Bob Hockensmith

Practical Assignment GIAC Level 2: Firewalls, Perimeter Protection and Virtual Private Networks

Capitol SANS – Version 1.4

Security Architecture (assignment 1)

This solution covers the implementation of a perimeter defense for a small e-business firm, GIAC Enterprises that sells fortune cookie sayings. The company has twenty employees with desktops located in one office. Internet access is provided with a border router connected to a single T-1 line to the ISP. Suppliers and partners have remote access via VPN for e-procurement and to conduct business-to-business transactions. These transactions are all powered by Oracle that resides only on the secured private network. The public has access to an external web server to browse the sales catalog. All sales transactions are performed using secured sockets layers (SSL).

The network is divided into two segments: public and private. A public mail server is configured to interact with external mail post offices on the Internet. No individual mailboxes are maintained on the public mail server. As mail arrives to the public mail server, it will be forwarded to the private mail server. There are also public and private Domain Name Service (DNS) servers. The split DNS configuration protects the private DNS from being compromised because it is hidden—that is, it never does any direct queries. The private DNS server does caching only; hence, unresolved (not cached) requests from the private network are forwarded to the public DNS server that then does the actual resolution request. Furthermore, the public DNS server will answer queries from the Internet concerning only the servers on the DMZ.

Unfortunately, an adversary attempting to compromise GIAC Enterprises information assets can do so by exploiting these LAN/Internet connections. With this security concern in mind, while at the same time under the constraint of limited budget, I have designed a scaleable network architecture that will deliver adequate performance while safeguarding GIAC's assets.

1.1 Perimeter Security

A border router will provide GIAC Enterprises access to the Internet as well as establish its own point of presence and it is the first line of defense. The border router will connect to a T1 from our ISP on the out interface and a 100Mbps Ethernet at the other. Furthermore, the border router will be capable of basic filtering on the inbound and outbound traffic, without being a bottleneck. According to bandwidth specifications, a Cisco 7500 series router would be more than sufficient, with the possibility to accept T3 connections for future expansion. The Cisco 7500 has good expansion possibilities and supports both standard Access Control Lists (ACL) that only provides filtering based on the source IP address and extended ACLs that can provide filtering based on source and destination IP addresses as well as port numbers (services). This will enable us to stop some attacks such as address spoofing before the packets can enter our network. For incoming traffic, the border router will be configured with minimal Ingress filtering to protect against the standard external attacks such as source IP address spoofing and source routing attacks. Egress filtering will be done on outbound traffic to ensure our network is not sending any spoofed packets and that it is not being used as a base to launch a distributed denial-of-service (DDoS) attack.

The second layer of defense will be a CISCO PIX firewall that can deliver strong security without impacting network. The PIX 500 product line does an excellent job enforcing secure access between an internal network and Internet, extranet, or Intranet links. As a dedicated appliance, the Cisco Secure PIX Firewall is easy to install and highly stable**.** The Cisco Secure PIX Firewall Series is cost effective both in cost and maintenance. The Cisco Secure PIX Firewall also scales well enabling exponential capacity when needed. I am going to propose starting with the 515 model which is intended for small to medium business and has throughput measured at 120 Mbps with the ability to handle up to 125,000 simultaneous sessions.

So that performance and access to the service network will not be impaired or restricted, I will configure this firewall to allow everything and deny only specific services (i.e. FTP, SNMP, telnet, finger) and IP addresses that I know has the potential to compromise the service network. Both the Cisco border router and the PIX firewall will use TACACS for authentication, authorization and accounting. They can be accessed from designated workstations from the secured network using SSH and Telnet.

The third layer of defense lies between the DMZ or services network and GIAC's secured network. I have chosen Check Point's VPN-1 Gateway, a combined package of FireWall-1 and VPN-1. Firewall-1 will be configured to provide proxy services (application-level gateway), access control, network address translation (NAT), user authentication, content security, anti-virus protection, URL and Java/ActiveX screening, auditing and reporting, intrusion detection, and malicious activity detection. Though the VPN connection will considered a "trusted path", it will be terminated in front of this firewall and therefore governed by its policy, proxy services, content security, auditing, and authentication.

Firewall-1 has a user-friendly visual interface that enables administrators to quickly and efficiently manage the firewall policy. Furthermore, it does stateful packet filtering; hence, no rules have to be added to allow for return packets to the port numbers greater than 1024. Also, with stateful filtering, attacks aimed at exploiting vulnerabilities due to invalid packet sequences are blocked (e.g. after a SYN, we expect a SYN/ACK back). We will also use proxy services provided by Firewall-1. There are many benefits to the deployment of application-level gateways. They give the network manager complete control over each service, since the proxy application limits the command set and determines which internal hosts may be accessed by the service. Also, the network manager has complete control over which services are permitted, since the absence of a proxy for a particular service means that the service is completely blocked. Application-level gateways have the ability to support strong user authentication and provide detailed logging information. Finally, the filtering rules for an application-level gateway are much easier to configure and test than for a packet-filtering router.

In general, this firewall it will be configured to block everything and allow only those protocols and services permitted according to the policy. This firewall will be implemented on a Windows NT 4.0 platform placed between the service network or DMZ and the secured private network

1.2 Services Network (DMZ)

A services network that will built containing a public web server, a mail server, external DNS server, and possibly at a latter time an FTP server. I will use a screened subnet, commonly referred to as the DMZ, to provide some security for the public services. Hence, the DMZ will be on the inside of the perimeter firewall. All hosts within the DMZ will be on a separate network segment, assigned legal addresses making them addressable from the Internet, and they will face both the Internet and the secured private network.

1.3 Secured Private Network (Intranet)

In order to further protect the private network (Intranet) as well as eliminate any performance bottlenecks due to the additional activity on the extranet, a second or internal firewall will be placed between the Intranet and the DMZ. The additional firewall will protect GIAC’s sensitive and proprietary information. The internal firewall will only allow incoming traffic from the DMZ and VPN-1.

Network Address Translation (NAT) is used to conceal the real addresses of the private network. It also provides flexibility in network design and growth by having more address space at our disposal than could be obtain from Internet Assigned Numbers Authority (IANA). Address translation will be applied by the firewall to all network traffic originating from the private network. That means that internal addresses will be replaced with the public address of the firewall as the packets' source addresses.

To break into the private network with this type of architecture, an attacker would have to get past both firewalls. Even if the attacker somehow broke in to the perimeter, he'd still have to get past the interior firewall to reach the private network. Hence, there is no single point of failure that will compromise the private network.

1.4 VPN (remote access)

GIAC will be able to conduct business with its partners and suppliers using the Internet as the business transaction carrier. This business flow will be implemented using a VPN to provide a secured tunnel between GIAC's partners or suppliers and its corporate servers and databases kept in the safe haven of its Intranet. VPN-1 meets our demanding requirements of Internet, intranet, and extranet VPNs by providing secure connectivity to our corporate network, remote and mobile users, and key partners and suppliers. VPN-1 supports sophisticated high availability configurations for IPSec traffic, and provides built-in resiliency for remote access VPNs. Extranets are made possible through support for industry standards as well as all leading PKI products and services.

The border router allow all VPN traffic to flow directly to the VPN-1 gateway, bypassing the external firewall, by routing directly through an additional Ethernet interface that links to the VPN-1/Checkpoint-1 host. VPN traffic will be terminated at the firewall so that service access will only be granted according to the firewall policy. VPN traffic will be decrypted and inspected to ensure that only appropriate content is allowed through the firewall. In all firewall rules, clients coming from a VPN connection will be considered “trusted”. Access to resources within the secured network will be based on that partner’s authentication and on a need-to-know basis.

There are several reasons why I feel the integrated VPN and firewall solution is the better choice. Stand-alone VPN gateways have limited means (i.e. packet filtering) of enforcing access control; hence, VPN devices placed in front of the firewall are vulnerable to Internet threats. If a VPN gateway is compromised by such an attack, all VPN communications will cease, or worse yet, may be transmitted in the clear. This is a potentially disastrous scenario for customers and business partners relying on GIAC's security infrastructure for confidential communication. Placing a stand-alone VPN gateway behind the firewall provides security for the VPN gateway but does not make any of the VPN traffic subject to any access control managed by the firewall policy. This type of configuration is not in keeping with the best practices for security. Access control ensures that VPN users including partners, employees and mobile workers have appropriate access to specific resources within a network. A VPN without sufficient access control only protects the security of the data in transit but cannot enforce secure access to resources on the network. Placing a VPN gateway in parallel with the firewall is even less secured configuration as it not exposes the gateway to attacks and offers only limited access control on the VPN traffic, it also introduces additional complexities for routing schemes (i.e. NAT, dynamic IP assignment, etc). The integrated VPN gateway and firewall solution resolves all of these issues.

Using VPN-1 SecuRemote, our business partners can connect to our perimeter via Internet connections and establish secure VPN sessions to access sensitive information from GIAC resources. The VPN client transparently encrypts and authenticates critical data to protect against eavesdropping and malicious data tampering. VPN-1 SecuRemote supports dynamic and fixed IP addressing for all Internet Service Provider (ISP) services--dial-up, cable modem, or Digital Subscriber Lines (DSL) and installs on any Windows 95, 98, 2000, or NT 4.0 platform—making it an ideal solution for GIAC's partners and suppliers. VPN-1 SecuRemote supports all IP-based network communications and interfaces with existing network adapters and TCP/IP network stacks for maximum compatibility. Because it operates at the IP layer, VPN-1 SecuRemote supports all IP services without modifications to any applications.

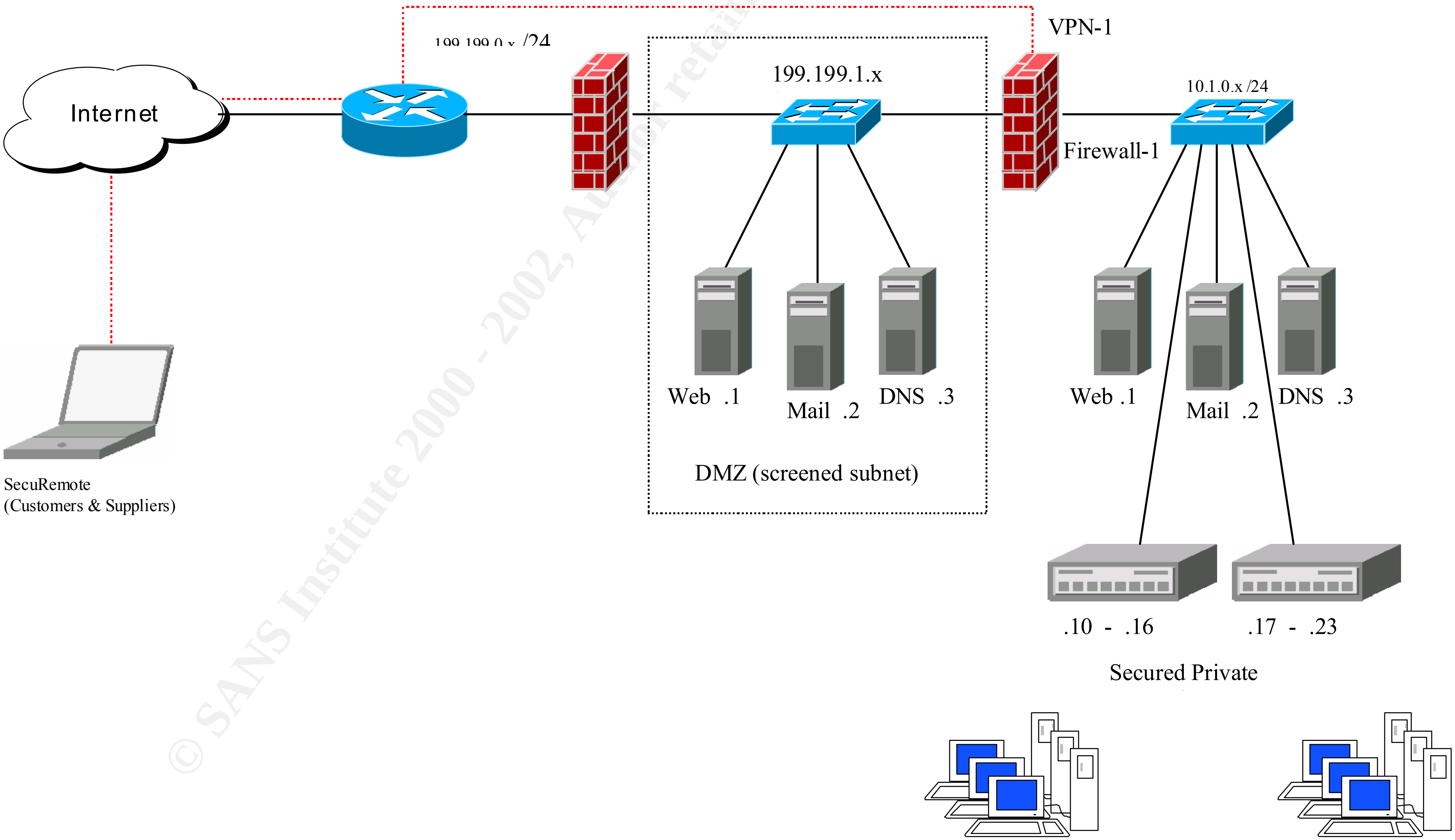


Figure 1: GIAC Enterprises Network

2.0 Security Policy (assignment 2)

The following will be implemented as the minimum level of security GIAC Enterprises will use to ensure protection, integrity, and availability of our IT resources:

1. We will check CERT, Microsoft, Checkpoint and CISCO sites on a regular basis in order to ensure GIAC Enterprises stays on top of all security advisories, software patches, and security enhanced releases.
2. All changes, updates, patches, installations and modifications will be fully tested for functionality or flaws. All tests will be logged by system administration
3. Any sensitive data such as customer purchases via our external Web server will be done via https utilizing SSL and our digital certificate that we have purchased from VeriSign.
4. In addition to our suppliers and partners using VPN, all business transactions will also be performed using both our digital certificate and our partner's digital certificate as the standard method for strong authentication.
5. On servers and client workstations, Norton Anti-Virus will be used to protect against viruses, worms, and Trojan horses. Virus definition files will be updated regularly.
6. Data access is restricted on a "need to know" basis for both internal users and our business partners and suppliers.
7. All unneeded services will be removed from each server.
8. All passwords are to be changed at least every 60 days. Never use vendor default passwords. Never electronically distribute assignment of new passwords. Passwords are to be 8 characters minimum and contain lower, uppercase and non-alpha characters.
9. The top ten vulnerabilities posted on www.sans.org will be addressed using their recommended solutions.

In addition to the above enterprise-wide policy, the border router, outside firewall, inside firewall, and VPN will have individual policies that will work in conjunction with each to provide a defense-in-depth strategy. For this exercise the policy for the internal firewall will not be reviewed since its policy is not a requirement for the practical.

2.1 Border Router

I will use a Cisco 7507 router running 12.1.5 IOS to perform border functions. This router will connect to the Internet and will route all traffic to either the VPN gateway or the exterior firewall. For incoming traffic, it will only protect against the standard external attacks (source IP address spoofing, source routing attacks, etc.) using Ingress filtering. Egress filtering will be done on outbound traffic to ensure our network is not sending any spoofed packets and is not being used as a base to launch a distributed denial-of-service (DDoS) attack.

Using global configuration mode to enter commands that affect the entire router enter the following commands:

```
config t
no ip source-route
no service tcp-small-servers
no service udp-small-servers
no service finger
service password-encryption
enable secret <*** put a password here *****>
```

No ip source route will not allow packets that are marked to use source routing. *No service tcp-small-servers* and *udp-small-servers* blocks access to the TCP/UDP services echo, chargen and discard. These services could be used as a denial of service attack against the router itself.

No service finger will block finger requests that would provide some information about what users are logged into a network device. This could potentially provide an attacker with some useful information. The *service password encryption* command encrypts the passwords in the configuration. *Enable secret* is used to enter the enable password. It is more secure than the *enable password* command.

Configure the router to only allow certain machines on the secured network to telnet to it. While in configuration mode, the following will be entered:

```
access-list 1 permit 10.1.0.10 0.0.0.12
line vty 0 4
access-class 1 in
```

The access-list 1 permits workstations with the IP addresses from 10.1.0.10 through 10.1.0.12. to Telnet and login to the router using the virtual terminals defined by *Line vty 0 2.* The *Access-class 1 in* command allows telnet only from the IP addresses defined in access-list 1.

The Ingress (access list 100) and Egress (access list 101) filtering rules for the border router will basically allow any traffic through and only protect against spoofing and pinging.

Vulnerability	Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses.
Description	IP addresses reserved for internal network use are: 10.0.0.0 – 10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255. None of these addresses should be seen originating from outside the router. We also need to consider the three "legal" ip addresses (199.199.1.1, 199.199.1.2 and 199.199.1.3) for the publicly addressable HTML server, SMTP/POP server, and DNS respectively
Filtering Rule	Access-list 100 deny ip 10.0.0.0 0.255.255.255 any Access-list 100 deny ip 172.16.0.0 0.15.255.255 any Access-list 100 deny ip 192.168.0.0 0.0.255.255 any Access-list 100 deny ip host 199.199.1.1 any Access-list 100 deny ip host 199.199.1.2 any Access-list 100 deny ip host 199.199.1.3 any
Test	From a machine outside the border router, use a tool that will generate the packets with valid destination addresses to servers on the DMZ and source addresses that should be blocked.

Vulnerability	Ensure that our network is not sending any spoofed packets.
Description	If any packet leaving the border router has a source address that does not belong to our range of legal addresses, block it. This will be done through the Egress filter access list 101. The implicit "deny all" that is in place will block everything not matching this rule
Filtering Rule	Access-list 101 permit 199.199.1.0 0.0.0.255 any
Test	From a host within the DMZ, use a tool that will generate the packets with source addresses that do not belong to our range of legal addresses. These packets should be blocked.

Vulnerability	ICMP—block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages
Description	The subject ICMP packets can be used to gather intelligence on a network.
Filtering Rule	Access-list 100 deny icmp any any echo Access-list 101 deny icmp any any echo-reply Access-list 101 deny icmp any any time-exceeded Access-list 101 deny icmp any any host-unreachable
Test	From a machine outside the border router, attempt these services using the ping and traceroute tools.

So that we do not block all remaining inbound traffic as a result of the implicit "deny all" that is in place, add the following rules to the Ingress filtering access list:

```
access-list  100 permit tcp any any
access-list  100 permit udp any any
```

Implement the Ingress and Egress filter rules with the following commands:

```
interface serial 0
ip access-group 100 in

interface Ethernet 0
ip access-group 101 in

interface Ethernet 1
ip access-group 101 in
```

The serial interface is linked to our Internet Service Provider. The Ethernet interfaces 0 and 1 are linked to the external firewall and the VPN gateway respectively.

2.2 External Firewall

PIX version 5.2.0 will be used to create the external firewall. Since this is traffic coming to and from the unsecured or public network residing in the DMZ, it will allow everything and deny only specific services (i.e. FTP, SNMP, telnet, and finger) and sometimes only allow specific services to specific hosts.

Vulnerability	Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
Description	These login services allow opportunities for outside users to authenticate themselves to internal machines. None of these services are required by GIAC or its partners; hence, they can all be blocked.
Filtering Rule	access-list 100 deny tcp any any eq 21 access-list 100 deny tcp any any eq 22 access-list 100 deny tcp any any eq 23 access-list 100 deny tcp any any eq 139 access-list 100 deny tcp any any range 512 514
Test	From a machine outside the border router, attempt these services using a

	valid address destination of a server on the DMZ. The connection attempt should fail.

Vulnerability	RPC and NFS—Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
Description	These services allow remote file system and operating system manipulation. remotely. None of these services are required by GIAC; hence, they can all be blocked.
Filtering Rule	access-list 100 deny tcp any any eq 111 access-list 100 deny udp any any eq 111 access-list 100 deny tcp any any eq 2049 access-list 100 deny udp any any eq 2049 access-list 100 deny tcp any any eq 4045 access-list 100 deny udp any any eq 4045
Test	From a machine outside the border router, attempt to use these ports. The connection attempt should fail.

Vulnerability	NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445(tcp and udp)
Description	These ports provide low-level Windows registration, authentication, and file services. This should not be allowed from any remote connection.
Filtering Rule	access-list 100 deny tcp any any eq 135 access-list 100 deny udp any any eq 135 access-list 100 deny tcp any any range 137 139 access-list 100 deny udp any any range 137 139 access-list 100 deny tcp any any eq 445 access-list 100 deny udp any any eq 445
Test	From a machine outside the border router, use a tool that will generate the packets to valid addresses on the DMZ for these ports.

Vulnerability	X Windows -- 6000/tcp through 6255/tcp
Description	X Windows services utilize this range of ports to manage user interfaces remotely. X Windows is not utilized by GIAC.
Filtering Rule	access-list 100 deny tcp any any range 6000 6255
Test	From a machine outside the border router, use a tool that will generate the packets to valid addresses on the DMZ for these ports.

Vulnerability	Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
Description	DNS is a major security threat. There are many known vulnerabilities and it provides the potential for intelligence gathering. The public DNS server (199.199.1.3) is the only host allowed to receive DNS requests. LDAP is not implemented; hence these ports should be blocked for all.
Filtering Rule	access-list 100 permit tcp any host 199.199.1.3 eq 53 access-list 100 deny tcp any any eq 53 access-list 100 permit udp any host 199.199.1.3 eq 53 access-list 100 deny udp any any eq 53 access-list 100 deny tcp any any eq 389 access-list 100 deny udp any any eq 389
Test	From a machine outside the border router, use nslookup to a host on the DMZ other than the DNS server (199.199.1.3). The request should be blocked This should be supplemented by the packet creation tool to test LDAP blocking.

Vulnerability	Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
Description	Mail servers are another major security threat due to the large number of known vulnerabilities. The public mail server (199.199.1.2) is the only host that is authorized to receive incoming SMTP traffic. All incoming POP should be blocked. IMAP is not implemented and therefor should be blocked.
Filtering Rule	access-list 100 permit tcp any host 199.199.1.2 eq 25 access-list 100 deny tcp any any eq 25 access-list 100 deny tcp any any range 109 110 access-list 100 deny tcp any any eq 143
Test	From a machine outside the border router, use a tool that will generate the packets to valid addresses on the DMZ for these ports.

Vulnerability	Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
Description	Web servers also constitute a weakness in network defenses due to their access-list accessibility. The public web server (199.199.1.1) is the only host authorized to provide web services to the internet. All other HTTP and HTTPS traffic should be blocked.
Filtering Rule	access-list 100 permit tcp any host 199.199.1.1 eq 80 access-list 100 deny tcp any any eq 80 access-list 100 permit tcp any host 199.199.1.1 eq 443 access-list 100 deny tcp any any eq 443 access-list 100 deny tcp any any eq 8000 access-list 100 deny tcp any any eq 8080 access-list 100 deny tcp any any eq 8888
Test	From a machine outside the border router, use a web browser to a host on the DMZ other than the web server.

Vulnerability	"Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
Description	Low numbered ports provide specified services (like echo and chargen) which should not be access-list accessible from outside the network. None of these services are required by GIAC or its partners; hence, they can all be blocked.
Filtering Rule	access-list 100 deny tcp any any lt 20 access-list 100 deny udp any any lt 20 access-list 100 deny tcp any any eq 37 access-list 100 deny udp any any eq 37
Test	From a machine outside the border router, use a tool that will generate the packets to valid addresses on the DMZ for these ports.

Vulnerability	Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
Description	Each of these services has known vulnerabilities and should be blocked unless they are absolutely needed. These services and routing protocols are not required by GIAC and its partners.
Filtering Rule	access-list 100 deny udp any any eq 69 access-list 100 deny tcp any any eq 79 access-list 100 deny tcp any any eq 119 access-list 100 deny tcp any any eq 123 access-list 100 deny tcp any any eq 515 access-list 100 deny udp any any eq 514 access-list 100 deny tcp any any eq 161 access-list 100 deny udp any any eq 161 access-list 100 deny tcp any any eq 162 access-list 100 deny udp any any eq 162
Test	From a machine outside the border router, attempt these services using the ping and traceroute tools.

So that we do not block all remaining inbound traffic as a result of the implicit “deny all” that is in place, add the following rules to the access lists:

```
access-list  100 permit tcp any any
access-list  100 permit udp any any
```

Implement the Ingress and Egress filter rules with the following commands:

```
interface serial 0
ip access-group 100 in

interface Ethernet 0
ip access-group 101 in
```

2.3 Internal Firewall

Firewall-1 will be configured to provide proxy services (application-level gateway), access control, network address translation (NAT), user authentication, content security, anti-virus protection, URL and Java/ActiveX screening, auditing and reporting, intrusion detection, and malicious activity detection. In general, it will be configured to block everything and allow only that which is permitted according to the policy. Currently, it will only allow the following services between the DMZ and the private network: inbound and outbound SMTP (25), outbound HTTP and HTTPS (TCP 80 and 443), and inbound and outbound DNS queries (UDP, TCP 53).

Note: since I do not have access to any equipment, there is no way to show any GUI screen shots of the rules that I would create.

3.0 Assessment (assignment 3)

The scope of the assessment is to determine the level of information assurance provided by the security architecture that I have designed. The assessment will be a dual approach.

First method will be the launching of a network penetration test from outside of the border router and then one from within the secured network to determine what weaknesses we may have against known vulnerabilities. The penetration test will be performed by using a tool such as Internet Scan by Internet Security System. I will want to launch a scan of our IP range from outside of the border router to identify accessible hosts and their available services. Attempts will then be made to enter accessible hosts by exploiting the discovered vulnerabilities. A similar test will be conducted from inside the network.

The second method will be the validation of the functionality of the rules defined for the border router and the exterior firewall. The assessment of the internal firewall is beyond the scope of my practical. Furthermore, since I do not have access to any of the equipment discussed in my practical, I will not be able to show any output from the commands or any of the logs. However, I will can describe what I could do and what should happen during the assessment. If I were able to display the logs, I would be able to show the results of the assessment thereby revealing the time, source address, destination address, service type, and action taken.

The estimated cost estimate to conduct this assessment will be $4,000 . It will require one network analyst forty hours at the rate of $100 per hour. The first day will be used primarily for setup and in briefing, day two through four will be used for network scanning and analysis of results. The last day will be used to create some reports and slides and deliver an out briefing. Since the scope of the work performed is perimeter analysis only, it is agreed that other network security issues such as password policies, physical connections, communication closet review, security of the server room, check of backdoor circuits, etc are outside of the scope of this assessment.

The reminder of this section will be describing how I would conduct an assessment of the border router and the exterior firewall. The source IP address to test the perimeter will be a non-local address that is not in the address range of the business partner since those addresses will be directly routed to the VPN-1 gateway.

3.1 Assessment of the border router

First I want to insure that access to the router is limited to the network management workstations and that the global configuration commands used to configure the router are functioning as we planned. I will try to telnet to it from various workstations. The only successful telnet should be from the machines that are defined in access-list 1 that was defined to the router. Also verify that a valid account on the TACACS+ server is required--all others should fail. I will try to telnet to different ports on the router such as 7(echo) and 19(chargen). These should not answer as a result of the *No service tcp-small-servers* and *udp-small-servers* commands that I configured the router with to block access to the TCP/UDP services echo, chargen and discard. I will try to run a finger to the router. It should not answer as a result of the *No service finger* command.

I configured the router to block any IP source routing with the *No ip source route* command. This can be tested by using Netcat to construct a loose-source-routed path. The following command will try to connect to the public web server using a source-routed packet. The source routed hops go through an interface at the border router and an interface at the exterior firewall.

```
 nc -g 199.199.0.2 -g 199.199.0.4 199.199.1.1 80
```

The packet should be dropped and logged.

I configured the border router to block inbound packets with addresses that match any of our private addresses.

10.0.0.0 0.255.255.255
172.16.0.0 0.15.255.255
192.168.0.0 0.0.255.255
199.199.1.1
199.199.1.2
199.199.1.3

From the test host outside of our network, I can use a tool such as sirc2 to generate packets using any of the above as source addresses for a service that is allowed such as HTTP. These packets should be denied by the border router and logged to the syslog server.

As discussed in the previous section, we do not want our network to be a base for a Distributed Denial of Service attack; therefore, we do not want any spoofed packets to leave our network. The egress filter checks if all the outbound packets have a legal IP address. This test scenario is performed by generating a packet using sirc2 from a host residing in the DMZ. The destination address of the packet will be for a host outside of our network; this will be done with a command similar to the following:

```
./sirc2 181.44.44.1 target_host 80
```

Network address translation is not done by the exterior firewall so the source address will be intact when it reaches the router. The packet should be dropped and logged to syslog.

The last check for the router assessment is to make sure that the router is blocking incoming echo requests. Using nmap from our test host outside of our network, the following command will invoke a ping sweep:

```
nmap -sP -PI 199.199.1.0/24
```

If nmap responds with "hosts appears to be up", then the router is not blocking ICMP echo requests.

3.2 Assessment of the Exterior Firewall

Assessment of the exterior firewall will be conducted in the same manner as the border router—that is, we will build test scenarios to insure that our rules are working properly. We will verify the results based on immediate outputs of the commands and by verifying the results with the log.

First check is to insure that login services initiated to any of our hosts from outside of our network are being blocked. Using our test host outside of our perimeter, I can attempt to telnet or ftp to any of the three hosts residing in the service network. The telnet should result in a "connect failed" message and the ftp command should result in a "host unreachable" message. If you do get through, then obviously the rules to block login services needs to be corrected.

Next I want to check access to web services. Using a web browser from the test host, I can attempt HTTP and HTTPS to the each of the hosts within the DMZ. They should all fail except for the HTTP request to the public web server.

For the remainder of the assessment testing, I will use a combination of Netcat, Nmap, and nslookup. The following table depicts the test plan for the remaining services.

Service	Command	Result
LDAP	nc -u 199.199.1.2 389 nc -t 199.199.1.2 389 nc -u 199.199.1.3 389 nc -t 199.199.1.3 389	Fail Fail Succeed Succeed
DNS	Nslookup 199.199.1.3 Nslookup 199.199.1.1	Succeed Fail
RPC	nc -u 199.199.1.2 111 nc -t 199.199.1.2 111	Fail Fail
NFS	nc -u 199.199.1.2 2049 nc -t 199.199.1.2 2049	Fail Fail
Lockd	nc -u 199.199.1.2 4045 nc -t 199.199.1.2 4045	Fail Fail
NetBIOS	nc -u 199.199.1.2 135 nc -t 199.199.1.1 135 nc -u 199.199.1.2 137 nc -u 199.199.1.3 138 nc -t 199.199.1.2 139	Fail Fail Fail Fail Fail
SMTP	nc -t 199.199.1.2 25 nc -t 199.199.1.1 25	Succeed Fail
POP	nc -t 199.199.1.2 109 nc -t 199.199.1.1 109 nc -t 199.199.1.2 110 nc -t 199.199.1.1 110	Succeed Fail Succeed Fail
IMAP	nc -t 199.199.1.2 143 nc -t 199.199.1.1 143	Succeed Fail
TFTP	nc -u 199.199.1.2 69	Fail
Finger	nc -t 199.199.1.1 79	Fail
NNTP	nc -t 199.199.1.1 119	Fail
NTP	nc -t 199.199.1.1 123	Fail
LPD	nc -t 199.199.1.1 515	Fail
Syslog	nc -u 199.199.1.2 514	Fail
SNMP	nc -u 199.199.1.2 161 nc -t 199.199.1.2 161 nc -u 199.199.1.2 162 nc -t 199.199.1.2 162	Fail Fail Fail Fail

BGP	nc -t 199.199.1.1 179	Fail
SOCKS	nc -t 199.199.1.1 1080	Fail
X Windows	Nmap –sT –p 6000-6255 –P0 –n 199.199.1.2	Fail

3.3 Recommendations for Improvement

Firewalls are the first line of defense for against external attack and usually the first system that professional intruders attempt to bypass. Unfortunately, firewalls are subject to faulty configurations that can leave the network unprotected. Routers, servers and switches also can have subtle configuration variations that allow unauthorized activity on the network. Openings in a firewall rule base represent another vulnerability. When an organization opens a hole through its firewall, it often bypasses the firewall's security services and relies instead on the security configurations of the internal network, which may not be adequate. Intrusion detection systems complement firewalls by detecting attempts to exploit firewall holes, by protecting the firewall itself from attack, and by identifying faulty configurations in the firewall rule base.

The Windows NT Version of Internet Security Systems Inc.'s RealSecure gives network administrators an impressive tool for patrolling their TCP/IP networks. RealSecure is an integrated network-based and host-based intrusion detection and response system. This maximum level of around-the-clock surveillance can extend unobtrusively across GIAC's enterprise, allowing administrators to automatically monitor network traffic and host logs, detect and respond to suspicious activity, and intercept and respond to internal or external host and network abuse before systems are compromised. An automated, real-time intrusion detection and response system. RealSecure runs on enterprise networks where critical data needs protection. RealSecure sensor modules monitor an enterprise network at a variety of points – raw traffic flow on key network segments, log files of critical servers, kernel level auditing – looking for patterns that indicate attack or misuse. When RealSecure detects an attempted intrusion, it can respond automatically to stop the attack and prevent damage or loss.

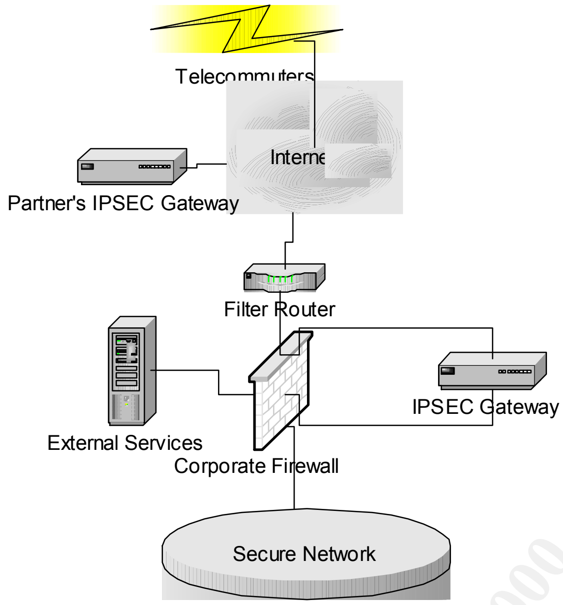
The Network Sensor looks at all the traffic on a single segment. The OS Sensor monitors the operating system log files for signs of unauthorized activity. Like the Network Sensor, it can take action automatically to prevent further system incursions. RealSecure Network Sensors can be deployed throughout the network to see all traffic, not just that which traverses a firewall boundary. In addition, RealSecure OS Sensors monitor user activity for unauthorized access attempts, even for users that are authorized to be on the system. Therefore, an attack or unauthorized activity anywhere on your network can be detected.

For added security I recommend placing an Intrusion Detection System (IDS) such as RealSecure within both the DMZ as well as the secured private network. In addition, I recommend installing RealSecure OS Sensors on all of the critical hosts. I believe this will give us our best return on investment from our security budget while greatly enhancing our defense-in-depth strategy.

4.0 Design Under Fire (**Assignment 4)**

For the purpose of simulating an strategic attack, I have selected the practical submitted by Jeremy Brown which is located at http://www.sans.org/y2k/practical/Jeremy_Browns_GCFW.zip .

The security architecture for Jeremy's network is comprised of four basic security layers: 1) the filter router is the main gateway to the outside, and contains a couple egress ACLs and a bunch of extended ACLs, 2) the corporate firewall, 3) IPSec service for all remote employee and partnership connections, and 4) the internal firewalls that divide the business into three business units and restrict information on a need-to-know basis.



The Boundary router (a Cisco 4000) is responsible for distinguishing traffic and forwarding it appropriately. The router has a main gateway connection (denoted as Serial 1/1), with an IP address of 192.21.71.1. The data arriving to this interface is immediately put through a series of ACLs.

Boundary Router Configuration:

```
No ip direct-broadcasts
No ip source-route
No service Finger
No ip http
No ip bootp
Banner //// Warning Unauthorized Usage of Fortune Maker's Network, Will Result in Arrest and Possible
Conviction /////
Access-list extended egress permit ip 192.71.21.0 255.255.255.0
Access-list extended egress deny ip any any logging

Interface serial 1/0
Ip address 192.21.71.1 255.255.255.0
access-group 100 in
access-list 100 deny udp any any eq 137
access-list 100 deny udp any any eq 138
access-list 100 deny tcp any any eq 139
```

```
access-list 100 deny tcp any any eq 109
access-list 100 deny tcp any any eq 110
access-list 100 deny tcp any any eq 111
access-list 100 deny udp any any eq 111
access-list 100 deny tcp any any eq 143
access-list 100 deny udp any any eq 520
access-list 100 deny tcp any any eq 389
access-list 100 deny udp any any eq 389
access-list 100 permit tcp any any
access-list 100 permit udp any any
```

The corporate firewall, which is a PIX, will be running NAT. The only external addresses that attackers can see are the external DNS, which by use of split DNS, only lists necessary addresses (Mail, HTTP and DNS server) . The firewall will deny all traffic and allow only specific services. The PIX has one incoming interface and one outgoing interface.

Pix configuration:

```
hostname pixfirewall
interface ethernet0 auto
interface ethernet1 auto
ip address outside 192.71.21.2 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip address services 192.71.28.1 255.255.255.0
ip address ipsec 10.2.1.1 255.255.255.0
static(outside, services) 192.71.21.2 192.71.28.1 netmask 255.255.255.0
syslog level 5
conduit permit tcp host 192.71.21.2 eq www any
conduit permit tcp host 192.71.21.2 eq 1080 any
conduit permit tcp host 192.71.21.2 eq ftp any
conduit permit tcp host 192.71.21.2 eq ssl any
conduit permit tcp host 192.71.21.2 eq dns any
conduit permit udp host 192.71.21.2 eq dns any
static(outside, inside) 192.71.21.2 10.1.1.1  netmask 255.255.255.0
syslog level 7
conduit permit tcp
conduit permit tcp host 192.71.21.2 eq tcp established-port
conduit permit udp host 192.71.21.2 eq udp establish-port
route outside 10.0.0.0 255.255.255.240 172.17.11.3 1
static(outside,ipsec) 192.71.21.2 10.2.1.1 netmask 255.255.255.
crypto isakmp policy 2
authentication pre-share
hash md5
crypto isakmp key inside address 10.2.1.1
crypto isakmp key outside address 192..0.20
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip services passive
no rip services defaultno snmp-server location
no snmp-server contact
```

4.1 Strategic Attack

My plan will be in three stages:

1. Attack the router and the firewall; exploit them so that I have many options to conduct stage two.
2. Compromise as much of the service network as I can. The DNS is the only host whose IP is exposed so that is where I will start.
3. Shut down a vital host inside the secured network with a denial-of-service attack.

4.2 Attack the router and the firewall

Jeremy did not restrict virtual connections to the router by IP address through the use of the *access-class* command. Nor is the *Enable secret* or the *enable password* command used. What I would try to do is to telnet to the router and run script to attempt to logon to it. Once I received the ">" prompt, I could then issue a *show config* command do see how the router is configured. I could then open up ports for my attack machine's IP address and begin to conduct a surgical attack—particularly on its service network. Now that I have found the address of the firewall, I can exercise the same attack against it. If I am successful there, I can virtually shut down Jeremy's network because it is a single point of failure—everything goes through it!

4.3 Attack the DNS server

Since the DNS server is the only IP address, other than the router, that I can see, I will obviously want to make an attack against it. There are several vulnerabilities that have been found in BIND (Berkeley Internet Name Domain), the popular domain name server from the Internet Software Consortium (ISC). Any one of these vulnerabilities may allow an intruder to gain privileged access to name servers. By exploiting these vulnerabilities, I can execute arbitrary code with the privileges of the user running *named*, typically root. I can also disrupt the ability of the name server to respond to legitimate queries seriously degrade the performance of the name server. If I try hard enough, I might even be able to gain write access to the zone files and cause *named* to crash.

4.4 Attack an internal host

A stateless IP packet filter, such as a traditional access list in Cisco IOS software, must make all of its forwarding decisions for any specific packet based only on information in that packet. If the filtering is based on criteria such as TCP or UDP port numbers, the necessary information is typically present only in the initial fragment of a fragmented datagram. It is therefore impossible to tell if a non-initial fragment is part of a forbidden datagram or of a permitted one. Therefore, stateless packet filters that use such criteria must pass all, or substantially all, non-initial fragments. Such filters rely on blocking of initial fragments to prevent completed delivery of any forbidden datagrams. Extended access lists in Cisco IOS software can filter based on TCP and UDP port numbers, as well as based on ICMP packet types, and therefore fall into the vulnerable category. A Cisco IOS software extended access list will pass any non-initial fragment of a fragmented IP datagram.

PIX Firewall software up through version 4.2(1) will pass any non-initial fragment destined for any host for which either a static or a dynamic NAT table entry exists. Static NAT table entries are created with the PIX Firewall *static* command, and dynamic entries are created by inside hosts initiating IP traffic exchanges with outside hosts. No checks are made as to whether or not non-initial fragments belong to actual existing connections, so it is possible for any outside host to send fragments to any inside host that has a NAT entry, regardless of whether or not there is a connection between the two hosts, and regardless of whether a conduit is configured.

Since Jeremy's PIX firewall is using NAT, looks like I have a good opportunity for exploitation. In order to exploit this vulnerability an IP fragment application such as jolt2 can be used to fragment packets and send them to the firewall with the destination of the victim host.