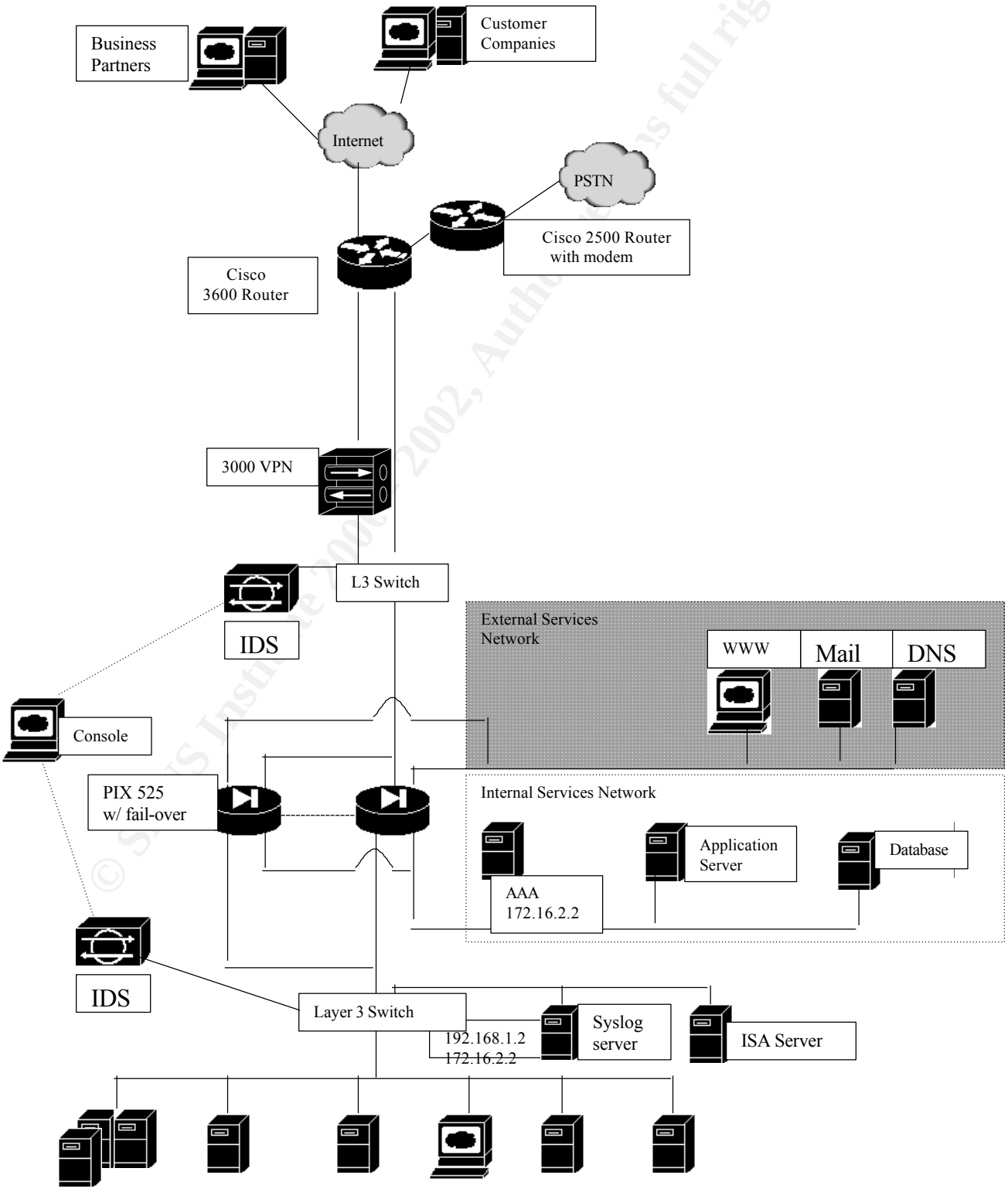
# Global Information Assurance Certification Paper

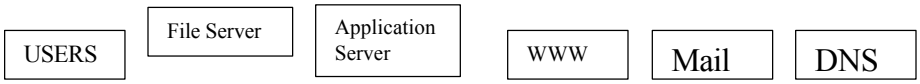
Gerald K. Clevenger
Nov 16, 2001

# Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment Retake
Version 1.6a
Orlando, Fla.

# TABLE OF CONTENTS






## GIAC Enterprises Layout

Border Router – A CISCO 3600 Router, provides access to the internet for GIAC employees, and access to the GIAC Web server for internet users via http and https. The Cisco 3600 uses Cisco IOS 12.1. The Cisco 3600 Router is used as a border router to filter out unwanted and malicious traffic from the network. Services that are not allowed into the GIAC network from the internet are blocked, and ingress/egress filtering is performed.

A Cisco 3000 VPN Concentrator provides a Site-to-Site Security Gateway for business partners and major clients, as well as a VPN access point for remote access clients running Cisco Secure VPN Client software. The 3000 VPN Concentrator provides IPSec compliant VPN connectivity using 3Des encryption at 24MBPS. The 3000 offer both Authentication Header (AH) and Encapsulated Security Payload (ESP) for secure connectivity with established Security Associations. Users authenticate is through an Interlink AAA Server Appliance located on the Private DMZ. The Cisco VPN 3000 Concentrator uses Cisco IOS 12.1

A Cisco 2500 router is equipped with a PSTN module to provide dial up access for smaller clients and employee remote access. The Cisco 2500 provides remote access through dial in modems.

IDS Sensors-ISS Real Secure Network Sensors, one connected to the External interface connection of the PIX firewall, and one connected to the Internal Interface of the PIX. The Real Secure Network Monitor will require a connection that has port mirroring enabled in order to monitor all traffic entering and exiting the network. Port mirroring may result in a performance hit on throughput. Two Ethernet Interface cards are required for Stealth monitoring.

The Firewall is a Cisco Secure PIX 525 Firewall with Fail-over configuration using IOS 5.0. Cisco Security PIX IOS 5.0 is IPSec compliant and supports NAT and PAT to effectively hide the internal network from the external Internet. Global address assignments allow access to external Internet resources with the PIX firewall handling the mapping of global addresses to internal addresses. Static assignments give Globally Unique addresses to resources that must be accessed from external sites.
Public External Services Network (DMZ) including Split DNS, External Web service, and a Mail forwarding server configured to scan for viruses.

The External WEB server sends request for data through an Application server located on a secondary Network Services Network. The Application Server sends SQL queries to the External

Database server.

The AAA Radius Server Appliance is an Interlink Pyramid appliance providing Authentication, Authorization, and Accounting services for remote, VPN, and internal users accessing corporate resources.

## GIAC ENTERPRISES

GIAC Enterprises maintains an E-Commerce Internet presence with access to on line sales through the Corporate External Web Server. Corporate business partners, suppliers, and distributors utilize a secure Web connection to complete orders through a site-to-site Virtual Private Network (VPN) connection utilizing a Cisco 3000 VPN Concentrator. The Cisco 3000 VPN provides Encapsulating Security Payload (ESP) and Authentication Head (AH) support. Site to site VPN tunnels will be configured for business partners as well as for large-scale clients using the Cisco 3000 as a Security Gateway to establish the needed Security Association between partners and clients. Business partners and clients equipped with Cisco routers can be easily configured using available Cisco Config Maker software.

Smaller suppliers and distributors utilize a 2500 router with integrated modem supporting dial in access. Authentication of external vendors and distributors are accomplished through an AAA server that validates users with access rights assigned by groups.

Due to the ease of installation and configuration, an Interlink AAA Radius appliance is used for the Authentication, Authorization, and Accounting server.

The 3600 Border router filters unnecessary protocols and services while allowing access to the Corporate External Web server, Mail server, and internet access to the employees of GIAC Enterprises. The internal interface of the Cisco 3600 router is connected to the External Interface of a Cisco PIX 525 Firewall with Fail Over configuration. A RealSecure® Network Intrusion Detection Sensor monitors all traffic passing into the External Interface of the Firewall. The RealSecure® Sensor monitors traffic through a Network Interface card that has NO bindings, and is therefore running in stealth mode. A second NIC in the RealSecure® Sensor connects to a Monitor Console that is not connected to the corporate network. The Real Secure Network Sensor is configured to issue a Reset in the event of an External ISS scan or NMAP scan of the External network. Along with the Reset, an email is issued to the Network Manager to notify him that the Network is under attack. The E-Mail initiates a Page to a Pager that is carried by the On-Call Network support person to notify Network Support that the network is under attack. The Monitor is configured to send the address of the attacking system to the Firewall to incorporate a block of the attacking IP address into the filter set of the Router.

The Cisco Pix Firewall uses the Cisco Adaptive Security Algorithm to provide stateful connection control of traffic through the Firewall. The rules for Adaptive Security may be simplified to mean that outbound connection or states are allowed, unless specifically denied by access control list; and that inbound connections or states are denied, unless specifically allowed. The Highest Security Level is the Internal Interface of the Firewall, while the lowest security level is the External Interface.

The External Port of the CISCO PIX is configured to drop packets addressed to the Firewall. Inward bound HTTP, HTTPS, SMTP, and DNS are allowed in through the External interface. Outgoing traffic is unrestricted, but monitored.

The DMZ port of the CISCO PIX 525 connects to the External Services Network, which is the location of the External Corporate Web Server where all transactions with clients and suppliers occur. It is also the location of the E-Mail forwarding server, where E-Mail is scanned for viruses and content before being forwarded to the internal E-Mail server. GIAC Enterprises uses split DNS, with the External DNS server located on the External Services Network. The

DMZ interface of the PIX firewall is configured to deny any session initiated by a system located on the External Services Network. The DMZ interface allows HTTP and HTTPS traffic from the external port of the PIX, as well as SMTP to the mail-forwarding server. DNS traffic is also allowed to the DMZ.

The External Services network utilizes Globally Unique Addresses for access by external resources. Systems connected to the Internal interface of the PIX Firewall use Network Address Translation. Network Address Translation hides internal addresses from external connections.

The External Web server interfaces with an application server located on a secondary network services interface. Group access rights determine which services are available to the user. A Database server is also located on the secondary Network services interface. The application server can make SQL queries to the Database server. Only SQL communications are allowed from the applications server to the Database server.

## Security Policy

### Objectives

- Protect the organizations' information by safeguarding the confidentiality, integrity, and availability of information.
- Establish safeguards to protect the organizations' information resources from theft, abuse, misuse, and unauthorized disclosure.
- Ensure that all employees and contractors receive security awareness training that informs them of their responsibility and accountability for the protection of information resources.
- Manage risk to all information resources.

## Controlling Access to Information and Systems

### Physical Access

GIAC Enterprises requires that all employees and contractors wear a picture ID while in GIAC facilities. Entrances to all areas require the employee to 'badge in' utilizing a bar code label printed on the back of the employees picture ID. Contractors, guest and service workers not normally assigned to GIAC facilities are required to sign in and receive temporary badges. Network equipment will be kept in locked rooms or cabinets to limit access to authorized personnel. Wiring closets will be kept locked unless authorized technicians are performing maintenance.

### Computer Access

All computer systems that support bios passwords will have power on passwords before the operating system loads. Additionally, a logon password will be required for access to system and network resources. Operating systems capable of timed screen savers will have password

protected screen savers set to no longer than 10 minutes unless otherwise approved by the security manager.

**Password Policy**

- User passwords will be a minimum of (8) characters with at least one character being a numeric or special character.
- Passwords must be changed every 180 days.
- Passwords cannot be shared, available, or known to others.
- Passwords should not be written unless stored in a locked container with controlled access.
- Prevent reusing of last 4 passwords.
- Encrypt passwords when possible.

**Accounts authorization**

- Suspend unused accounts after 30 days.
- Revoke accounts and privileges of terminated and transferred employees.
- Suspend account of user after 5 unsuccessful logon attempts.
- Display a warning banner before logon indicating that GIAC computing resources are for company business.

**Network Access: (Internal)**

Network access for computing resources shall be granted to the user under the following conditions.

- The user must request a computer and system account through the Office of Information Technology; the users supervisor must approve the request.
- The user must complete the current Computer Security Awareness training.
- The User must sign a GIAC Enterprises User Agreement and Acceptable Use statement.
- The computer is setup utilizing Configuration Guidelines.
- Information Technology Support activates the Port on the Network Switch.

**Remote Access**

Remote access is accomplished through the use of Site-to-site VPN, remote VPN, and Dial-up access authenticated through the AAA Radius Server Appliance. Remote access to mail and protected Web services is accomplished through HTTPS.

Site to site VPN will require a Security Association configured between the 3000 VPN concentrator, acting as a Security Gateway, and the business partner or client resource. Shared secret keys can be used by simply calling the sites Network Administrator. Key updates shall be facilitated by ensuring compatible time settings or by utilizing an NTP service.

**System Architecture**

An external firewall shall be used in conjunction with routers, encryption, and VPN tunnels to control and protect GIAC Enterprises Information resources. Firewall and router software shall be maintained with current release patches. Auditing of perimeter protection effectiveness will be conducted whenever changes are made to the IOS or to the configuration of the routers or firewall.

**Perimeter Router Policy**

A Border Router Filter policy is designed to block 'noise' from the Internet. The Border Router blocks ports known to be problematic. This provides a layered security model, with the Firewall being used as the second layer of security.
Ordering of rules is very important in the configuration of a router. The Border router Rule set is designed to list general rules first, and more specific rules last. When the router receives a packet, the packet is checked to see if it matches a rule. The check begins at the top of the rule set and works down. If the packet matches a rule, the rule is applied. In the event that the packet does no match any rule, the packet is discarded. The goal is to allow traffic that is desired, and to deny everything else. Therefore, the last rule of a rule set is to 'deny all.'
The Access Control List is the completed rule set applied to the router. As an example, look at the rule to allow the Internal users to access the Internet.

| Rule | Interface | Source Add | Destination Add | Protocol | Source Port | Dest Port | Action |
|---|---|---|---|---|---|---|---|
| HTTP | Int | Giac Internal | Any | HTTP | any | 80 | Allow |

The rule name is HTTP.
The first variable is the **Interface of the router**-usually internal or external. In this case it is the Internal Interface of the router.
The next field is **Source Address** of the packet (Giac Internal-indicating a source address of an internal system).
The next field is the **Destination Address** (Any-indicating any external address, there are no restrictions on where Giac employees can go on the internet.)
The next field is the **Protocol Field**, in this case the Protocol is HTTP.
Next is the **Source Port** (any)
Next is the **Destination Port** (The assigned port for HTTP is port 80)
The last field is the **Action** to be taken by the router (Allow)
Possible actions are Allow, deny, allow and log, deny and log.

Routers must also keep track of connection information. If you computer makes an HTTP connection to a Web server, the router must know to allow the response from the Web server to the port used to initiate the session. This is referred to as an established session. Every session has a session ID. In the event that the Web server does not respond in a reasonable amount of time, the router keeps the session opened until it times out. The amount of time before a session times out is designated in the router configuration.

Following is the basic rule set of the Router

First, designate what to allow.

(Allow all outgoing HTTP traffic from inside the site. The Router remembers the State and lets the response come in for the HTTP session)

Allow Outgoing TCP port 80
Allow Incoming Response (established) any IP/TCP 80

(Allow outgoing and incoming exchange mail, as well as the response. The Exchange server establishes a session on a high numbered port)

Allow outgoing Exchange.giac.com /TCP port 25
Allow incoming Exchange.giac.com /TCP port 25
Allow Exchange.giac.com /any established port TCP

(Allow outbound name server traffic, as well as the response on the established session)

Allow nameserver.giac.com /TCP/UDP port 53
Allow nameserver.giac.com /TCP/UDP established port 53

(Allow outgoing SSH, as well as the response on the established session)

Allow outgoing SSH /port 22
Allow outgoing SSH /established port 22

(Allow incoming HTTPS for the GIAC Web access, as well as outgoing established sessions)

Allow incoming www.giac.com HTTPS /TCP port 443
Allow outgoing www.giac.com HTTPS /TCP established port 443

| Rule | Interface | Source Add | Destination Add | Event | Source Port | Dest Port | Action |
|---|---|---|---|---|---|---|---|
| HTTP | Int | Giac Internal | Any | HTTP | 80 | any | Allow |
| Mail | Int<br>Ext | Giac Internal<br>Any | Any<br>Giac Internal | Mail | 25 | Any<br>Any | Allow |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DNS | Ext | Giac .Com | Giac Nameservers | DNS | 53 | 53 | Allow |
| DNS | Int | Giac.com | Giac Nameservers | DNS | 53 | 53 | Allow |
| SSH | Both | Giac.com | Any | SSH | 22 | 22 | Allow |
| HTTPS | Both | Any | www.giac.com | HTTPS | 443 | 443 | Allow |

After the allows, the denys should be configured. The goal is to identify which ports are needed and to block all others. Over time, the goal is to deny access unless specifically allowed.

1. Block addresses reserved for private and Test networks Since these addresses are not supposed to be routable, any traffic with these source addresses can be assumed to be someone doing malicious behavior, such as a Denial of Service.
2. Block external access to internal only addresses: Block outbound traffic from internal addresses. This is ingress and egress filtering- also known as sanity checks. An internal address attempting to come into the network through the external port of the router is a form of spoofing that could indicate a DDOS attack or a Trino. An external address on the internal interface would indicate that an internal system had been compromised.
3. Block Broadcast and Multicast addresses (Junk Mail, etc.) This is associated with bombardment attacks.
4. Block low level pinging and TCP,UDP, and, and FTP services. These services allow unauthorized information gathering.
5. Block known problematic ports. This would include Finger, NFS traffic, SMB traffic, SNMP,NTP, Netbios, and Windows Services.
6. Block packets where the source and destination are the same. This is a crafted packet and indicates malicious traffic.

| Rule | Interface | Source Add | Destination Add | Protocol | Source Port | Dest Port | Action |
|---|---|---|---|---|---|---|---|
| Block Private | Ext | 10.0.0.0/8 172.16.0.0/12 | Any | Any | Any | Any | Deny |
| Block Test | Ext | 192.0.2.0/24 | Any | Any | Any | Any | Deny |
| Block Reserved | Ext | 240.0.0.0/5 | Any | Any | Any | Any | Deny |
| Block Spoof In | Ext | GIAC Internal Address | Any | Any | Any | Any | Deny |
| Blocked Spoof Out | Int | External | Internal | Any | Any | Any | Deny |
| Block Spoofed Ext | Int | External | External | Any | Any | Any | Deny |
| Block Multicast | Ext | Any | 0.0.0.0/8 255.255.255.255/32 | Any | Any | Any | Deny |
| Block small tcp/ udp | Ext | Any | Any | TCP / UDP | Any | Any | Deny |

The Border Router controls access to the network from the Internet, making router security critical. Telnet, HTTP, and SNMP access to the router should be strictly controlled. Access to the router should be through the console port or through the use of Terminal Access Controller Access Control Plus (TACACS+).

The Security policy for the Border Router should block high risk and unnecessary protocols.

When configuring the Border router, all ACLs should first be written onto a worksheet. Inputting ACLs must be in order since the Access is processed from the top down. ACLs are added to the bottom of the list. When processing packets, the rules are checked form the top down. Once a rule is matched, the packet is processed.

The Configuration of the Border Router is as Follows

**GIACRTR**

```
Version 12.1
no service finger
hostname GIACRTR
logging buffered
!                                    (Syslog server address)
logging 192.168.1.2
enable secret 5 ********
username admin password 7 ********
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no ip source-route
no service tcp-small-servers
no service udp-small-servers
no ip directed-broadcast
no ip proxy-arp
no ip unreachables
ntp disables
no cdp enable
!
interface serial 0/0
 ip address 201.1.1.1   255.255.255.0
 ip-access group 101 in
 ip-access group 105 out
 no mop enabled
Interface Ethernet 0/0
 ip access-group102 out
 no mop enabled
Interface Ethernet 1/0
 ip access-group 103 in
 ip access-group 104 out
 no mop enabled
!              (deny private and unassigned addresses)
```

```
access-list 101 deny ip 10.0.0.0        0.255.255.255          any     log
access-list 101 deny ip 172.16.0.0      0.15.255.255           any     log
access-list 101 deny ip 192.168.0.0     0.0.255.255            any     log
access-list 101 deny ip 127.0.0.0       0.255.255.255          any     log
access-list 101 deny ip 0.0.0.0                                any     log
access-list 101 deny ip 240.0.0.0       15.255.255.255         any     log
!               (deny netbios traffic)
access-list 101 deny tcp any any eq 135 log
access-list 101 deny udp any any eq 135 log
access-list 101 deny udp any any range 137 138 log
access-list 101 deny tcp any any eq 139 log
access-list 101 deny udp any any eq 445 log
access-list 101 deny tcp any any eq 445 log
!               (allow established connections)
access-list 101 permit tcp 201.1.1.0    0.0.0.255  gt 1023 est
!               (allow ipsec/ike traffic)
access-list 101 permit tcp 201.1.1.2    any eq 22
access-list 101 permit tcp 201.1.1.2    any eq 500
access-list 101 permit udp 201.1.1.2    any eq 500
access-list 101 permit esp 201.1.1.2    any
access-list 101 permit  ah  201.1.1.2    any
!               (allow mail, dns, web access)
access-list 101 permit tcp any 201.1.1.8 eq 25
access-list 101 permit tcp any 201.1.1.6 eq 53
access-list 101 permit udp any 201.1.1.6 eq 53
access-list 101 permit tcp any 201.1.1.7 eq 80
access-list 101 permit tcp any 201.1.1.7 eq 443
!               (allow icmp echo reply)
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any unreachable
!               (egress filter)
access-list 105 permit 201.1.1.0  0.0.0.255      any
access-list 105 deny icmp any any time-exceeded
!               (allow replies from web/mail/dns)
access-list 102 permit tcp 201.1.1.8 any gt 1023 est
access-list 102 permit tcp 201.1.1.7 any gt 1023 est
access-list 102 permit tcp 201.1.1.6 any gt 1023 est
access-list 102 permit udp 201.1.1.6 any eq 53
access-list 102 permit tcp 201.1.1.6 any eq 53
!               (allow traffic to VPN concentrator)
access-list 103 permit tcp 201.1.1.2 any eq 22
access-list 103 permit udp 201.1.1.2 any eq 500
access-list 103 permit tcp 201.1.1.2  any eq 500
access-list 103 permit tcp 201.1.1.2  any eq 50
```

```
access-list 103 permit udp 201.1.1.2 any eq 50
!                    (allow traffic from VPN concentrator)
access-list 104 permit tcp any 201.1.1.2 eq 22
access-list 104 permit udp any 201.1.1.2 eq 500
access-list 104 permit tcp any 201.1.1.2  eq 500
access-list 104 permit tcp any 201.1.1.2  eq 50
access-list 104 permit udp any 201.1.1.2 eq 50
login
!
end
```

## Firewall Policy

**External Interface**

Connections from the Public Internet may be initiated using HTTP and SSL to the External Web server located on the External Network services Network (DMZ). Connections may also be initiated to the Public Mail Server located on the DMZ from the Public Internet for SMTP communications. Valid DNS queries are allowed from the Public Network to the Public DNS server.
Access to any other Network in the GIAC Network Architecture is prohibited except for established connections initiated from the internal network.

**Public Network Services Interface (Public DMZ)**

Communications may be initiated from the Internet to servers on the DMZ for the Web server using HTTP and SSL request. Communications to the Mail server may be initiated from the Public Internet using SMTP. The Name server may be reached from the Public Internet using valid DNS queries.
The Public WEB server can initiate connections to the Application server located on the Private DMZ.

**Private Network Services Interface (Private DMZ)**

No connection can be initiated from the Public Internet to the Private DMZ.
Host on the Public DMZ may initiate communications to host on the Private DMZ. Connections are restricted to particular host with the needed protocols.
Host on the Private Network may only initiate communicate with host on the Private DMZ for administrative proposes using one time Passwords. Access is limited to designated systems.
No connections may be initiated from the Private DMZ to the Internal network.

**Internal Network**

No external network may initiate communications to the Internal Network-including External Network, Public DMZ, and Private DMZ.
The Internal Network has unrestricted but monitored access to the Internet.

Sessions initiated to the Public DMZ or Private DMZ from host located on the Internal Network must use One-time passwords and are limited to designated administrator machines.
The internal network configuration utilizes a Cisco 3500 layer 3 switches with unused ports disabled. Port security is enabled. This results in the port being enabled for one hardware address. Connecting different Ethernet hardware device to a port causes the port to be disabled.

**Security Levels**
The PIX firewall uses security levels to designate the trust assignment of an interface. The inside interface is the highest security level and has default setting of 100. This setting cannot be changed. The internal network should be behind the inside or trusted interface.
The outside interface is the least trusted and has the lowest security level. The External interface of the Pix firewall has a default security level of 0. Any resource outside of the External interface is unprotected.
Other interfaces of the Pix firewall can be assigned security levels from 1-99, Traffic is allowed from a higher security level to a lower security level. Therefore, traffic is allowed from the inside interface with a security level of 100, to the outside interface, with a security level of 0. To allow communications from a lower security level interface to a higher security level interface, the conduit command must be used to specifically allow the traffic. Cisco uses the nameif command to assign a name and security level to each interface. The interface command configures the properties of each interface, including interface type and speed of the connection. The IP address command follows the interface command and assigns an IP address to the interface.

**Network Address Translation**
Network Address Translation is enabled with the NAT command. NAT translates internal addresses used by the local network to globally unique addresses that are used on the internet. NAT acts as a shield to hide internal addresses form the outside global network. When a packet is received by the PIX firewall from an internal address, the PIX assigns a global address from a global address pool. The address is assigned for a default period of 2 minutes. The global address pool is a range of legal, globally unique IP address for use on the internet. The global address pool may be only one address, in which case, PAT-or port address translation-is used to map internal addresses to the correct traffic by the port sequence number.

In order to use NAT, the global address or address pool must be assigned through the Global command. A global address can be assigned to a NAT address through static mapping in order to map traffic to an internal system. This can be done using static mapping through the use of the route command. The route command defines a default route for an interface. The route command can be used to send all traffic destined for a particular IP to a specific internal address, (201.1.1.7 ->172.16.1.6) or to send all traffic traffic to a particular port to a specific host (to send all HTTP to the web server.) This action is know as Network Address Port Translation is often used to map port specific traffic to a web server (tcp 80) or a RAS server (tcp 1723 gre ).

PIX Version 5.0

! (name interfaces)

```
! (lower security cannot access higher unless specified, higher security allowed access to lower )
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security 40
nameif ethernet3 intf3 security 60
enable password ********** encrypted
hostname giacfw
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
!                   (fixup used to enable, disable, change, or list a protocol)
fixup protocol http 80
fixup protocol smtp 25
fixup protocol sqlnet 1521
arp timeout 1440
!                    (floodguard provides protection against flood attacks)
floodguard enable
names
pager lines 24
!                    (enables syslog logging)
logging buffered debugging
logging queue 512
!                    (Identify the IP address of each interface)
ip address (outside) 201.1.1.3 255.255.255.0
ip address dmz1 172.16.1.1 255.16.0.0
ip address dmz2 172.16.2.1 255.16.0.0
ip address inside 192.168.0.1          255.255.255.0
!                    (Disable RIP)
no rip outside default
no rip inside passive
no rip inside default
!                    (Set outside default route)
route outside 0.0.0.0   0.0.0.0          201.1.1.1  1
conduit permit icmp any any
!                    (timeout for half open connections)
timeout xlate 3:00:00
conn    1:00:00 half-closed
0:10:00 udp 0:02:00
!                    (timeout for pix resources to remain idle)
no snmp-server location
no snmp-server contact
snmp-server community public (*****)
!
mtu outside 1500
```

```
mtu inside 1500
mtu pix/intf2 1500
!                       (let inside users start connections on lower security levels)
nat (inside)    1       0       0
nat (dmz1)      1       0       0
nat (dmz2)      1       0       0
!                       (give access to dmz to inside users)
global (dmz1)  1
172.16.1.10-172.16.1.254
netmask 255.255.255.0
global (dmz2)  1
172.16.2.10-172.16.2.154
netmask 255.255.255.0
!                       (give inside nat access to outside)
global (outside 1
201.1.1.10-201.1.1.254
netmask 255.255.255.0
!                       (let outside users access dmz mail)
static (dmz1, outside)
201.1.1.8       172.16.1.5
netmask 255.255.255.255
!
conduit permit tcp host
201.1.1.8 eq smtp any
!                       (let outside users access Public Web)
static (dmz1,outside)
201.1.1.7       172.16.1.6
netmask 255.255.255.255
conduit permit tcp host
201.1.1.7 eq www any
!
aaa-server  TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
no snmp-server enable traps
telnet timeout 5
terminal width 80
Cryptochecksum:**********************************
:end
```

Installation of a firewall can create unforeseen problems; a method for identifying and applying firewall exceptions is needed to deal with communication problems that may be created. A Firewall exception form should be available for users to report problems and the IT staff should inform the help desk of the procedure for addressing problems caused by the implementation of

the firewall. The IT staff should plan the firewall implementation at a time when the maximum installation and testing time will be available, notify users of the event, and prepare to work long hours to correct problems.

## Virtual Private Networks

Site-to-Site, Virtual Private Network connections are completed with Business Partners and large Vendors through the use of a VPN enabled Cisco 3600 series Router. The Access is authenticated through the AAA Radius Server Appliance with access rights controlled through Group Access. Each Site-to-Site VPN will establish a Security Association with the VPN enabled Cisco 3600 router acting as a Security Gateway. To establish a Security Association the IP address orf the Client Security Gateway must be configured into the GIAC Security Gateway to establish a Security Association. The Cisco Config Maker Software facilitates this setup using a graphical interface for ease of use. Non-standardization of VPN support by manufactures could make some Security Associations more difficult to configure. In cases where the Security Association configuration causes a delay, a Client connection configuration could be configured on an individual need basis using Cisco Secure VPN client software. Remote VPN service is also available for a limited number of users.

IP addresses are assigned which allows access into the Public DMZ.

VPN Policy
Encryption algorithm: 3DES-Data Encryption Standard (128 bit)
Hash algorithm: Secure hash standard
Authentication Method: Pre Shared Key
Lifetime: 86400 seconds

The Customer or Business partner will set a pre-shared key to establish a security association between routers. In the event that a customer does not utilize a Cisco router, or a router that is IPSEC compliant and is able to establish a security association with the Cisco VPN concentrator, a desktop system may be configured using Cisco Secure software to connect through the VPN concentrator. In order to configure a VPN security association, the router of the security gateway at each end of the VPN tunnel must be configured to communicate. The IPSec protocol Authentication Header or Encapsulation Security Payload must be designated, as well as the type encryption (DES, 3DES), the hash algorithm, and the authentication method. Each tunnel must also be mapped to the security gateway of the business partner or customer the tunnel is created with. These configurations combine to create a security association between the sites and the VPN concentrator.

**Extranet VPN Configuration**

Version 12.0
Service timestamps debug uptime
Service timestamps log uptime
No service password-encryption
!

```
hostname GIACVPN
no logging buffered
!crypto isakmp policy 1
!                          (Designates using a preshared key vs a certificate authority)
authentication pre-share
!                                  (the time before the key is regotiated)
lifetime 84600
crypto isakmp key ******** address 204.24.2.5
crypto isakmp key ******** address 204.23.2.7
!                                  (this describes the encryption type )
crypto ipsec transform-set giaccust ah-sha-hmac esp-des esp-sha-hmac mode transport
crypto ipsec transforms-set giacpart ah-sha-hmac esp-des esp-sha-hmac
!
crypto map s1first local-address serial1/0
crypto map s1first 1 ipsec-isakmp
set peer 204.24.2.5
set transform-set giaccust
match address 101
!
crypto map s4second local-address serial2/0
crypto map s4second 2 ipsec-isakmp
set peer 204.23.2.7
set transform-set giacpart
match address 111
!
interface tunnel0
bandwidth 180
!                                  (Business Part desktop system address)
ip address 204.17.3.3 255.255.255.0
tunnel source 204.23.2.7
tunnel destination 201.1.1.2
crypto map s1first
!
interface ethernet0/0
ip address 201.1.1.2 255.255.255.0
no ip directed-broadcast
no keepalive
full-duplex
no cdp enable
!
interface serial2/0
ip address 201.1.1.2 255.255.255.0
no ip directed-broadcast
no keepalive
no cdp enable
```

```
crypto map s4second
!router bgp 10
network 201.1.1.2 mask 255.255.255.0
!ip router\201.1.1.2 255.255.255.0 tunnel0
ip nat inside soruce static 201.1.1.7
access-list 101 permit gre host 204.24.2.5 host 204.24..2.5
access-list 111 permit ip host 201.1.1.2 host 204.23.2.7
!line con 0
line aux 0
line vty 0 4
login
!
end
```

## Remote Access

Remote access is available through a modem installed into the Remote Access Enabled Cisco 2500 series router. The AAA Radius Server Appliance controls access through authentication, with access controls assigned by groups. Remote access enables smaller suppliers and vendors access to the Public DMZ, as well as allowing remote employees access to their mail through an HTTPS connection to the private mail server.

The Router PPP configuration follows

```
Version 11.2
Service timestamps debug datetime msec
No service password-encryption
No service udp-small-servers
No service tcp-small-servers
!
hostname giacrtr2
enable secret
!
radius-server host giacaaa
radius-server key *****
!                    (designates radius server authentication)
aaa authentication login giac3a radius
aaa authentication ppp if-needed radius
aaa authorization network radius
aaa authorization exec radius
!
login authentication giac3a
interface group-async1
  ppp authentication chap
!
interface Ethernet0
ip address 201.1.1.4  255.255.255.0
```

```
interface group-async1
ip unnumbered ethernet0
encapsulation ppp
async mode interactive
peer default ip address pool dialup
!
no cdp enable
ppp authentication chap
group-range 1 16
!       (set a range of ip addresses for the dialup pool)
ip local pool dialup 192.168.0.239 192.168.0.254
line con –
login
line 1 16
login local
modem inout
password ***
login
!
end
```

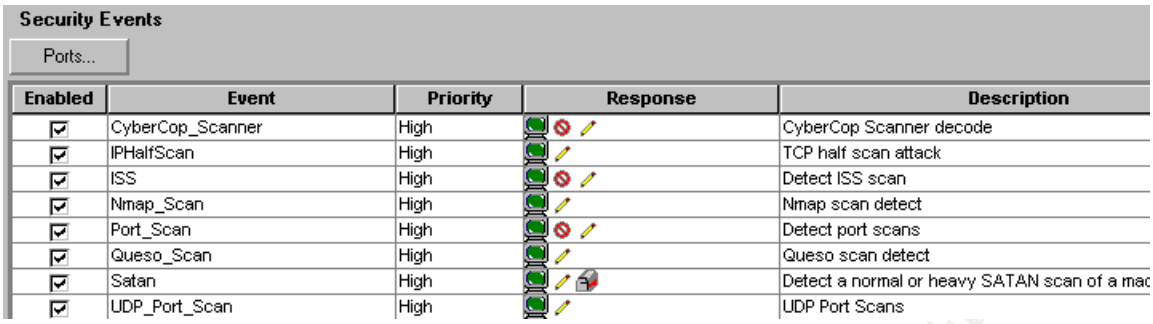
## Incidents and Intrusion Detection

**Intrusion Detection**

The network shall maintain Intrusion Detection Systems to aid in identifying unauthorized use of GIAC Enterprises network resources.

The Intrusion Detection System will consist of Internet Security Systems Real Secure® Network Sensor located on a switch outside the firewall with all switch traffic mirrored to the port where the IDS sensor is connected. The system will be running in stealth mode with a second Ethernet card connecting to the Real Secure console over a dedicated run to an Information Security monitoring console. A modified DMZ policy will be used which will generate a RSKILL in the event of a network scan, 10 pings to one address within 1 minute, or 20 pings to multiple addresses within 1 minute are detected. Other security events will generate events and logs which will be monitored and appropriate actions taken. A second Real Secure Network Monitor will be located on a switch connected to the Internal Port of the Firewall with all traffic mirrored to the port where the IDS sensor is connected and will monitor all traffic that reaches the internal network. The resulting reports and logs will be evaluated to determine the effectiveness of Firewall and Router configuration in stopping unwanted or unauthorized traffic through the Perimeter. Certain Scanning and discovery events are configured for resets to be sent, and others are configured for an e-mail and page to alert the network manager of a possible attack. The responses include: log-represented by a pencil icon, send an email or pager alert- represented by the mailbox icon, and the kill response-represented by a stop (red circle with a line through it) icon.

Real Secure Network Monitor Policy for scanning events:




**Vulnerability Scanning**

Internet Security Systems Scanner will be utilized to scan each system upon initial connection to the Network to ensure compliance with configuration control policies. Any High vulnerability must be corrected within one day or the system will be removed from the network. Medium vulnerabilities must be corrected with 1 week. Low vulnerabilities should be corrected if possible. The entire network space should be scanned at least once per quarter. Each quarter, the Information Security Specialist performing vulnerability scans should prepare a comprehensive report for the Information Security Manager detailing vulnerabilities on the network.

**Virus Protection**

Most viruses are introduced through E-Mail. GIAC Enterprises will employ Trend Micro Scan Mail for Exchange 3.0 to scan all mail and attachments before they infiltrate the Network. McAfee Antivirus will be used on desktop systems to scan for viruses introduced through media, shared files, or other means.

**Administrative**

**Network use and Responsibility**

Guidance is given to all employees stating that GIAC Enterprises computing resources are for official business use in support of assigned work duties, and resources are not to be used in any manner that is not consistent with company policy. This also applies to external use of the World Wide Web. Anyone who has access to the Internet using GIAC Enterprises computing resources must be aware that transactions to and from the Internet are traceable and are routinely monitored.

**Acceptable Use Policy**

Guidelines for appropriate use of the World Wide Web and Email is made known to employees and states that as a responsible member of the community, employees are expected to apply common sense and civility to the use of the internet and e-mail. Use of the Internet and e-mail is expected to be legal, ethical, and responsible.
Configuration Control

All computer systems connecting to GIAC Enterprises networks will be under configuration control. Configuration control should be checked before connecting to the company network. A security scan for vulnerabilities should be completed immediately upon connecting to the company network. The following minimum requirements should be checked for compliance:

**All Systems:**

No shared passwords
User ID and password for all accounts
Vendor supplied account passwords removed
Password protected screen saver enabled for 10 minutes

**NT Systems**:

The NTFS file system must be used.
Account Policy
Maximum password age 180 days
Minimum password length 8 characters
Account lockout after 5 incorrect attempts
Reset count after 20 minutes

User Rights
Manage auditing and security logs: Administrator
Restore files and directories: Administrator
Take ownership of files: Administrator
Generate Security Audits: Administrator
Log on as a service: Administrator

Audit Policy
Logon and Logoff: Success and Failure
Use of User Rights-Failure
User and Group management-Success and Failure
Security Policy changes-Success and Failure

**UNIX Systems:**

Passwords are not echoed to the screen
The /dev/ttys file limits root login to system console
The /etc/host.equiv file has been removed
The .rhosts file has been removed

The etc/inetd file has the following commented out-
tftp
fingerd
ruserd
rlogind

**Vendor Agreements**

All vendors and business partners should submit a summary of their Information Security Plan, which describes their risk mitigation techniques for the following:

Access controls
- Physical access
- Network access
- Computer access

Virus Protection
- E-mail virus scanning
- Media scanning
- Desktop scanning
- Network and system vulnerability testing

**Awareness and Education**

User Computer awareness training is available on the internal Web server. Users must complete the User Awareness Training before their user account is activated. All users must complete a computer security awareness refresher in order to revalidate their account each time the password expires.

## Security Audit

A security audit will be designed to test each risk mitigation solution.
Due to the extensiveness of the audit, written approval from the management is needed. A written notification of the intended audit, including times and the origin of external scans, should be sent to the ISP to avoid blocking of scans and possible legal action.

**Plan the assessment**:

Objective
Test for the correct and effective implementation of the Security Policy.
Review the procedures for responses to attacks on network resources.
Review system logs, Intrusion Detection techniques and procedures, password policies, and system configuration guidelines.
Analyze the results of the assessment and determine any recommendations for changes as a result of the assessment.

Estimated time spent on the assessment and evaluation would be approximately 22 hours.
Cost for the audit would be approximately $2200 in manpower.

Scope of the assessment
Perform a network assessment from an external location. Include test of Firewall policies, router filters, and network security.
Test automated filters during off shift times to avoid disruption of services (pinging resources).
Test access from the Network Services subnet to external resources (this should be blocked).
*Note: Running an ISS scan of Network resources can cause routers to reset. This test should be performed when network access is minimal with a network technician present.*

Network Access:
Attempt to gain access to an area with a computer or network connection. Connect a laptop to an available Network Port.

1. The Ethernet card is not registered and should not be assigned an IP address by the DHCP server. No connection should be made.
2. The Port security should disable the port so that a system cannot be attached with sniffer software.

Computer Access:
Check for password-protected screensavers that protects the computer from unauthorized access after an authenticated user leaves his system unattended.

Audit an NT workstation for minimum password length. (Administrative tools/local security)
Ensure that the guest account is disabled. (Administrative tools/local security)
Check to ensure NTFS file system is being used.(Right click 'C' drive/properties/file system)

Run an ISS Scan on the Internal network to check for vulnerabilities.

External Access:
Attempt to access the DMZ using HTTP to access the Vendor database from the Public Web Server.

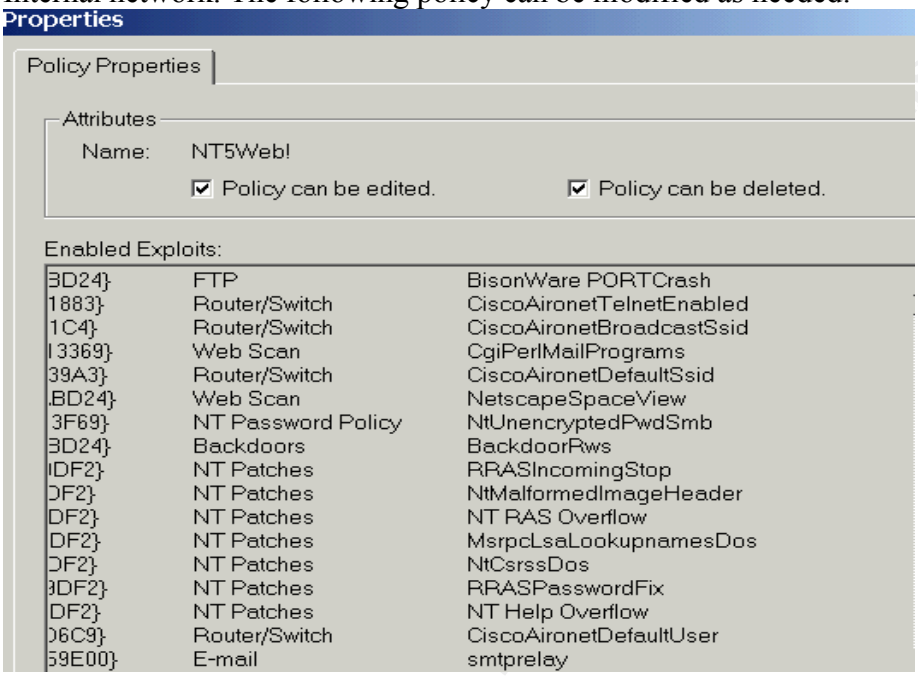
1. Public access to unprotected information should be available using HTTP.
2. Some secure access available through the use of HTTPS for secure ordering over the Internet.
3. Vendor specific information should be available only through VPN and Remote access authentication.

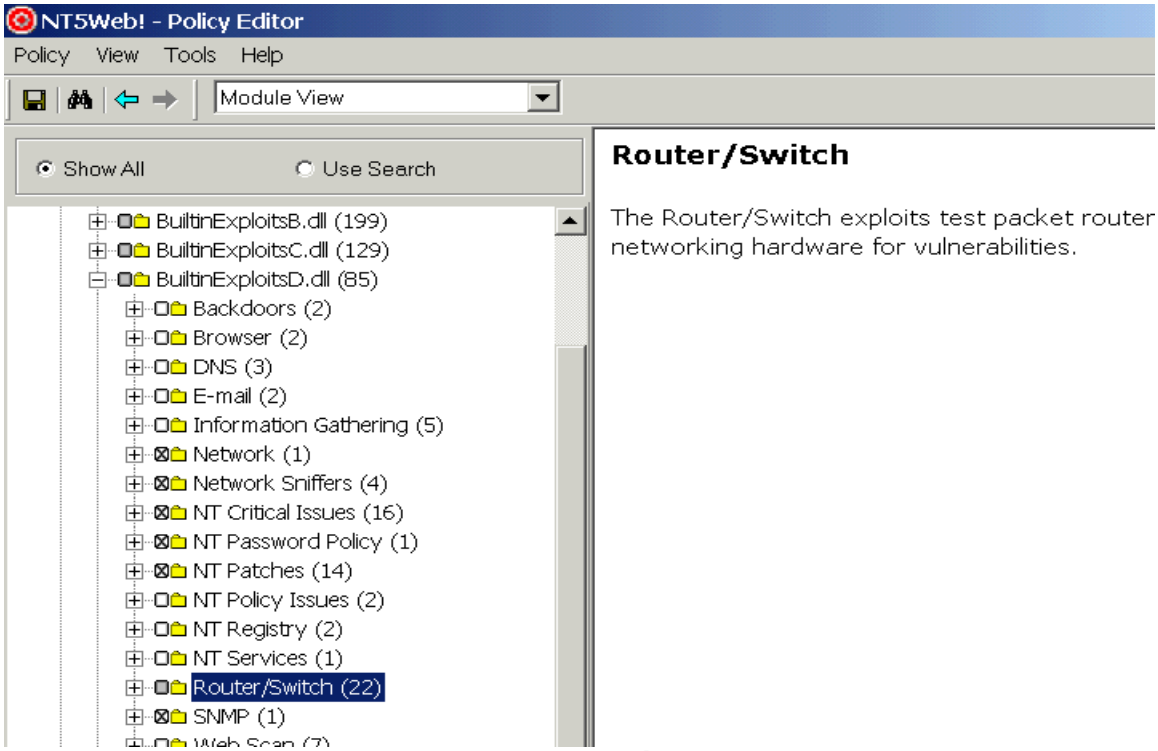
Attempt to access the internal web server form the Internet.

1. No access should be available to Internal resources.

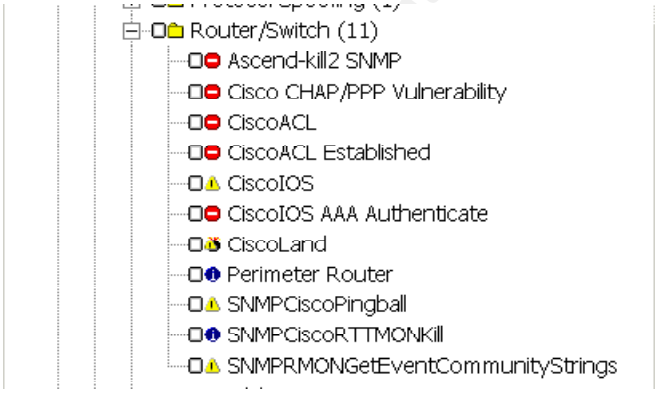
Run ISS scan from a system external to the GIAC Enterprises router. The ISS L5 NTWeb Server policy includes most of the testing that would adequately check the External access controls. The scan should take place external to the router. Another scan should take place outside the border router. The scanning system can be set up to scan over the weekend or during off shift hours. The primary concern is that the shared servers such as the GIAC Web server be on during the scanning. After a test against the firewall and externally available Web, Mail, and DNS servers,

the connection should be moved outside the Border router for a test of the complete perimeter defense system. Configuration of the Scanning system should take about 1 hour, plus the connection to the external interface. After the external testing, the scanning system can be used to scan the internal network for potential vulnerabilities. The External scan should be repeated after any IOS upgrade of routers or the Firewall. A scan of the Externally accessible Web servers, DNS servers, and Mail servers should be repeated at least quarterly, as well as after OS upgrades, patches, or evidence of suspicious activity is seen in the firewall or system logs. A license for ISS Scanner should be purchased for the GIAC IP range, including the NAT addresses used on the Internal network. The following policy can be modified as needed.






Select the following Router Vulnerability Checks.

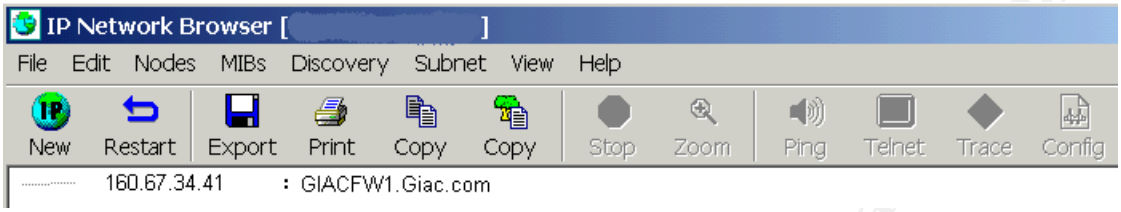



1. The Public Web server, DNS server, and SMTP server should be the only systems accessed from outside.

Run an SNMP scan against the Border Router and GIAC Firewall to ensure proper configuration

of SNMP

Use Solar Winds to perform an SNMP scan of the Firewall. Solar Winds is available in a 30 day evaluation version which would be adequate for the testing of the Router and Firewall initial configuration.
HTTP://www.solarwinds.net




Solar Winds will try to discover the community string of the router and Firewall. If the community string is left at the default setting, the tool may be used to discover the Router Table of the router or Firewall.

Initiate at least 20 pings on the Firewall address from an external address.
Initiate a series of pings that walk through the network address space from a single address.

Verify that a filter script was generated to block the offending address at the border router.
Verify that the script sent an E-Mail to the Network Manager with a notification and description of the block.
Verify that a page was sent to the Duty pager notifying of the block.

Attempt to access the GIAC Firewall and Internal resources.
Testing the rule:

1. Attempt to access an internal address from an external location with an internal address as the source address. Use Nmap –D option to spoof an internal address.
2. Attempt to access an external address from an internal location using an external address as the destination address. Use Nmap –D option to spoof an external address.

This test will check for proper ingress and egress filtering. This prevents the network from being used as an agent in a Trino attack, or prevents an address from being spoofed in order to gain access to network resources.

3. Attempt to access the network from an external location using an RFC 1918 address.
4. Scan the system using ISS or Sharesniffer. This test will identify netbios shares on systems on the internal network if the netbios ports are not blocked at the router.

Telnet into the GIAC Firewall

1. Should receive a warning Banner stating that the operation is not permitted.
2. The session should be terminated.
3. The event should be written in the event log of the syslog server.

Telnet to an Internal system

1. The session should be terminated.
2. The event should be written into the syslog

FTP into the GIAC Firewall

1. Should receive a warning Banner stating that the operation is not permitted
2. The session should be terminated
3. The event should be written into the syslog

FTP into an Internal resource

1. The session should be terminated.
2. The event should be written into the syslog

HTTP into the Giac Firewall

1. Should receive a warning banner stating that the operation is not permitted.
2. The session should be terminated
3. The event should be written into the syslog

rlogin into the GIAC Firewall

1. Should receive a warning banner stating that the operation is not permitted.
2. The session should be terminated
3. The event should be written into the syslog

rlogin into internal resources

1. Connections to internal host are rejected

The testing of the Network perimeter should be planned for a Friday if possible. The Network engineer and 1 technician should be able to complete the test in 4 hours. Additionally, the configuration of the scanning system and connection to the external interface would add 2hours, with another hour for removing the system and returning it to the original configuration. Checking the ISS scan report on the following Monday morning would require another hour, with the report to management requiring 4 hours for preparation and presentation.

Considering that the Network Engineer and Technician are salaried employees, the manpower estimate is more important than the cost estimate.

Review Firewall Syslog

1. Firewall logs should indicate the source address of the system used to attempt access to the internal Web Server.
2. Logs should indicate the source address of the system trying to telnet into the Firewall.
3. Logs should indicate system running ISS scan from an external address.

***The Following is part of the Firewall Logs indicating attempted Telnet sessions. These attempts are denied by the firewall.***

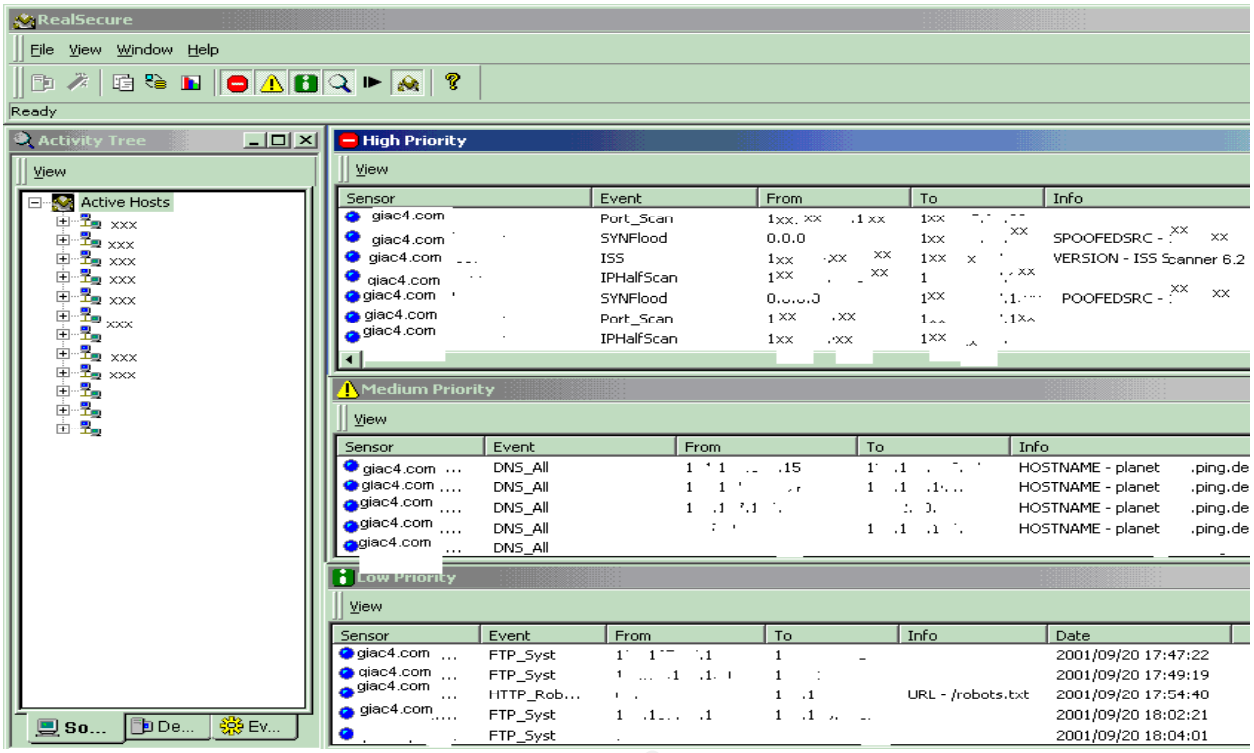
```
Sep 9 02:01:22 GIACFW1-inside.com %PIX-4-1XXXXX: Deny udp src outside:
1XX.1XX.1XX.1XX/138 dst inside:1XX.1XX.1XX.1XX/138 by access-group "outy"
Sep 9 02:01:46 GIACFw1-inside.Com %PIX-4-1XXXXX: Deny tcp src outside:
1XX.1XX.1XX.1XX/49138 dst inside:1XX.1XX.1XX.1XX/23 by access-group "outy"
Sep 9 02:01:46 GIACfw1-inside.Com %PIX-4-1XXXXX: Deny tcp src outside:
1XX.1XX.1XX.1XX/3858 dst inside:1XX.1XX.1XX.1XX/23 by access-group "outy"
Sep 9 02:01:46 giacfw1-inside.Com %PIX-4-1XXXXX: Deny udp src outside:
1XX.1XX.1XX.1XX/4422 dst inside:1XX.1XX.1XX.1XX/23 by access-group "outy"
Sep 9 02:02:44 giacfw1-inside.com %PIX-4-1XXXX: Deny tcp src outside:
1XX.1XX.1XX.1XX/2512 dst inside:1XX.1XX.1XX.1XX/23 by access-group "outy"
```

***Following are Firewall logs indicating an attempted ISS scan of the internal network space. These connections were denied by the firewall***

```
Sep 9 17:37:59 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:38:02 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:38:02 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:42:59 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:42:59 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:43:02 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:43:02 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:47:59 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:47:59 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:48:02 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:48:02 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:52:59 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:52:59 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:53:02 giacfw1-inside.com %PIX-3-1XXXXX: Dst IP is
network/broadcast IP, translation creation failed for icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 9 17:53:02 giacfw1-inside.com %pix-3-1XXXXX: Deny inbound icmp src
outside:1XX.1XX.1XX.1XX dst inside:1XX.1XX.XXX.XXX (type 8, code 0)
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1451 dst outside
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1472 dst outside
:1XX.1XX.1XX.1XX/102 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src inside:
```

```
1XX.1XX.XXX.XXX/1457 DST outside
: 1XX.1XX.1XX.1XX/22 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny top src inside:
1XX.1XX.XXX.XXX/1473 DST outside
: 1XX.1XX.1XX.1XX/103 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny top src inside:
1XX.1XX.XXX.XXX/1479 DST outside
: 1XX.1XX.1XX.1XX/113 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny top src inside:
1XX.1XX.XXX.XXX/1452 DST outside
: 1XX.1XX.1XX.1XX/13 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny top src
inside:1XX.1XX.XXX.XXX/1466 dst outside
:1XX.1XX.1XX.1XX/79 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1460 dst outside
:1XX.1XX.1XX.1XX/37 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1448 dst outside
:1XX.1XX.1XX.1XX/1 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1474 dst outside
:1XX.1XX.1XX.1XX/104 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1462 dst outside
:1XX.1XX.1XX.1XX/53 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1453 dst outside
:1XX.1XX.1XX.1XX/15 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1475 dst outside
:1XX.1XX.1XX.1XX/105 by access-group "iny"
Sep 10 07:51:55 giacfw1-inside.com %PIX-4-1XXXXX: Deny tcp src
inside:1XX.1XX.XXX.XXX/1470 dst outside
```

***Following are Real Secure Network Sensor logs of the same ISS scan from external to the Firewall. The ISS scans are indicated by a port scan, the identified ISS scan, and the IPHalfScan.***




**Observation:**

The external ISS Real Secure Network sensor in conjunction with the Firewall logs provides adequate logs to identify what is attempting to enter the network, But a second RealSecure Network Sensor located internal to the Firewall would provide a view of what gets through the firewall. Although this could be accomplished with the firewall logs, the sensor would make the detection a bit easier to see and provide an automated alert. This also gives a layered approach to the perimeter protection of the network. The RealSecure Network Sensors should be equipped with two NICs in order to run the monitoring NIC in stealth mode.
The Firewall logs are only configured to log what is 'Denied' access. This may be good to let us know who is 'knocking on the door,' but it leaves the question unanswered as to who got in. The ISS scan report would indicate that only the Web server, Mail server, and DNS server were accessible form the internet, that means that those systems are the most susceptible to attack.

### *Auditing the Configuration Control of the network*

The following ISS scan of an NT system from an internal address indicates an NT 4.0 OS that has not applied the current Microsoft Service Pack. The system administrator of the system in question should be instructed to apply the latest Microsoft Service Pack and the system should be rescanned to ensure configuration control

**ISS Scan Results**

# Network Vulnerability Assessment Report **Sorted by IP Address** 6/19/2001

## Report Description

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High-risk vulnerabilities are those, which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those, which provide access to sensitive, yet non-lethal, network data. It is recommended that all high-risk vulnerabilities be corrected as soon as possible.

ISS Scan

**Session Name:** Session1 **Session ID:** **6**

**File Name:** Session1_010525 **Template:** L5 NT Web Server

**Comment:** **Termination Status:** Finished

**Scan Summary Information**

**Hosts Scanned:** **Scan Start:** 2001/05/25 08:51:05
**Hosts Active:** **Scan End:** 2001/05/25 08:56:13
**Hosts Inactive:** **Elapsed: 00:05:08**

| Host IP Address | DNS Name | Operating System |
|---|---|---|
| *.*.*.* | giac.com | Windows NT 4.0 |

**Vulnerability Name**

**Severity**

**Additional Info** **More Info** **Session ID**
6

**Vulnerability Name**

**Severity**

Critical key permissions incorrect Medium

**Description:**

A registry key that can lead to higher access levels is writable by non-administrators. Each of these keys can be used to insert a Trojan horse program that is then invoked when another user logs in. The AeDebug key can be used to directly gain higher access if the attacker can cause a service running at a privileged user level to crash.

The vulnerable keys under HKEY_LOCAL_MACHINE are:
- Software\Microsoft\Windows\CurrentVersion\Run
- Software\Microsoft\Windows\CurrentVersion\RunOnce
- Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- Software\Microsoft\Windows NT\CurrentVersion\AeDebug
- Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

**Fix**
Set permissions on each of these keys. Grant Administrators and System users full access, and Everyone read access.
To set key permissions, follow these steps:
1. Open Registry Editor. From the Windows NT Start menu, select Run, type regedt32, and click OK.
2. Go to the registry key listed in the description.
3. From the Security menu, select Permissions to display the Registry Key Permissions dialog box.
4. Examine the permissions for the following characteristics:
- Verify that Administrator and System are Full Access.
- Verify that Everyone is Read access.
- Remove unauthorized names, or change the Type of Access to Read.
5. Click OK when you have completed setting the permissions.
6. Repeat steps 2 to 5 for all the keys listed above

| Additional Info | More Info | SessionID |
|---|---|---|
| Software\Microsoft\Windows\CurrentVersion\Run | | 6 |

The result of the internal network scan indicates that an internal system is not configured correctly. The resulting vulnerability indicates that the system has not applied the most recent service pack or has inadequate access controls. The system should be examined for the service pack version and access rights.

***Recommendation as a result of the Audit of the Perimeter and the security of the Network:***

The Firewall Logs should be configured to log all access to systems located on the External Services Network. This would allow review of logs for traffic to the Web server and the mail server. It would also allow for the review of VPN traffic, which is an avenue for un-trusted access into the network. Review of the firewall logs should be done every morning, with VPN and all 'allowed' traffic coming into the network being examined for malicious activity.
Due to the public accessibility of the systems located on the Network Services network, the installation of a product such as 'Tripwire' or 'Real Secure System Scanner' should be applied. The use of Real Secure Network Sensor and the availability of a Real Secure Workgroup Console make the Real Secure System Scanner a logical choice. The Real Secure System Scanner is "host-based risk assessment and policy management system." The function of the Real Secure System Scanner is "to monitor system access rights, user privileges, file system access rights, service configurations, and suspicious activities that indicate and intrusion." The System Scanner will report these changes to the real secure console. By monitoring the Real Secure Console, reported changes can be investigated to determine if the changes indicate an authorized change or suspicious activity. The Real Secure System Scanner should also be installed on the system located on the Internal Services Network, since these systems have access to the External Services Network.

Configuration Control on the internal network should include the initial setup and configuration of the OS, as well as the application of patches and Service Packs in order to keep the OS current. Providing a means to 'push' patches and service packs to the desktop may be costly. An alternative would be to send out instructions on patches and service pack installs and to provide a network share where current patches and service packs are stored. Regular Vulnerability scans can alert IT staff of systems that need to apply the latest service pack or OS

patch.

The Firewall IOS is revision 5.0, this indicates that the IT staff have not applied the latest IOS upgrades to the Firewall. The Firewall IOS should be upgraded to the most current version as soon as possible. The most recent version of the PIX IOS is Version 6.0, which comes with some added features and security patches.

The GIAC network internal architecture includes a Microsoft Internet and Acceleration Server, but the ISA server is not included in the present configuration. The IT staff should configure the ISA server to wok with the radius appliance and Cisco router to provide a more secure NAT as well as to check access controls on internal system. The ISA server also has the capability to provide proxy services for internal network resources. ISA server 2000 has several plug-in applications that should be evaluated and considered for internal traffic monitoring.

Another possible security enhancement is the implementation of CBAC (Context Based Access Control) on the Border router. The Cisco IOS running on the Border Router supports CBAC filtering, which is a part of the Firewall Feature Set, but it is not being implemented at this time. There is a possible performance penalty for running CBAC.

Part of the assessment should be to measure the load on the Border router and firewall. Since much of the filtering occurs on the Border router, the Firewall does not appear to be under a heavy load, therefore the Context Based Access Control would probably run on the firewall without a significant performance decrease.

The Audit of the Perimeter Protection is a snapshot in time and should not be considered as a one time only validation of the security of the network. As network devices are replaced or added to the network, service packs and patches are applied to Operating systems, and additional partners and services are introduces, the perimeter security should be reevaluated for indications of newly introduced vulnerabilities.

Reference: Internet Security Systems System Scanner 4.1

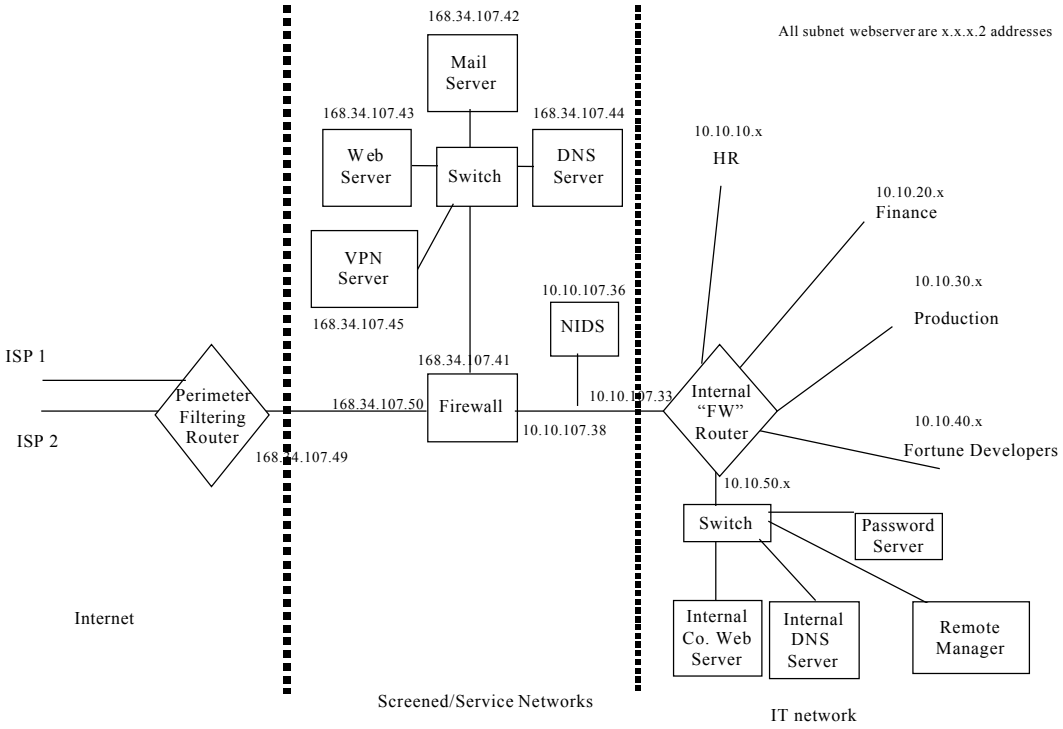
## Design Under Fire

I have selected the following design

http://www.sans.org/y2k/practical/Heather_Bard_GCFW.doc

The primary reason for selecting this particular design is the use of the Raptor Firewall and possible vulnerabilities of the Firewall. I am assuming that this does not have all the current patches (not likely considering Ms. Bard's vulnerability assessment.) I am also assuming that one of the Web Servers inside the firewall would be running Internet Information Server. One weakness of the design is that the VPN traffic does not appear to pass through the Intrusion detection system. This leaves the traffic entering the site from Business Partners and Customers unmonitored. If someone compromises the Business Partners or customers site, the Giac site is vulnerable to an attack through a trusted system without ever seeing the traffic.

**Figure 1. GIAC Security Architecture**




## *Axent Firewall Vulnerabilities:*

Three identified vulnerabilities of the Axent Raptor Firewall are listed. The first is used to attack the firewall, causing it to crash. The Third is utilized in the Attack 2 Scenario to allow the attacker to gain access to an Internet Information Server Web Server connected to the Raptor Firewall.

1. "Axent Raptor firewalls can be crashed by packets containing zero length IP options." (ISS Xforce raptor-ipoptions-dos(3350)). The ip Timestamp and Security options can be set to zero length. This causes the Axent Raptor Firewall to enter an unrecoverable loop and freeze-creating a denial of service.

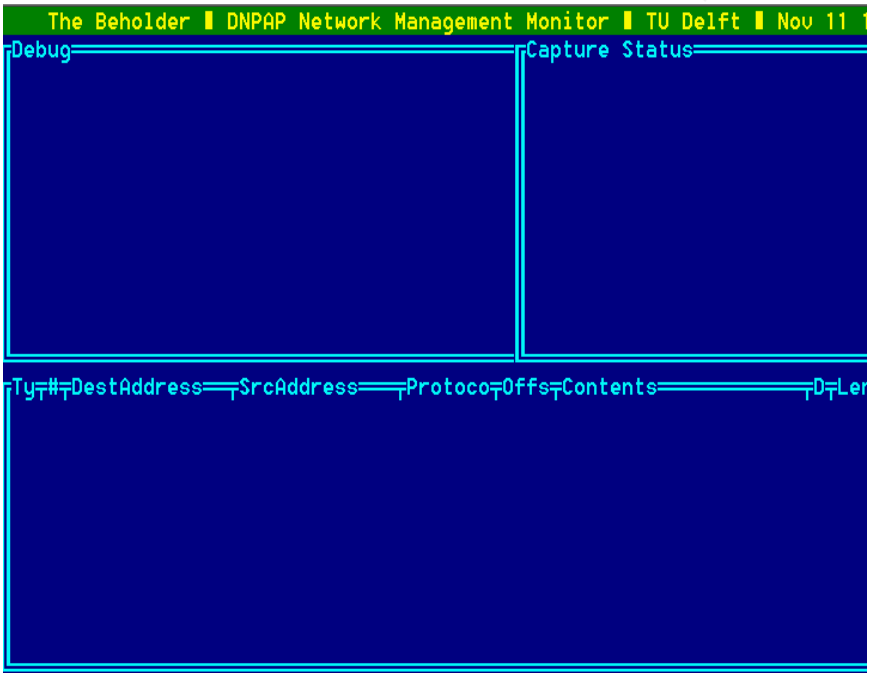
   **Applying the most recent Raptor Firewall IOS upgrade can mitigate this vulnerability.**
2. An open telnet account has been detected on the Raptor Firewall. A scan of the firewall indicates an easily guessable password on the telnet account. (ISS Xforce firewall-raptoropen(389)). **Changing all vendor-supplied passwords can mitigate this.**
3. Axent Raptor Firewall http.noproxy vulnerability (Bugtraq:20010324) The vulnerability allows attackers to use the firewall as a proxy to access internal web resources when the http.noproxy rule is set. **To mitigate this, disable the HTTP Proxy or disable other**

**listeners at the web server.**

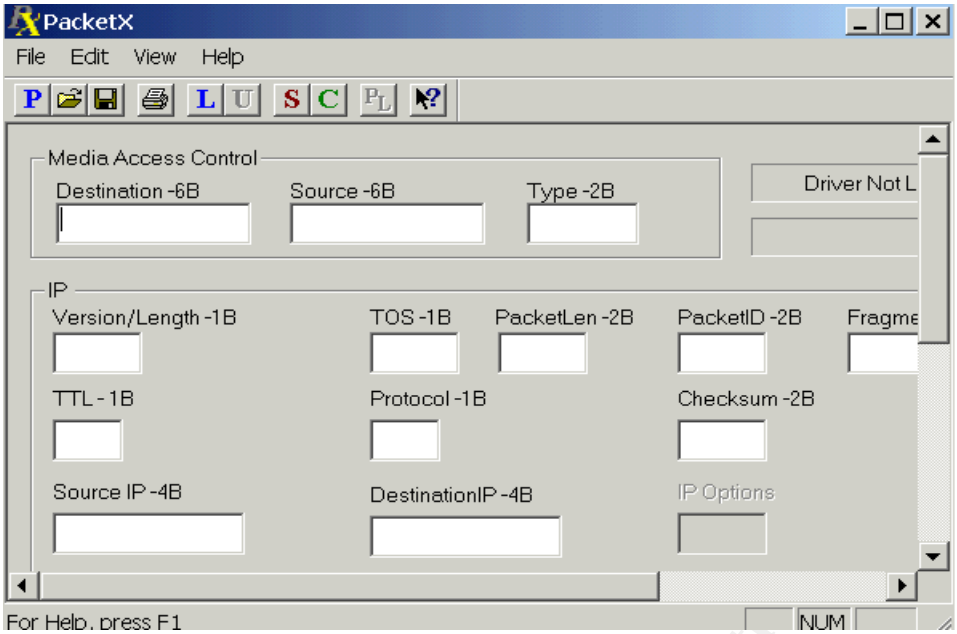
***Attack 1***: Craft an IP Packet having a Zero length IP header. Use a tool like Nmap or SNOT to generate an IP Packet. If using Snot, use the Snort rule setting the IP Header Length (ihl: "0") should indicate the header length in 32 bit words. This field follows the Version (set to 4). Also, use the snort rule setting for Time to Live value (ttl: "<number>") set the TTL value to "0". This field is followed by the protocol type, which should be set to 6 for TCP. Set the source address as any valid globally unique IP address, and the destination as the IP address of the Web server.

The newest version of Nmap has the capability to send packets as well as performing probes, and the packets can be modified to change the source address, destination address, as well as some custom crafting that would allow for a '0' TTL

An easy tool for crafting packets is Goobler, which can be found at:http://packetstorm.decepticons.org/




PacketX, also from Packetstorm has a menu that allows you to PLUG in the source, destination, header size, TTL, and port number.




After crafting a packet with a zero length IP header and Zero time to live, send the packet to the firewall. The firewall will crash.

**Applying the most recent Raptor Firewall IOS upgrade can mitigate this vulnerability.**

## *Attack 2:*

*Attempt to exploit the Axent Raptor Firewall http.noproxy vulnerability.*
*Bugtraq:20010324*
*The vulnerability allows attackers to use the firewall as a proxy to access internal web resources when the http.noproxy rule is not set.*
*This exploit uses the nearest interface of the firewall as a proxy. This makes it possible to access a system connected to firewall within ports 79-99 and 200-65535.*
*"Attacker configures browser to use IP address of the Raptor firewall as HTTP Proxy, then begins probing internal network"(ref: Securityfocus.com)*
To exploit this vulnerability, configure the Raptor firewall as the proxy to access the internal Web Server. Also, use the vulnerability to run Stealth or Super Scan against the network.

**To mitigate this attack**, *disable the HTTP Proxy or disable other listeners at the web server. This attack utilizes different ports besides port 80 to gain access to the Web Server.*

## *Attack 2B.*

This attack utilizes a vulnerability in the Microsoft Unicode Transformation Format. The XML file should be UTF-8 for this attack to be effective
*( An unpatched Raptor Firewall used as a proxy will return the Webserver header to the attacking machine)*

*By discovering the address of the Web server an identified IIS 4.0 or 5.0 server can be compromised by using UTF command:.*
*http://168.34.107.43/scripts/..%u005c..%u005cwinnt/system32/cmd.exe?/c+dir+c:*

*http://168.34.107.43/msadc/..%255..%255..%255..%255cwinnt/system32/cmd.exe?/c+copy+c:\winnt\repair\sam._+c:\inetpub*

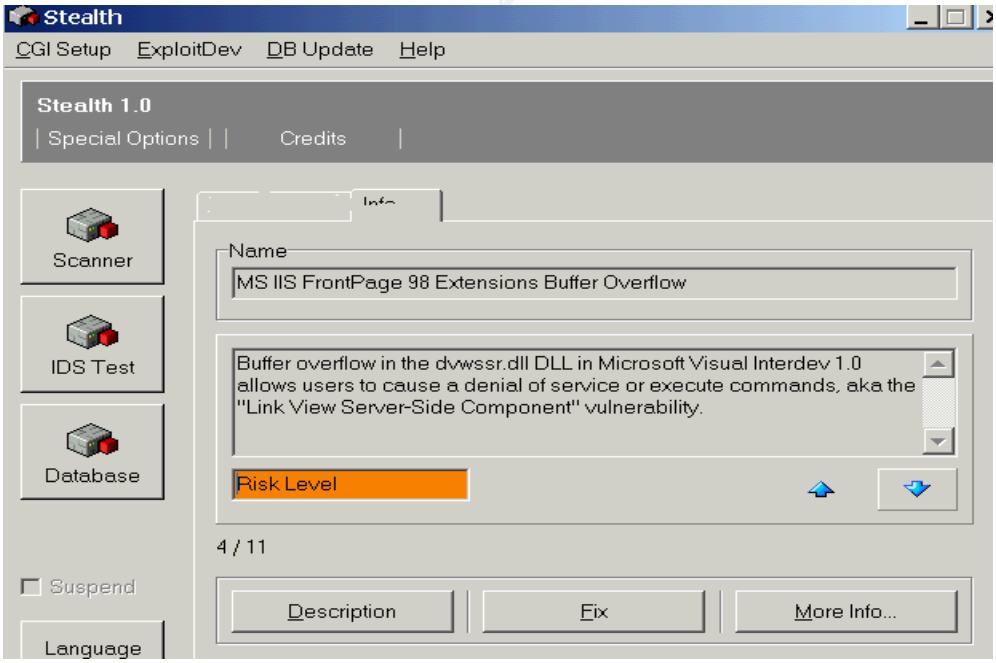
*A directory list of C:\ will be revealed.*
*An attacker can run commands under the IUSR_ account.*
*You can also run a command under the cmd.exe under the IUSR account*
*GET /scripts/..%co%af..%co%af..%co%af../winnt/system32/cmd.exe?+/c+dir'c:\' HTTP /1.0*

**To mitigate this attack:** Apply the latest patch to the Raptor Firewall. Also, apply the Unicode patch from Microsoft to correct the vulnerability in IIS.
*The patch for this vulnerability is available from Microsoft:*
*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iischk.asp*

## *Attack 3*

After identifying the IP address of the Web server, use Stealth to identify Web vulnerabilities in the Web Server that may be used to launch an attack. Stealth will find the vulnerability and tell the Stealth user the correct exploit to use to compromise the target system.

Stealth can be downloaded from http://www.nstalker.com/stealth.php



By accessing the Stealth Report, the Stealth User can examine the identified vulnerability for an exploit.

DVWSSR Test

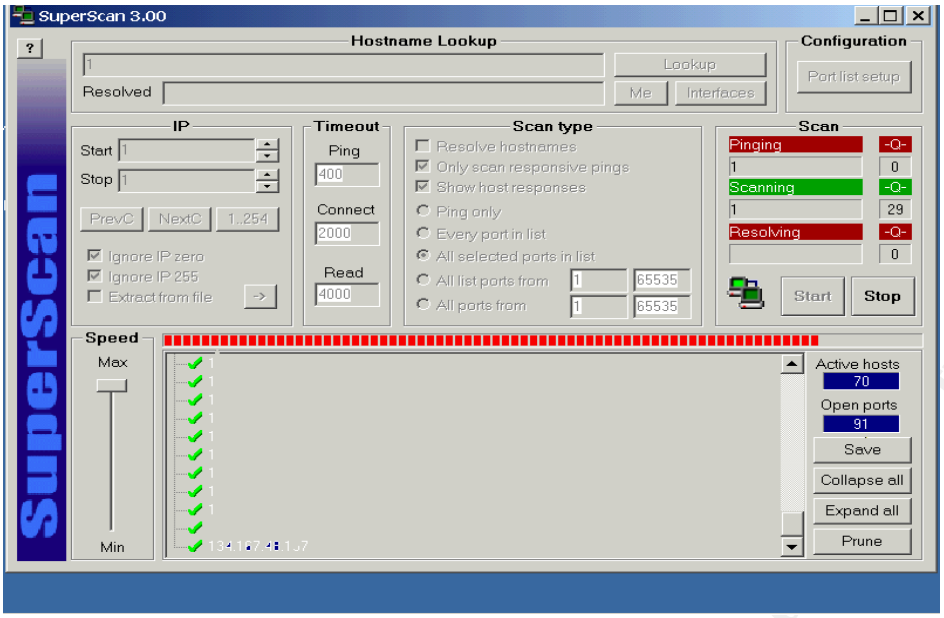
MS IIS FrontPage 98 Extensions Buffer Overflow

CVE: CVE-2000-0260
Risk Level: Medium
Location: http://168.34.107.43/_vti_bin/_vti_aut/dvwssr.dll
BugTraq ID: 1109

Buffer overflow in the dvwssr.dll DLL in Microsoft Visual Interdev 1.0 allows users to cause a denial of service or execute commands, aka the "Link View Server-Side Component" vulnerability.

Access the report from the Stealth scan to identify exploitable vulnerabilities. If a system is found to have a mis-configured web server, access to the entire C: drive may be possible. In the event that a writ able area of a system is compromised, Install 'BUTTSNIFFER' on the writable area of the system. "Buttsniff 0.9.3 (http://www.evilhackr.com/hacking.html) is a remote installable sniffer that can be installed and launched without the system owner knowing that it is active on the system. First, the _Dump.DLL must be installed, then the ButtSniff.exe command is launched with a _d to designate the interface to monitor. This will log any activity on port 80. by accessing the logs from ButtSniff, we are looking for an Admin password that will give access to the development and production machines. In the event that a user logs in, the user ID and Password is logged and can be retrieved.

Another useful tool to find an open share to install the sniffer on is SuperScan 3.0, available from the following site http://www.webattack.com/get/superscan.shtml. Superscan identifies shares and when a share is found, allows the user to click on the share and map a drive.



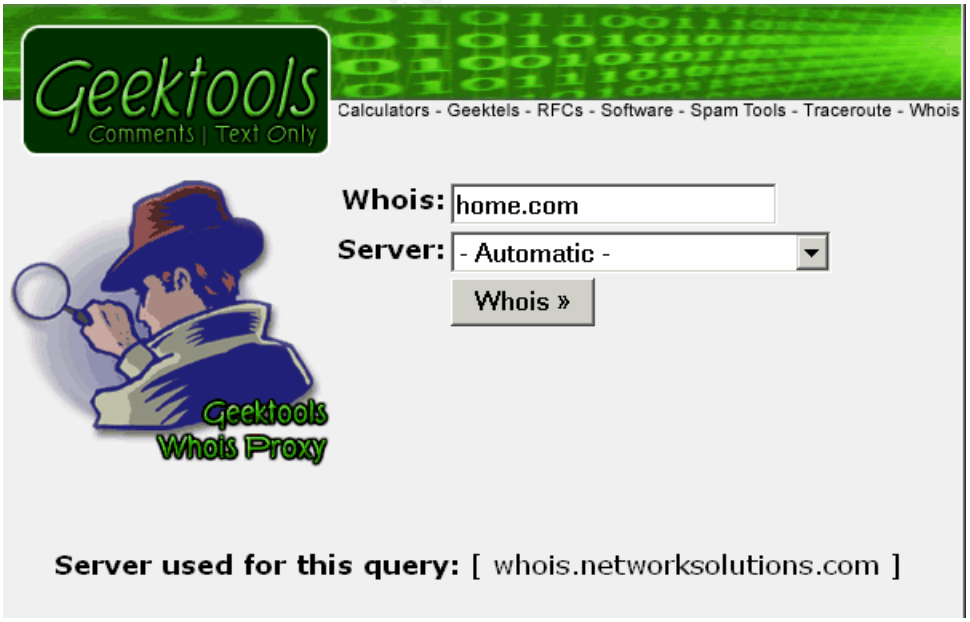

By creating a visual basic script to exploit the vulnerability, utilize unsuspecting Cable Modem users to launch a Denial of Service against the Web Server.

1. Research the IP address range of a Cable modem ISP. This can be accomplished from http://www.geektools.com using the whois lookup

2.Search for the range of addresses assigned to home.com

```
Domain servers in listed order:

   **.HOME.COM                  **.**.**.**
   **.HOME.COM                  **.**.**.**
   **.HOME.COM                  **.**.**.**
```



3. Run sharesniffer against the range of addresses. (http://sharesniffer.com/)

4. After identifying available shares, utilize the cablemodem subscribers to launch an IP Fragment-driven Denial of Service Vulnerability on the GIAC.com address space.

5. By identifying default configured schedule service on several subscribers, configure a Windows Ping using the –l switch to set the ping size at 65500 and the interval at every 2 minutes. If the compromised systems have their time set correctly, you should be able to flood the network at 2-minute intervals.

A Distributed Denial of Service attack on the Giac site would result in the flooding of all bandwidth and possible crashing of the Firewall. Proper configuration of the Axent Raptor firewall should result in the system crashing 'closed' to prevent access to the site. The result is a Denial of service that prevents users from accessing the system as well as preventing anyone from access the Internet from inside GIAC enterprises.

Of course, attacking through a firewall is more difficult than entering through the front door. By running WindSurffer on the Perimeter Filtering Router, we can get the routing table of a router that does not have proper community strings set to require passwords. Since this is the most likely place for security to be lacking, it is very probable to find the default community string. By using the router table we can identify the router and system of the business partner or customer who has trusted access to the GIAC site and perform discovery probes of the Business partners and customers sites to identify vulnerable systems. After compromising a vulnerable system, use the trusted access to enter the Giac site through the front door. A scan of business partners and customers sites could turn up a system with an open share (perfect for installing a sniffer) or a blank Admin password. In the case of a blank admin password, use the following command to map the vulnerable system drive:
(net use \\IP Address\ipc$ " " /user:administrator.) you can then give yourself a user account and run the remote access software to access the GIAC web server with more privileges than a regular web user.

A very common vulnerability, the SNMP community string used by most routers and network devices is often left to the default string. In many instances, snmp community strings are not secured if the service is not being used, and the default snmp community string is left on the system. By accessing snmp information, the router table can be used to provide addresses to users, business partners, and customer that can be used to gain access into their site, and then into the target site. If a malicious user entered the GIAC site through a VPN tunnel from a business partner or customer, it is unlikely the NIDS log would alert the IT staff. Since the design in question does not monitor decrypted VPN traffic, the activity of a VPN user while on the 168.34.107 network would not even be notices. The malicious user would have unobserved access to the Web server, Mail server, and DNS server. Having unencumbered access to the DNS server could be the most damaging of the three, since DNS poisoning would result in traffic being diverted to another site.

The goal is to gain access to the 10.10.10 network. The malicious user who has gained

access to the web server and can exploit the proxy vulnerability of the firewall can most likely run an internal scan and find vulnerability. A user system is more likely to have an open share or a blank administrator or guest account. To exploit a blank guest account, use the net use \\IP address\ipc$ " " /user:guest to gain access to the system.

Another common vulnerability is Shares enumerated by a null session. After compromising the external web server, use the proxy vulnerability of the firewall to perform network discovery. If an open netbios share is identified (shares enumerated by a null session) attempt to create an unauthenticated session using the null session exploit: net use \\10.10.10.10\ipc$ " " /u: " ". This command connects to a hidden share as an anonymous user. The hidden netbios share would be a great place to install a remote sniffer or to launch attacks on other systems.

**To mitigate the shares enumerated by a null session, edit the registry to restrict anonymous:**

*Edit the registry*
*HKLM\system\current control set\control\lsa*
*Add the folloing key*
*Value name: restrict anonymous*
*Data type: Reg_Dword*
*Value:1*

Another Easy exploit is to install a sniffer in the power chute directory of a system using the UPS software in the default configuration. Power chute installs and sets up a share with 'everyone' that is often overlooked by system managers. This area is usually writable and can be easily exploited for malicious purposes.

Of course, an easy target again is the SNMP community string of the internal router. If we can log in to the Internal router with a RW community string, changing configuration to reroute traffic is possible. SNMP is not limited to routers, NT systems may also have SNMP vulnerabilities. SNMP is used for SMS on NT networks, as well as certain backup programs.

The design selected for the Design under fire portion of the practical would not be susceptible to these attacks if the Firewall and web servers were patched with the latest software, unneeded access points were disabled, and proper configuration controls were in place.

Compromising an internal machine is easy to simulate by assuming that a particular system has vulnerability, but system discovery scanning is designed to identify vulnerabilities and the malicious user has a tool kit to exploit whatever vulnerability is available. Since the possibility of someone on the system having an open share or blank admin password is very good if a consistent configuration control policy is not adopted, the best plan is to find a share or vulnerable system and install a sniffer. I selected ButtSniffer0.9.3 because it could be remotely installed and executed and was readily available. I also assumed that I was dealing with NT systems. If the system that I compromised were a Unix system, a better sniffer to install would be Egg drop. A good site about egg drop is the following.
http://johoho.eggheads.org/eggdrop/attacks.htm
to download the tar file visit the following:
http://www.xes.cx/eggstuff.htm

A good Intrusion detection system and diligent employees should notice someone using FTP to transfer Egg Drop or Buttsnif to the network.
Of course, host based intrusion detection systems would report the installation of a DLL or an executable, as well as the creation of a new user account. Since most hackers try to cover their tracks, a common thing that a hacker does is to delete the log files from when he entered the system. The intruder can use the tool elsave (http://www.ibt.ku.dk/jesper/Nttools/ ) to clear the event log (c:\elsave –s \\giacweb -l "Security" –C).
A good Host IDS sensor should also detect this action, as well as the creation of user accounts and administrative logon.

Real Secure Network Sensor will identify the presence on the network of a sniffer in most cases; so running Real Secure Network sensor on the internal network would help to mitigate the installation of a malicious sniffer.

Proper border router configuration, a good firewall, network and host Intrusion detection, and diligence in keeping current with patches and IOS updates are all part of an effective Perimeter protection policy. But without a dynamic and effective configuration control policy that is supported by management and enforced on every system, a penetration into the network can result in multiple systems being compromised, data being altered, the loss of integrity of sensitive information. The perimeter of the network should be considered to consist of all systems that have access to the resources of the network. That includes not only the border router, firewall, and Remote access servers, but also trusted host that are give access through VPN and remote access servers, and all user systems and servers connected to the network, and any system that connects to the network for testing, training, demos, or any business purpose.

## References


Karanjit Sijan, Chris Hare, "Internet Firewalls and Network Security" New Riders Publishing 1995

Cisco Systems, "Safeguarding the E-Business Network Cisco Safe: A Primer to Implementing a Secure Cisco Network" Osborne/McGraw Hill 2000

Cisco Systems, Cisco-Safe: A Security Blueprint for Enterprise Networks
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

Cisco Systems, A Beginner's Guide to Network Security
http://www.cisco.com/warp/public/cc/so/neso/sqso/netsp_pl.htm

Cisco Systems, Cisco VPN and Security Reference Guide
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/sevpn_wp.htm

Visa Account Information Security Best Practices Guide Version 1.3:
https://www.visa.com/nt/gds/standards.html

Network Working Group Request for Comments: 2827 Network Ingress Filtering

http://www.ietf.org/rfc/rfc2827.txt?number=2827

Network Working Group RFC: 1918 Address allocation for Private Internets
http://www.ietf.org/rfc/rfc1918.txt

Common Vulnerabilities and Exposures
http://www.securityfocus.com

Internet Security Systems, Inc. :X-Force
http://gvws11.iss.net/

Packet Storm
http://packetstorm.decepticons.org/

Joel Scambray, Stuart McClure, George Kurtz "Hacking Exposed" Osborne /McGraw Hill 2001