

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.

Paul Mason Ford
GCFW Practical Assignment Version 1.5e

GIAC Enterprises' Network Security Architecture

Assignment 1 – Security Architecture

The Work Environment

GIAC Enterprises, an e-fortune cookie saying company, has requested a security architecture that will incorporate proven security components and be cost effective to purchase and maintain. GIAC Enterprises is expecting to conduct $200 million in business, annually. However dot-coms have been failing at a dramatic rate. Therefore, constraints have been placed on how much can be spent and reuse of existing equipment has been requested. The corporate CIO does recognize the need for proper information assurance and will support limited expenditures.

In order to conduct business, GIAC Enterprises requires the following connectivity:

1. Customers must be able to access a web site to obtain general information about the company, its products and their cost.
2. Customers must be able to purchase products and receive them over the Internet in a secure manner that does not divulge personal or financial information to third parties.
3. Suppliers must be able to upload new fortune cookie sayings to GIAC Enterprises.
4. GIAC and its partners must be able to exchange development software and business information without exposing the information to competitors.
5. GIAC employees must be able to access the Internet to exchange information with customers, suppliers, and partners. Also, the Internet is used to perform market and product development research.
6. Dial-up access is required to GIAC Enterprises by its employees. The dial-up connection is only used when an employee is at a location that does not have Internet access available. The Internet is the preferred connection method.

A restriction exists on the implementation. Customers can not be expected to download and install additional software to increase security. The standard for accessing information securely over the Internet is using Secure Sockets Layer (SSL) over HTTP.

Security Architecture Overview

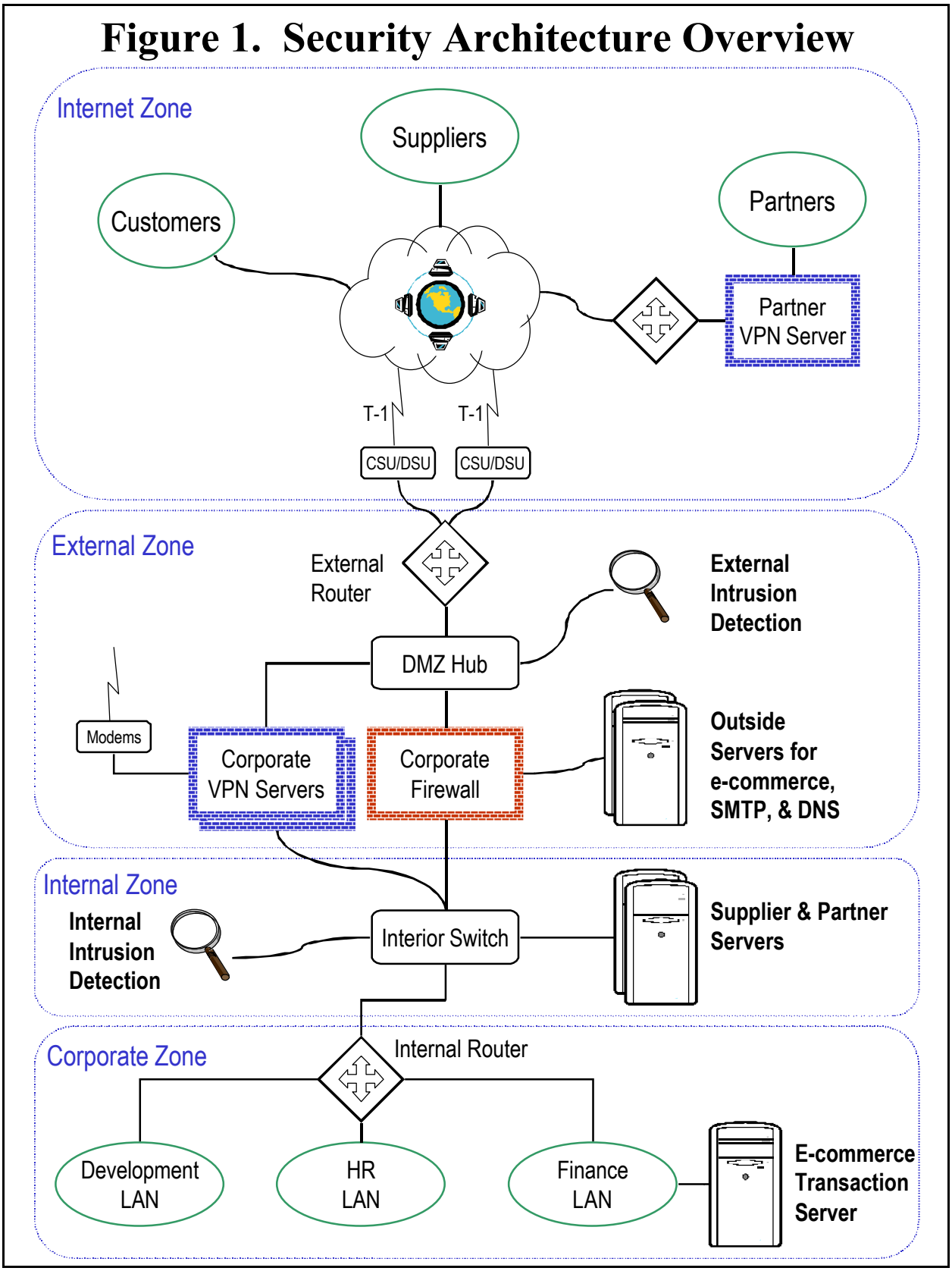
This section describes the components of the architecture. Figure 1, located on the next page, is an overview of the architecture. The configuration is divided into protection zones. The protection zones have devices on the perimeter to control access to/from the zone. The devices have been selected and configured to provide a balance between the control and DDoS mitigation. Customers, suppliers, and partners are permitted limited access to resources located at GIAC Enterprises. The network is also used to provide GIAC employees with Internet access.

© SANS Institute 2000 - 2005 Author retains full rights.

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

© SANS Institute 2000 - 2005 Author retains full rights.

Figure 1. Security Architecture Overview

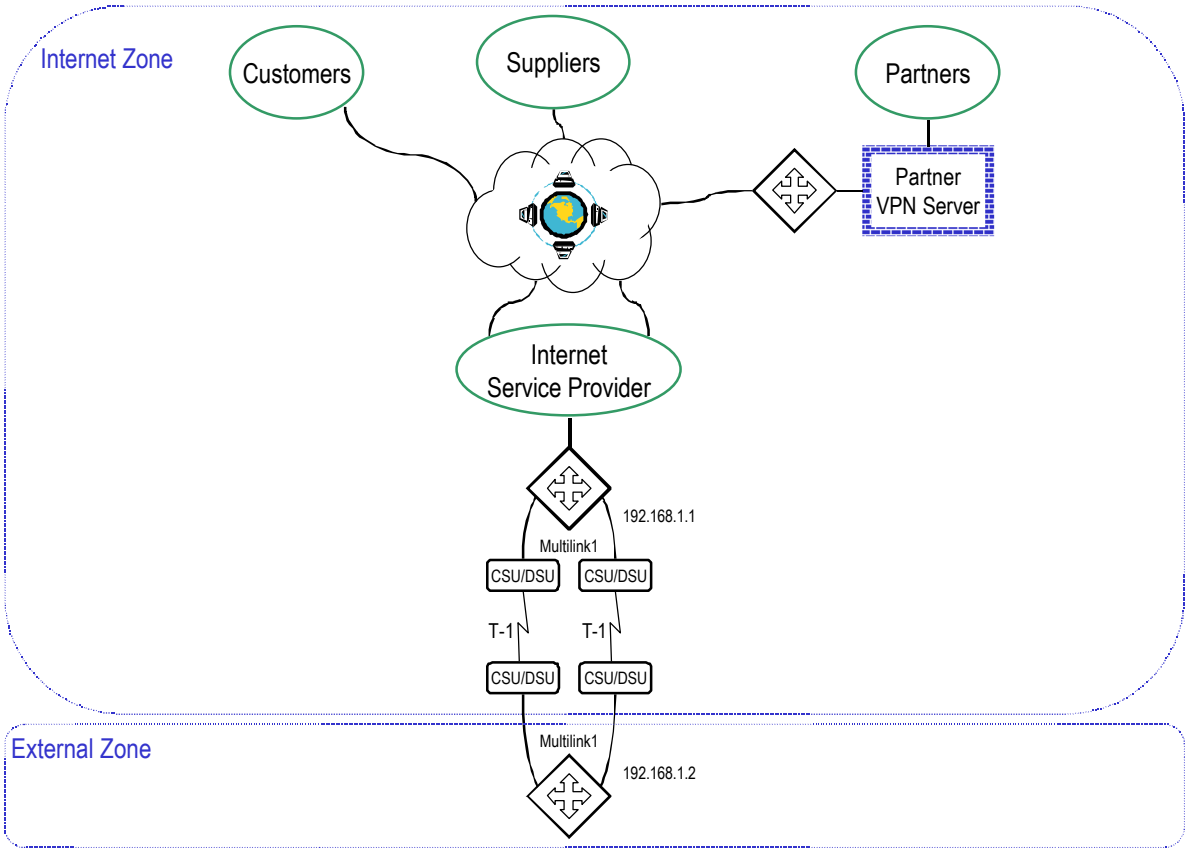


Protection Zone: Internet

© SANS Institute 2000 - 2005 Author retains full rights.

Figure 2 shows how GIAC Enterprises is connected to the Internet. It has been determined that two T-1 links to the ISP is more than sufficient to handled Internet traffic to/from GIAC Enterprises. All customers, suppliers, and partners use the Internet for connectivity. This is a requirement because the cost of installing and maintaining high-speed direct links would make

Figure 2. Protection Zone: Internet



the business unprofitable.

Partners have a VPN server at their site to reduce administration costs by not having to install and maintain accounts for individual users. Also, the Intel NetStructure VPN Gateway does not support non-Windows clients. By having a server at each partner site, all systems running IP can use the VPN to connect to GIAC Enterprises.

Suppliers use SSL to connect to the supplier server at GIAC Enterprises. Customers also use SSL to connect to the external web server.

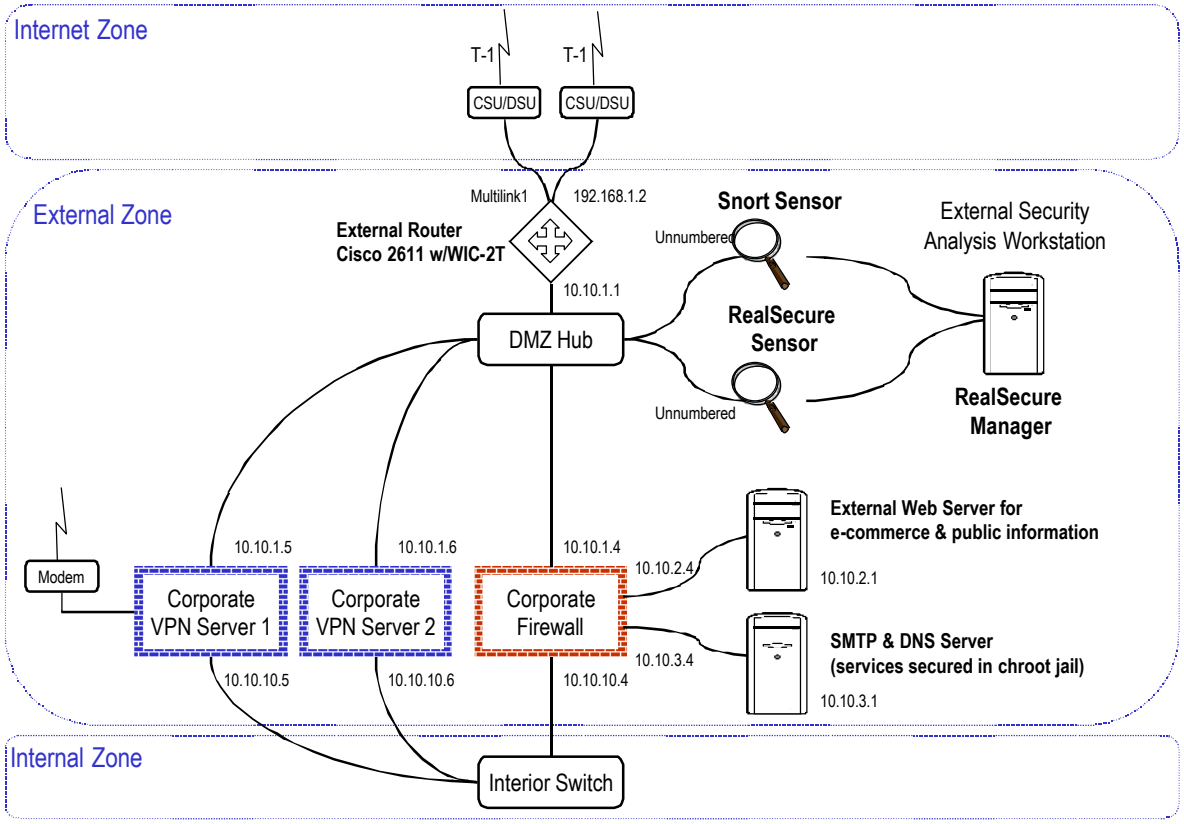
Protection Zone: External

The External Zone is depicted in Figure 3. GIAC Enterprises connects to their ISP via a Cisco 2621 router, with a WIC-2T serial module. The ISP also has a Cisco router on their end of the connection. The serial interfaces on the routers are configured for Multilink PPP. This provides load balancing and redundancy over the links (Cisco, "White Paper: Alternatives"). A

© SANS Institute 2000 - 2005 Author retains full rights.

disadvantage to this configuration is when one of the links becomes noisy. Since the large packets are being fragmented, losing packets causes additional delays and overhead in the traffic between the routers. However, since Multilink PPP allows traffic to be quickly rerouted around broken links and uses multiple lines efficiently, the advantages outweigh the disadvantages.

Figure 3. Protection Zone: External



Network address translation is performed on the external router. NAT helps protect the internal network by requiring an inbound translation rule on the router in order to pass traffic. The only inbound address translations that are defined are for the services required to conduct business, such as, port 80 to the web server and port 25 to the mail server.

The external router has an access list to prevent common attacks and to block addresses that are not within registered address spaces. Details are covered in Assignment 2.

The corporate firewall is running Checkpoint Firewall-1. It is primarily used to regulate traffic to the supplier server and between the external web server and the e-commerce server. The firewall also restricts outbound traffic from the employees. This is to reduce the ability for backdoor and DDoS programs to communicate with their handlers.

The VPN servers provide partner sites and employees at remote locations access to proprietary GIAC Enterprises resources. The VPN servers are redundant and load sharing. They also have

© SANS Institute 2000 - 2005 Author retains full rights.

modems attached to provide remote dial-up access. The VPN servers are permitted to bypass the firewall. This is because they contain their own firewall software to control traffic. Also, they log traffic information and security alerts to the syslog server.

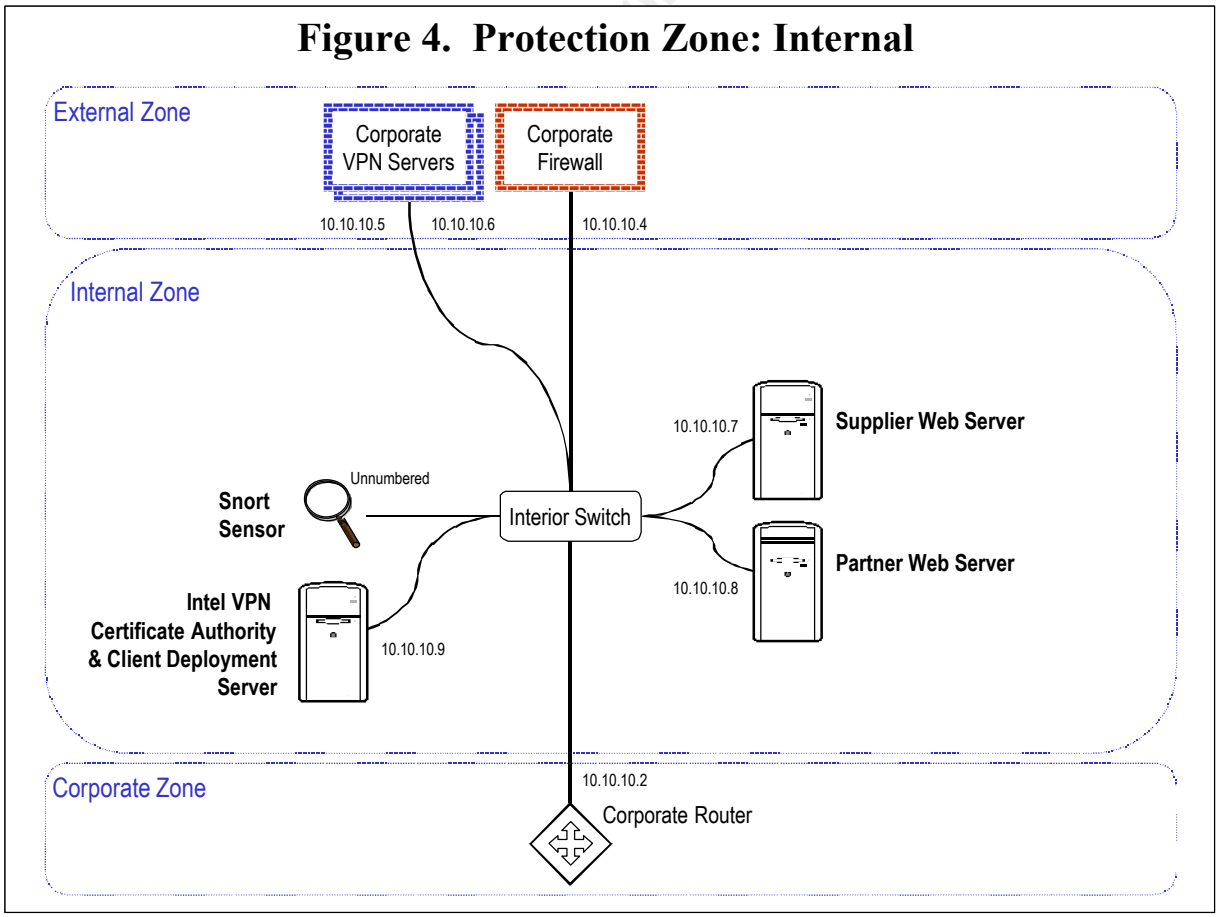
External services have been placed on separate interfaces on the firewall. This will limit information that could be obtained by placing the interfaces in promiscuous mode. Also this limits the systems' access to other systems, in case of a compromise. Personal and financial information is kept on a corporate server located inside the firewall and corporate router (with firewall software) instead of the external web server.

The external web server provides public information about the company and is the external interface for the e-commerce software.

The intrusion detection systems run Snort and RealSecure. These systems have the ability to inspect traffic for anomalous activity. RealSecure can also block some types of traffic by sending TCP resets to kill sessions. Both systems are able to inspect the entire packet and provide the ability to customize the inspection parameters.

The RealSecure kill feature is the reason why a hub is utilized in the DMZ vs. a switch. If a switch is used and the port for RealSecure is being mirrored, then RealSecure can not send out

Figure 4. Protection Zone: Internal



© SANS Institute 2000 - 2005 Author retains full rights.

the kill packets.

Protection Zone: Internal

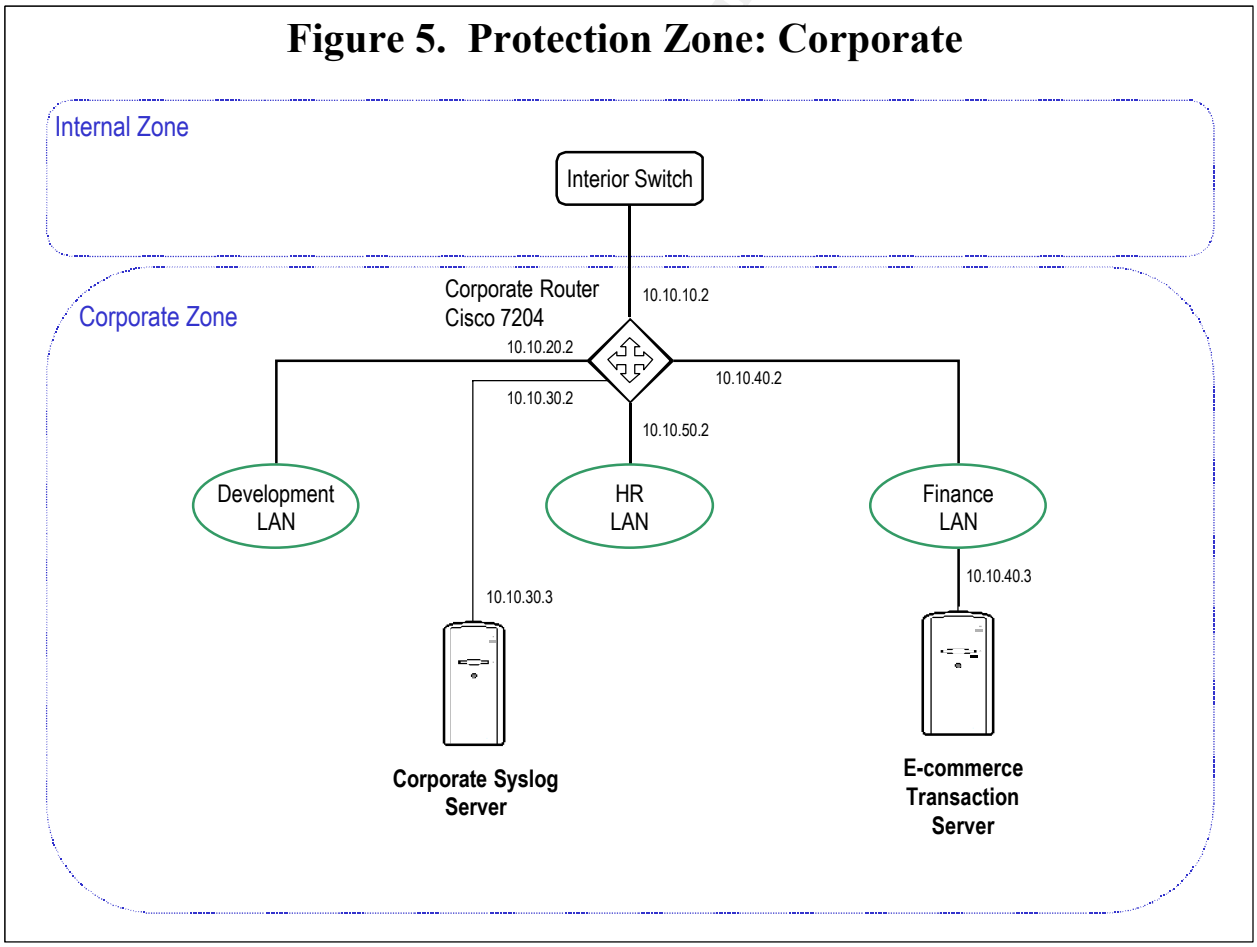
The Internal Zone is shown in Figure 4. This zone provides another layer between the Internet and sensitive corporate assets. This zone is also used as the access point for the supplier and partner web servers and provides another point to monitor network traffic.

The Supplier and Partner Web Servers are provided as a place to exchange information. The only access to the servers from the outside is via SSL.

The VPN Certificate Authority and Client Deployment Server is used to issue digital certificates to the VPN servers and clients. It also is used to preconfigure the client software that users download. This prevents configuration mistakes by the users.

Snort is used on the inside network to monitor the unencrypted traffic from the VPN servers and to analyze the traffic that has passed through the firewall.

Figure 5. Protection Zone: Corporate



© SANS Institute 2000 - 2005 Author retains full rights.

Protection Zone: Corporate
The most sensitive assets are placed in this zone. Figure 5 shows that GIAC Enterprise's internal networks are divided up based on function.

The Cisco router has the firewall and intrusion detection version of the operating system installed. This provides protection against inside attacks from people located in other departments.

The Corporate Syslog Server is the central point for logging from the various systems and network devices. Firewalls and routers restrict access to the syslog to reduce the chance that syslog traffic may be spoofed. No other devices are connected to the router port.

The E-commerce Transaction Server contains the software and database for carrying out the purchases. Although it is on the Finance LAN, critical and sensitive financial systems, such as payroll, are placed on a separate network that can not be accessed via the Internet.

Component Hardware/Software/Configuration Details

This section describes in detail the hardware, software and configuration of the components that make up the security architecture. It also describes why products were selected.

Routers
Cisco routers are used in the architecture because they are a proven technology. Every ISP and practically every networking professional has worked with Cisco routers. Cisco provides excellent support for their product and timely updates and/or workarounds for their software when a problem is discovered.

The Cisco Internetworking Operating System version of the software chosen for the routers is "IOS v12.2.1b." The reasons for selecting this release are:

1. For the outside router, the IP-only version of software was selected because this router needs to be able to execute quickly as possible. Using a version that does not have features that are not required reduces the processing overhead.
2. For the outside router, the IP-only version does not have advanced routing features and support for other protocols. This reduces the number of possible vulnerabilities. For example, if BGP is not installed on the router, the router can not be attacked with a BGP denial of service.
3. For the corporate router, the IP/FW/IDS version of the software provides the ability to bundle some of the security functions into existing hardware. The router is already protected from the Internet by a filtering router, firewall, and other intrusion detection systems.
4. The release of software currently listed as "Limited Deployment". These versions usually are well tested and stable. "Early Deployment" versions of the software are more susceptible to reliability problems and vulnerabilities because of the introduction of new functions in the software. "General Deployment" versions offer the most stability. However, since Cisco updates their software in a rapid fashion, versions of the IOS rarely obtain the status of "General Deployment". Currently, the GD releases

© SANS Institute 2000 - 2005 Author retains full rights.

of the software for the Cisco 2621 do not have the newer version of the Multilink PPP function that permits it to be defined as an interface. This permits advanced configuration options (Cisco, "Configuring PPP").

5. Cisco does not list any vulnerabilities for this version of the IOS. However, vulnerabilities in functions that have been plaguing Cisco will be controlled by being disabled or via access lists.

The Cisco 2621 router was selected for the outside router because it has more processing power than the 2500 series routers. The additional speed of the router allows for larger access lists and will be less likely to drop packets during a DDoS attack. The WIC-2T module contains two serial ports for the T-1 connections. A second module can be installed to further increase the bandwidth to the Internet.

The corporate router is a Cisco 7204 with an 8-port Ethernet VIP module. This router was already in place. It has been upgraded with a 20MB Flash card and a 128MB RAM module to accommodate the additional storage required to run the IP/FW/IDS version of the IOS.

The routers are secured by removing services that are not required and by placing access lists on all services. Cisco provides a comprehensive guide on securing their routers (Cisco, Improving Security on Cisco Routers). The routers have been configured in accordance with the Cisco security guidelines:

```
! tcp- & udp-small-services off by default in this IOS
```
TCP and UDP small services that Cisco routers offered contained potential vulnerabilities. They are now off by default and do not need a command to disable them.
```
service tcp-keepalives-in
```
This command guards against malicious attacks and orphaned sessions by ensuring that sessions are valid and healthy.
```
service password-encryption
```
Enables password encryption. However, some passwords are still protected using weak encryption.
```
enable secret 5 $1$rcdK$bZiImachxO9XXfjezPXEN0
```
Encrypts the enable password using strong encryption (MD5 hash)
```
no ip source-route
```
Disable source routing to avoid malicious redirection of packets.
```
ip cef
```
Enable router to use Cisco Express Forwarding to examine packets and reduce DDoS effects.
```
no ip finger
```
Disable finger to prevent giving up information about accounts.
```
no cdp run
```
Disable Cisco Discovery Protocol to avoid giving up info about router.
```
passive-interface FastEthernet0/0
passive-interface Multilink1
```
Static routes are uses since only one multilink path exist and multilink does not require a routing protocol to mange the link.
```
no ip http server
```


© SANS Institute 2000 - 2005 Author retains full rights.

The http management interface is too dangerous to leave enabled.

```
logging 10.10.30.3
logging 10.10.10.2
```

Events are sent via syslog to the corporate syslog server and an alternate.

```
banner motd _
******************************************************************************
* THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK*
* DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR    *
* AUTHORIZED USE.  COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES,*
* INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE    *
* SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY*
* SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY.  DURING       *
* MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR     *
* AUTHORIZED PURPOSES.  ALL INFORMATION, INCLUDING PERSONAL INFORMATION,     *
* PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.  USE OF THIS COMPUTER *
* SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF   *
* THIS SYSTEM.  UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION.    *
* EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR   *
* ADMINISTRATIVE, CRIMINAL OR ADVERSE ACTION.  USE OF THIS SYSTEM CONSTITUTES*
* CONSENT TO MONITORING FOR THESE PURPOSES.                                  *
******************************************************************************

_
```

Stripped version of a DoD banner containing warning about unauthorized access and notice about monitoring.

```
line con 0
 exec-timeout 5 0
```

Console set to timeout session after five minutes.

```
line vty 0 4
 access-class 10 in
 exec-timeout 5 0
```

Remote access to router permitted but limited via access list.

```
scheduler allocate 30000 2000
```

Reserve time for housekeeping tasks (anti-DDos).

Web Servers

All of the web servers are running Windows NT 4.0 with Internet Information Server. This is a requirement by the e-commerce software and by corporate. They have been secured using the procedure listed in the SANS *Windows NT Security Step by Step* guide (SANS, Windows NT Security). Windows NT 4.0 Service Pack 6a and the new Security Rollup Package have been installed to ensure the latest patches have been applied.

SMTP/DNS Server

The SMTP and DNS services are running on a Red Hat Linux 7.1 server. The server has been configured according to the SANS *Securing Linux Step-by-Step* guide (SANS, Securing Linux). Normally, it is recommended to run the services on separate servers. However, chroot jail reduces the impact of possible sendmail and BIND vulnerabilities by creating a contained environment for the daemons. Detailed instructions on how to configure chroot jail are contained in the August 2001 issue of the Sys Admin magazine. (Widdowson)
RedHat Linux 7.1 comes with BIND 9.1.0. Due to ongoing problems with BIND security, the latest version of BIND (9.1.3) was downloaded and recompiled. BIND 9.1.3 contains new

© SANS Institute 2000 - 2005 Author retains full rights.

features, therefore, the possibility for new vulnerabilities. Although new problems may exist, ISC has strongly recommended using BIND 9 over BIND 8 versions (ISC BIND 8).

Intrusion Detection Sensors

RealSecure

Internet Security Systems description of their network sensor:

> **"RealSecure Network Sensor** runs on a dedicated system that monitors network traffic for attacks and other security related events – definitive identifiers that an intrusion is underway. Attack recognition, incident response, and intrusion prevention occur immediately, with full customization of signatures and response capabilities." (RealSecure Product Literature)

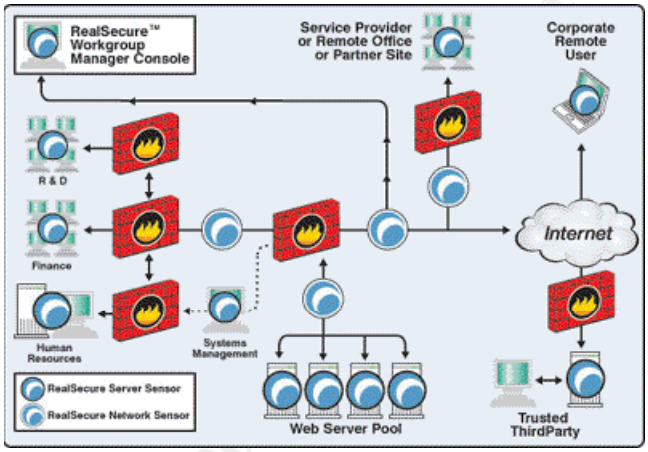


Figure 6. RealSecure Suite, Copyright © 1996-2001 Internet Security Systems.

The ISS RealSecure Network Sensor is running V6.0.2001.144 on Windows NT 4.0. It has been configured by the RealSecure Manager to detect and react to numerous attacks, scans, and unauthorized activity including, backdoors, DoS, e-mail, file sharing, finger, firewall, FTP, HTTP, ICMP, ident, IDS evasion, IRC, NetBIOS, NFS, NNTP, RIP, scanners, SNMP, RPC, telnet, TFTP, and Windows.

The RealSecure sensor responses are:

RealSecure Kill -	TCP reset packets are sent to both the source and destination addresses. This will terminate the session by causing the hosts to abort it.
OPSEC -	RealSecure communicates with the firewall to modify the policy to temporarily block the traffic or create a firewall log entry.
E-mail -	Notifies the personnel via SMTP.
User-Defined -	An external program is executed. Since syslog is not an option, a syslog program was developed in-house to send events to the syslog server.

Snort

© SANS Institute 2000 - 2005 Author retains full rights.

The snort.org web site describes Snort:

> "Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient. (Roesch)"

Snort and RealSecure both provide a signature-based analysis of traffic and can be configured to log traffic in detail. Some differences have been noted in the products. Snort signatures are updated more frequently than RealSecure signatures, and Snort signatures are more numerous. However, Snort produces more false alarms by not looking carefully at the context of the signature, whereas RealSecure will only alarm on a signature if it occurs in the correct context (a URL-based attack will only be recognized as HTTP command data and not in the body of a web page). Both IDS systems can log in detail, but Snort's output is easier to extract and process with other tools. Overall, both systems are good IDS tools and both contribute to the analysis of network traffic.

Both sensors, along with other network components, are configured to send syslog messages to the syslog servers. Upon receiving a notice of high risk traffic, the primary syslog server sends popup messages to the security analysts. All log entries are displayed and saved to the current log file.

VPN Servers

VPN services are provided by the Intel NetStructure 3110 VPN Gateways. The servers and clients are running V6.9 of the software. The VPN servers use a hardened operating system called ShivICE, which is a modified version of ICE. Most of the communication between sites is via site-to-site tunnels. Some partners at small sites and employees have the client software installed on their systems.

Modems are connected to the VPN servers to permit remote access via a dial-up connection. Users must have the VPN client installed and authenticate to the VPN server in order to use the dial-up service.

Authentication is provided via digital certificates generated by the Intel NetStructure Certificate Authority Pro v6.6 server. The VPN servers encrypt the data using IPsec tunnels.

Firewall

The firewall is running Checkpoint 2000 Firewall-1 SP2 on Microsoft Windows NT 4.0. The operating system was chosen based on in-house expertise with Microsoft operating systems and due to the lack of maturity of the Linux version of the firewall software. The firewall will be

© SANS Institute 2000 - 2005 Author retains full rights.

changed to Linux when the firewall product reaches maturity.

The Windows operating system has been updated by applying all the current service packs and patches. All services that are not required have been disabled.

Syslog Server
The syslog server is running Kiwi's Syslog Daemon v6.2.9 on Windows NT 4.0. It is installed on the network management workstation and is isolated behind its own Corporate Router port. This provides additional protection against intrusions and the altering of syslog records. Kiwi's Syslog Daemon provides numerous advanced functions that run real-time:

- Filters can be defined for actions. These filters are based on the syslog facility, level, originator, content, and time of day.
- Responses to messages can be to display, forward, or log messages. Messages can also be stored in ODBC-compatible databases or as an NT event. Alerts can be generated in the form of audible sounds and e-mail messages. Finally, the message can be passed to an external program that produces a popup alert, notification via pager, or other function.
- Name resolution for IP addresses of originators and within messages provides a quicker and easier way to provide additional information about alerts.
- Alerts regarding the violation of minimum or maximum number of messages received per hour can be sent via e-mail or other means. This is useful for spotting unusual traffic trends. If the log file grows too large, a message can be sent to the administrator so that they can take corrective action before the log overflows the hard drive.
- Log files can be automatically archived and compressed.

Assignment 2 – Security Policy

Overview
The security policies are designed to limit access to/from GIAC Enterprises systems to services that are required to carry out the company's business. The security devices chosen regulate traffic using stateful inspection methods. These devices are faster and less susceptible to DDoS attacks. The intrusion detection systems monitor content to detect and, if possible, block unauthorized traffic. Since the devices do not sit directly in the path of the traffic, they do not slow down the network's performance or create another single point of failure.

Web content could be further regulated by the installation of a Firewall-1 plug-in, such as, SuperScout by SurfControl or WebSense Enterprise by WebSense. This would add to the security by prohibiting access to sites that might have a negative impact on network availability (music downloads, file sharing, etc.) and sites that are known to contain malicious code.

© SANS Institute 2000 - 2005 Author retains full rights.

ISP router

The ISP router has been configured to act as a first line of defense and to minimize the impact of DDoS attacks. The link to GIAC Enterprises has a lower bandwidth (3Mbps) than the ISP's access to their POP (45Mpbs). Therefore, access lists must be placed on the interface to GIAC to limit the bandwidth of packets that are usually used in a DDoS attack; HTTP SYN, ICMP, and HTTP. By limiting these packets, some bandwidth is kept available for other traffic, such as, SMTP. Applying the access lists on the GIAC side would be ineffective because the traffic has to be controlled before it reaches the choke point.

Multilink1 is the multilink PPP interface for the two serial lines connecting GIAC to their ISP. Commands to regulate traffic is placed on this interface instead of the individual serial links. The following commands regulate traffic from the ISP to GIAC:

```
interface Multilink1
 description ISP connection
 ip address 192.168.1.1 255.255.255.252
```

The following lines limit ICMP (100Kbps), HTTP SYN (100Kbps), and HTTP traffic (2.5Mbps).

```
 rate-limit output access-group 2020 100000 50000 50000 conform-
action transmit exceed-action drop
 rate-limit output access-group 152  100000 10000 10000 conform-
action transmit exceed-action drop
 rate-limit output access-group 153 2500000 10000 10000 conform-
action transmit exceed-action drop
```

Commands to enable multilink ppp.

```
ppp multilink
multilink-group 1
!
! access list to rate limit http syn traffic
access-list 152 permit tcp any host 44.1.1.3 eq www
! access list to rate limit http traffic
access-list 153 permit tcp any host 44.1.1.3 eq www established
! access list to rate limit icmp replies
access-list 2020 permit icmp any any
```

If additional types of packets are used in a DoS attack, they can be added to the access lists and rate limit commands.

Border router

The external router hides GIAC Enterprises' assets through the use of Network Address Translation (NAT). Two forms of NAT are used; static and dynamic. Static assignments are used for services, which are accessed from the Internet and require a fixed IP address and port. The GIAC network uses dynamic entries for outbound traffic that is not otherwise statically defined.

The static entries are:

```
! Inbound translation to the DNS/SMTP server
ip nat inside source static 10.10.3.2 44.1.1.2
! Inbound translations to the web servers
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
ip nat inside source static tcp 10.10.2.2 80 44.1.1.3 80
ip nat inside source static tcp 10.10.2.2 443 44.1.1.3 443
ip nat inside source static tcp 10.10.10.7 443 44.1.1.7 443
! Inbound translations to the VPN servers
ip nat inside source static 10.10.1.5 44.1.1.5
ip nat inside source static 10.10.1.6 44.1.1.6
! Inbound translation to the VPN CA/CDT server
ip nat inside source static tcp 10.10.10.9 443 44.1.1.9 443
ip nat inside source static udp 10.10.10.9 10027 44.1.1.9 10027
```

The outbound traffic that has not been statically defined is translated using a single address. This performs the functions of hiding the inside network and only permitting inbound traffic that has an entry in the dynamic table. The entries in this table are based on outbound connection requests. The NAT pool commands are:

```
! Outbound translation of addresses to a proxy address
ip nat pool PROXY 44.1.1.1 44.1.1.1 prefix 24
! NAT access list for PROXY
access-list 1 permit 10.10.0.0 0.0.255.255
```

Multilink1 is the multilink PPP interface for the two serial lines connecting GIAC to their ISP. Commands to regulate traffic are placed on this interface instead of the individual serial links. The following commands regulate traffic to and from the ISP:

```
interface Multilink1
 description ISP connection
 ip address 192.168.1.2 255.255.255.252
 ip access-group 100 in
```

Limits inbound traffic. See access list below.

```
 ip access-group 101 out
```

Limits outbound traffic. See access list below.

```
 ip verify unicast reverse-path
```

Validates routing of packets to stop SMURF attacks.

```
 no ntp enable
```

Disable ntp on the outside interface.

```
 ppp multilink
 multilink-group 1
```

Commands to enable multilink ppp.

```
 ip nat outside
```

Command to define the outside interface for NAT.

```
!
interface Serial0/0
 description Line 1
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
 multilink-group 1
!
interface Serial0/1
 description Line 2
 no ip address
 encapsulation ppp
 no fair-queue
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
ppp multilink
multilink-group 1
```

As suggested by the SANS Instructor, access list 100 was developed to not only block IP addresses designated as "private use" and internal address to limit attacks, it also includes numerous address spaces listed as "Reserved" by IANA (IANA, "Internet Protocol V4 Address Space."). This access list is applied to traffic that is inbound from the ISP.

```
! access list to block internal, reserved, and private use
! source addresses to reduce spoofing
! "log-input" on denys to monitor activity via syslog
! block icmp redirects (anti-spoofing)
access-list 100 deny icmp any any redirect
! permit link adddresses
access-list 100 permit ip 192.168.1.0 0.0.0.3 any
! 000/8 IANA Reserved
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log-input
! 001/8 IANA Reserved
access-list 100 deny ip 1.0.0.0 0.255.255.255 any log-input
! 002/8 IANA Reserved
access-list 100 deny ip 2.0.0.0 0.255.255.255 any log-input
! 005/8 IANA Reserved
access-list 100 deny ip 5.0.0.0 0.255.255.255 any log-input
! 007/8 IANA Reserved
access-list 100 deny ip 7.0.0.0 0.255.255.255 any log-input
! 010/8 IANA Private Use
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log-input
! 023/8 IANA Reserved
access-list 100 deny ip 23.0.0.0 0.255.255.255 any log-input
! 027/8 IANA Reserved
access-list 100 deny ip 27.0.0.0 0.255.255.255 any log-input
! 031/8 IANA Reserved
access-list 100 deny ip 31.0.0.0 0.255.255.255 any log-input
! 036/8 IANA Reserved
access-list 100 deny ip 36.0.0.0 0.255.255.255 any log-input
! 037/8 IANA Reserved
access-list 100 deny ip 37.0.0.0 0.255.255.255 any log-input
! 039/8 IANA Reserved
access-list 100 deny ip 39.0.0.0 0.255.255.255 any log-input
! 041/8 IANA Reserved
access-list 100 deny ip 41.0.0.0 0.255.255.255 any log-input
! 042/8 IANA Reserved
access-list 100 deny ip 42.0.0.0 0.255.255.255 any log-input
! 044/24 Internal Global addresses
access-list 100 deny ip 44.1.1.0 0.0.0.255 any log-input
! 049/8 IANA Reserved
access-list 100 deny ip 49.0.0.0 0.255.255.255 any log-input
! 050/8 IANA Reserved
access-list 100 deny ip 50.0.0.0 0.255.255.255 any log-input
! 058/8 IANA Reserved
access-list 100 deny ip 58.0.0.0 0.255.255.255 any log-input
! 059/8 IANA Reserved
access-list 100 deny ip 59.0.0.0 0.255.255.255 any log-input
! 060/8 IANA Reserved
access-list 100 deny ip 60.0.0.0 0.255.255.255 any log-input
! 069/8 IANA Reserved
access-list 100 deny ip 69.0.0.0 0.255.255.255 any log-input
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
! 070/8 IANA Reserved
access-list 100 deny ip 70.0.0.0 0.255.255.255 any log-input
! 071/8 IANA Reserved
access-list 100 deny ip 71.0.0.0 0.255.255.255 any log-input
! 072/8 - 079/8 IANA Reserved
access-list 100 deny ip 72.0.0.0 7.255.255.255 any log-input
! 082/8 - 083/8 IANA Reserved
access-list 100 deny ip 82.0.0.0 1.255.255.255 any log-input
! 084/8 - 087/8 IANA Reserved
access-list 100 deny ip 84.0.0.0 3.255.255.255 any log-input
! 088/8 - 095/8 IANA Reserved
access-list 100 deny ip 88.0.0.0 7.255.255.255 any log-input
! 096/8 - 127/8 IANA Reserved
access-list 100 deny ip 96.0.0.0 31.255.255.255 any log-input
! 172.16 - 172.31 IANA Private Use
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log-input
! 192.168/16 IANA Private Use
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log-input
! 197/8 IANA Reserved
access-list 100 deny ip 197.0.0.0 0.255.255.255 any log-input
! 219/8 IANA Reserved
access-list 100 deny ip 219.0.0.0 0.255.255.255 any log-input
! 220/8 - 223/8 IANA Reserved
access-list 100 deny ip 220.0.0.0 3.255.255.255 any log-input
! 240/8 - 255/8 IANA Reserved
access-list 100 deny ip 240.0.0.0 15.255.255.255 any log-input
! Services offered by VPN Servers
access-list 100 permit 50 any host 44.1.1.5
access-list 100 permit 50 any host 44.1.1.6
access-list 100 permit udp any host 44.1.1.5 eq isakmp
access-list 100 permit udp any host 44.1.1.6 eq isakmp
! Inbound DNS queries
access-list 100 permit udp any host 44.1.1.2 eq domain
! SMTP
access-list 100 permit tcp any host 44.1.1.2 eq smtp
! Web server
access-list 100 permit tcp any host 44.1.1.3 eq www
access-list 100 permit tcp any host 44.1.1.3 eq https
! Supplier server
access-list 100 permit tcp any host 44.1.1.7 eq https
! multilink interface
access-list 100 permit ip 192.168.1.0 0.0.0.3 host 192.168.1.2
! user proxy – only valid ports will be accepted by NAT
access-list 100 permit ip any host 44.1.1.1
access-list 100 deny ip any any log-input
```

Access list 101 regulates outbound traffic:

```
! Limit source & dest traffic to permitted only (anti spoof and minimum
firewall)
! VPN servers
access-list 101 permit 50 host 44.1.1.5 any
access-list 101 permit 50 host 44.1.1.6 any
access-list 101 permit udp host 44.1.1.5 any eq isakmp
access-list 101 permit udp host 44.1.1.6 any eq isakmp
! DNS Queries
access-list 101 permit udp host 44.1.1.2 any eq domain
access-list 101 permit udp host 44.1.1.2 any gt 1023
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
! SMTP
access-list 101 permit tcp host 44.1.1.2 any eq smtp
access-list 101 permit tcp host 44.1.1.2 any gt 1023 est
! Web server
access-list 101 permit tcp host 44.1.1.3 any gt 1023 est
access-list 101 permit tcp host 44.1.1.3 any gt 1023 est
! Supplier server
access-list 101 permit tcp host 44.1.1.7 any gt 1023 est
! multilink interface
access-list 101 permit ip host 192.168.1.2 192.168.1.0 0.0.0.3
access-list 101 deny ip any any log-input
! user proxy
access-list 101 permit ip host 44.1.1.1 any
access-list 101 deny ip any any log-input
```

The access lists are tested by successfully passing normal traffic through the router. Alerts regarding blocked traffic will be sent to the syslog servers. If normal traffic cannot be passed, the access list will be modified to permit the traffic. Penetration testing and the firewall logs will validate the function of the access lists.

RealSecure

ISS' RealSecure product is an active intrusion detection system that provides the ability to block many forms of inappropriate traffic. Sending TCP reset packets and/or setting temporary rules on the firewall blocks the offending traffic. RealSecure also categorizes the risk of the traffic detected as high, medium, and low risk. These risk categories assist with the assessment of alerts and how to react to them.

A danger with active defenses is that if a hacker detects that the system is present, they could use it against you. By sending offending traffic that spoofs addresses of legitimate customers and business partners, they could create a denial of service. Therefore, care must be exercised when configuring active defenses to minimize the possibility of this situation.

Filters are grouped into categories based on how they are defined. "Security Events" are predefined filters for detecting anomalous traffic. "Connection Events" are user-defined filters that detect traffic based on source, destination, protocol, and port. They are used to detect and block unauthorized traffic, such as, users surfing to mp3.com. "User Defined Events" are content filters. Some content of packets can be inspected, such as, e-mail sender, recipient, subject, or text, URLs, DNS query, file name, news group, user name, password, or SNMP community string. "User-Specified Filters" allows the user to ignore traffic based on source, destination, protocol, and ports. It is used to reduce false positives and to ignore known situations without completely disabling the other rules.

The full rule set for the RealSecure policy contains 563 records. A summarized version of the rules is as follows:

- **Security Events, High/Medium Risk** – These signatures detect such activity as backdoor communications, risky and vulnerable services, and DDoS attacks. Alerts are sent to the RealSecure Manager console and to the syslog server. Events that

© SANS Institute 2000 - 2005 Author retains full rights.

detect attacks which, can be stopped by using TCP reset, use the RealSecure Kill option to stop the event. Other attacks are stopped by setting a temporary rule on the firewall via OPSEC. However, the OPSEC option must be used carefully to avoid creating a DoS situation.

- **Security Events, Low Risk** – These signatures detect threats that are not likely to cause damage, activity that indicates misuse of resources (downloading music, etc.), and protocol decodes (NNTP groups joined, etc.). Notifications of these activities are sent to the console and syslog for informational purposes and later analysis.
- **Connection Events** – These events analyze traffic based on source/destination addresses, ports, and protocols. They are used to block undesirable traffic, such as, sites used by viruses to upload information, music sites, and chat programs that are not detected by security events. These events send an alert to the console and syslog server and they block the traffic using TCP resets.
- **User-Defined Events** – These are user-definable signatures. This permits the security analyst to enter context-sensitive strings to build a signature for an attack without having to wait for an update from ISS. For example, the Code Red worm can be detected by selecting the "URL Data" context and entering the string "/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN". This signature will detect the worm if sent as a URL to a web server but will ignore it if seen in the server's page content. This significantly reduces false positives. The limitation is that it can only be used for the contexts listed earlier.
- **UserSpecified Filters** – The filters are used to ignore traffic. This is a dangerous practice because it turns off all event checking for the specified traffic, but it is required to filter out "noise". An example is an ftp filter to ignore all file transfers to and from the sites that provide the Norton Antivirus updates. The filter reduces the log entries regarding known traffic and enables the analysts to more easily detect anomalous traffic.
- **False Positives** – A downfall of RealSecure is that it is not sensitive to the direction of traffic. Basically, it detects events that indicate a vulnerability or potential problem with another site on the Internet. A good example is a browser vulnerability. RealSecure will alert about Internet users who are using outdated versions of Internet Explorer or Netscape. Also, it will generate this alert for every packet it sees. This causes a flood of information that is useless and must be turned off. Some other signatures generate too many false positives. If left enabled, they would disrupt normal network traffic if they were used to block packets.

VPN servers

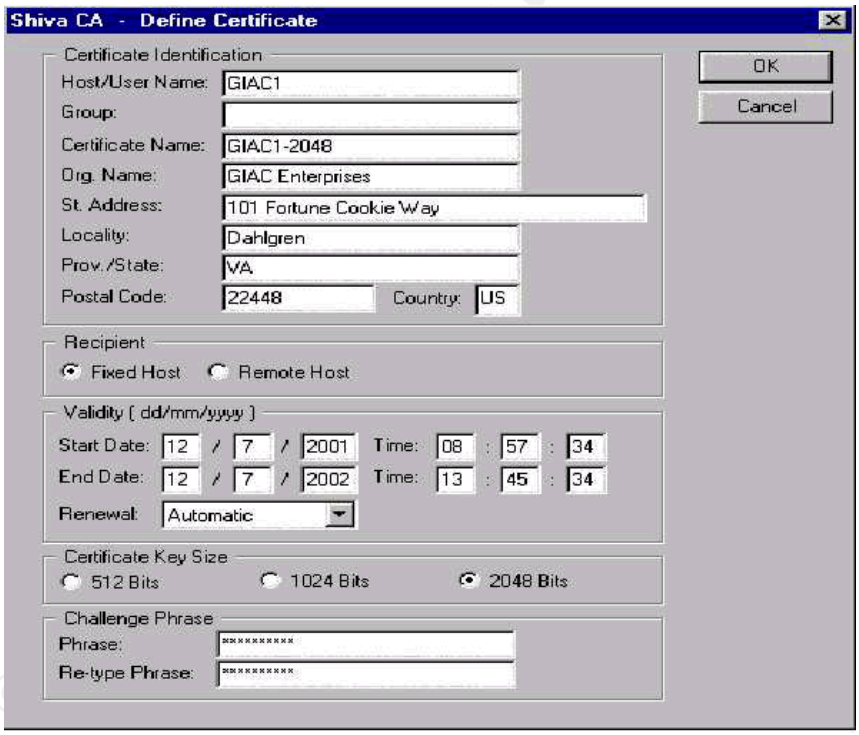
The VPN servers provide authenticated and encrypted communications from the partner sites and dial-up accounts to GIAC Enterprises. IPSEC tunnels use digital certificates, created using the Intel (formerly Shiva) Certificate Authority Pro server, to validate the identity of the remote VPN servers and VPN clients. The CA Pro server also maintains a certificate revocation list (CRL). The CRL enables potentially compromised certificates to be invalidated. This prevents the situation that Microsoft experienced when an illegitimate certificate was issued and could not

© SANS Institute 2000 - 2005 Author retains full rights.

be easily or automatically revoked. This was because the CRL mechanism was not implemented in the client software, the user would not be alerted that the certificate was invalid.

Certificates are defined for each VPN server and client (see Figure 7). Standard identifying information is entered into the form. In the Recipient section, if a host is defined as "Fixed" then CRL updates are sent immediately to the last IP address the host used to connect to the CA. This permits immediate revocation of certificates. This is required for servers since the CA is not contacted as part of the tunnel negotiation. The servers use data from their certificate, the remote system's certificate, and the CRL to authenticate tunnel requests. If the CRL is out of date, a session with a system, which has revoked credentials, could be permitted. Certificates are renewed automatically on an annual basis, unless only temporary access is required. The certificate key size is set to the maximum size, 2048 bits. This requires additional processing time for key generation and tunnel negotiation, but the longer key length provides additional protection against having the key broken and data decrypted by third parties.

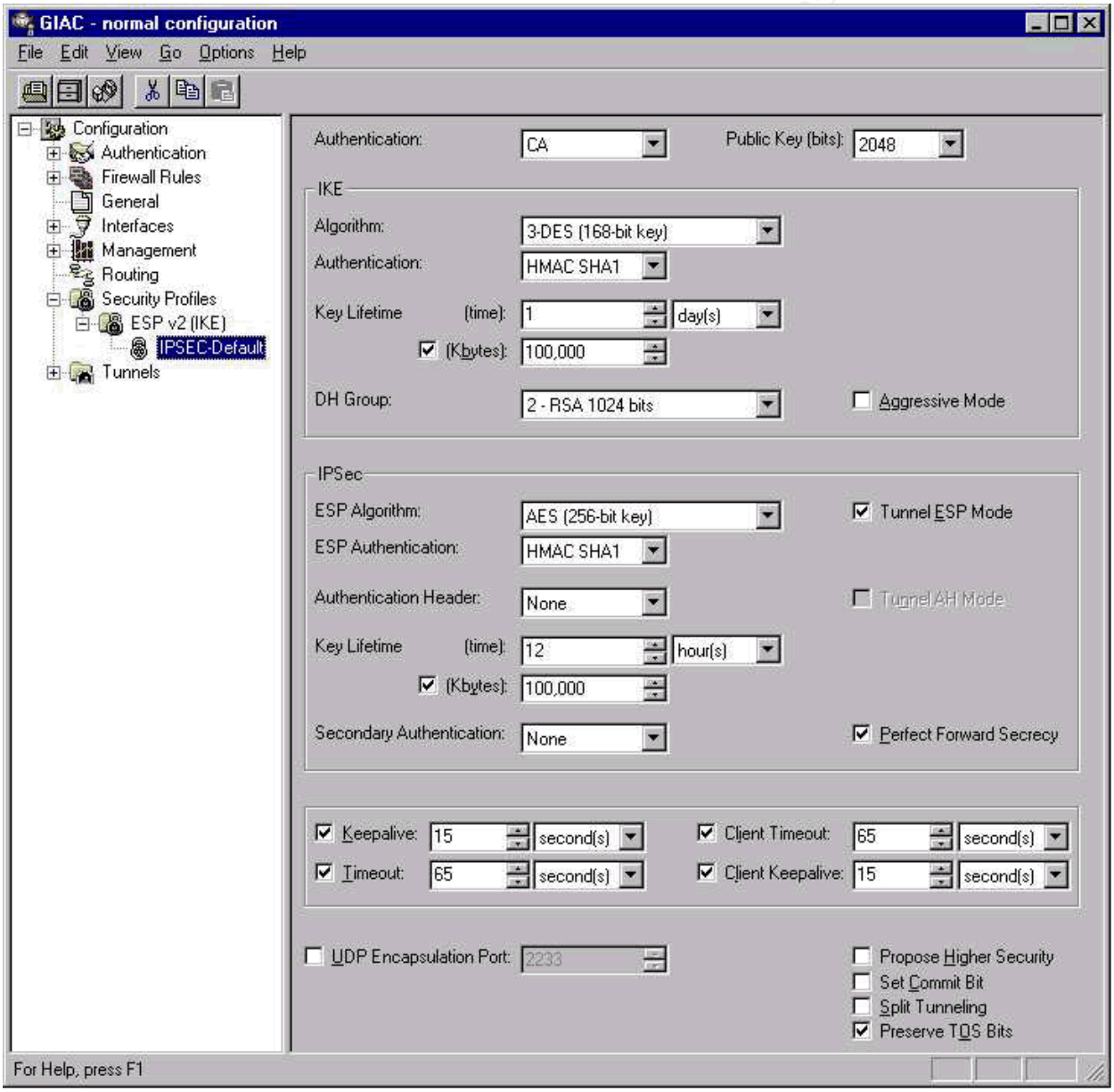
Figure 7. Digital Certificate Definition Form.



For the servers, the challenge phrase is sent to the remote site via a secure means, such as, PGP-encrypted e-mail. The VPN user's certificate challenge phrase is entered into the user's profile on the Intel VPN Client Deployment Tool (CDT). The CDT generates a second challenge phrase, which the user must have to download the client software and configuration. This password must also be securely passed to the user.

© SANS Institute 2000 - 2005 Author retains full rights.

Figure 8. IPSEC Tunnel Configuration Form.



The above screen is used to configure most of the parameters required to establish an IPSec ESP

© SANS Institute 2000 - 2005 Author retains full rights.

v2 (IKE) tunnel. The following list the configuration items and parameters selected:

- **Authentication** – via certificate authority with 2048-bit digital certificates.
- **IKE Algorithm** – sets the encryption used for Internet Key Exchange to 3-DES. The only other choice with this system is to use DES, which is easily broken.
- **Key Lifetime** – set to 1 day or 100 megabytes of data for IKE, and 12 hours or 100 megabytes for IPSec. This is to limit the damage that occurs if a key is compromised.
- **DH Group** – uses "Main Mode" (Aggressive Mode is not checked) to perform additional authentication during the IKE process. Aggressive mode is faster but performs less authentication.
- **ESP Algorithm** – is set to use the US Government's new Advanced Encryption Standard (AES). AES (Rijndael) provides a newer and publicly scrutinized encryption standard. NIST's assessment of Rijndael:

> "When considered together, Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility make it an appropriate selection for the AES.
>
> Specifically, Rijndael appears to be consistently a very good performer in both hardware and software across a wide range of computing environments regardless of its use in feedback or non-feedback modes. Its key setup time is excellent, and its key agility is good. Rijndael's very low memory requirements make it very well suited for restricted-space environments, in which it also demonstrates excellent performance. Rijndael's operations are among the easiest to defend against power and timing attacks.
>
> Additionally, it appears that some defense can be provided against such attacks without significantly impacting Rijndael's performance. Rijndael is designed with some flexibility in terms of block and key sizes, and the algorithm can accommodate alterations in the number of rounds, although these features would require further study and are not being considered at this time. Finally, Rijndael's internal round structure appears to have good potential to benefit from instruction-level parallelism." (Advanced Encryption Standard)

- **Authentication Header** – is not enabled. This option does not work with network address translation. Therefore, when attempting to establish sessions, the sessions never complete because the packet header was modified by NAT and fails the AH check.
- **Perfect Forward Secrecy** – is checked to prevent information about a compromised key from being used to compromise other keys. This option disables using existing key information to derive a new key.
- **Keepalives and Timeouts** – is set to ensure that tunnels that are created are actually in working order. If one end of the tunnel becomes unusable, then the keepalive packets are not received by the other end. After four packets fail to reach the other end, the tunnel is torn down. This is to prevent leaving tunnels open after they become unusable.

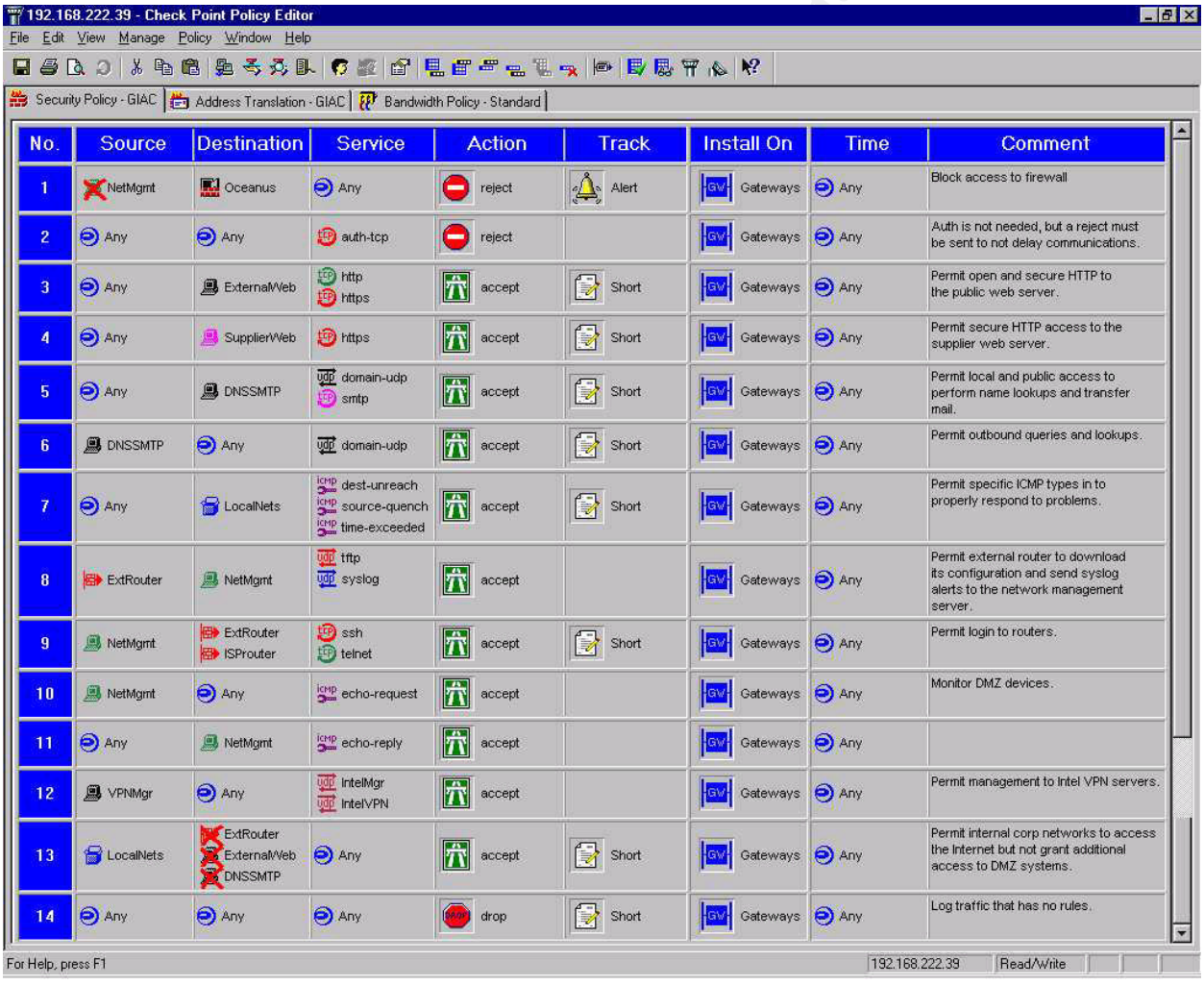
© SANS Institute 2000 - 2005 Author retains full rights.

VPN servers also act as stateful inspection firewalls. The servers are configured with firewall rules that permit HTTP and FTP access to the Partner Web Server. Even though HTTPS is not used, users must still authenticate to the web server via user ID and password. Also, the web server will only accept network connections from the VPN servers' IP address space. The reason for the use of unencrypted communications is to permit the internal IDS sensor to inspect traffic.

Internet Firewall

The Internet firewall is running Checkpoint's Firewall-1. Network objects are defined according to GIAC Enterprise's network architecture. The policy properties are configured to remove some hidden holes (all implicit rules are disabled) and to defend against SYN floods, etc.

Figure 9. GIAC Corporate Firewall Policy.



No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	NetMgmt	Oceanus	Any	reject	Alert	Gateways	Any	Block access to firewall
2	Any	Any	auth-tcp	reject		Gateways	Any	Auth is not needed, but a reject must be sent to not delay communications.
3	Any	ExternalWeb	http https	accept	Short	Gateways	Any	Permit open and secure HTTP to the public web server.
4	Any	SupplierWeb	https	accept	Short	Gateways	Any	Permit secure HTTP access to the supplier web server.
5	Any	DNSSMTP	domain-udp smtp	accept	Short	Gateways	Any	Permit local and public access to perform name lookups and transfer mail.
6	DNSSMTP	Any	domain-udp	accept	Short	Gateways	Any	Permit outbound queries and lookups.
7	Any	LocalNets	dest-unreach source-quench time-exceeded	accept	Short	Gateways	Any	Permit specific ICMP types in to properly respond to problems.
8	ExtRouter	NetMgmt	tftp syslog	accept		Gateways	Any	Permit external router to download its configuration and send syslog alerts to the network management server.
9	NetMgmt	ExtRouter ISProuter	ssh telnet	accept	Short	Gateways	Any	Permit login to routers.
10	NetMgmt	Any	echo-request	accept		Gateways	Any	Monitor DMZ devices.
11	Any	NetMgmt	echo-reply	accept		Gateways	Any	
12	VPNMgr	Any	IntelMgr IntelVPN	accept		Gateways	Any	Permit management to Intel VPN servers.
13	LocalNets	ExtRouter ExternalWeb DNSSMTP	Any	accept	Short	Gateways	Any	Permit internal corp networks to access the Internet but not grant additional access to DMZ systems.
14	Any	Any	Any	drop	Short	Gateways	Any	Log traffic that has no rules.

Information on rules:

1. This rule blocks everyone from connecting to the firewall except the network management workstation. The firewall management client is currently located on the firewall.

© SANS Institute 2000 - 2005 Author retains full rights.

2. The auth protocol may give up information about systems. If it is dropped, then delays will occur when sending e-mail. The "reject" action is used to send a reset to notify the host that auth is not available, then communications will continue immediately.
3. Everyone is permitted to contact the External web server on HTTP and HTTPS.
4. The suppliers are located in various locations on dynamic IP addresses. They must use an encrypted user ID and password to authenticate to the Supplier web server.
5. Everyone is permitted to query the DNS server and contact it to send and receive mail.
6. The DNS server must be able to query other DNS servers to perform recursive searches.
7. Some types of ICMP traffic must be accepted to carry out normal communications. Destination unreachable and time exceeded messages assist with troubleshooting communications problems. Source quench is used to slow communications. It could also be used as a form of DoS but it is not a common attack.
8. The External Router must be able to communicate with the network management workstation. For CM purposes, commented versions of the router's configuration are stored in text files on the network management workstation and the startup configuration on the router. This aids with router troubleshooting and rebuilding.
9. Permits logins from the network management workstation to the External Router.
10. The network management workstation is the only IP address permitted to perform pings. This cuts down on the risk of ICMP echo and echo reply packets being used to send covert communications.
11. Partner to rule 10.
12. The VPN management workstation is permitted to contact the VPN servers directly. Normal VPN traffic is passed through the VPN servers and around the firewall.
13. The corporate subnets (HR, Devel, and Finance) are permitted outbound access on any port. The RealSecure and Snort sensors are responsible for detecting anomalous traffic, such as, back doors and blocking it. Using the firewall to block specific outbound ports to prevent unauthorized activity is minimally effective.
14. The final rule is to log all other blocked traffic. The traffic is analyzed and new rules will be generated, as appropriate.

Assignment 3 – Audit Your Security Architecture

Planning the Assessment

Overview

The security assessment is designed to confirm the level of access that is granted to remote systems, uncover any known or possible vulnerabilities, and test the denial of service defensive countermeasures. The components of the test are the perimeter defense components, scanner programs, and performance monitoring software. This test will use some of the same programs used by hackers to search for vulnerabilities. Analyzing data gathered during the attacks will demonstrate the effectiveness of the IDS sensors to detect anomalous traffic.

© SANS Institute 2000 - 2005 Author retains full rights.

Scans of active networks and systems will only occur after normal working hours. This is possible since the firewall policy is not configured to regulate traffic based on time of day. Some scans may create a DoS by crashing systems, overloading them, or via network congestion. A router similar to the ISP's will be used in-house to simulate an attack from the Internet.

The testing will occur in phases:

1. **Functionality Tests** – The connectivity of all systems will be checked before testing begins. Workstations on the simulated ISP and Partner LANs must be able to access the normal services offered to prove that they are running and accessible from the appropriate locations.
2. **Penetration Tests** – These scans will be conducted from the ISP LAN to simulate Internet penetrations and from the Partner LAN to check for potential problems due to additional access granted by the VPN. The scanner will scan for vulnerabilities, attempt DoS floods, and collect information about the site.
3. **Inside Tests** – Since we are practicing "defense in depth", the systems must be checked from within the DMZ. This is to verify that if a penetration should occur, the damage will be minimized. The scanner will check GIAC's systems during a designated downtime period. The links to the Internet and corporate router will be broken to isolate the DMZ systems. The firewall will be configured to pass all traffic to expose all systems directly to the scanner.

Scanners

Nessus

Running Nessus on Linux is a very low cost solution for conducting scans. Since the software can be downloaded for free, the only cost is the hardware and the manpower to configure the software. Commercial scanners usually do not have the latest attack scripts or plugins available. Nessus and SAINT are quick about coming out with new scripts. However, only the commercial users of SAINT receive their updates immediately. Nessus scripts are immediately available to all Nessus users.

Nessus v1.0.8 is installed on the scanning workstation that is running Red Hat Linux 7.1. The scripts (plugins) are kept up to date by running "nessus-update-plugins -v" on a regular basis (cron job).

Nessus Options:

- All plugins are enabled including dangerous plugins.
- Pinging is turned off since the tests will be conducted through the firewall and the hosts are already known to be active. Specific targets will be defined for the scan.
- Scanning will be attempted using all TCP scanning techniques (connect(), SYN, FIN Xmas tree, and Null). Since only one technique can be defined at a time, multiple passes will have to be performed.
- In addition to TCP scans, UDP and RPC scans are enabled.
- The "Fragment IP packets" option will be to test the ability of the security systems to

© SANS Institute 2000 - 2005 Author retains full rights.

detect and block the traffic.

- The port range for the scan is changed to cover all ports (0-65535).

SAINT

Running the publicly available version of SAINT on Linux is also a low cost solution. The version used during the scans was v3.2.4. The limitation is that it does not contain the most up-to-date scan options that are only available in the commercial version.

SAINT will be run at strongest level, Heavy+. It warns that Windows NT systems may be crashed. Also, the "Firewall Support" option will be selected to assist SAINT with firewall penetration.

Performance Monitoring

Performance of the network will be monitored using two tools; IPSwitches' WhatsUp Gold v6.02 and Network Associates' Sniffer Pro v4.0.12. In addition to monitoring, the Sniffer will also be used to generate traffic.

WhatsUp Gold monitors devices and the services running on them. A map will be generated and all devices monitored via ICMP. To monitor services during the tests, the properties for the appropriate servers will be modified to include the services offered by the server (HTTP for the corporate web server, etc.). Green icons indicate normal responses from the hosts. If communication is lost, the icons change to red. A loss of one or more service changes the host's icon to purple. Finally, gray indicates that the device is not being monitored.

In addition to the real-time graphical display, WhatsUp logs events and gathers response time statistics. This information includes statistics on packets sent, received, and missed, and round trip time average, minimum, and maximum. These statistics provide important information about the health of the network and hosts.

Conducting the Assessment

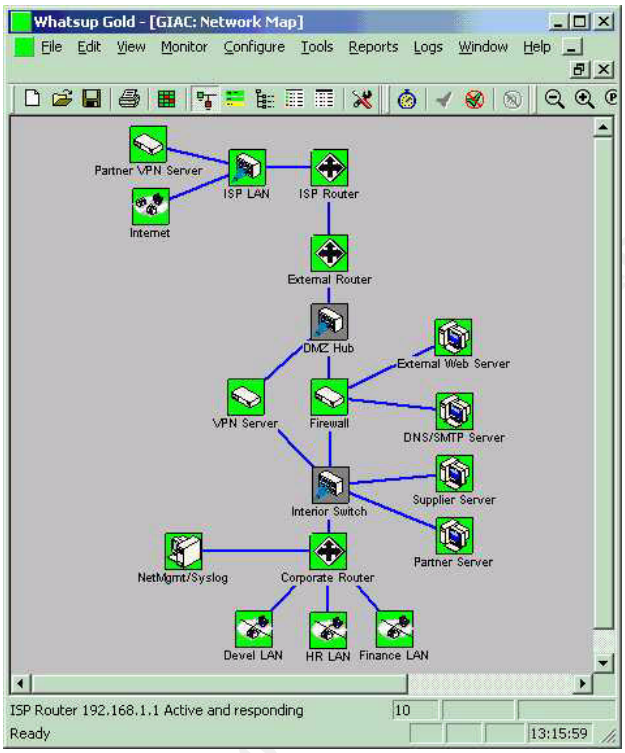
Functionality Tests

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Using WhatsUp, a map was created to monitor the components of the network and the services offered by the host systems.

Figure 10. WhatsUp map of GIAC Enterprises.



DNS, SMTP, and web services were accessed before the tests were conducted to verify that these services were performing correctly.

Penetration Tests

Nessus Scans

Nessus was unable to gain any information about inside systems or have any affect on them. Scans were performed using all possible TCP scanning techniques. The External Router stopped many of the attempts:

Bounded traffic due to failed NAT translations
%SEC-6-IPACCESSLOGP: list 101 denied udp 45.1.1.45(2225) (Multilink1 *PPP*) -> 44.1.1.3(5135), 1 packet
%SEC-6-IPACCESSLOGP: list 101 denied udp 45.1.1.45(2227) (Multilink1 *PPP*) -> 44.1.1.3(69), 1 packet
%SEC-6-IPACCESSLOGP: list 101 denied udp 45.1.1.45(123) (Multilink1 *PPP*) -> 44.1.1.3(137), 1 packet
Blocked inbound traffic with spoofed IP addresses
%SEC-6-IPACCESSLOGP: list 100 denied tcp 44.1.1.3(26454) (Multilink1 *PPP*) -> 44.1.1.3(60242), 1 packet
%SEC-6-IPACCESSLOGP: list 100 denied tcp 44.1.1.3(26647) (Multilink1 *PPP*) -> 44.1.1.3(60242), 1 packet
%SEC-6-IPACCESSLOGP: list 100 denied tcp 44.1.1.2(39207) (Multilink1 *PPP*) -> 44.1.1.2(64603), 1 packet
%SEC-6-IPACCESSLOGP: list 100 denied tcp 44.1.1.2(39303) (Multilink1 *PPP*) -> 44.1.1.2(64603), 1 packet

Nessus was able to detect a couple low risk vulnerabilities on the External Router:

© SANS Institute 2000 - 2005 Author retains full rights.

- Does not use random IP IDs – Received a warning that the host could be used for port scanning other systems. However, the use of private network addresses prevents this activity. Only systems that can communicate with the router are located at GIAC and the ISP.
- Received response to ICMP timestamp – Received a warning that this could be used to defeat time-based authentication protocols. This should not be a risk, but the service will be turned off anyway.

Nessus was also stopped at the DNS/SMTP server. Attempts at performing unauthorized DNS queries generated the message, "named[862}: client 45.1.1.45#xxxx: query denied". SMTP connection attempts were stopped and mail log messages read, "sendmail[13336]: NOQUEUE: [45.1.1.45] did not issue MAIL/EXPN/VRFY/ETRN during connection to MTA".

SAINT Scan

The SAINT scan was run at the Heavy+ level. Numerous attempts were blocked at the router and firewall in the same manner as the Nessus scan. In addition, Firewall-1 also produced alerts regarding the port scanning:

daemon alert product MAD proto ip src 45.1.1.45 dst 10.10.2.2 addtionals: attack=blocked_connection_port_scanning"

Sendmail also played a part in blocking the attempts:

```
  sendmail[13071]: f7GEoNS13071: [45.1.1.45]: VRFY root [rejected]
  sendmail[13073]: f7GEoYS13073: [45.1.1.45]: EXPN root [rejected]
  sendmail[13073]: f7GEoYS13073: [45.1.1.45]: EXPN administrator [rejected]
  sendmail[13285]: NOQUEUE: [45.1.1.45] did not issue MAIL/EXPN/VRFY/ETRN during
connection to MTA
  sendmail[13295]: f7GFOxS13295: SYSERR: putoutmsg ([45.1.1.45]): error on output
channel sending "220 ns1.giac.com ESMTP Sendmail 8.11.2/8.11.2; Thu, 16 Aug 2001
11:24:59 -0400": Connection reset by [45.1.1.45]
  sendmail[13419]: f7GFhWS13419: [45.1.1.45]: VRFY root [rejected]
  sendmail[13419]: f7GFhWS13419: [45.1.1.45]: VRFY administrator [rejected]
  sendmail[13421]: f7GFhhS13421: [45.1.1.45]: EXPN root [rejected]
  sendmail[13421]: f7GFhhS13421: [45.1.1.45]: EXPN administrator [rejected]
```

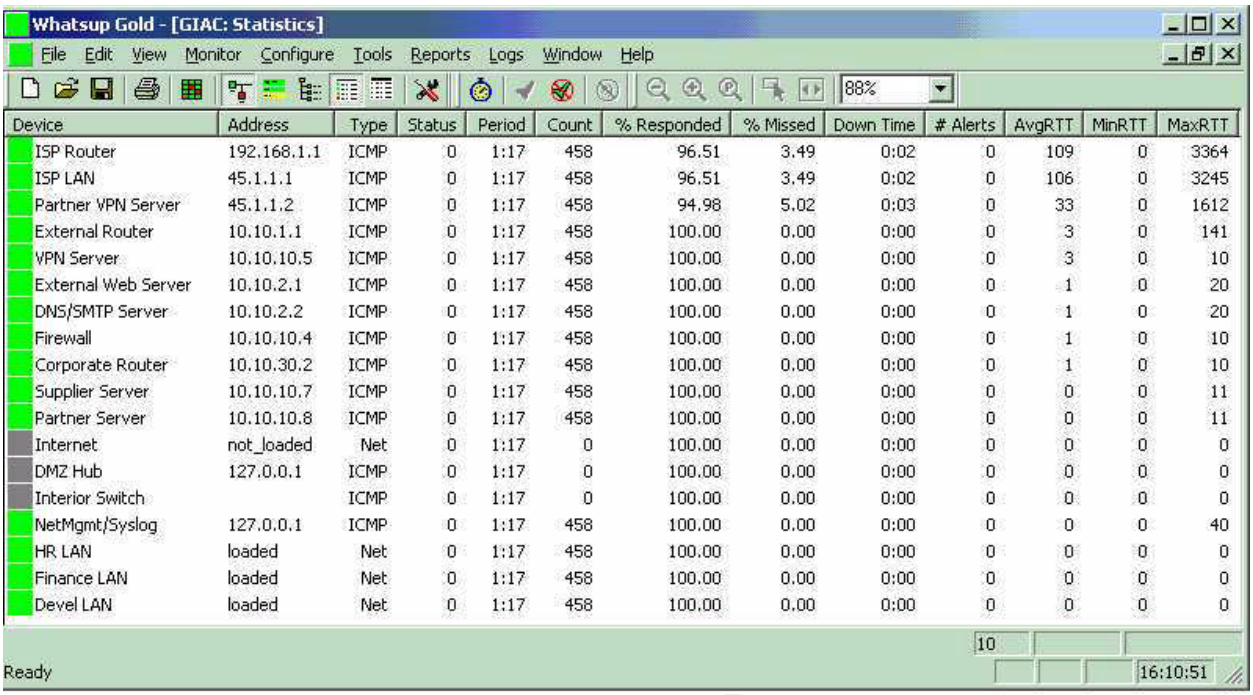
SAINT did discover that the External Web Server is running IIS. It did return one brown level message warning about a possible vulnerability, "Possible buffer overflow in IIS 4". The advisory states that one of the fixes to the problem is to apply Windows NT Service Pack 6 – This has been done.

Performance Monitoring

Statistical data on response times and network reliability was gathered using WhatsUp.

Figure 11. Performance Data from WhatsUp.

© SANS Institute 2000 - 2005 Author retains full rights.



Device	Address	Type	Status	Period	Count	% Responded	% Missed	Down Time	# Alerts	AvgRTT	MinRTT	MaxRTT
ISP Router	192.168.1.1	ICMP	0	1:17	458	96.51	3.49	0:02	0	109	0	3364
ISP LAN	45.1.1.1	ICMP	0	1:17	458	96.51	3.49	0:02	0	106	0	3245
Partner VPN Server	45.1.1.2	ICMP	0	1:17	458	94.98	5.02	0:03	0	33	0	1612
External Router	10.10.1.1	ICMP	0	1:17	458	100.00	0.00	0:00	0	3	0	141
VPN Server	10.10.10.5	ICMP	0	1:17	458	100.00	0.00	0:00	0	3	0	10
External Web Server	10.10.2.1	ICMP	0	1:17	458	100.00	0.00	0:00	0	1	0	20
DNS/SMTP Server	10.10.2.2	ICMP	0	1:17	458	100.00	0.00	0:00	0	1	0	20
Firewall	10.10.10.4	ICMP	0	1:17	458	100.00	0.00	0:00	0	1	0	10
Corporate Router	10.10.30.2	ICMP	0	1:17	458	100.00	0.00	0:00	0	1	0	10
Supplier Server	10.10.10.7	ICMP	0	1:17	458	100.00	0.00	0:00	0	0	0	11
Partner Server	10.10.10.8	ICMP	0	1:17	458	100.00	0.00	0:00	0	0	0	11
Internet	not_loaded	Net	0	1:17	0	100.00	0.00	0:00	0	0	0	0
DMZ Hub	127.0.0.1	ICMP	0	1:17	0	100.00	0.00	0:00	0	0	0	0
Interior Switch		ICMP	0	1:17	0	100.00	0.00	0:00	0	0	0	0
NetMgmt/Syslog	127.0.0.1	ICMP	0	1:17	458	100.00	0.00	0:00	0	0	0	40
HR LAN	loaded	Net	0	1:17	458	100.00	0.00	0:00	0	0	0	0
Finance LAN	loaded	Net	0	1:17	458	100.00	0.00	0:00	0	0	0	0
Devel LAN	loaded	Net	0	1:17	458	100.00	0.00	0:00	0	0	0	0

Statistics gathered during the scans indicated that some packets were lost and communications slowed, but the services remained available.

HTTP SYN Denial of Service Test

The Sniffer was used to capture HTTP SYN packets. It was then configured to play back the packets onto the network as fast as possible. Since an HTTP SYN packet is small, the maximum play back rate was about 8600 packets per second. This yielded a throughput of 6.7Mbps. The maximum bandwidth to GIAC is only 2.88Mbps. During the tests, it was observed that the link quit passing traffic a couple of times for a brief period and once the PPP Multilink when down for a second. The firewall also assisted with blocking the SYN flood. Firewall-1 posted the message "message SYNDefender warning SYN -> SYN-ACK -> RST" and that it rejected the traffic.

Recommendations for Improvements and Design Alternatives

The ISP router, a Cisco 2611, reached 99% CPU utilization during the denial of service test. This shows that additional processing power is required to defend against this attack on the router. Recommend upgrading the router to another Cisco model with a faster CPU.

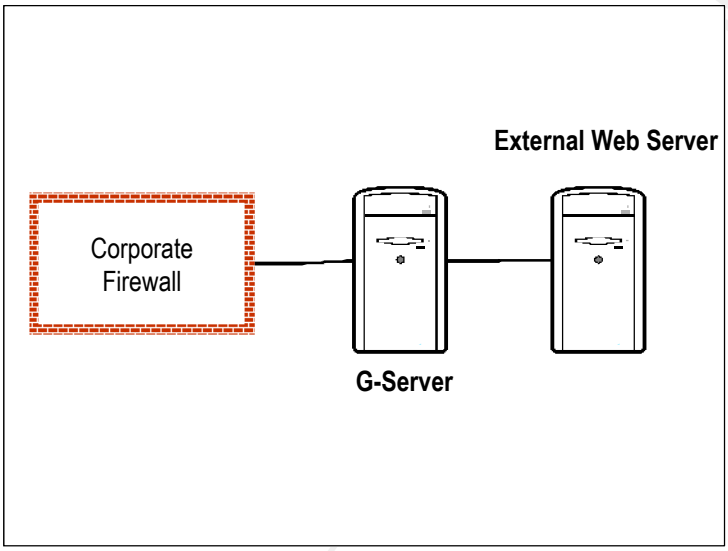
The rate limit access list on the ISP router may require modifications. Instructions for implementing rate limiting are contained on the Cisco web site, but they were tuned for an ISP with a large amount of bandwidth. Further research and tested is required to better validate the effectiveness of the anti-DDoS functionality.

The External Web Server permits anonymous access. This presents a security problem because

© SANS Institute 2000 - 2005 Author retains full rights.

hackers or automated scripts could find an unknown vulnerability and modify the corporate web pages. To protect against this situation, the server could use Gilian's G-Server to protect the content. The process works by creating a digital fingerprint of the content of the web pages. When the content is sent out to the user, it is compared to the digital signature. If they do not match, then the page on the web server is replaced with the page from the secure cache, and the administrator is notified. (Haber)

Figure 12. Network Diagram showing the inclusion of Gilian's G-Server.



Assignment 4 – Design Under Fire

Design Chosen
Tim Alton's design was chosen for this exercise <http://www.sans.org/y2k/practical/Tim_Alton_GCFW.doc>.

Firewall Attack
Tim Alton specifies that he is using Checkpoint's Firewall-1 v4.1 on a Nokia appliance. Tim Hall has found out that Firewall-1 v4.1 on Solaris (and probably on the Nokia IPSO) can be brought down. The attack causes the firewall to think the number of licensed addresses has been violated:

> "On firewall modules with a limited-IP license, Firewall-1 counts the number of unique source IP addresses entering all non-outside interfaces. The outside interface typically is Internet-facing. If more IP addresses are counted

© SANS Institute 2000 - 2005 Author retains full rights.

that the firewall module is licensed for, a warning message is output to the firewall's console. In 4.1, the warning includes a list of all IP addresses counted in the Firewall-1 licensing calculation. The 4.0 message only included the number of IP addresses corresponding to the licensed limit.

By sending a large number of packets with spoofed source addresses to any inside interface, enough addresses will be included in the console output to cause a new warning message to be issued before the previous one can finish. As a result the console device will be overrun and begin to consume large amounts of CPU time. This output makes the console virtually unusable making it more difficult to recover from this situation.

There is no way to block this behavior in the rule base. Even if the spoofed packets in question are dropped explicitly by a rule or implicitly by antipspoofing they will still be included in the license calculation. A reboot will not clear this problem either, since Firewall-1 will begin sending the license violation messages to the console immediately upon rebooting. Clearing the license count as described at PhoneBoy's site will help temporarily, but if the flood of spoofed packets continues Firewall-1 will rapidly end up in the same state again." (Hall)

A countermeasure has been suggested:

"Similar to the IP Frag attack, issuing a 'fw ctl debug -buf' will prevent this console logging from consuming excessive CPU. While many firewall administrators installed this workaround earlier to combat the frag problem, it was probably removed from the fwstart script when they upgraded to SP2 or later." (Hall)

If the fix has not kept in place, then the firewall will be vulnerable to the attack.

Denial of Service Attack

Tim Alton does not specify the line speed between GIAC and their ISP. It is a serial interface on a Cisco router, therefore, it is probably a T-1 or slower line. A denial of service can be easily accomplished by flooding the link from the ISP to GIAC.

An example of this is in Steve Gibson's write up of the attack against his site. This attack was employed by getting Windows users to inadvertently install a DoS server (zombie) via a Sub7Server Trojan onto their systems. The zombies then communicate with their controller via IRC. (Gibson)

© SANS Institute 2000 - 2005 Author retains full rights.

This attack floods the target using UDP and ICMP traffic. If not filtered at the ISP, then the attack traffic will flood out the legitimate traffic. The web site, mail, and name services will all become unusable. Simply adding bandwidth to the link does not work. If 50 cablemodem users with T-1 access attacks the site, then it would take over 72Mbps of bandwidth just to take in all the traffic. An attack that can be pulled off with 50 users could also be pulled off using 500 or 5000 users. What if someone infected the KaZaA client? In the evenings, KaZaA has about 650,000 users online.

Internal System Compromise

Tim Alton's design shows the DNS, SMTP, and web servers all on the same segment. This is a dangerous practice. All his servers are running Windows 2000. If the web server is compromised using the "Unchecked Buffer in Index Server ISAPI Extension" as discussed in Microsoft's Security Bulletin MS01-033, then a trojan can be installed permitting the hacker full access to the server. The newer versions of the Code Red worms are currently exhibiting this activity by installing a back door. Once the web server has been compromised, then the other Windows 2000 servers on the switch can be attacked from the web server. This makes it more likely that the other servers will also fall. Connecting servers to separate ports on the firewall helps limit the damage to a single system.

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

© SANS Institute 2000 - 2005 Author retains full rights.

Works Cited

"Advanced Encryption Standard." National Institute of Standards and Technology. Online. 08 August 2001. <http://csrc.nist.gov/encryption/aes/>

"Configuring Media-Independent PPP and Multilink PPP." Cisco Systems, Inc. 18 July 2001. <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnspr t9/dcdppp.htm>

"Configuring Network Address Translation." Cisco Systems, Inc. Online. 20 July 2001. <http://www.cisco.com/warp/public/556/12.html>

Gibson, Steve. "The Attacks Against GRC.COM." Gibson Research Corporation. Online. 04 July 2001. <http://grc.com/dos/grcdos.htm>

Haber, Lynn. "Shoring Up Security." Network World 28 May 2001: 53, 56.

Hall, Tim. "Firewall-1 DoS Attack." secureroot. Online. 18 January 2001. <http://www.secureroot.com/security/advisories/9798443762.html>

"Improving Security on Cisco Routers." Cisco Systems, Inc. Online. 20 July 2001. <http://www.cisco.com/warp/public/707/21.html>

"Internet Protocol V4 Address Space." The Internet Assigned Numbers Authority. Online. 24 June 2001. <http://www.iana.org/assignments/ipv4-address-space>

"ISC BIND 8." Internet Software Consortium. Online. 14 August 2001. <http://www.isc.org/products/BIND/bind8.html>

"Microsoft Security Bulletin MS01-033." Microsoft Corporation. Online. 18 June 2001. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ MS01-033.asp>

"RealSecure Product Literature." Internet Security Systems, Inc. Online. 31 July 2001. <http://documents.iss.net/literature/RealSecure/rs_ps.pdf>

"Securing Linux Step-by-Step." The SANS Institute. Version 1.0. 2000.

"Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks." Cisco Systems, Inc. Online. 20 July 2001. <http://www.cisco.com/warp/public/707/newsflash.html>

© SANS Institute 2000 - 2005 Author retains full rights.

"What is Snort?" Martin Roesch, et al. Online. 08 August 2001.
<http://www.snort.org/>

"White Paper: Alternatives for High Bandwidth Connections Using Parallel T1/E1 Links." Cisco Systems, Inc. 18 July 2001.
<http://www.cisco.com/warp/public/cc/pd/ifaa/pa/much/tech/althb_wp.htm>

Widdowson, Liam. "Jailed Internet Services." Sys Admin August 2001: 39-45.

"Windows NT Security Step by Step." The SANS Institute. Version 2.15. 30 July 1999.

Figures

Figure 6. "RealSecure Suite." Internet Security Systems, Inc. Online. 31 July 2001.
<http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_networksensor/index.php>

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

© SANS Institute 2000 - 2005 Author retains full rights.