# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

**SANS Network Security 2000, Monterey**
**GIAC Firewall and Perimeter Protection Curriculum**
**Eric Rupprecht**
**November 16, 2000**

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

# Assignment 1: Security Architecture

## *Assignment:*

***Assignment 1: Security Architecture - 25 Points***
*Define a security architecture. The goal of your policy is to use filtering routers, firewalls, VPNs and internal firewalls to rapidly implement the VISA "Ten Commandments" to the extent possible at GIAC Enterprises, a new Internet Startup that expects to earn 200 million per year in sales of online fortune cookie sayings. The "Ten Commandments" are listed below:*

1. *Install and maintain a working network firewall to protect data accessible via the Internet.*
2. *Keep security patches up-to-date.*
3. *Encrypt stored data accessible from the Internet.*
4. *Encrypt data sent across networks.*
5. *Use and regularly update anti-virus software.*
6. *Restrict access to data by business "need to know."*
7. *Assign unique IDs to each person with computer access to data.*
8. *Track access to data by unique ID.*
9. *Don't use vendor-supplied defaults for system passwords and other security parameters.*
10. *Regularly test security systems and processes*

*The student assignment is to produce a diagram, or set of diagrams with explanatory text defining how to use perimeter technologies to implement as many of the requirements above as possible. For this assignment you are a large and growing E-business that just completed a merger/acquisition you must consider the need for customers, suppliers, and partners.*

## *Overview:*

A security architecture for GIAC Enterprises will be designed to fit the VISA 'Ten Commandments" as listed in the assignment above. The security architecture will layer the defenses for GIAC Enterprises. Each layer will be explained below. The end of the document will cover some general security guidelines that GIAC Enterprises will need to follow to maintain the security architecture.

## *Design:*

The following diagram shows the network design for the security architecture.

© SANS Institute 2000 - 2002, Author retains full rights.

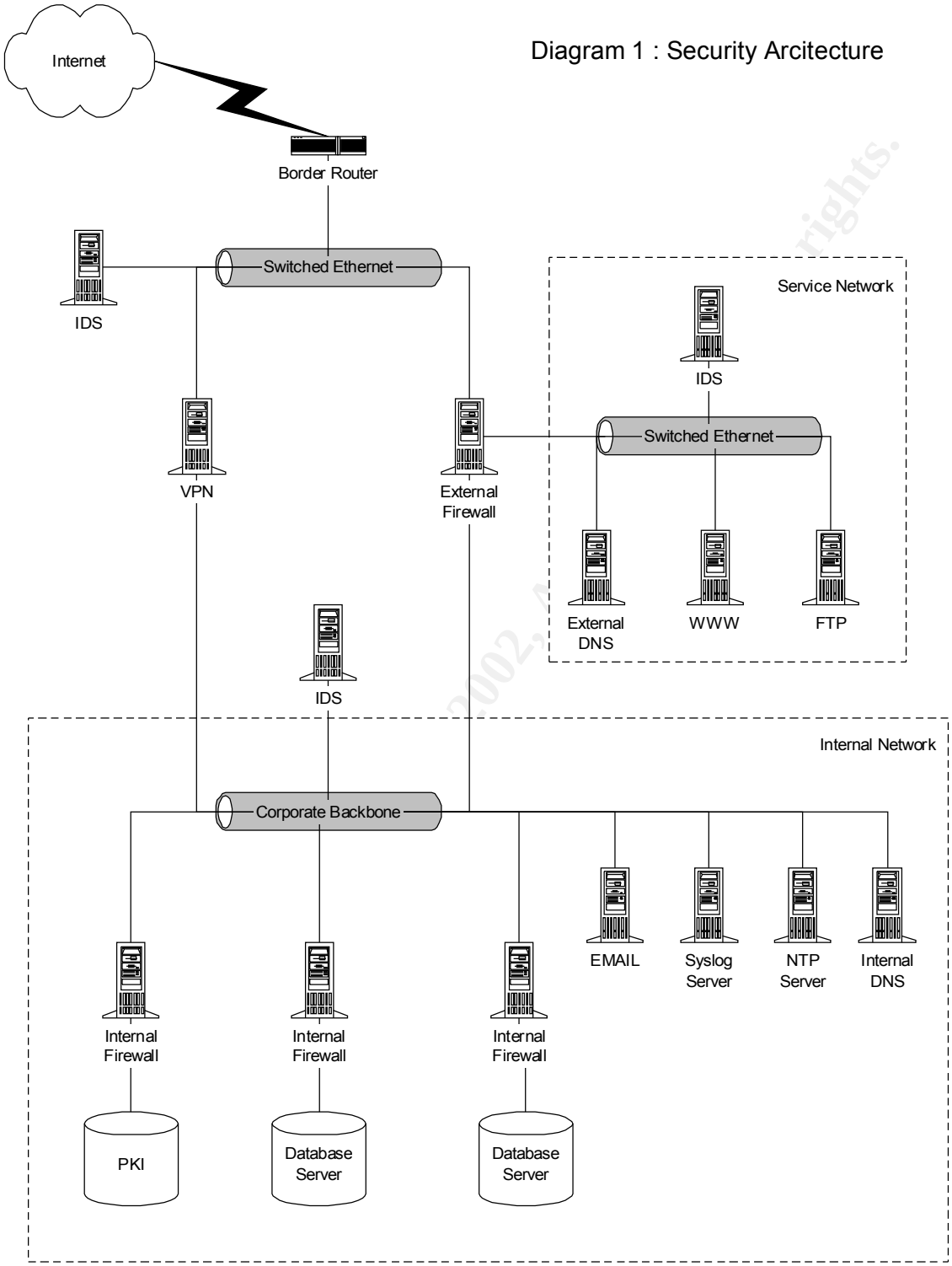



Diagram 1 : Security Arcitecture

## Border Router

The border router will have ACL's in place to drop specific traffic. The ACL's will filter the following:

- The router will have ingress ACL's to drop spoofed IP packets.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The router will have egress ACL's to drop spoofed packets. This will help prevent a hacker from using the GIAC network to attack other networks.
- The router will block all addresses that are in the private address space (RFC1918 and network 127 addresses).
- ICMP broadcasts and destination unreachable will be blocked.
- The router will drop all packets that have source routing enabled in the IP header options field.

The border router should have all unnecessary services disabled. These include the small services (chargen, date-time, etc), as well as finger, http, bootp, etc. Snmp should be disabled if it is not necessary for router management. If snmp is used, the community name needs to follow strong password guidelines. Do not use default community strings like public, private, or secret. Also, set access lists to limit whom can connect directly to the router through services like telnet or snmp. The router should be configured to send log files to a syslog server as well as keep logs locally.

## External Switch

This external switch sits outside the firewall and is unprotected. An attacker could compromise a switch with an ip stack and deny service to GIAC Enterprises customers by shutting down ports, changing VLANs, etc. This switch should not have an IP stack to prevent it from being compromised remotely. A simple switch with no remote management capabilities is the best choice here.

The same policy exists for switches used in the service network.

## Firewall

The firewall is the layer that will enforce most of the security policy. The selected network design implements a service network (screened subnet) that holds the untrusted GIAC servers. These include web, external DNS, and ftp servers.

A firewall rule base will be created that will allow Internet (Untrusted network) connections only to specific services on service network. For example, the Internet can connect to port 80 or 443 on the web server, but no other ports on that server. All other access to the service network will be blocked. Also, the Internet will not be allowed to connect to services on the internal (Trusted) network.

The Internal network will be allowed to access the service network with the same restrictions as the Internet. In addition, special groups will be created that will be allowed specific people to access the service network servers to perform administrative tasks. These connections should be encrypted using services like ssh and sftp to prevent connection sniffing. Services like telnet, ftp, and the r-commands will be disabled.

The firewall will not allow connections directly to the box except for a group of administrators. Ssh and sftp should be used for this connection. Each administrator should have a user account on the firewall and needs to login under this account. Direct login as root or Administrator should not be allowed. This will allow actions to be tracked by user ID. Choose strong passwords for all accounts, but especially for root or Administrator accounts. Run password-checking programs like Crack or l0phtcrack regularly to verify passwords are strong.

The firewall will maintain logs internally and also send the logs to the syslog server. NTP should be used to synchronize system clocks and maintain accurate log times. Only static routes should be used on the firewall. Dynamic routing protocols like RIP created a risk of DOS.

The firewall rules should block zone transfers. Zone transfers can reveal to much information about your organization. Use firewall rules to restrict access if zone transfers need to be done to an offsite secondary DNS server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

It is very important to keep all operating system and firewall software patches up to date. Subscribing to vendor mailing lists and regularly checking vendor websites is a good way to keep up to date about available patches. The firewall OS needs to be hardened before the firewall software is installed.

The firewall should be set up with network address translation (NAT) or application proxies to hide internal network addresses.

## VPN

The VPN server will be used to allow secure connections with business partners and suppliers (B2B). The VPN could be the firewall, or it could be a separate dedicated box. The design shows the VPN as a separate device in case the firewall does not support VPN functionality. IPSec protocols are recommended. Encapsulation Payload (ESP) is required to encrypt the information. Authentication header (AH) can be used to increase the security of the packet, but does not work if NATing is involved. All user connections should be done by a unique user id to track individual connections and strong passwords should be required.

## Service Network Servers

The firewall rules will block the service network servers from initiating a connection to the internal network. This is to prevent attackers that compromise the service network from gaining access to the Trusted network. This works in theory, but not in real life. These servers will need to connect to the trusted network to transfer logs to the syslog server. Many e-commerce webservers make calls to internal database servers which requires a connection to the internal network. Network Time Protocol (NTP) clients need to initiate a connection to a network time server which may be located in the internal network.

The servers in the service network need to be hardened. These servers should only run a single service. That is, a single server should not be running both EMAIL and DNS. Different services should be located on separate servers.

Root or Administrator passwords should be different for each service in the service network. This way, a cracked password on one server will not give access to the other servers. Administrators should be required to login with unique user ids. Password checking tools should be run periodically to verify that users are using strong passwords.

All logs should be maintained locally and transferred to a syslog server. NTP should be used to synchronize clocks to maintain accurate log times.

It is very important to keep all operating system and service software up to date with the most current patches. Subscribe to vendor mailing lists and regularly checking vendor web sites to keep up to date about available patches.

Split DNS will be used in this architecture. The external DNS server is located in the service network and will be authoritative for the GIAC Enterprises domain. The external DNS server will have addresses for any servers seen by the Internet, but will know nothing about the internal network. DNS should be run in a chroot environment under a non-privileged user account.

The internal DNS server will hold all addresses for the internal network. It will also have the addresses of the servers in the screened network so the internal DNS Server does not need to contact the external DNS server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Some B2B communications may still require ftp to transfer files. Typically, these files contain sensitive information that should be encrypted. Sftp (ftp over ssh) can be used to initiate an encrypted connection to the ftp server. Alternatively, the files can be PGP encrypted if standard FTP is used.

Sensitive information can also be distributed to other companies through a web server. Connections to sensitive information must to use SSL and require username/password authentication.

### Syslog Server

The syslog server will hold all logs from service network servers, firewalls, VPNs, and routers.

### Internal Firewalls

Internal firewalls will be deployed to further layer the lines of defense. An internal firewall will be used to segment off sensitive internal subnets. These subnets may contain database servers, payroll, PKI, etc. These firewalls should have the same security constraints as the external firewall.

### General Considerations

IDS should be installed at various areas of the network: between the border router and the firewall, on the trusted side of the firewall, and in the service network. IDS should be used to check for connections that are outside the security policy. This will help find configuration errors in the firewall rules and help determine when the network has been compromised.

Network time protocol (NTP) needs to be used to synchronize the clocks on all servers sending logs to the syslog server. Synchronize time is important for tracking an attackers moves through your network.

All hosts on the internal network should run anti-virus software. A host-based IDS or firewall software can be used on internal hosts for additional security.

## Assignment 2: Security Architecture

### *Assignment:*

> ***Assignment 2: Security Policy - 25 Points***
> *For the purposes of this assignment, your security policy should be focused on implementation of requirement number 1 above "Install and maintain a working network firewall to protect data accessible via the Internet." For a baseline policy, use the filtering recommendations located at www.sans.org/topten.htm. You DO NOT need to repeat that information. Instead, focus on ADDITIONAL filtering you would recommend and why. Keep in mind you are an E-Business with customers, suppliers, and partners, you MAY NOT simply block everything! Your policy should implement your design above.*
> *Write a tutorial on how to implement each additional recommended action in the filtering policy below on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. The base policy is taken from the recommended perimeter defense actions in the "Top Ten" document. Screenshots, network traffic traces, firewall log information and URLs to find further information should all be used. Be certain to include the following:*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

*1. The reason these services might be considered a vulnerability*
*2. Relevant information about the behavior of the protocol or service on the network*
*3. Syntax of the filter*
*4. Description of each of the parts of the filter*
*5. Explain how to apply the filter*
*6. If this filter is order dependant, what other rules should this filter precede and follow***
*7. Explain how to test the filter*
*8. Be certain to point out any tips, tricks, or gotcha's.*

*** You may find it easier to create a section of your practical that describes the order you would apply all of the rules rather than trying to do it with each policy cluster. Be certain to explain your reasons for the order you choose, we cannot read your mind.*

***Base Security Policy***

*Please note, we are not asking you to repeat the blocking instructions for the "top ten" security vulnerabilities. You may wish to reference one of the later practicals in your work since they were focused on blocking the "top ten" they can be found:*
*http://www.sans.org/giactc/gcfw.htm*
*In this section, we list the base security policy so you know what additional services to recommend blocking. These are ports that are commonly probed and attacked. Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order. Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.*

*1) Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.*
*2) Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)*
*3) RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)*
*4) NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)*
*5) X Windows -- 6000/tcp through 6255/tcp*
*6) 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)*
*7) Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)*
*8) 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.)*
*9) "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)*
*10) 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)*
*11) ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages.*

## *Overview:*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The security architecture will be implemented using a Cisco router as the border router and a NAI Webshield 300 E-ppliance as the external firewall. The internal firewalls will also be NAI Webshield E-ppliances. The Webshield runs NAI's Gauntlet 5.5 Application Proxy firewall. The default policy for Gauntlet is to deny all. Services will need to be enabled to allow specific protocols through the firewall.

## *Design:*

Diagram 1 above shows the network architecture. Table 1 below lists the names (network objects) that will be used to represent IP addresses and networks. It is assumed for this assignment that all addresses for the firewall, VPN, and service network fall in the 2.2.2.2/24 address space.

| Server | Server Name | Part of Network |
|---|---|---|
| Border Router | Router | dmz-net |
| External DNS | Ext-dns-server | Service-net |
| Web server | Www-server | Service-net |
| Ftp Server | Ftp-server | Service-net |
| Syslog Server | Syslog-server | Internal-net |
| NTP Server | Ntp-server | Internal-net |
| Email Server | Email-server | Internal-net |
| Internal DNS Server | Int-dns-server | Internal-net |

**Table 1: Network Objects**

### Border Router Rules

The border router will be set up with ACLs to prevent spoofing and drop selected ICMP. The router will forward all other traffic to the firewall or VPN. Cisco IOS 12.0 was used on the border router.

Ingress ACLs are added to the routers outside interface to block packets with spoofed source addresses. These rules drop all packets that have source addresses in the private address space.

```
!Block RFC 1918 addresses
access-list 1 deny 10.0.0.0 0.255.255.255 log
access-list 1 deny 172.16.0.0 0.15.255.255 log
access-list 1 deny 192.168.0.0 0.0.255.255 log
!block loopback and other illegal addresses
access-list 1 deny 127.0.0.0 0.255.255.255 log
access-list 1 deny 0.0.0.0 0.255.255.255 log
access-list 1 deny 255.255.255.255 0.0.0.0 log
!Block spoofing of internal addresses (This includes the firewall and service network servers)
access-list 1 deny 2.2.2.0 0.0.0.255 log
!Allow everything else
access-list 1 permit any

! (outside interface of router)
interface serial 0
ip access-group 1 in
```

Egress ACLs are set up on the inside interface of the router to prevent your network from sending spoofed packets.

```
!allow firewall and service network server source addresses.
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
access-list 2 permit 2.2.2.0 0.0.0.255
!block everything else because it is spoofed
access-list 2 deny any log

! (inside interface of router)
interface ethernet 0
ip access-group 2 in
```

The following will prevent ICMP broadcasts, ICMP unreachable messages, and IP source routing. Also, we want to disable SNMP,all unused tcp and udp services, and cisco discovery protocol.

```
!(gobal config mode)
no ip source-route
no snmp.
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http service
no ip bootp service

!(on the interface)
no ip directed-broadcast
no ip unreachables
no cdp enable
```

The logs need to be transferred to the syslog server.

```
logging <syslog server address>
```

Place an access list defining the IP addresses that can connect to the router. Only IP addresses listed in the access list will be allowed to make a telnet connection to the router. The telnet connection will appear to come to the firewall since a telnet proxy is used.

```
access-list 3 permit <firewall-address>
line vty 0 4
        access-class 3
        login
```

The border router will use only static routes. Routing protocols like RIP will be disabled.

## Firewall Rules

The firewall chosen is the Gauntlet 5.5 Application Proxy firewall. The gauntlet management software makes it difficult to display information because source and destination rules are on different screens. For the purpose of this assignment, the rules will be shown in a format that is easier to read. Also, Gauntlet does not allow the use of network objects as a destination. This will report will use network objects for destinations for ease of readability.

Gauntlet blocks and logs all ports by default. The following section will explain what proxies need to be enabled to allow access as defined by the security policy. The following proxy rules need to be created to allow internet access to the Service Network Servers.

© SANS Institute 2000 - 2002, Author retains full rights.

Gauntlet has default rules that limit access to the firewall. The r-commands, telnet, and ftp to the firewall will all be disabled at the application proxy. There is a specific rule set up to allow access to the firewall management service.

| Source | Service | Destination | Action |
|---|---|---|---|
| Firewall-management | ESPM | firewall | Allow |

Internet DNS queries will be allowed by setting up a packet filter bound to the outside interface of the firewall. Gauntlet 5.5 does not have a DNS specific or generic UDP proxy. Therefore, a packet filter must be used. 53/TCP will not be allowed because we do not want to allow zone transfers.

| Source | Source Port | Destination | Destination Port | Filter Access |
|---|---|---|---|---|
| Any | * | Ext-dns-server | Dns (53/udp) | Allow UDP with replies |

We need to allow the Internet to access the web server. This is typically done with a generic tcp plug listening on port 80/tcp instead of the full http application proxy. Port 443/tcp will also be allowed for ssl traffic.

| Source | Service | Destination | Action |
|---|---|---|---|
| Any | Http (80/tcp)<br>Ssl (443/tcp) | www-server | Allow |

We need to enable EMAIL to get to the email-server. Gauntlet 5.5 has a proxy for handling SMTP EMAIL. The firewall is configured as the mail exchanger in DNS. EMAIL is delivered to the firewall where the smap process caches the message to disk. The smapd process reads the message and delivers it to the mail hub specified in the proxy. The mail hub is the email-server in the internal network. Virus Scanning will be enabled at the proxy to check all EMAIL before entering the trusted network. Anti-spam and anti-relay rules can be enabled as needed.

| Source | Service | Destination | Action |
|---|---|---|---|
| Any | Mail (25/tcp) | email-server | Allow |

The Internet will be able to access the ftp service on the ftp-server. The ftp proxy allows the commands in the ftp protocol to be restricted. For example, ftp GET can be allowed while PUT is disallowed. The ftp proxy should only allow the minimum commands necessary.

| Source | Service | Destination | Action |
|---|---|---|---|
| Any | ftp (21/tcp) | ftp-server | Allow |

In general, the Service network will not be allowed to initiate a connection to the Internal Network. There are a couple exceptions to this, NTP and syslog.

The servers in the service-network will sends logs to the syslog server. This will be done through packet filters allowing 514/udp. A packet filter is not needed for the firewall to send logs to the syslog server. There also needs to be a packet filter to allow the Border Router to send logs to the syslog server.

| Source | Source Port | Destination | Destination Port | Filter Access |
|---|---|---|---|---|
| Service-net | * | Syslog-server | syslog (514/udp) | Allow UDP with replies |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| | | | | |
|---|---|---|---|---|
| Router | * | Syslog-server | syslog (514/udp) | Allow UDP with replies |

The service network servers and the border router also need to be able to call the internal ntp server. The packet filter rules are similar to those needed for syslog.

| Source | Source Port | Destination | Destination Port | Filter Access |
|---|---|---|---|---|
| Service-net | * | ntp-server | ntp (123/udp) | Allow UDP with replies |
| Router | * | ntp-server | ntp (123/udp) | Allow UDP with replies |

Rules need to be created to allow ssh through the firewall. This is to allow Administrators to access the servers in the Service Network. The rule should only allow specific IP addresses to access the service network. Sftp will be used for all file transfers.

| Source | Service | Destination | Action |
|---|---|---|---|
| Administrator IP Addresses | ssh (22/tcp) | Service-net | Allow |

A rule does not need to be created to enable ssh to the firewall for administration, but there is an issue that needs to be addressed. Gauntlet 5.5 will have a generic proxy listening on port 22 to enable ssh to the service network. This means that the ssh daemon cannot run on port 22 on the firewall. To resolve this, ssh on the firewall will be bound to a high port like 2022. Ssh connections to the firewall will be initiated on port 2022 while ssh connections to the service network will use the normal port 22.

Rules need to be created to allow telnet through the firewall to the border router. This is to allow access the to the border router for administration. The rule should only allow specific IP addresses to access the border router. Ssh would be preferable to telnet, but ssh is not available on Cisco routers at this time.

| Source | Service | Destination | Action |
|---|---|---|---|
| Administrator IP Addresses | telnet (23/tcp) | Router | Allow |

Appendix A shows all the rules combined together.

## VPN

The VPN gateway is shown as a separate device in the security architecture. The VPN could be a separate device or could be the firewall. Both Gauntlet 5.5 and Checkpoint Firewall-1 have VPN capabilities available as an add-on to the firewall. This creates one management point for all firewall and VPN rules, but will also make the rules much more complex. There is a greater potential for configuration errors as more rules are added. It may be advantageous in your environment to separate the VPN gateway from the firewall.

The Nortel Conitivity Extranet Switch 4500 is hardware VPN solution. This solution supports host-to-gate connections for mobile users and gate-to-gate connections between remote sites and vendors. The Nortel VPN comes with basic firewall support built in or supports a checkpoint firewall module add-in. This allows for a separation in rules between the external firewall and the VPN. The main advantage to this is debugging. It is much easier to debug configuration errors and problems when the firewall and VPN are separate devices.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

# Assignment 3: Audit your Security Architecture

***Assignment 3: Audit your security architecture - 50 Points***

*For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises, a electronic commerce facility that is the largest supplier of electronic fortune cookie sayings in the world. The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly. Your assignment is:*

- *Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.*
- *Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.*
- *Perimeter analysis. Based on your assessment and referring to data from your assessment, analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.*

***NOTE:*** *Assignment 3 should be primarily focused on VISA requirement number 1, "Install and maintain a working network firewall to protect data accessible via the Internet." and your base + recommended security policy. Credit towards honors status will be given to students that are able to design an audit that can test all or a good deal of the VISA requirements.*

## *Plan the assessment.*

The approach for validating the security architecture will be to test each layer independently of the others. As each layer is tested, compare the results to the security policy. The security policy at each layer needs to be well defined so that it can be validated. Some companies change policies often and the security policy must be kept up to date.

The assessment will be done outside of peak hours for a couple reasons. First, GIAC Enterprises depends on e-commerce for their sales. Any disruption in this service would not be acceptable for this company, their customers, or their business partners. Second, evaluating log files for the perimeter assessment is often easier when production traffic is at a minimum.

The general procedure for assessing each layer is as follows:

1. *Assess the security of the device.*

This step will verify network connections to that box. Is telnet enabled when only ssh is allowed for remote connections? Is NFS enabled when it shouldn't be?

The patch level will be checked to see if it is up to date. All OS patches need to be up to date. Application patches must also be at the current version. Applications include things like BIND on the DNS server, the web server software, or the firewall software.

User security must also be verified. Password will be checked to make sure they are strong. Verify that administrators must login under individual accounts and that direct root logins are not permitted.

2. *Assess the security through the device.*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This step will verify the router ACL and firewall rules. Verify that only authorized ports are open. Verify that the firewall restricts sources and destinations to services where appropriate.

3. *Verify local logs.*

The local logs on the device should be logging access success and failure events. Verify that this is correct.

*4. Verify remote logs*

The local logs are also being sent to the syslog server. Verify that the logs on the syslog server match the local logs.

*5. Verify IDS*

Verify that IDS is alerting on security violations at each layer. The IDS rules also need to be checked to verify they are up to date with the security policy.

## *Implement the assessment.*

### Border Router

**Ingress ACL**

The ingress ACL's on the border router will be validated using NMAP. NMAP will use the –S option to spoof the source address to simulate private and illegal source addresses. The NMAP commands used are:

```
nmap -sS -v -S 10.1.1.2 -e eth0 -P0 -p 23 2.2.2.2
nmap -sS -v -S 172.16.1.2 -e eth0 -P0 -p 23 2.2.2.2
nmap -sS -v -S 192.168.1.2 -e eth0 -P0 -p 23 2.2.2.2
nmap -sS -v -S 127.0.0.1 -e eth0 -P0 -p 23 2.2.2.2
nmap -sS -v -S 255.255.255.255 -e eth0 -P0 -p 23 2.2.2.2
nmap -sS -v -S 2.2.2.2 -e eth0 -P0 -p 23 2.2.2.2
```

The following is the output from one of the NMAP scans showing the results are filtered.

```
[root@t00c23c /root]# nmap -sS -v -S 10.1.1.2 -P0 -p 23 -e eth0 2.2.2.2

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Initiating SYN half-open stealth scan against  (2.2.2.2)
The SYN scan took 36 seconds to scan 1 ports.
Interesting ports on  (2.2.2.2):
Port       State       Service
23/tcp     filtered    telnet

Nmap run completed -- 1 IP address (1 host up) scanned in 116 seconds
```

The success of this test is verified by looking at the router logs. These logs should also be compared to the logs on the syslog server to verify that they match. The IDS server between the router and the external firewall should be checked. The IDS server should show alerts if this test traffic is leaking through the router. The router logs show the denied packets:

```
23:01:39: %SEC-6-IPACCESSLOGS: list 1 denied 10.1.1.2 6 packets
```

© SANS Institute 2000 - 2002, Author retains full rights.

23:08:40: %SEC-6-IPACCESSLOGS: list 1 denied 172.16.1.2 5 packets
23:13:40: %SEC-6-IPACCESSLOGS: list 1 denied 192.168.1.2 5 packets
23:14:52: %SEC-6-IPACCESSLOGS: list 1 denied 127.0.0.1 1 packet
23:37:25: %SEC-6-IPACCESSLOGS: list 1 denied 255.255.255.255 1 packet
23:47:17: %SEC-6-IPACCESSLOGS: list 1 denied 2.2.2.2 1 packet

**Egress ACL**

The egress ACL's on the border router will also be validated using NMAP. Several spoofed addresses could be tried, but this test only used one. The following command was used to spoof packets leaving the internal network.

nmap -sS -v -S 1.1.1.3 -e eth0 -P0 -p 23 1.1.1.2

The logs showed the following packet was denied. Again, this result should be compared to the syslog server. Review the IDS server alerts since IDS should detect these spoofed packets.

23:59:19: %SEC-6-IPACCESSLOGS: list 2 denied 1.1.1.3 1 packet

**ICMP Broadcast**

Ping the outside interface of the router to create ICMP Broadcasts. Use ping with a destination broadcast address.

ping 2.2.2.255

The router should drop these packets. This can be verified by placing a network sniffer on the opposite side of the router to see if the router forwards these packets.

**Router services**

Finally, NMAP was used to scan the router to check for open services. The command used is:

nmap -sS -v -P0 1.1.1.1
nmap -sU -v -P0 1.1.1.1

The results are as follows:

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Initiating SYN half-open stealth scan against (1.1.1.1)
Adding TCP port 23 (state open).
The SYN scan took 15 seconds to scan 1523 ports.
Interesting ports on (1.1.1.1):
(The 1506 ports scanned but not shown below are in state: closed)
Port State Service
23/tcp open telnet

Nmap run completed -- 1 IP address (1 host up) scanned in 95 seconds

These results show that almost all services have been closed. We expected telnet to be open. The UDP scan resulted in no ports open.

© SANS Institute 2000 - 2002, Author retains full rights.

## External Firewall

**External Interface**

The external interface of the firewall will be scanned with nmap.

```
Nmap –sS –v –P0 –p 1-65535 2.2.2.2
Nmap –sU –v –P0 2.2.2.2
```

The results of the scan are as follows:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host firewall.domain.com (2.2.2.2) appears to be up ... good.
Initiating SYN half-open stealth scan against firewall.domain.com (2.2.2.2)
The SYN scan took 559 seconds to scan 65535 ports.
Interesting ports on firewall.domain.com (2.2.2.2):
(The 65520 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
111/tcp    filtered    sunrpc
113/tcp    open        auth
443/tcp    open        https
7070/tcp   open        unknown
8004/tcp   open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 561 seconds


Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host firewall.domain.com (2.2.2.2) appears to be up ... good.
Initiating FIN,NULL, UDP, or Xmas stealth scan against firewall.domain.com (2.2.2.2)
The UDP or stealth FIN/NULL/XMAS scan took 1287 seconds to scan 1448 ports.
Interesting ports on firewall.domain.com (2.2.2.2):
(The 1442 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp     open        domain
111/udp    filtered    sunrpc
123/udp    open        ntp
500/udp    open        isakmp
514/udp    open        syslog
32774/udp  open        sometimes-rpc12
34887/udp  open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 1289 seconds
```

The firewall logs should reflect the rejected port scans. The following shows a few lines from the logs.

```
Nov 13 21:21:16 firewall unix: securityalert: udp if=qe0 from 1.1.1.2:43143 to 2.2.2.2 on
unserved port 6148
```

© SANS Institute 2000 - 2002, Author retains full rights.

Nov 13 21:21:17 firewall unix: securityalert: udp if=qe0 from 1.1.1.2:43143 to 2.2.2.2 on unserved port 962
Nov 13 21:21:17 firewall unix: securityalert: udp if=qe0 from 1.1.1.2:43143 to 2.2.2.2 on unserved port 776
Nov 13 21:21:18 firewall unix: securityalert: udp if=qe0 from 1.1.1.2:43143 to 2.2.2.2 on unserved port 293

Nov 13 18:52:29 firewall unix: securityalert: tcp if=qe0 from 1.1.1.2:63740 to 2.2.2.2 on unserved port 30545
Nov 13 18:52:29 firewall unix: securityalert: tcp if=qe0 from 1.1.1.2:63740 to 2.2.2.2 on unserved port 65529
Nov 13 18:52:29 firewall unix: securityalert: tcp if=qe0 from 1.1.1.2:63740 to 2.2.2.2 on unserved port 26902
Nov 13 18:52:29 firewall unix: securityalert: tcp if=qe0 from 1.1.1.2:63740 to 2.2.2.2 on unserved port 35476

Compare the results of the scan to the IDS alerts and the logs on the syslog server. Also, the results of the scan need to be compared to the security policy. This will be done in the next section.

**Service and Internal Interface**

The service and internal interfaces of the firewall will also be scanned. The service interface needs to be checked for configuration errors that would allow a compromised service network server to access the internal network. The internal interface needs to be checked for configuration errors that would allow the internal network unauthorized access to the service network and Intranet.

**The servers**

The service network servers need to be scanned. Nessus is a port scanner that checks for vulnerabilities and configuration errors in services. I highly recommend running Nessus or an equivalent product against the service network servers and the gauntlet firewall on a regular basis.

The following is an edited version from a Nesses scan of the ftp server.

```
Nessus Scan Report
------------------
SUMMARY
 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 4
 - Number of security warnings found : 8
 - Number of security notes found : 6

TESTED HOSTS

 2.2.2.5 (Security holes found)

DETAILS
+ 2.2.2.5 :
 . List of open ports :
   o ftp (21/tcp) (Security hole found)
   o ssh (22/tcp)
   o auth (113/tcp)
```

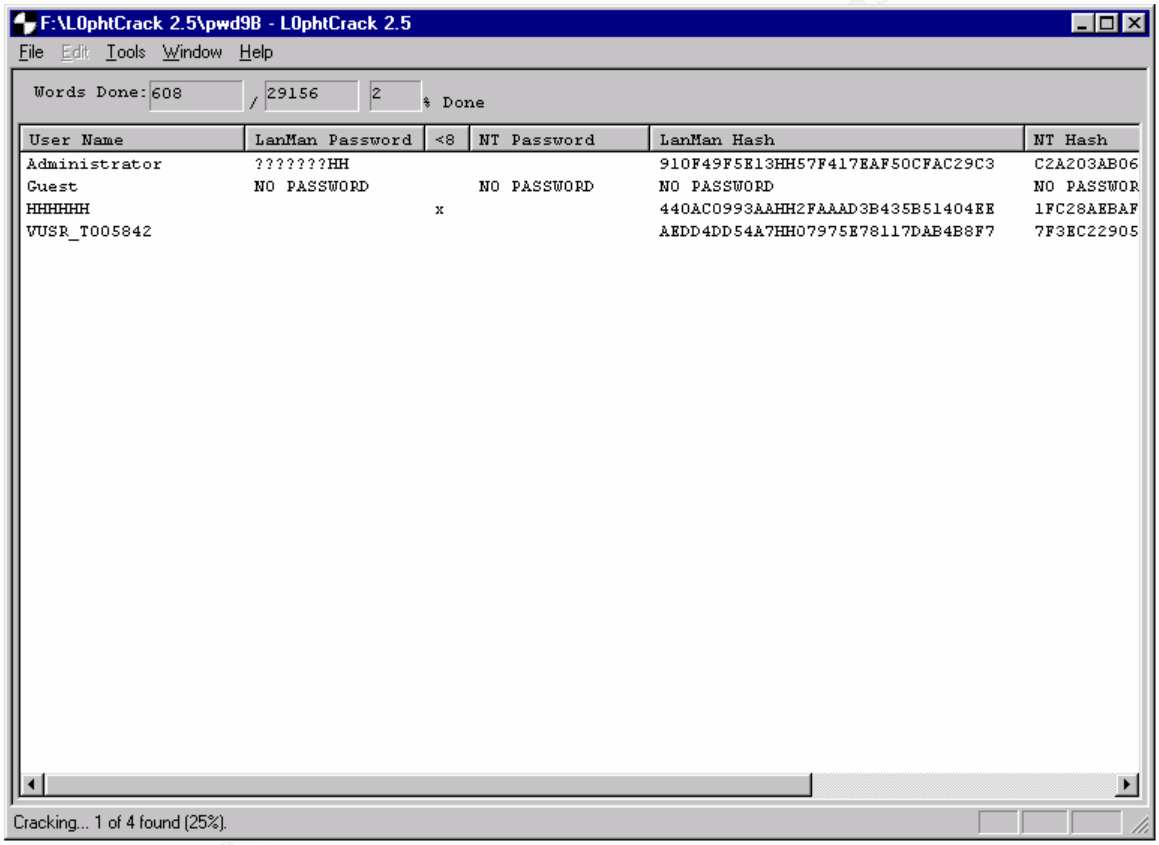
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
  o general/tcp (Security notes found)
  o general/udp (Security notes found)

. Vulnerability found on port ftp (21/tcp) :
   The remote FTP server closes
   the connection when one of the commands
   USER, PASS or HELP is given with a too
   long argument.

   This probably due to a buffer overflow, which
   allows anyone to execute arbitrary code
   on the remote host.

   This problem is threatening, because
   the attackers don't need an account
   to exploit this flaw.

   Solution : Upgrade your FTP server or change it
   Risk factor :
    High

. Warning found on port ftp (21/tcp)

   The FTP service allows anonymous logins. If you do not want
   to share data with anyone you do not know, then you should
   deactivate
    the anonymous account, since it can only cause troubles.
    Under most Unix system, doing :
     echo ftp >> /etc/ftpusers
    will correct this.

    Risk factor : Low
   CVE : CAN-1999-0497

. Warning found on port ftp (21/tcp)

   It was possible to
   shut down the remote FTP server by issuing
   a CWD command followed by a too long
   argument.

   This problem allows crackers to prevent
   your site from sharing some resources
   with the rest of the world.

    Solution : upgrade to the latest version your FTP server.

   Risk factor : Medium
   CVE : CAN-1999-0838

. Information found on port ftp (21/tcp)

   Remote FTP server banner :
    ftpserver.domain.com FTP server (Version wu-2.6.1(1) Wed
    Aug 9 05:54:50 EDT 2000) ready.

. Information found on port general/tcp
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
    Nmap found that this host is running Solaris 2.6 -
    2.7, Solaris 7

--------------------------------------------------
This file was generated by the Nessus Security Scanner
```

The servers in the service network and the firewall need to be checked for strong passwords. There are several utilities that can do this. Crack or John the Ripper will crack UNIX passwords. L0phtcrack can be used for NT servers. The goal here is not to crack every password, just to find weak passwords. Therefore, cracking does not need to be run to completion. The following is an example of l0phtcrack at work.




**External DNS**

Split DNS was implemented to prevent exposing the internal network addresses to the Internet. Zone transfers should be blocked. DIG (Unix) or Samspade (NT) can be used to test DNS functionality. The following is an example of DIG.

```
> dig domain.com any

; <<>> DiG 8.2 <<>> domain.com any
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr aa ra; QUERY: 1, ANSWER: 6, AUTHORITY: 2, ADDITIONAL: 4
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
;; QUERY SECTION:
;;        domain.com, type = ANY, class = IN

;; ANSWER SECTION:
domain.com.          1H IN A      2.2.2.50
domain.com.          1H IN MX     10 ns4.domain.com.
domain.com.          1H IN MX     10 ns5.domain.com.
domain.com.          1H IN NS     ns1.domain.com.
domain.com.          1H IN NS     ns2.domain.com.
domain.com.          1H IN SOA    domain.com. hostmaster.domain.com. (
                                  2000102001     ; serial
                                  1H             ; refresh
                                  2H             ; retry
                                  1W             ; expiry
                                  1H )           ; minimum


;; AUTHORITY SECTION:
domain.com.          1H IN NS     ns1.domain.com.
domain.com.          1H IN NS     ns2.domain.com.

;; ADDITIONAL SECTION:
ns4.domain.com. 1H IN A      2.2.2.55
ns5.domain.com. 1H IN A      2.2.2.200
ns1.domain.com. 1H IN A      2.2.2.4
ns2.domain.com. 1H IN A      2.2.2.7

;; Total query time: 83 msec
;; FROM: test to SERVER: default -- 1.1.1.2
;; WHEN: Mon Nov 13 23:17:20 2000
;; MSG SIZE  sent: 31  rcvd: 262
```

A zone transfer can be attempted with the host –l command. This query should be refused if zone transfers have been properly blocked.

```
> host -l domain.com
Server failed: Query refused
```

## *Perimeter Analysis*

The following section will analyze the results of the perimeter assessment. Configuration errors will be identified and security enhancements suggested.

### Border Router

The router ACL rules can be improved by blocking ICMP time exceeded messages, Ingress ICMP echo-requests, and egress ICMP echo-replies. This can be accomplished by using extended access lists on the Cisco router. The previous router ACL should be converted to extended ACLs and combined with the rules below.

```
!on the router external interface
!block ICMP echo requests
access-list 101 deny icmp any any echo-request log
access-list 101 permit any any
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
!on the router internal interface
!block ICMP echo replies
access-list 102 deny icmp any any echo-reply
!block outgoing TTL exceeded messages
access-list 102 deny icmp any any time-exceeded
access-list 102 permit any any
```

The Cisco Router in this security architecture limits incoming telnet sessions by IP address and has a global login password. A change should be made here to force authentication be unique user ID. A tacacs server should be implemented to verify the incoming connections by user account. The port 49/udp will need to be opened on the firewall to allow tacacs authentication to the tacacs server.

## Firewall

The follow table shows the result to the port scan on the external interface and explains the results.

| Port | State | Service | Explanation |
|---|---|---|---|
| 21/tcp | open | ftp | The security policy allows for ftp to the Service Network ftp server. |
| 22/tcp | open | ssh | The security policy allows for ssh to the Service Network from the administrator IP addresses on the internal network. The firewall rules reject connections to this port for invalid source IP addresses. This was tested by telneting to port 22 on the firewall with various source IP addresses. |
| 23/tcp | open | telnet | The security policy allows for telnet to the border router from the administrator IP addresses on the internal network. The firewall rules reject connections to this port for invalid source IP addresses. This was tested by telneting to port 23 on the firewall with various source IP addresses. |
| 25/tcp | open | smtp | The security policy allows for smtp mail to be accepted by the firewall and relayed to an internal mail hub. |
| 53/tcp | open | domain | This port is for tcp zone transfers. Zone transfers are currently not allowed by bind on the external DNS server, but this port should be closed on the firewall also. |
| 80/tcp | open | http | The security policy allows for http to the Service Network www server. |
| 111/tcp | filtered | sunrpc | Sunrpc has vulnerabilities associated with it and should not be running. The gauntlet installation program generally removes this service, but did not this time. RPC can be stopped by running: /etc/rc2.d/S71rpc stop Sunrpc can be disabled by renaming the above script. |
| 113/tcp | open | auth | Ident is frequently used by ftp and email servers. This should remain open. |
| 443/tcp | open | https | The security policy allows for https to the Service Network www server. |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| | | | |
|---|---|---|---|
| 7070/tcp | open | unknown | This port is for the Gauntlet RealAudio proxy and should not be running. This can be disabled in the gauntlet administration program. |
| 8004/tcp | open | unknown | This is the gauntlet administration port. The rules prevent connection to this port except by administrator IP addresses. |
| 53/udp | open | domain | The security policy allows dns queries. This port forwards DNS requests to the external DNS server in the Service Network. |
| 111/udp | filtered | sunrpc | Sun rpc should not be running. This port was disabled when 111/tcp was disabled. |
| 123/udp | open | ntp | The security policy allows the border router to make ntp requests to the NTP server. |
| 500/udp | open | isakmp | This port is used for IPSEC key exchange. This is not necessary since the Nortel box is used as the VPN solution. The VPN addon-product for Gauntlet should not have been installed on this box. |
| 514/udp | open | syslog | The security policy allows for logs to be transferred from the border router to the syslog server. |
| 32774/udp | open | sometimes-rpc12 | This is part of sunrpc and should be running. This port was disabled when 111/tcp was disabled. |
| 34887/udp | open | unknown | This port is part of syslogd |

## Protecting Against Attacks

The firewalls and service network service have been hardened against attack, but new exploits are continuously being discovered. The attacker will install backdoors as soon as the box is exploited. Attackers may add SUID binaries to give easy root-shell access. Catalogs of SUID binaries can be created with the command:

```
> find / -perm –4000 –type f > /catalog/suid.list
```

This catalog should be compared against the SUID binaries on the system regularly.

System Administrators can also protect against Trojans by doing system integrity checks of files on the system. Tripwire is a commercial product that can provide this protection. Tripwire creates a database that holds filenames, permissions, sizes, timestamps, checksums, and hashes of critical files and directories. The critical files and directories to be checked are listed in the Tripwire configuration file. The following is a sample configuration file.

```
#Monitor for new/deleted entries in / and /home.  Do not traverse subdirectories.
=/                      R
=/home                  R
#Check the Permissions and attributes of the /tmp directory.
=/tmp                   L
# Check if roots hidden files have changed
/home/root/.cshrc       R
/home/root/.rhosts      R
/home/root/.forward     R
/home/root/.profile     R
# The following directories should be fairly static
/opt                    R
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
/sbin                   R
/stand                  R
/usr                    R
# Check for changes in the /etc directory
/etc                    R
```

The Tripwire database is configured once and updated any time valid system changes are made. Tripwire is run periodically in Integrity Checking Mode to verify the current system against the database, and can EMAIL results to the administrator.

## Load balancing firewall

The security architecture has only one firewall on the perimeter. Two firewalls should be implemented in this architecture in a load-balanced configuration. Most companies load balance firewalls to provide higher throughput through the firewalls and eliminate single-points-of-failure. There are also security benefits to load balancing firewalls (and all service network servers). Many companies cannot afford to have an interruption in service and require all service work and patches to be done in service windows outside of peak hours. Load balancing allows a firewall (or service network server) to be removed from service during normal business hours. Patches can be tested and applied immediately instead of waiting for a maintenance window.

© SANS Institute 2000 - 2002, Author retains full rights.

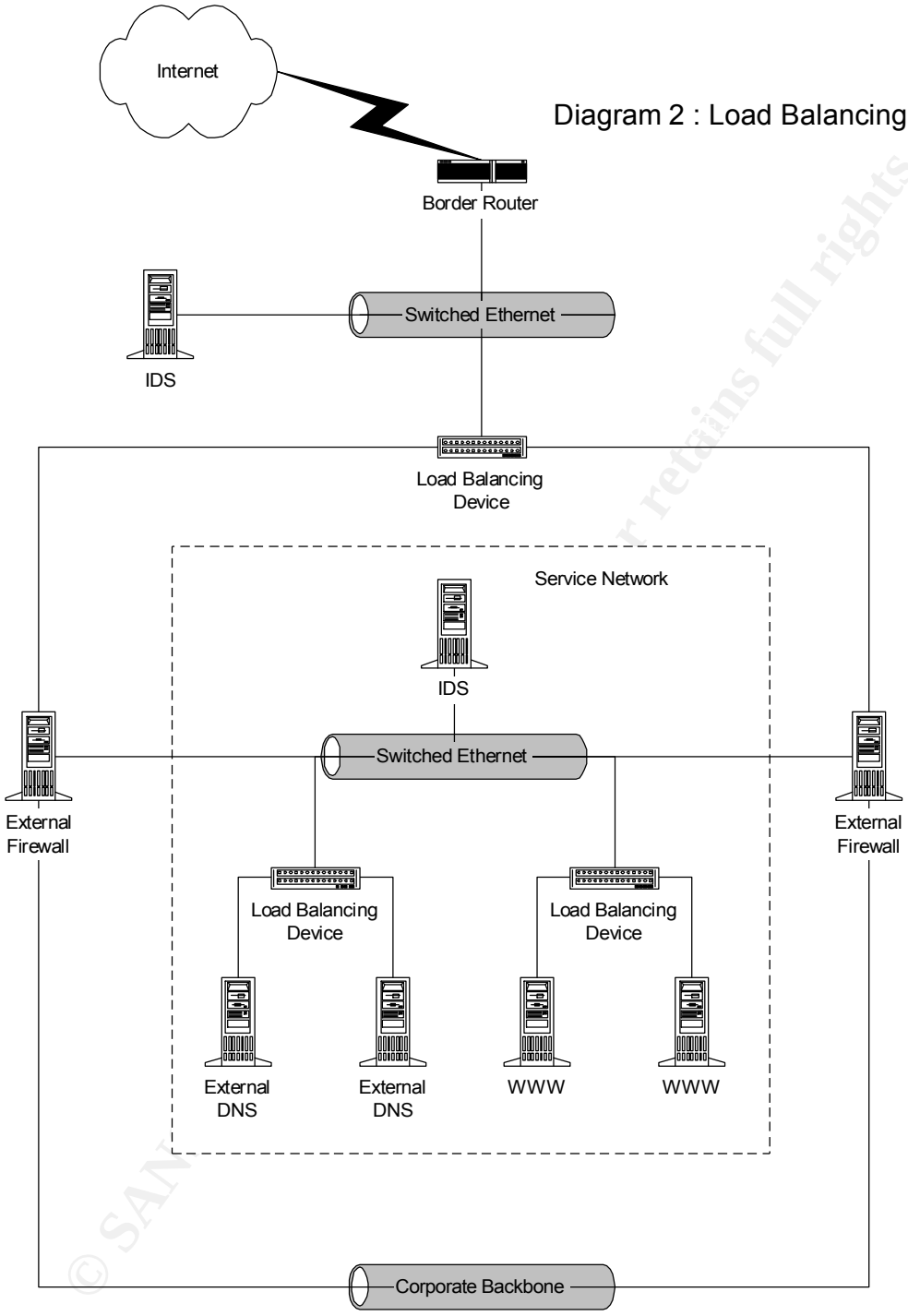



Diagram 2 : Load Balancing

## Firewall DMZ

E-commerce web servers typically need to make backend calls to corporate database servers on the Internal network. The rule of thumb for the service network designed above is that the service network cannot initiate a connection to the internal network. This rule does not hold up for the above mentioned web-servers. A two-layer firewall DMZ can be used in this case. The external firewall layer allows connections

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to services on DMZ servers. The external firewalls are typically high speed packet filter or stateful inspection firewalls. Checkpoint FW-1 is used in this example.

The Internal firewalls allow the DMZ servers to make backend calls to the Internal Network. These calls are typically to directory, database or transaction servers. The internal firewalls are typically application proxy firewalls that provide high security, but do not need the high speed of the external firewalls. NAI Gauntlet is used in this example.

The DMZ servers typically have two network interfaces. One allows connection to the external firewalls and the other to the internal firewalls. This separation means that there is no direct path from the external firewalls to the internal firewalls.

This design increases the security of the perimeter. If an attacker compromises the external firewall or a DMZ server, the internal firewall is still protecting the internal network. Exploiting the internal network is made even more difficult by having different vendor's firewalls at each layer. The attacker would need two different exploits since each layer users different vendor firewalls to penetrate the perimeter and gain access to the internal network.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

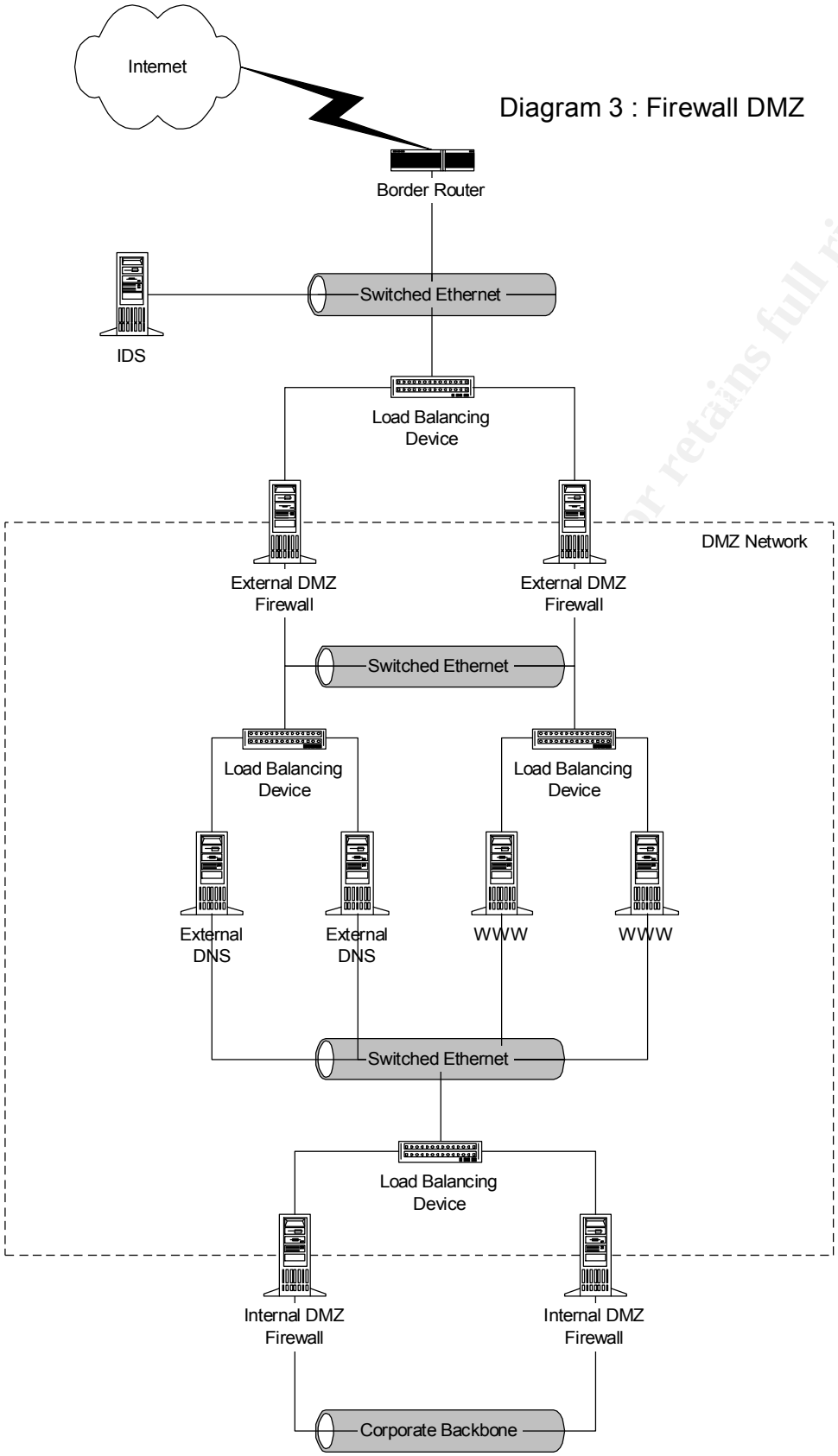



Diagram 3 : Firewall DMZ

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

## *Appendix A: Firewall Rules*

Packet Filter Rules:

| Source | Source Port | Destination | Destination Port | Filter Access |
|---|---|---|---|---|
| Any | * | Ext-dns-server | Dns (53/udp) | Allow UDP with replies |
| Service-net | * | Syslog-server | syslog (514/udp) | Allow UDP with replies |
| Router | * | Syslog-server | syslog (514/udp) | Allow UDP with replies |
| Service-net | * | ntp-server | ntp (123/udp) | Allow UDP with replies |
| Router | * | ntp-server | ntp (123/udp) | Allow UDP with replies |

Application Proxy Rules:

| Source | Service | Destination | Action |
|---|---|---|---|
| Firewall-management | ESPM | Firewall | Allow |
| Any | http (80/tcp)<br>Ssl (443/tcp) | www-server | Allow |
| Any | Mail (25/tcp) | email-server | Allow |
| Any | ftp (21/tcp) | ftp-server | Allow |
| Administrator IP Addresses | ssh (22/tcp) | Service-net | Allow |
| Administrator IP Addresses | telnet (23/tcp) | Router | Allow |

## *References*


Garfinkel, Simson and Gene Spafford, *Practical UNIX & Internet Security*, O'Reilly Publishing, 1996

No Author, *Practical UNIX and Network Security*, HP Educational Services, 2000

McClure, Stuart, Joel Scambray, George Kurtz, *Hacking Exposed*, Osbourne, 1999

Hunt, Craig, *TCP/IP Network Administration*, O'Reilly

Cheswick, William and Steven Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994

Chapman, D. Brent and Elizebeth Zwicky, *Building Internet Firewalls,* O'Reilly, 1995


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.