rule five **shown above** will allow Firewall Admins to SSH into the FW Management Console or any device in the DMZ. The admins can only access the firewalls using SSH to the firewall management stations in the Secure Net.

Rule #6 Rule six **shown above** allows the firewall management consoles to talk to the firewalls. Once the admin SSH's into the mgmt console using rule five, rule six lets him have access to the firewalls using SSH because the management station can talk to the firewalls. The FW1 protocol is needed to communicate between the mgmt station and the firewalls.

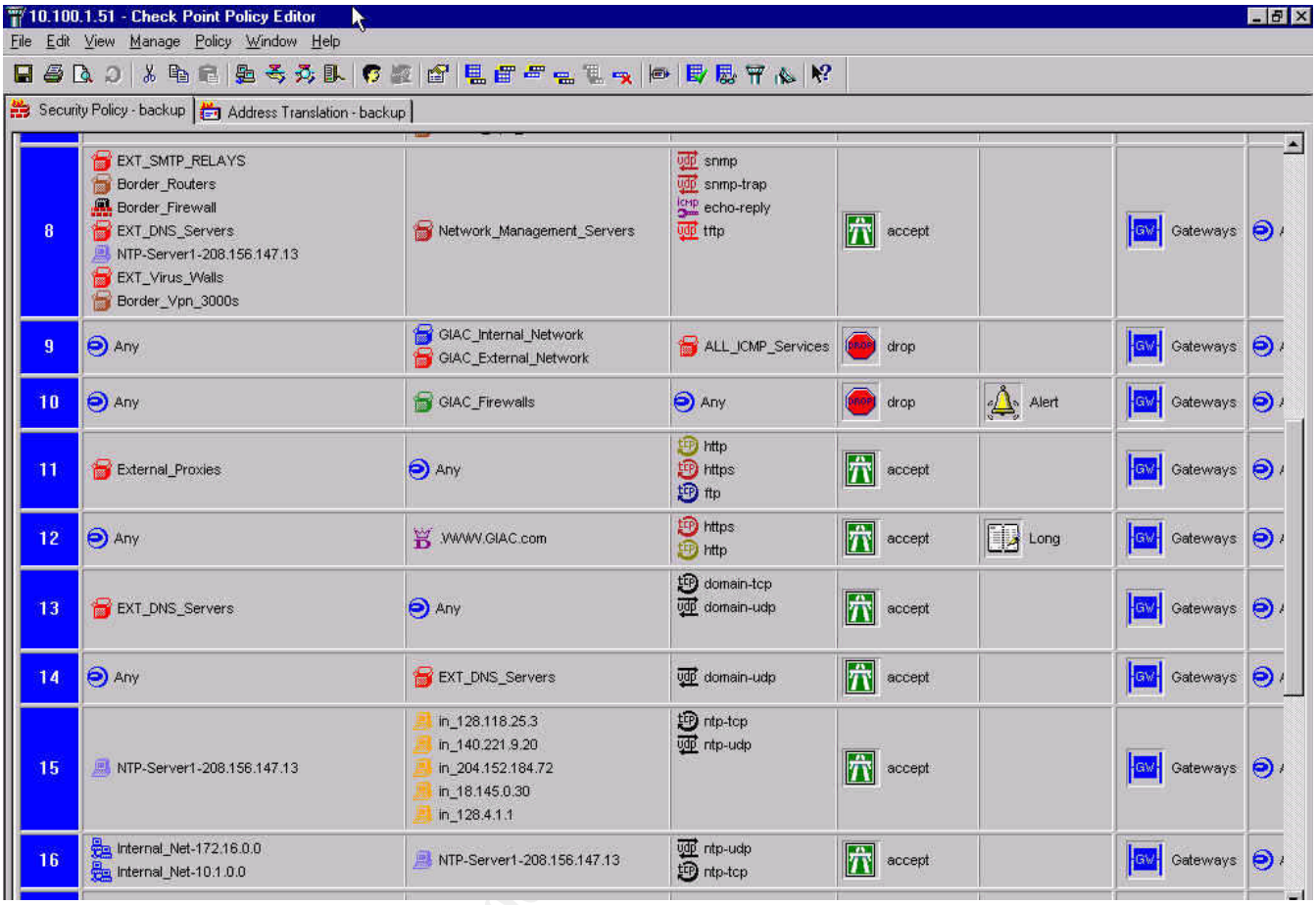
Rule #7 Rule seven **shown above** will allow HP Openview and Cisco Works Access traffic from the Network Management Servers, to all devices in the External Net including the Border Router, Border Firewall, and VPN 3030 Concentrator. Protocols used are snmp and snmp trap for device management, echo-request so the mgmt station can ping the devices, SSH, and TFTP for data transfer.

Rule #8 Rule eight **shown below** will allow return Access from devices in the External Net back to HP Openview and Cisco Works Management Servers. The echo-reply is return traffic for the echo-requests allowed in rule seven.

Rule #9 Rule nine **shown below** says to drop any ICMP services destined for our network. Any special allowed ICMP Services must be allowed before this rule like rule # 4, 7, and 8.

Rule #10 AKA called the "Stealth Rule". This rule **shown below** will drop anything destined for the firewall interface addresses and sound an alert!. No traffic should ever be destined for the firewall interface there are vulnerabilities exposed shown in assignment 4 when you leave out the stealth rule.

Rule #11 Rule eleven **shown below** allows the external proxies outbound to the Internet using http, https, and passive ftp thru the browser interface. Because the firewall keeps state tables of these initiated internal connections, a return rule is not needed



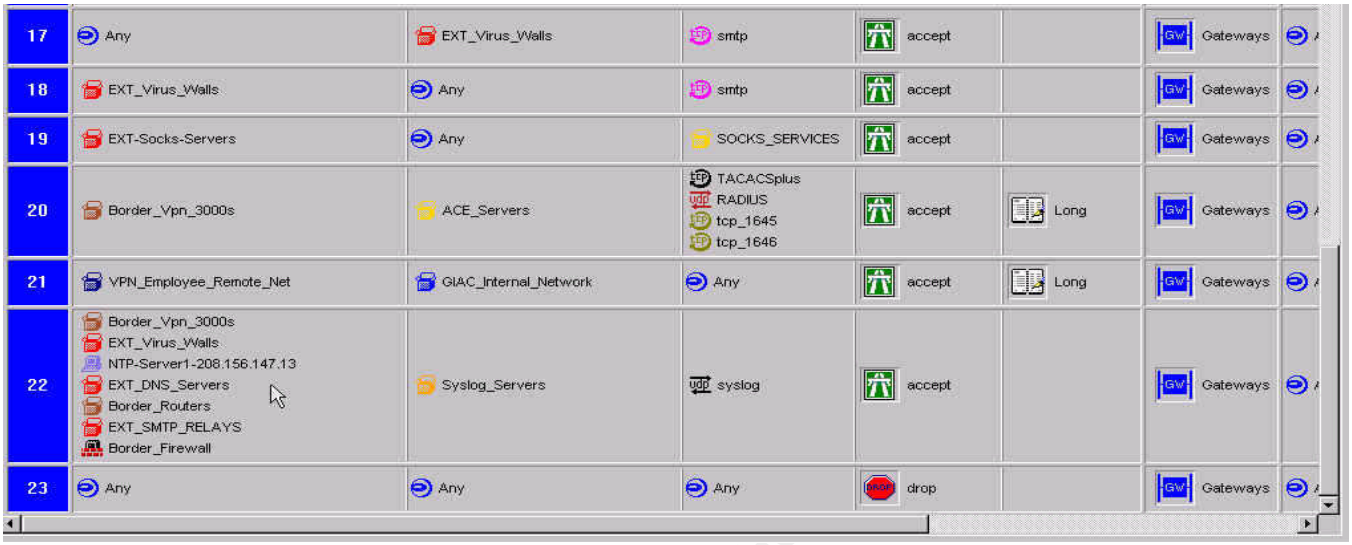
Rule #12 Rule twelve **shown above** will allow inbound Web Traffic to the GIAC.com Corporate site. This is the only http and https traffic to get logged. Queries from the Internet to the giac.com domain point to the reverse proxies in the proxy layer. Because the firewall keeps state tables of these initiated external connections, a return rule is not needed.

Rule #13 Rule thirteen **shown above** will allow outbound DNS Servers to the Internet using tcp and udp 53 outbound for outbound zone transfers only to root servers since it is authoritative for the GIAC.com zone.

Rule #14 Rule fourteen **shown above** will allow inbound DNS to DNS servers using only udp 53.

Rule #15 Rule fifteen **shown above** will allow the NTP servers to access to stratum 1-time servers on the Internet.

Rule #16 Rule sixteen **shown above** will allow the internal net to do NTP queries to NTP server.



17	Any	EXT_Virus_Walls	smtp	accept		Gateways	
18	EXT_Virus_Walls	Any	smtp	accept		Gateways	
19	EXT-Socks-Servers	Any	SOCKS_SERVICES	accept		Gateways	
20	Border_Vpn_3000s	ACE_Servers	TACACSplus RADIUS tcp_1645 tcp_1646	accept	Long	Gateways	
21	VPN_Employee_Remote_Net	GIAC_Internal_Network	Any	accept	Long	Gateways	
22	Border_Vpn_3000s EXT_Virus_Walls NTP-Server1-208.156.147.13 EXT_DNS_Servers Border_Routers EXT_SMTP_RELAYS Border_Firewall	Syslog_Servers	syslog	accept		Gateways	
23	Any	Any	Any	drop		Gateways	

Rule #17 Rule seventeen **shown above** will allow smtp mail (port 25) from the Internet to Virus Wall servers. Only the virus walls which, are in series with the SMTP relay, can talk to the actual external SMTP server to improve security.

Rule #18 Rule eighteen **shown** above will allow the Virus Wall Servers to send outbound SMTP services and allow External Virus Wall Servers to also talk to the Internal Mail Servers

Rule #19 Rule nineteen **shown above** will allow the needed Socks Services outbound. The socks servers will be using TCP wrappers to enforce a policy of who gets inbound and outbound access. Anything that cannot use the Internet proxies must use socks to connect over the Internet.

Rule #20 Rule twenty **shown** above will allow VPN User Authentication to the ACE servers

Rule #21 Rule twenty-one **shown above** will allow Vpn traffic over the Internet into the network and log it.

Rule #22 Rule twenty-two **shown above** will allow the External Services Devices including the Border Router, Border Firewall, and VPN 3030 Concentrator to send syslog data to syslog servers.

Rule #23 Rule twenty-three **shown above** will be the "Clean Up Rule". It will drop and log any traffic not defined in the rule base. A drop ensures that there is no message sent back to the sender of the packet.

Assignment #3 - Scott Baker - Audit Primary Firewall Security Architecture

Audit Plan:

Action Items #

1) Interview owners and system administrators for business requirements for inbound and outbound traffic, VPN remote access, virus protection, and fail over.

2) Create logical diagrams of traffic flow from company interviews and reviewing the security policy.

3) Review firewall architecture to see if it meets business requirements. Issues to review would be:

    a. Perimeter design
    b. Physical layouts of switches
    c. Network Address Translation,
    d. Firewall type such as stateful inspection

4) Review Firewall platform and application. Ensure that the latest tested and approved patches are applied to the firewall OS platform and the firewall application by checking with vendor sites for latest updates.

5) Review rulebase manually one by one for unneeded or unauthorized rules. Test for vulnerable open services.

    a. Confirm that the firewall is secure by using tools to check installed packages and scan for vulnerable open services.
    b. Try consolidating rules if possible to reduce the size of the rulebase. Ensure that comments in the rulebase include a description of the rule, ticket or request number, administrator's initials, and date for tracking and auditing purposes.
    c. Review rulebase backup procedures for quick back out plan when a new rulebase is implemented.

6) Test any firewall applications such as virus scanners, fail over, proxy filters, encryption, and authentication schemes.

7) Review firewall logging and alerting for proper detection.

8) Review firewall admin password policies, read/write access, admin account creations, patch back out procedures, and standardization for OS builds for the firewalls.

9) Review change control policies for adding or removing hardware, rule changes, change

documentation, and backing out changes.

GIAC Security Policy

The following security policy was submitted to the Audit Team from the GIAC Management Team.

Outbound Internet Policy – All internal users will access the Internet thru the internal Internet proxies. No http or https traffic will be allowed outbound unless it meets this requirement.

Inbound Internet Policy – Any traffic destined for the company site www.giac.com will use the reverse proxy, which will point to the actual internal web server. Incoming traffic to the company site will never actually make a direct request to the actual web server.

SMTP Mail Services – All outgoing internal mail will point to the internal mail servers. The internal mail servers will forward the mail to the virus walls for virus scanning and content checking. The virus walls will send the scanned mail to the SMTP Relay and off to its destination. Incoming mail will take the reverse path into the network. Its first stop will be to the virus wall servers. The virus wall servers will send it to the SMTP relay, which will forward it on to the internal mail servers. Any mail with detected viruses will be quarantined with a message sent to the administrator and internal user stating the nature of the findings and action taken.

Socks Services – All other traffic destined for the Internet must use the socks servers. The appointed security team must approve any exceptions.

Remote Access – Any employees needing remote access will access the network thru the company provided VPN using two factor SecureID authentication. After security team and management approval, the employee will download the latest approved VPN client from the company web site, which will include configuration instructions.

Business Partner Access – Business Partner access traffic must use a VPN to connect and encrypt the traffic to and from the company network. IPSec, Triple DES, and ESP will be the company standard for encryption schemes. A CiscoVPN 3030 will be used for Business Partner's to connecting to the company network.

Business Partner FTP Services – An ftp server Drop Box will be provide for the Business Partners to transfer data to and from the company network. All users will be required to authenticate to the ftp server with a user name and password. Anonymous ftp will not be permitted. **SFTP** will be used if any transfers enter the internal network or DMZ.

Firewall Admin Access – All firewall admin's will use the SSH protocol to connect to management devices on the network. To access the firewalls the admin must SSH to the management station in the secure net first to manage them.

© SANS Institute 2000 - 2005 Author retains full rights.

Firewall Rule Requests – Any firewall rule requests will be submitted using the company ticket system for tracking. Before applying the request it must be approved by the security team and submitted to change control for tracking. The ticket number along with the description of the rule will be put in the comments field in the firewall rule base for auditing purposes

Conduct The Audit:

Action Item # 1

Interview owners and system administrators for business requirements for inbound and outbound traffic, VPN remote access, virus protection, and fail over.

Interviews were conducted with the owners and system administrators discussing business requirements for inbound and outbound traffic, VPN remote access, virus protection, and fail over.

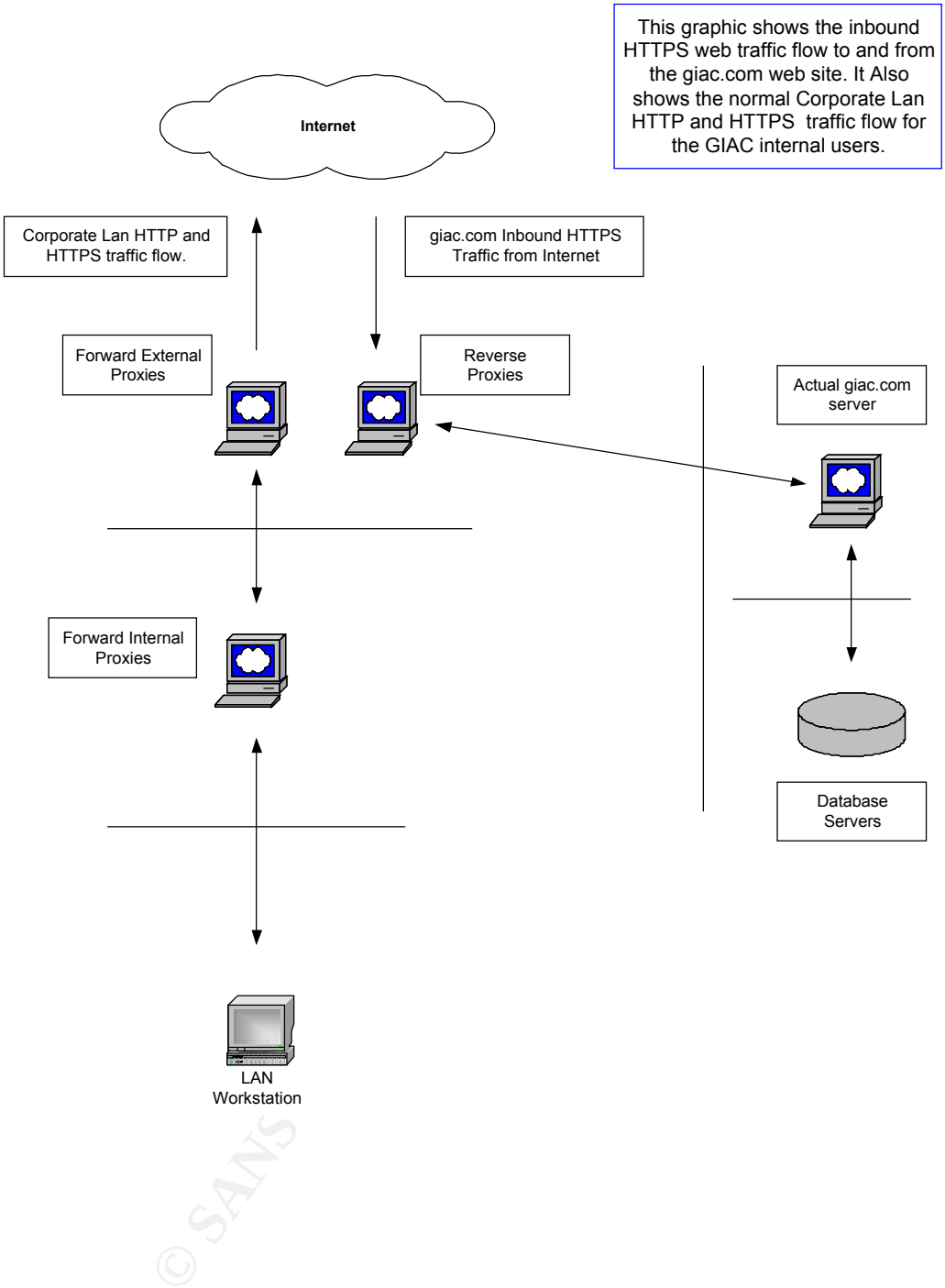
Recommended Action item # 1

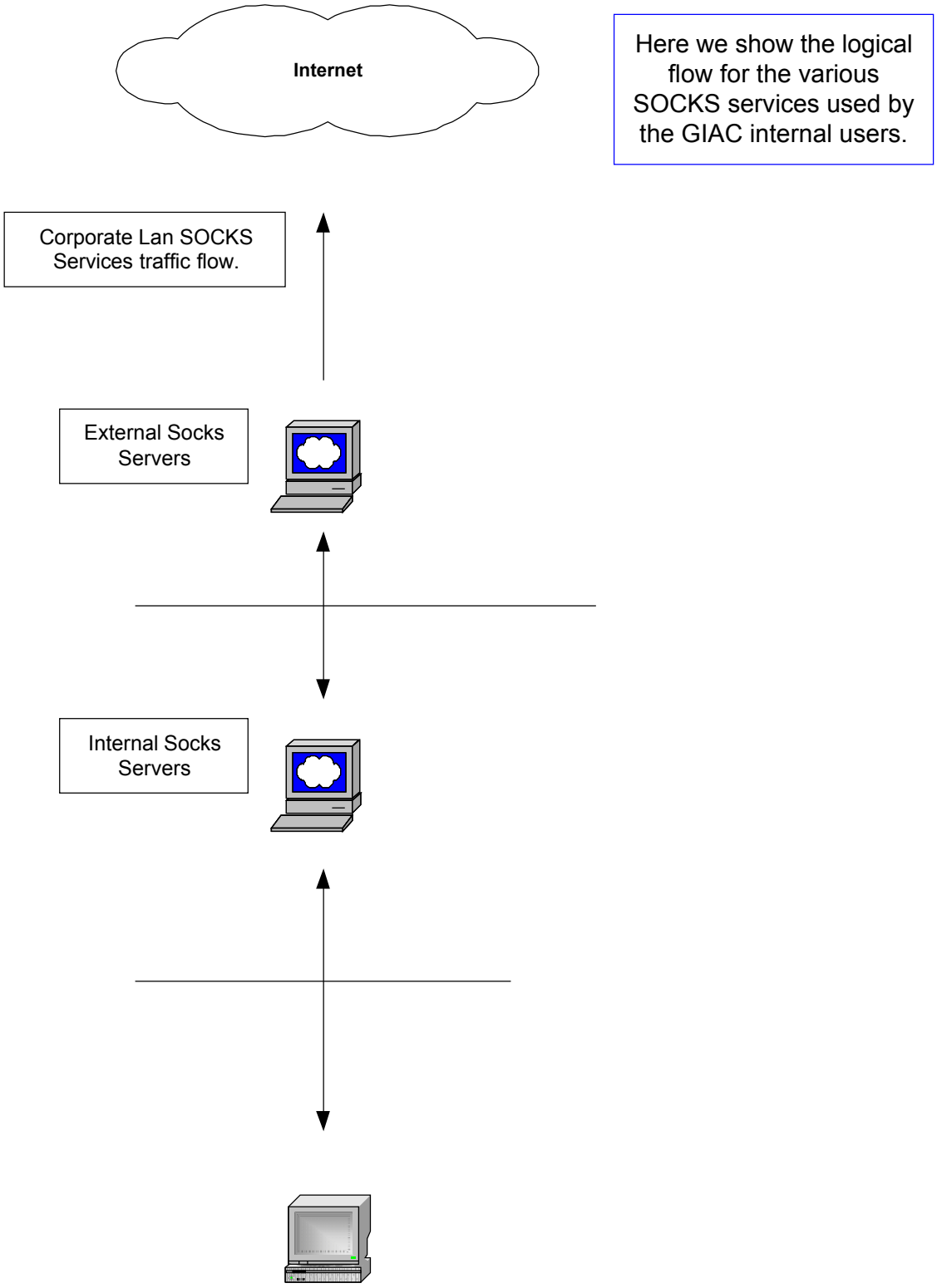
After interviewing the owners and system administrators and viewing physical diagrams it is recommended that we create logical diagrams to show the flow of traffic for the different special services. These logical diagrams are shown on the next few pages.

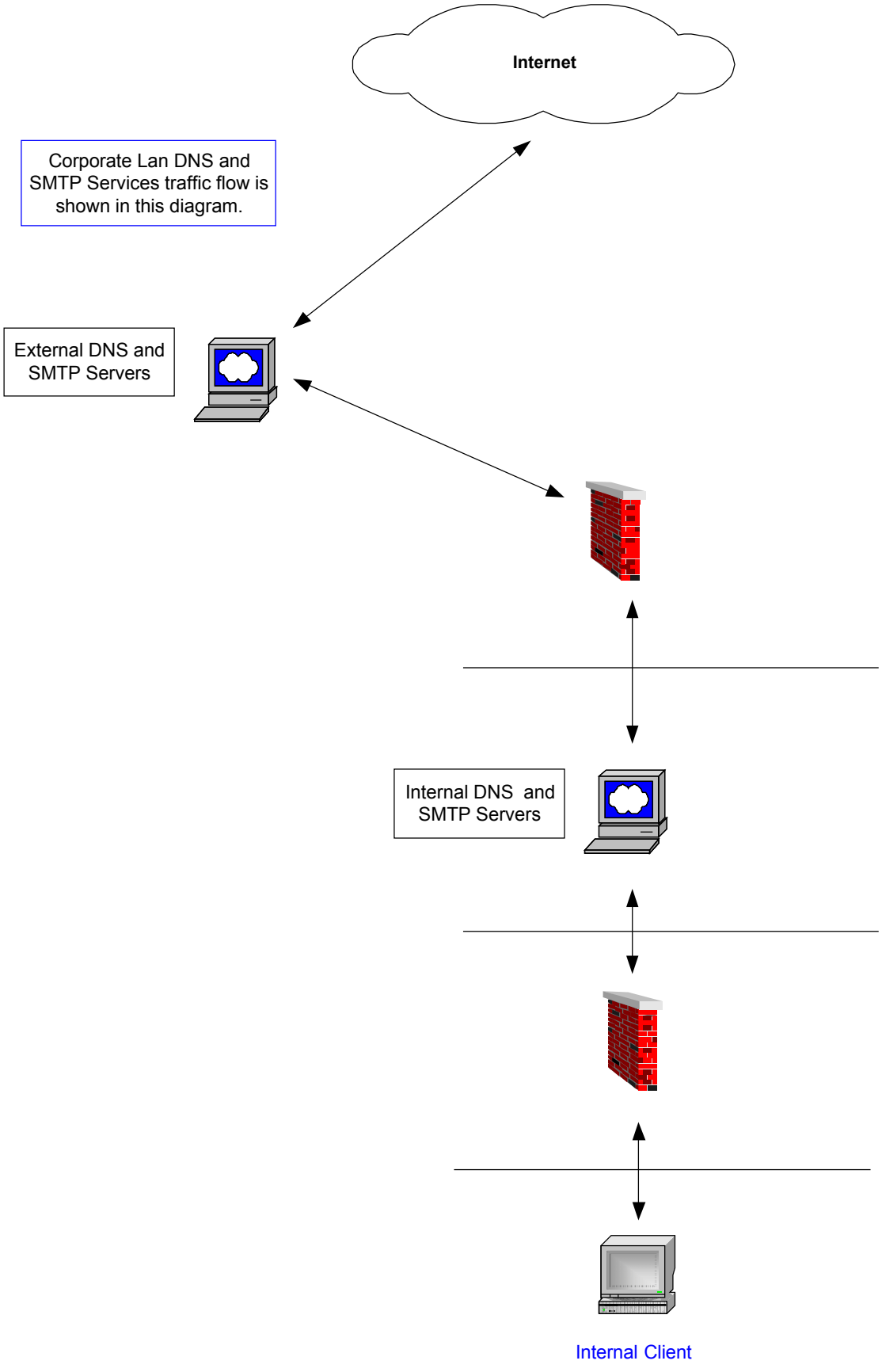
Action Item # 2

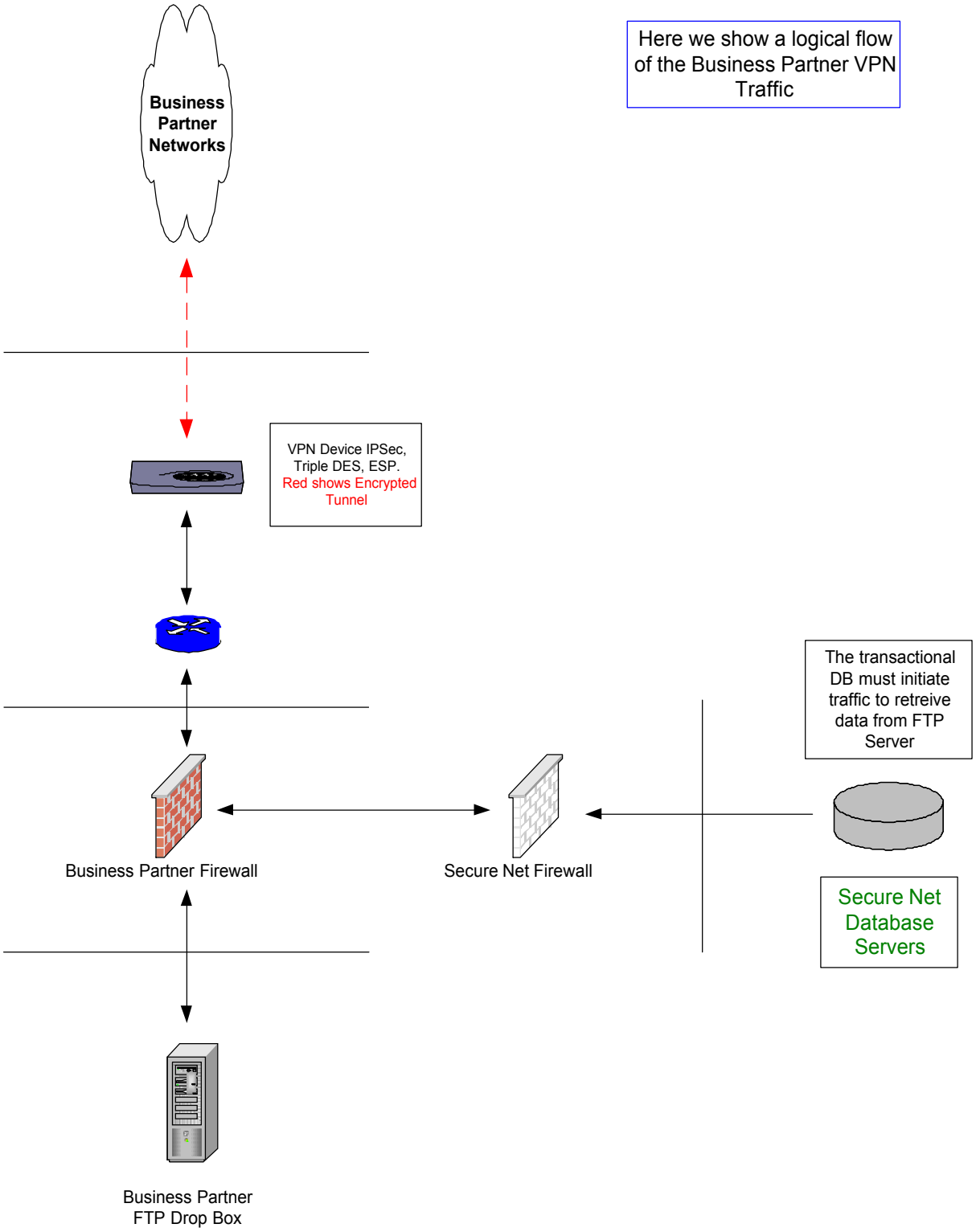
Create logical diagrams of traffic flow from company interviews and reviewing the security policy.

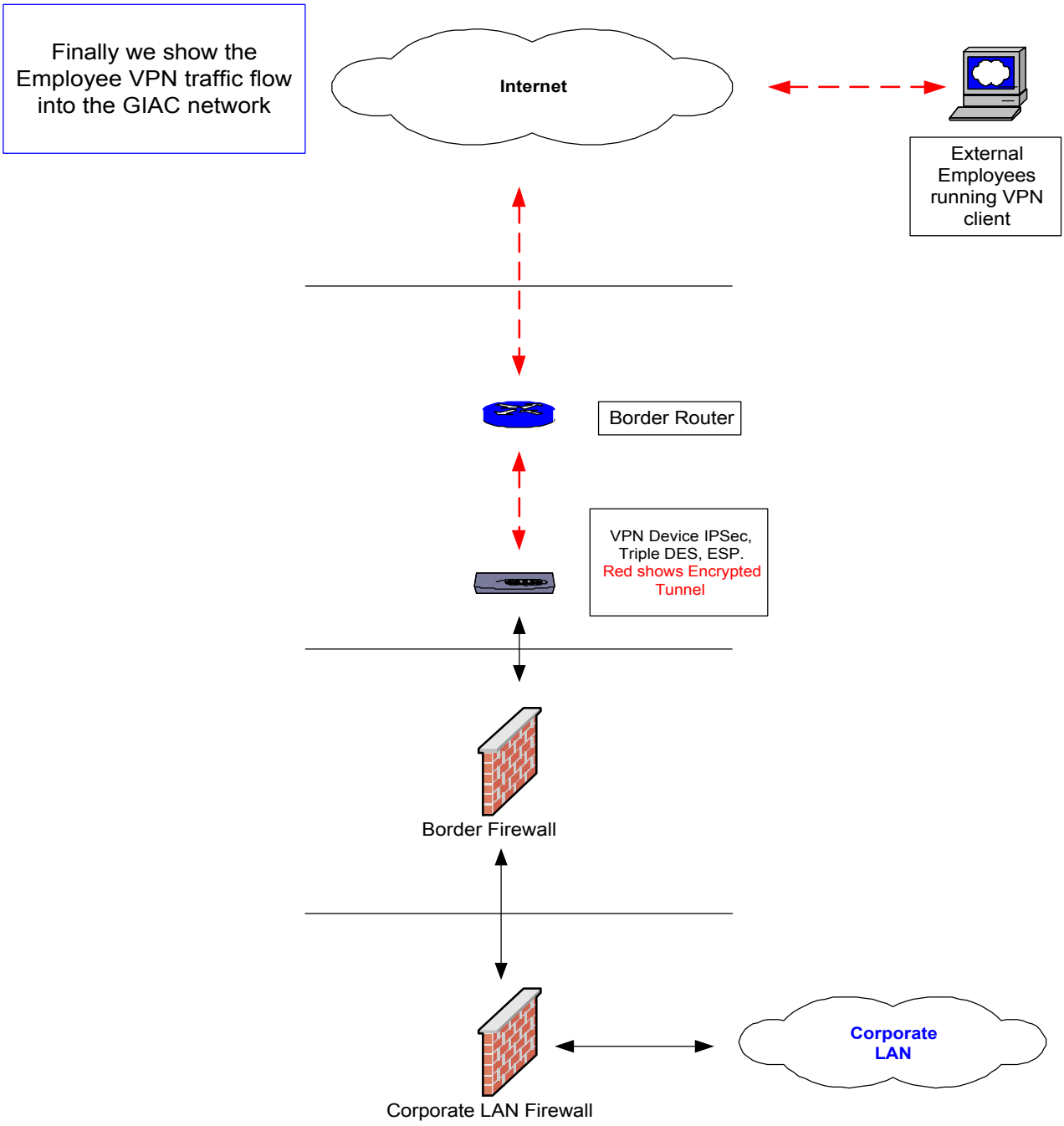
GIAC Logical Diagrams Shown Starting on Next Page


This graphic shows the inbound HTTPS web traffic flow to and from the giac.com web site. It Also shows the normal Corporate Lan HTTP and HTTPS traffic flow for the GIAC internal users.
Internet
Corporate Lan HTTP and HTTPS traffic flow.
giac.com Inbound HTTPS Traffic from Internet
Forward External Proxies
Reverse Proxies
Actual giac.com server
Forward Internal Proxies
Database Servers
LAN Workstation


Internet
Here we show the logical flow for the various SOCKS services used by the GIAC internal users.
Corporate Lan SOCKS Services traffic flow.
External Socks Servers
Internal Socks Servers
Socks Internal Client







Action Item # 3

Review firewall architecture to see if it meets business requirements

The Audit Team researched the architecture of the Nokia IP650 firewall at https://www.support.nokia.com/ and found that the architecture is a hardened secure appliance that meets the GIAC requirements. It supports NAT, uses Stateful Inspection, supports SSH secure connections, and has tools for web based configuration management using Nokia Voyager over SSL or Lynx for a command line version. The appliance comes pre-configured. Some of the findings are listed below:

IP Network Security Solutions
P R OT E C T YO U R N E T W O R K
The Nokia IP650 is an optimized, mid-range carrier-class security platform delivering firewall, VPN, and intrusion detection systems to corporate data centers and large enterprises. The Nokia IP650 is purpose-built for the most demanding network environments such as high traffic e-commerce sites, data warehouses, and service provider data centers. At two rack units, the Nokia IP650 is a high port density system, conserving valuable rack space. With redundant power supplies and hot-swappable interface cards, the Nokia IP650 is intended for environments that require the highest levels of network uptime.
The Nokia IP650 comes with five CPCI slots for optional WAN and LAN interfaces. The wide variety of connectivity options include quad port 10/100 Ethernet, optical Gigabit Ethernet, high speed ATM, HSSI, and wide area network interfaces such as V.35/X.21, or T1/E1 allowing the IP650 to be easily integrated into any network architecture.

Nokia IP650 at a Glance

Internet Protocol
• IP RFC791
• ICMP RFC792
• ARP RFC826
• ICMP Router Discovery (Server) RFC1256
• CIDR RFC1519
• Static Routes
• RIP RFC1058
• RIP Version 2 (with authentication) RFC1723
• OSPF RFC2328
• DVMRP (multicast) RFC1075
• IGMP (multicast) RFC2236
• PIM-DM (multicast)
• PIM-SM
• Multicast Tunnels
• IGRP (optional) Cisco
• BGP4 (optional) RFC1771
• IPv6 core RFCs
• Requirements for IPv4 Routers RFC1812
• Differentiated Services (EF) RFC2598
• Bootp/DHCP Relay RFC2131
• Route Aggregation
• Route Redistribution
• Unnumbered Interfaces

LAN Support
• 10/100 Mbps Ethernet
• Multi-mode fiber Gigabit Ethernet

WAN Support
• PPP RFC1661, 1662
• Frame Relay FRF.1, RFC1490
• HDLC Cisco
•ATM
• ISDN BRI
• T1/E1 (optional)
• V.35/X.21 (optional)

Nokia IP650

Nokia IP650

Standard:
5 Hot-swap CPCI Interface Slots
Optional Interfaces:
- Quad-port 10/100 Ethernet
- T1/E1 with CSU/DSU
- Single- and dual-port serial V.35/X.21
- HSSI
- ATM Multi-Mode Fiber
- External Modem
- ISDN-BRI (Euro-ISDN)
- Multi-mode fiber Gigabit Ethernet

Height 3.5 in. / 9 cm (2RU)
Depth 18 in. / 46 cm
Width 17 in. / 43 cm
Weight 35 lbs. / 16 kg
Standard 19-inch rack mountable

Management
• SNMP RFC1157
• SNMPv2c
• SNMPv3
• Telnet RFC854
• FTP RFC959
• SSHv2 (secure Telnet & FTP)
• HTTP Server RFC2068
• SSL/TLS RFC2246
• Command Line Utilities
• Supported in Nokia Horizon Manager

High Availability
• VRRP RFC2338
• FireWall-1 State Sync

Security
• Secure Administrative Access
• Read/Write and Read-Only Access Modes
• SSH (secure Telnet & FTP)
• SSL/TLS (secure HTTP) RFC2246
• S/Key (one-time password) RFC1760
• Access Control Lists
• Traffic Management
• MD5 Routing
Authentication (RIPv2) RFC1723
• Centralized Authentication
• Native IPSEC (for non-firewall applications)

Application Acceleration
• Firewall Flows
• VPN Acceleration Card (optional)

System Status
Indications
• 10/100 Ethernet port status

Environment
• Temperature: 5°C to 40°C
• Humidity: 10% - 90% (non-condensing)

• Altitude: 10,000 ft.

Safety

• UL1950, CE Mark, CUL/CSA 22.2
NO. 950-M93, IE950, TUV EN60950

Emission Compliance

• FCC Part 15, Class A, EN55022
(CISPR22, Class A) CEMark

Nokia Internet Communications

Americas

Tel: 1 877 997 9199
E-mail: internet.na@nokia.com

Europe, Middle East and Africa

European Customer Inquiry Number
(toll-free): 00800 5543 1816
Outside toll-free area: +49 231 754 6011
E-mail: internet.emea@nokia.com

Asia Pacific

Tel: +65 588 3364
E-mail: internet.apac@nokia.com

An integrated security solution

By integrating market-leading Check Point™ VPN-1™ and FireWall-1 ® software with high-performance IP routing on an optimized network security platform, Nokia delivers the industry‘s most powerful Internet security solutions.
With Nokia Firewall/VPN appliances, organizations can deploy a single, integrated solution providing secure Internet communi-cations and access control for enterprise networks ranging from carrier-class central office solutions to the smallest regional office environments. A full suite of routing protocols such as RIP, OSPF, DVMRP, BGP, VRRP, and IGRP are included on the Nokia Firewall/VPN appliance.

High availability firewalls

Mission-critical applications in today‘s e-business environments require continuous network availability in a fail-safe infrastrucure. Virtual Router Redundancy Protocol (VRRP, RFC2338)—a standard on all Nokia IP Network Security Platforms enables load-sharing and active redundancy between two or more Nokia systems. Coupled with firewall synchronization technology from Check Point Software Technologies, Ltd., VRRP ensures that access to the network is always available.
Substantial financial loss can occur if a VPN gateway or firewall becomes unreachable for even a few seconds. Should a failover occur, Nokia Firewall/VPN appliances maintain all

VPN and firewall connections.

Virtual Private Networking

With VPN technology, the Internet is securely leveraged to reduce the costs previously associated with private network communications while also increasing the confidentiality of information being transmitted. Check Point and Nokia have teamed up to provide a VPN solution that is intuitive and cost effective, with a typical return on investment within a few months. As VPN traffic grows, Nokia Firewall/VPN appliances scale to meet the increasing network demands—protecting the invest-ment while securing the assets.

Ease of deployment

Nokia simplifies deployment by integrating key network functionality and applications into a single access device. Nokia Firewall/VPN appliances are security specific devices delivered onsite with all the necessary security software, hardware drivers, and IP routing pre-installed for out-of-the-box deployment. Many of the preliminary tasks required to implement a security solution, such as installing and testing network interfaces and patching and optimizing the security application and operating system, are performed at the factory before a system is shipped. This dramatically reduces commissioning time and eliminates the need for administration at remote sites. With Nokia Firewall/VPN appliances, network managers can begin enforcing security policy and enabling trusted communications within minutes.

Centralized and remote management

There are three complementary tools available to perform comprehensive management functions. Nokia Voyager provides element management using a browser over secure sockets layer (SSL). Nokia Horizon Manager performs software inventory and updates

Action Item # 3 continued

The audit team looked at switch selection and perimeter design also. GIAC uses Cisco 2950's switches that have Gigabit capabilities and satisfy today's requirements. They are described in detail in assignment one.

Recommended Action item #3

The perimeter design was studied by reviewing physical diagrams, logical diagrams, hardware used, and the security policy. The team found that when configured correctly, the design meets the secure business needs and requirements for the customers, suppliers, partners, and GIAC employees.

Action Item # 4

Review Firewall platform and application.

The audit team will ensure that the latest tested and approved patches are applied to the firewall OS platform and the firewall application by checking with vendor sites for latest updates.

The firewall platform is a modified Free BSD OS running on a Nokia IP650. By typing the following command "**uname –a"** at the IPSO command line, the IPSO version that the machine is running can be found. The GIAC version 3.3.1 output is shown below.

NokiaIP650Machine #**uname –a**
output: IPSO Borderf 3.3.1 -FCS5 ericveum 911 11.07.2000-013201 i386

IPSO version is 3.3.1

Nokia's web site also provides information on the latest Checkpoint 4.1 patches. GIAC is currently running version SP4 and SP5 has been released for 3 months. By going into the Lynx tool or Voyager you can look at your IPSO and Checkpoint patch levels also.

Recommended Action item # 4

The Audit team found that the GIAC firewalls were running IPSO version 3.3.1. The new release notes shown below state lots of new interesting features that can be useful. The team will recommend updating to the latest IPSO version 3.4.1. You must be running Check Point VPN-1/FireWall-1, version 4.1, SP5 for IPSO 3.4.1. GIAC is currently running SP4 and will upgrade to SP5 to support the new IPSO version.

.

Nokia Corporation IPSO 3.4.1 Release Notes 3

What's New in IPSO 3.4

the available applications are described in separate documents and release notes.

• Check Point VPN-1/FireWall-1, version 4.1, SP5; and NG
• RealSecure for Nokia (intrusion detection), version 6.0

What's New in IPSO 3.4

IPSO release 3.4, a full version of the Nokia IPSO operating system, contains the following new features, new inline help, and enhancements to existing features:

• New Inline Help Design
•IPsec
• Authentication, Authorization, and Accounting
• Secure Shell version 2
• SNMP version 3
• Protocol-Independent Multicast Sparse-Mode
• Quality of Service Enhancements
• Gigabit Ethernet
•IP O ver A TM
• PCMCIA Modem Support

• Fault Management
• Monitoring Enhancements
• Routing Enhancements
• RIPv2 MIB

New Inline Help Design

IPSO 3.4 enhances the appearance of and access to inline help. You can now access inline help either for a particular feature or procedure only or for an entire configuration screen. To access context-sensitive inline help, click on the **H** icon and a pop-up window appears, which you can move as necessary. To see the inline help for an entire configuration screen, click the Help button at the bottom of the page.

Action Item # 5

Review rule base manually one by one for unneeded or unauthorized rules. Test for vulnerable open services.

The audit team will confirm that the firewall is secure by using tools to check installed packages and scan for vulnerable open services.

First we do a **netstat –an** on the firewall to view open ports on the firewall. The output is shown below.

```
nokia-650[sbaker]# netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address        Foreign Address       (state)
tcp        0      0  *.22                 *.*                   LISTEN
tcp        0      0  *.80                 *.*                   LISTEN
tcp        0      0  *.256                *.*                    LISTEN
tcp        0      0  *.259                *.*                    LISTEN
tcp        0      0  *.262                *.*                    LISTEN
tcp        0      0  *.264                *.*                    LISTEN
tcp        0      0  *.265                *.*                    LISTEN
tcp        0      0  *.900                *.*                    LISTEN
tcp        0      0  *.1039               *.*                     LISTEN
tcp        0      0  *.1040               *.*                     LISTEN
tcp        0      0  *.1041               *.*                     LISTEN
tcp        0      0  *.1042               *.*                     LISTEN
tcp        0      0  *.1043               *.*                     LISTEN
tcp        0      0  *.1044               *.*                     LISTEN
tcp        0      0  *.18183              *.*                      LISTEN
tcp        0      0  *.18184              *.*                      LISTEN
tcp        0      0  *.19190              *.*                      LISTEN
```

```
udp     0    0  *.259          *.*
udp     0    0  *.1027          *.*
udp     0    0  *.1026          *.*
udp     0    0  *.161          *.*
udp     0    0  *.514          *.*
```

We see a lot of lower ports in the 25X range that are Checkpoint used ports.
By doing a **grep** on the objects.C file in $FWDIR/conf directory for FW1 you will get a list of FW1 ports and their descriptions. After parsing just the ports and their comments, the output is shown below.

Tcp	256	Checkpoint VPN1 & Firewall 1 Service
Tcp	257	Checkpoint VPN1 & Firewall 1 Service (Logging)
Tcp	258	Checkpoint Point Management
Tcp	259	Checkpoint VPN1 & Firewall Client Authentication
Udp	259	Checkpoint VPN1 FWZ Key Negotiations – Reliable Datagram Protocol
Udp	260	Checkpoint VPN1 & Firewall 1 SNMP Agent
Tcp	261	Checkpoint VPN1 & Firewall 1 Session Authentication
Tcp	264	Checkpoint VPN1 & SecuRemote Topology Requests
Tcp	265	Checkpoint VPN1 Public Key Transfer Protocol
Tcp	900	Checkpoint VPN1 & Firewall 1 Client Authentication (HTTP)
Udp	2746	Checkpoint VPN1 SecuRemote IPSEC Transport Encapsulation Protocol
Tcp	18181	Checkpoint OPSEC Content Vectoring Protocol
Tcp	18182	Checkpoint OPSEC URL Filtering Protocol
Tcp	18208	Checkpoint Remote Installation Protocol
Tcp	19190	User Authority simple protocol (netso)
Tcp	19191	Checkpoint OPSEC User Authority API
Tcp	18207	Policy Server Logon protocol
Tcp	18184	Checkpoint OPSEC Log Export API
Tcp	18187	Checkpoint OPSEC Event Logging API
Tcp	18183	Checkpoint OPSEC Suspicious Activity Monitor API

Now that we compare the netstat –an output to the Firewall 1 port list in the objects.C file, we see that all of the 1818X and 2XX ports are Checkpoint ports along with 900 and 19190. It is recommended that these port types get evaluated and any unknown or unused ports get turned off. There were some unidentified ports also that should be turned off. Although these ports show listening, they are still protected by the firewall via the any any any drop or clean up rule. This will be verified in the scan.

Outside Firewall Interface Scan
The outside interface will be scanned in a few different ways. First we will try spoofing an external internet source address while using a stealth port scan against the external firewall interface. Tcpdump will be running on the internal interface to check for any packets that get thru.

Nmap –v –P0 –sS –S 12.12.27.42 –e E100B1 208.156.147.1

-v verbose mode recommended
-P0 don't ping hosts
-sS SYN stealth port scan
-e source network interface

Next we will try the same scenario but this time we do a UDP port scan by changing the –sS switch to –sU shown below. Tcpdump will be running on the internal interface to check for any packets that get thru.

Nmap –v –P0 –sU –S 12.12.27.42 –e E100B1 208.156.147.1

Next we try another stealth scan like the first one but we try and spoof internal source addresses, which should never come from the outside. Tcpdump will be running on the internal interface to check for any packets that get thru.

Nmap –v –P0 –sS –S 172.16.1.3 –e E100B1 208.156.147.1

Next we might want to scan the external services network devices like DNS and SMTP from the outside external interface side while sniffing packets with tcpdump on the external services network interface to see what gets thru. We could make the source port look like dns by using the –g53 switch shown below.

Nmap –v –g53 –P0 –sA –S 12.12.27.42 –e E100B1 208.156.147.11

The –g53 switch emulates a DNS packet while the sA switch determines what packets are filtered and unfiltered. The 208.156.147.11 address is the DNS server in the external services network.

External Services Interface Scan

Next we scan the external services network firewall interface for open ports where DNS, SMTP, and NTP servers reside.

Nmap –v –P0 –sS 208.156.147.9

The external DNS and SMTP servers can only talk to the internal DNS and SMTP servers internally so we could spoof the external DNS server address and scan an internal address other than the internal DNS or SMTP servers to see what gets dropped. We could make the packet emulate the external DNS destined for a 10.0.0.0 net address and run tcpdump on the internal interface to see what gets thru. We could do the same for SMTP using –g25 also. This also emulates the service network being compromised. The nmap command might look like this.

Nmap –v –g53 –P0 –sA –S 208.156.147.11 –e E100B1 10.1.10.50

The process would be repeated to scan every network from every other network using sniffers to see what gets thru.

Internal Services Interface Scan

First we scan the internal network firewall interface to look for open ports.

Nmap –v –P0 –sS 208.156.147.25

Since all outbound internal services are either using a proxy or socks connection, we will test going around these devices also while running tcpdump on the internal and external firewall interfaces to ensure the traffic gets dropped.
Rulebase Procedures – Review rule base one by one and try consolidating rules if possible to reduce the size of the rule base. Look for any unneeded or unauthorized rules. Ensure that comments in the rule base include a description of the rule, ticket or request number, administrator's initials, and date for tracking and auditing purposes.

Recommended Action item # 5

During testing some identified and unidentified ports were found open. All of the 1818X and 2XX ports are Checkpoint ports along with 900 and 19190. Although the rule base protects them, it is recommended that these port types get evaluated and any unknown or unused ports get turned off. There were some unidentified low range ports shown in the graphic above that also should be turned off. Unauthorized traffic was being dropped properly and logged.

Rule base rules were reviewed and it was found that most rules had only a brief description in the comments field. It is recommended that the comments field located in the rule base include a description of the rule, ticket or request number, administrator's initials, and date for tracking and auditing purposes as stated in the security policy. Rule base backup procedures were found to be adequate.

Action item # 6

Test any firewall applications such as fail over, virus scanners, proxy filters, and encryption.

The **fail over connection** was tested doing FTP transfers and browsing HTTP sites after hours for the proper expected fail over results by changing the Master and Secondary VRRP (Virtual Routing Redundancy Protocol) priorities. When running the VRRP with the Nokia appliance, you set priorities for the Primary and Secondary monitored VRRP circuit. Say the Primary priority is 90 and the Secondary is 85. In this configuration the primary functions as master

because it has a higher priority. By changing the Secondary firewall to a higher priority of 95, it now had a higher priority thus becoming master. After the secondary was failed over, the primary firewall was shutdown by doing a **shutdown –H now** command to ensure it was truly down. A sample screen shot from the Nokia lynx configuration tool is shown below. By running lynx at the command line, choosing **Config-VRRP**, we can view the VRRP configuration. A sample config on the next page shows what it look like.

Interfaces:
outside
208.156.147.1/27 Mode: ( )off ( )VRRPv2 (*)Monitored Circuit
Virtual Router: 10 (*)on ( )off Priority: 95_____ Hello Interval: 3_____
208.156.147.5 (*)on ( )off
Backup Address: _____
inside (*)on ( )off Priority Delta: 10
Monitor Interface: [None_____] Priority Delta: _____
Create Virtual Router: _____
Authentication: (*)None ( )Simple

- The Virtual Router ID must be the same on both primary and backup for each interface. This points them to the multicasts they should be listening to.
- Under the Backup Address field is a list of interfaces. This one listed is called **inside** which is the inside interface. These are the monitored circuits. If any of these circuits go down, we want the Nokia to fail over to the secondary. The Priority Delta determines this. If one of the interfaces listed goes down, the Priority Delta is subtracted from the Priority and the Nokia with the higher priority becomes the active firewall. The hello interval is set to 3. This means that every three seconds each firewall will send a multicast on each interface stating it's priority. When the secondary detects the higher priority for itself, it will assume the master status.
  Ex. s1p1c0 goes down on the primary
  Priority = 95
  P Delta = 10

  The Primary's priority is now 85 and the secondary, which in this case is set to 90, would take over as the active firewall

© SANS Institute 2000 - 2005 Author retains full rights.

By typing **ipconfig –a** and doing a grep on mac at the command line you can verify if the VRRP MAC addresses show up on each interface of the master shown below. The master will always have these VRRP IP and MAC addresses.

```
Master[sbaker]# ifconfig -a | grep mac
   inet 208.156.147.5 /29 broadcast 208.156.147.8 vrrpmac 0:0:5e:0:1:a
```

Summary

During this test the network behavior was monitored for lost or failed state table connections. No interruption in connectivity was noticed or found in the logs.

Sample viruses were downloaded and tested to ensure they were detected and cleaned. Virus alerts were properly generated and virus file quarantines are working as designed.

By surfing unauthorized websites, proxy URL filters were tested, working properly, and being logged.

Encrypted connections were verified by using sniffers to view the encrypted packets on the wire.

Recommended Action Item # 6

No recommended action is needed at this time. The Nokia Appliance failed over as designed with no lost connections. Virus detection and alerting, URL filters, and encrypted connections all worked as designed.

Action Item # 7

Review firewall logging and alerting for proper detection.

Firewall and IDS logs were reviewed and verified after rule base scanning to ensure that the probe signatures were detected, alerts were generated, and that the proper rules were dropping and logging the traffic.

Recommended Action Item # 7

None. IDS and log detection worked as designed. A sample outside log scan destined for the firewall interfaces is shown below.

```
"12.12.27.42" "208.156.147.1" "tcp" "10" "4420"  "firewall" " len 40"
"104608" "03Dec2001" "15:07:16" "eth-s1p1c0" "208.156.147.1" "log" "drop" "domain"

"12.12.27.42" "208.156.147.1" "udp" "10" "1857"  "firewall" " len 58"
"147090" "03Dec2001" "15:08:44" "eth-s1p1c0" "208.156.147.1" "log" "drop" "domain"

"12.12.27.42" "208.156.147.25" "udp" "10" "3774" "" "firewall" " len 58"
"149568" "03Dec2001" "15:08:49" "eth-s1p1c0" "208.156.147.1" "log" "drop" "34633"
```

"12.12.27.42" "208.156.147.9" "tcp" "10" "17714" "" "firewall" " len 40"
"157512" "03Dec2001" "15:09:05" "eth-s1p1c0" "208.156.147.1" "log" "drop" "smtp"

"12.12.27.42" "208.156.147.9" "tcp" "10" "33341" "" "firewall" " len 44"
"166886" "03Dec2001" "15:09:25" "eth-s1p1c0" "208.156.147.1" "log" "drop" "domain"

"12.12.27.42" "208.156.147.25" "udp" "10" "1454" "" "firewall" " len 58"
"178141" "03Dec2001" "15:09:48" "eth-s1p1c0" "208.156.147.1" "log" "drop" "smtp"

"12.12.27.42" "208.156.147.1" "tcp" "10" "4979" "" "firewall" " len 44"
"184819" "03Dec2001" "15:10:01" "eth-s1p1c0" "208.156.147.1" "log" "drop" "domain"

"12.12.27.42" "208.156.147.9" "udp" "10" "1716" "" "firewall" " len 58"

The number between the protocol "udp" and the destination port "1716" is the rule number. In these samples you will see that they are all logged and dropped by rule 10, which is the stealth rule. The stealth rule drops anything destined for the firewall interfaces.

Action Item # 8

Review firewall admin password policies, read/write access, admin account creations, patch back out procedures, and standardization for OS builds for the firewalls.

Administrators and Management were interviewed to obtain policy information for firewall admins.

a. It was determined that the Security Team Lead will create accounts for all firewall admins.
b. Passwords must be changed every 60 days or immediately in the event that a firewall admin leaves the company.
c. Standards for OS builds are currently in place and new patches are evaluated based on security risks then tested in the lab and the proper change control policy is followed before installation.
d. Patch back out procedures were adequate and the findings are shown below.

Recommended Action Item # 8

None. Security policies for firewall admin password policies, account creations, patch back out procedures, and standardization for OS builds for the firewalls are in place.

It was demonstrated that with the Nokia Appliances, backing out patches is a very simple process. By running the lynx command line tool and choosing **Config** then **Manage Installed Packages**, we can choose a previous patched version by simply selecting it shown in the graphic below. Note that version 4.1 SP-4 IPSO 3.4 is turned off and 4.1 SP5 IPSO 3.4 is active. By selecting the on radio button for the previous version 4.1 SP-4 IPSO 3.4 and turning the 4.1 SP5 IPSO 3.4 off, we back the patch out and return to the previous build.

Installed Packages

Firewalls
( )On (*)Off Check Point FireWall-1 (Strong) v4.1 SP-4 (Mon July18 15:05:45 PDT 2000 bld 15.4)
/opt/FireWall-1-strong.v4.1.SP-4.ipso-3.4

(*)On ( )Off Check Point FireWall-1 (Strong) v4.1 SP-5 (Mon May04 15:05:45 PDT 2001 bld 15.5)
/opt/FireWall-1-strong.v4.1.SP-5.ipso-3.4

Applications
(*)On ( )Off F-Secure SSH client and server, version 1.3.6 /opt/f-secure-ssh

Documentation
(*)On ( ) Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list

Action item # 9

Review change control policies for adding or removing hardware, rule changes, change documentation, and backing out changes.

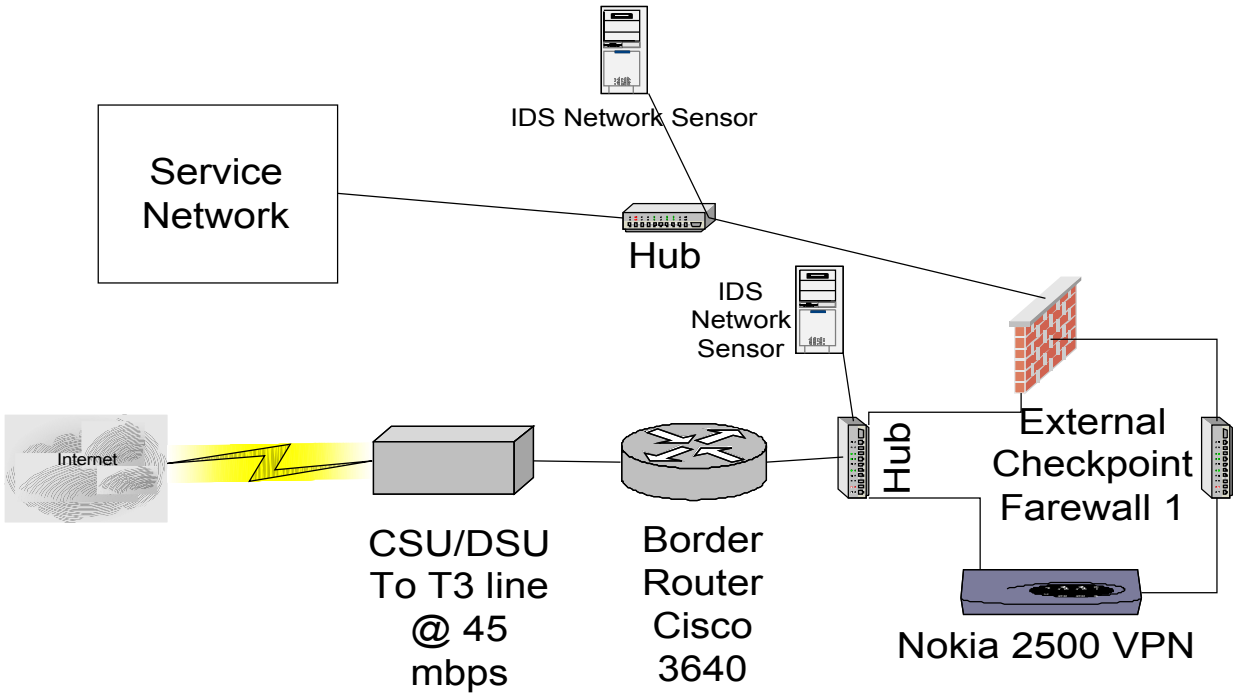
Change control policies were reviewed and adequate for the above item. The results are shown below.

a. Adding or removing hardware will be done during scheduled downtime and coordinated with change control for tracking unless its an emergency break fix which will be coordinated with change control and replaced immediately.
b. Rule changes or requests must be requested and approved thru the company's remedy ticket system for tracking and documentation.
c. When applying the new rule base changes, the new rule base will be saved by policy name – date. This ensures a quick back out plan by simply re-installing the old policy.

Recommended Action item # 9

© SANS Institute 2000 - 2005 Author retains full rights.

None. The change control policies are adequate and do not require modifying.



Assignment # 4 - Scott Baker - Design Under Fire: *Justin Ginsberg Practical*
http://www.sans.org/giactc/gcfw.htm/Justin_Ginsberg_GCFW.zip

DOS Attack -Theoretical attack from 50 compromised cable modem/DSL systems

For this design I decided to choose a Smurf DOS attack on the router. By examining the border router, I noticed that ICMP is wide open other than the ICMP unreachable messages being blocked. Since this design has a T3 pipe, we will need some amplification to bring it to a halt. A Smurf attack takes advantage of directed broadcasts using other network broadcast addresses as amplification. By pinging large broadcast addresses like 12.12.255.255, you identify your amplifier to use for the attack when it floods you to death with hundreds of replies. It is the same as pinging every host on the 12.12.0.0 network. That is if the broadcast address is not blocked. Once you find a killer amplifier then run nmap and send a flood of spoofed ICMP ECHO packets to the broadcast address of the amplifying network. The source address would be set or

spoofed to the border router's external address. This makes its look like the border router initiated the request. Say you have 250 addresses respond to one directed broadcast to 12.12.255.255. You have just multiplied your force by 250. So for every single directed broadcast ICMP ECHO you send to the amplifier, **250** replies are sent to the border router. Now say you have 50 compromised cable modem/DSL systems. Next you have them all send directed broadcast ICMP ECHO requests to multiple different amplifiers with a spoofed source address of the border router. Now with just one echo request from all systems gives you 50 x 250 = **12,500** replies to the router.
Send a flood of directed broadcast ICMP ECHO packets to your amplifiers from all 50 systems and you will echo reply the router do death.

Counter measures:

The designer does have the **no ip directed broadcast** command set to prevent his router from being used as an amplifier but should at least filter Ingress ICMP at the border router. Immediately put an ACL on the border router. You could also work with the ISP to filter out this traffic if it persists.

!Deny all icmp:
Access-list 101 deny icmp any any

I found another Cisco DOS syslog crash vulnerability which might be worth a try at:
http://packetstorm.decepticons.org/9901-exploits/cisco-ios-DoS.alert.txt
Shown Below:

```
Date: Mon, 11 Jan 1999 16:00:56 -0000
From: security-alert@cisco.com
Reply-To: psirt@cisco.com
Found this on
http://packetstorm.decepticons.org/9901-exploits/cisco-ios-DoS.alert.txt
To: BUGTRAQ@netspace.org
Subject: Cisco Security Notice: Cisco IOS Syslog Crash

-----BEGIN PGP SIGNED MESSAGE-----

Field Notice:
Cisco IOS Syslog Crash
============================================================
Revision 1.1
For release 08:00 US/Pacific, Monday, January 11, 1999

For Cisco internal use only until release date

Summary
=======
Certain versions of Cisco IOS software may crash or hang when they receive
invalid user datagram protocol (UDP) packets sent to their "syslog" ports
(port 514). At least one commonly-used Internet scanning tool generates
packets which can cause such crashes and hangs. This fact has been
announced
on public Internet mailing lists which are widely read both by security
professionals and by security "crackers", and should be considered public
information.
```

This vulnerability affects devices running Cisco IOS software version 11.3AA, version 11.3DB, or any 12.0-based version (including 12.0 mainline, 12.0S, 12.0T, and any other regular released version whose number starts with "12.0"). The vulnerability has been corrected in certain special releases, and will be corrected in maintenance and interim releases which will be issued in the future; see the section on "Software Versions and Fixes" for details on which versions are affected, and on which versions are, or will be, fixed. Cisco intends to provide fixes for all affected IOS variants.

There is a configuration workaround for this vulnerability.

Who is Affected
==========
All Cisco devices which are running classic Cisco IOS software with any of the versions listed as affected under "Software Versions and Fixes" are vulnerable to attack. This includes 11.3AA, 11.3DB, and all 12.0 versions, up to the repaired releases listed in the table. No particular configuration
is needed to make a Cisco IOS device vulnerable.

It is possible to filter out the attack traffic using access lists; see "Workarounds" in this document. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. You should carefully evaluate your configuration before assuming that any filtering you
have already configured protects you against this attack.

Affected Devices
- ----------
It is impossible to list all Cisco products in this notice; the lists below include only the most commonly used or most asked-about products.

If you are unsure whether your device is running classic Cisco IOS software,
log into the device and issue the command "show version". Classic Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices either will not have the "show version"
command, or will give different output.

Cisco devices that run classic Cisco IOS software include:

* Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 8xx, ubr9xx, 1xxx, 25xx, 26xx, 30xx, 36xx, 38xx, 40xx, 45xx, 47xx, AS52xx, AS53xx, AS58xx, 64xx, 70xx, 72xx (including the ubr72xx), 75xx, and 12xxx series.
* Most recent versions of the LS1010 ATM switch.
* Some versions of the Catalyst 2900XL LAN switch.
* The Cisco DistributedDirector.

© SANS Institute 2000 - 2005 Author retains full rights.

Attack Against the Firewall:

Border Router ACL Review:

After reviewing the border router ACL's, I found that telnet was not blocked on the router. I began to research to see if I could find a Cisco password cracker. It didn't take very long before I found one called Cisco crack. It's a brute force password cracker. The filename is Cisco_crack.tar.gz and I got it from from packetstorm.decepticons.org
Cisco Crack is Cisco device login brute force tool. By B-root. After cracking the password on the router, I would give myself some rights to move around a bit by adjusting some ACL's. First I remove the ACL's that stop me from targeting the firewall interface. I noticed that the designer did not have a stealth rule on the external firewall policy. He put his stealth rule for the firewall on the Border Router. Now that I have the router I can finagle the ACL's enough so that I have access to port UDP 257 which may give me a shot at the RDP vulnerability listed below. I might also remove his internal net spoofing rules. Or I could just slip an access-list 101 permit any any statement at the top of the access list to make it less obvious. Three vulnerabilities from **Checkpoint** are listed below and two are listed after that from the **Packetstorm** site at: http://packetstorm.decepticons.org/0001-exploits/checkpoint-fw1.vuln.txt.
Now that I have removed the ACL that blocked access to the external firewall interface, I can possibly exploit the **#2 packetstorm** vulnerability below which states that the default configuration in FW-1 allows for rlogin management of the server. The rlogin prompt is available on all NICs. Unless a rule is placed in your rule set to drop or reject all connections to the firewall, the authentication problem above can be used to remotely administer someone else's firewall without them knowing. Since the designer **did not** put a stealth rule on the firewall, I would try for an rlogin connection to the firewalls external interface. It is also possible that I could spoof an internal source address to get to the inside of the network also. If all else failed the firewall is open to a SYN flood attack since the stealth rule was removed on the Border Router, I could target the external interface of the firewall. You could change the password on the border router before you begin the attack to put a damper on countermeasures. A SYN flood attack would overload the connections table since the firewall is waiting on a SYN Ack for these connections. It would also slow down the firewall by consuming its resources, and may cause

the firewall to crash. Checkpoint recommends that you leave SynDefender turned off until you are actually attacked so it's a good possibility that this function is disabled.

Counter Measures

Counter measures here would be to filter ICMP, telnet, and ftp on the border router and install a stealth rule on the firewall, which drops anything, destined for the firewall interfaces. I may go as far as to block the services listed above on the firewall also just in case the border router gets compromised.

The firewall is running Checkpoint 4.1. Research for the vulnerabilities below were found at: http://www.checkpoint.com/techsupport/alerts/

RDP Communication Vulnerability

Addendum - July 12, 2001

Updated September 13, 2001

Summary:
Check Point uses a proprietary protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/FireWall-1 allows RDP packets to traverse firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/FireWall-1 gateway without being explicitly allowed by the rule base. In the 4.1 SP4 hot fix and all future service packs and releases, this default behavior is changed and RDP communication is blocked unless a specific access rule is written.

Solution:
For all users, upgrade to VPN-1/FireWall-1 4.1 Service Pack 4 and install the SP4 hot fix, then install a policy. This hot fix only needs to be applied to management stations, not firewall modules.

Who is affected?
Any VPN-1/FireWall-1 gateway is potentially susceptible to this unauthorized traffic, which is not an attack or denial of service but could be used in some circumstances to establish a surreptitious communication channel.

Change made in the hot fix:
RDP communication is blocked by default.

Format Strings Vulnerability

Updated September 13, 2001

Summary:
A security issue exists in VPN-1/FireWall-1 version 4.1 whereby a valid firewall administrator connecting from an authorized management client may send malicious data to a management station inside a control connection, possibly preventing proper operation of the management station. This issue exists because some instances of improper string formatting occur in VPN-1/FireWall-1 version 4.1. By sending specially constructed commands through authorized communication channels, arbitrary code may be inserted onto the operating system stack of a VPN-1/FireWall-1 management station. This vulnerability may only be exploited by an authorized and authenticated VPN-1/FireWall-1 administrator connecting from a workstation explicitly trusted by the management station, although read/write permission is not required in order to perform this attack. Since full access (read/write) administrators and those at the local system console already have direct access to the firewall system, this is an escalation of privilege only for read-only administrators.

Solution:
For all users, upgrade to VPN-1/FireWall-1 4.1 Service Pack 5.

Who is affected?
All installations of VPN-1/FireWall-1 which allow remote GUI connections should be assumed vulnerable to this exploit. It should be noted again that the attack must be made by an authorized and valid VPN-1/FireWall-1 administrator connecting from an authorized GUI client station.

Immediate workaround:
Restrict remote GUI access for read/only firewall administrators; review list of administrators and authorized GUI clients.

Changes made in the hot fix:
Improper string formatting statements have been converted to secure ones in this hot fix and all future releases. This has no other impact on firewall operation.

GUI Buffer Overflow

© SANS Institute 2000 - 2005 Author retains full rights.

September 19, 2001

Summary:

An issue exists in VPN-1/FireWall-1 Management Server running on Windows NT or Windows 2000. A malicious administrator can exploit a buffer overflow condition in the GUI authentication code to potentially impair management station functionality or to execute code. Any attack must come from an IP address explicitly defined as an authorized GUI client. Only management stations running Windows NT or Windows 2000 are affected. This includes any standalone VPN-1/FireWall-1 Gateways (with Management Server and enforcement points installed on the same machine), but does not include module-only (enforcement point) installations.

This issue affects VPN-1/FireWall-1 4.0, 4.1, and Next Generation systems. Hot fixes for VPN-1/FireWall-1 4.0 SP8, 4.1 SP4, 4.1 SP5, and Next Generation Hotfix-2 are available for immediate download at http://www.checkpoint.com/techsupport/index.html.

Solution:

Apply the relevant GUI Buffer Overflow Hot fix to the management station.

Who is affected?

All installations of VPN-1/FireWall-1 with Management Servers running on Windows NT or Windows 2000.

Immediate workaround:

Allow GUI connections only from trusted hosts.

Changes made in the Hot fix:

The buffer checking on the Management Server has been improved.

Two more Checkpoint vulnerabilities were found at:

http://packetstorm.decepticons.org/0001-exploits/checkpoint-fw1.vuln.txt

There are two vulnerabilities in FW-1. The first is an authentication issue, the other is a configuration issue.

Vulnerability #1

The basic authentication used in Checkpoint FW-1 used for inside/outbound and outside/inbound allows unlimited attempts to authenticate without a timeout or disconnect between unsuccessful attempts. To make matters worse, the attempt at authentication will let you know if you have the wrong username before you are allowed to enter the password.

The exploit is trivial, grind away at user names until you hit one that works and then grind away at passwords with the username you just found until you find one that works.

For an example of this, set authentication on the FW-1 software to authenticate telnet connections. Telnet to a destination past the firewall, when prompted for a username, pound away. A script could crack the authentication in a very short time.

The workaround is to use Checkpoint's encrypted authentication program "Secure Remote" and not allow clear text authentication (browser based, telnet, etc.) to destinations beyond the firewall.

Vulnerability #2

The default configuration in FW-1 allows for rlogin management of the server. The rlogin prompt is available on all NICs. Unless a rule is placed in your rule set to drop or reject all connections to the firewall, the authentication problem above can be used to remotely administer someone else's firewall without him or her knowing. The workaround is to include the stealth rule.

References

1. Brenton, Chris. Mastering Cisco Routers; Network Designs by Andrew Hamilton and Gary Kessler
2. Northcutt, Steven. Auditing Routers and Firewalls, SANS 2001, San Diego CA, Oct. 2001
3. Brenton, Chris. Firewalls 101: Perimeter Protections and Defense, In-Depth, SANS 2001, San Diego CA, Oct. 2001
4. Brenton, Chris. Firewalls 102: Perimeter Protections and Defense, In-Depth, SANS 2001, San Diego CA, Oct. 2001
5. Brenton, Chris. VPNs and Remote Access, SANS 2001, San Diego CA, Oct. 2001
6. Brenton, Chris. Network Design and Performance, SANS 2001, San Diego CA, Oct. 2001
7. Scambray, Joel; McClure, Stuart; Kurtz, George, Hacking Exposed, Second Edition.
8. http://www.incident.org/
9. http://www.intrusion.org/
10. http://www.cisco.com/warp/public/707/newsflash.html
11. http://www.cisco.com/warp/public/707/21.html
12. https://support.nokia.com/iprg_software/ipso_34_relnotes.html
13. http://www.cacheflow.com/products/700/features.cfm
14. http://www.cacheflow.com/products/600/features.cfm
15. http://www.cisco.com/warp/customer/cc/pd/hb/vp3000/prodlit/vpn3k_ov.htm
16. http://www.checkpoint.com/techsupport/alerts/
17. http://www.cisco.com/warp/public/cc/pd/rt/7400rt/

18. http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm
19. http://www.antivirus.com/products/isvw/
20. http://www.cisco.com/warp/public/471/ALTIGAR.shtml
21. http://www.sans.org/giactc/gcfw.htm/ Justin_Ginsberg_GCFW.zip
22. http://packetstorm.decepticons.org/0001-exploits/checkpoint-fw1.vuln.txt
23. http://packetstorm.decepticons.org/9901-exploits/cisco-ios-DoS.alert.txt