Global Information Assurance Certification Paper

Introduction

GIAC Enterprises (GENT) is a pre-IPO, family-owned fortune cookie manufacturer and supplier. Its business has existed for forty years. The business plan for GIAC has been conservative. However, due to erosion of market share and tighter margin, GIAC has decided to venture into e-Business in order to revamp and reverse the company's fortune. The president of GENT is fully cognizant of the importance of Internet security and supportive of building a scalable, effective and efficient security infrastructure for the new e-Business initiative.

Currently, GENT has four main groups of information users:

1. The Customers

This group represents outside companies/restaurants that purchase bulk online fortunes

2. Suppliers

This group currently represents the authors of fortune cookie sayings that connect to supply fortunes. There is a future plan to create an extranet with other suppliers such as flour supplier, egg supplier etc..

3. Partners

This group represent the international partners that translate and resell fortunes. GENT is part of the International Fortune Alliance.

Purpose

The purpose of this document is to define an efficient and cost effective security architecture for GENT. The security architecture must serve the important role of assisting in protecting the confidentiality, integrity and availability of current GIAC information.

Scope

The scope of this document will entail defining the security architecture which will include the following components:

- Filtering routers
- Firewalls
- VPNs to Business Partners and Suppliers
- Secure Remote Access
- Internal Firewalls

This document will provide a set of diagrams which will describe the proposed security infrastructure.

To minimize Internet related security risks; the security infrastructure will incorporate a layered approach to security which eliminates single points of failure.

Network Access Requirement

There are four main groups of users that require network access:

Customers

The companies that purchase bulk online fortunes. Business conducted with this group of customers will be through www.gent.com. All transactions will be secured with Secure Socket Layer (SSL) which 128-bit encryption will be enforced.

Suppliers

The suppliers are authors of fortune cookie sayings that connect to supply fortunes. Because proprietary information may be involved, VPN access will be provided to this group of users.

Partners

The international partners are partners that translate and resell fortunes. Similar to the suppliers, due to potential proprietary information is involved; this group will be given VPN access to GENT internal systems and databases.

GENT

The employees located on GENT's internal network. This group needs to be provided with Email and Internet access. Some remote users will require VPN while on the road and systems administrators will require secure remote access to the internal systems for administration purposes.

Assignment 1

Security Architecture-Perimeter Network Security Design

Border Router

Cisco 3660 multi-service platform running IOS v12.2 is selected for its performance, flexibility and scalability.

For the border router, a security policy will be created and maintained. This policy will identify who is allowed to log in to the router, who is allowed to configure and update it, and who should outline the logging and management practices for it.

Access list filters will be implemented to permit only those protocols and services that the network users really need, and denying everything else. This will alleviate some of the loads and increase the performance of the firewall.

Primary Firewall

Checkpoint Firewall 1 (FW1) running on Nokia IP330 appliance will be the platform for the network/firewall security solution.

IP330 is selected for as it is pre-configured and tested for rapid deployment and supports a comprehensive suite of IP routing protocols and remote management capabilities. www. http://www.nokia.com/securitysolutions/platforms/330.html This will lower the set up, system administration and maintenance costs at least initially.

FW1 is a stateful inspection which "extracts the state-related information required for security decisions from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts". http://www.checkpoint.com/products/security/firewall-1_primer.html This solution is more secure when compared to other types of firewall solutions such as application proxy (firewall) and packet filtering. Security policy will be defined and created based on the "Default to Denial" rule. Every Internet connectivity path and Internet service not specifically permitted by this policy will be blocked by the firewall.

VPN

Contivity 1600 will be used as the VPN solution for providing secure tunnelling for remote access for staff who is on the road and extranet for the suppliers and partners. Contivity 1600 is selected as it is relatively easy to deploy, support a wide range of interfaces and interoperate with GENT's existing network perimeter defense components such as the Cisco border router, FW1 and NT web servers.

Secondary Firewall

A secondary firewall running OpenBSD v2.9 is deployed to protect the internal network. OpenBSD firewall tools such as IPF(IP filtering) and IPNAT (Network Translation) will be used. For this firewall, no remote log-in and console access only will be allowed.

IP Address Assignment and Subnets

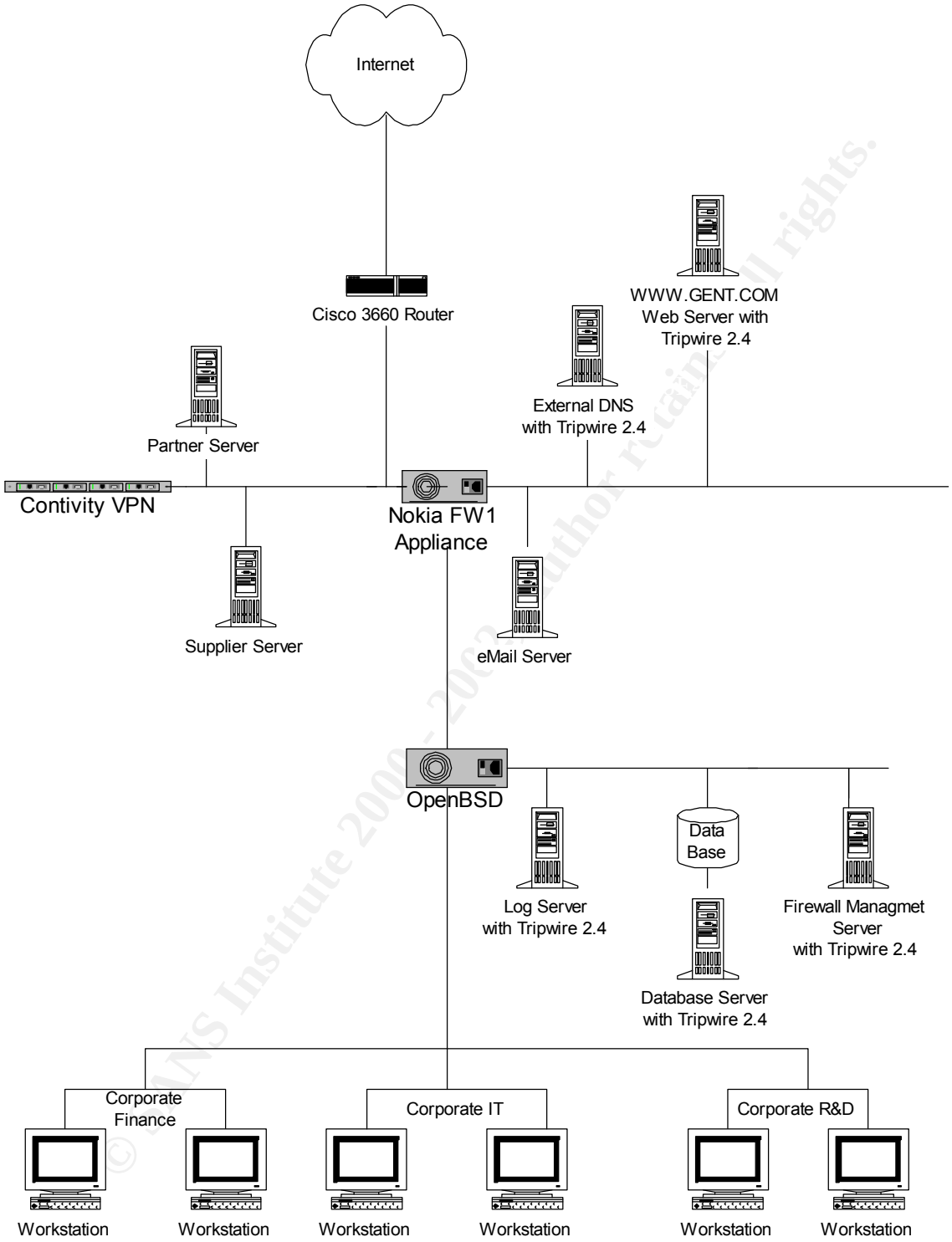
GENT has a class C network. Its registered class C subnet is 192.3.3.0. Following is the addressing scheme of the network:

Border Router:	192.3.8.1 External Interface, 192.3.3.5 Internal Interface
Primary Firewall:	192.3.3.7
Internal Firewall:	192.2.3.8

External DNS Server:	172.16.2.2
eMail Server:	172.16.2.4
Web Server:	172.16.2.3
Log Server:	172.17.2.2.
Firewall Management Server:	172.17.2.4
Data Base Server:	172.17.2.3
Partner Server:	172.18.2.4
Supplier Server	172.18.2.3
VPN Contivity Switch:	172.18.2.2
Corporate Finance:	10.0.1.0
Corporate IT:	10.0.2.0
Corporate R&D:	10.0.3.0

Architecture Diagram

Following is the GENT security architecture diagram:



Assignment 2

Security Policy

Based on the security architecture discussed above, a security policy that outlines the requirement and rules for the three major components will be provided below.

Border Router General Policy

Routers provide services that are essential to the correct, secure operation of the networks they serve. Compromise of a router can lead to various security problems on the network served by the router, or even other networks with which that router communicates. "In general, well-configured secure routers can greatly improve the overall security posture of a network. Furthermore, security policy enforced at a router is a difficult for end-users to circumvent, thus avoiding one very serious potential source of security." http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>

Before specific router policy is defined, the following guide which is derived from the various technical readings from http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/ and http://www.nsa.gove will be used to govern the security design of the Cisco border router:

1) Unnecessary Services Are Disabled

Unnecessary or insecure services present vulnerabilities, which could alter the functionality of the router. For each interface, disable unnecessary services. All routers managed or connected directly to the GENT's infrastructure should have the following rules to each router as shown in the section below:

Syntax: **no IP directed-broadcast**	*Directed broadcast can be used for attacks, disable it.
Syntax: **no IP proxy-ARP**	*Disable this, unless the router is serving as a LAN bridge.

In global configuration mode, disable unnecessary services.

Syntax: **no IP source-route**	*This rarely-used feature can be helpful in attacks, disable it.
Syntax: **no service udp-small-servers**	* Legacy Feature not required
Syntax: **no service tcp-small-servers**	* Legacy Feature not required

2) Unnecessary "Unix" Services Are Disabled

Several devices offer an implementation of the UNIX 'finger' and 'ntp' service. The finger service is used to find out which users are currently logged into the device while the ntp service is used to obtain the system time. Since this information can sometimes be valuable to an attacker, issuing the following commands should disable both 'ntp' and 'finger' services: **no service finger, no ntp enable.**

3) Remove the Cisco Discovery Protocol

All Cisco devices are configured by default with the Cisco Discovery Protocol (CDP) service turned on. This service enables an attacker to obtain detailed hardware and software information such as firmware numbers, make and model of the device, etc. Issuing the following command will disable the CDP service: **no cdp enable.**

4) Remove Management HTTP Servers

Many devices allow remote system management through a mini HTTP server. Authentication is generally performed in clear text and poses a significant risk to security. As well, many mini HTTP implementations are rarely audited for security vulnerabilities and often contain holes. Network administrators can disable the HTTP service by using the command: **no IP http.**

5) Security Advisories and Support

After the initial installation of the Internetwork Operating System (IOS), the latest recommended Cisco patches should be installed. These patches can be obtained from the supported vendor if the patch files have been obtained from a source other than directly from Cisco their cryptographic checksums are to be verified prior to installation. Timely implementation of security patches should be installed on a timely and consistent basis.

Ensure that all router(s) are running a current major version number of Cisco IOS. The minor version number difference is not greater than 3. Network Administrators should frequent online vulnerability sites like www.securityfoucs.com to verify if all Cisco hardware is not susceptible to any known security vulnerabilities.

6) SNMP access is secured with an access list and unique community names.

SNMP is used to query the router for operational information as well as updating the router configuration. These functions, if not secured, could cause a security breach of the router. Unauthorized users could gather network information to help customize attacks or could maliciously change the router configuration. Set the snmp community name and access permissions with the 'snmp-server' command. Ensure the basic community strings like "public" or "private" are not used. All references to **snmp-server community** <string> should be modified. To remove the default community string and set a better read-only string

Router (congfig) # **no snmp community public**

Router (congfig) # **no snmp community private**

Router (congfig) # **snmp community** P@55**Word**

7) The TCP Intercept feature is used to prevent the TCP SYN-flood denial of service attacks.

The Cisco IOS operating environment contains several mechanisms that can be used to develop a comprehensive rule set that will further safeguard the network from bandwidth consumption and amplification attacks. One of these mechanisms is the **tcp-intercept** command. The **tcp-intercept** command mitigates the effects of flooding attacks by intercepting and validating Transmission Control Protocol (TCP) connection requests. The intercept mechanism works by intercepting TCP synchronization packets from clients to servers that match a defined ACL. Once authenticated, the server end connection is established on behalf of the connecting client by the router. This allows the router to have more control over connection establishment and termination as options such as connection timeouts can be enforced. If performance is a concern, the TCP Intercept mechanism can be implemented in 'watch mode', which passively watches connection requests passing through the router. If a connection fails to be established within a specified time interval the router intervenes and terminates the connection attempt.

8) Router Terminal Settings Are Set Securely

Ensure that TCP keepalives are configured using the service tcp-keepalives-in. This will prevent 'ghosted' sessions from forming after a router crash/reboot.

Ensure that the command **transport input none** is used on all public asynchronous/modem lines to prevent reverse telnetting / interactive logons.

9) Enable TFTP Services Only When Needed

Administrators use the Trivial File Transfer Protocol (TFTP) to update a device's IOS configuration. However, the protocol relies upon insecure means of authentication and is highly susceptible to IP spoofing/TCP hijacking/insertion attacks and should be enabled only when updating the device's IOS configuration/image. Many devices' have this service enabled out-of-box.

10) Shutdown Unnecessary Interfaces

An unnecessary interface on a router increases the likelihood of compromise and mis-use. It is prudent for GENT to disable all unused or interfaces that are not required. It is possible to shut down unused interfaces by using the shutdown command. Check

interfaces with the **show interfaces** command. If the router has an auxiliary console port (aux port) and it is not in use, shut it down as shown below.

11) All Login Devices On The Router Utilize Advanced Password Authentication

The 'enable secret' command is used to set the password that grants privileged administrative access to the IOS system. An enable secret password should always be set. Do not use the 'enable password' option, as the password algorithm is weak.

12) The Router Is Configured To Log Off Idle User Sessions After A Set Timeout Period

Failure to log off idle user sessions wastes valuable router resources and could potentially leave a backdoor open onto the router. Ensure that all terminal lines are configured with a connection timeout limit. This can be done using the **exec-timeout** command on all lines. This will mitigate the effects of an attacker performing a Denial of Service attack by consuming all possible VTYs.

13) Third Party Accounts Disabled

All vendor support accounts are by disabled except when needed, and then only for the period of the immediate need. This ensures that vendor accounts can not make changes accidentally or maliciously to production routing devices.

14) Warning banners are displayed upon attempted access to the router

Failure to display adequate warning messages could result in the loss of litigation capabilities. One requirement for prosecution on grounds of invasion of private systems is to mark them clearly as private. **If a legal caption notice is not used, GENT may not be able to prosecute in the event that a user misappropriates corporate resources. A typical router banner usually reads as follows:**

"This router is restricted exclusively to authorized users. All other users will be prosecuted to the full extent of the law."

Configure appropriate legal banners using the banner login command. To set the router's banner use the command: **banner motd** *delimiter message delimiter*

15) Shared Root Passwords On Multiple Routers Disallowed

All Cisco routers must have unique passwords.

16) Extended Access Lists Are Used To Prevent IP Spoofing

An unauthorized user may try to gain access or disrupt service to site systems by forging or "spoofing" legitimate IP addresses. Create an access list with the access-list command to prevent IP spoofing. All internal IP addresses should be configured based on RFC 1918 unroutable Internet addresses.

17) Account and Change Management

Privileges for the user account should commensurate with the user's job function. Any request for an addition, change or delete to a user account must be approved by the user's manager.

18) Only Authorized GENT Administrator Shall Have Access To Production

It is critical to maintain strict control over the production environment. Clients, 3rd party vendors and other business partners increase the risk over the security and integrity of the production environment. Only authorized GENT employees will have full access to the production routers.

19) Modem Access To Router Only Enabled When Necessary

Only if absolutely required should a modem be connected to the aux port as a backup or remote access method to the router. Attackers using simple war-dialling software will eventually find the modem, so it is necessary to apply access controls to the aux port. All connections to the router should require authentication (using individual user accounts) for access.

20) All System Logs Are Purged

All router logs are to be purged and retained at least 6 months. Logs must be securely stored to prevent unauthorized access or modification to data.

21) The level of SNMP logging is set to a minimum of CRITICAL

If the SNMP logging level is set below the critical level, important security and administration events will not be logged. Set the SNMP trap level to the appropriate level with the logging trap command. Logging should be set to a minimum of critical and is enabled on routers to ensure that all administrative actions are documented.

Syntax: logging trap <level>

Example: logging trap critical

This example sets the logging level to critical. Any message, which is categorized as critical, alert or emergency, will be sent to the syslog server.

22) Cisco ACL Violation Logging

By default, IOS does not log ACL violations. When an ACL violation is detected, IOS can be configured to log detailed packet information such as IP address, port numbers, MAC addresses, etc. ACL violation logging can be enabled with the **log-input** command. GENT shall enable ACL logging only when there is a suspicion of unauthorized events.

23) Current Versions Of The Router Configuration Files Are Stored On A Secure Server And Are Periodically Validated

Without adequate monitoring of router configuration for changes there is a risk that an unauthorized user could access the router and modify the configuration file without detection. The site should create a formal change management and backup guidelines on all routers.

24) Backup Procedures Are Documented

The implementation of a comprehensive backup schedule suited to organizational needs will be documented. Data backups not only allow recovery from hardware failures and accidental deletions, they also protect against unauthorized filesystem changes made by an intruder. In some cases, if the intruder is very active or destructive, the backups may be the only way to restore the system to a known state. Additionally, backups may be useful in providing evidence of an intruder's activities (by capturing a file that he later deleted).

More commonly backup are a prudent process when upgrading the current Cisco IOS. Before updating the administrator should complete some checks:

Determine the memory requirements for the update, and if necessary install additional memory to the router.

Set up and test file transfer capability between the administrator's computer and the router.

Schedule the required downtime (usually after regular business hours) for the router to perform the update.

After obtaining an update from the router vendor, the administrator should follow procedures similar to the following:

- Shut down or disconnect the interfaces on the router.
- Back up the current operating system and the current configuration file to the administrator's computer.
- Load the update for either the operating system or for the configuration file.
- Perform tests to confirm that the update works properly.

If the tests are successful then restore or reconnect the interfaces on the router. If the tests are not successful then back out the update.

Border Router Configuration Policy

After defining the general router policy, a carefully designed configuration policy is required. The border router will serve as the first line of defence in the "Defence in Depth" concept that is used in the overall security design. As such, proper configuration is of paramount importance. Following is the configuration policy used for the GENT's Cisco border router:

```
banner motd !
   WARNING: "This router is restricted exclusively to authorized users.  All other users
                    will be prosecuted to the full extent of the law."

Config t
           Interface Serial 1/0
              ip access-group 125 in
              ip access-group 126 out
              no ip directed-broadcast
              no ip proxy-arp
              no ip source-route
              no service finger
              no ntp enable
              no cdp enable
              no IP http
              no snmp
              no ip unreachables
              no service udp-small-servers
              no service tcp-small-servers


 !     Filtering for inbound traffic:
access-list 125 deny ip 10.0.0.0.255.255.255 any log
access-list 125 deny ip 172.16.0.0.0.31.255.255 any log
access-list 125 deny ip 192.168.0.0.0.255.255 any log
access-list 125 deny ip 127.0.0.0.0.255.255.255 any log
access-list 125 deny ip 224.0.0.0.31.255.255.255 any log
access-list 125 deny ip 192.3.3.0.0.0.0.255 any log
access-list 125 deny icmp any any redirect
access-list 125 deny ip host 0.0.0.0 any log any log

access-list 125 deny tcp any any range ftp telnet log
access-list 125 deny tcp any any range exec lpd log

access-list 125 deny udp any any eq sunrpc log
access-list 125 deny tcp any any eq sunrpc log
access-list 125 deny udp any any eq 2049 log
access-list 125 deny tcp any any eq 2049 log
access-list 125 deny udp any any 4045 log
```

```
access-list 125 deny tcp any any eq 4045 log


access-list 125 deny tcp any any 135 log
access-list 125 deny udp any any 135 log
access-list 125 deny udp any any range 137 138 log
access-list 125 deny tcp any any eq 139 log
access-list 125 deny tcp any any eq 445 log
access-list 125 deny udp any any eq 445 log


access-list 125 deny tcp any any range 6000 6255 log

access-list 125 permit tcp any any 0.0.0.0 eq 53
access-list 125 permit udp any any 0.0.0.0 eq 53

access-list 125 permit any any 0 eq 25

access-list 125 permit any any 0 eq 80
access-list 125 permit any any 0 eq 443

access-list 125 deny udp any any 69 log
access-list 125 deny tcp any any 179 log
access-list 125 deny tcp any any 1080 log


Log 172.16.2.3

access-list 125 deny ip any any log



!       Filtering for outbound traffic:
access-list 126 permit ip 192.3.3.0.0.0.0.255 any
access-list 126 deny ip any any log
```

A tutorial is provided below on how to implement the above border router policy and the commands used will be explained:

Although Cisco supports three types of ACL; the Standard access list, Extended access list and the Reflexive access list, the Extended access list will be used to define the ACL for GENT's border router. Extended Access List is defined by Nancy Navato's **"Easy Steps to Cisco Extended Access List"** http://www.sans.org/infosecFAQ/netdevices/easy_steps.htm as an ordered list of statements that can deny or permit packets based on source and destination IP address, port numbers and upper-layer protocols. Standard access list can deny or permit packets by source address only and permit or deny entire TCP/IP protocol suite. Therefore by extended, it means greater functionality and flexibility. Extended access list is a good example of "packet filtering" where the flow of data packets can be controlled in your network. It can filter based on source and destination, specific IP protocol and port number. Extended access list is defined by a list number between 100 and 199. "125" will be used for our purposes.

Banner MOTD

To set the router's banner login, ***banner motd*** command is used.

Config t

In order to put the router into configuration mode, ***config t*** command is used.

Interface Serial 1/0

ip access-group 125 in
ip access-group 126 out
no ip directed-broadcast
no ip proxy-arp
no ip source-route
no service finger
no ntp enable
no cdp enable
no ip http
no snmp
no ip unreachables
no service udp-small-servers
no service tcp-small-servers

This is the configuration of the external interface.

- ***Ip access-group 125 in and ip access-group 126*** out are used to activate the extended ACLs for IP traffic on the current interface.
- ***No ip direct-broadcast*** command is used because direct broadcast can be used as attack and should therefore be disabled.

- ***No ip proxy-arp*** command is used because this can prevent disclosure of information to other computer MAC addresses.
- ***No ip source-route*** is the command that prevents the router from accepting IP source routing packets
- ***No service finger*** is the command that prevents reconnaissance and gathering of network topology information by malicious hackers.
- ***No ntp enable*** is the command that prevents hackers from obtaining the system time.
- ***No cdp enable*** is the command that prevents the Cisco Discovery Protocol from running so that information about the router can be obtained.
- ***No ip http and No snmp*** is the command that prevents malicious hackers from obtaining useful information about the network and the router. These services often contain vulnerabilities and if not patched, can leave the router vulnerable to attacks.
- ***No ip unreachable*** is the command that prevents the router from sending ICMP IP unreachable messages. Removing this will be reconnaissance and gathering of network topology information by malicious hackers.
- ***No service udp-small-servers and no service tcp-small-servers*** are legacy commands that should not be required and therefore disabled.

ACLs are required to provide filtering for the inbound traffic.

- ***Access-list 125 deny ip 10.0.0.0.255.255.255 any log***
  Access-list 125 deny ip 172.16.0.0.0.31.255.255 any log
  Access-list 125 deny ip 192.168.0.0.0.0.255.255 any log
  These are the commands that block incoming packets from GENT's private subnets. Specifically, "Spoofed" addresses and source routed packets should be blocked. No packets coming from outside GENT should be sourced from internal or private addresses. Any exception will be logged.

- ***Access-list 125 deny ip 127.0.0.0.0.255.255.255 any log*** is the command that blocks packets coming externally from the 127.0.0.local subnet. Any exception will be logged.

- ***Access-list 125 deny ip 224.0.0.0.31.255.255.255 any log*** is the command that blocks external packets from a broadcast address. Any exception will be logged.

- ***Access-list 125 deny ip 192.3.3.0.0.0.0.255 any log*** is the command that blocks external packets that appeared to be sourced internally from GENT's private subnets. Any exception will be logged.

- ***access-list 125 deny icmp any any redirect*** is the command that block any icmp redirect. This will prevent spoofing attack. Any exception will be logged.

- ***Access-list 125 deny ip host 0.0.0.0 any log any log*** is the command that blocks external packets from 0.0.0.0. Any exception will be logged.

- ***Access-list 125 deny tcp any any range ftp telnet log***
  Access-list 125 deny tcp any any range exec lpd log
  These are the commands that block the login services such as Telnet, FTP and Rlogin. These services are generally high risk and should be disabled and added back as needed. Any exception will be logged.

- ***Access-list 125 deny udp any any eq sunrpc log***
  Access-list 125 deny tcp any any eq sunrpc log
  Access-list 125 deny udp any any eq 2049 log
  Access-list 125 deny tcp any any eq 2049 log
  Access-list 125 deny udp any any 4045 log
  Access-list 125 deny tcp any any eq 4045 log
  These are the commands that block the Remote procedure calls (RPC) and Network File Services (NFS). These services contain many vulnerabilities. As these vulnerabilities can be exploited, therefore, they should be disabled. Any exception will be logged.

- ***Access-list 125 deny tcp any any 135 log***
  Access-list 125 deny udp any any 135 log
  Access-list 125 deny udp any any range 137 138 log
  Access-list 125 deny tcp any any eq 139 log
  Access-list 125 deny tcp any any eq 445 log
  Access-list 125 deny udp any any eq 445 log
  These are the commands that block the external Netbios over TCP (NBT). NBT should be blocked as Netbios is not a secure protocol and can allow for global sharing over the internet. Blocking these will also alleviate the firewall workload.

- ***Access-list 125 deny tcp any any range 6000 6255 log*** is the command that blocks the X Window ports. The purpose of this block is to secure an internal X Windows configuration. Any exception will be logged.

- ***Access-list 125 permit tcp any any 0.0.0.0 eq 53***
  Access-list 125 permit udp any any 0.0.0.0 eq 53
  These commands are necessary in order to allow DNS traffic to only the name server.

- ***Access-list 125 permit any any 0 eq 25*** is the command that allows SMTP traffic to only the mail server.

- ***Access-list 125 permit any any 0 eq 80***

Access-list 125 permit any any 0 eq 443
These commands are to permit http/https traffic to only the web server.

- ***Access-list 125 deny udp any any 69 log***
  Access-list 125 deny tcp any any 179 log
  Access-list 125 deny tcp any any 1080 log
  These commands are to block other high risk, exploitable services that are not in used. Specifically, they are TFTP port 69, BGP port 179 and Socks port 1080. Any exception will be logged.

- ***Log 172.16.2.3*** is the command that specified logging to the log server.
- ***Access-list 125 deny ip any any log*** is the command that block all other incoming traffic. All exception will be logged.

ACLs are required to provide filtering for the outbound traffic.

- ***access-list 126 permit ip 192.3.3.0.0.0.0.255 any*** is the command that permits traffic from GENT internal subnets traversing to the Internet.
- ***access-list 126 deny ip any any log*** is the command that blocks all other outgoing traffic. All exception will be logged. This command will prevent spoofed address attacks that originate from GENT internal network.

Firewall General Policy

Firewall is an integral part of our "Defence in Depth" strategy. The following GENT's general firewall policy will define what is to be enforced; specifically, what is to be allowed and denied.

1.0 Default To Denial

Every Internet connectivity path and Internet service not specifically permitted by this policy must be blocked by GENTS firewalls. In addition, any network connectivity path not specifically permitted must be denied by firewalls.

2.0 Auditing, Logging and Accounting

2.1 Auditing of Firewall

Because firewalls provide such an important barrier to unauthorized access to GENT networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures.

2.2 Logging of Critical Files

All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner

3.0 Backup, Recovery and Contingency Planning

3.1 Current Versions Of The Firewall Configuration Files Are Stored On A Secure Server And Are Periodically Validated

Without adequate monitoring of firewall configuration for changes, there is a risk that an unauthorized user could access the firewall and modify the configuration file without detection. The site should create a formal change management and backup guidelines on all firewall.

3.2 Backup Procedures Are Documented

The implementation of a comprehensive backup schedule suited to GENT's needs will be documented. Before updating the administrator should complete some checks:

- Determine the memory requirements for the update, and if necessary install additional memory to the router.
- Set up and test file transfer capability between the administrator's computer and the router.
- Schedule the required downtime (usually after regular business hours) for the firewall to perform the update.

After obtaining an update from the firewall vendor, the administrator should follow procedures similar to the following:

- Shut down or disconnect the interfaces on the firewall.
- Back up the current operating system and the current configuration file to the administrator's computer.
- Load the update for either the operating system or for the configuration file.
- Perform tests to confirm that the update works properly.

If the tests are successful then restore or reconnect the interfaces on the firewall. If the tests are not successful then back out the update.

3.3 Contingency Planning

Technical staff working on firewalls must prepare and obtain from GENT corporate IT approval for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, and Internet Service provider (ISP) unavailability. These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable information systems environment.

4.0 External Connections

All in-bound real-time Internet connections to GENT internal networks and/or multi-user computer systems must pass through a firewall before users can reach a log-in banner. Aside from personal computers which access the Internet on a single-user session-by-session dial-up basis, no GENT computer system may be attached to the Internet unless it is protected by a firewall. The firewall must have a log-in screens that have a notice indicating that: (1) the system may only be accessed by authorized users, (2) users who log-in represent that they are authorized to do so, (3) unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and (4) system usage will be monitored and logged.

5.0 Extended User Authentication

Inbound traffic making access to GENT networks through a firewall must in all instances involve extended user authentication measures.

6.0 Virtual Private Networks

To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic (with the exception of Internet mail and push broadcasts) making access to GENT networks must be encrypted. These connections must be established through virtual private networks or VPNs.

7.0 Firewall Access Mechanisms

All GENT firewalls must have unique passwords or other access control mechanisms. Those who administer GENT firewalls must have their identity validated via extended user authentication mechanisms (as defined above). In certain high security environments, such as the GENT E-Business site, remote access for firewall administrators is prohibited. For these environments, all firewall administration activities must take place in person.

8.0 Firewall Access Privileges

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically trained individuals with a business need for these same privileges.

9.0 Secured Subnets

Portions of GENT's internal network that contain sensitive or valuable information must employ a secured subnet. Access to this and other subnets must be restricted with firewalls and other control measures.

10.0 Demilitarized Zones

All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls in a demilitarized zone (DMZ).

11.0 Network Management Systems

Firewalls must be configured so that they are visible to internal network management systems. Firewalls must also be configured so that they permit the use of remote automatic auditing tools to be used by authorized GENT staff members.

12.0 Disclosure of Internal Network Information

The internal system addresses, configurations, and related system design information for GENT networked computer systems must be restricted such that both systems and users outside GENT's internal network cannot access this information.

13.0 Virus Screening and Content Screening

Virus screening and content screening software must be installed and enabled on all GENT firewalls.

14.0 Firewall Dedicated Functionality

Firewalls must run on dedicated machines which perform no other services. To reduce the chances of security compromise, firewalls must have only the bare minimum of operating systems software resident and enabled on them.

15.0 Firewall Change Control

Any change to the firewall must be tested before being used in a production environment.

16.0 Monitoring Vulnerabilities

GENT staff members responsible for managing firewalls must subscribe the CERT advisories and other relevant sources providing current information about firewall vulnerabilities. Any vulnerability which appears to affect GENT networks and systems must promptly be brought to the attention of the corporate IT.

17.0 Standard Products

Unless advance written approval is obtained from the corporate IT, only those firewalls appearing on the list of approved vendors and products may be deployed with GENT networks.

18.0 Firewall Physical Security

All GENT firewalls must be located in locked rooms accessible only to those who must have physical access to such firewalls to perform the tasks assigned by management. These rooms must have burglar alarms as well as an automated log of all who gain entry to the room.

Firewall I Configuration Policy

The general firewall policy will dictate how the firewall configuration policy should be designed. As with the border router , the firewall will serve as the front line of defence in the "Defence in Depth" concept overall security design. Therefore, proper design of the policy is critical. Following is the firewall 1 rulebase that will be implemented:

Firewall 1 Rulebase

10.71.28.29 - Check Point Policy Editor

Print... | Next Page | Prev Page | Two Page | Zoom In | Zoom Out | Close

No.	Source	Destination	Service	Action	Track	Install On	Time	Com
1	FW-Manager	Gent-FW1	Any	accept	Long	Gateways	Any	
2	Any	Gent-FW1	Any	drop	Long	Gateways	Any	
3	Any	EXT_DNS	dns	accept	Short	Gateways	Any	
4	Any	E-MAIL	smtp	accept	Short	Gateways	Any	
5	Any	WWW	http https	accept	Short	Gateways	Any	
6	WWW PARTNER_SERVER SUPPLIER_SERVER	DB	sqlnet1 sqlnet2	accept	Short	Gateways	Any	
7	Any	GENT-VPN	IPSEC	accept	Long	Gateways	Any	
8	GENT-NETWORK	SUPPLIER_SERVER PARTNER_SERVER SERVICE-SERVER	SSH	accept	Long	Gateways	Any	
9	GENT-NETWORK	SUPPLIER_SERVER PARTNER_SERVER SERVICE-SERVER	Any	accept	Long	Gateways	Any	
10	NK-FW1 BORDER-ROUTER	LOGGING-SERVER	syslog	accept	Long	Gateways	Any	
11	Any	Any	Any	drop	Short	Gateways	Any	

Page 1 | 10.71.28.29 | CAP | NUM

Start | 10.71.28.29 ... | TEST-FW-POL... | EN | 10:44 AM

Explanation of the Firewall Rulebase

Source	Destination	Service	Action	Track	Install On	Time
1)FW-Manager	**FW-1**	**Any**	**Accept**	**Long**	**Gateways**	**Any**

This rule is to allow firewall manager to establish connection to the firewall. No remote administration will be allowed as per the firewall policy.

Source	Destination	Service	Action	Track	Install On	Time
2) Any	**FW-1**	**Any**	**Drop**	**Long**	**Gateways**	**Any**

This rule will drop any attempt connection or traffic to the firewall.

Source	Destination	Service	Action	Track	Install On	Time
3) Any	**Ext DNS**	**DNS**	**Accept**	**Short**	**Gateways**	**Any**

This rule allows public access to the DNS server. This will allow the public to resolve the IP addresses of GENT external hosts.

Source	Destination	Service	Action	Track	Install On	Time
4)Any	**E-Mail**	**SMTP**	**Accept**	**Short**	**Gateways**	**Any**

This rule allows emails to get through to the email server through smtp.

Source	Destination	Service	Action	Track	Install On	Time
5) Any	**WWW**	**http/https**	**Accept**	**Short**	**Gateways**	**Any**

This rule will allow www connection to the web server using either http or https.

Source	Destination	Service	Action	Track	Install On	Time
6) www						
Partner/Supplier	**DB**	**SQL**	**Accept**	**Short**	**Gateways**	**Any**

This rule will allow the public users, partner and supplier to place order in their respective locations and the order will be transferred, stored and processed in the database server.

Source	Destination	Service	Action	Track	Install On	Time
7) Any	**GENT-VPN**	**IPSEC**	**Accept**	**Long**	**Gateways**	**Any**

This rule will allow the remote workers, suppliers and partners to connect to the restrictive GENT servers using VPN.

Source	Destination	Service	Action	Track	Install On	Time
8) GENT-Net.	**Supplier-Server** **Partner-Server** **Service-Server**	**SSH**	**Accept**	**Long**	**Gateways**	**Any**

This rule allows administration and management to the supplier, partner and service servers using only SSH for security purposes. Any other service will be blocked.

Source	Destination	Service	Action	Track	Install On	Time
9) GENT-Net	**Xsuppiler-Server** **Xpartner-Server** **Xservice-Server**	**Any**	**Accept**	**Long**	**Gateways**	**Any**

This rule allows GENT internal users to access any service except those at the supplier, partner and service server.

Source	Destination	Service	Action	Track	Install On	Time
1) NK-FW1 **Border Router**	**Logging Server**	**syslog**	**Accept**	**Long**	**Gateways**	**Any**

This rule allows firewall and border router to forward its log information to the logging server using syslog.

Source	Destination	Service	Action	Track	Install On	Time
11) Any	**Any**	**Any**	**Drop**	**Short**	**Gateways**	**Any**

This is the default rule that drops any other traffic unless it is permitted by the above rules.

VPN Configuration

VPN is configured for tunneling from the partner, supplier systems as well as any remote workers connecting to the email server and internal system resources. Nortel Contivity 1600 series VPN is selected as the VPN switch since Contivity is the choice amongst GENT, its partner and supplier. As a result, all users will be loaded with the same client software.

Contivity switches typically have two interfaces:

Public: this interface attached to a public data network like the internet. On a public interface, the switch rejects non-tunneled protocols and accepts only tunneled protocols such as IPSec, PPTP etc. In our architecture, the switch public interface is connected directly to the FW1 and will allow only IPSec tunneled protocol.

Private: this interface is attached to the private network and that it can accept non-tunneled network protocols such as TCP/IP, FTP and HTTP. The private interface also accepts tunneled protocols that can be used for secure management access to the switch. The private interface are connected to the Supplier and Partner Server.

Configuration of the switch can be performed locally or remotely. Remote administration is secured by IPSec. The administrator of the switch will be given switch management rights to "view switch" and "manage switch" as well as user management switch in "view users" and " manage users".

Service Menu will be used to configure the security policy and allowed services in the switch. The Services screen enable the user to manage the available services, control the type of tunnel access to the switch and configure the authentication and firewall services. Following is the setting for the Services menu (√ denotes as Enable):

Allowed Services

Tunnel Type	**Public**	**Private**
IPSec	√	√
PPTP		
L2TP & L2F		
Management Protocol	**Public**	**Private**
HTTP		
SNMP		
FTP		
TELNET		
FIREWALL		

CRL Retrieval

Authentication Protocol	Public	Private
RADIUS		

Certification Modes

Mode	Status	Action
	Disabled	

For the Allowed Services, only the IPSec will be used for both the public and private interface. Switch management can only be accomplished through tunneling and no other protocols such as HTTP, SNMP will be allowed. Radius will not be used as the authentication protocol as authentication will be performed through User Name and Password/Pre-Shared Key. No certification modes will be enabled as GENT will not attempt to conform with the Federal Information Processing Standard (FIPS) 140-1 level 2.

IPSec standard defines a set of security protocols that authenticate IP connections, add data confidentiality and integrity to IP packets and are transparent to applications and the underlying network infrastructure. The IPSec Server within the contivity switch will be configured as following:

Authentication

User Name and Password/Pre-Shared Key √

RSA Digital Signature

Radius Authentication

AXENT Technology Defender
Security Dynamics SecurID
User Name and Password

Encryption

ESP – Triple DES SHA-1 √

AH- Authentication Only (HMAC-SHA-1) √

Authentication Order

Order	Server	Type	Associated Group	Action
1)	LDAP	Internal/External		

Load Balance

Load Balance	**Enable**	**Management IP Address**
Alternate Host		

Fail-Over

Fail-Over	**Enable**	**Public IP Address**
Host 1		
Host 2		
Host 3		

For the IPSec Server, authentication will be set as User Name and Password/Pre-Shared Key. GENT currently supports neither the certificate or PKI. Authentication with Radius will also not be supported. Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams by encrypting the payload data to be protected. 168-bit Triple DES SHA 1 will be enabled as the encryption method. SHA-1 is used as this is regarded by some crytographers as being more resistant to attacks than MD5 and Triple DES offers more protection than DES. Authentication Header(AH) provides data integrity and source authentication. HMAC-SHA-1 will be selected. HMAC stands for Hashed Message Authentication Code and is a technique that uses a secret key and a message digest function to create a secret message authentication code. The HMAC strengthens the SHA-1. LDAP is being selected as the authentication server. Contivity switch will always attempt to authenticate a remote user against the LDAP database. If a User ID and password are found, the switch uses the attributes that are defined for that user's group. No Associated Group will be selected as this is the group which authorization and operational settings are taken if a group attribute is not found in the authentication database. Currently, GENT will not support switch load balancing and fail-over due to limited users and monetary constraints.

Assignment 3

Audit Your Security Architecture

Audit provides feedback about the usage and the effectiveness of the established security functions. Specifically, auditing the firewall is essential to ensuring the integrity of the firewall. This review will look at the configuration of the firewall and validate that the firewall is actually implementing the GENT's security policy stated above.

Planning of the Audit

Before the audit can be conducted, a careful plan must be in place. The audit plan will include scope of the audit, risk considerations and technical approach to the audit. However, before this audit can be conducted, support from various groups within the company must be secured.

Management: Management must be aware of the importance of security. Since this review will require resources both internally and externally, management must be included and kept abreast of the planning and reporting process.

GENT IT: The IT department will be the focal point to provide support in this exercise. Two staff from the IT department will be participating in the audit so that they will get the benefits on the experience. In the future, the plan is for the IT to conduct such tests on a periodic basis.

Business Operations: The business operations must be supportive of this initiative. They must also be made aware of the potential risks and intrusion involved during this review. However, in the long run, a secure system will benefit all groups within the company.

Scope

The scope of the audit will entail validating that the firewall is actually implementing the GENT's security policy. Scanning will be performed through Nmap. Specifically, the perimeter network will be scanned from outside the border router. Ingress and egress filtering testing will also be performed to ensure that the ingress and egress filtering is being blocked as defined previously.

Tools Used

Nmap Version 2.53 will be used as the primary tool for the audit. This can be downloaded from www.insecure.org. Nmap will be downloaded and run on a Linux laptop. Cybercop will be run from inside the GENT internal network for detection of potential vulnerabilities.

Audit Considerations

Regular review is of paramount important to ensure that changes to the firewall do not open security holes. Changes can come about as a result of action by an administrator, software installation or operation, non-administration users of the system or even attacker/intruder. Since they are so many sources for changes that can affect the security of a firewall, it is recommended that subsequent regular review be conducted. This review will be used as a test and learning experience for any future reviews.

As discussed previously, GENT IT staff will participate in the audit in order to obtain the necessary exposure and training for future subsequent review.

In order to minimize intrusion, the testing and probing will be performed during week-end off business hours.

Costs

Because this is the first audit of its kind, the prudent approach is to engage a third party consultant to conduct the audit and provide training to our staff. External cost will be estimated to be $6,000($300X20hrs). In order to save on budget, the external consultant will perform the scanning and GENT's internal IT staff will follow up with the findings. There will be no hardware or software costs associated with this exercise. An existing Linux laptop will be used to run the test and Nmap will be downloaded free from www.insecure.org. Cybercop will be provided by the consultant as part of the service provided.

Perimeter Scan:

Nmap TCP –sS -P0 Ports Scanning

According to the Nmap specifications, TCP SYN scan is often referred to as "half open" scan because a full TCP connection is not opened. A SYN packet is sent as if a real connection is opened and waiting for response. A SYN/ACK indicates the port is listening and a RST represents a non-listener. If a SYN/ACK is received, a RST will immediately be sent to terminate the connection. The primary advantage of this scanning technique is that fewer sites will log it.

From the "outside" of GENT's border router, the following TCP ports and hosts will be scanned:

1. Nmap –sS –P0 –p 1-1024 192.3.8.1 (Border Router)
2. Nmap –sS –P0 –p 1-1024 192.2.3.7 (Primary Firewall)
3. Nmap –sS –P0 –p 1-1024 172.16.2.2 (External DNS)
4. Nmap –sS –P0 –p 1-1024 172.16.2.3 (Web Server)
5. Nmap –sS –P0 –p 1-1024 172.16.2.4 (eMail Server)
6. Nmap –sS –P0 –p 1-1024 172.17.2.2 (Log Server)
7. Nmap –sS –P0 –p 1-1024 172.17.2.3 (DB Server)
8. Nmap –sS –P0 –p 1-1024 172.17.2.4 (Firewall Management Server)
9. Nmap –sS –P0 –p 1-1024 172.18.2.2 (VPN Contivity Server)

The above command can be explained as –sS denotes the SYN half open for TCP ports 1 to 1024. P0 is used to prevent pinging hosts before they are being scanned. This allows the scanning of the networks/hosts that do not allow ICMO echo requests or responses through the firewall.

Nmap UDP –sU –P0 Ports Scanning

According to the Nmap specifications, UDP scan is to determine which UDP ports are open on a host. The technique is to send 0 byte udp packets to each port on the target machine. If an ICMP port unreachable message is received, then the port is closed. Otherwise it is assumed to be open.

The following UDP ports scanning will be performed:

1. Nmap –sU –P0 –p 1-1024 192.3.8.1 (Border Router)
2. Nmap –sU –P0 –p 1-1024 192.2.3.7 (Primary Firewall)
3. Nmap –sU –P0 –p 1-1024 172.16.2.2 (External DNS)
4. Nmap –sU –P0 –p 1-1024 172.16.2.3 (Web Server)
5. Nmap –sU –P0 –p 1-1024 172.16.2.4 (eMail Server)
6. Nmap –sU –P0 –p 1-1024 172.17.2.2 (Log Server)
7. Nmap –sU –P0 –p 1-1024 172.17.2.3 (DB Server)
8. Nmap –sU –P0 –p 1-1024 172.17.2.4 (Firewall Management Server)
9. Nmap –sU –P0 –p 1-1024 172.18.2.2 (VPN Contivity Server)

The above command can be explained as –sU to determine which UDP ports 1 to 1024 are opened on a host. P0 is used to prevent pinging hosts before they are being scanned. This allows the scanning of the networks/hosts that do not allow ICMO echo requests or responses through the firewall.

Nmap Scanning Results:

1. All 1024 scanned ports on (192.3.8.1) are: Closed

This result shows that both TCP and UDP scans found no port appeared to be opened on the border router.

2. All 1024 scanned ports on (192.2.3.7) are: Filtered

This results shows that both TCP and UDP scans found no port appeared to be opened on the firewall. As seen, the state of the firewall is listed as "Filtered". Filtered means that a firewall, filter, or other network obstacle is covering the port and preventing Nmap from determining whether the port is open.

The above results show that the firewall functions properly.

3. *All 1024 scanned ports on (172.16.2.2) are: Filtered*

   Interesting ports on (172.16.2.2):
   (The 1023 ports scanned but not shown below are in state: filtered)
   Port State Service
   53/udp open domain

This results shows that the TCP scan found no port appeared to be open on the external DNS server. As seen, the state listed as "Filtered". Filtered means that a firewall, filter, or other network obstacle is covering the port and preventing Nmap from determining whether the port is open. The TCP ports are blocked by the firewall.

This results also shows that UDP ports 53 is open which is expected.

The above results show that the firewall functions properly.

4. *Interesting ports on (172.16.2.3):*

   The 1022 ports scanned but not shown below are in state: filtered

   Port State Service

   80/tcp open http

   443/tcp open https

   All 1024 scanned ports on (172.16.2.2) are: filtered

This results shows that TCP scan found http port 80 and https port 443 are open which is an expected result.

The UDP scan shows that all UDP ports are blocked by the firewall.

The above results show that the firewall functions properly.

5. *Interesting ports on (172.16.2.4):*

   The 1023 ports scanned but not shown below are in state: filtered

   Port State Service

   25/tcp open smtp

   All 1024 scanned ports on (172.16.2.4) are filtered

This results shows that TCP scan found that port 25 is open which is an expected result.

The UDP scan shows that all UDP ports are blocked by the firewall.

The above results show that the firewall functions properly.

6. *All 1024 scanned ports on (172.17.2.2) are: filtered*

   All 1024 scanned ports on (172.17.2.2) are: filtered

This result shows that both TCP and UDP scans found no port appeared to be open on the logging server. This shows that all TCP and UDP ports are blocked by the firewall.

The above results show that the firewall functions properly.

7. *All 1024 scanned ports on (172.17.2.3) are: filtered*

   All 1024 scanned ports on (172.17.2.3) are: filtered

This result shows that both TCP and UDP scans found no port appeared to be open on the DB server. This shows that all TCP and UDP ports are blocked by the firewall.

The above results show that the firewall functions properly.

8. *All 1024 scanned ports on (172.17.2.4) are: filtered*

   All 1024 scanned ports on (172.17.2.4) are: filtered

This result shows that both TCP and UDP scans found no port appeared to be open on the firewall server. This shows that all TCP and UDP ports are blocked by the firewall.

The above results show that the firewall functions properly.

9. *All 1024 scanned ports on (172.18.2.2) are: filtered*

Interesting ports on (172.18.2.2):

(The 1023 ports scanned but not shown below are in state: filtered)

Port	*State*	*Service*
500/udp	*open*	*isamp*

This result shows that all TCP ports on the VPN switch server appeared to be closed. The UDP scan indicates that ISAMP port 500 is open to the VPN switch which is an expected result.

The above results show that the firewall functions properly.

Ingress and Egress Filtering Testing

Ingress and Egress Filtering testing is performed to ensure that they are being blocked as defined. All the non-routable address and GENT network address will be tested. This is to ensure that no packets can get through the border router. The following commands will be used:

Nmap –sS –P0 –v –p80 –oN ingress.out –S [source_IP_address] –I eth0 [dest_IP_address]

Nmap –sS –P0 –v –p80 –oN egress.out –S [source_IP_address] –I eth0 [dest_IP_address]

As discussed earlier, sS is the TCP SYN scan and often referred to as "half-open" scanning. P0 is used to prevent pinging hosts before they are being scanned. This allows the scanning of the networks/hosts that do not allow ICMO echo requests or responses through the firewall. –v is the Verbose mode. This will give more information about what is going on. –p80 is the port that is going to be scanned. –oN ingress.out. This will log the results of this scan in a normal human readable form into the ingress and egress out files. –S is the source, non-routable and internal network addresses ip address. I eth0 is the interface. Finally the dest_IP-address is the destination IP address to be scanned.

The results we have for both of the above scans showed that "Attempt was denied". We can conclude that the filtering is functioning properly.

Cybercop Scan

Following is the scan results pertained to the firewall. The scan was configured and executed from inside the GENT internal network.

CyberCop Scanner Results

Report Sorted By Risk Factor

13006 ***Firewall-1 S/Key Authentication*** **12/26/2001 1:34:46PM**
Vulnerability

Risk Factor: High
Complexity: Low
Popularity: Widespread
Impact: System Integrity
Root Cause: Software Implementation Problems
Ease of Fix: Simple
Description: In some versions of FireWall-1, the implementation of S/Key authentication uses a poor source of entropy in regeneration of chains, and is therefore susceptible to a simple brute force attack.
NOTE: You must configure the FW1 Management IP and FW1 Management Module Port settings in CyberCop Scanner's Module Options screen in order for this module to return valid results.
Security Concerns: Weak or easily bypassed authentication mechanisms could provide attackers with a simple avenue of approach to penetrate your network and mount further attacks against internal systems.
Suggestion: Checkpoint has produced a patch to address this issue. If your firewall is found to be vulnerable to this check, you should upgrade to the latest version immediately.
CC_FW1_MANAGEMENT_IP: Management IP not specified.

13007 ***Firewall-1 FWN1 Authentication*** **12/26/2001 1:34:46PM**
Vulnerability

Risk Factor: High
Complexity: Low
Popularity: Widespread

Impact:	System Integrity
Root Cause:	Software Implementation Problems
Ease of Fix:	Simple
Description:	In some versions of FireWall-1, the implementation of FWN1 authentication is susceptible to a trivial replay attack, rendering it ineffective. NOTE: You must configure the FW1 Management IP and FW1 Management Module Port settings in CyberCop Scanner's Module Options screen in order for this module to return valid results.
Security Concerns:	Weak or easily bypassed authentication mechanisms could provide attackers with a simple avenue of approach to penetrate your network and mount further attacks against internal systems.
Suggestion:	Checkpoint has produced a patch to address this issue. If your firewall is found to be vulnerable to this check, you should upgrade to the latest version immediately.

CC_FW1_MANAGEMENT_IP: Management IP not specified.

Two related vulnerabilities were found as a result of the Cybercop scan. As stated in the scan report, weak or easily bypassed authentication mechanisms could provide attackers with a simple avenue of approach to penetrate your network and mount further attacks against internal systems.

Recommendation

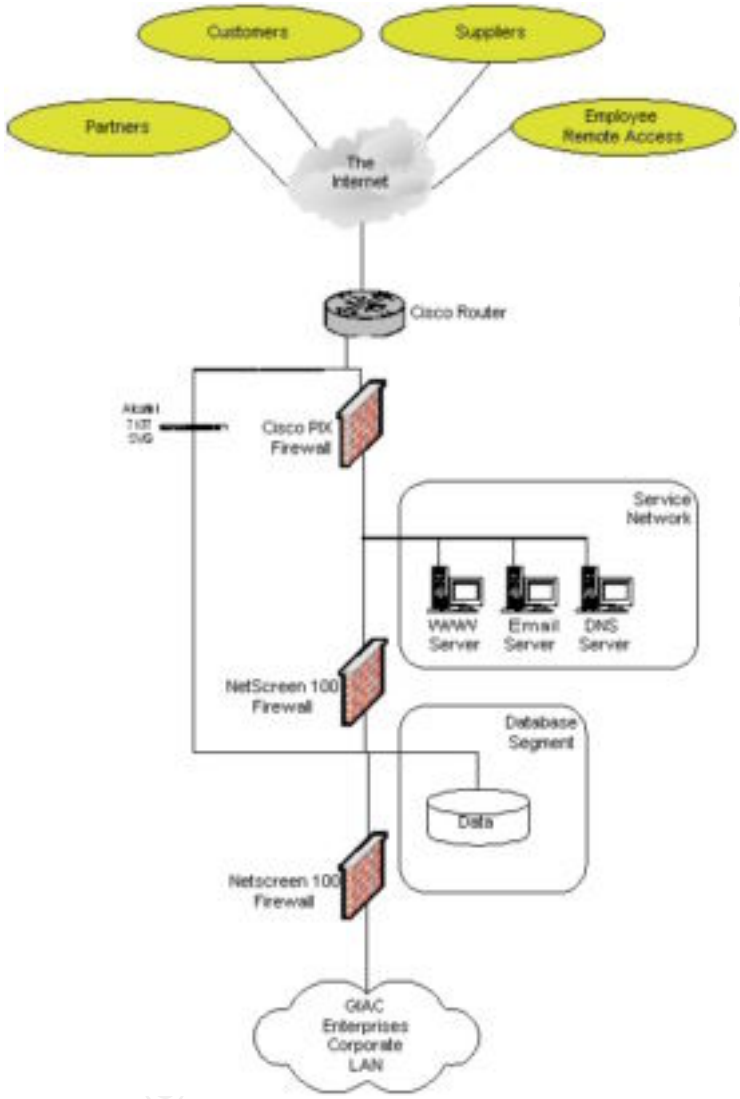
- Overall Nmap scanning did not indicate anything that is out of ordinary. The results from the above exercise indicates that the network and firewall are run in accordance to GENT security policy. All the results were expected.
- Nmap scanning should be conducted on a monthly basis by GENT IT network staff to allow system and network administrators to scan the network to see what hosts are up and what services they are offering. Corrective action should be taken immediately should exceptions are found.
- As for the Cybercop scan, it was noted that Checkpoint has produced a patch to address this issue. GENT IT network staff should upgrade to the latest version immediately.
- Because this audit is of limited scope, a more comprehensive review on the e-Business infrastructure should be conducted in the near future. Specifically, a detailed host based vulnerability assessment and general controls review should also be included in any future audit. The general controls review entails reviewing of the current policies, procedures and standards for the following:
    - Physical Security and Environmental Controls

- Change Management Process
- Disaster Recovery Planning
- Security Awareness and Training
- Backup and Recovery
- Security Administration
- Auditing, Logging, Monitoring, and Capacity Planning

Assignment 4

Design Under Fire

For the purpose of this assignment, I have selected the design by Brian Rickle (www.sans.org/y2k/practical/brian_rickle_gcfw.zip) for analysis and possible attack. Attached is Brian's security architecture design for his company.



In Brian's design, the perimeter protection was provided by a Cisco router. Brian is running Cisco PIX as the main firewall. The PIX firewall will be our target of attempt attacks. The main source of our research of vulnerabilities was concentrated on Securityfocus (www.securityfocus.com) Bugtraq and Security Tracker (www.securitytracker.com). Hacking Exposed 2nd edition was used for researching attacks on firewall and technical incursion countermeasures. For the purpose of this assignment, two of the three types of attacks as stated in the assignment requirement will

be researched and designed. They are a) An attack against the firewall itself; b) A denial of service attack.

A) Research and Describe Three Vulnerabilities For PIX

1) **Name of Vulnerability**:

PIX Firewall Manager (PFM) Vulnerability

Release Date:

October 10, 2001

Description of Vulnerability:

The PIX Firewall Manager is a software product that allows the configuration of Cisco PIX Firewall devices via a web-based GUI. PFM is installed and run on a standard Windows NT workstation or server that serves as the management station. There is a flaw in PFM that upon successful connection to a PIX device, the enable password is saved in plaintext on the management station. The password is recorded in an unencrypted log file stored in a directory created by the install, which by default has no access restrictions. If the management station is compromised, the attacker can retrieve the enable password. This can be then be used to grant full access to the PIX Firewall.

As stated above, for the malicious attacker to exploit this vulnerability, the attacker would have to have access to the local Windows NT workstation or server. It should be noted that most security breaches originated from internally. Internal breaches or weaknesses can include poor physical security, deliberate sabotage, carelessness, not applying patches on a timely basis or poor technical incompetence. Because in Brian's example, GIAC enterprise is still a start-up, it is conceivable and not unrealistic that someone within GIAC enterprise, who has the malicious intent could get to the firewall management workstation physically. Once physical access is obtained, the next steps would be to obtain a valid username/administrator and start password guessing. Hacking Exposed published a list of common user/password pairs which they call "high probability combinations". Some of them are listed to be: User Name: administrator, Password: Null, password or administrator, User Name: Username, Company_Name. (In the past, I have personally gained access to a NT production server by typing in Administrator as User Name and Password) Alternatively, performing automated password guessing is relatively simple with some publicly available tools such as Legion. Legion can be found in ftp://ftp.technotronic.com/rhino9-products/legion.zip

To sum up, once physical access is gained to the firewall management workstation, it is relatively simple to recover the password and gain access to the PIX firewall.

Attacking This Vulnerability

Following is the exploit:

1) Install PFM as instructed.
2) Run PFM, and connect to the PIX firewall with the correct IP and enable password.
3) Wait for PFM to finish gathering data from the firewall.
4) A PFM.LOG file is created, by default in C:\Program Files\Cisco\PIX Firewall Manager\protect.
5) The enable password is stored in plaintext in an entry that looks like:
Aug 01 2001 14:59:18 <Receiving msg> - 9004 192.168.1.100 0 0 0 1 5 **enable_pswd_here**

To mitigate this risk, Cisco has recommended that PFM should be replaced by the PIX Device Manager. However, if PFM has to be used, access rights for the directory in which PFM.LOG resides must be restricted. As well, after connecting to a PIX firewall using PFM, attempt should be made to edit the PFM.LOG, search for the PIX enable password and manually delete it.

1) **Name of Vulnerability**

PIX Firewall SMTP Vulnerability

Release Date

September 26, 2001

Description of Vulnerability

The behaviour is a failure of the command fixup protocol smtp [portnum], which is enabled by default on the Cisco Secure PIX Firewall. The impact and description of this defect is similar to a defect outlined in a previous security advisory, http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml, however, this instance of mail filtering bypass was re-introduced by the defect CSCds90792.

To exploit this vulnerability, attackers must be able to make connections to an SMTP mail server protected by the PIX Firewall. If the Cisco Secure PIX Firewall has configuration lines similar to the following:

fixup protocol smtp 25
and either
conduit permit tcp host 192.168.0.1 eq 25 any
or
conduit permit tcp 192.168.0.1 255.255.255.0 eq 25 any
or
access-list 100 permit tcp any host 192.168.0.1 eq 25
access-group 100 in interface outside

The expected filtering of the Mailguard feature can be circumvented by an attacker.

2) **Name of Vulnerability**

PIX Firewall Authentication Denial of Service Vulnerability

Release Date

October 3, 2001

Description of Vulnerability

When AAA authentication services are configured on the Cisco Secure PIX Firewall, it is possible for a single source address to consume all of the authentication resources, preventing other legitimate users from authenticating. This is a denial of service strictly for the authentication resources; other established traffic continues unaffected, and only new authentication requests are prevented.

Denial of Service (DOS) Attack

This vulnerability will be exploited in order to launch a DOS attack. For this vulnerability, an attacker from inside or outside interfaces of a PIX Firewall 515 or 520, 5.1.4 version running AAA authentication against a TACACS+ Server could cause the PIX to crash and reload by overwhelming it with authentication requests. As it is unclear whether Brian is running TACACS+ Server for authentication, this attack may or may not be successful. For the purpose of this demonstration, it is assumed that TACACS+ is running. Following is the detail of how the attack can be launched:

From an inside host generate http request with sweep source port directed to a global address on port 80.
In this case I would generate a http request from port 2000, the PIX starts an authentication process: 109001: Auth start for user '???' from 10.10.10.1/2000 to 216.46.233.11/80 after that I then generate a http request from port 2001, 109001: Auth start for user '???' from 10.10.10.1/2001 to 216.46.233.11/80 and so on. After

426 requests (this number is not always the same) generated in 3 seconds the PIX give the message: Panic: uauth1 - open: no more channels (tcp/UNPROXY/1/0)! and crashed in: Thread Name: uauth1 (Old pc 0x80070b4f ebp 0x810c56dc) and reloads.

To mitigate this risk, a maximum limit of three open authentication requests per user should only be allowed by the administrator.

B) Distributed Denial of Service Attack

The type of Distributed Denial of Service Attack we will attempt on Brian's network will be Tribe Flood Attack (TFA). TFN is made up of client and daemon programs, which implement a distributed network denial of service tool capable of waging ICMP flood, SYN flood, UDP flood, and Smurf style attacks, as well as providing an "on demand" root shell bound to a TCP port. The TFN network is made up of a tribe client program ("tribe.c") and the tribe daemon ("td.c"). The malicious attacker(s) control one or more clients, each of which can control many daemons. The daemons are all instructed to co-ordinate a packet based attack against one or more victim systems by the client. This type of attack can be found in more details in CERT (http://www.cert.org/incident_notes/IN-99-04.html)

The requirement of this assignment stated that a maximum of 50 compromised hosts could be used to launch the attack. The hosts are usually Linux and SUN computers. For the purpose of this attack, 2 compromised hosts will be designated as the "clients" and each of the client will control 20 other daemons. Communication from the TFN client to daemons is accomplished via ICMP_ECHO REPLY packets. There is no TCP or UDP based communication between the client and daemons at all. This attack will be launched at Brian's Cisco border router

Because the programs use ICMP_ECHO REPLY packets for communication, it will be very difficult (if not impossible) to block it without breaking most Internet programs that rely on ICMP. According to the Phrack's research paper on Loki (http://www.phrack.org/show.php?p=49&a=6), ***"the only sure way to destroy this channel is to deny ALL ICMP_ECHO traffic into your network."*** If this traffic is not rejected, it will be necessary to observe the difference between normal use of ICMP_ECHO and ICMP_ECHO REPLY packets by programs like "ping". This will be difficult to implement, especially on large networks. According to Cisco's paper on DDOS (http://www.cisco.com/warp/public/707/newsflash.html#overview), it offers the following preventive measures:

Use CAR to rate limit ICMP packets.

Refer to the following example:

interface xy
rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop

access-list 2020 permit icmp any any echo-reply

Upon reviewing Brian's router configuration file, his Cisco 4500 router will perform the basic screening out ICMP packets. However, no specific ACL was incorporated in the policy to address the handling of ICMP packets. As a result, his perimeter defence may be susceptible to a DDOS attack.