Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment v1.6a (Revised October 26, 2001)

Klear Sideris

May 1, 2002

Table of Contents

Assignment 1:1 Security Architecture

1.1 Requirements

1.1.1 Access Requirements

Partners are international organizations that have multiple employees accessing GLF to select fortunes suitable for translation & resale. They can place an order, review order status, transaction histories, examine account information and create reports. In addition, they need to have OS level access to the GLF App Server via Telnet and FTP. All accesses have a high dollar loss if compromised and consequently need to be protected through strong authentication and confidentiality when in areas subject to attack.

Suppliers are geographically dispersed individuals that create & submit fortunes to the GLF system, which enforces uniqueness & content requirements. They can review existing fortunes for new ideas, examine sales performance, submit orders, see status, account information, and create reports. All transactions are handled by the application with a subset leading to a moderate dollar loss if compromised. Consequently, this subset needs to be protected through moderate strength authentication and corresponding confidentiality in areas of high likelihood .

Customers are characterized as multi national companies. They access GLF to select fortune sayings for bulk purchase, review order status, transaction histories & create reports. All transactions are handled by the application with some being confidential & requiring encryption. Authentication needs to address the low $ value of compromise.

GIAC salesmen need remote access to the corporate Email from the road.

GIAC technical employees need remote access to all GIAC S/W & H/W components. for after hours support. All accesses have a high dollar value if compromised and consequently need to be protected through strong authentication and confidentiality.

All GIAC employees need local access from within the Corporate LAN to File & Print services, the Internet & local & Internet Email. They also need to use Microsoft's Netmeeting to videoconference with outside consultants using the Internet. The GIAC technical staff need access to all S/W & H/W components.

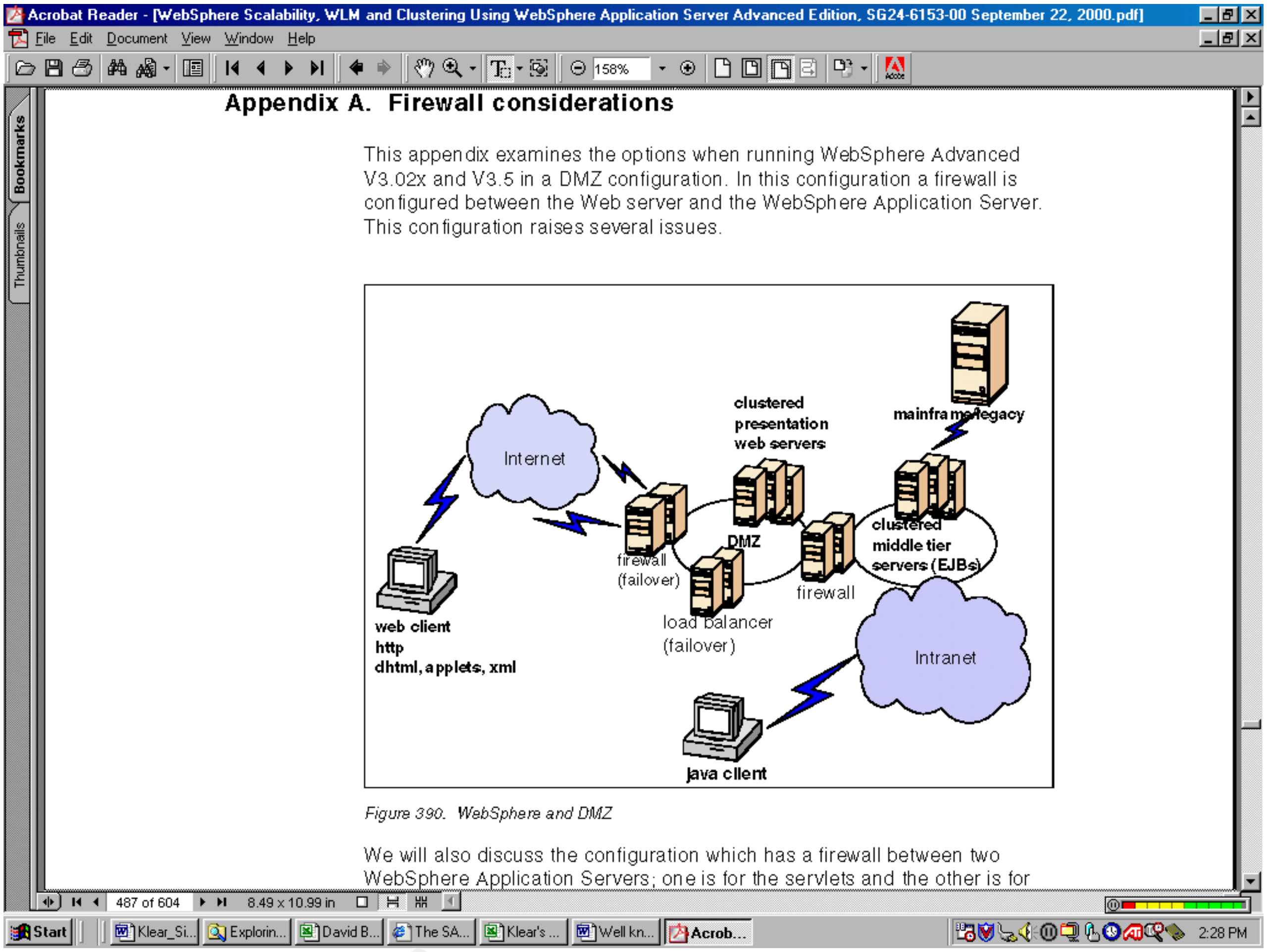
1.1.2 Performance Requirements

GLF needs to provide 24x7 availability with sub second response times and accommodate a three-fold increase in capacity in the next two years.

There are over 100 Partners, 2,000 Suppliers, 50,000 Customers & 500 Employees impacting the GLF system, with a peak volume of 500 transactions per minute.

1.1.3 Application Components

IBM's v4.1 Web Sphere Application Server is chosen for the Good Luck Fortune (**GLF**) System using a 4-tier architecture model encompassing Browser, Presentation, Business & Data Layers as shown below. The complexities of distributed processing communication, Corba, IIOP, Naming Services, security, fault tolerance, scalability and interoperability are simplified by the selected platform.


Acrobat Reader - [WebSphere Scalability, WLM and Clustering Using WebSphere Application Server Advanced Edition, SG24-6153-00 September 22, 2000.pdf]
File Edit Document View Window Help
158%
Bookmarks
Thumbnails
Internet
clustered presentation web servers
mainframe/legacy
firewall (failover)
DMZ
clustered middle tier servers (EJBs)
firewall
load balancer (failover)
web client http dhtml, applets, xml
Intranet
java client
487 of 604
8.49 x 10.99 in
Start
Klear_Si...
Explorin...
David B...
The SA...
Klear's ...
Well kn...
Acrob...
2:28 PM

Appendix A. Firewall considerations

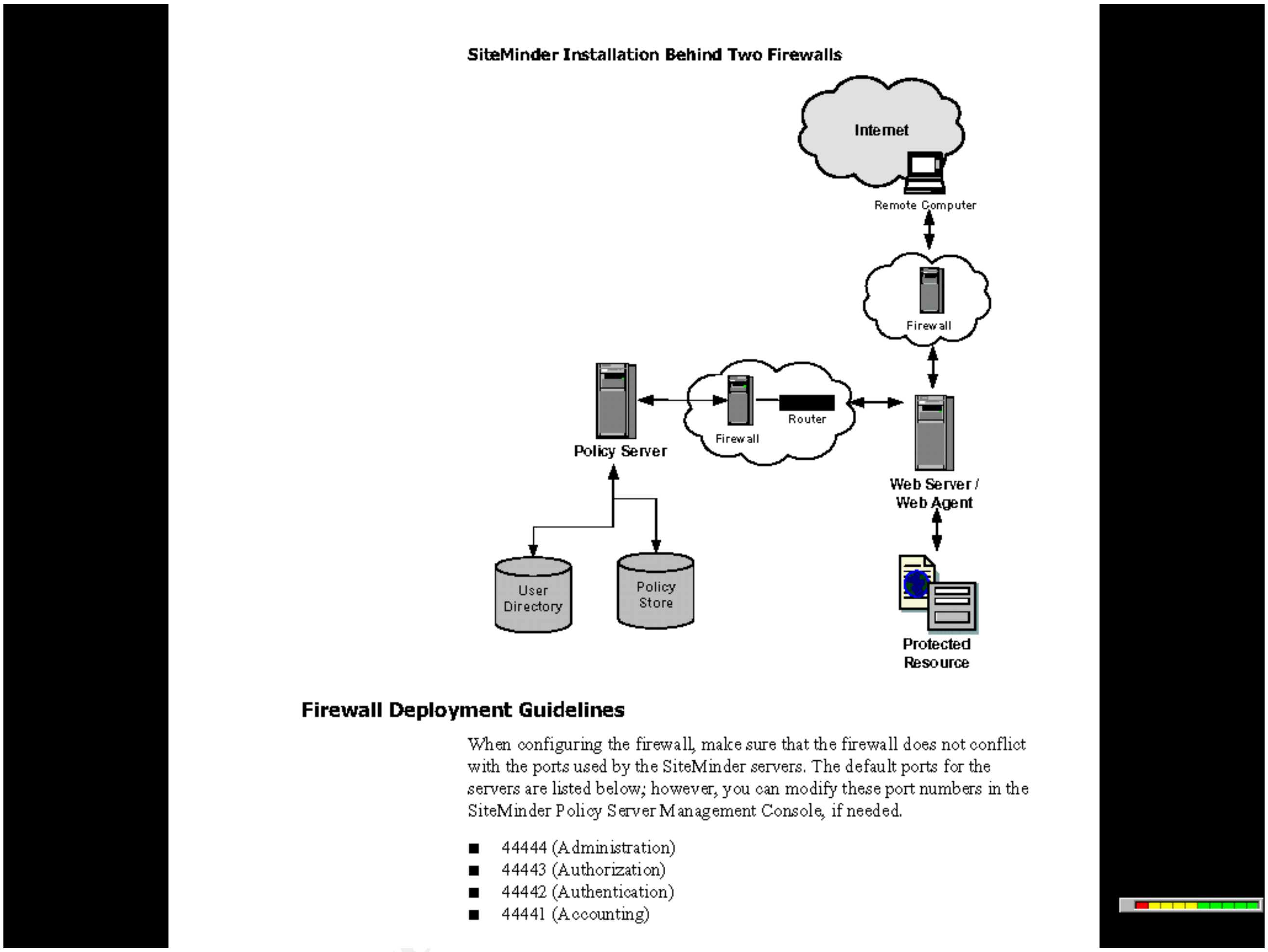
This appendix examines the options when running WebSphere Advanced V3.02x and V3.5 in a DMZ configuration. In this configuration a firewall is configured between the Web server and the WebSphere Application Server. This configuration raises several issues.

Figure 390. WebSphere and DMZ

We will also discuss the configuration which has a firewall between two WebSphere Application Servers; one is for the servlets and the other is for

In the Web Sphere design the Web Server is responsible for receiving the requests from the Web Clients, filtering those that need to be serviced by Web Sphere, and forwarding these to the Servlet Engine in an Application Server for processing. The forwarding of requests from the Web Server to the Application Server is accomplished through Corba and IIOP transports that simplify the variety of IPC mechanisms provided by the underlying operating system to effect the actual transport of data: pipes, UNIX-domain sockets, and TCP/IP sockets.

Although WebSphere has Authentication, Authorization and Accounting functionality, Netegrity's Site Minder is used to provide these services and enhance security through vendor heterogeneity, as shown below.



SiteMinder Installation Behind Two Firewalls

Firewall Deployment Guidelines

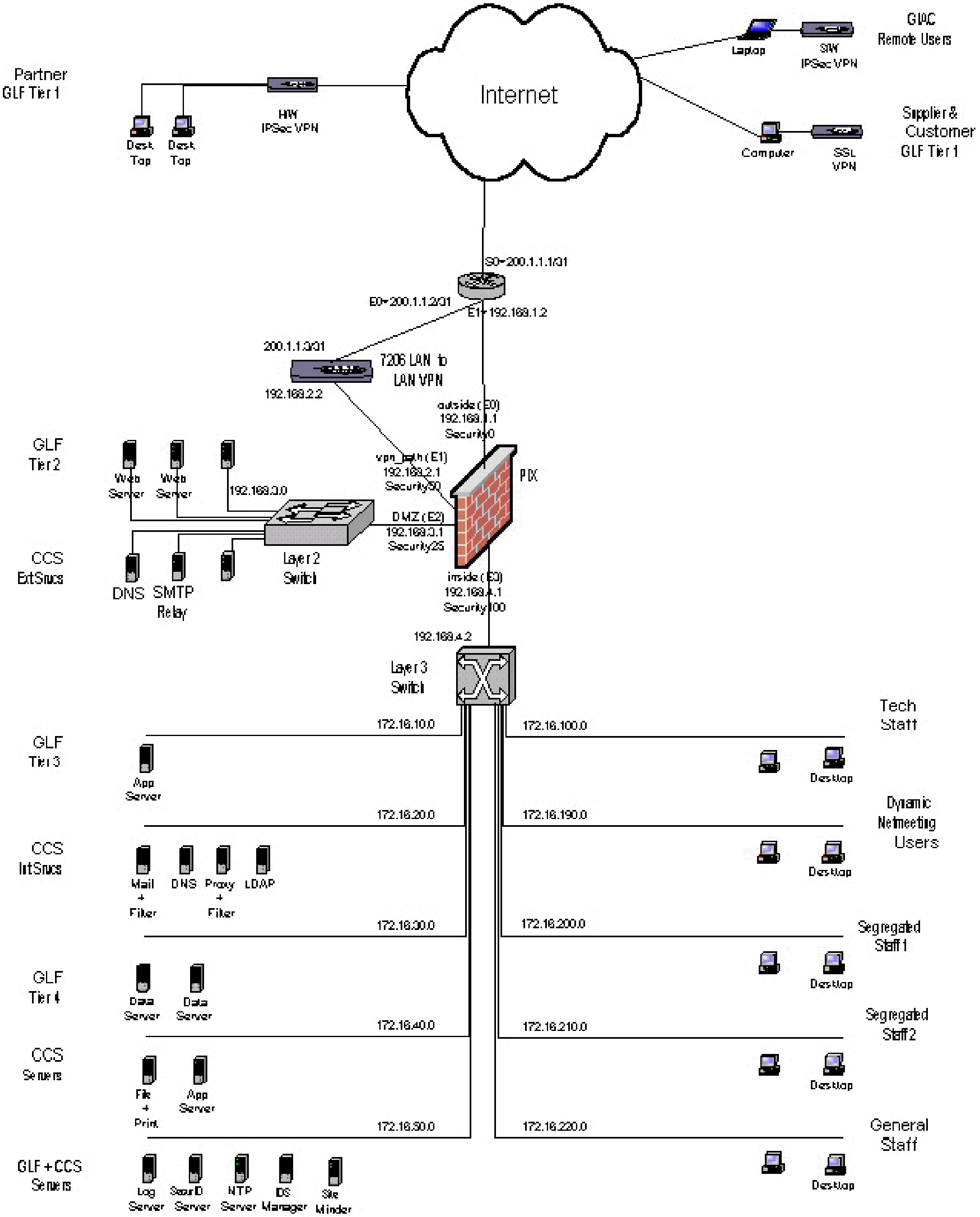
When configuring the firewall, make sure that the firewall does not conflict with the ports used by the SiteMinder servers. The default ports for the servers are listed below; however, you can modify these port numbers in the SiteMinder Policy Server Management Console, if needed.

- 44444 (Administration)
- 44443 (Authorization)
- 44442 (Authentication)
- 44441 (Accounting)

Role & exposure determined differential authentication is provided through URIs that enforce a range of strengths from basic (static something you know) to intermediate (static something you know & have) to highly secure dual factor authentication (something you know & a dynamic something you have) utilizing RSA's SecurID.

1.2 Solution

1.2.1 Security Architecture Diagram



1.2.2 Border Router Selection

The border router is selected based on criteria of high availability, scalability, protocol support, stability, performance, value, ease of use and security.

In addition to providing Internet communications the border router will act as a protective device (packet filtering firewall) by dropping all traffic that does not meet address and transport layer criteria.

Since configuration errors may compromise communications to the entire site, the filtering needs to require minimal change to ensure stability.

A Cisco 7505 with v12.2 of IOS for Internet connectivity is selected.

1.2.3 Firewall Selection

Firewalls protect physical areas from attack & also contain the damage in the event of a compromise. **Protection** is achieved through the basic tenant of initially denying all inward traffic and then only allowing passage of protocols and source and destination addresses necessary for the required functionality. **Containment** is achieved by analogous limitations on outward traffic.

We decide to focus the selection to the top two products to maximize our real world exposure. The matrix & subsequent discussion show how we choose PIX 525, v6.1. In the "Design Under Fire" assignment we choose Checkpoint-1 to complement our experience.

Criteria	Weight	Checkpoint Unweighted	Pix Unweighted	Checkpoint Weighted	Pix Weighted
High availability, user transparency	1	2	1	2	1
Scaleability, performance	2	2	3	4	6
Life expectancy	3	3	3	9	9
Usability, support	2	3	2	6	4
Functionality, test of time	3	3	2	9	6
Value	3	1	3	3	9
Rating (Gartner, Network Computing, etc.)	3	2	3	6	9
User Rating (SANS, CISSP, CISA)	3	2	2	6	6
Total				**45**	**50**

1.2.3.1 Firewall Types

Firewalls are characterized by the degree of rigor used to verify each protocol's validity.

Static packet filtering firewalls provide the weakest but fastest form of validation. They typically check the Packet IP and Transport Header fields including Source & Destination IP addresses, Source & Destination Ports and Flags. They are well suited for recognition & dropping of: Ingress packets with Source addresses containing Private addresses or spoofed (internal) Public addresses.

Stateful packet filtering firewalls keep track of the state of a session and validate the exchange based on sequence number and flag value verifications.

Stateful inspection firewalls extend Stateful packet filtering by understanding the protocols in use and making decisions based on the payloads of the packets.

Application firewalls provide the greatest level of protocol validation, by duplicating the application process, processing a message and then forwarding it on.

As the rigor used to verify each protocol is increased, message latency and throughput are adversely affected. Incorporation of new protocol verification introduces vendor dependent time delays for understanding & implementation.

1.2.3.2 PIX Characteristics

Part of the functionality evaluation revolves around how many protocols are intercepted & fully scrutinized by the firewall, as well as how well this is done. Lack or inclusion of protocols that lead to greater vulnerability for GIAC may be determinative. Checkpoint's Firewall-1 list of protocols exceeds 100 whereas PIX's has the following (referred to as fixup):

```
fixup protocol ftp [strict] [port]
fixup protocol http [port[-port]
fixup protocol h323 [port[-port]]
fixup protocol rsh [514]
fixup protocol rtsp [port]
fixup protocol sip [5060]
fixup protocol smtp [port[-port]]
fixup protocol sqlnet [port[-port]]
fixup protocol [protocol [skinny | sip | ...]] [port]
```

If one accepts the argument that proxy / full scrutiny firewalls provide higher security, it follows that the implementation mechanics need to be published for review by the security community. Unfortunately there are no details as to how the fixup commands are implemented.

The hardware availability for PIX is as follows:[1]

> The **Cisco PIX 535 Firewall**, intended for large Enterprise and Service Provider environments, provides over 1 Gbps of firewall throughput with the ability to handle up to 500,000 concurrent connections. Certain PIX 535 models include stateful high-availability capabilities, as well as integrated hardware acceleration for VPN, providing up to 95 Mbps of 3DES VPN and support for 2,000 IPsec tunnels. The Cisco PIX 535 provides a modular chassis with support for up to 10 10/100 Fast Ethernet interfaces or 9 Gigabit Ethernet interfaces.
>
> The **Cisco PIX 525 Firewall**, intended for Enterprise & Service Provider environments, provides over 360 Mbps of firewall throughput with the ability to h&le as many as 280,000 simultaneous sessions. Certain PIX 525 models include stateful high-availability capabilities, as well as integrated hardware acceleration for VPN, providing up to 70 Mbps of 3DES VPN & support for 2,000 IPsec tunnels. The PIX 525 provides a modular chassis with support for up to 8 10/100 Fast Ethernet interfaces or 3 Gigabit Ethernet interfaces.
>
> The **NEW Cisco PIX 515E Firewall** intended for Small-to-Medium Business & Enterprise environments, provides up to 188 Mbps of firewall throughput with the ability to h&le as many as 125,000 simultaneous sessions. Certain PIX 515E models includes stateful high-availability capabilities, as well as integrated support for 2,000 IPsec tunnels. The PIX 515E provides a modular chassis with support for up to six 10/100 Fast Ethernet interfaces.
>
> The **NEW Cisco PIX 506E Firewall**, intended for Remote Office/Branch Office environments, provides up to 20 Mbps of firewall throughput and 16 Mbps of 3DES VPN throughput. The PIX 506E uses a compact, desktop chassis and provides two auto-sensing 10Base-T interfaces.
>
> The **Cisco PIX 501 Firewall**, intended for Small Office and Enterprise Teleworker environments, provides up to 10 Mbps of firewall throughput and 3 Mbps of 3DES VPN throughput. The PIX 501 delivers enterprise-class security in a compact, plug-n-play security appliance, and includes an integrated 4-port Fast Ethernet (10/100) switch and one 10Base-T interface.

[1] http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

> Built upon a hardened, purpose-built operating system for security services, PIX OS, PIX firewalls provide the highest levels of security and have earned many industry accolades including ICSA Firewall and IPsec certification as well as Common Criteria EAL4 evaluation status. PIX Firewalls provide a wide range of security and networking services including Network Address Translation (NAT), Port Address Translation (PAT), content filtering (Java/ActiveX), URL filtering, AAA (RADIUS/TACACS+) integration, support for leading X.509 PKI solutions, DHCP client/server, PPPoE support (coming in Q1 2002) and much more. PIX Firewalls also provide advanced security services for multimedia applications and protocols including Voice over IP (VoIP), H.323, SIP, Skinny and Microsoft NetMeeting, giving you the peace of mind when deploying next generation converged network services.

The PIX component break down shown below is less than 20% of the total.

Product	Product Description	Price
PIX Firewall Bundles		
PIX-515-FO-BUN	PIX 515FO Bundle (Chassis, failover SW, 2 FE ports)	
PIX-525-R-BUN	PIX 525R Bundle (Chassis, restricted SW, 2 FE ports)	
PIX-525-UR-BUN	PIX 525UR Bundle (Chassis, unrestricted SW, 2 FE ports, VAC)	
PIX Firewall Series Chassis		
PIX-525	PIX Firewall 525 Chassis	
PIX-525-DC	PIX 525 DC Chassis	
PIX-535	PIX Firewall 535 Chassis	
PIX Firewall Software		
SF-PIX-6.1	PIX v6.1 Software for the PIX Chassis	
PIX-6.1-DOC=	PIX OS v6.1 documentation, guides, release notes	
PIX Firewall Feature Licenses		
PIX-515UR-SW	Unrestricted feature license for PIX 515/515E Firewall	
PIX-525-SW-FO	Failover feature license for PIX 525 Firewall	
PIX-525-SW-R	Restricted feature license for PIX 525 Firewall	
PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall	
PIX Firewall Encryption Licenses		
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	
PIX-VPN-3DES=	168-bit 3DES VPN feature license for PIX Firewall	
PIX Firewall Interfaces and Cards		
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	
PIX-VPN-ACCEL=	VPN Accelerator Card (VAC) for PIX Firewall	
PIX Firewall Software License Upgrades		

PIX-525-SW-FO-UR=	PIX 525 failover to unrestricted license upgrade

PIX Firewall Memory Upgrades

PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)
PIX-FLASH-16MB=	PIX 16MB ISA Flash card

PIX Firewall Spares and Accessories

PIX-535-HW=	PIX 535 rack mounts, console cable, failover cable
PIX-535-PWR-AC	Redundant AC power supply for PIX 535

PIX Documentation

DOC-7813512=	Cisco PIX Firewall System Log Messages
DOC-7813513=	Cisco PIX Firewall Command Reference
DOC-7813562=	Cisco PIX Firewall and VPN Configuration Guide

PIX Firewall Relicensing for Used Equipment

LL-PIX-525-SW-UR	PIX 525 Unrestricted Function Software License

1.2.4 VPN Selection

The need for encryption of data is determined through the ease of its capture and degree of financial loss due to its misuse. As was discussed in the Requirements section, the dollar value of compromise is low for Customers, medium for Suppliers and high for GIAC staff & Partners.

VPN encryption methods utilize various algorithm and key lengths, with tradeoffs of speed and strength, and hardware encryption offering higher performance.

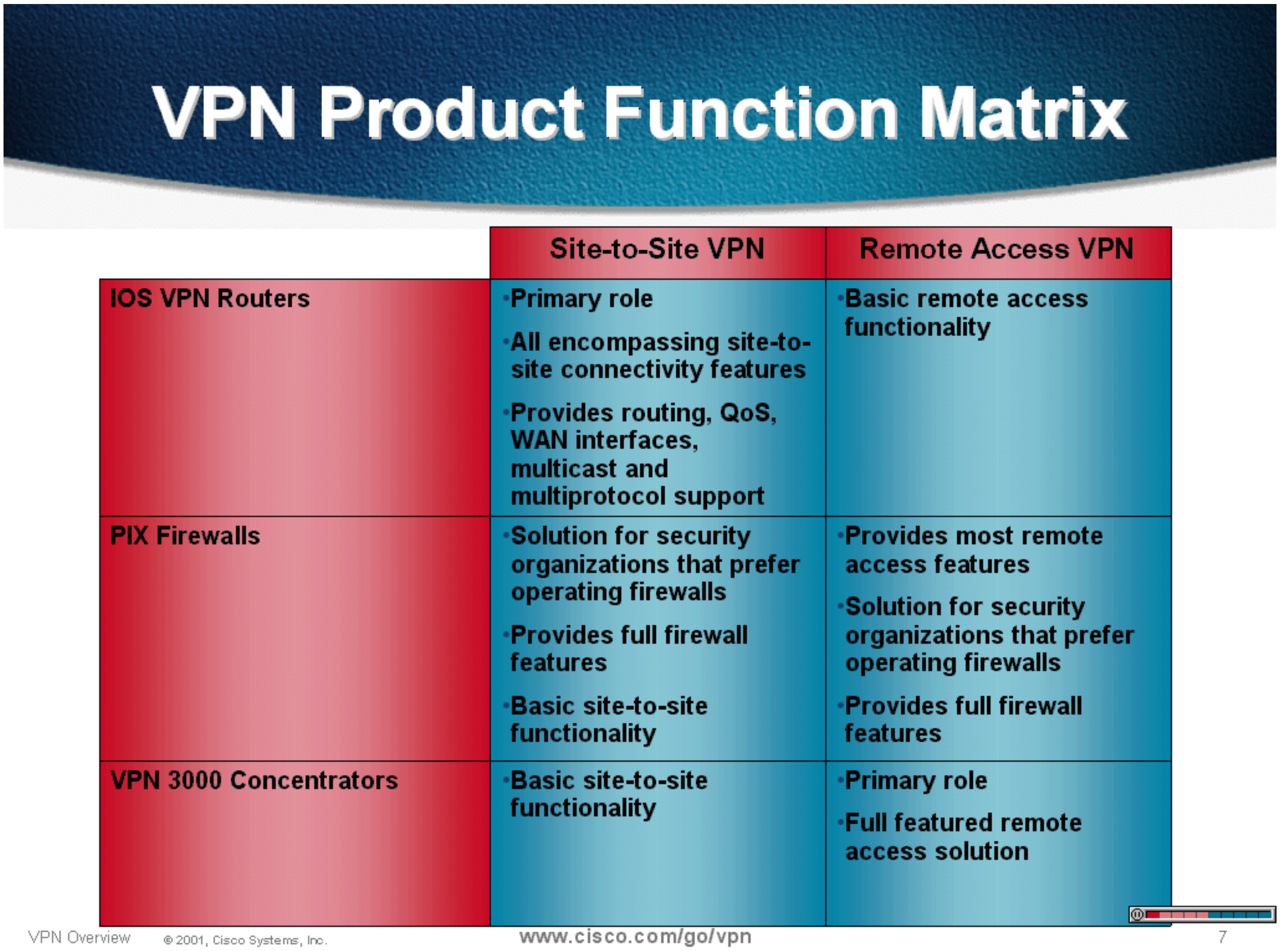
Authentication methods come in various degrees of complexity with the strongest combining authentication w/ message non-repudiation. Various digests such as SHA or MD5 provide message integrity. Tunneling protocols utilize the network / transport or application layers. They include PPTP, IPSec, L2TP, SSL, SSH, SOCKS and ICA.

VPN implementations are becoming increasingly more prevalent, including in Firewalls, appliances, routers, concentrators and PCs. Best practice methods require firewall changes be kept at a minimum, thus decreasing their suitability for frequently changing VPNs. Low cost solutions offer confidentiality & integration with third party authentication. Higher end solutions have access control functionality by limiting access to specific TCP/IP applications at the Gateway, as well as centrally controlled firewall functionality at the VPN client.

There are significant risks to both entities utilizing a VPN, since there is little control over the remote environment. VPN Clients may be compromised through split tunneling (concurrent VPN sessions) especially with continually connected Internet technologies such as cable & DSL. A hacker may hijack or initiate legitimate VPN sessions and obtain access to remote networks. The risks may be mitigated by placement of screening devices (e.g. filter routers, firewalls, content inspectors) to ensure messages / protocols traversing the link are of the expected format and content.

VPNs can be categorized as providing Site-to-Site, or Remote Access functionality. In a Site-to-Site configuration all traffic between the two sites is routed through VPN devices. This is suitable for a many to many access, and is transparent to the communicating devices. A Remote Access VPN involves single devices accessing a VPN Concentrator that provides access to remote location resources. The devices have IPSec implemented internally

The following graphic shows the selection of Cisco's product offerings for Site-to-Site VPNs and Remote Access VPNs.

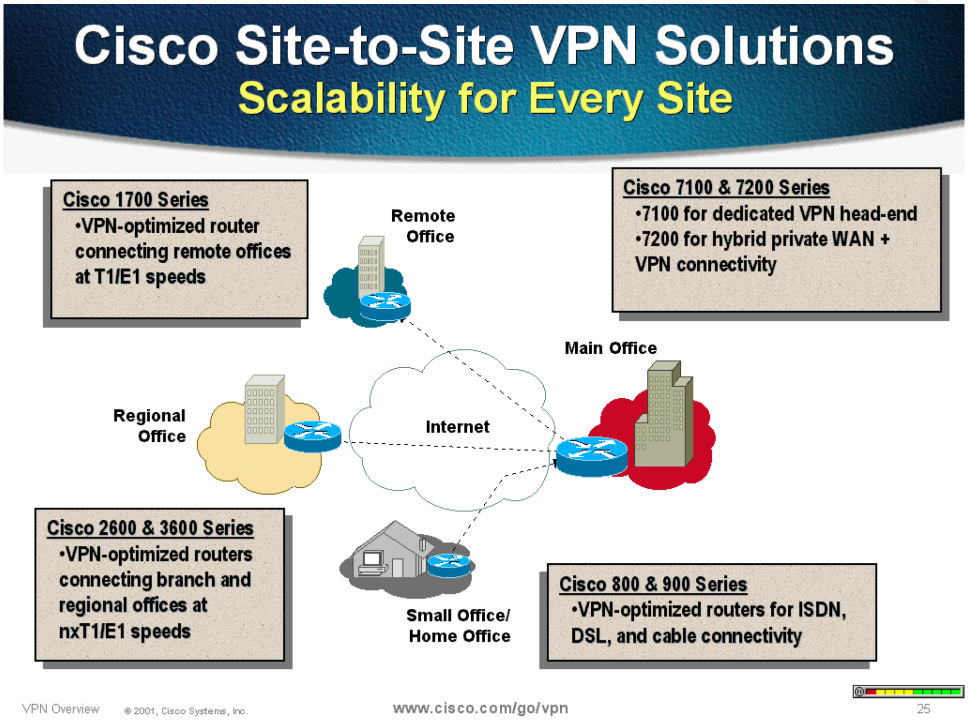


VPN Product Function Matrix

	Site-to-Site VPN	Remote Access VPN
IOS VPN Routers	·Primary role ·All encompassing site-to-site connectivity features ·Provides routing, QoS, WAN interfaces, multicast and multiprotocol support	·Basic remote access functionality
PIX Firewalls	·Solution for security organizations that prefer operating firewalls ·Provides full firewall features ·Basic site-to-site functionality	·Provides most remote access features ·Solution for security organizations that prefer operating firewalls ·Provides full firewall features
VPN 3000 Concentrators	·Basic site-to-site functionality	·Primary role ·Full featured remote access solution

VPN Overview © 2001, Cisco Systems, Inc. www.cisco.com/go/vpn 7

The following graphic shows various Cisco products for Site-to-Site VPNs.



Cisco Site-to-Site VPN Solutions

Scalability for Every Site

Cisco 1700 Series
- VPN-optimized router connecting remote offices at T1/E1 speeds

Cisco 7100 & 7200 Series
- 7100 for dedicated VPN head-end
- 7200 for hybrid private WAN + VPN connectivity

Cisco 2600 & 3600 Series
- VPN-optimized routers connecting branch and regional offices at nxT1/E1 speeds

Cisco 800 & 900 Series
- VPN-optimized routers for ISDN, DSL, and cable connectivity

We choose the 7206 since it provides the greatest level of performance. In the event that the decreased functionality for Remote Access as mentioned in the prior graphic becomes an issue we will augment the architecture with a 3000 Concentrator.

The IOS VPN 7206 router will limit access as a function of the Source device or LAN. The 7206 is placed between the Border Router and Firewall to allow the Firewall to also provide another layer of defense by ensuring the traffic allowed into the GIAC is limited to the desired functionality.

1.2.5 Security Architecture Details

The Security Architecture Diagram from §1.2.1 should be referenced for this section.

GIAC uses [1] private Class B address range, 172.68.0.0 sub netted to Class C subnets using a 24 bit mask and [4] private Class C address ranges, 192.168.1.0/24 through 192.168.4.0/24. Also used are [64] public addresses, 200.1.1.0/26 to 200.1.1.63/26.

The Border Router uses public addresses 200.1.1.1/31, 200.1.1.2/31 and 192.168.1.2/24 to communicate w/ the ISP, 7206 VPN and PIX respectively.[2]

The 7206 VPN uses the unregistered public address 200.1.1.3/31 and private address 192.168.2.2/24 to communicate with the Border Router and PIX respectively.

The PIX Outside interface uses the private address of 192.168.1.1/24, 192.168.2.1/24, 192.168.3.1/24, and 192.168.4.1/24 to communicate with the Border router, VPN, DMZ, and Inside LAN.

A private class B address range of 172.16 is used for the GIAC Internal LAN as front ended by the Layer 3 switch. The Layer 3 switch is not used to provide any internal LAN security through segmentation, but rather to limit broadcast traffic collisions. As circumstances change, it may be used to limit traffic between segments.

The Firewall provides Static, Dynamic NAT'g and PAT'g as discussed in detail in the Security Policy Section.

Servers in the DMZ are Static NAT'd to Public addresses and advertised through the Naming Services for Public access. The Web Sphere App Server is Static NAT'd to a Public address but not advertised in the Naming Services for protection.

Partner VPN traffic is Dynamically NAT'd to a GIAC Private address subnet that is used to define the access limitations. Similarly as to GIAC staff remote access through the VPN with different GIAC Private address subnets to distinguish between the access rights of Sales and Technical staff.

[2] A 31 bit subnet conserves addresses by eliminating broadcast addresses on point to point connections. The Cisco reference to RFC 3021 is: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft31addr.htm#

Local GIAC staff have their private addresses PAT'd to a Public address for Internet access. With respect to the Netmeeting requirement, Users are given a 172.16.190.0/24 address which is recognized by the PIX and dynamically NAT'd to a Public address for the Session duration.

The GIAC LAN is segregated into GLF and Corporate Computer Services (CCS) segments. This emphasizes the unrelated nature of a Web based application and a Corporate LAN.

The GLF Components are:

Tier 1 – Browsers provide **access** to the GLF application Web Servers over the Internet for **Customers, Suppliers & Partners**. HTTP is used for non-confidential transactions and SSL for confidential.

Partner access to the GLF Web Sphere App Server for Telnet & FTP activities is done through the Site-to-Site VPN. The message flow is from Partner Desktop to Partner VPN, to GIAC Border Router, GIAC 7206 VPN, GIAC 525 PIX, and lastly to the GIAC Web Sphere App Server.

Tier 2 – These are Web Sphere Web Servers located in the PIX DMZ segment.

Tier 3 - These are Web Sphere App Servers located in the PIX Inside segment.

Tier 4 – These are the GLF Data Servers located in the PIX Inside segment.

The CCS Components are:

Remote Access – The GIAC Sales & Tech staff use laptops w/ Cisco's Secure IPSec VPN Client to access the GIAC LAN. Sales access is limited to Email, whereas the Tech staff have access to all GIAC components. Authentication & Authorization is done at the 7206 and PIX.

Local Access – The GIAC staff is segregated into distinct Class C segments that are used to determine their access rights.

The CCS External Services segment contains the DNS and SMTP relay servers. They both receive and send information to the Internet using Public addresses as NAT'd by the PIX firewall.

The CCS Internal Services segment contains the Mail Server & associated filter, internal DNS, Proxy and associated filter & LDAP servers. The Mail filter protects against attachments that may be harmful and similarly for the Web Proxy. The Mail Server receives and sends messages to the SMTP Relay located in the DMZ.

The GLF & CCS Servers segment contains servers that pertain to both GLF and CCS functionality. These include the Log SecurID, NTP, IDS and Site Minder Servers. All of the DMZ, VPN, Server, Router, Firewall, etc., devices send messages to the Log Server using Syslog. Similarly as to the IDS agents sending and receiving messages to the IDS Manager as discussed in the Security Policy assignment.

Assignment 2:1 Security Policy

2.1 Border Router

In April 2002 the Center for Internet Security (**CIS**) released a Cisco Router Audit program [3]. It was used in conjunction with the NSA Security Recommendation Guide to crosscheck the procedures developed here.

2.1.1 Differentiate between Policies and Procedures

Policies are high level statements of required conduct, and procedures are detailed instructions for the implementation of policies. The specific demarcation point varies as a function of targeted audience expertise and topic complexity.

A conceptual way of illustrating the policy / procedure interplay is shown below. Policies are in blue, procedures in green.

Policies
Level 1
Level . . .
Level n
Procedures
Level n+1
Level . . .
Level z

An example is shown below, with the policy definitions extending to significant detail.

Ensure Network Devices are impervious to attack:
For Border Routers:
Add needed functionality:
Of remote logging:
Enable traffic to traverse intervening Firewall(s)
Add an ACL permit statement for UDP 514
Access-list acl_in permit UDP host a.b.c.d host w.x.y.z eq 514
Enable connectivity at the Log Server
Time synchronization for event correlation
Eliminate unneeded functionality.

[3] http://www.cisecurity.org/bench_cisco.html

For Firewalls:

Thus the Policies in increasing specificity are:

- Ensure Network Devices are impervious to attack.
- Ensure the Network Devices that are Border Routers are impervious to attack.
- Ensure the Network Devices that are Border Routers are impervious to attack by the addition of needed functionality.
- Ensure the Network Devices that are Border Routers are impervious to attack by the addition of the needed functionality of remote logging.

And the associated Procedures in increasing specificity are:

- Enable log traffic to traverse intervening Firewalls.
- Enable log traffic to traverse intervening Firewalls w/ an ACL permit for UDP 514.
- Enable log traffic to traverse intervening Firewalls by the addition of an ACL permit for UDP 514 – "Access-list acl_in permit UDP host a.b.c.d host w.x.y.z eq 514".

2.1.2 Add Needed Functionality

```
!
! Add Needed Functionality to ensure the router is impervious to attack
!
!
service password-encryption             ! Enable MD5 hashing
enable secret !@#$%                                ! Store the enable password in
non reversible crypto
I
line console 0                          ! Password protect console & set session
timeout
  login
  password SECRET
  exec-timeout 1 30
banner /  WARNING:  We prosecute trespassers /
!
line vty 0 4
! Prevent non SSH Telnet access & set session timeout
  transport input ssh
  exec-timeout 1 30
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging 172.16.50.2
logging buffered 10000
logging facility border_router
logging trap debugging
logging console emergencies
```

```
  !
  clock timezone PST
  clock summer-time PST recurring
  ntp authenticate
  ntp authenticaton key 1234 md5 104D000A0618 7
  ntp trusted-key 1234
  ntp server 172.16.50.4 key 1234
  ntp access-group query-only
```

2.1.3 Eliminate Unneeded Functionality – SNMP, HTTP, etc.

For the sake of security, SNMP is viewed as non essential. The issues with authentication for community strings and version specific bugs are thus avoided. As GIAC evolves, a network management platform may be implemented. A work around to SNMP is to have a management server periodically send traffic to each interface & empirically determine state.

IP's loose source routing protocol is disabled so that the router will drop any packets so enabled. This is done to prevent delivery of harmful packets to destinations that normally cannot be reached due to access lists. Unnecessary services include TCP & UDP services used for echo, character generation & discarding data. Similarly as to the Finger server which can provide a hacker with information such as who is logged in and from where. Similarly as to BOOTP and HTTP. Layer 3 to layer 2 broadcast mapping and Smurf amplification are disabled since both can result in denial of service problems. ICMP unreachable messages are disabled since they give out network information.

```
!
! Eliminate unneeded / undesired functionality
!
no snmp server
no ip source-route
!
!               Don't forward packets w/ no clear route
no ip classless
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http server
no ip bootp server
!
!               don't show internal addresses
no ip proxy-arp
no cdp run
!
!               Disable network autoloading from a TFTP host
no service config
!
!
interface Ethenet 0
  no ip directed-broadcast
  no ip unreachables
```

```
   no ip redirects
   no ip proxy-arp
interface Ethenet 1
   no ip directed-broadcast
   no ip unreachables
   no ip redirects
   no ip proxy-arp
!
!                 Disable the auxiliary port
no access-list 50
access-class 50 deny 0.0.0.0 255.255.255.255
line aux 0
  access class 50 in
!
!                 Shut down the unused Ethernet ports 3
interface eth 0/3
  shutdown
  exit
```

2.1.4 Implement First Layer Protective Device Functionality

The primary role of the border router is to provide reliable & rapid communications. In addition, it is well suited as a first layer protective device that drops & logs undesirable traffic. The protective functionality is limited in scope to simplistic static packet filtering to ensure rapid processing and stability.

Rule sequencing involves a balance of potentially opposing objectives of speed optimization and comprehension, which is essential to correct functionality. Since the H/W performance to cost ratio is continually improving, the GIAC implementation generally treats comprehension as controlling.

Nevertheless, it is important to understand that in the event of latency / throughput / utilization problems the rule ordering may be adjusted based on empirical traffic counts so that the most frequently exercised rules are processed first. It is also important to recognize the fact that stress occasions with peak utilizations and dropped packets are determinative rather than average metrics.

The border router policy is that everything is allowed except what is specifically not allowed. The firewall policy is that everything is disallowed except what is specifically allowed. A nice consequence is that the firewall does not have to verify the border router functionality.

2.1.4.1 Drop Undesired Inward Packet ACL’s

```
!  Drop undesired ingress packets
!
no access-list ingress_drop                                ! start out clean
```

```
ip access-list extended ingress_drop
!
! Create access list
! RFC 1918 – priv address
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log
!
!               Link local networks
deny 169.254.0.0 0.0.255.255 any log
!
!               Test Net
deny 192.0.2.0 0.0.0.255 any log
!
!               Multicast or engineer
deny ip 224.0.0.0 31.255.255.255 any log
!
!               Class E reserved
deny ip 240.0.0.0 63.255.255.255 any log
!
!               Unallocated
deny ip 248.0.0.0 31.255.255.255 any log
deny ip 255.0.0.0 0.255.255.255 any log
deny ip 0.0.0.0 0.255.255.255 any log
deny ip 1.0.0.0 0.255.255.255 any log
deny ip 2.0.0.0 0.255.255.255 any log
! …
! Unallocated, 3-20 in 1st
deny ip 219.0.0.0 0.255.255.255 any log
deny ip 220.0.0.0 0.255.255.255 any log
!
! Missing source IP add
deny ip host                0.0.0.0 any log
!
! An internal add as source
deny ip 200.1.1.0 0.0.0.15 any log
!
! TFTP
deny udp any any equ 69 log
deny icmp any any 13
deny icmp any any 17
!
!               Loopback
deny host 127.0.0.0 0.255.255.255.255 log
!
! Permit remaining traffic
permit ip any any
  exit
!
!               Apply access list
```

```
interface serial 0
  ip address 200.1.1.0 255.255.255.254
  no
  ip access-group ingress_drop in
exit
```

2.1.4.2 Drop Undesired Outward Packet ACL's

```
!  Drop undesired egress packets
!                Define access list
no access-list egress_drop              ! start out clean
ip access-list extended egress_drop
   deny tcp any any range 135 139 log ! netbios/ip
  deny udp any any range 135 139 log ! netbios/ip
  deny udp any any equ 69 log           ! tftp
  deny udp any any range 161 162 log ! snmp
  deny udp any any 514 log              ! syslog
  permit ip 200.1.1.0 0.0.0.15          ! Allow our pub add's
  deny ip any any log                   ! Drop remaining traffic
!
interface Ethernet 1                    ! Apply to internal I/F
  ip access-group egress_drop in
```

2.1.4.3 Tutorial on Implementation of Static Packet Filtering

Until relatively recently the Cisco commands & tools available for creating static packet filtering were very rudimentary. The progression evolution has been from standard access-lists, to extended access-lists, to named access-lists, etc. As always there is a tradeoff of between processing speed and enhanced feature set or ease of use.

Implementation of static packet filtering may be viewed as a two part process. Part one involves the creation of a set of rules through the ***ip access-list*** command and part two defines which interface they are applied to through the ***ip access-group*** command.

The authoritative source for the use of these two commands is provided by Cisco. To get a sense of the format used, the simpler command ***ip access-group*** is shown below.

ip access-group - To control access to an interface, use the **ip access-group** interface configuration command. To remove the specified access group, use the **no** form of this command.	

ip access-group {*access-list-number* | *access-list-name*}{**in** | **out**}
no ip access-group {*access-list-number* | *access-list-name*}{**in** | **out**}	

Syntax Description	
access-list-number	Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
access-list-name	Name of an IP access list as specified by an **ip access-list** command.
In	Filters on inbound packets.
Out	Filters on outbound packets.
Defaults - No access list is applied to the interface.	
Command Modes - Interface configuration	

Usage Guidelines

Access lists are applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

For standard outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.
If the specified access list does not exist, all packets are passed.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable input access lists on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—an SSE configured with simple access lists can still switch packets, on output only).

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
interface ethernet 0
ip access-group 101 out
```

An access list is compromised of one or more lines that present match criteria and a permit or deny action in the event of a match. The match criteria are based on packet field contents. Each packet as it arrives or as it prepares to go out has its field contents examined against the match criteria.

The access list lines are executed in a top down sequence until a match is found or the list ends. The sequential processing represents a rudimentary approach to logic flow and does not allow for more sophisticated constructs such as "if / then" statements. Cisco does not provide an Editor for manipulating the ACL information so an essential work around is a telnet program that allows "cut and paste" functions.

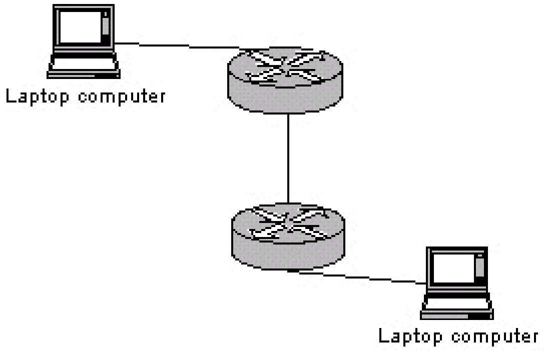
The sequential ordering of rule execution has the obvious requirement for correct order placement. For example, consider our earlier two commands for the egress_drop access list:

```
deny tcp any any range 135 139 log   ! netbios/ip
permit ip 200.1.1.0 0.0.0.15         ! Allow our pub add's
```

Clearly if we had reversed the order of the two rules a different outcome would exist. Namely, any netbios/ip traffic w/ a GIAC public address would get through, contrary to our objective. A Venn Diagram could be used to enhance visibility.

A potential gotcha exists when entering nonexistent ACL identifiers and the O/S responds with a succeeded prompt. However, by allowing this it may be possible to define the ACL subsequent to its reference in interface & direction statements.

A methodology for confirming a rule has been correctly applied is shown below.



One laptop will initiate the desired message using suitable packet crafting SW such as HPING2, NetCat, or NMAP.. The other laptop will have sniffer SW such as TCPdump or WINdump to confirm dropping or permitting of the traffic. In a Lab environment cross connect cables may be used to simplify the connectivity. Although less certain, one of the laptops may be eliminated by using the Router log for confirmation of the action or inaction taken.

Three rules that may be tested with this approach are:

```
ip access-list extended egress_drop
   deny tcp any any range 135 139 log                    ! netbios/ip
  deny udp any any range 135 139 log                     ! netbios/ip

ip access-list extended ingress_drop
  deny ip 10.0.0.0 0.255.255.255 any log
  deny ip 172.16.0.0 0.15.255.255 any log
```

2.2 Primary Firewall

2.2.1 Create the Policy Matrix

We use a Policy Matrix to aggregate all of the Company Policies. The Policy Matrix is essential since it translates more verbose policy statements into succinct statements and forces enumeration of all the requirements. The Matrix allows visibility into rule inter relationships for global verification and results in the creation of tight and effective rules.

The Matrix as derived in the subsequent sections is shown below.

Rule #	What Detailed	Protocol	Source IP Address (Interface-Host or Segment)	Destination IP Address (Interface-Host or Segment)	Source TCP Port(s)	Dest TCP Port(s)	Source UDP Port(s)	Dest UDP Port(s)
1	Access GLF to purchase / provide / bulk obtain fortune sayings, review order status, transaction histories & create reports.	HTTP, HTTPS	Outside-Any Inside-Any	DMZ - Web Servers	Any	80, 443	na	na
2	Authentication, authorization, accounting, administration using Netegrity Site Minder	Custom: Siteminder	DMZ-Web Servers	nside- Netegrity Site Minder	Any	52441-52444	na	na
3	Web Server Presentation Layer to App Server Business Logic Layer	Custom: Corba	DMZ-Web Servers	Inside-App Servers	gt 1023 gt 1023 gt 1023 gt 1023	5400 27000 14015 3899	na	na
4	App Server Business Logic Layer to Web Server Presentation Layer	Custom: Corba	Inside-App Servers	DMZ - Web Servers	gt 1023 gt 1023 gt 1023	35000 55323 26888	na	na
5	Remote control	SSH	Inside-Tech Staff	DMZ-All Servers	Any	22	na	na

6	Log events remotely to prevent intruder manipulation	Syslog	Outer-Router DMZ-Any	Secure area - Log Server	Na	na	any	514
7	FTP from & to Web app servers	FTP	Partner VPN group	Tier 3- App Servers	20, 21			
8	Remote access level equal to that when local: NT file & print servers, Notes Email, Various application servers, Internet access??, routers, switches, hubs.	Netbios, NBT/CIFS, Telnet, FTP, Netfinity, SSH	Employee VPN group	Tiers 3 & 2	Many			
9	IDS agents communicating w/ the IDS management server	Custom: ITA	External services seg servers	Secure Area - Management Server	23569-23589	6051		
10	IDS manager initiating session w/ IDS agents	Custom: ITA	Secure area Management Server	External Services seg servers	33569-33589	6052		
11	Probes to Manager communication	Get	Probes	Secure Area - Management Server				
12	Receive & send Email to Mail Relay	IMAP, SMTP, POP3	Bidirectional - SMTP relay, Internet	Bidirectional - SMTP relay, Internet		SMTP-25 POP3-110 IMAP-143		
13	Receive & send Email to Mail Relay	SMTP	Bidirectional - SMTP relay, Mail Server	Bidirectional - SMTP relay, Mail Server				
14	Configure Firewall to provide NAT'g	na	External services seg servers	Internet				

2.2.1.1 Ports for Web Sphere Inter-process Communication

The ports used between the Web Sphere HTTP and application servers are illustrated below.

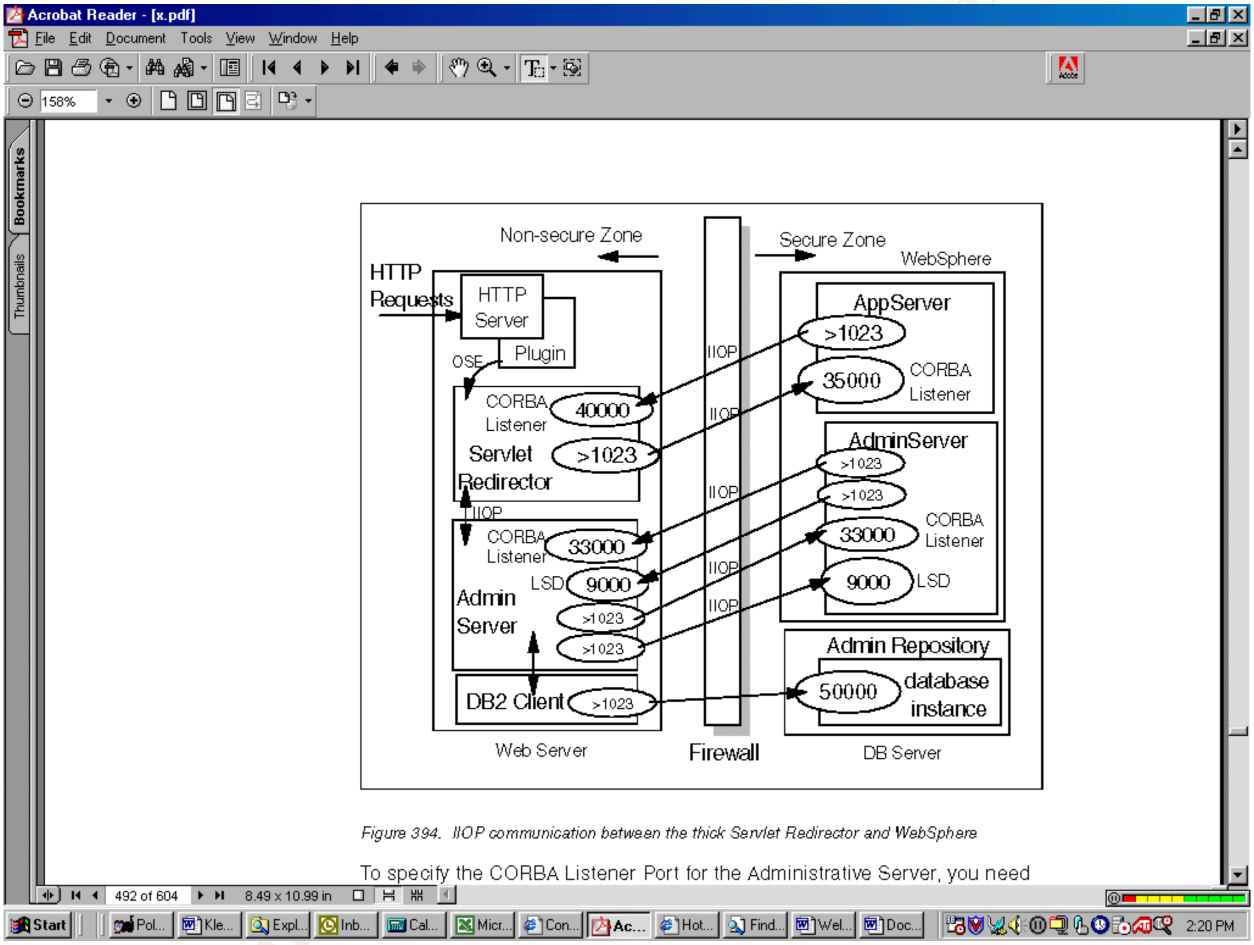


Figure 394. IIOP communication between the thick Servlet Redirector and WebSphere

To specify the CORBA Listener Port for the Administrative Server, you need

Since we will be using a Stateful Firewall, we only need to create openings for the initiating process. We further simplify things by assuming that the ephemeral ports can be locked & changed at installation. Thus, we have:

Web Server to App Server:

Servlet redirector:	>1023 to 5400;
Admin Server:	>1023 to 27000; >1023 to 14015
DB2 Client:	>1023 to 38999

App Server to Web Server:

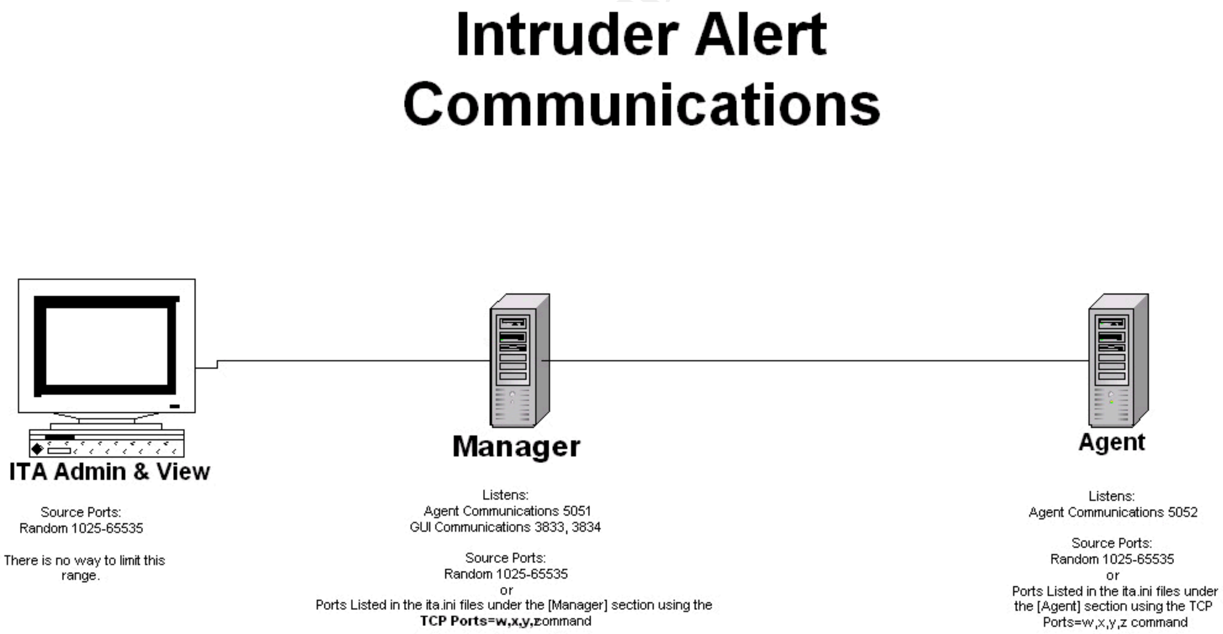
Corba	>1023 to 35000
Admin	>1023 to 55323; >1023 to 26888

2.2.1.2 Ports for Authentication, Authorization & Accounting (AAA) Services

The Site Minder default ports for inter-process communication between Web agents & the Policy Server are modified by the Site Minder Policy Server Management Console to be 52441 through 52444.

2.2.1.3 Ports for IDS

Host IDS is implemented in the GIAC network with Server installed Agents alternatively initiating and responding to the Manager Server. The firewall has to accommodate for the exchange of messages shown below.


Intruder Alert Communications
ITA Admin & View
Source Ports:
Random 1025-65535
There is no way to limit this range.
Manager
Listens:
Agent Communications 5051
GUI Communications 3833, 3834
Source Ports:
Random 1025-65535
or
Ports Listed in the ita.ini files under the [Manager] section using the
TCP Ports=w,x,y,zcommand
Agent
Listens:
Agent Communications 5052
Source Ports:
Random 1025-65535
or
Ports Listed in the ita.ini files under the [Agent] section using the TCP Ports=w,x,y,z command

2.2.1.4 Ports for Netmeeting

Netmeeting requires Internet connected participating workstations to have public addresses. Based on Business Unit requirements a determination is made that a maximum of six concurrent workstations will suffice. Microsoft's firewall requirements for Netmeeting are as follows:

> You can configure firewall components in a variety of ways, depending on your organization's specific security policies and overall operations. While most firewalls are capable of allowing primary (initial) and secondary (subsequent) Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections, they might be configured to support only specific connections based on security considerations. For example, some firewalls allow only primary TCP connections, which are considered the most secure and reliable.
>
> To enable NetMeeting 3 multipoint data conferencing — program sharing, Whiteboard, Chat, file transfer, and directory access— your firewall only needs to pass through primary TCP connections on assigned ports.
>
> NetMeeting audio and video features require secondary TCP and UDP connections on dynamically assigned ports. Therefore, if you establish connections through firewalls that accept only primary TCP connections, you will not be able to use the audio or video features of NetMeeting.
>
> <u>Establishing a NetMeeting Connection with a Firewall</u>
>
> When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection. The following table shows the ports, their functions, and the resulting connection.

Port	Function	Outbound Connection
389	Internet Locator Service (ILS)	TCP
522	User Location Service	TCP
1503	T.120	TCP
1720	H.323 call setup	TCP
1731	Audio call control	TCP
Dynamic	H.323 call control	TCP
Dynamic	H.323 streaming	Real-Time Transfer Protocol (RTP) over UDP

> If you use a firewall to connect to the Internet, it must be configured so that the IP ports are not blocked. To establish outbound NetMeeting connections through a firewall, the firewall must be configured to do the following:
>
> Pass through primary TCP connections on ports 389, 522, 1503, 1720, and 1731. Pass through secondary TCP and UDP connections on dynamically assigned ports (1024-65535).
>
> The H.323 call setup protocol dynamically negotiates a TCP port for use by the H.323 call control protocol. Also, both the audio call control protocol and the H.323 call setup protocol dynamically negotiate UDP ports for use by the H.323 streaming protocol, called the Real-Time Transfer Protocol (RTP). In NetMeeting, two UDP ports are determined on each side of the firewall for audio and video streaming, for a total of four ports for inbound and outbound audio and video. These dynamically negotiated ports are selected arbitrarily from all ports that can be assigned dynamically.
>
> NetMeeting directory services requires port 389. Microsoft Internet Locator Service (ILS) servers, which support the Lightweight Directory Access Protocol (LDAP) for NetMeeting, also require port 389.”

2.2.2 Implement Firewall Ruleset

2.2.2.1 Apply Configuration Basics

The addressing is based on:

- The 64 public addresses GIAC has purchased 200.1.1.0 / 26 (0-63).
- The DMZ segment is static NAT’d from 192.168.3.33 - 63 to 200.1.1.33 – 63.
- Netmeeting users are dynamically NAT’d from 172.16.190.0 to 200.1.24-30.
- Internet users are PAT’d from 172.16.0.0 to 200.1.1.23

```
:
:                  Create logical names & Assign security levels
nameif ethernet0 outside security0
nameif ethernet1 vpn_path security50
nameif ethernet2 dmz security25
nameif ethernet3 inside security100
:
:                  Define interfaces and line speeds
interface ethernet0 10full
interface ethernet1 10full
interface ethernet2 10full
interface ethernet3 10full
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
:
:                Define IP addresses for DMZ servers
name 200.1.1.33 web_server_pub
name 200.1.1.34 dns_server_pub
name 200.1.1.35 smtp_server_pub
name 192.168.3.33 web_server_priv
name 192.168.3.34 dns_server_priv
name 192.168.3.35 smtp_server_priv
:
:                Define IP addresses for PIX interfaces
name 192.168.1.1 pix_if_outside
name 192.168.2.1 pix_if_vpn
name 192.168.3.1 pix_if_dmz
name 192.168.4.1 pix_if_inside
:
:                Define IP Addresses for Border router, VPN, Layer 3 switch interfaces
name 192.168.1.2 bord_route_if_in
name 192.168.2.2 vpn_if_inside
name 192.168.3.2 layer2_switch
name 192.168.4.2 layer3_switch
:
:                Define IP Addresses for Network Segments
name 192.168.3.0 dmz_sgmnt_priv
:
:                Define IP Addresses for Inside located Servers
name 172.16.10.3 app_server
name 172.16.20.3 mail_server
name 172.16.50.6 siteminder_srvr
name 172.16.50.2 log_server
name 172.16.50.5 ids_mgr_server
name 172.16.100.50 remote_cntrl_hst
:
:                Assign interface IP addresses
ip address outside pix_if_outside 255.255.255.0
ip address vpn_path pix_if_vpn 255.255.255.0
ip address dmz pix_if_dmz 255.255.255.0
ip address inside pix_if_inside 255.255.255.0
ip address intf4 127.0.0.1 255.255.255.255
ip address intf5 127.0.0.1 255.255.255.255
:
:                Define prompt, arp, mtu, etc.
hostname PIX-525
:
:                Select an ARP timeout of 4 hours
arp timeout 14400
:
:                Enable logical name usage
names
```

```
:
:                    Define the number of lies per diplay page
pager lines 24
:
:                    Define the MTU size
mtu outside 1500
mtu vpn_path 1500
mtu dmz 1500
mtu inside 1500
mtu intf4 1500
mtu intf5 1500:
:
:   Assign the default route for the Outside interface as the Border Router with a hop distance of 1
route outside 0 0 192.168.1.2 1
:
:   Assign a static route for the Inside interface:  The Layer 3 Switch for the 172.16 network, 1 hop
route inside 172.16.0.0 255.255.0.0 192.168.4.2 1
```

2.2.2.2 Harden

```
:
:                Remote logging to log server and IDS manager server
logging on
logging buffered notifications
logging host in_if_name inside ip_address log_server protocol udp
logging host in_if_name inside ip_address ids_mgr_server udp
:
:                enable ntp
clock set 21:0:0 apr 1 2002
logging timestamp
:
:                Remote control: Disallow Telnet, allow SSH v1.x clients only from tech segment
no telnet
ssh 172.16.100.0 255.255.255.0 inside
ssh timeout 15
:
:                Password protect console & set session timeout, generate banner
enable password go
:
:                Explicitly state default idle values for PIX resources to be freed
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
timeout udp 0:02:00 rpc 0:10:00 h323 0:05:00
timeout sip 0:30:00 sip_media 0:02:00
:
:                Change default value for reauthentication due to inactivity
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
:
:                Disable SNMP access and SNMP trap generation; disable HTML access
no snmp-server location
no snmp-server contact
no http server enable
```

2.2.2.3 Implement NAT and PAT

Access to the Internet from within the secure portion of the network for GIAC employees is implemented through Hide NAT. Hide NAT facilitates the use of private address space by requiring only one public address for all Users accessing the Internet. Hide NAT does a many to one translation with the mapping being kept at each message in the TCP Source port number which is used to determine the internal address through a mapping table upon return. Cisco's calls this Port Address Translation (PAT).

Netmeeting functionality will not work with PAT because the TCP Source field is required for the protocol to function. NAT address pooling overcomes this by providing a temporarily dedicated public IP address.

So, the requirement becomes for differential NAT usage based upon the application: PAT for HTTP and NAT for Netmeeting. The present version of PIX v6.1 does not have this ability, but v6.2 is expected to. The solution may involve Access lists to differentiate based upon the TCP ports.

An unlikely solution is given in Cisco’s v6.1 documentation:

> There should be enough global addresses to handle the number of users each interface may have trying to access the lower security interface. You can specify a single PAT entry, which permits up to 64,000 hosts to use a single IP address. PAT has some restrictions in its use such as it cannot support H.323 or caching nameserver use, so you may want to use it to augment a range of global addresses rather than using it as your sole global address. For example:
>
> ```
> global (outside) 1 209.165.201.5 netmask 255.255.255.224
> global (outside) 1 209.165.201.10-209.165.201.20 netmask 255.255.255.224
> ```
>
> The first **global** command statement specifies a single IP address, which the PIX Firewall interprets as a PAT. You can specify PAT using the IP address at the interface using the **interface** keyword. The PAT lets up to 65,535 hosts start connections to the outside. PIX Firewall permits one PAT global command statement for each interface The second **global** command statement augments the pool of global addresses on the outside interface. The PAT creates a pool of addresses used only when the addresses in the second **global** command statement are in use. This minimizes the exposure of PAT in the event users need to use H.323 applications.”

The offered solution fails when the NAT addresses get used up by HTTP users & is not available to H.323 users. The problem is accentuated by the consequent lack of specificity in differentiating between application & NAT failures.

Instead of the Cisco solution, a work around is implemented that allows up to six concurrent Net meeting users by manually configuring their IP addresses to be 172.16.190.2 through 172.16.190.7 prior to initiating Net Meeting. The DHCP address space for GIAC staff is configured to exclude these addresses. So, PIX is configured as follows:

```
:
:               Provide dynamic NAT for Netmeeting use and PAT for Internet access
nat (inside) 1 172.16.190.0 255.255.255.248
nat (inside) 2 172.16.0.0 255.255.0.0
nat (inside) 3 172.16.100.0 255.255.255.0
global (outside) 1 200.1.1.24-200.1.1.30
```

```
global (outside) 2 200.1.1.23
global (dmz) 3 192.168.3.32-192.168.3.254
:
:                    Provide static NAT for DMZ servers
static (dmz, outside) web_server_pub web_server_priv
static (dmz, outside) dns_server_pub dns_server_priv
static (dmz, outside) smtp_server_pub smtp_server_priv
```

An unexpected requirement (a.k.a. gotcha) exists in needing to create a Private Dynamic NAT for Users from the Inside (Tech Staff, 172. 16.100.0/24 segment) to reach the DMZ (3rd global group above). Assuming that NAT provides security, kudos to Cisco for forcing this protection in the event a DMZ located device is compromised.

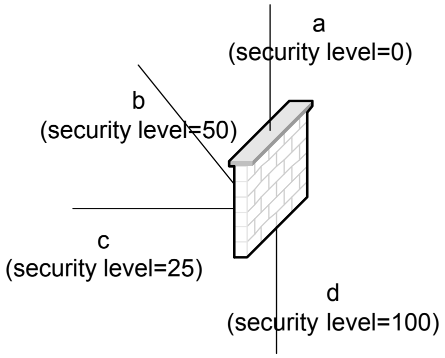
2.2.2.4 PIX Interface Design Utilizing Security Levels

For a firewall with n interfaces, the number of possible paths is (n-1)*n. So for a firewall with 2 interfaces the following 2 paths exist: a to b, and b to a. For a firewall with 3 interfaces the following 6 paths exist: a to b, a to c, plus b to a, b to c, plus c to a, c to b. For a firewall with 8 interfaces there are 56 paths to consider, so a structured approach is essential.

PIX uses security levels for each interface, and defines outbound connections as those where the originating interface has a higher security than the destination. Conversely, inbound connections are those where the originating interface is of lower security than the destination.

PIX implements the defaults that outbound connections are allowed except those specifically denied and inbound connections are disallowed except those specifically allowed. Explicit denial or permit is done through access list groups. There can be only one access list group per interface which can only be used for the **in** direction (in contrast to the IOS design which allows two access lists groups, one in the in and one in the out direction per interface).

The PIX differential default simplifies the number of rules required. It is still necessary to review the path traversal possibilities (b to c, b to d, etc.), & confirm that the defaults achieve the required action of drop or permit, when the destination is "**any**". For example, consider the following topology:



For connections initiating on the C segment, inbound connections are {c to d} where the default is that all is allowed. Outbound connections are {c to b and c to a} with the default that all is denied.

Let's assume that we want a server on the **c** segment to be able to initiate a conversation with **any** server off of the **a** segment. The PIX design provides rules that apply to the source segment but not the destination (a specific destination server or network may indirectly identify the destination segment).

Thanks to the differential defaults based on inbound or outbound classifications, a rule allowing traffic from c to **any,** is simplified by not allowing traffic from c to d nor c to b. If the differential defaults were not in effect we would need to add explicit rules to block traffic to those two segments.

It is seen that the PIX design does not scale very well with respect to interfaces, & requires judicious selection of security levels to simplify things.

With these characteristics in mind we develop the access lists for the 4 interfaces to the GIAC firewall.

2.2.2.4.1 Apply Outside Interface Ruleset

```
:
:                       OUTSIDE INTERFACE
:
:            Inbound:  Outside to DMZ.  (all connections are disallowed except those permitted).
:            Permit HTTP, HTTPS, DNS, SMTP
:
:            HTTP
access-list outside_if permit tcp any host web_server_pub eq 80
:
```

```
:                 HTTPS
access-list outside_if permit tcp any host web_server_pub eq 443
:
:                 DNS
:                 UDP port 53 is used for small & quick responses
:                 TCP port 53 is used for resps greater than 512 bytes, and zone transfers.  Since we can limit
:                 our DNS replies & want to prevent / don't require zone transfers we don't open the TCP port.
:
access-list outside_if permit udp any host dns_server_pub eq 53
:
:                 SMTP
access-list outside_if permit tcp any host smtp_server_pub eq 25
:
:                 Inbound:  Outside to VPN.  (all connections are disallowed except those permitted).
:                 The default state of all connections being disallowed is sufficient.
:
:
:                 Inbound:  Outside to Inside.  (all connections are disallowed except those permitted).
:                 Syslog, NTP, IDS
:                 Stop Java, Active X (eventually)  do so Klear now, & modify requirements
:
:                 IDS
access-list outside_if permit tcp host bord_route_if_in range 33569 33589 host ids_mgr_server eq 6052
:
:                 Syslog
access-list outside_if permit udp host bord_route_if_in host log_server eq 514
:
:                 Apply access list group to interface
access-group outside_if in interface outside
```

2.2.2.4.2 Apply VPN Interface Ruleset

```
:
:                                 VPN INTERFACE - Klear do after doing VPN (get IP addresses)
:
:                 Inbound:  VPN to inside.  (all connections are disallowed except those permitted).
:                 For partners:  Telnet, FTP (how limit Telnet to specified destination)
:                 For GIAC remote users:  Netbios, NBT/CIFS, Telnet, FTP, PCanywhere, SSH
:                 IDS, Syslog
:
:                 IDS
access-list vpn_if permit tcp host vpn_if_inside range 23569 23589 host ids_mgr_server eq 6051
:
:                 Syslog
access-list vpn_if permit udp host vpn_if_inside host log_server eq 514
:
:                 Outbound:  VPN to DMZ.  (all connections are allowed except those denied).
:                 For partners:  close all openings
:                 For GIAC remote users sales staff:  close all openings
:                 For GIAC remote users tech staff:  close all openings except remote control,
:
:
```

```
:               Outbound:  VPN to outside.  (all connections are allowed except those denied).
:
:               For partners:  close all openings
:               For GIAC remote users sales staff:  don't change default access to all
:               For GIAC remote users tech staff:  don't change default access to all
:
:
:               Apply access list group to interface
:
access-group vpn_if in interface vpn_path
```

2.2.2.4.3 Apply DMZ Interface Ruleset

```
:
:                               DMZ INTERFACE
:
:               Inbound:  DMZ to VPN.  (all connections are disallowed except those permitted).
:               The default state of all connections being disallowed is correct & sufficient.
:
:               Inbound:  DMZ to inside.  (all connections are disallowed except those permitted).
:               Siteminder, Corba, IDS, SMTP, Syslog
:
:               Siteminder
access-list dmz_if permit tcp host web_server_priv host siteminder_srvr range 52441 52444
:
:               Corba, IIOP
access-list dmz_if permit tcp host web_server_priv gt 1023 host app_server eq 5400
access-list dmz_if permit tcp host web_server_priv gt 1023 host app_server eq 2700
access-list dmz_if permit tcp host web_server_priv gt 1023 host app_server eq 14015
access-list dmz_if permit tcp host web_server_priv gt 1023 host app_server eq 3899
:
:               SMTP
access-list dmz_if permit tcp host smtp_server_priv host mail_server eq 25
:
:               Create ICMP opening to return to Inside I/F
access-list dmz_if permit icmp any any
:
:               IDS
access-list dmz_if permit tcp dmz_sgmnt_priv 255.255.255.0 range 33569 33589 host ids_mgr_server eq
6051
:
:               Syslog
access-list dmz_if permit udp dmz_sgmnt_priv 255.255.255.0 host log_server eq 514
:
:               Outbound:  DMZ to outside.  (all connections are allowed except those denied).
:               Disallow everything except SMTP, SSL, DNS
:
:               DNS - allow tcp in addition to udp in the event some replies exceed 492 bytes
access-list dmz_if permit tcp host dns_server_priv any eq 53
access-list dmz_if permit udp host dns_server_priv any eq 53
:
:               SMTP
```

```
access-list dmz_if permit tcp host smtp_server_priv any eq 25
:
:                   SSL - may be covered in PIX's HTTP fixup command (fully scrutinized) Klear check
access-list dmz_if permit tcp host web_server_priv any eq 443
:
:                   Allow ICMP traffic
no access-list dmz_if deny ip any any
:
:  disallow all other outbound traffic
access-list dmz_if deny ip any any
:
:                   Apply access list group to interface
:
access-group dmz_if in interface dmz
```

2.2.2.4.4 Apply Inside Interface Ruleset

```
:
:                                       INSIDE INTERFACE
:
:                   Outbound:  Inside to outside.  (all connections are allowed except those denied).
:
:                   Allow an internal host to SSH to network devices
access-list inside_if permit tcp host remote_cntrl_hst any eq 22
:
:                   Deny any one else to SSH through firewall
access-list inside_if deny tcp any any eq 22
:
:                   Block NetBIOS/IP, TFTP, SNMP and Syslog
access-list inside_if deny tcp any any range 135 139
access-list inside_if deny tcp any any eq 69
access-list inside_if deny tcp any any range 161 162
access-list inside_if deny tcp any any eq 514
:
:                   Disallow any access to firewall except ping
:  default PIX is to disallow pinging accross PIX to another PIX interface
:  access-list inside_if permit icmp any host pix_if_inside eq echo-request
:  access-list inside_if deny ip any host pix_if_inside
:  access-list inside_if deny ip any host pix_if_outside
:  access-list inside_if deny ip any host pix_if_vpn
:  access-list inside_if deny ip any host pix_if_dmz
:
:                   Drop all broadcast traffic
access-list inside_if deny tcp any host 172.16.255.255
access-list inside_if deny tcp any host 255.255.255.255
:
:                   Netmeeting - takes more research as to what's broken that the next version of PIX will
provide.
:                   Did fix the PIX approach of using PAT through the use of NAT, earlier.
:                   Default condition of all outbound being allowed may suffice.
:
:                   Outbound:  Inside to VPN.  (all connections are allowed except those denied).
:                 Review / Covered above.
:
:
:                 Outbound:  Inside to DMZ.  (all connections are allowed except those denied).
:                 Review / Covered above.
:
:
:                 Apply access list group to interface
:
access-group inside_if in interface inside
```

2.2.2.5 Tips, Tricks or Potential Problems (gotchas)

The PIX does not store comments in the configuration, so strict configuration control combined with the cut & paste approach needs to be used to maintain current documentation.

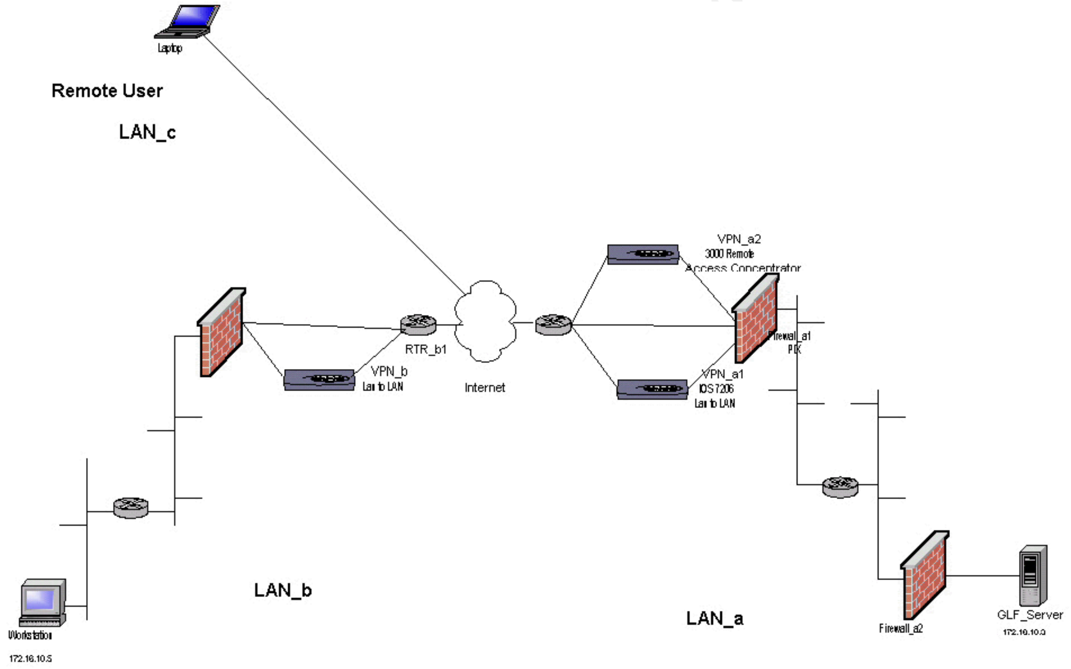
There is a partial incompatibility between Microsoft's Hyperterminal and PIX. When pasting a series of configuration lines, the PIX intermittently responds with an error message regarding the syntax. Yet when the pasted configuration is checked with the *write terminal* command it is seen to have been accepted correctly.

2.3 VPN

2.3.1 Addressing Considerations

A key aspect of the GIAC implementation of VPNs for Partner & Staff access is the addressing scheme. Cisco’s NAT Order of Operation document is useful in reaching the solution.[4]

This diagram is used to clarify the discussion that follows.



Topic 1: How to eliminate the possibility of overlapping private address spaces between the Bank and Partner LANs for the **servers**.

[4] http://www.cisco.com/warp/public/556/5.html

VPN_a1 does a **static NAT** of 172.16.10.3 to 200.1.1.10 (200.1.1.10 is a bank owned public address) of **outbound** traffic from LAN a to external LANs. Upon return, VPN_a1 does the reverse mapping from 200.1.1.10 to 172.16.10.3 to allow proper routing within LAN_a. The public address is not identified with Name Servers. The PIX could also do the NAT.

Topic 2: How to eliminate the possibility of overlapping private address spaces between the Bank and Partner LAN **workstations** when they access the GLF _Server.

GIAC tells each Partner what GIAC private address they need to dynamically NAT to at VPN-b. This allows GIAC to control access as to allowed protocols at Firewall_a1 and Firewall_a2. PAT is avoided in case FTP or Telnet use the TCP fields overwritten by PAT. PIX cannot NAT the source, eliminating this as a solution. Even if the Partners do a dynamic NAT **at their** VPNs to a public address, GIAC would want to NAT to the internal address at VPN_a1 for proper routing of the message reply back to VPN_a1.

Topic 3: How to identify GLF_Server at Partner LANs.

Use manually updated DNS entry at Partner LANs mapping “GLF Server” to 200.1.1.10 (thus each workstation uses GLF_Server rather than 200.1.1.10). So if Server is replaced by hot spare or DR site with diff, only need to modify one location per Partner site. Not true, the NAT function will take care of any new IP address at LAN_a; however, its still preferable to use Logical mnemonic address rather than physical.

Topic 4: How to limit a partner once they have Telnet access to GLF_Server from telneting to other devices internal to the GIAC LAN.

It seems reasonable to do this through a Telnet proxy that intercepts all traffic and disallows a Telnet session to hop to another system, however Cisco’s security devices including the IOS VPN, PIX, and IOS Firewall do not have this feature. Place Firewall_2 which does not allow Telnet messages to be initiated from 172.16.10.3. Place a Network IDS sensor to alert of such activity.

Topic 5: How to route within Partner LANs for the GLF_Server.

A static route needs to be created at LAN_b routers pointing the GLF_Server public address to VPN_b rather than the default for public addresses, RTR_b1. VPN_b does not automatically update (e.g. using RIP) all LAN_b routers of public addresses at the other end of the tunnel, unless GRE protocol rather than IPSec is used, overkill for the intended use.

Topic 6: How to eliminate Split Horizon risks.

IOS VPN v12.218 w/ VPN Client allows split tunneling control, but less so than a 3000 Remote Access Concentrator which can push policies to workstations. For the workstations at LAN_b we can’t control this. We assume that their firewall protects their workstations sufficiently. And this is why we have the answer to Question 4 above, w/ placement of an extra Firewall_2.

Topic 7: How to implement addressing for remote workstations using a VPN client.

The remote workstations have a modem adapter interface w/ the ISP public address & DNS.

These are used to create & maintain the tunnel to the concentrator. The remote workstations are given a logical VPN adapter once they hook up w/ the concentrator, which gives them a private address from LAN_a and LAN_a DNS that allows them to function as if they are at LAN_a. This assumes permitted flow of IP/Netbios from the LAN_a internal subnets through Firewall_a1 and through the VPN_a2 pipe.

Topic 8: How to have two classes of remote workstations, with one class only being able to access their Email remotely, and the other being able to access NT domains, Unix servers, SSH, Telnet, FTP, etc.

Based upon the remote workstation login to the concentrator, the "callers" are placed in one of two groups. Group 1 is given an address from a specific internal subnet that is given access to the Mail Server destination address for SMTP by Firewall_a1. Group 2 is given an address from a different internal subnet that allows them access to everything by Firewall_a1 via a corresponding access list.

2.3.2 IPSec Policy

An excellent document in this area is Cisco's, IOS Security Configuration Guide, and in particular, the IP Security and Encryption chapter.

IPSec can provide confidentiality, data integrity and data authentication between participating peers at the network layer.

2.3.2.1 Selection of security protocols AH & ESP

AH is a security protocol which provides data authentication and optional anti replay services. ESP is a security protocol which provides data privacy services and optional data authentication and anti replay services. ESP encapsulates the data it protects whereas AH is embedded in the data. Data authentication includes data integrity (verification that the data has not been altered), and data origin authentication (verification that the data was actually sent by the claimed sender).

We note that the sequencing of the AH header generation in relation to NAT is crucial. If it precedes NAT then it breaks it, since NAT will change the source address causing the security check at the destination to fail and the packet to be discarded. On the other hand, the authentication provided by ESP is limited compared to AH, because ESP authentication does not cover IP headers.

We therefore conclude that we will only use ESP for the Partner VPN's and AH & ESP for the GIAC staff remote access. We also note that data origin authentication in a LAN to LAN configuration provides no assurance as to the actual person using the VPN.

2.3.2.2 Selection of Key Exchange Parameters

IKE is a hybrid protocol that provides authentication of the IPSec peers, negotiates IPSec security associations and establishes IPSec keys. When IKE is used the security associations have an expiration period, whereas if IKE is not used and security associations are manually established, they don't have an expiration period.

We choose to implement IKE due to the increased security of expiration periods and that anti-replay services will be available.

We select the following options for the five IKE parameters:[5]

Encryption algorithm: 3des for Partners (multiple year protection), des for GIAC staff (multiple day protection). Since GIAC staff will be implementing encryption through SW, the response time will be less impacted by the lesser standard.

Hash algorithm: We will use the default, SHA-1

Authentication method: We will use preshared keys, since we don't have control over the Partners and this represents the most universal solution.

Diffie-Hellman group identifier: We will use the more secure 1024 bit Diffie Hellman option.

Lifetime of the Security Association: We choose the default of one day (86,400) seconds for Partners, and 1 hour (3,600) for GIAC staff. .

2.3.2.3 Other Considerations

We consider the length of time the contents need to be secure, since this will determine the needed encryption strength. We conclude that the information needs to be secured for several years, which results in our selection of 168 bit 3-DES. This in turn leads to the selection of Cisco's Hardware encryption component, the VPN Access Module **VAM**, to meet the additional processing demand.

We concur with the Cisco recommendation to use mirror images at peer IPSec devices to eliminate the logical complexities, and will adopt this with GIAC Partners.

We note and concur with the Cisco admonition to not use the **any** keyword to specify source or destination addresses.

We see no benefit to using the **set security-association level per-host** command since it results in additional resources. Thus at each Partner location all the workstations will

[5] Configuring Internet Key Exchange Security Protocol: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fipsenc/scfike.htm

share the same SA.

We note the need for implementation of Dynamic Crypto Maps for the GIAC staff remote access since they will be assigned dynamic IP addresses by their ISP. The GIAC VPN's authenticating IKE will utilize a fully qualified domain name rather than a source IP address.

2.3.2.4 Split Tunneling

Split Tunneling is discussed in the following excerpt from a Cisco document. At GIAC, the Mode Config command will be used to disable this functionality for Remote GIAC staff. It is not possible to do this for the Partner desktops since they are using LAN to LAN VPN connectivity, so we rely upon the Partner's environment to provide the necessary security.

> **Split Tunneling.** Split tunneling gives the user simultaneous access to the corporate network via an encrypted tunnel and to the Internet via a cleartext tunnel directly from the client PC. The Mode Config feature enables split tunneling by delivering two IP filters to the client, specifying one for the encrypted tunnel and the other for the clear text one. The decision to allow or deny this feature is a tradeoff between scalability and security. Without split tunneling, users must access the Internet through the encrypted VPN tunnel to the corporate network and out the corporate Internet gateway, using valuable network resources. With split tunneling, administrators have less traffic coming into the corporate network for greater scalability, but increase their exposure to hacker penetration through the clear text tunnel.[6]

The conclusion "Without split tunneling, users must access the Internet through the encrypted VPN tunnel to the corporate network and out the corporate Internet gateway, using valuable network resources", is not necessarily correct. For example, the compromised User's desktop may be able to open a connection with a remote controlling system over GIAC's Internet line. The safest course would be to disallow Internet access to GIAC remote Users.

2.3.2.5 The configuration in detail

The configuration for a Partner IPSec follows:

[6] http://www.cisco.com/warp/public/784/packet/oct00/p68-cover.html

```
!
!               Enable IKE
crypto isakmp enable
!
!               Configure the IKE parameters
crypto isakmp policy 1
  encryption 3des
  hash sha
  authentication pre-share
  group 2
  lifetime 86400
exit
!
!               Define which traffic to protect
no access-list 101
access-list 101 permit ip Partner-net 192.168.100.0 0.0.0.255 200.1.1.3 0.0.0.254
!
!               Define how the traffic will be protected
crypto ipsec transform-set myset1 esp-des esp-sha
!
!               Join the IPSec access list and transform wet
crypto map toPartner 10 ipsec-isakmp
match address 101
set transform-set myset1
set peer 192.168.100.10
!
!               Apply to interface
interface serial0
ip address 100.1.1.3
crypto map toPartner
```

The differences for configuration of GIAC staff IPSec includes the following:

```
encryption des
lifetime 3600
etc.
```

Assignment 3:1 Audit Your Security Architecture

3.1 Strategy Determination

We initially search for a PIX simulation / configuration analysis S/W package that takes the configuration file as input and generates a report indicating the Rulebase openings in an orderly fashion as well as an evaluation of the Firewalls hardening strength and some obvious misconfigurations such as rules that will never be executed.

Although our search did not turn up any such product, we feel it's only a matter of time before one becomes available.[7] In any event, we proceed with the traditional approach of ensuring the Firewall itself is secure, the Policies are correct and the Rulebase implements the policies correctly.

We note the distinction that the Firewall functions as a Router and listens on the typical ports a Router does and not the ports that the devices it protects do. Thus a Firewall **listens** on very few Ports, such as SSH for remote control and possibly SNMP for remote management. The Firewall **allows** many Ports through by first examining its routing table to see where to forward the packets and then executing the Firewall functionality of determining whether or not to allow the forwarding to occur.

To simplify & focus our task we will obtain and utilize all relevant documentation from GIAC Enterprises, including the Policy Matrix, Network Architecture diagram, IP addressing document, and Router & Firewall configurations.

3.1.1 How to Audit the Firewall Host characteristics

We will utilize the Score Checklist below to evaluate the Firewall host characteristics. The process will include a walk-through exam, determining who has access and why, when, how, and what recording tools are in place and when & how often the procedures are checked. We will include a review of the Firewall's backup procedure, fault tolerance design, avoidance of single points of failure, SW upgrade methodology, using standard networking criteria.[8]

[7] By an impressive coincidence(!), the Center for Internet Security just released such a product for Cisco routers: http://www.cisecurity.org/bench_cisco.html.

[8] http://www.cisecurity.org/bench_cisco.html

No.	Description	Score (Hi, Med, Lo)	Comments
100	**Physical Security**		
110	Defines controls on placement & use of console & other direct access port connections.		
120	…	`	
200	**Static Config Security**		
210	Designates procedures and limits on use of automated remote management and monitoring facilities (e.g. SNMP).		
220	…		
300	**Dynamic Config Security**		
310	Identifies the routing protocols to be used, and the security features to be employed on each.		
320	…		
400	**Network Service Security**		
410	Describes security procedures and roles for interactions with external service providers and maintenance technicians.		
420	…		
500	**Compromise Response**		
510	Defines response procedures, authorities, and objectives for response after a successful attack against the network.		
520	…		

We will verify that the most recent releases and hot patches are installed on the PIX firewall, by issuing the ***write terminal*** command and correlating the response to the Vendor product information..

We will conduct a Host Scan against the Firewall to see what ports it's listening to. A more sophisticated scanner may have a fingerprinting capability to identify the version of the O/S and also confirm the latest Service Pack and Hot Patches, but we have already taken care of this by the "Write Terminal" command above. In any event, our Scanner requirements are minimal with the essential ingredient being execution of the scan from **every interface**. We choose an evaluation copy of the commercial scanner Retina, since it won the Network World Fusion Blue Ribbon Award in February 2002[9].

[9] The article evaluates more than twenty commercial & freeware scanners, including NMAP & NESSUS;

We consider conducting a DoS attack against the firewall w/ Nessus, but a review of sights shows that the present version has corrected previous vulnerabilities.

3.1.2 How to Audit the Policies

We will utilize the Policy Matrix to scrutinize the inter-policy relationships and rule correctness.

The Matrix format is:

Rule #	What Detailed	Protocol	Source IP Address (Interface-Host or Segment)	Destination IP Address (Interface-Host or Segment)	Source TCP Port(s)	Dest TCP Port(s)	Source UDP Port(s)	Dest UDP Port(s)
1	Access GLF to purchase / provide / bulk obtain fortune sayings, review order status, transaction histories & create reports.	HTTP, HTTPS	Outside- Any Inside- Any	DMZ - Web Servers	any	80, 443	na	na
2	Authentication, authorization, accounting, administration using Netegrity Site Minder	Custom: Siteminder	DMZ- Web Servers	nside- Netegrity Site Minder	any	52441-52444	na	na

3.1.3 How to Audit the Ruleset

The ruleset portion of the audit considers whether the Firewall meets the organizations policies as specified in the Policy Matrix.

We assume that the PIX configuration is working in the sense that desired traffic is allowed through or the Users would complain. **The Ruleset audit is being conducted to see if larger than necessary openings exist.**

www.nwfusion.com/cgi-bin/mailto/x.cgi.

We will do this by selecting a scanning product that efficiently & effectively exercises the Firewall for openings. The list of tools is large and varies in many ways, including:

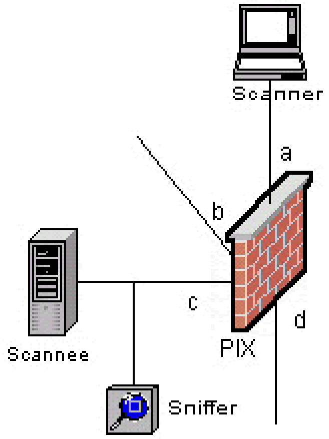
- **Price** – Commercial and freeware products abound
- **Suitability** – Products vary as to which platform their product is designed to analyze. Some are well suited for OS checking with their Vulnerability Data Base with a distinction between specific OSs, others for Applications such as IIS and Apache, CGI scripts, etc. What we need is a scanner that is designed to check PIX as a host (version, patch, etc.), and PIX as a Firewall (checks the Rulebase).
- **Automation** – Some tools are well suited for single hole testing, others for entire IP and Port range testing.
- **Intrusiveness** – Some tools are more invasive & may result in a DoS condition.
- **User friendliness** – GUI is always nice, but not if it means sacrificing functionality.
- **Thoroughness** – A Firewall tool requires the ability to vary the Source IP address and Port to simulate conditions that result in differential handling by the Firewall. Host tools don't need this functionality.
- **Effectiveness** – Minimal false positives and false negatives.
- **Reporting** – It is essential that the results are suitably prioritized and organized.
- **Etc**.

The fact that a scanner identifies N thousand vulnerabilities is of passing interest since we are focused on vulnerabilities specific to the PIX from the two dissimilar perspectives of its functionality as a Host and Firewall.

3.1.3.1 Approach Considerations

The accepted methodology for auditing a Firewall involves the issuance of a stimulus by Device A (Scanner) through Device B (Firewall) to Device C (Scannee) to see whether the stimulus is filtered or allowed through by the firewall.[10] A Lab environment might be constructed as shown, with the Sniffer possibly being located inside the Scannee: The combinatorics quickly get out of hand, for we need to test the Scannee from every one of the other interfaces, then repeat as we move the Scannee through the remaining interfaces. For a firewall with n interfaces the number of combinations is n(n-1), or for the four shown below, 12.

[10] An outstanding paper by Lance Spitzner, December 12, 2000, is "Auditing Your Firewall Setup": www.enteract.com/~lspitz/audit.html.



<u>filter on Source</u> addresses and Source TCP and UDP ports as well as ICMP, we need a Scanner that is capable of automatically cycling through the ranges we request.

The necessity of this was demonstrated during the Execution Phase of our Audit (see graphic in the Execution section below). When the Scanner address was not that of the device allowed to SSH to the Firewall, the opening was not found. To verify the SSH opening it was necessary to change the Scanner TCP/IP stack to the required IP address, a totally unworkable scheme when testing for unnecessary openings rather than confirming required ones.

The requirement for Source ranges is not discussed in any of the tool documents, with the exception of NMAP, which provides a –g option to vary the Source address, but not Port. A script will be required to provide the desired automated range functionality.

The lack of alternating Source fields reflects the immaturity of the industry for auditing Firewall rulesets. The conclusion is reinforced by the lack of a Responding Scannee program to facilitate the process, as mentioned below.

3.1.3.1.1 Response recognition

To verify the Firewall functionality based on its ability to filter on Destination addresses and Destination TCP and UDP ports as well as ICMP we need to determine **whether the Scannee needs to respond** to the stimulus for the outcome to be known, or whether a Sniffer needs to be involved. A Sniffer solution is undesirable since it does not lend itself to automation, which is an essential requirement for testing the millions of possibilities involved.

In a Lab environment we have the luxury of placing a Responding Scannee configured to respond to a range of IP addresses and TCP, UDP and ICMP packets. The IP addresses may be handled by multi-netting or a S/W module that listens to and responds to a configurable range of addresses by utilizing the Network Interface Card's (NIC's) promiscuous mode.

A program with some of these features is PortSentry, as mentioned in an earlier practical.[11]

In a Production environment we can't utilize the Responding Scannee approach so we need to understand the numerous scan options available through utilities such as NESSUS, HPING2, NETCAT, etc.

The NMAP options below, are discussed and annotated in yellow to indicate the relevance to our objective of mapping the Firewall Ruleset (**are the messages allowed through**) rather than what ports are open on the Scannee. The calculated "certainty" percentages are correct for the 100%'s, but simplistic guesses for those less.

3.1.3.1.2 Scan Types

-sT **TCP scan.** This option issues a TCP connect() command. If the Scannee port is listening it responds with an accept() message. This response has a **100% certainty** that a rule to **allow** for this specific Source & Destination IP address & port is in place: (An accept message can only mean that the firewall port allows the Scanners message through (For the Source IP address & Port and Destination IP address & Port)). A lack of response has a **50% certainty** that a rule to **drop** for this specific Source & Destination IP address & port is in place. (No reply may mean that the firewall filtered the message, **or** that the Scannee was not listening / up).

-sS **TCP SYN scan.** The Scanner sends a SYN packet. A SYN/ACK indicates the port is listening. A RST indicates a non listening port. Either of these 2 responses has a **100% certainty** that a rule to **allow** this specific Source & Destination IP address &

[11] Alan_Moe_GCFW

port is in place: Both responses require a Scannee with a functioning TCP/IP stack. In addition, the scan requires that the Scannee network did not recognize the scan and drop it by intent. A lack of response has a **50% certainty** that a rule to **drop** this specific Source & Destination IP address & port is in place. (No response can mean that the firewall filtered the message, **or** that the Scannee was not listening / up).

-sF sX sN Stealth FIN, Xmas Tree, or Null scan.

-sR **RPC scan.**

-sA **ACK scan**. This advanced method is used to map out firewall rulesets by sending an ACK message. **0% certainty** since **Stateful firewalls such as PIX** or Checkpoint-1 will drop the out of sequence handshake message.

-sU **UDP scan.** A 0 byte UDP packet is went to each port on the Scannee. If an ICMP "port unreachable" message is received, then the port is closed. This response has a **100% certainty** that a rule to **allow** for this specific Source & Destination IP address & port is in place. (This response requires a Scannee with a functioning TCP/Ip stack). A lack of response has a **33% certainty** that a rule to **drop** this specific Source & Destination IP address & port is in place. (No response can mean that the firewall filtered the message, **or** that the Scannee was not up, **or** that the Firewall has ICMP filtered out).

3.1.3.1.3 Completeness

Many firewalls are configured to deny / drop traffic with no response (i.e. no RST packet or ICMP error message). This means that the scans will take longer as the scanner does not get immediate feedback, but rather has to timeout on **blocked** ports.

The danger with conclusions based on lack of response is that we may conclude that a filter is in place when its not, and when a new device is brought up it is vulnerable. A sniffer can resolve the uncertainty but is very labor intensive.

If we limit the audit with language that the conclusions **only apply to the present configuration** we have a workaround for the uncertainty. For example, the TCP SYN scan becomes 100% conclusive as to whether there is a rule in place to drop traffic or allow it for the specific Source & Destination IP address & port. Any response means the rule is to allow, and lack of response means the rule is to drop.

So our strategy becomes to run an automated TCP SYN scan as follows:

```
For Source IP address A {range A1 to An}
  For Source TCP port B {range 1 to 65,536}
    For Destination IP address C {range C1 to Cn}
      For Destination TCP port D {range 1 to 65,536}
        Send a TCP SYN message
             If we get a SYN/ACK or RST,
               Source address & port AB to Dest address & port CD, Firewall is open.
             If we timeout,
               AB to CD Firewall drops (or Scannee is not listening / up)
```

The result reports have to merge adjoining responses into ranges for comprehension. Thus, rather than the following 100 statements:

AB to CD
AB to C(D+1)
AB to C(D+2)
…
AB to C(D+100)

We want to see just 1 statement:

Source {IP A, Port B} to Destination {IP C, Ports D to D+100} are open

Better yet will be a statement that identifies the interfaces as well for ease of comprehension

Source {Interface-VPN, IP A, Port B} to Destination {Interface-DMZ, IP C, Ports D to D+100} are open.

If we want to improve on the **completeness** of the audit, we can leave a Scannee in the Production interface side being scanned, and configure the Scannee to respond to all IP addresses not in use by Production equipment. This will allow us to **totally map** the Firewall Ruleset. The process will proceed relatively rapidly since there will not be any response timeout associated delays.

We compare the Retina scan program with Superscan in conducting the same scan of a Host. Retina is seen to be 30 times faster, but upon closer examination is seen to default to testing 1,400 probable Ports rather than the full 65,000. Based on our incomplete knowledge, our initial conclusion is that the Retina approach is not appropriate for detecting vulnerabilities associated w/ programs that use random ports.

3.1.3.2 Time Considerations

Although the iterative approach mentioned above would be complete, it is unrealistic in terms of the time involved, so we need to make some exclusionary decisions.

In order to **save time**, the strategy in a Production environment will be to place the Scanner on the Scannee segment and do a quick IP scan to see which IP addresses and Ports are up. Then use that list to create the Target Scannee list on the Scanner, and place the Scanner on the other side of the Firewall. The results as to the Firewall ruleset will be 100% conclusive with respect to the Production devices that are up and the whole process will be much faster due to the avoidance of timeout associated delays.

If we further want to improve on the time involved, we can prioretize the testing based on likelihood of finding a vulnerability. For example, since **all** traffic is allowed from greater security level interfaces to less, we don't have to check that this is indeed the case. Rather, we only need to confirm that the traffic **explicitly denied is indeed denied**.

Even with this simplification, the time to confirm lack of traffic from interfaces with a lesser security level to greater would extend into multiple days. Simplifying assumptions will have to be developed specific to each interface based on a review of the PIX configuration file. For example, the Outside to DMZ path will need to be scrutinized heavily. The VPN & Outside interfaces will have one or few addresses to scrutinize and thus greatly simplify the process.

Some excellent suggestions for improving the timing on NMAP and NESSUS scans are available from a study at the University of Missouri. [12]

- UDP scans are slow. However an unauthorized remote control program such as Subseven likes to hide out on an arbitrary UDP port. Doing an NMAP scan of all 65536 UDP ports may take as little as 2 minutes on a Windows system or 11 hours on a Solaris system due to RFC 1812 error-reply rate-limiting.
- If you are testing against a firewall doing TCP scans can take a while as well.
- Scanning 1 port on 10,000 computers can be faster than scanning 10,000 ports on one computer.
- Configure the timeout value for NESSUS as a function of the network speed. For fast networks change it from 15 seconds to 5.
- A NESSUS server can handle simultaneous tests of multiple hosts.
- Use multiple computers to speed throughput. Try NMAP one port on many

[12] http://bengal.missouri.edu/~johnsong/audit/audit_files/frame.htm

comuters simultaneously rather than many ports on one computer.
- Avoid diminishing returns. Some tests consume much more time that others, but rarely find a host with this vulnerability. (Since we concerned about the Firewall rather than the Host, we can't make this assumption in the event a variable Port program may take advantage of an opening).

3.1.3.3 Risk Considerations

With respect to the risks involved, the same Missouri study recommends:

- Enabling of the "safe check" option on Nessus, which results in banners being used to identify vulnerabilities rather than exploiting real flaws. (Since we are testing the Firewall ruleset, testing the actual vulnerability is unnecessary).
- NMAP and especially NESSUS can freeze scanning targets and require restarting.
- Scanning multiple targets through one network device can slow that subnet's performance. (In our case may create a DoS attack on the Firewall).

With the above in mind we adopt a strategy of spreading the audit over multiple days, with scanning done during off hours with someone ready to restart systems.

So, we conclude that this will be our strategy. Since we have substantially simplified things, we need a less versatile scanner than NMAP, and will use our familiar Retina product. The addressing ranges will also be available from the documentation we have reviewed and we can verify as we go along.

3.1.4 Costs, Effort

The audit will be done by SecCheck Professional Services, with an eventual shift to in house personnel as the necessary skill levels are acquired.

The cost will be impacted by how well prepared GIAC Enterprises is for the Audit. For example, if the documents we require are available and correct, our task will be much more predictable. These include the Policy Matrix, Network Architecture diagram, IP addressing document, Router & Firewall configurations. In the alternative, preparation of these documents can be viewed as a one time cost. In any event, our cost determination excludes the cost of obtaining current documentation.

Our account manager / sales engineer obtains and forwards the necessary documents to our senior consultant. The two work jointly in preparing the following proposal:

Activity	Skill (Daily Pay Rate)	Duration (Days)	Cost

Review GIAC network & firewall documents & develop strategy	$ 2,400	2	$ 4,800
Execute Audit	$ 1,200	4	$ 4,800
Evaluate Results	$ 1,600	2	$ 3,200
Make Recommendations	$ 2,400	1	$ 2,400
Total			**$ 15,200**

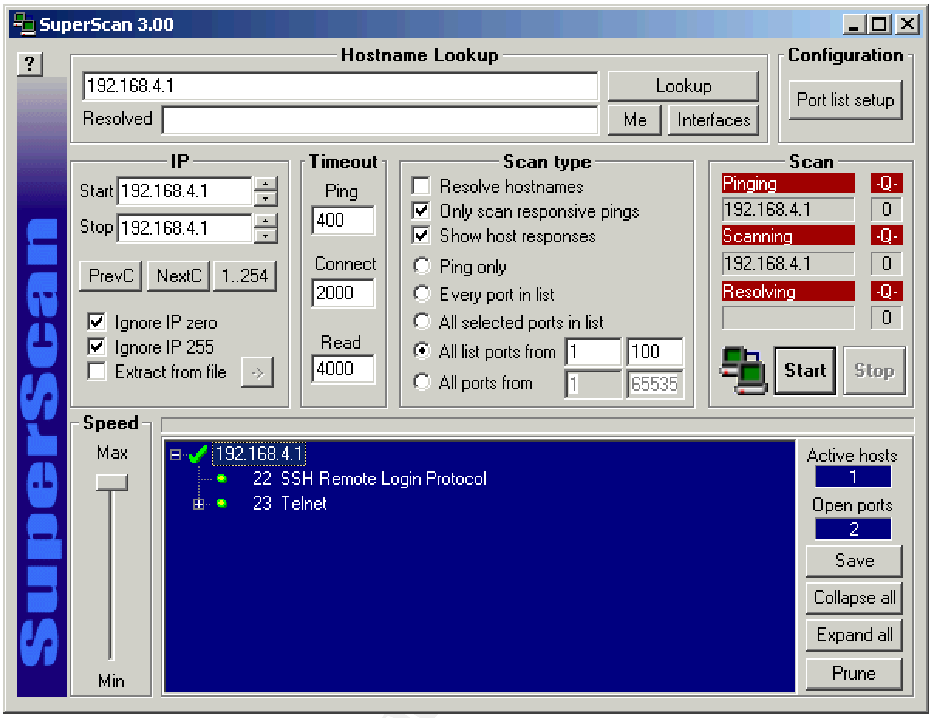
3.2 Execution

3.2.1 Execution of Firewall Host Audit

We determine the Software version:

```
pixfirewall> enable
Password:
pixfirewall# write terminal
Building configuration...
: Saved
:
PIX Version 6.1(1)
```

We see that the only open port is SSH and only from the Internal network, consistent with our expectations, shown below (The Telnet port was opened by us explicitly to allow debugging & was removed upon completion). We confirm that no TCP ports were open from the DMZ interface, nor the Outside interface.



SuperScan 3.00

Hostname Lookup: 192.168.4.1
Resolved:

IP
Start 192.168.4.1
Stop 192.168.4.1
☑ Ignore IP zero
☑ Ignore IP 255
□ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
□ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
● All list ports from 1 100
○ All ports from 1 65535

Scan
Pinging 192.168.4.1 0
Scanning 192.168.4.1 0
Resolving 0

192.168.4.1
22 SSH Remote Login Protocol
23 Telnet

Active hosts 1
Open ports 2

We obtain the following information from execution of a WHOIS query:

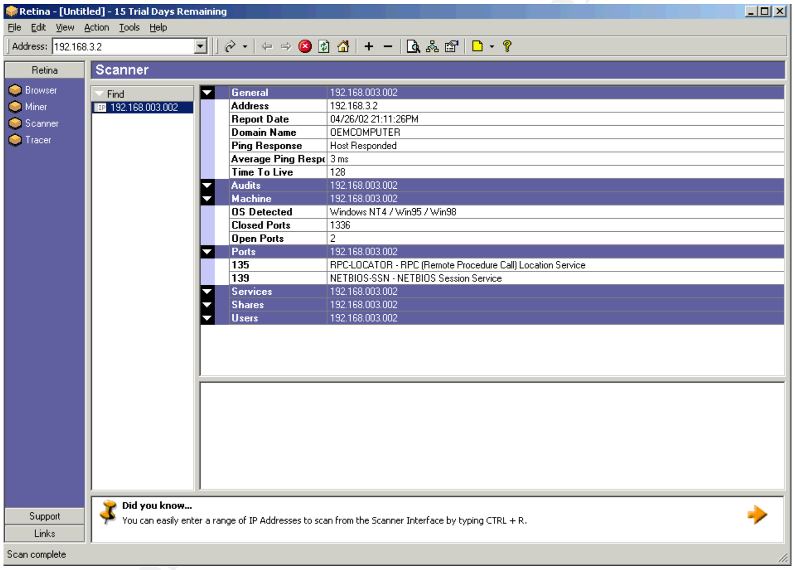
Administrative Contact:
Jones, Gail gaijon@GIAC.COM
GIAC Corporation
GIAC Plaza
Seattle, WA 98185
310-545-3195 (FAX) 310-545-3414
Technical Contact:
VanCorbach, Jerry jevanc@GIAC.COM
GIAC Insurance
4333 Brooklyn Ave N E
Seattle, WA 98185
310-545-5315 (FAX) 310-545-3414
Billing Contact:
Dann, Coni condan@GIAC.COM
GIAC Insurance Companies
GIAC Plaza
Seattle, WA 98185
(310) 545-6429

3.2.2 Execution of Firewall Policy Audit

This is discussed in terms of the Policy Matrix. We see that many of the fields are incomplete and result in larger opening creations than necessary, as discussed in the Evaluation & Recommendation section.

3.2.3 Execution of Firewall Ruleset Audit

A screen shot for the Scannee utilizing Retina, is shown below. In the production environment, or with a Program to respond to **all** stimulus as with PortSentry (requires a Unix platform Scannee), we would obtain complete results as discussed earlier.



General	192.168.003.002
Address	192.168.3.2
Report Date	04/26/02 21:11:26PM
Domain Name	OEMCOMPUTER
Ping Response	Host Responded
Average Ping Respo	3 ms
Time To Live	128
Audits	192.168.003.002
Machine	192.168.003.002
OS Detected	Windows NT4 / Win95 / Win98
Closed Ports	1336
Open Ports	2
Ports	192.168.003.002
135	RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
139	NETBIOS-SSN - NETBIOS Session Service
Services	192.168.003.002
Shares	192.168.003.002
Users	192.168.003.002

Did you know...
You can easily enter a range of IP Addresses to scan from the Scanner Interface by typing CTRL + R.

Scan complete

3.3 Results Evaluation & Recommendations

3.3.1 Firewall (Host perspective) Recommendations

Implement changes to eliminate Scores of Lo from the Score Checklist. The only such item is the S/W Upgrade methodology requirement which does not identify a fallback mechanism nor an approach to maintain 24x7 availability. We recommend purchasing a spare Firewall for a Lab environment to achieve these objectives.

Implement the newly released version of PIX, 6.2(1)[13], subsequent to a 45 day waiting period to ensure stability as proven by other Cisco customers.

We see that the Netmeeting issues we discussed in the Security Policy section with the NAT / PAT solution in version 6.1 may be resolved with the new Software Feature in v6.2 entitled: Port Address Translation (PAT) for H.323 and SIP fixups.

The Host Scan indicated a very hardened profile with only SSH being open and only for the Interior segment and even then only for the Tech Staff address range.

The Whois query provided enough information to determine the naming convention for GIAC's Email system, which can lead to a targeted attack by social engineering or Email attachments with Trojans targeted to less sophisticated Users. We suggest elimination of this type of information from the Name Services.

[13] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/index.htm

3.3.2 Policy Audit Recommendations

We recommend that the Policy Matrix be expanded to incorporate functionality for the new VPN Remote Access Concentrator as mentioned in the next section entitled Architectural Recommendations to be used by GIAC Sales staff & Technical staff. Similarly for the additional Firewall shown in the diagram below.

We also recommend discussion of limiting download of Applets & Active-X browser script lets, executables, and limiting access to dangerous sites.

Rule #	What Detailed	Protocol	Source IP Address (Interface-Host or Segment)	Destination IP Address (Interface-Host or Segment)	Source TCP Port(s)	Dest TCP Port(s)	Source UDP Port(s)	Dest UDP Port(s)
1	Download executables that run under Browser control (e.g. applets, active x)		Secure area employeeds Could be at proxy	Internet				
2	Download potentially harmful executables (e.g. program files) Enforce Certs from trusted vendors?		Secure area employeeds Could be at proxy	Internet				
3	Download files presumed safe (e.g. Adobe Acrobat,) Have to decompress files to evaluate (zip,).		Secure area employeeds Could be at proxy	Internet				
4	Browse Internet, except certain URIs	HTTP, HTTPS, SSL	Secure area employeeds Could be at proxy	Internet				
5	Limit Remote Access by Sales Staff to Email	SMTP	VPN2-Sales Segment	Internal-Mail Server		SMTP	na	na
6	Allow Remote Access by Tech Staff to Email	All	VPN2-Tech Segment	All	all	all	na	na
7	Allow Syslog out from App Server to Log Server	Syslog	Internal-App Server	Internal-Log Server	-	-	-	514
8	Deny all access from App Server to the Inside Network except SYSLOG	All	Internal-App Server	All	-	-	-	-

3.3.3 Ruleset Audit Recommendations

Since our efforts to ping from a Higher Security interface to a lower were unsuccessful, we needed to implement dynamic NAT to meet the PIX requirement for insuring security. The actual implementation required the following commands:

```
nat (inside) 3 0 0
global (dmz) 3 192.168.3.32-192.168.3.254
```

We recommend tightening the opening to only allow hosts from the Tech Staff segment 172.16.100.0 into the DMZ.

We recommend Increasing the level of logging to the maximum possible.

```
Logging buffered debugging
```

We suggest that as GIAC technical staff configure several laptops w/ Linux, NMAP, NESSUS, Responding Scannee S/W modules, etc. for conducting their own audits in the future.

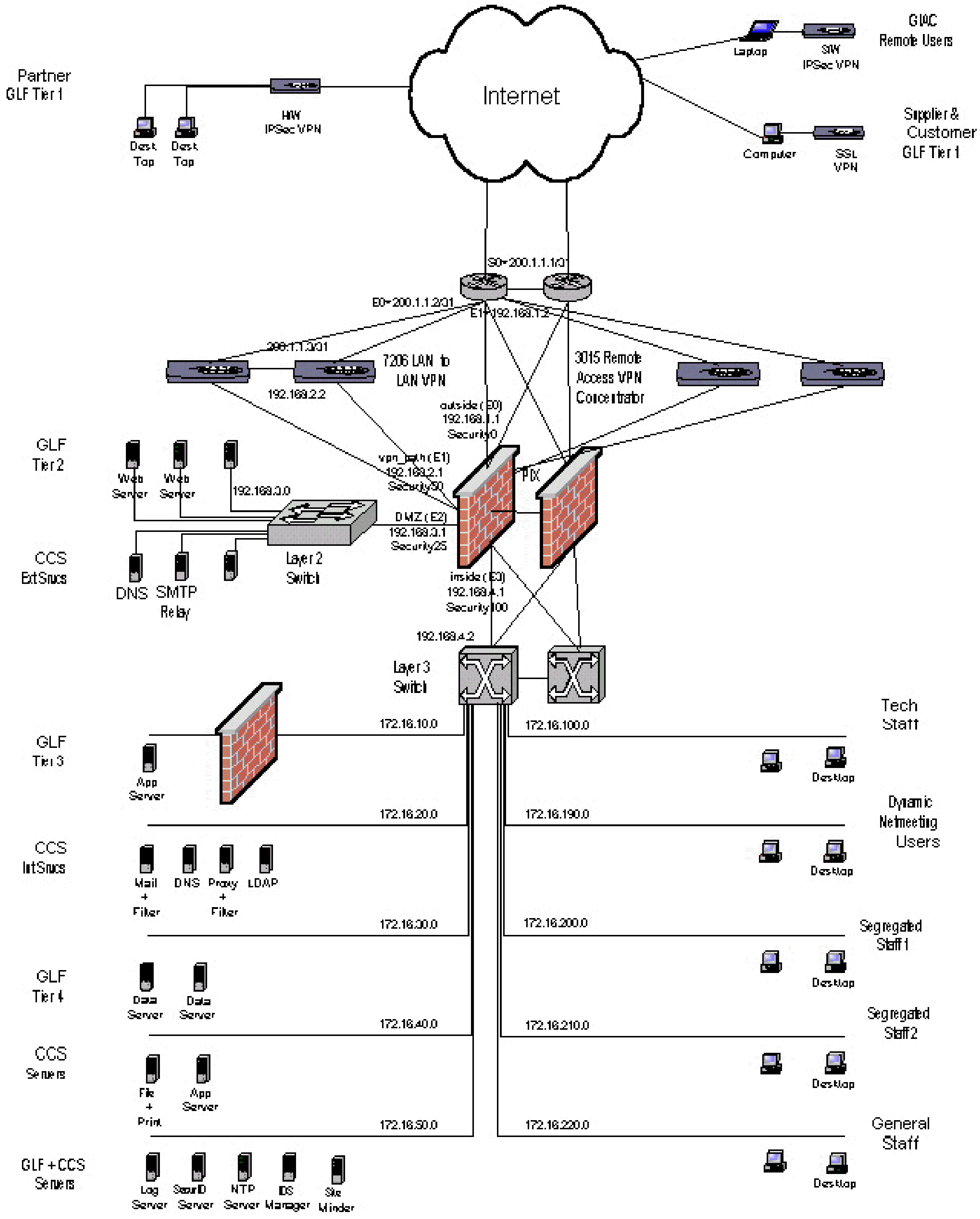
3.3.4 Architectural Recommendations

We point out the risk that the Telnet access that GIAC partners have to the App Server may be used as an attack point into our protected network. This may occur due to an unscrupulous Partner employee or someone that has infiltrated the Partner's site.

We therefore recommend the use of a packet filter firewall in front of the application server to disallow outbound Telnet sessions. The implementation would occur in the Layer 3 switch, rather than through the additional device shown. An alternative might be to deactivate Telnet initiation at the Server while keeping telnet reception. Another is to install a personal firewall on the server itself. A detection and corrective approach rather than preventative could be to implement a Network IDS probe on the application server segment.

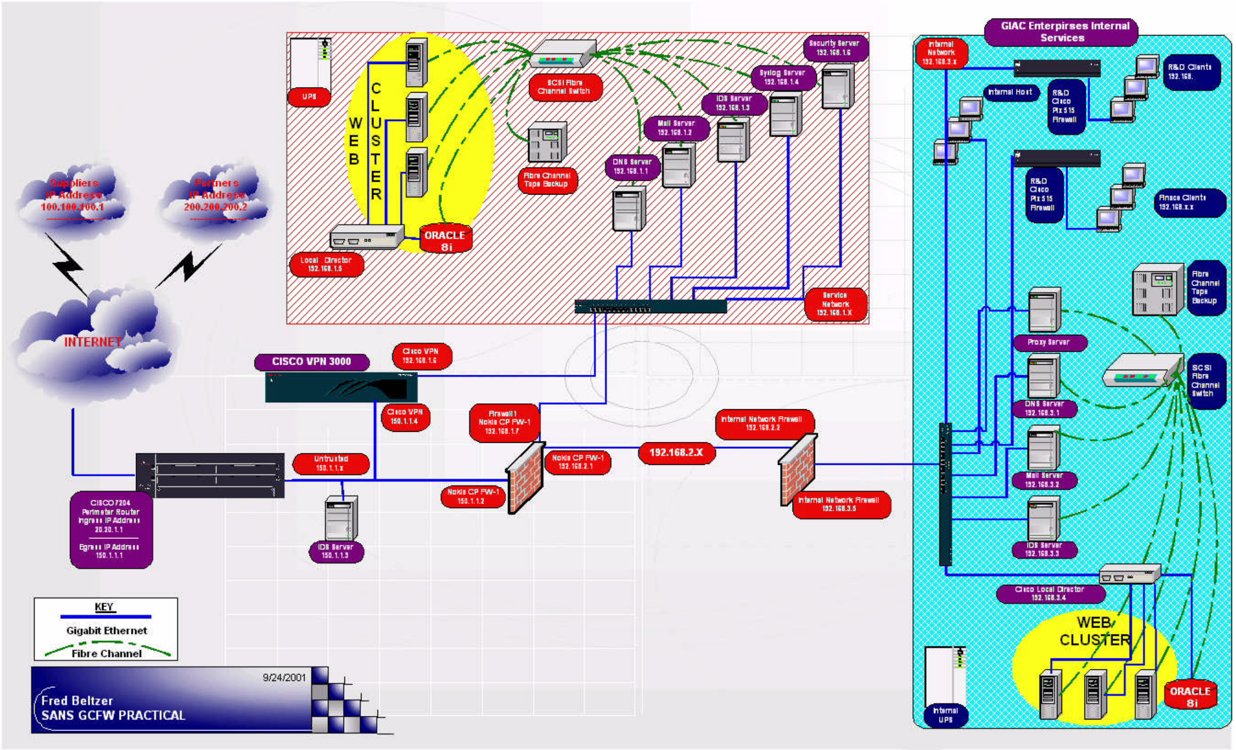
We also concerned that although the 7206 IOS VPN solution is well suited for LAN to LAN VPN's, it is missing key functionality available through the Cisco 3000 series Remote Access VPN Concentrator. This may include an inability to enforce policies for personal firewalls at the remote workstations such as not allowing split horizon modes of operations. We also favor the Concentrator approach because of its ability to scale to a greater extent for concurrent User sessions.

Further recommendations are for elimination of Single Points of Failure, as shown in the diagram below.


Internet
GIAC
Remote Users
Laptop
SW
IPSec VPN
Supplier &
Customer
GLF Tier 1
Computer
SSL
VPN
Partner
GLF Tier 1
Desk
Top
Desk
Top
HW
IPSec VPN
S0-200.1.1.1/31
E0-200.1.1.2/31
E1-192.168.1.2
200.1.1.3/31
7206 LAN to
LAN VPN
192.168.2.2
3015 Remote
Access VPN
Concentrator
outside (E0)
192.168.1.1
Security0
vpn_path (E1)
192.168.2.1
Security50
PIX
DMZ (E2)
192.168.3.1
Security25
inside (E3)
192.168.4.1
Security100
192.168.4.2
GLF
Tier 2
Web
Server
Web
Server
192.168.3.0
CCS
ExtSrvcs
DNS
SMTP
Relay
Layer 2
Switch
Layer 3
Switch
GLF
Tier 3
App
Server
172.16.10.0
172.16.100.0
Tech
Staff
Desktop
172.16.20.0
172.16.190.0
Dynamic
Netmeeting
Users
Desktop
CCS
IntSrvcs
Mail
+
Filter
DNS
Proxy
+
Filter
LDAP
172.16.30.0
172.16.200.0
Segregated
Staff 1
Desktop
GLF
Tier 4
Data
Server
Data
Server
172.16.40.0
172.16.210.0
Segregated
Staff 2
Desktop
CCS
Servers
File
+
Print
App
Server
172.16.50.0
172.16.220.0
General
Staff
Desktop
GLF + CCS
Servers
Log
Server
SecurID
Server
NTP
Server
IDS
Manager
Site
Minder

Assignment 4:1 Design Under Fire

With the objective of gaining expertise with the two major firewall products, we decide to look for a practical that utilizes Checkpoint's Firewall-1 and thus complement our selection of PIX as the dominant firewall in our design. Our other criteria are for currency (and consequent relevance) and recognition for excellence (based on high scores). This leads us to Mr. Beltzer's recent paper and the graphic shown below, which we will refer to as the Target Installation from here on.[14]


UPS
WEB CLUSTER
SCSI Fibre Channel Switch
Fibre Channel Tape Backup
Security Server 192.168.1.6
Syslog Server 192.168.1.4
IDS Server 192.168.1.3
Mail Server 192.168.1.2
DNS Server 192.168.1.1
ORACLE 8i
Local Director 192.168.1.5
Service Network 192.168.1.X
Suppliers IP Address 100.100.100.1
Partners IP Address 200.200.200.2
INTERNET
CISCO VPN 3000
Cisco VPN 192.168.1.6
Cisco VPN 150.1.1.4
Firewall1 Nokia CP FW-1 192.168.1.7
Untrusted 150.1.1.x
Nokia CP FW-1 192.168.2.1
Nokia CP FW-1 150.1.1.2
192.168.2.X
Internal Network Firewall 192.168.2.2
Internal Network Firewall 192.168.3.5
CISCO7204 Perimeter Router Ingress IP Address 20.20.1.1
Egress IP Address 150.1.1.1
IDS Server 150.1.1.3
KEY
Gigabit Ethernet
Fibre Channel
9/24/2001
Fred Beltzer
SANS GCFW PRACTICAL
GIAC Enterpirses Internal Services
Internal Network 192.168.3.x
Internal Host
R&D Cisco Pix 515 Firewall
R&D Clients 192.168.
R&D Cisco Pix 515 Firewall
Finace Clients 192.168.x.x
Fibre Channel Tape Backup
Proxy Server
SCSI Fibre Channel Switch
DNS Server 192.168.3.1
Mail Server 192.168.3.2
IDS Server 192.168.3.3
Cisco Local Director 192.168.3.4
WEB CLUSTER
ORACLE 8i
Internal UPS

4.1 An Attack that Results in a Firewall Compromise

We assume that v5.1(3) of Checkpoint's Firewall-1 and v3.4.1 of Nokia's IPSO O/S are

[14] The original paper is at http://www.giac.org/practical/Fred_Beltzer_GCFW.zip.

installed since they were current at the time of the practical submission.

4.1.1 Determine the Vulnerabilities

Our approach is to look for weaknesses by evaluating subsequent Firewall-1 releases that contain security fixes rather than functional enhancements. This is followed by a check for O/S fixes that also pertain to security rather than functionality. A review of Firewall-1 E-mail focus groups is then conducted, with a final pass being made in examining sites that may have discovered a vulnerability that Checkpoint has not yet provided a fix for.

4.1.1.1 Checkpoint Acknowledged Vulnerabilities

Of the 13 issues and their associated fixes posted by Checkpoint in the Alerts Archive for Firewall-1, six pertain to versions greater than the Target Installation of v5.1(3).[15] The latest release for Firewall-1 is v4.1 SP5a, dated February 5, 2002. SP6 is available for non Nokia H/W-O/S platforms.

February 22, 2002 - HTTP Connect Commands
February 14, 2002 - SNMP Alert
October 25, 2001 - RDP Communication Issue
September 19, 2001 - GUI Buffer Overflow
July 11, 2001 - (Updated September 13, 2001) - Format Strings Vulnerability
July 9, 2001 - (Updated February 12, 2002) - RDP Communication Vulnerability

A review of the vulnerabilities indicates that (3) results in decreased functionality with no compromise in security, and (4) and (5) only apply to internal threats. Vulnerabilities (1), (2) and (6) are copied below for closer analysis.

Vulnerability 1: HTTP Connect Commands – February 22, 2002 [16]

Check Point Statement on use of HTTP Connect commands:

As noted in the original posting, no escalation of privilege is granted via the use of HTTP Connect commands with FireWall-1 HTTP security server; that is, connections via the HTTP security server are blocked unless specified in the rule base. Therefore, a properly constructed rule base mitigates the effect of this malicious use of a valid function of an HTTP proxy.

[15] The Checkpoint list of vulnerabilities for Firewall-1 are at http://www.checkpoint.com/techsupport/alerts/.

[16] The HTTP alert is presented at http://www.checkpoint.com/techsupport/alerts/http_connect.html.

> Check Point is taking action to give administrators enhanced control of this type of connection, and will offer that improved functionality in the next product update.

The language **"… this malicious use of a valid function of an HTTP proxy"** is unclear but makes us want to know more. We note that the statement "… will offer that improved functionality in the next product update" implies the present work around is to disable the HTTP proxy service.

We will look to the Email focus group discussions for greater insight.

> **Vulnerability 2: SNMP Alert** – February 14, 2002 [17]
>
> Recently, an automated suite was released which tests products for known SNMP vulnerabilities.
>
> Check Point knows of no SNMP-related security issues in any of its products, and has conducted an extensive review to ensure that none exist. SNMP communication is not required for correct functionality of any Check Point products.
>
> FireWall-1, by default, blocks all SNMP communication to, from, or across a FireWall-1 gateway. The SNMP service is disabled by default, and SNMP communication is enabled only if the administrator writes a specific rule which allows the communication.
>
> If SNMP monitoring of Check Point firewalls or internal networks is needed, Check Point recommends that the FireWall-1 rule base tightly restrict SNMP communication.

The language "…knows of no SNMP-related security issues … has conducted an extensive review to ensure that none exist" persuades us to not pursue this vulnerability any further.

> **Vulnerability 6: RDP Communication Vulnerability** - Addendum - July 12, 2001 - Updated February 12, 2002 [18]
>
> Summary: Check Point uses a proprietary protocol called RDP (UDP/259) for

[17] The SNMP alert is presented at http://www.checkpoint.com/techsupport/alerts/snmp_alert.html.

[18] The RDP alert is presented at http://www.checkpoint.com/techsupport/alerts/rdp.html.

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 hotfix 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 5 and install the SP5 hotfix, then install a policy. This hotfix 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 hotfix: RDP communication is blocked by default.

Download information:

1) For AIX, HPUX, Linux, Solaris, Windows NT & Windows 2000 select the following options from the Software Subscription Download Site:
   a) Product: VPN-1/ FireWall-1 or Provider-1
   b) Version: 4.1
   c) Operating System: [Appropriate OS]
   d) Encryption: [VPN+Des or VPN+Strong]
   e) SP/Patch Level: SP5
2) For IPSO 3.4 select the following options from the Software Subscription Download Site:
   a) Product: Nokia IP Series Appliance
   b) Version: 4.1
   c) Operating System: IPSO 3.4
   d) Encryption: [VPN+Des or VPN+Strong]
   e) SP/Patch Level: SP5

Addendum - July 12, 2001 RDP Bypass workaround for VPN-1/FireWall 4.1 SP

RDP communication may be blocked in VPN-1/FireWall-1 versions 4.1 and 4.1 without applying the security hotfix by the applying the INSPECT changes below to the management station. No changes need to be applied to the modules themselves. The files referenced below may be found in $FWDIR/lib/. Please make sure all management GUIs are closed before editing the files. After editing the files, install a policy to push the changes to the modules.

Known Limitations: Please note these changes will disable FWZ encryption, MEP resolution and automatic interface resolving (automatically determining closest interface for remote VPN connections to gateways with multiple interfaces). Blocking RDP on edge routers will achieve the same results, with the same limitations. The files referenced below may be found in $FWDIR/lib/. Please make sure all management GUIs are closed before editing the files. After editing the files, install a policy to push the changes to the modules.

For 4.1: Comment (or remove) the following line in base.def; comments begin with the symbol "/*" (omitting quotes) and conclude with the symbol "*/" (omitting quotes).

```
/*accept_fw1_rdp;*/
```

Acknowledgement: This issue was reported by Jochen Bauer and Boris Wesslowski of Inside Security GmbH, Stuttgart, Germany.

The language **"… could be used in some circumstances to establish a surreptitious communication channel"** for vulnerability (6) is also unclear. However, it's not surprising that the product vendor will not tell the world how to hack into their own product. Once again, we will look at the Email focus groups and hacker sites for greater insight.

4.1.1.2 Nokia O/S Acknowledged Vulnerabilities

Nokia provides several Hardware models for Checkpoint's Firewall-1. The Nokia operating systems, called IPSO, is a hardened Unix offering, with the present version being 3.4.2.[19] Little information is available from this Vendor's site, except for an incompatibility issue with v3.4.x that caused Checkpoint to pull their image for short term period.

4.1.1.2.1 Email Focus Group Discussed Vulnerabilities

A search with Google.com identifies a public forum Email group at SecurePoint called CheckPoint FireWall-1 that creates more than ten thousand messages per year.[20] We

[19] The Nokia web site requires a support contract for access to technical information. http://www.nokia.com/securenetworksolutions/nokia.html

[20] This current / archive depository of Emails is open to the public and offers excellent search capabilities:

continue with our strategy to determine whether we can benefit from the two Checkpoint vulnerabilities.

4.1.1.2.2 Research the RDP Vulnerability

The first few hits from the search engine for the Checkpoint RDP fix are as follows:

82% **RE: [FW1] FW: CERT Advisory CA-2001-17** (gjuppunov@bofasecurities.com) - Thu, 12 Jul 2001 17:36:42 GMT
76% **Untitled** (pradeepv@emirates.com) - Tue, 17 Jul 2001 05:25:38 GMT
76% **[FW1] CERT Advisory CA-2001-17** (oaviles@cosapisoft.com.pe) - Tue, 10 Jul 2001 22:00:55 GMT
76% **[FW1] Check Point FireWall-1 RDP Bypass Vulnerability** (JonasT@guld.spray.se) - Wed, 11 Jul 2001 06:00:56 GMT
76% **RE: [FW1] CERT Advisory CA-2001-17 Check Point RDP Bypass Vulnerability** (pradeepa@infy.com) - Thu, 12 Jul 2001

A review of the conversations shows this reasoned insight from George Juppunov:[21]

> … The exposure is not as much the gateway as the networks or hosts behind it. In other words, if you target a host in your internal network on port 259 (or vice versa) Firewall-1 would by default pass the packet whether or not you have a rule that allows the communication path. In other words, if I plug an executable in your WWW server on the DMZ, I would be able to communicate with the outside (i.e. my battle station) whether or not you are allowing your WWW server to establish outbound connections.
>
> To some extent, the implications of the vulnerability relate more to your containment strategy than to your exposure. Although I cannot speak for NT environments, in the Unix world, in order to bind a lower port you need to execute your program with root's uid. For all intents and purposes, at this point it's game over. Once an intruder has acquired unauthorized access to a host, containment is a little e bit trickier, i.e. you don't want him to publish your customers' passwords on the web. In this respect not having this surreptitious path allowed might help, although even then it's a moot point. A good hacker, and most of them a pretty good, could easily find let's say your mailhub's IP address (probably a host on the DMZ), either exploit the mailhub, or spoof the IP address and open a feed back connection on port 25. Your firewall will be more than happy to allow that etc. etc.

http://msgs.securepoint.com/fw1/. The archive goes back several years.

[21] Goerge Juppunov's Email is at http://msgs.securepoint.com/cgi-bin/get/fw1-0107/268.html.

> I'm not suggesting you ignore the vulnerability, but don't lose your sleep over it yet. Make sure your Inet exposed hosts are secured, and your IDS sensors tuned up; take your security audits seriously and keep your rules tight.

The question now becomes whether the RDP vulnerability applies to the Targeted Installation. A search for the key word RDP in the Practical does not result in a match, so we conclude that the following language by Checkpoint is controlling:

> 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.

Since the Targeted Installation combines VPN and Firewall functionality in the same server, it may be safe to assume that the default condition of allowing RDP packets through has shifted to becoming a required one.

We conclude that this vulnerability exists and will be useful once we've compromised one or more of the internal systems.

4.1.1.2.3 Research the HTTP vulnerability

The first few hits from the search engine for the Checkpoint HTTP fix are as follows:

94% **Re: [FW-1] HTTP Proxy Security Hole!!!** (volker.tanger@DISCON.DE) - Tue, 19 Feb 2002 15:52:58 GMT
94% **Re: [FW-1] HTTP Proxy Security Hole!!!** (volker.tanger@DISCON.DE) - Tue, 19 Feb 2002 14:51:14 GMT
94% **Re: [FW-1] HTTP Proxy Security Hole!!!** (gfraize@GENUITY.NET) - Thu, 21 Feb 2002 18:53:53 GMT
94% **Re: [FW-1] HTTP Proxy Security Hole!!!** (Amin@EPLUS.COM) - Tue, 19 Feb 2002 16:50:53 GMT
94% **Re: [FW-1] HTTP Proxy Security Hole!!!** (don@BLACKSUN.ORG) - Tue, 19 Feb 2002 15:21:24 GMT

The dialogue sounds promising so we place the key excerpts below and identify separate responses through distinct colors.

> **Try this on your firewall if you are running HTTP Proxy! Checkpoint has yet to release a fix.**
>
> **Step one: telnet to a machine behind the checkpoint firewall on port 80 (it can**

be a fake machine that doesn't exist, as long as the name resolves)

Step two: Type the following:

- **CONNECT mailserver.somecompany.com:25 / HTTP/1.0**
- **User-Agent: eeep**
- **Cache-Control: private,no-cache**
- **Pragma: no-cache**

Step three: wait a moment for your SMTP banner to pop up.

You can then send SPAM email, and it looks like it came from your firewall. I also found out that one can telnet to machines on a network that are protected by the Firewall.

I also found out that one can telnet to machines on a network that are protected by the Firewall.

I just tested and confirmed for FW1 V4.1 SP5 (plus hotfixes). Even worse: you can connect to any TCP port on any machine the firewall can connect to. Telnet, SMTP, POP, etc.

I've tested this on CP4.1 SP4 and SP5(no hot fix's) and I can not re-produce this enture bug/feature.

If my rule read: Src: any Dst: 1.1.1.1 Service: http security server, tunnle enalbe, with a *:* in the host path, I can only connect to the 1.1.1.1 host on any port....I can not connect to any host on any port. It seems I can only connect to the hosts that are in the dst field. If I update the dst to be 1.1.1.1 and 2.2.2.2, I can connec to both 1.1.1.1 and 2.2.2.2 on any port. If I change the dst to any, I can connect to any host on any port.

I would like to re-produce this, so if you can reply to this list, and directly to me, with the exact hotfix, that would be great!

The last author's inability to confirm the vulnerability dampens our mood of success, however, Checkpoint's alert language "…this malicious use of a valid function of an HTTP proxy… will offer improved functionality in the product update" continues to motivate us.

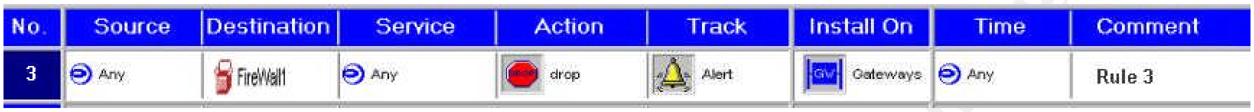
Since we still don't quite understand the vulnerability, we search the securepoint (bugtraq) archives & get a similar Email from Volker Tangent as in the securityfocus archives, except that an example is included. It is not obvious if Volker wrote to two Email forums, or one of them edited the contents of his Email. In any event, this clarifying Email follows:[22]

The question now becomes whether the HTTP vulnerability applies to the Targeted Installation. Here are some of the possibilities:

We see that Firewall-1 Rule 3 below, drops all traffic to the firewall, (including HTTP), but

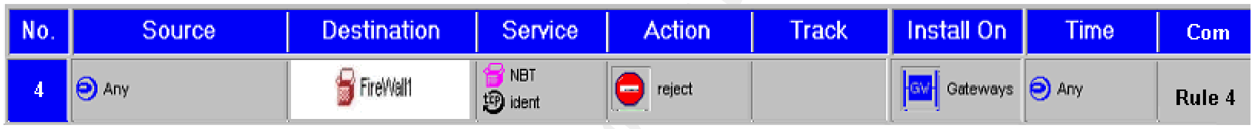
[22] Voker Tanger's clarifying Email is at http://online.securityfocus.com/archive/1/257016.

the vulnerability is for the HTTP proxy allowing HTTP traffic through, so it has no bearing.



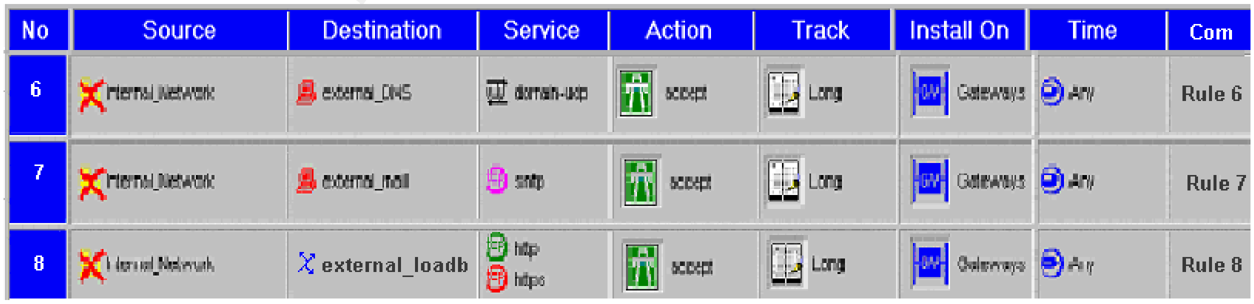
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
3	Any	FireWall1	Any	drop	Alert	Gateways	Any	Rule 3

We note that Firewall-1 rule 4 below, is out of sequence in that it will never be executed, & needs to be placed prior to rule 3. In any event, this error is of no obvious value to us. It does pose the question of why Firewall-1 does not verify rule sequencing to create error messages in situations such as this.



No.	Source	Destination	Service	Action	Track	Install On	Time	Com
4	Any	FireWall1	NBT ident	reject		Gateways	Any	Rule 4

We see that Firewall-1 rule 8 below, allows all HTTP traffic to the Web Server segment, which allows the vulnerability to occur (we think), subject to the ability of authenticating to the targeted service (e.g. Telnet to the Web Server disguised as HTTP protocol 80) through the necessary User ID and password.



No	Source	Destination	Service	Action	Track	Install On	Time	Com
6	Internal_Network	external_DNS	domain-udp	accept	Long	Gateways	Any	Rule 6
7	Internal_Network	external_mail	smtp	accept	Long	Gateways	Any	Rule 7
8	Internal_Network	external_loadb	http https	accept	Long	Gateways	Any	Rule 8

4.1.2 Conduct the Attack

We now visit UCLA and use one of the publicly available workstations to iteratively telnet through several remote campus sites and mount an attack. The first step is to verify the RDP vulnerability so that we may send information stolen from DMZ serves to a hidden directory at a University remote compromised server. The second step is to use the HTTP vulnerability to access DMZ web servers via Telnet and then infiltrate them with the installation of monitoring packages that steal transaction information and send it to us via the RDP tunnel. If the application security controls prove too difficult, we try to alter / destroy file contents by obtaining root or administrative privileges. An alternative approach may be to Telnet to the DNS server & change its configuration to allow cash poisoning, or zone transfers.

In determining other possible vulnerabilities in the Targeted Installation design we consider:

1) Presence, or lack of, control of Active-X downloads, Java applets, which can allow Trojans into the internal network.
2) Presence, or lack of, containment at the Targeted Installation accessed server in the event of VPN partner compromise.
3) Presence, or lack of, Email virus checking, which opens the door for Trojans to be brought into the internal network.
4) Presence, or lack of, FTP to internal network lack of controls, which can allow download of Trojans into the internal network.
5) Proper placement, or not, of the Log Server, to a secure portion of the network.
6) Presence, or lack of, controls to prohibit / screen download of executables, which can allow Trojans into the internal network.

4.1.3 Countermeasures to the Attack

The RDP vulnerability is fixed by SP5, so a timely installation will resolve things. In the alternative, the Border Router may be configured to filter out RDP messages. It is also possible to deactivate the service on the firewall itself & still maintain functionality.

The HTTP vulnerability has no fix, so we configure the Firewall-1 to disable HTTP tunneling, remove the wildcard "other" from matching CONNECT, and replace all rules containing the service HTTP+Resource w/ plain HTTP. [23]

4.2 An Attack that Results in a Denial of Service (DoS)

4.2.1 Distinguishing between Network and Service DoS

A Denial of Service (DoS) attack makes a **service** or **network** unavailable by exhausting its resources or making it fail. A **network** DoS has a greater impact because it compromises **every** service behind the network link.

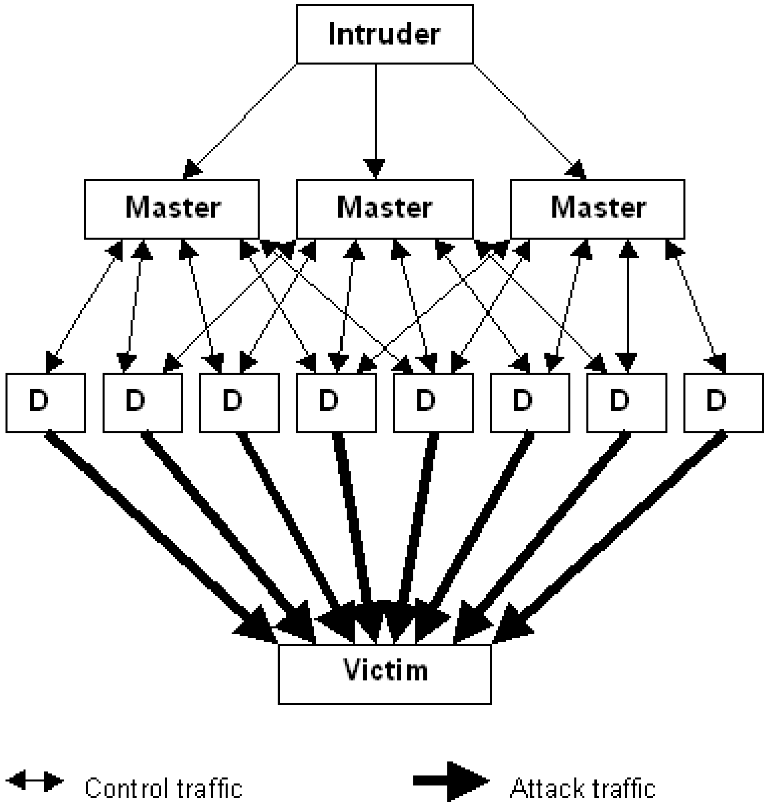
A more sophisticated implementation of DoS is a Distributed Denial of Service (DDoS) which utilizes multiple systems to attack a victim in a coordinated fashion.[24]

The typical DDoS configuration involves an Intruder who controls a small number of Masters, which in turn control a large number of Daemons. The Daemons are used to launch attacks against Victims targeted by the Intruder.[25] The indirection provided by this multi-layered approach protects the Intruder's identity.

[23] http://msgs.securepoint.com/cgi-bin/get/fw1-0202/583/1/2.html

[24] A January 2001 review of the evolution of DDoS attacks is available in Brooke Paul's article: http://www.networkcomputing.com/1201/1201f1c1.html

[25] A December 1999 paper that is still very relevant is "Results of the Distributed-Systems Intruder Tools Workshop" by CERT, at: http://www.cert.org/reports/dsit_workshop-final.html



4.2.2 Determine the Vulnerabilities

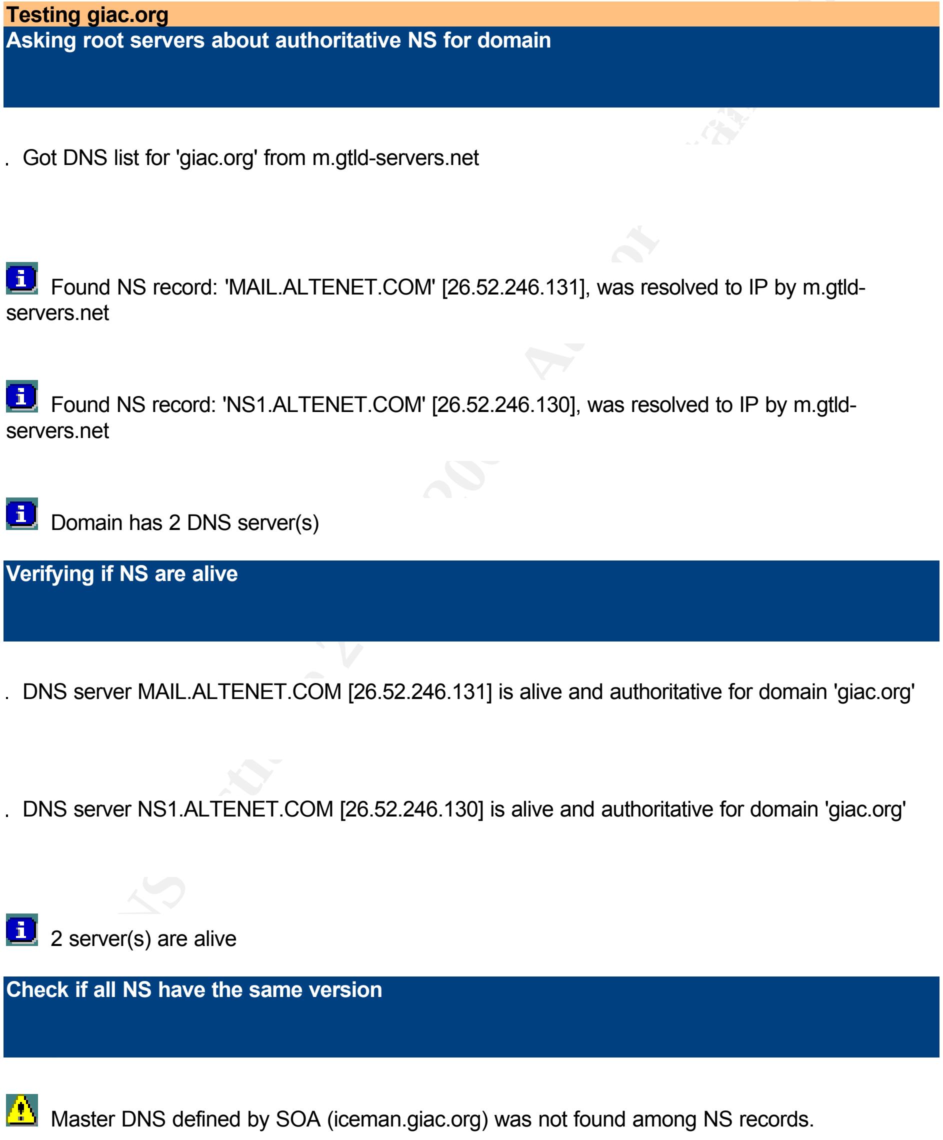
The subsequent section in this paper, entitled Countermeasures to the Attack, mentions several potential solutions, which are not present in the Targeted Installation. We therefore believe that any of the half dozen DDoS attack programs readily available will succeed.

We elect the latest version of the Stacheldraht attack program because it encrypts intruder-to-master TCP sessions & has an auto-update feature.[26]

[26] A December 1999 detailed analysis by David Dittrich of the early releases of Stacheldraht is at: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

4.2.3 Conduct the Attack

We select as the Victim servers the target's Web and DNS servers and obtain their IP addresses through a tool to test DNS zone hosting, mail and web servers called CheckDNS.[27]



Testing giac.org

Asking root servers about authoritative NS for domain

. Got DNS list for 'giac.org' from m.gtld-servers.net

ℹ Found NS record: 'MAIL.ALTENET.COM' [26.52.246.131], was resolved to IP by m.gtld-servers.net

ℹ Found NS record: 'NS1.ALTENET.COM' [26.52.246.130], was resolved to IP by m.gtld-servers.net

ℹ Domain has 2 DNS server(s)

Verifying if NS are alive

. DNS server MAIL.ALTENET.COM [26.52.246.131] is alive and authoritative for domain 'giac.org'

. DNS server NS1.ALTENET.COM [26.52.246.130] is alive and authoritative for domain 'giac.org'

ℹ 2 server(s) are alive

Check if all NS have the same version

⚠ Master DNS defined by SOA (iceman.giac.org) was not found among NS records.

[27] The web site is http://www.checkdns.net

ℹ All 2 your servers have the same zone version (2002042004)

Checking www. Records

ℹ Checking http server www.giac.org [26.54.47.46]

ℹ HTTP server www.giac.org [26.54.47.46] answers on port 80

ℹ Received: HTTP/1.1 200 OK (Server: Apache) 113f . . .GIAC: Global Information Assurance Certification - Home Page. . . . .The SANS Institute.... ....Incidents.org.... ....SANS Reading Room.... ....SANS Forum.... ....Contact Us.... . . . .Global Information Assurance Certification.. ..The Indust

Check mail-servers

⚠ Domain giac.org has only one mail-server

ℹ Checking mail server (PRI=100) iceman.giac.org [26.52.247.3]

ℹ Mail server iceman.giac.org [26.52.247.3] answers on port 25

```
.  <<< 220 iceman.giac.org - Welcome to our SMTP server ESMTP

.  >>> HELO checkdns.uniplace.com

.  <<< 250 iceman.giac.org - Welcome to our SMTP server

.  >>> MAIL FROM: <dnscheck@uniplace.com>

.  <<< 250 ok
. >>> RCPT TO: <postmaster@giac.org>

. <<< 250 ok

. >>> QUIT
```

ℹ Mail server iceman.giac.org [26.52.247.3] accepts mail for giac.org

ℹ All MX are configured properly

A publicly available workstation at a busy & unregulated airport location is used to start a multi Telnet hop session to an Intruder so that a forensic investigation does not lead back to us. Assuming that we use Master & Daemon attack modules already installed in the 50 Cable / DSL systems and advertised at our favorite hacker site, this is a very safe & easy crime to execute. The commands related to the attack are:

```
!
!         Add IP addresses of DNS & Web servers to attack list
.madd 26.52.256.131:26.52.246.130:26.52.247.3:26.54.47.46
!
!         Use large ICMP & UDP packet sizes to reach the network unavailable objective
.setusize            1400
.setisize            1400
!
!         Set the range of ports for SYN flooding
.sprange 0-1023
!
!         Set timer for attack duration for 10 hours
.mtimer 36000
!
!         Start a flood attack consisting of mixed ICMP, UDP, SYN, TCP random flags & IP
headers.[28]
.mhavoc
```

Our DDoS attack could have been targeted at the ISP to GIAC link (**network**) or a particular device. For example, small SYN packets will exhaust Server resources rather

[28] A September 2000 analysis of new capabilities in later releases of Stacheldraht is at: http://www.iss.net/security_center/alerts/advise61.php

than network. We chose large packets since they exhaust the ISP to GIAC link and thus make **all** of the devices unavailable. The same global impact would be achieved if any Single Point of Failure device is brought down, such as the border router or firewall device.

4.2.4 Countermeasures to the attack

The key aspects to dealing w/ DDoS attacks are prevention, detection, notification and correction. This is best done through a policy of preparedness that includes selection of a competent ISP, training & the purchase of special S/W. In addition, good neighbor policies assure that our own systems cannot be compromised and used as DDoS daemons.

4.2.4.1 Network Targeted Solutions

Network DDoS attacks need to be stopped as close to the source as possible. When an Enterprise access link is exhausted, an ISP based solution is best, such as the one available from an Israeli company called WanWall.[29] Their product analyzes web based traffic for DDoS characteristics, terminates it, and identifies the source for further intervention and prosecution. It is designed for placement at strategic ISP peering points. DDoS characteristics involve a baseline, threshold tuning and signature recognitions.

Thus prevention from an Enterprise's perspective means selection of an ISP that implements such a solution for Network DDoS attacks and corresponding SLA contractual language.

A different approach that may work against current DDoS attack programs relies on the distinction that the attack programs use IP addresses to designate Victims whereas legitimate Users use DNS entries.[30] Thus if a new public address space is put into place subsequent to a successful network DDoS attack and pushed out to legitimate Users through an immediate DNS update, the DDoS attack will have been subverted. This is recognized as a short-term evasive maneuver since the attackers can do another Nslookup to determine the new IP addresses & redefine the target accordingly. In any event, the steps for an installation with two ISPs might be:

1) Disable ISP1 link
2) Change firewall Static NATs for public servers to ISP2 addresses (use a previously

[29] www.wanwall.com/solution

[30] This is seen in the Stacheldraht implementation discussed at http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

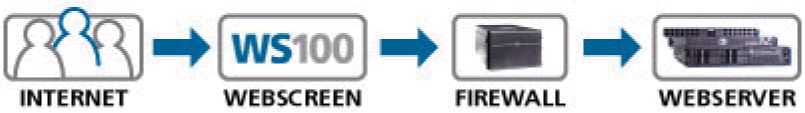
created and tested batch file)

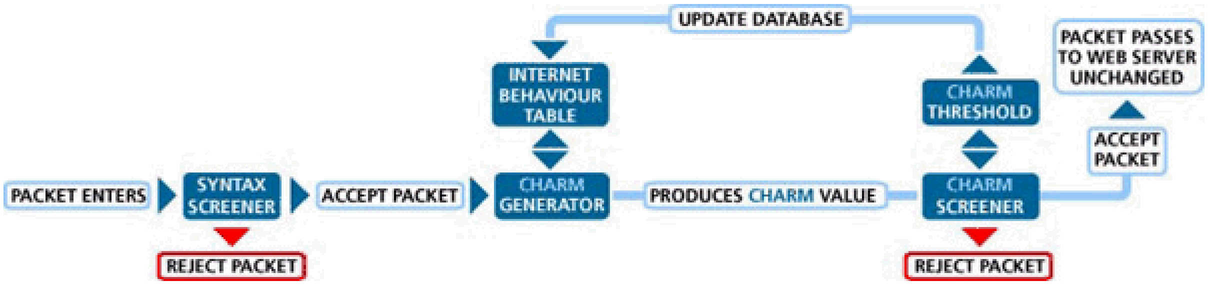
3) Bring up ISP2 link (the expense of having two ISPs can be ameliorated by usage based billing)
4) Push out new addresses through an immediate DNS update
5) Call ISP1 to investigate and contain source of attack
6) Have ISP1 give us a different public address space to fall back onto once ISP2 is compromised

Another possibility may be to push out the static NAT functionality to the ISP so that evasionary actions may be taken by them without inter organization communication delays. Or to implement IPv6 where QoS features provide further choices. We note that CERT suggests assuring out-of-band communications procedures with upstream operators or emergency response teams in the event of a debilitating attack. [31]

4.2.4.2 Service Targeted Solutions

DDoS attacks that target Services rather than Networks may be stopped more easily by placement of a defense device on the Enterprise network. Such a product is the WS100 device available from the British company, Webscreen.[32] The positioning of the product and a process flow diagram are shown below.





[31] http://www.cert.org/incident_notes/IN-99-07.html

[32] http://www.webscreen-technology.com/the_solution/solution.html

Real world experience will dictate the need for and practicality of such tools.[33] Certainly DDoS attacks are easy to execute and certainly the financial loss is non trivial. High profile attacks in the past three years against organizations such as Amazon.com, CNN.com, eBay and E-Trade have been calculated to result in multi billion dollar losses, although the accounting has been criticized as being excessive. Since the suggested solutions are new, independent evaluations by impartial entities such as Gartner, Meta, Forrester, or Network Computing will be of value.

As with all security related preventative actions a prioritization needs to be done based on exposure & likelihood. It is worth recognizing that the exposure increases as additional functionality is placed over the Internet link, which in the present case relates to the VPN traffic. In addition, in regulated industries such as finance or health, there may be a maximum period that services can be unavailable. For example, a multi day outage as that which occurred at E-Bay with the 1999 DDoS attack may be unacceptable in a bank environment.

[33] Additional DDoS products include: http://www.mazunetworks.com/index.html and http://www.captusnetworks.com/.

Appendix – Assignment 1 Security Architecture (15 points)

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

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

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

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

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

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

filtering routers;
firewalls;
VPNs to business partners.

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

internal firewalls (are internal firewalls appropriate for additional, layered protection; to segment internal networks…?);

secure remote access (is additional remote access required by administrators, salespeople, telecommuters…?).

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

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

Appendix – Assignment 2 Security Policy (35 points)

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

- Border Router
- Primary Firewall
- VPN

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

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

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

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

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

1. A general explanation of the syntax or format of the ACL, filter, or rule for your device.
2. A general description of each of the parts of the ACL, filter, or rule.
3. An general explanation of how to apply a given ACL, filter, or rule.
4. For each ACL, filter, or rule in your security policy, describe:
   - the service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.
   - Any relevant information about the behavior of the service or protocol on the network.
   - If the **order** of the rules is important, include an explanation of why certain rules must come before (or after) other rules.
5. Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

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

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

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

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

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

Appendix – Assignment 4 Design Under Fire (25 points)

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!
Select a network design from any previously posted GCFW practical (http://www.giac.org/GCFW.php) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Research and design two of the following three types of attacks against the architecture:

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

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

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

In designing your attacks, keep the following in mind:

- The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.
- The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should not assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)
- You **must** supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.
- The attack does not necessarily have to succeed (though a successful attack is often the more interesting approach). If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.