

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5e
July 2001

James R. LaPiedra

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

© SANS Institute 2000 - 2005 Author retains full rights.

Assignment 1 – Security Architecture

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

You must consider and define access for:

- *Customers (the companies that purchase bulk online fortunes):*
- *Suppliers (the authors of fortune cookie sayings that connect to supply fortunes):*
- *Partners (the international partners that translate and resell fortunes).*

Since GIAC Enterprises requires access for customers, suppliers, and partners, all with various business requirements, proper planning is required. The primary challenges of these business requirements is to establish secure communication channels for each of the users to access their resources and perform their transactions. The confidentiality, integrity, and availability of information on the network must be protected. This must include data that is stored or in transit. To accomplish this goal strong perimeter defenses must be deployed to control traffic. Although there are several methods utilized to secure an e-commerce business, I have chosen to segment the network for greater control of traffic and increased management capabilities. These segments are as follows:

Border Internet Segment

This segment is designed to establish a perimeter for commerce and public web servers. The router and firewall pairs serve as a means of defining what type of traffic is allowed in and out or the commerce.

The following is the specification for the Router and firewall interfaces:

Cisco Router Pair:

HSRP Interface = 165.68.70.1
RTR1:
Interface1 = ISP Specified
Interface2 = 165.68.70.3
RTR2:
Interface1 = ISP Specified
Interface2 = 167.68.70.4

Check Point FW-1 Pair:

© SANS Institute 2000 - 2005 Author retains full rights.

Check Point Firewall-1/Stonebeat V4.1 SP 3 operating on the Nokia IP650. This firewall pair serves as an access point to the infrastructure from the Internet for potential and existing customers. Additionally, the firewall will handle DNS and EMAIL traffic on the "Public Utility Segment".

Internet Segment: V-Lan 1
Virtual IP address Interface1 = 165.68.70.2
FW1 Interface1 = 165.68.70.5
FW2 Interface1 = 165.68.70.6

Commerce Segment: V-Lan 2
Virtual IP address Interface2 = 165.68.70.33
FW1 Interface2 = 165.68.70.34
FW2 Interface2 = 165.68.70.35

Public Utility Segment: V-LAN 3
Virtual IP address Interface3 = 165.68.70.65
FW1 Interface3 = 165.68.70.66
FW2 Interface3 = 165.68.70.67

Application / VPN Connectivity LAN: V-LAN 4
Virtual IP address Interface4 = 165.68.70.99
FW1 Interface4 = 165.68.70.97
FW2 Interface4 = 165.68.70.98

Commerce Segment:

VLAN 2: 165.68.70.32/27

The Commerce Segment consists of the devices required to conduct e-business by providing the user with a web interface to products and services. The customer can access a secure site via the standard SSL port 443 to conduct a transaction with the application layer of the network. Existing customers can use this segment to get access to fortunes without being tied down to a dial-up or VPN solution. New customers can securely establish accounts and conduct business.

Public Utility Segment:

VLAN 3: 165.68.70.64/27

The Public Utility Segment provides several areas of service required in a commerce site. Domain Name Service via a redundant pair of BIND name servers, an Internet E-mail gateway via a pair of Sendmail Servers, and a public web server cluster providing relevant information about the company, products, and services are all provided for on this segment.

The purpose of removing the components of the Public Utility Segment from the Commerce results in

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

enhanced security. Additional security comes from the ability to restrict the service ports allowed to and from the commerce site (via firewall rulebases) without concern for additional services such as Public DNS and SMTP. Such restrictions enhance security on the commerce segment and limit a potential attacker's exploit capability.

As an added benefit the speed of the response from both Commerce Segment and Public Utility Segments are enhanced. Users may access information about the company, Email can be routed, and Domain requests can be handled without infringing upon the capability to do business.

Application / VPN Connectivity LAN:

VLAN 4: 165.68.70.96/27

As the site is muti-purposed, so is the solution muti-functional. The Application / VPN Connectivity LAN is evidence of this design aspect. First, access to the fortune database is given to authorized users from the commerce segment through a finite set of firewall rules and defined application security procedures. Second, the segment provides for a route through the SUPPLIER/PARTNER VPN to the application and the fortune database for partners who want to obtain bulk fortunes for translation and resale.

A layered approach to providing commerce enhances the overall security by limiting the number of devices with which the application can be accessed (FW ACLs). The design of this segment demonstrates a functional layered technology deployment that protects products and customers from potential security threats.

A CISCO 3030 VPN Concentrator Bridges this LAN with a pair of Check Point FireWall-1 firewalls.

VPN Segment:

The purpose of this segment is to provide the suppliers and partners with high speed secure access to the site without compromising the security of the site. The network segment is split into two smaller subnets to preserve IP address space for security architecture considerations in protecting the VPN device, and to provide the capability to assign an address pool for VPN clients.

VLAN 5a: 165.68.70.128/28
VLAN 5b: 165.68.70.144/28

The VPN LAN segment is designed to provide the following functionality:

- Secure Remote Access
- Partner Connectivity
- Supplier Connectivity

The hardware components used in this segment are defined as follows:

Cisco Router Pair:

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

HSRP Interface = 165.68.70.129

RTR3:

Interface1 = ISP Specified
Interface2 = 165.68.70.131

RTR4:

Interface1 = ISP Specified
Interface2 = 167.68.70.132

Check Point VPN-1 FW-1 Pair:

Check Point Firewall/Stonebeat V4.1 SP 3 operating on the Sun Solaris 8. This firewall pair serves as an access point to the infrastructure from the VPN Internet connection for Suppliers to the segmented supplier application LAN, Partners to the fortune database, and remote users to the internal network. The IPSEC protocol is used to tunnel application protocols for authenticated users.

VPN Segment1 (Internet Side): V-LAN 5a
Virtual IP address Interface1 = 165.68.70.130
FW3 Interface1 = 165.68.70.133
FW4 Interface1 = 165.68.70.134

VPN Segment2: V-LAN 5b
Virtual IP address Interface2 = 165.68.70.145
FW3 Interface2 = 165.68.70.146
FW4 Interface2 = 165.68.70.147

CISCO 3030 VPN Concentrator:

This device provides a VPN solution for all users who require remote access to the site through the IPSEC protocol. The inner network is protected via the 28bit netmask established on a segregated firewall pair's virtual interface and Firewall ACLs. The ACLs restrict the traffic that is sent to it from the VPN Internet segment. Allowed traffic remains routed to the device through the firewall.

VPN Segment2: V-LAN 5b
Interface1 = 165.68.70.148

Application / VPN Connectivity LAN: V-LAN 4
Interface2 = 165.68.70.102

Supplier LAN Segment: V-LAN 6
Iterface3 = 165.68.70.161

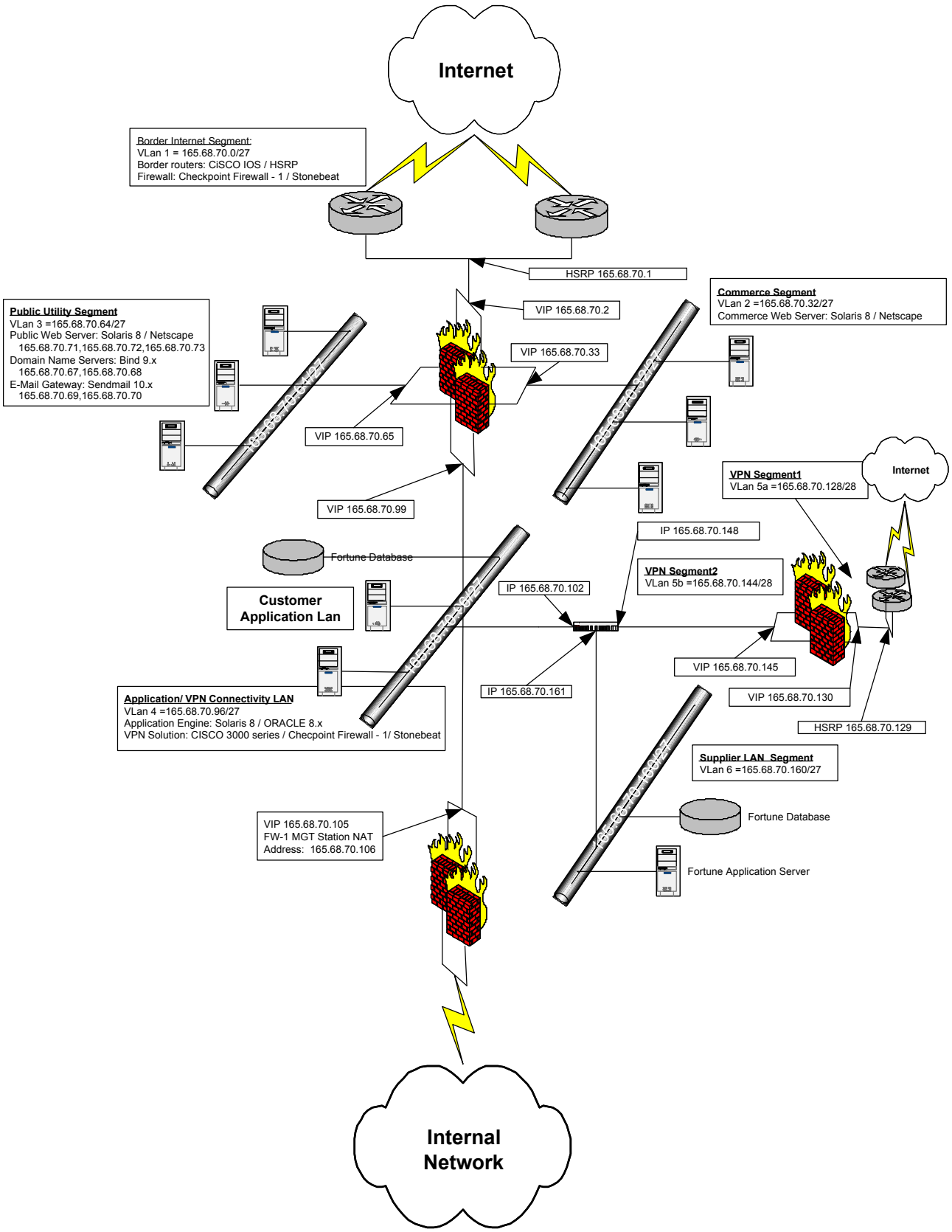
© SANS Institute 2000 - 2005, Author retains full rights.

Supplier LAN Segment:
VLAN 6 =165.68.70.160/27

This segment is designed strictly for fortune supplier access. Access is provided for suppliers through the VPN only. The fortune supplier application and a fortune database are housed on this LAN.

Security Architecture Diagram for GIAC Enterprises
Diagram view on following page.

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



© SANS Institute 2000 - 2005

Author retains full rights.

Assignment 2 – Security Policy

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

- *Border Router*
- *Primary Firewall*
- *VPN*

Perimeter Internet:

Router Filters RTR1 & RTR2:

- Routers are CISCO 3620 hardware using CISCO IOS 12.2. Service patches applied in a timely manner. Additional security is provided by the adherence of configuration guidelines recommended by SANS and the National Security Agency system guides located at: http://www.nsa.gov
- Rule ordering – each rule in each ACL is checked from the top down; when a match is encountered the specified action is applied to the packet. If matches are not found there is a default deny policy applied.
- All border routers have "Warning Banner" messages displayed to all incoming remotely accessible links.

RTR1 Configuration:

```
! ******************************************************************
! CSRT3620a.cfg - Cisco router configuration file
!   Thursday, July 19, 2001, 02:59:25 PM
!
! Hostname: CSRT3620a
! Model: 3620
! ******************************************************************
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service tcp-small-servers
no service udp-small-servers
no ip directed-broadcast     ! don't send out broadcasts
no ip proxy-arp   ! don't respond to arps
no ip unreachables     ! Don't send icmp for denied items in access-list.
ntp disable ! disable network time protocol for the router
!
hostname CSRT3620a
!
enable password ########
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
```

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

```
!
controller T1 0/0
!
interface FastEthernet 1/0
 no shutdown
 description connected to EthernetLAN
 ip address 165.68.70.3 255.255.255.224
 standby 1 ip 165.68.70.1
 standby 1 preempt
 standby 1 priority 110
 standby 1 authentication upfront
 standby 1 timers 5 15
 keepalive 10
!
ip classless
!
! Deny local subnet addresses:
!
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
!
! Deny packets with localhost, broadcast, multicast, and missing destination IPs
!
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny   ip host 0.0.0.0 any log
!
! Prevent spoofing. Deny incoming packets that have
! our internal address:
!
access-list 101 deny   ip  0.0.0.255 any log
!
! Allow smtp traffic to mail servers only:
!
access-list 101 permit tcp any host 165.68.69.69 eq smtp pop
access-list 101 permit tcp any host 165.68.70.70 eq smtp pop
!
! Allow incoming dns traffic to name servers only:
!
access-list 101 permit udp any host 165.68.70.67 eq domain
access-list 101 permit udp any host 165.68.70.68 eq domain
!
! Allow incoming HTTP, HTTPS to public and commerce web servers
!
access-list 101 permit tcp 255.255.255.255 0.0.0.0 165.68.70.32 0.0.0.32 eq http
access-list 101 permit tcp 255.255.255.255 0.0.0.0 165.68.70.32 0.0.0.32 eq https
access-list 101 permit tcp any host 165.68.70.71 eq http
access-list 101 permit tcp any host 165.68.70.72 eq http
access-list 101 permit tcp any host 165.68.70.73 eq http
!
! Log everything that does not meet the above rule set
!
access-list 101 deny   ip any any log
!
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
! End of access-list 101
!
! Beginning of access-list 102
!
! Only allow packets from our network.
!
access-list 102 permit ip 165.68.70.0 0.0.0.255 any
!
! Log everything else:
!
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any any log
!
! End of access-list 102
!
! Apply access list to external interface
!
ip access-group 101 in
ip access-group 102 out
!
ip accounting access-violations
!
! IP Static Routes
!
ip route 0.0.0.0 0.0.0.0 FastEthernet 1/0 1 permanent
no ip http server
!
snmp-server community ######## RO
snmp-server community ######## RW
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password ########
 login
!
end
```

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

RTR2 Configuration:

```
! ******************************************************************
! CSRT3620b.cfg - Cisco router configuration file
!   Thursday, July 19, 2001, 02:59:25 PM
!
! Hostname: CSRT3620b
! Model: 3620
! ******************************************************************
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service tcp-small-servers
no service udp-small-servers
no ip directed-broadcast     ! don't send out broadcasts
no ip proxy-arp  ! don't respond to arps
no ip unreachables     ! Don't send icmp for denied items in access-list.
ntp disable ! disable network time protocol for the router
!
hostname CSRT3620b
!
enable password ########
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
controller T1 0/0
!
interface FastEthernet 1/0
 no shutdown
 description connected to EthernetLAN
 ip address 165.68.70.4 255.255.255.224
! HSRP Configuration
 standby 1 ip 165.68.70.1
 standby 1 preempt
 standby 1 priority 110
 standby 1 authentication upfront
 standby 1 timers 5 15
 keepalive 10
!
ip classless
!
! Deny local subnet addresses:
!
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
!
! Deny packets with localhost, broadcast, multicast, and missing destination IPs
!
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 101 deny    ip 240.0.0.0 7.255.255.255 any log
```

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

```
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny   ip host 0.0.0.0 any log
!
! Prevent spoofing. Deny incoming packets that have
! our internal address:
!
access-list 101 deny   ip  0.0.0.255 any log
!
! Allow smtp traffic to mail servers only:
!
access-list 101 permit tcp any host 165.68.69.69 eq smtp pop
access-list 101 permit tcp any host 165.68.70.70 eq smtp pop
!
! Allow incoming dns traffic to name servers only:
!
access-list 101 permit udp any host 165.68.70.67 eq domain
access-list 101 permit udp any host 165.68.70.68 eq domain
!
! Allow incoming HTTP, HTTPS to public and commerce web servers
!
access-list 101 permit tcp 255.255.255.255 0.0.0.0 165.68.70.32 0.0.0.32 eq http
access-list 101 permit tcp 255.255.255.255 0.0.0.0 165.68.70.32 0.0.0.32 eq https
access-list 101 permit tcp any host 165.68.70.71 eq http
access-list 101 permit tcp any host 165.68.70.72 eq http
access-list 101 permit tcp any host 165.68.70.73 eq http
!
! Log everything that does not meet the above rule set
!
access-list 101 deny   ip any any log
!
! End of access-list 101
!
! Beginning of access-list 102
!
! Only allow packets from our network.
!
access-list 102 permit ip 165.68.70.0 0.0.0.255 any
!
! Log everything else:
!
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any any log
!
! End of access-list 102
!
! Apply access list to external interface
!
ip access-group 101 in
ip access-group 102 out
!
ip accounting access-violations
!
```

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

```
! IP Static Routes
!
ip route 0.0.0.0 0.0.0.0 FastEthernet 1/0 1 permanent
no ip http server
!
snmp-server community ######## RO
snmp-server community ######## RW
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password ########
 login
!
end
```

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

Check Point Firewall-1 Rules for FW1 & FW2:

Allow or Deny	Source Address(es) or Network(s)	Destination Address(es) or Network(s)	Protocol	Port	Service	Comment
A	ANY	165.68.70.67 165.68.70.68 165.68.70.69 165.68.70.70	ICMP		PING	Allow ping of DNS, SMTP
A	ANY	165.68.70.67 165.68.70.68	TCP,UDP	53	DNS	Domain Name Service
A	ANY	165.68.70.69 165.68.70.70	TCP	25	SMTP	Email Gateway
A	ANY	165.68.70.32/27 165.68.70.71 165.68.70.72 165.68.70.73	TCP	80	HTTP	
A	ANY	165.68.70.32/27	TCP	443	HTTPS	For secured commerce transactions
A	165.68.70.32/27	165.68.70.96/27	TCP	7575	Customer Fortune Application	See Footnote to table
A	165.68.70.106	165.68.70.99 165.68.70.98 165.68.70.97	TCP	22	SSH	For Local Management
A	165.68.70.106	165.68.70.99 165.68.70.98 165.68.70.97	TCP	257	FW1 Log	Firewall Logging
A	165.68.70.106	165.68.70.99 165.68.70.98 165.68.70.97	TCP	258	FW1 Management	Management from internal network via
D	ANY	ANY	ALL	ANY	ALL	Default deny just to be sure

***Note**: TCP 7575 is an arbitrary Customer fortune application service port for use between the Commerce Segment and Application Segment.

Rulebase Ordering (All firewalls) – packets are inspected from the top down. The firewall will compare the packets to every rule in order until it finds a rule that matches. The packet is applied to the first rule that applies. If no rule is found to match, the packet is denied by default.

Perimeter VPN:

Router Filters RTR3 & RTR4:

- Routers are CISCO 3620 hardware using CISCO IOS 12.2.

RTR3 Configuration:

```
! ************************************************************************
! CSRT3620c.cfg - Cisco router configuration file
!   Thursday, July 19, 2001, 02:59:25 PM
!
! Hostname: CSRT3620c
! Model: 3620
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname CSRT3620c
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
controller T1 0/0
!
interface FastEthernet 1/0
 no shutdown
 description connected to EthernetLAN
 ip address 165.68.70.131 255.255.255.224
! HSRP Configuration
 standby 1 ip 165.68.70.129
 standby 1 preempt
 standby 1 priority 110
 standby 1 authentication upfront
 standby 1 timers 5 15
 keepalive 10
!
ip classless
!
! Deny local subnet addresses:
!
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
!
! Deny packets with localhost, broadcast, multicast, and missing destination IPs
!
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 101 deny    ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any log
```

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

```
access-list 101 deny   ip host 0.0.0.0 any log
!
! Prevent spoofing. Deny incoming packets that have
! our internal address:
!
access-list 101 deny   ip  0.0.0.255 any log
!
! Allow VPN traffic to VPN Server
!
access-list 101 permit tcp any host 165.68.70.102 eq 50
access-list 101 permit ip any host 165.68.70.102 proto eq 500
!
! Log everything that does not meet the above rule set
!
access-list 101 deny   ip any any log
!
! End of access-list 101
!
! Beginning of access-list 102
!
! Only allow packets from our network.
!
access-list 102 permit ip 165.68.70.0 0.0.0.255 any
!
! Log everything else:
!
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any any log
!
! End of access-list 102
!
! Apply access list to external interface
!
ip access-group 101 in
ip access-group 102 out
!
ip accounting access-violations
!
! IP Static Routes
!
ip route 0.0.0.0 0.0.0.0 FastEthernet 1/0 1 permanent
no ip http server
!
snmp-server community ######## RO
snmp-server community ######## RW
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password ########
 login
!
end
```

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

RTR4 Configuration:

```
! ************************************************************
! CSRT3620d.cfg - Cisco router configuration file
!   Thursday, July 19, 2001, 02:59:25 PM
!
! Hostname: CSRT3620d
! Model: 3620
! ************************************************************
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname CSRT3620d
!
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
controller T1 0/0
!
interface FastEthernet 1/0
 no shutdown
 description connected to EthernetLAN
 ip address 165.68.70.132 255.255.255.224
! HSRP Configuration
 standby 1 ip 165.68.70.129
 standby 1 preempt
 standby 1 priority 110
 standby 1 authentication upfront
 standby 1 timers 5 15
 keepalive 10
!
ip classless
!
! Deny local subnet addresses:
!
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
!
! Deny packets with localhost, broadcast, multicast, and missing destination IPs
!
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 101 deny    ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny   ip host 0.0.0.0 any log
!
! Prevent spoofing. Deny incoming packets that have
! our internal address:
!
access-list 101 deny   ip  0.0.0.255 any log
```

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

```
!
! Allow VPN traffic to VPN Server
!
access-list 101 permit tcp any host 165.68.70.102 eq 50
access-list 101 permit ip any host 165.68.70.102 proto eq 500
!
! Log everything that does not meet the above rule set
!
access-list 101 deny   ip any any log
!
! End of access-list 101
!
! Beginning of access-list 102
!
! Only allow packets from our network.
!
access-list 102 permit ip 165.68.70.0 0.0.0.255 any
!
! Log everything else:
!
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any any log
!
! End of access-list 102
!
! Apply access list to external interface
!
ip access-group 101 in
ip access-group 102 out
!
ip accounting access-violations
!
! IP Static Routes
!
ip route 0.0.0.0 0.0.0.0 FastEthernet 1/0 1 permanent
no ip http server
!
snmp-server community ######## RO
snmp-server community ######## RW
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password ########
 login
!
end
```

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

Check Point Firewall-1 VPN-1 Rules for FW3 & FW4:

Allow or Deny	Source Address(es) or Network(s)	Destination Address(es) or Network(s)	Protocol	Port	Service	Comment
A	165.68.70.148 165.68.70.129 165.68.70.130 165.68.70.131	165.68.70.148 165.68.70.129 165.68.70.130 165.68.70.131	ICMP		PING	Allow ping of VPN Concentrator from VPN border routers
A	ANY	165.68.70.148	IPSEC		IPSEC VPN	IPSEC to CISCO 3030
A	165.68.70.148	ANY	IPSEC		IPSEC VPN	IPSEC to CISCO 3030
A	165.68.70.106	165.68.70.145 165.68.70.146 165.68.70.147	TCP	22	SSH	For Local Management
A	165.68.70.106	165.68.70.145 165.68.70.146 165.68.70.147	TCP	257	FW1 Log	Firewall Logging
A	165.68.70.106	165.68.70.145 165.68.70.146 165.68.70.147	TCP	258	FW1 Management	Management from internal network via
D	ANY	ANY	ALL	ANY	ALL	Default deny just to be sure

***Note**: IPSEC Consists of services provided by the VPN-1 component. Services include ISAKMP(port 500udp), 3DES encryption specified, AH(match ip_p=0x39), ESP(ip_p=0x32), SKIP(ip_p=0x39).

CISCO 3030 VPN Concentrator:

The selected configuration of the 3030 Concentrator's interfaces is as follows:

Ethernet 1: VPN Segment2: V-LAN 5b
Interface1 = 165.68.70.148

Ethernet 2: Application / VPN Connectivity LAN: V-LAN 4
Interface2 = 165.68.70.102

Ethernet 3: Supplier LAN Segment: V-LAN 6
Iterface3 = 165.68.70.161

© SANS Institute 2000 - 2005

Author retains full rights.

Configure the interfaces correctly:

The concentrator will display the following after interface configuration has been completed properly.

```
    Interface          IP Address/Subnet Mask           MAC Address
-------------------------------------------------------------------------
Ethernet 1 - Public   | 165.68.70.148/255.255.255.240 | 00.10.5A.1F.4F.07
Ethernet 2 - Private  | 165.68.70.102/255.255.255.224 | 00.B0.D0.7D.8D.33
Ethernet 3 - External | 165.68.70.161/255.255.255.224 | 00.B0.D0.83.C9.F3
-------------------------------------------------------------------------
```

Tunneling Protocols:

The tunneling protocol of choice in the deployment is IPSEC. By default PPTP and L2TP are enabled. The first step is to disable PPTP and L2TP. While these protocols are more "*Microsoft friendly*" they are not the best from a security perspective. The CISCO VPN client will allow users to create a tunnel with the device easily from a sufficient number of platforms to make it useable.

Disable PPTP:

```
-- : Configure protocols and encryption options.
-- : This table shows current protocol settings

         PPTP          |        L2TP         |
-----------------------------------------------
|       Enabled       |       Enabled       |
|  No Encryption Req  |  No Encryption Req  |
-----------------------------------------------

1) Enable  PPTP
2) Disable PPTP

-> [ 2 ] _
```

Disable L2TP:

```
         PPTP          |        L2TP         |
-----------------------------------------------
|       Enabled       |       Enabled       |
|  No Encryption Req  |  No Encryption Req  |
-----------------------------------------------
1) Enable  L2TP
2) Disable L2TP

-> [ 2 ] _
```

Enable IPSEC:

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

```
1) Enable  IPSEC
2) Disable IPSEC

-> [ 1 ] _
```

At this point the interfaces and protocols are configured. The remaining work is to configure the authentication and address pooling characteristics of the VPN concentrator.

- Enable DHCP Address Assignment

Configure Address pool (10 addresses are left for VPN clients to share in the VLAN 5b subnet):

```
> Configured Pool Range Start Address

Quick -> _ 165.68.70.149

> Configured Pool Range End Address

Quick -> [ 0.0.0.0 ] _ 165.68.70.159
```

Configure the authentication mechanism of the device. For simplicity, the VPN Concentrator will act as the authentication device. This device is capable of handling 100 users. This should be plenty in the case of our suppliers and partners.

```
-- : Specify how to authenticate users.

1) Internal Authentication Server
2) RADIUS Authentication Server
3) NT Domain Authentication Server
4) SDI Authentication Server
5) Continue

Quick -> _ 1
```

Once completed the device is ready to be deployed. Users should be added on a per access request basis.

© SANS Institute 2000 - 2005 Author retains full rights.

Assignment 3 – Audit Your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignment 1 and 2. Your assignment is to:

1. *Plan the assessment. Describe the technical approach you recommend to assess your perimeter. 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. *Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, include the tools and commands used. Include screen shots in your report if possible.*
3. *Conduct a perimeter analysis. 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 annotate the output.

Plan the assessment:

The primary objective of a firewall assessment is to determine if the security policy is being complied with. Once a policy has been adopted, management must have assurance of this compliance. In addition to determining if policy is being complied with, the assessment will determine if the assessed systems are subject to service disruption, subversion or corruption. The assessment will provide information to security decision makers that allows effective planning based on facts rather than guesses. Armed with this information, GIAC Enterprises will maintain a stronger security posture.

The scope of the assessment will be the primary firewalls and I have recommended adding the border routers as well. The perimeter security layer relies on these routers for added protection. Since the routers are relied upon to perform security functions, it should be verified that they are working in accord with the firewalls. The results of the assessment will be communicated to GIAC Enterprises Executive management, Infrastructure management, and concerned Technicians.

A review of GIAC Enterprises network traffic revealed that the activity peaked each day between the hours of 2:00 pm to 4:30 pm. It was determined that the assessment would be conducted during business hours but not within the peak hours mentioned. It was estimated that this assessment would require two business days of testing, two standby technicians, and one half day for administration. The cost has been estimated to be $8,500.

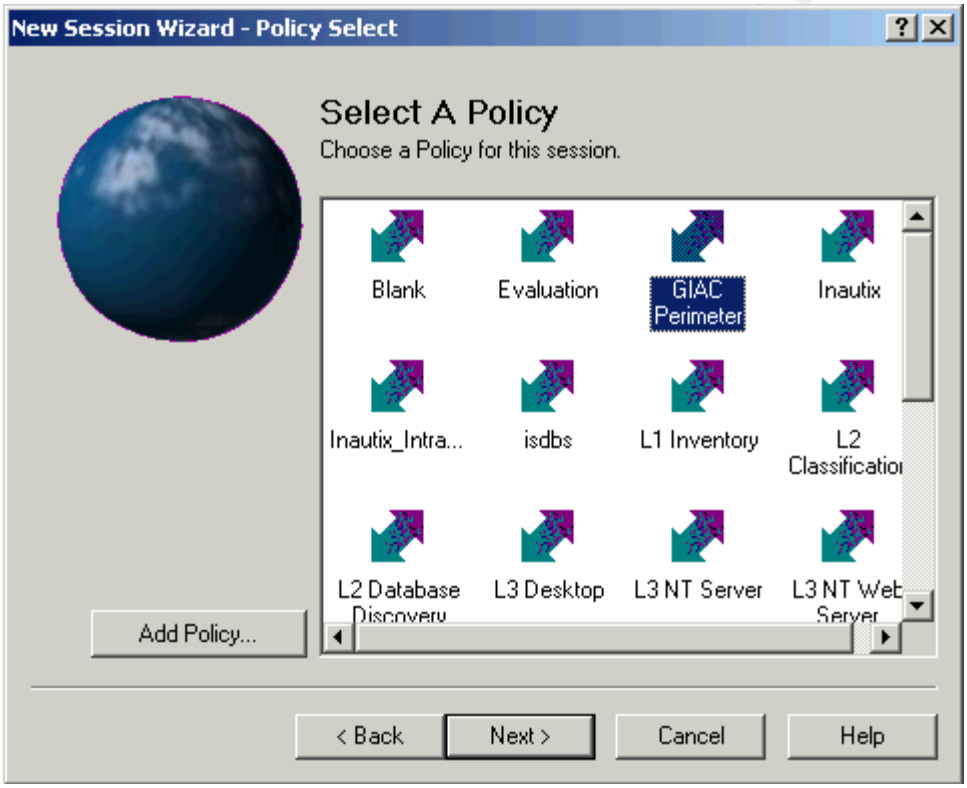
© SANS Institute 2000 - 2005, Author retains full rights.

The tool selected is Internet Security Systems Internet Scanner 6.1. This tool provides the functionality required to meet management objectives with policy compliance as well as testing for susceptible vulnerabilities. Internet Scanner is a product in the Internet Security Systems SAFEsuite product line. http://www.iss.net .

Implement the assessment:

NOTE: Prior to implementing the planned assessment, ***written*** approval by executive management will be obtained.

The initial phase of the assessment with the IIS Internet Scanner is to create a policy. Internet Scanner has five default policies that are listed by levels. Level 1 would be a soft scan which would identify the types of operating systems running on a network, whereas a level 5 would be a stronger scan directed at critical systems requiring more protection. A level 5 policy would scan for compromised systems by highly skilled attackers or signs that a system is misconfigured. Given our unique objectives of assessing the perimeter defenses, we must create a policy that is customized to our needs. Internet Scanner provides this capability.

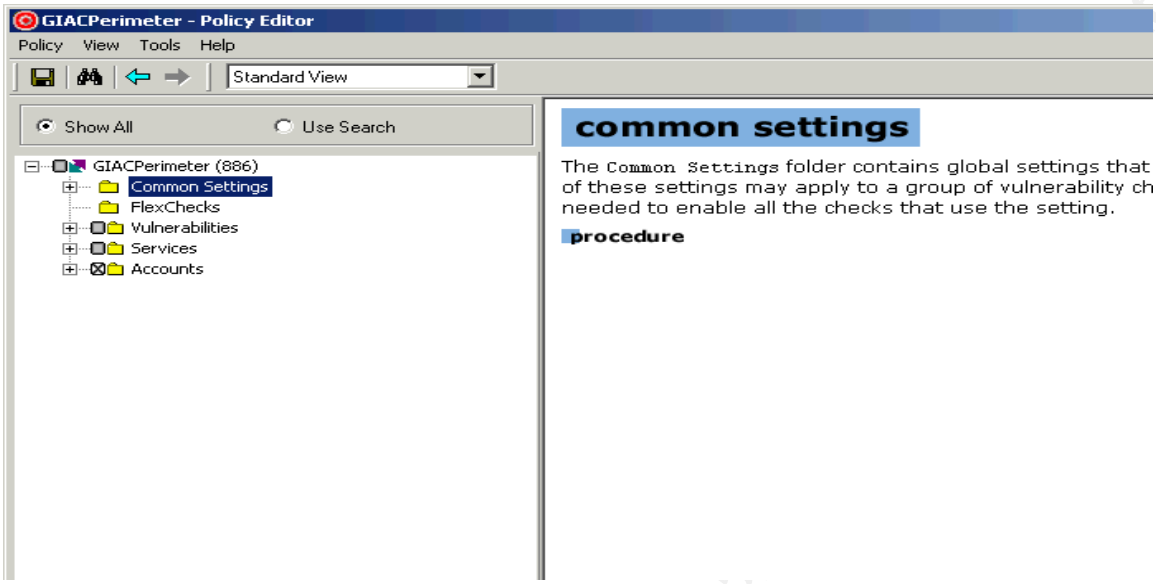


The above screen shot illustrates the policy selection screen that indicates the creation of a GIAC Perimeter policy. This newly created policy has default checks that will be conducted. Since we will want to customize our new policy, we will have to make adjustments to remove unwanted checks and add new requirements. This is performed in the Policy Editor menu, which has five different views such as Standard View (shown

© SANS Institute 2000 - 2005

Author retains full rights.

below) and Built-Ins/Plug-Ins, Category, Module, and Risk Views. It is through these browser-enabled windows that I will customize my policy by adjusting my checks that will be scanned. My checks will be more specific towards my firewall and router policies as well as known operating system vulnerabilities.



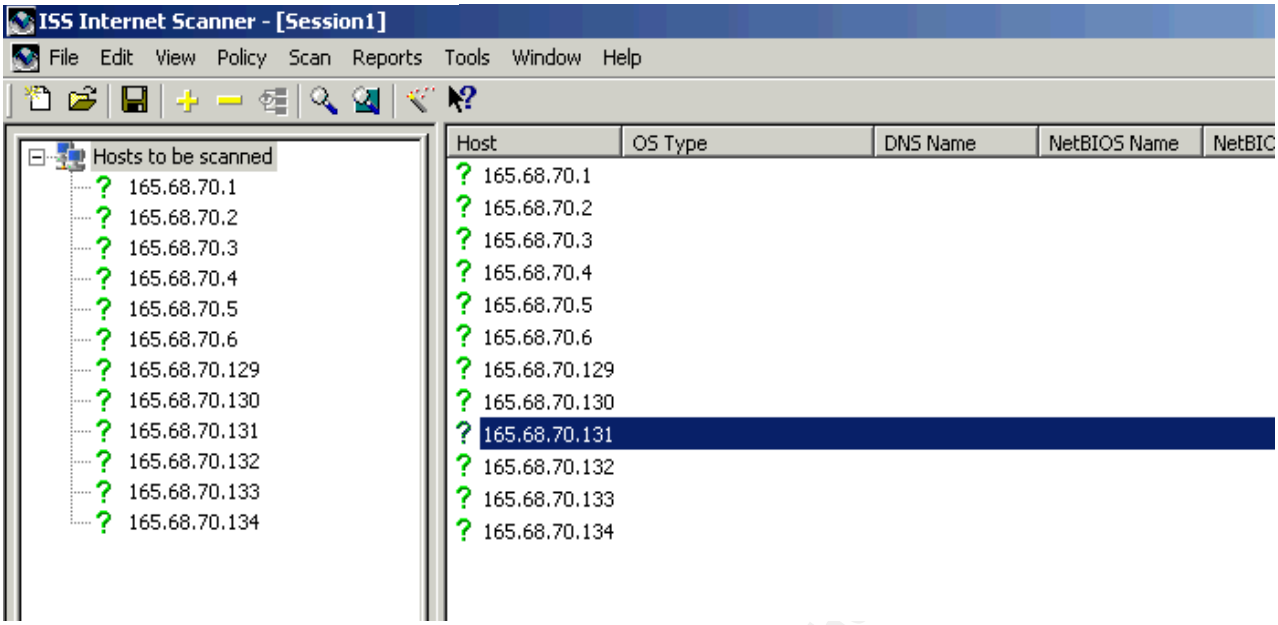
Once I have completed my policy editing I am now ready to establishing a session. An Internet Scanner session defines which devices to scan and which checks to perform. There are three session features:

- The policy selected.
- The key file – defines maximum number and allowable range of machines to scan.
- The group of systems to scan, identified by a list of IP addresses.

The below screen shot illustrates the set of devices that will be scanned with their IP addresses.

© SANS Institute 2000 - 2005

Author retains full rights.



I now start the scan from the existing session1 by clicking Scan > Scan Now. When the scan is complete the results can be viewed and the required reports generated.

Conduct a perimeter analysis:

Once the assessment is complete I would analyze the results of my port scans and determine if my firewall rulebases and router ACLs are compliant with policy. Router and Firewall logs will also be examined to determine if the scan was detected. In addition, any known vulnerabilities detected will be reported. This data will be analyzed and any deviations of policy or vulnerability alerts uncovered will be immediately investigated. Once investigated, an action agenda will be prepared outlining corrective measures to be taken. An independent review will be conducted to ensure corrective measures have been implemented when required.

During this analysis two weaknesses were discovered. One being the lack of intrusion detection and the second being the deployment of one firewall product. Intrusion detection tools are critical for timely detection of attacks and deploying two different firewall applications reduce the risk of single point of failure if one application is effected by an exploit. The below is a proposed diagram that will be forwarded to executive management for review.

Intrusion Detection – I have proposed adding Intrusion Detection probes at five points. The IDS product proposed is the Internet Security Systems RealSecure.

1. Between primary border routers and firewalls
2. Behind firewalls in front of Public Utility Segment
3. Behind firewalls in front of Commerce Segment
4. Behind VPN firewalls front of VPN Connectivity Segment

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

5. Front of Internal Network

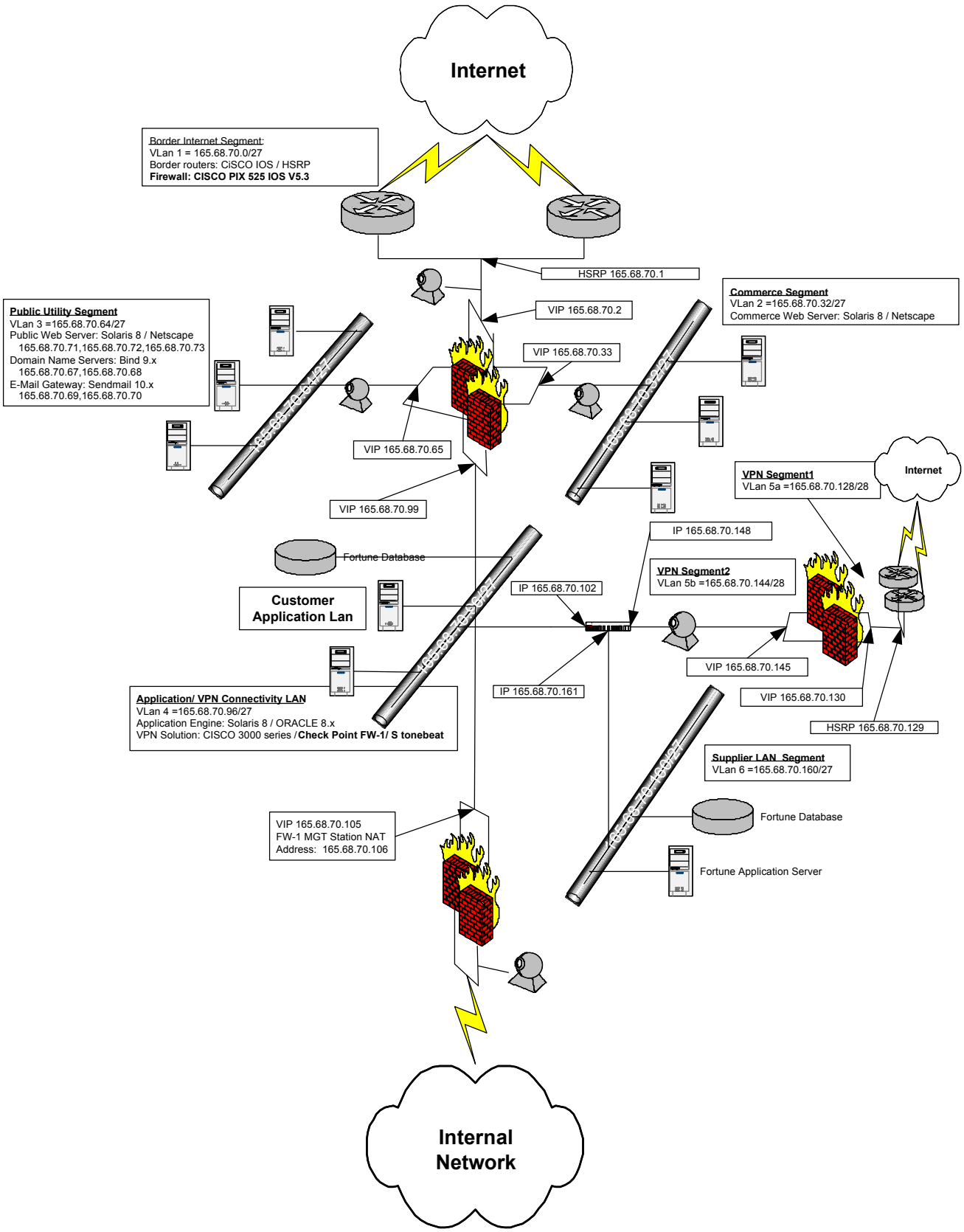
IDS symbol in proposed diagram:



Firewalls - I have proposed changing the firewall pair deployed behind the border routers at the Border Internet Segment. The Check Point Firewall-1 pairs would be changed with CISCO PIX 525 IOS V5.3. This change would mitigate the threat of a firewall failure.

Diagram illustrated on the following page.

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


Internet
Border Internet Segment:
VLan 1 = 165.68.70.0/27
Border routers: CiSCO IOS / HSRP
Firewall: CISCO PIX 525 IOS V5.3
HSRP 165.68.70.1
VIP 165.68.70.2
VIP 165.68.70.33
VIP 165.68.70.65
VIP 165.68.70.99
Public Utility Segment
VLan 3 =165.68.70.64/27
Public Web Server: Solaris 8 / Netscape
165.68.70.71,165.68.70.72,165.68.70.73
Domain Name Servers: Bind 9.x
165.68.70.67,165.68.70.68
E-Mail Gateway: Sendmail 10.x
165.68.70.69,165.68.70.70
Commerce Segment
VLan 2 =165.68.70.32/27
Commerce Web Server: Solaris 8 / Netscape
VPN Segment1
VLan 5a =165.68.70.128/28
Internet
IP 165.68.70.148
VPN Segment2
VLan 5b =165.68.70.144/28
Fortune Database
Customer
Application Lan
IP 165.68.70.102
VIP 165.68.70.145
IP 165.68.70.161
VIP 165.68.70.130
HSRP 165.68.70.129
Application/ VPN Connectivity LAN
VLan 4 =165.68.70.96/27
Application Engine: Solaris 8 / ORACLE 8.x
VPN Solution: CISCO 3000 series / Check Point FW-1/ S tonebeat
Supplier LAN Segment
VLan 6 =165.68.70.160/27
VIP 165.68.70.105
FW-1 MGT Station NAT
Address: 165.68.70.106
Fortune Database
Fortune Application Server
Internal
Network

Assignment – 4 Design Under Fire

The purpose of this exercise is to help you think about 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 previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

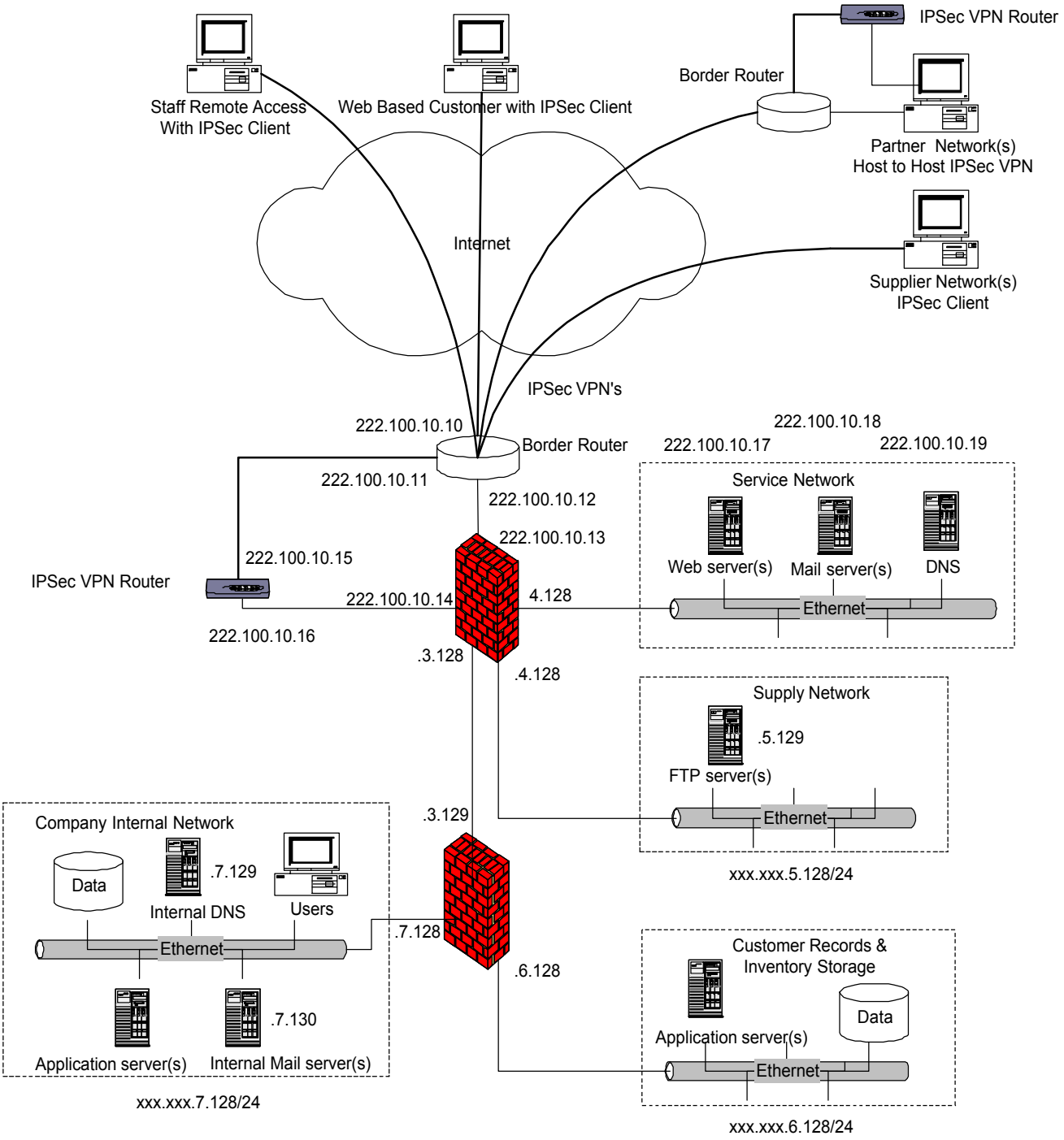
1. *An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.*
2. *A denial of service attack. Subject the design to a theoretical attack from 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.*

NOTE: *this is the second time this assignment has been used. The first time, a number of students came up with magical "hand waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.*

The diagram for the Design Under Fire Assignment has been provided by Gordon Crease. (**http://www.sans.org/y2k/practical/Gordon_Crease_GCFW.zip**)

The diagram has a strong security posture with logical segmentation. I have taken some assumptions in regards to the security state of certain applications such as specific service patches or applied workarounds. The chosen design is located on the following page.

© SANS Institute 2000 - 2005 Author retains full rights.



© SANS Institute 2000 - 2005

Author retains full rights.

Firewall Attack:

As many security professionals know, firewalls are no panacea. They are only one layer of the "defense in layers" strategy. Firewalls, when deployed correctly, are very effective defense tools. However, many fail due to misconfiguration, poor maintenance, and lack of monitoring. Firewall logs in many organizations are not reviewed. This is why an attack directly on a firewall can succeed.

In the preceding diagram, Gordon Crease has selected a Gauntlet firewall, version 5.5 from Network Associates as his perimeter firewall defense. If I had received this diagram during my attack planning stage, I would still have to do some reconnaissance to verify this information. This verification can be obtained by several methods. Three common methods are:

- Port scanning
- Route tracing – Unix's traceroute or NT's tracert.exe
- Banner grabbing

Once I have mapped his network I can research for known vulnerabilities that will exploit his systems. For the attack against his firewall I discovered a known vulnerability that exists due to an unchecked buffer overflow in the CyberPatrol daemon on Gauntlet Firewalls and web appliances. Since the Gauntlet firewall described in Gordon Crease's practical does not indicate what patches are applied, I will assume this system is still vulnerable. Remember most firewall failures result due to human error. A remote attacker that sends packets that overflow the unchecked buffer exploits the vulnerability. Details from ISS X-Force Database http://xforce.iss.net/static/4503.php

gauntlet-cyberdaemon-bo(4503)

Description:
Gauntlet is a multi-platform firewall system produced by Network Associates. One feature of the firewall is its integration with the CyberPatrol content monitoring system. CyberPatrol, a component of the Gauntlet, is vulnerable to a buffer overflow in the Cyberdaemon component. A remote attacker can overflow the buffer to crash the system and deny further proxied HTTP connections to legitimate users, or execute arbitrary code on the firewall with root privileges.

Platforms Affected:
Gauntlet Firewall 5.0
Gauntlet Firewall 5.5
Gauntlet Firewall 4.2
Gauntlet Firewall 4.1
WebShield 100 Series
WebShield 300 Series
WebShield Solaris 4.0

Remedy:

© SANS Institute 2000 - 2005 Author retains full rights.

Apply the appropriate "cyber.patch" for your system, available from the Gauntlet Support Patch Status Web page. See References.

Consequences:

Gain Access - root uid

References:

http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-05-15&msg=392961F5.2240B376@ai.org
http://www.tis.com/support/patchpage.html

Standards associated with this entry:

CVE-2000-0437: Buffer overflow in the CyberPatrol daemon "cyberdaemon" used in gauntlet and WebShield allows remote attackers to cause a denial of service or execute arbitrary commands.

Jim Stickley of Garrison Technologies is credited for discovery of this vulnerability.

Reported May 2000 / Entered May 2000

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0437

Denial Of Service Attack:

Denial of service (DoS) attacks have caused mayhem for many organizations connected to the internet. The goal of DoS and distributed denial of service (DDoS) attacks is to cause disruption or a complete denial of service to legitimate users. These attacks are perpetrated for various reasons and directed at organizations with malicious intent. Additionally, what makes these attacks such a high threat is the fact that they can be executed with little effort or sophistication. There are three types of denial of service attacks. They are:

- Bandwidth consumption – This attack is focused on consuming all available bandwidth of the target organization.
- Resource starvation – This attack is focused on consuming the target systems resources such as CPU utilization, memory, and system processes.
- Programming flaws – This attack is focused on taking advantage of program weaknesses (bugs) by applying exceptions that the particular program, O/S cannot handle. Ultimately crashing the target system.
- Routing and DNS attacks – This attack focuses on the manipulation of routing tables to deny services. The DNS attack focuses on poisoning the cache of a DNS server thereby redirecting traffic to a site selected by the attacker.

The type of attack I will initiate is a SYN flood attack against the Web server within the Service Network. This is a protocol manipulation attack that would be focused on depleting the targets resources, thus a Resource Starvation attack. This attack will be launched with the assistance of 50 compromised high-speed cable modem/DSL systems. My goal is to exhaust all resources allocated to setting up a TCP connection by sending SYN packets from all my compromised systems to the target web server 222.100.10.17 port 80. These initial SYN requests will occur simultaneously with spoofed IP addresses. Since the target system sends a SYN/ACK packet to all SYN packets received, it will be in a SYN_RECV state and placed in a connection queue. This situation occurs because the targets SYN/ACK response is never received by sending machines. Therefore the 3-way handshake is in left open. The target system is exhausting resources while this state is

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

maintained. The potential connection will only be removed from the queue when the connection-establishment timer expires. Since the connection queue is usually small, just a few SYN packets establishing the SYN_RECV state will exhaust my targets resources. My goal is accomplished.

Countermeasures:
The DoS attack is very difficult to prevent. Having a determined attacker with an inventory of resources, there is little you can do. However there are several ways to mitigate the risks of SYN Flood attacks. They are:

1. Increase the size of the connection queue. However this may affect performance.
2. Decrease the connection establishment timeout period
3. Research and deploy current vendor patches which address SYN Flood attacks
4. Deploy intrusion detection systems – some IDS can detect SYN Flood attacks and take countermeasures.

Internal System Attack Plan:

The internal system that I will plan an attack on is again the web server. Since I am not supplied the operating system the web for the server, I will assume it to be a Microsoft IIS Server 4.0 or 5.0. This particular application is widely deployed, however many vulnerabilities exist. My goal will be to gain access to the server, escalate my privileges and obtain valuable information from trusted back end servers or databases. My plan will be executed in stages utilizing several techniques in each. These stages are as follows:

1. Footprinting – whois, ARIN whois look ups, DNS zone transfers
2. Scanning – Ping sweep, TCP/UDP port scans
3. Enumeration – lists of user accounts, file shares, applications
4. Gain access – brute force, obtaining password files, executing buffer overflows
5. Escalating privileges – known exploits (many with IIS), crack passwords of privileged users
6. Pilfering – gain information on trusted systems (my goal databases, other servers)

Once I have obtained the information I need with easily accessible tools, I will research for known vulnerabilities with my target system. A search that I conducted revealed a vulnerability that exists in the Indexing Service used by Microsoft IIS 4.0 and IIS 5.0. Outlined below is the vulnerability details provided by CERT in CERT Advisory CA-2001-13 Buffer Overflow in IIS Indexing Service DLL.
(http://www.cert.org/advisories/CA-2001-13.html)

CERT:
A vulnerability exists in the Indexing Services used by Microsoft IIS 4.0 and IIS 5.0 running on Windows NT, Windows 2000, and beta versions of Windows XP. This vulnerability allows a remote intruder to run arbitrary code on the victim machine. Since specific technical details on how to create an exploit are publicly available for this vulnerability, system administrators should apply fixes or workarounds on affected systems as soon as possible. I. Description
There is a remotely exploitable buffer overflow in one of the ISAPI extensions installed with most versions of

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

IIS 4.0 and 5.0 (The specific Internet/Indexing Service Application Programming Interface extension is IDQ.DLL). An intruder exploiting this vulnerability may be able to execute arbitrary code in the Local System security context. This essentially can give the attacker complete control of the victim system.

This vulnerability was discovered by eEye Digital Security. Microsoft has released the following bulletin regarding this issue: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Affected versions of Windows include Windows NT 4.0 (installed with IIS 4.0 and Index Server 2.0), Windows 2000 (Server and Professional with IIS 5.0 installed), and Windows 2000 Datacenter Server OEM distributions; however, not all of these instances are vulnerable by default. The beta versions of Windows XP are vulnerable by default. The only precondition for exploiting this vulnerability is that an IIS server is running with script mappings for Internet Data Administration (.ida) and Internet Data Query (.idq) files. The Indexing Services do not need to be running. As stated by Microsoft in MS01-033:

> The buffer overrun occurs before any indexing functionality is requested. As a result, even though idq.dll is a component of Index Server/Indexing Service, the service would not need to be running in order for an attacker to exploit the vulnerability. As long as the script mapping for .idq or .ida files were present, and the attacker were able to establish a web session, he could exploit the vulnerability.

This vulnerability has been assigned the identifier CAN-2001-0500 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500

Conclusion:

The growth of business that is being conducted on the Internet is growing exponentially. The challenges facing Information Security professionals are increasing at the same rate. This assignment has illustrated the numerous talents required of security professionals today. We as a security community must work smarter by sharing information and resources. Network design, policy development and compliance, and vulnerability analysis are just a few of the competencies needed to be successful. These competencies can be matured by increasing information sharing projects and developing methods for easy access to required resources. This will not only result in more secure perimeters for individual borders, but will enhance efforts to secure larger global borders.

© SANS Institute 2000 - 2005 Author retains full rights.

List of References:

Scambray, Joel, McClure, Stuart, Kurtz, George, *Hacking Exposed: Network Security Secrets & Solutions 2nd Edition,* Berkeley:McGraw-Hill 2001

Russell, Ryan, Cunningham, Stace, *Hack Proofing Your Network: Internet Tradecraft*, Maryland:Syngress Media 2000

Cheswick, William R., Bellovin, Steven M., *Firewalls and Internet Security: Repelling the Willy Hacker*, Massachusetts:Addison-Wesley, 1994

Crume, Jeff, *Inside Internet Security: What Hackers Don't Want You To Know*, England:Addison-Wesley, 2000

Taylor, Paul: *Hackers: crime in the digital sublime*, London: Routledge, 1999

Anderson, Ross: *Security Engineering: A Comprehensive to Building Dependable Distributed Systems*: John Wiley & Sons, 2001

Additional Resources:

http://www.sans.org

http://www.cert.org

http://www.microsoft.com

http://www.cve.mitre.org

http://www.iss.net

http://www.globalintegrity.com

http://www.securityfocus.com

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

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