GIAC Enterprises with VACLs and PVLANs

Giac Certified Firewall Analyst Practical Assignment v4.0
Clint Couse
12/19/04

Abstract: GIAC Enterprises access control and layer two security.
GIAC enterprises is a small company that recently redesigned their network to offer protection at all network layers. After a worm infection, layer two security was improved by upgrading switches and implementing PVLANs, VACLs, and Port Security. Router ACLs, Firewalls, and DMZ gateway servers combine to protect layers three and up.

Access requirements have been carefully examined and modified to provide only required access for all groups of users. The requirements for each group have been examined and documented. The restrictions for each group have also been noted. Finally an audit on the main Internet firewall has been performed. Each rule was examined and verified to meet the companies security stance.

Assignment 1: Future state of security technology: From the topic wish-list, I have selected VLAN ACLs (VACLs) and Private VLANs (PVLANs) and their use in network defense. The minimal switch that would support these is the Cisco Catalyst 6500. GIAC enterprises recently suffered a major worm infection and has determined workstation access should be locked down to only the necessary servers and subnets.

Private VLANs were originally designed for use by service providers to provide “Efficient IP Address Aggregation”[1]. Service providers that hosted co-located servers and customer managed servers wanted to be able to provide segregation between each customer’s servers. This was burdensome, as it required providers to develop a large number of discrete networks with only a few IP addresses on each subnet. The result was inefficient use of IP address space causing many unusable IP addresses. The solution was Private VLANs. They enable the service providers to put servers from many customers on the same subnet while still segregating their access.

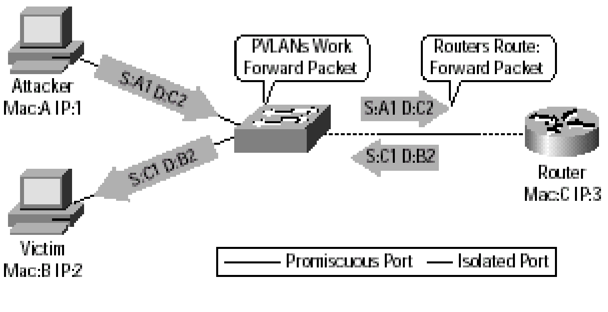
Private VLANs or Super VLANs (depending on the vendor) allow segregation of the traffic on a subnet. The segregation is performed on layer 2 and configured at the switch. Let’s consider Cisco’s implementation of private VLANs. When configuring the switch port, you must select the port be one of three types: isolated, community, or promiscuous. Each type provides different levels of access.

- Isolated: Devices on isolated ports are only allowed to talk to devices connected to promiscuous ports.
- Community: Devices on community ports are allowed to talk to devices that are part of the same community or promiscuous ports. Multiple communities can be created on the same subnet allowing for granular control.
- Promiscuous: Devices on promiscuous ports are allowed to talk to any other device on the subnet.

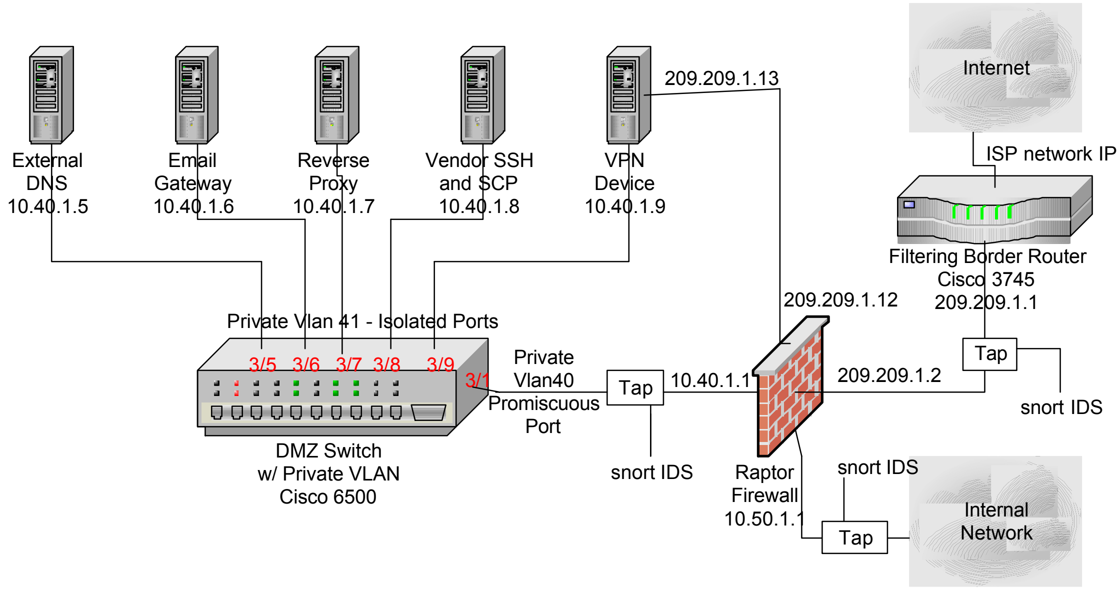
There are some security concerns that must be considered when deploying private VLANs. First and foremost, they have many of the same security implications as normal VLANs. While many people have criticized VLAN security, Cisco's VLAN implementation has been analyzed by @stake for vulnerabilities. "The results of @stake's test sequences clearly demonstrate that VLANs on Cisco Catalyst switches, when configured according to best-practice guidelines, can be effectively deployed as security mechanisms."[2] Private VLANs have an additional security issue that must be understood when designing secure networks. Private VLANs are vulnerable to a form of spoofing called private VLAN attack.[3] If a packet is sent from an isolated port to the IP address of a machine on another isolated port with destination MAC address of a local router (or other IP forwarding device), the router will pass the traffic and so will the switch. The switch considers the packet to be traveling isolated to promiscuous (source server to router) and then promiscuous to isolated (router to destination server). Because of this, any device connected to a promiscuous port must be scrutinized and evaluated to ensure it doesn't IP forward packets, or if it does, this must be considered in the design.

Here is a diagram from Cisco that depicts the private vlan attack[3]:

Figure 4
L2 Proxy



There are many benefits to private VLANs. They were designed to perform layer two segregation. They do a good job as long as the private VLAN attack vulnerability is considered. The most beneficial use of private VLANs is in a DMZ directly connected to a perimeter firewall. The DMZ should use a firewall as default gateway. This will prevent the previously mentioned private VLAN attack. Each DMZ host should be connected to the switch on an isolated port. The firewall port will be set to promiscuous. The net result is complete isolation for every machine in the DMZ. Each DMZ machine will only be allowed to talk to the firewall or through the firewall to select machines based on the firewall ruleset. This can be considered equivalent to have a unique firewall interface for every machine in the DMZ.



Consider the previous diagram. This DMZ was created using a private VLAN on a Cisco 6500 switch. Security is greatly improved by isolating all of the gateway servers from each other. If someone were to compromise the email gateway they would not be able to directly attack the reverse proxy, VPN server, or any other device in the DMZ. This configuration defeats man-in-the-middle attacks as well as stopping the spread of worms within the DMZ. Using a private VLAN in the DMZ provides the best segregation and earliest possible alerting when a NIDS tap is placed between the switch and firewall. A compromised machine should be immediately exposed as there are no targets available without going through the NIDS and firewall. Another benefit is the internal interface of the VPN device can be terminated within the DMZ instead of dedicating another firewall interface for it. All VPN connections are forced through the NIDS and firewall, which also helps protect against a compromised machine or worm at one of the remote offices.

Private VLANs are easy to configure on Cisco switches. You must first create a primary VLAN containing all private VLAN ports. One secondary VLAN is created for all of the isolated ports. Each community requires another VLAN as well. Devices on isolated ports transmit on the secondary VLAN and receive traffic from the primary VLAN. Typical Cisco switches can handle several thousand VLANs (primary or secondary).

Consider the 6500 in GIAC's DMZ. Port numbers have been added to the drawing in red. Lets assume we want to use VLAN 40 for the primary VLAN and VLAN 41 for the secondary isolated VLAN. Only a few commands are required for configuration[4]:

- Set vlan 40 pvlan primary
- Set vlan 41 pvlan isolated
- Set pvlan 40 41 3/5-9
- Set pvlan mapping 40 41 3/1
- Show pvlan

GIAC's DMZ is safe from the private VLAN attack because the default gateway is a firewall (which drops everything not implicitly allowed) instead of a router. If we were connected to a router, we could secure our switch to prevent the private VLAN attack by creating a VLAN ACL (VACL) with the following commands[5]:

- Set security acl ip no_spoof permit ip 10.40.1.0 0.0.0.255 any
- Commit security acl no_spoof
- Set security acl map no_spoof 41

Another good use of private VLANs is on user subnets. While this shouldn't be the primary source of security, it adds value in a layered security model. User subnets are typically not monitored as closely as server subnets or the DMZ and may include a wide range of operating systems and devices. The cost of placing NIDS on every subnet can be prohibitive, and often laptops or other user devices are not secured or patched properly. Without layer two segregation an aspiring hacker is free to test his "hacks" and "cracks" on other local workstations, passing only through the switch, and typically avoiding detection by the network or security admins. Private VLANs (PVLANs) prevent this. Worms are unable to spread from workstation to workstation. Man-in-the-middle attacks are thwarted, along with a plethora of other ARP-based attacks. Rogue DHCP servers and DHCP starvation attacks are stopped cold.

When configuring PVLANs on user subnets, the gateway will typically be a router. Because of this, we must again be aware of the private VLAN attack. There are two very simple ways to stop the private VLAN attack. The first is to configure ACLs on the router to prevent traffic destined for a VLAN with the same source VLAN. This is a good choice as we should already have ACLs on the router to prevent traffic from one user VLAN to another. The second method is to configure VACLs on each VLAN to prevent this traffic. Using VACLs on each VLAN stops any illegitimate traffic on the switch at wire speed. This can be very beneficial as it prevents the traffic from traversing the link between switch and router. This is especially beneficial in stopping DoS attacks.

VLAN access control lists (VACLs) are very similar to access control lists and perform all the same type of functions. However, they are performed in hardware at layer 2 and thus able to control traffic within a subnet. All of the benefits of PVLANs can be achieved by using VACLs. In fact, VACLs provide an even more granular level of control than PVLANs and have no inherent weaknesses such as the private VLAN attack.

Cisco says, “When you configure a VACL and apply it to a VLAN, all packets entering the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet coming in to the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL applied to the routed interface and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny.”[6]

Here are some diagrams from Cisco that show this behaviour:[6]

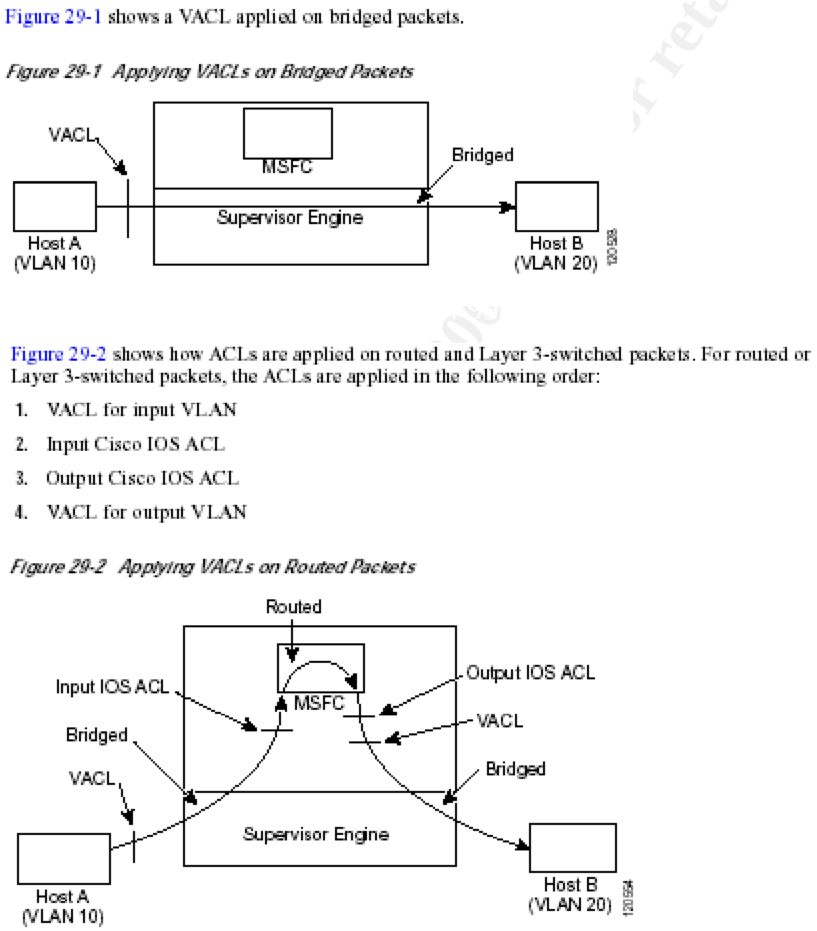


Figure 29-1 shows a VACL applied on bridged packets.

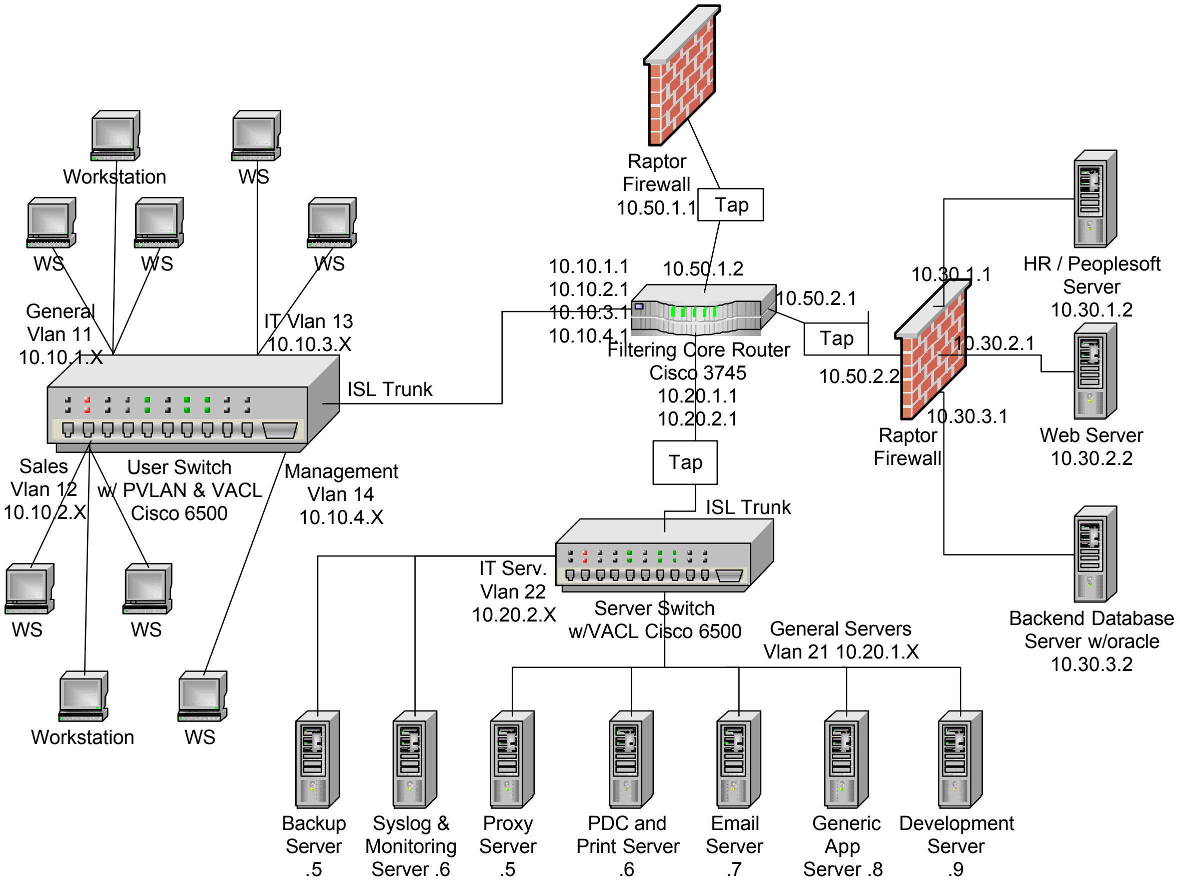
Figure 29-1 Applying VACLs on Bridged Packets

VACL
MSFC
Bridged
Supervisor Engine
Host A
(VLAN 10)
Host B
(VLAN 20)
120528

Figure 29-2 shows how ACLs are applied on routed and Layer 3-switched packets. For routed or Layer 3-switched packets, the ACLs are applied in the following order:

1. VACL for input VLAN
2. Input Cisco IOS ACL
3. Output Cisco IOS ACL
4. VACL for output VLAN

Figure 29-2 Applying VACLs on Routed Packets



As stated, VACLs can provide excellent layer 2 segregation. Examine the drawing above. We have determined that it is not necessary for any workstation to communicate directly with another workstation. This traffic can all be blocked with a VACL. With a good subnetting scheme we are able to implement this rather easily on a Cisco 6500. We would like to permit traffic from the router, but deny all traffic with both source and destination on the user subnets. Finally we will allow all other traffic.

- Set sec acl ip user_subnets permit ip host 10.10.1.1 any
- Set sec acl ip user_subnets permit ip host 10.10.2.1 any
- Set sec acl ip user_subnets permit ip host 10.10.3.1 any
- Set sec acl ip user_subnets permit ip host 10.10.4.1 any
- Set sec acl ip user_subnets deny ip 10.10.0.0 0.0.255.255 10.10.0.0 0.0.255.255
- Set sec acl ip user_subnets permit ip any any
- Commit sec acl user_subnets
- Set sec acl map user_subnets 11
- Set sec acl map user_subnets 12
- Set sec acl map user_subnets 13
- Set sec acl map user_subnets 14
- Show sec acl – to verify

We must also look at VACLs and PVLANs to see if there is any cost in terms of network performance. “VACLs can be configured on a Catalyst 6500 at

L2 without the need for a router (you only need a Policy Feature Card (PFC)). They are enforced at wire speed so there is no performance penalty in configuring VACLs on a Catalyst 6500. Since the lookup of VACLs is performed in hardware, regardless of the size of the access list, the forwarding rate remains unchanged."[4] "Even in the case that one of the servers is involved in a Distributed Denial of Service (DDoS) attack as a source, the switch will drop all illegitimate traffic at wire speed, without any performance penalty."[4]

Many of the benefits of PVLANs and VACLs have been shown above. They can be summarized by saying that PVLANs and VACLs enforce a good host trust model in a switched environment [5]. After defining which hosts need to communicate and the required protocols, we deny all other traffic. Proper NIDS placement becomes even more effective and we thwart many issues resulting from the insecurity of the ARP protocol.

These technologies should become more mainstream as we progress towards protecting assets at all layers of the OSI model and practice defense-in-depth. Security personnel should spend some time learning how to protect assets at layer two. Once this initial time investment is complete, they reap large rewards as these technologies require little maintenance other than occasionally changing a VACL and greatly improve security.

Assignment 2: Security Architecture. GIAC Enterprises is a small business which markets fortune cookie saying to customers worldwide. GIAC employs fifty people with the majority located in or near its head office and the remainder located in or near the four regional satellite offices geographically distributed around the world. All of GIAC enterprises sales are done via the Internet.

Due to a recent worm problem, GIAC redesigned their network with the trust model. All access requirements have been strictly defined and everything else is denied. This model is deployed through the use of PVLANs on Cisco 6500 switches, VACLs on Cisco 6500 switches, ACLs on Cisco 3745 routers, and Raptor firewalls to protect both the DMZ and the several crucial servers including: web server, backend database server running oracle, and the HR server which contains confidential employee information.

Access requirements were the first consideration. Six different groups of people need access including the following: customers (who purchase bulk online fortunes), suppliers (who supply the fortunes), partners (who translate and resell fortunes), GIAC internal employees (several different employee classifications have been considered), GIAC remote employees (sales), and the general public.

Customers include both individuals and companies that purchase bulk online fortunes. Customers typically interact with GIAC Enterprises through the company's web page. The website is reached through the reverse proxy in the DMZ. Once reaching the web server, customers are able open an SSL connection to the login page for authentication. The web server opens an oracle connection to the backend database. Once authenticated, Customers are able to purchase fortunes, change customer information, view past purchases, or randomly sample a few of the bulk fortunes. Customers require connections from anywhere on TCP port 80 (HTTP) and TCP port 443 (HTTPS) to the reverse proxy in the DMZ.

Customers may also send email to GIAC employees. To do this a connection from anywhere on TCP port 25 (SMTP) to the email gateway is required. Customers also require access to DNS for sending email or browsing the webpage. DNS requires a connection from anywhere to UDP port 53 (DNS) on the external DNS box in the DMZ. In rare cases, DNS can switch to TCP port 53 (DNS), so we want to also open this up as well from anywhere to the external DNS server.

Suppliers provide the fortunes that GIAC Enterprises sells. Suppliers log into the main website and authenticate over an SSL connection. From here, they are able to determine what volume of fortunes they need to deliver. Connections from anywhere on TCP port 80 (HTTP) and TCP port 443 (HTTPS) to the reverse proxy are required to log into GIAC's website. To deliver the bulk fortunes, suppliers open an SSL connection to the Supplier's SSH box in the DMZ and transfer the fortunes via SCP. This is done by connecting to TCP port 22 (SSH/SCP). For security, GIAC supplies unique public keys and logins to each customer. For additional security, the firewall only allows SSH connections from pre-defined vendor IP Addresses and blocks all other SSH connections.

Similar to customers, suppliers are able to send emails and require DNS services. Email requires TCP port 25 (SMTP) to the email gateway and DNS requires UDP port 53 (DNS) to the external DNS server.

Partners are international companies that translate and resell fortunes. Just like customers and suppliers, partners will mainly interact with GIAC Enterprises through the website. Once authenticated through SSL, they are able to check their account information and buy fortunes to download. This is done through TCP port 80 (HTTP) and TCP port 443 (HTTPS) to the reverse proxy which connects to the web server which connects to the backend database server. Partners are also allowed email on TCP port 25 (SMTP) and require DNS on UDP port 53 (DNS).

GIAC also has employees with workstations on the internal network. Because of the newly adopted trust model, employee access is very restricted. Employees are currently broken up into four separate groups: general employees, IT staff, management, and the sales force. Each group has it's own VLAN which determines what servers and subnets they may connect to. These access policies are enforced by ACLs on the core router. The user switch also employees a VACL which blocks all access between workstations. Both firewalls also restrict access to all employees by default. All employees are allowed access to the general servers on all ports.

General employees require no special access. They are allowed access on all ports to the general servers on VLAN 21 only. These servers include the proxy server, PDC and print server, email server, generic app server, internal DNS server, and development server. ACLs in the core router enforce these access policies.

IT staff has the most access of all of the employee groups. This small group of employees performs all necessary functions including: server maintenance and upgrades, all server backups, security, device configuration, and various other IT tasks. This requires access to all servers and devices. Access to the DMZ (VLAN 40/41), general servers (VLAN 21), IT servers (VLAN 22), and all protected networks behind the internal firewall (all 10.30.X.X networks) are allowed. Access through the main Internet firewall from IT workstations to the DMZ is restricted to TCP port 22 (SSH). Access through the internal firewall to the 10.30.X.X network is enabled on TCP port 22 (SSH). TCP port 80 (HTTP) and TCP port 443 (HTTPS) are also allowed to the web server (10.30.2.2). IT employees may SSH to the snort sensors by hopping through the syslog server which also runs the ACID database. The filtering border router may only be accessed via console. All access from internal workstations and servers to external addresses is blocked by default. Exceptions to this rule may be obtained by showing business justification.

Management has access to all general servers (VLAN 21) on all ports, but access to the DMZ (VLAN 40/41) and IT servers (VLAN 22) is strictly blocked by ACLs in the core router. Access to all devices behind the internal firewall (10.30.X.X) is allowed by the core router and internal firewall. The internal firewall restricts access to TCP port 22 (SSH) on the 10.30.X.X network, plus TCP ports 80 (HTTP) and 443 (HTTPS) on the web server.

Internal Sales has access to the general servers on VLAN 21 on all ports. ACLs in the core router block access to IT servers (VLAN 22) and the DMZ (VLAN 40/41). The internal firewall allows sales access to the web server on TCP port 80 (HTTP) and TCP port 443 (HTTPS).

GIAC Enterprises also has 4 regional offices which house some of the sales force. These remote employees are allowed access to all generic servers and the internal production web server. Once authenticated on the web server, they are able to perform all sales functions through scripts that connect to the backend database. These regional offices each have a Symantec SFVA 200R

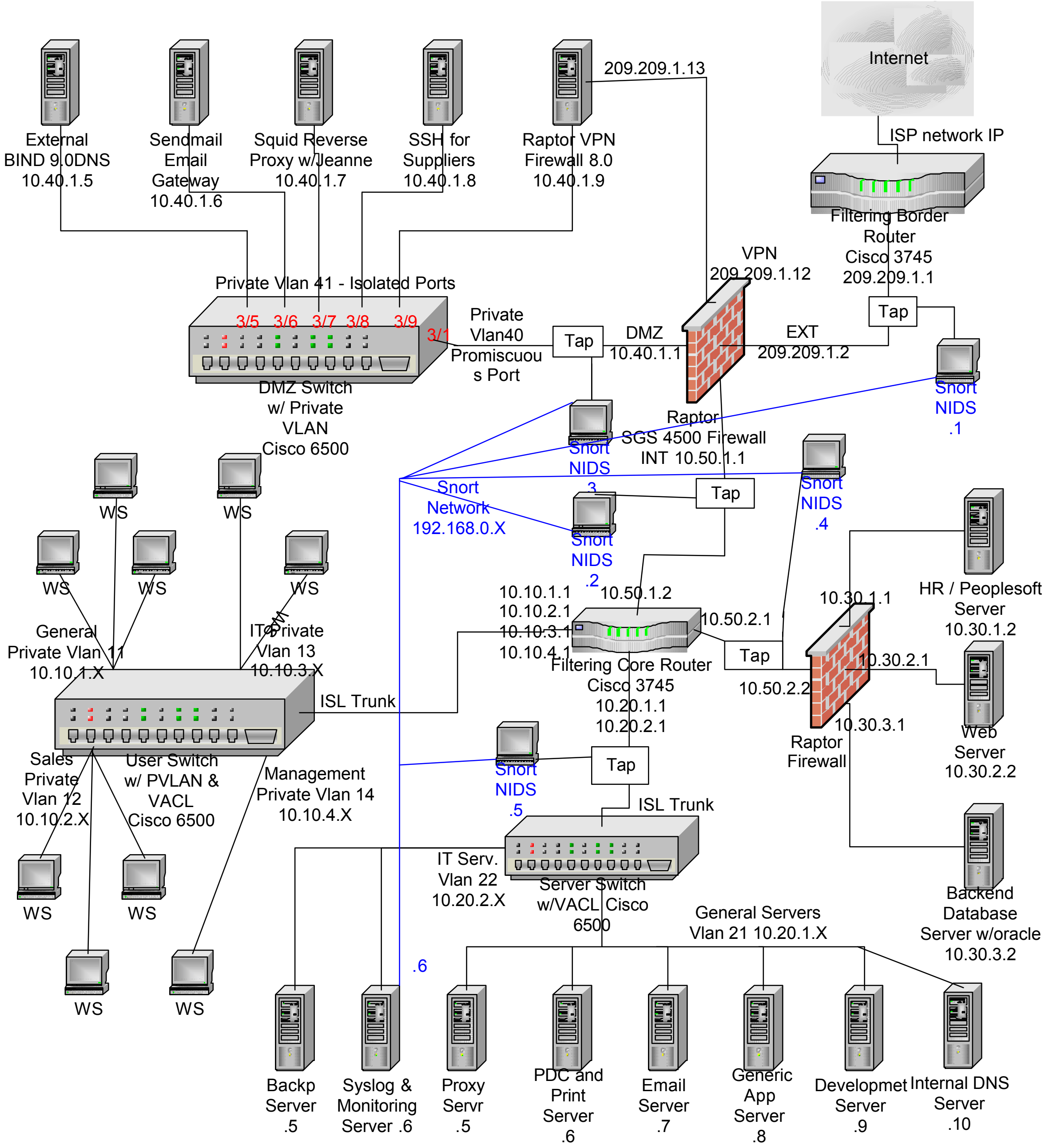
VPN appliance with static IP that connects to the Raptor VPN server's public IP address (209.209.1.13). The Internet firewall only allows VPN connections from the regional offices and blocks all other IP Addresses attempting VPN connections. These VPN connections use IPSec and require: Encapsulation Header uses IP type 50 (ESP), IP type 51 (AH) and UDP 500 (IKE - isakmp). The external firewall allows connections from the VPN server in the DMZ to the general servers subnet (VLAN 21) on all ports. The external firewall and internal firewall both allow the Raptor VPN server to connect to the internal web server on TCP port 80 (HTTP) and TCP port 443 (HTTPS). The external firewall blocks the VPN device from all other network access. This policy grants sales staff at the regional offices access to the exact same resources on the internal network as local sales staff, even though they come in through a VPN tunnel.

Occasionally remote sales staff will need access from a client site, or another remote location not in one of the regional sales offices. This access is enabled through the main web page. After authenticating over SSL, the sales force is able to perform sales duties including viewing and modifying customer data or establishing new accounts. Because this connection is initiated from a non-standard location, web certificates are employed as extra security. They are also allowed rudimentary email access through a web mail service run on the web server. This access requires TCP port 80 (HTTP) and TCP port 443 (HTTPS) to the reverse proxy. Additionally, external DNS services are required on UDP port 53 (DNS) to the external DNS server for name resolution.

The general public has access to GIAC Enterprises website and may send emails to GIAC Enterprises employees. The website's public pages require access to TCP port 80 (HTTP) to the reverse proxy in the DMZ. Email requires TCP port 25 (SMTP) to the email gateway. DNS requests to the external DNS box are also required on UDP port 53 (DNS).

There are some general access rules that apply to all groups of people. For web access, everyone connects to the reverse proxy in the DMZ. These connections are allowed from anywhere on TCP port 80 (HTTP) and TCP port 443 (HTTPS). The reverse proxy then initiates a connection through both the external and internal firewalls to the web server on TCP port 80 (HTTP) and TCP port 443 (HTTPS). Any time a supplier, customer, or remote salesman authenticates, connections are made from the web server through the internal firewall to the backend database on TCP port 1521 (oracle) and TCP port 1433 (SQL).

Email is another commonly used service. An email gateway sits in the DMZ. Connections are allowed from anywhere through the external firewall to the email gateway on TCP port 25 (SMTP). The external firewall blocks all POP3 connections. The email gateway forwards all valid incoming email to the internal mail server on TCP port 25 (SMTP). Outgoing email is allowed from the internal email server through the external firewall on TCP port 25 (SMTP) to anywhere.



Internet
ISP network IP
Filtering Border Router Cisco 3745 209.209.1.1
Tap
Snort NIDS .1
External BIND 9.0DNS 10.40.1.5
Sendmail Email Gateway 10.40.1.6
Squid Reverse Proxy w/Jeanne 10.40.1.7
SSH for Suppliers 10.40.1.8
Raptor VPN Firewall 8.0 10.40.1.9
209.209.1.13
Private Vlan 41 - Isolated Ports
3/5 3/6 3/7 3/8 3/9 3/1
DMZ Switch w/ Private VLAN Cisco 6500
Private Vlan40 Promiscuous Port
Tap
DMZ 10.40.1.1
VPN 209.209.1.12
EXT 209.209.1.2
Raptor SGS 4500 Firewall INT 10.50.1.1
Snort NIDS .3
Snort Network 192.168.0.X
Tap
Snort NIDS .4
Snort NIDS .2
10.50.1.2
10.10.1.1
10.10.2.1
10.10.3.1
10.10.4.1
10.50.2.1
Filtering Core Router Cisco 3745 10.20.1.1 10.20.2.1
Tap
10.50.2.2
10.30.1.1
10.30.2.1
10.30.3.1
Raptor Firewall
HR / Peoplesoft Server 10.30.1.2
Web Server 10.30.2.2
Backend Database Server w/oracle 10.30.3.2
WS
WS
WS
WS
WS
General Private Vlan 11 10.10.1.X
IT Private Vlan 13 10.10.3.X
ISL Trunk
User Switch w/ PVLAN & VACL Cisco 6500
Sales Private Vlan 12 10.10.2.X
Management Private Vlan 14 10.10.4.X
WS
WS
WS
WS
Snort NIDS .5
Tap
ISL Trunk
IT Serv. Vlan 22 10.20.2.X
Server Switch w/VACL Cisco 6500
General Servers Vlan 21 10.20.1.X
.6
Backp Server .5
Syslog & Monitoring Server .6
Proxy Servr .5
PDC and Print Server .6
Email Server .7
Generic App Server .8
Developmet Server .9
Internal DNS Server .10

When designing the network, the trust model was considered and VLANs were chosen with this in mind. The user subnets are all located on the 10.10.X.X network and span the range from 10.10.1.X through 10.10.4.X.

Workstations are not allowed to directly speak to other workstations within GIAC Enterprises. GIAC's subnetting scheme allows for ACLs to be implemented on the core router to block all user subnets with a filter blocking 10.10.0.0 with mask 0.0.255.255. VACLs have been applied that block workstation to workstation traffic. The core router is the default gateway and .1 IP address on all user subnets.

Server subnets are all located on the 10.20.X.X network. All general servers are on 10.20.1.X (VLAN 21), and all internal users are granted full access to this subnet. Another subnet which hosts IT and security servers is located on 10.20.2.X (VLAN 22) Only members of the IT staff (VLAN 13) are allowed access. All other user subnets are blocked from access to VLAN 22 through ACLs on the core router. The core router is the default gateway and .1 IP address for all server subnets.

Protected servers are all placed behind the internal firewall and are on discrete subnets from the 10.30.X.X network. The internal firewall has an interface on each of these subnets (10.30.1.1, 10.30.2.1, and 10.30.3.1) and blocks all access not explicitly allowed. The isolated servers behind the internal firewall include: HR, internal web server, and backend database server.

The DMZ addresses are all on the 10.40.1.X subnet. The external firewall is the default gateway and has IP address 10.40.1.1. A redirect exists on the outside interface of the external firewall redirecting from 209.209.1.X to 10.40.1.X. The last octet of the each servers IP in the DMZ matches the last octet of the redirect on the firewall. For example: the redirect for the email gateway is 209.209.1.7 and forwards incoming packets (on port 25 only) to 10.40.1.7.

External hosts are on the 209.209.1.X subnet. Devices on this subnet include the filtering border router (209.209.1.1), the external firewall (209.209.1.2), the external interface of the VPN device (209.209.1.13) and five redirects for each server in the DMZ (209.209.1.5 – 9).

Our NIDS network is 192.168.0.X and has snort sensors on the .1 through .5 addresses. 192.168.0.6 exists on the syslog and monitoring server, and this server is the only way to reach the snort management subnet. The snort sensor interfaces connected to the taps do not have IP addresses.

A Cisco 3745 running IOS 12.3(4)T is the external filtering border router and GIAC Enterprise's first level of defense. The Cisco 3745 is considered a modular access router and has enough horsepower to easily pass all of GIAC Enterprises traffic. It is reasonably priced and very flexible because it can house a wide array of voice, data, IDS, VPN, and other network modules.

The main purpose of this router is to router traffic between the ISP's network and GIAC enterprises public network (209.209.1.0 / 24). A static route for 209.209.1.0 / 28 points to the firewall's external IP address (209.209.1.2). The default route points out towards the ISP. This router's secondary responsibility is blocking many forms of unnecessary traffic. Blocking unwanted traffic at the router frees up more firewall resources and allows for easier reading of the firewall log files. The firewall can block traffic based on either IP address or protocol and has an extended access control list to block both types of traffic.

Here is a copy of the ingress filter applied to the external router's ISP facing interface:

1. access-list 105 deny udp any any eq 135
2. access-list 105 deny udp any any eq 137
3. access-list 105 deny udp any any eq 138
4. access-list 105 deny udp any any eq 139
5. access-list 105 deny udp any any eq 445
6. access-list 105 deny udp any any eq 593
7. access-list 105 deny tcp any any eq 23
8. access-list 105 deny ip 10.0.0.0 0.255.255.255 any any
9. access-list 105 deny ip 192.168.0.0 0.0.255.255 any any
10. access-list 105 deny ip 172.16.0.0 0.15.255.255 any any
11. access-list 105 deny ip 127.0.0.0 0.255.255.255 any any
12. access-list 105 deny ip 209.209.1.0 0.0.0.255 any any
13. access-list 105 permit ip any any

Rules 1-6 block windows NETBIOS and file sharing. These protocols should not be coming in from outside our network. Rule 7 blocks all telnet access. Rules 8-11 block private and loopback addresses that should not be found on the Internet. Rule 12 prevents external devices from spoofing our address space and sending packets to the external firewall.

Several other steps have been taken to further secure the filtering border router. They include:

1. no ip unreachables
2. no ip source-route
3. no ip direct-broadcast
4. no cdp run
5. no ip proxy-arp
6. no snmp
7. no ip bootp
8. no ip http server
9. no service finger
10. no services tcp-small-servers
11. no services udp-small-servers
12. no tftp-server
13. passive-interface Ethernet 0

14. no ip redirects
15. banner motd * Property of GIAC Enterprises – Unauthorized access is prohibited *
16. service password-encryption

The filtering core router in GIAC's network is also a Cisco 3745. GIAC Enterprises has been considering using IP telephony and this router would be a good candidate. By deploying the same type of router both internally and externally allows GIAC to keep 1 cold standby that can be easily configured to replace either router in the case of failure. The core router includes many ACLs to enforce the host trust model. The ACLs are described above in the access requirements section. Here is a sample ingress ACL applied on the user facing port of the filtering core router:

1. access-list 107 allow ip 10.0.0.0 0.255.255.255 10.20.1.0 0.0.0.255 any
2. access-list 107 allow ip 10.10.3.0 0.0.0.255 10.0.0.0 0.255.255.255 any
3. access-list 107 allow tcp 10.10.4.0 0.0.0.255 10.30.0.0 0.0.255.255 eq 22
4. access-list 107 allow tcp 10.10.4.0 0.0.0.255 10.30.2.2 255.255.255.255 eq 80
5. access-list 107 allow tcp 10.10.4.0 0.0.0.255 10.30.2.2 255.255.255.255 eq 443
6. access-list 107 allow tcp 10.10.2.0 0.0.0.255 10.30.2.2 255.255.255.255 eq 80
7. access-list 107 allow tcp 10.10.2.0 0.0.0.255 10.30.2.2 255.255.255.255 eq 443
8. access-list 107 deny ip any any

Another egress filter is applied on the interface facing the server subnets:

1. access-list 108 allow udp 10.0.0.0 0.255.255.255 10.20.2.6 255.255.255.255 eq 514
2. access-list 108 allow udp 209.209.1.1 255.255.255.255 10.20.2.6 255.255.255.255 eq 514
3. access-list 108 allow tcp 10.10.3.0 0.0.0.255 10.20.2.0 0.0.0.255 eq 22
4. access-list 108 allow tcp 10.10.3.0 0.0.0.255 10.20.2.0 0.0.0.255 eq 80
5. access-list 108 allow tcp 10.10.3.0 0.0.0.255 10.20.2.0 0.0.0.255 eq 443
6. access-list 108 allow ip any 10.20.1.0 0.0.0.255 any
7. access-list 108 deny ip any any

Finally, an egress filter is applied on the interface facing the internal firewall and protected servers. This list only allows internal or DMZ addresses access to the protected servers:

1. access-list 109 permit ip 10.0.0.0 0.255.255.255 10.30.0.0 0.0.255.255 any
2. access-list 109 deny ip any any

The external firewall protects the DMZ and all internal components of GIAC Enterprises network. This makes it crucial in defense against attacks. Several firewalls were considered and Symantec's Gateway Security Series 5400 was chosen. This decision was based on many factors that include[7]:

- proxy technology – the Symantec SGS can proxy many protocols which offers the most protection for DMZ and internal hosts. "Proxies are more secure when it comes to dealing with fragmentation and payload based attacks."[8]
- Built in anti-virus – By using anti-virus on both the firewall and internal devices, we provide a layered defense to improve security. This is enabled

for HTTP and SMTP.
- Built in IDS / IPS – performs deep packet inspection including RFC checking and drops packets which don't meet RFC requirements
- Load Balancing and statefull fail-over – May be deployed as a cluster which shares state information and eliminates any downtime even in the event of device failover
- Throughput – even the smallest SGS appliance provides 200 Mbps throughput even when anti-virus is engaged.
- IP-Sec compliant VPN tunnels are supported
- SSL based authentication for management. Management is performed via a GUI running on the firewall which only answers on the internal interface.
- Statefull packet inspection and content filtering are also supported.

Proxy based firewalls do have one disadvantage in that they must open a port for each protocol that is proxied. This could potentially be abused to gain access to the firewall. GIAC security personnel are aware of this fact and must frequently check with Symantec to obtain any patches as soon as they become available.

The Internet firewall protects both the DMZ and internal network. Packets sourced outside GIAC's network and destined for the DMZ must be NATd to internal addresses. All outward connections from within GIAC Enterprises get NATd which hides the IP address of the internal devices. The firewall placement and heavy use of gateways within the DMZ allows us to force all incoming connections through the DMZ before they enter our internal network. The packets must then travel through the firewall again before gaining access to the internal network. This design gives us two layers of protection for all internal devices.

Redirects are employed on the external firewall for devices in the DMZ. Each DMZ server has an external IP address on the external interface of the firewall. The redirects and firewall ruleset only allow the necessary protocols to be forwarded to the DMZ servers. For example: The redirect to Supplier's SSH server only forwards packets destined to 209.209.1.8 port 22 to 10.40.1.2 port 22. Any packets destined to other ports on 209.209.1.8 are dropped. This system gives us the highest level of defense for our DMZ servers. Attacks directed at any other ports are all dropped by the firewall.

The internal firewall is running Symantec's Enterprise Raptor Firewall version 8.0. The main purpose of this firewall is to protect crucial data sitting on the HR server and backend database server. Not all employees need access to this information and this firewall blocks all connections not explicitly allowed. The Web server has also been placed behind the internal firewall. This configuration was chosen because the web server is able to directly interface with the backend database and thus also needs the highest level of protection. The net result is that all crucial data is protected from internal employees by the internal firewall. Packets sourced from outside GIAC Enterprises network must pass through the external firewall twice and the internal firewall before they are able to reach these crucial servers.

Remote offices each employ a small network behind a Symantec SFVA 200R VPN appliance. Each network uses 192.168.Y.X locally, and there is a unique 3rd octet for each branch. Workstations are deployed behind the appliance which protects them from any incoming traffic not originated over the VPN connection. The appliance is configured to use IPSec and 3DES and MD5 are used for encryption to protect the traffic from any snooping that might occur on the Internet. Pre-shared keys are configured on each device by GIAC IT staff before they are sent to the remote branch. IKE is used for key exchange and the SA Lifetime is set for 6 hours. Each device has 2 WAN ports and can be configured for automatic fail-over if the primary WAN link drops. Static IPs were ordered from the different local ISPs for each WAN port. This prevents scenarios where a single ISP failure would cause total communication loss. These appliances are ideal for the remote offices because they are inexpensive, have good fail-over, and protect the remote workstations. ACLs on the appliance only allow connections to and from the home office VPN server and drop all other traffic.

The main VPN server in the DMZ is Symantec's Enterprise Raptor Firewall version 8.0 with VPN running on Solaris 8.0. This device currently serves as the only ingress point into the network for all regional satellite offices. This device was originally the main Internet firewall but saw extended use when it became the VPN server during a recent main Internet firewall upgrade. GIAC personnel were already familiar with Raptor 8.0 configuration which was a nice added bonus. VPN connections are restricted to the static IP addresses of each remote office's VPN appliance only. Two tunnels are created for each regional office to provide immediate failover if one of a regional satellite office's WAN links drops.

By placing this VPN server / firewall with one connection into the DMZ and one connection to the main Internet firewall, we are able to completely control all traffic entering or leaving. Logs are available from both the external Raptor firewall and the VPN server. Having a public IP address on the external interface of the VPN server prevents any type of NAT issues that could arise. This provides the most security possible.

GIAC Enterprises has invested a large amount into their Cisco 6506 switches. The 6500s were placed strategically at each network that warranted complete layer two protection including: the DMZ, user subnets, and server subnets. After the recent worm problem, layer two security became top priority. Cisco 6500s provide excellent layer two security through PVLANs, VACLs, and port security. PVLANs and VACLs block all server to server traffic within the DMZ and workstation to workstation traffic on the user subnets. On the server switch, all traffic is blocked from the general servers VLAN (VLAN 21) to the IT servers VLAN (VLAN 22). Each switch has a PFC currently and Port Security has been enabled on all non-trunk ports. Port security is configured on each port to allow traffic from a single manually specified MAC address. Packets from any other MAC address are dropped. Sample command:

- Set port security 3/5 enable 00-90-2b-62-ae-16

As usual, all unnecessary protocols are disabled on the switch, and management is only enabled via SSH. Each Cisco 6506 chassis can house six or more blades. In the case of chassis failure in any switch, either chassis has enough room to support all of the switching blades from several switches and can be used until the failed chassis can be repaired or replaced. This helps to reduce downtime, and helps to offset the large cost associated with using several Cisco 6500 switches. Cisco 6500's can add a MSFC for layer 3 switching as well as hosting a large variety of cards including VPN, IDS, Firewall, and VOIP. All of this makes them extremely flexible and giving them a long product lifetime.

GIAC Enterprises has deployed four systems within the DMZ to act as gateway devices. Placement in the DMZ protects all internal servers should a vulnerability arise. All DMZ systems have little or no access to the internal network. All of these systems were deployed using Fedora Core two with minimal packages installed. Red Carpet is used for package management and patching to keep the systems up to date. Server administration and file transfers are only allowed via SSH and SCP. All systems run tripwire for file integrity checking. Internet daemons have been chroot-ed and run as non-root user to protect the operating system. "The idea behind chroot is fairly simple. When you run BIND (or any other process) in a chroot jail, the process is simply unable to see any part of the filesystem outside the jail."[9]

The external DNS server runs BIND 9.0 to provide non-recursive DNS to the public. A split DNS design allows only external IP addresses to be available to the public. Zone transfers are restricted to only our legitimate secondary DNS servers. Any other attempted zone transfers are logged. No access into the internal network is allowed from this server.

The email gateway runs Sendmail 8.13.2 and has anti-spam modules with blacklists maintained by IT and Security staff. The email gateway has access through the external firewall to the internal email server where it forwards all legitimate email.

The reverse proxy runs Squid reverse proxy in caching mode. For additional security the Jeanne add-on is also installed. Jeanne blocks all requests that don't match a previously defined list of files and directories. Our internal web server has access to the backend database and requires the best possible protection. The reverse proxy is allowed access to the internal web server on HTTP and HTTPS ports.

GIAC Enterprises has deployed five workstations with Fedora Core 2 as NIDS running snort 2.3.0 RC2 to detect any malicious traffic. They are all kept current with Red Carpet and meet all the security guidelines for the Fedora Core 2 DMZ servers. By using open source code for NIDS boxes, the whole system can be inexpensively built. The sensors were all deployed on a separate network only accessible through the syslog server. This keeps out all but IT staff out due to the ACLs on the core router.

Snort is a popular NIDS and was chosen for many reasons. Signatures are often quickly available on the Internet for new vulnerabilities. Rule management is easy with Oinkmaster. The syslog server has been configured to collect the alerts and runs the ACID database for easy viewing and correlation. Two separate views were created separating internal alerts from external. Taps were installed on key network segments and send data to a non-addressed interface on each snort sensor. The snort sensors have been built with the kill functionality but it is only used as a last resort.

The external tap and snort sensor (192.168.0.1) sits outside our main Internet firewall. This NIDS is crucial as it will detect scans and attacks that should be dropped by the internet firewall. Persistent attackers will be identified and action can be taken if required. Unfortunately, large numbers of alerts from worms and attacks will be generated, even though almost all alerts will receive no action by GIAC security. A separate view has been created in the ACID database to separate these alerts from the far more critical alerts from internal snort sensors.

The DMZ tap and snort sensor (192.168.0.3) has been strategically placed to be the first line of defense for any internal attacks. Because all traffic into the network must first go to a DMZ server, we should see any attacks that are passed through the external firewall, even if the DMZ server isn’t compromised. If any DMZ server does become compromised, it cannot attack anything without the traffic again going through the DMZ tap directly to the firewall. These security layers adhere to the ideas of defense-in-depth.

The tap just inside the main internet firewall and snort sensor (192.168.0.2) takes advantage of the chokepoint between the main internet firewall and core router. Anything that makes it into the internal network must go past this tap. This positioning is leveraged in cases where the kill functionality becomes desirable.

The remaining two snort sensors and taps were placed just outside segments with important servers to detect any sort of threats against these servers.

Networks should be protected at all layers of the OSI model. GIAC Enterprises network design does a good job of this through layered defense. Access rules are strictly enforced at layer two through PVLANs, VACLs, and port security on the Cisco 6500 switches. Layer three defense is performed by ACLs on both the filtering border router and the core router. GIAC's Raptor firewalls provide defense at layers three and up by requiring packets to meet source IP, destination IP, and protocol criteria before passing them. The extended access list on the filtering border router also protects against many protocols that have no need to enter our network. Finally, GIAC's liberal use of gateways within the DMZ provides excellent application level protection.

The GIAC Enterprises security team performs several functions that exhibit defense-in-depth. All security devices send syslogs to the syslog server. NTP is run to correlate time between the logfiles. The logs are reviewed daily by security staff and analyzed with Logwatch. Custom scripts have been developed to help determine critical threats. Tripwire has been installed on all servers and the results are analyzed daily. Scripts are run daily on each server to check for new accounts and new open ports. Strong password policy is enforced and encrypted passwords are required on all systems. These HIDS policies form a strong second line of defense when combined with the Snort NIDS.

GIAC security staff perform network scans regularly with several different applications. Nessus scans and SARA scans are done twice a month via laptop and all network segments are tested. The web server is also scanned for vulnerabilities using whisker and nikto. New snort signatures are applied when available and checked for daily.

GIAC security staff verify builds against the security checklists. Windows workstations are built with Microsoft XP Pro and keep are kept current on patches and anti-virus. Security audit kits are downloaded from the Center for Internet Security[10] and run on all servers and workstations.

Assignement 3: Firewall Policy. Provide a rulebase for the primary firewall defined in assignment 2. The rulebase of the Symantec SGS 4500 external firewall will be examined.

Raptor firewalls all have an implicit deny all functionality. Rule order is not important as any connection attempts matching a firewall rule are passed, unless the rule has been set to deny. Logfile examination has shown packets matching multiple rules, which indicates that all rules are examined before the packet is passed. This would seem to negate any apparent gain from placing the most used rules first.

Raptor firewall rules allow specification of source and destination interfaces. Rules should be as specific as possible when defining the interfaces to stop unexpected threats. GIAC Enterprise's external Raptor firewall has the following interface definitions:

- EXT – the external interface of the firewall (209.209.1.2)
- INT – the internal interface of the firewall (10.50.1.1)
- DMZ – the DMZ interface of the firewall (10.40.1.1)
- VPN – the VPN interface of the firewall (209.209.1.12)

Several redirects exist on the firewall that forward traffic to the appropriate servers in the DMZ. These redirects will only forward traffic that is addressed to a unique IP and port to the destination IP and port. Additionally, these redirects will not function unless a matching firewall rule is found.

Redirect #	Original IP	Original port	Redirected IP	redirected port
Redirect 1	209.209.1.5	UDP 53	10.40.1.5	UDP 53
Redirect 2	209.209.1.5	TCP 53	10.40.1.5	TCP 53
Redirect 3	209.209.1.6	TCP 25	10.40.1.6	TCP 25
Redirect 4	209.209.1.7	TCP 443	10.40.1.7	TCP 443
Redirect 5	209.209.1.7	TCP 80	10.40.1.7	TCP 80
Redirect 6	209.209.1.8	TCP 22	10.40.1.8	TCP 22

Rule #	Source	Source Interface	Destination	Dest Interface	Dest port	Allow or deny
1	Any	EXT	DMZ-DNS	DMZ	UDP 53	Allow
2	Any	EXT	DMZ-DNS	DMZ	TCP 53	Allow
3	Any	EXT	DMZ-EMAIL	DMZ	TCP 25	Allow
4	Any	EXT	DMZ-WEB	DMZ	TCP 443	Allow
5	Any	EXT	DMZ-WEB	DMZ	TCP 80	Allow
6	SUPPLIERS	EXT	SUPPLY-SSH	DMZ	TCP 22	allow

These first six rules and redirects combine to provide NAT for machines in the DMZ and setup redirects for external devices to reach them on the specified ports. Note that the source interface is specified to only the external interface (EXT), so these rules only allow connections originating from outside our firewall.

Rule #	Source	Source Interface	Destination	Dest Interface	Dest port	Allow or Deny
7	INT-DNS	INT	ANY	EXT	UDP 53	Allow
8	INT-DNS	INT	ANY	EXT	TCP 53	Allow

DNS is allowed from outside of the firewall to the external DNS server in the DMZ on TCP port 53 and UDP port 53. This is accomplished with redirects #1-2 and rules #1-2. These combine to support DNS for all external clients. Internal clients get name resolution from the internal DNS server. The internal DNS server must be able to query outside DNS servers for name resolution. This is supported by rules #7-8. INT-DNS is a group that currently has only the internal DNS server as a member (10.20.1.10)

Rule #	Source	Source Interface	Destination	Dest Interface	Dest port	Allow or Deny
9	DMZ-EMAIL	DMZ	INT-EMAIL	INT	TCP 25	Allow
10	INT-EMAIL	INT	ANY	EXT	TCP 25	Allow

Email is allowed from all outside email servers to the email gateway in the DMZ. This is accomplished through redirect #3 and rule #3. Notice only SMTP is allowed, not POP3. Once the email gateway validates the email, it is sent to the internal mail server. This is allowed with rule #9. Internal clients send their mail to the internal email server which needs access to send email to the world. Rule #10 provides this access for internally sourced emails. DMZ-EMAIL is defined as the email gateway (10.40.1.6) and INT-EMAIL is defined as the internal email server (10.20.1.7).

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
11	DMZ-WEB	DMZ	INT-WEB	INT	TCP 443	Allow
12	DMZ-WEB	DMZ	INT-WEB	INT	TCP 80	Allow

Web traffic is a very important part of the access requirements for GIAC Enterprises. Web traffic from outside is sent to the squid reverse proxy in the DMZ. Redirects #4-5 and Rules #4-5 allow the external requests to reach the squid reverse proxy. Once the squid reverse proxy identifies the request as valid, it forwards the packets to the Internal web server sitting behind the internal firewall. Rules #11-12 support the squid reverse proxy sending packets to GIAC Enterprises production web server. There are similar rules on the internal Raptor firewall to support this connection. DMZ-WEB is defined as the squid reverse proxy (10.40.1.7) and INT-WEB is defined as our production web server (10.30.2.2).

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
13	INT-PROXY	INT	ANY	EXT	TCP 443	Allow

14	INT-PROXY	INT	ANY	EXT	TCP 80	Allow
15	PROXY-BYPASS	INT	ANY	EXT	TCP 443	Allow
16	PROXY-BYPASS	INT	ANY	EXT	TCP 80	Allow

Rules #13-16 support web traffic from inside our network. GIAC Enterprises enforces strict proxy usage, and special exceptions are required to bypass the proxy. Rules #13-14 support outbound HTTP and HTTPS from the proxy. Rules #15-16 support devices with special proxy bypassing exceptions. Proxy Bypass is utilized by IT staff to test and verify proxy functionality and granted in special cases for applications that don't work well through a proxy such as red carpet. INT-PROXY is defined as the internal proxy server (10.20.1.5). PROXY-BYPASS is a dynamic group that contains IT staff and whatever other workstations or servers that need temporary access to bypass the proxy for web traffic.

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
17	DATABASE-SERV	INT	SUPPLY-SSH	DMZ	TCP 22	Allow
18	NET-IT	INT	NET-DMZ	DMZ	TCP 22	Allow
19	NET-ITSERV	INT	NET-DMZ	DMZ	TCP 22	allow

The SSH protocol is desirable for system management and for suppliers to deliver fortunes via SCP to the SSH for Suppliers server in the DMZ. Supplier access is granted via Redirect #6 and Rule #6. Bulk fortunes also need to be retrieved from this server. The backend database server can use SCP to pull the files through Rule #17. By preventing the SSH connections from originating in the DMZ, GIAC has made it very hard for threats to get into our internal network, even if a server in the DMZ is compromised. IT staff also need SSH connectivity to servers within the DMZ from their workstations and also from servers on the IT servers subnet (VLAN 22). This allows them to administrate the servers as well as SCP backups to the backup server. Rules #18-19 support these needs for SSH administration. DATABASE-SERV is defined as the backend database server (10.30.3.2). SUPPLY-SSH is defined as the SSH for suppliers server (10.40.1.8). NET-IT is defined as VLAN 13 (10.10.3.X), and NET-ITSERV is defined as VLAN 22 (10.20.2.X). NET-DMZ is defined as all hosts in the DMZ (10.40.1.X). SUPPLIERS is a group that contains the IP Addresses from our suppliers that deliver fortunes to the SUPPLY-SSH server.

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
20	NET-10	INT	DMZ-NTP	DMZ	UDP 123	Allow

21	NET-DMZ	DMZ	DMZ-NTP	DMZ	UDP-123	Allow
22	DMZ-NTP	DMZ	EXT-NTP	EXT	UDP 123	Allow

NTP has been enabled on GIAC's network to time synchronize all servers and logging devices. Anything on the 10.X.X.X network should time synchronize with the NTP server in the DMZ. Rule #20 supports this internal hosts and Rule #21 supports this for DMZ hosts. DMZ-NTP is the current server in the DMZ that is acting as time server for GIAC's network. Currently it is set to the supplier's ssh server in the DMZ (10.40.1.8). EXT-NTP is a group of trusted external time servers with low stratum.

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
23	NET-DMZ	DMZ	SYSLOG-SERV	INT	UDP 514	Allow
24	EXT-ROUTER	EXT	SYSLOG-SERV	INT	UDP 514	allow

Syslog is used throughout GIAC's network to send logs to a centralized syslog server.   UDP port 514 is used for the transfers. SYSLOG-SERV is defined as the internal syslog server on VLAN 22 (10.20.2.6). Access to the syslog server is granted by Rule #23 for the DMZ servers and Rule #24 for the external router. EXT-ROUTER is defined as our external router (209.209.1.1).

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
25	NET-IT	INT	ANY	ANY	ICMP	Allow
26	NET-ITSERV	INT	ANY	ANY	ICMP	Allow

IT staff and servers are able to ping outside of the network and into the DMZ through Rules #25 and #26.

Rule #	Source	Source Interface	Destination	Dest Interface	Dest Port	Allow or Deny
27	REM-OFFICES	EXT	EXT-VPN	VPN	IP type 50	Allow
28	REM-OFFICES	EXT	EXT-VPN	VPN	IP type 51	Allow
29	REM-OFFICES	EXT	EXT-VPN	VPN	UDP 500	Allow
30	DMZ-VPN	DMZ	NET-SERV	INT	ANY	Allow

31	DMZ-VPN	DMZ	INT-WEB	INT	TCP 80	Allow
32	DMZ-VPN	DMZ	INT-WEB	INT	TCP 443	allow

VPN connections are needed for the regional satellite offices to connect to the home office. The VPN is done over IPSec using IKE. Encapsulation Header uses IP type 50 (ESP). IP type 51 (AH) and UDP 500 (IKE - isakmp) are also required for IPSec. Rules #27-30 support these requirements. Only remote offices are allowed to connect via VPN.

Once they have established a VPN connection that terminates at the Raptor 8.0 VPN Server / Firewall within the DMZ, they will need access to some parts of the internal network. These include the general servers subnet (Rule #30) and HTTP and HTTPS access to the internal web server to perform sales functions (Rule #31-32)

REM-OFFICES is a group that contains the both external static IP addresses for each regional offices. All other VPN connections are denied. EXT-VPN is defined as the external VPN interface (209.209.1.13). DMZ-VPN is the DMZ interface of the VPN (10.40.1.9). NET-SERV is defined as the general servers VLAN 21 (10.20.1.X).

References:

[1] TechWorld “Are Private VLANs really secure?” Dec 10, 2003
http://www.techworld.com/security/features/index.cfm?featureid=238

[2] @STAKE “Secure Use of VLANs: An @stake Security Assessment” August 2002
http://www.cisco.com/application/pdf/en/us/guest/products/ps708/c1697/ccmigration_09186a008012ed31.pdf

[3] Cisco Systems “Virtual LAN Security Best Practices” 2002
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf

[4] Cisco Systems “Securing Networks with Private VLANS and VLAN Access Control Lists” Sept 8, 2004
http://www.cisco.com/warp/public/473/90.shtml

[5] John Sasso Jr. “Private VLANS” Feb 11 2003
http://www.cs.rpi.edu/~kotfid/cn4_spring_03/pvlans.html

[6] Cisco Systems “Catalyst 6500 Seriest Switch Cisco IOS Software Configuration Guide, Release 12.2.SX” Chapter 29:Configuring VLAN ACLs
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.pdf

[7] Symantec “Symantec Gateway Security 5400 Series” 1995-2004
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=133

[8] Sans Institute “Track 2 – Firewalls, Perimeter Protection & Virtual Private Networks Volume 2.3, Sans Press, Jan 28, 2004

[9] Scott Wunsch “Chroot-BIND HOWTO v1.5” Dec 1 2001
http://www.losurs.org/docs/howto/Chroot-BIND.html

[10] Center for Internet Security
http://www.cisecurity.org