



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.

GIAC Enterprises Perimeter Security Policy

**GCFW
Practical Assignment
Version 2.0
Vicki Barnett
April 2004**

© SANS Institute 2004. All rights reserved. Author retains full rights.

TABLE OF CONTENTS

Abstract	
1.0 Security Architecture	3
1.1 Introduction	3
1.2 Business Operations	3
1.3 Access Methods	5
1.4 Defense in Depth.....	7
1.4.1 Routers.....	8
1.4.2 Firewalls	9
1.4.3 Network Address Translation (NAT)	10
1.4.4 Service Network (DMZ)	10
1.4.5 Intrusion Detection Systems (IDS)	10
1.4.6 Virtual Private Network.....	11
1.4.7 Servers.....	12
1.4.8 Hardening of OS Servers	12
1.4.9 Checkpoint Management Server	12
1.4.10 Token Authentication Server	13
1.4.11 DNS Server	13
1.4.12 Logging Server	13
1.4.13 Tripwire Manager	14
1.4.14 E-mail Server.....	14
1.4.15 Database Server	15
1.4.16 Web Server	15
1.4.17 Workstations.....	15
1.4.18 Antivirus/Personal Firewall	15
1.4.19 Backup Policy	15
1.4.20 Security Maintenance.....	16
1.4.21 Internet Service Provider.....	16
1.4.22 Network Encryption	16
1.5 Addressing Scheme	17
1.6 Topology	18
1.7 Security Awareness.....	19
2.0 Security Policy & Tutorial	20
2.1 Router	20
2.2 Firewall.....	32
2.3 Virtual Private Network (VPN)	41
3.0 Verify the Firewall Policy	42
4.0 Designs Under Fire	47
4.1 Attack against the Firewall	48
4.2 Distributed Denial of Service (DDOS)	49
4.3 Attack Plan	50
5.0 References.....	52
6.0 Appendix	55

ABSTRACT

The purpose of this paper is to provide GIAC Enterprises, an online company that sells fortune cookie sayings, a layered security design, coinciding with the expansion of their business into a 24/7 e-commerce environment with remote access.

There will be four parts for this assignment:

- 1) Security Architecture- defining business operations, access requirements, diagram of the GIAC Enterprises network and location of components, components use for the Defense-In-Depth principle
- 2) Security Policy and Tutorial-security policy for a border router, firewall, VPN and a tutorial for one the devices listed.
- 3) Verify the Firewall Policy-technical evaluation of the primary firewall with explanation of the output.
- 4) Design under Fire- evaluate a GCFW practical that has been posted within the last 6 months and examine vulnerabilities and list ways to mitigate these vulnerabilities.

The paper will outline a “defense-in-depth” approach to network security. The initial “defense-in-depth” architecture for GIAC Enterprises will include a router, firewall, VPN’s, access control, IP addressing schemes and the appropriate configuration files for the router and firewall.

To support the “defense-in-depth” approach there will be mention of the following network concerns:

- Backup policy/strategy
- Antivirus/personal firewall
- Intrusion Detection System
- Hardening of the OS
- Security Maintenance

Also, discussed will be the importance of security awareness for the users. The network security policy will only be as strong as the weakest link, and we are going to avoid the common mistake of the user being that weakest link. Security Awareness is outside the scope of the Perimeter Security Project that we are currently involved in with GIAC Enterprises; however, there will be a Phase II of this project that will include a complete security awareness program.

1. Security Architecture

1.1 Introduction

GIAC Enterprises has requested that my company design and implement a security architecture that will protect their company from potential loss. GIAC Enterprises is a company that buys and sells fortune cookie sayings. They are a global company and therefore have communications around the world.

We will first conduct a thorough needs analysis with GIAC Enterprises. The goal will be to determine their assets and then identify potential vulnerabilities concerning their assets and list possible threats. Finally we will identify ways of mitigating the threats and vulnerabilities with a layered defense approach. The layered defense approach will include both hardware and software solutions. Defense in Depth will be also discussed. The architecture will include access controls for the following individuals:

- 1) Customers- They will be purchasing the fortune cookie sayings.
- 2) Suppliers- They will be providing GIAC Enterprises with cookie sayings.
- 3) Partners- They will be international and assists GIAC Enterprises with the translation of the fortune cookie sayings.
- 4) GIAC Enterprises local employees- They are the employees who work in the local office.
- 5) Mobile Sales force- They will be connecting from various locations globally.
- 6) General Public- The general public will need access to the web server.

During the analysis phase of this project it was determined that there were two critical areas that needed to be addressed. First, of course, was security of the fortune cookie database. This will be discussed in detail in a later section of this practicum. Normally a company's most important asset is their information and this is true of GIAC Enterprises. Second is the access method and controls for the customers.

1.2 BUSINESS OPERATIONS

Access Requirements

Our policy for access requirements is to implicitly deny access and then permit only the traffic that we wish to enter our network. We have explained to GIAC Enterprises that at the beginning this will be a dynamic process meaning that as we work through the access controls, there will be areas that we need to allow access that are implicitly denied and make change accordingly.

Customers

Customers are defined as clients that will be purchasing fortune cookie sayings from GIAC Enterprises. This will be an on online transaction and therefore will require a secure method for authentication and access using SSL (https:443). The customer access must be simple and user friendly while establishing trust that the site they are transacting with is secure. This is critical. If a customer becomes confused or the site is difficult to navigate, the customer could become discouraged and attempt to find another fortune cookie vendor.

Partners

Partners are defined as international companies that GIAC Enterprises supplies with the “English” fortune cookie sayings and they translate into the appropriate foreign language. They will access the English version through SSL (https:443) to the fortune cookie server that will be placed in the Service Network (DMZ) of the network architecture. They will also be supplied by GIAC Enterprises a secure user ID and password of their choice for authentication. (Note: the password must meet the password policy outline by GIAC Enterprises in the password security policy which is outside the scope of this practicum.)

Suppliers

Suppliers are the creators of the fortune cookie sayings who sell their “product” to GIAC Enterprises. They will need access to the web server that will be located on the Service Network #1 (DMZ). Access to the web server will be authenticated with a user account and password via a SSL connection (https:443).

Mobile Sales Force

The mobile sales force will need access to files on the internal network as they travel. Since they need access to internal files they have different access needs and different controls need to be in place compared to other remote users who just need access to files/information that is placed in the DMZ. They will be using the Virtual Private Network (VPN) solution for access. Virtual Private Networks will be discussed in further detail in a later section.

Local Employees

The local employees will have local access to devices/files/applications according to the security policy for each area. They will access the Internet through HTTP (80) and HTTPS (443). They will have email access via the email server. Email access will be discussed later in this section.

General Public

The general public will be connecting to the GIAC Enterprises web site for general information concerning the company. The web site will contain a brief history, associated links, contact information and information about the nature of their business- selling fortune cookie sayings. They access the web server located on Service Network #1 through http (80). (Note: “Contact” information on

the GIAC Enterprises web site will be carefully planned as this can sometimes be a source of information for people who are on a reconnaissance mission against the company.)

1.3 Access Methods

A. SSL – Secure Socket Layer¹

Since SSL is going to be implemented in the security design of GIAC Enterprises, it is necessary to explain SSL, why it has been selected as a secure access method, and how it works. SSL is used to provide encryption for the exchange of information.²

There are 3 fundamental aspects to SSL:

1. SSL server- The server authenticates the user who is trying access the information that is being protected. Also, companies that use SSL generally have been issued a Certificate from a validating company, like Verisign, proving that they are a trustworthy company.
2. SSL client- The client validates with the SSL server. The client software can check with the validating company before conducting a transaction with that company.
3. Encryption- When transmitting sensitive information everyone wants the peace of mind that the information is being protected. One of the ways that SSL provides that is through encryption. This provides for confidentiality that only the parties involved can interpret the information that is being transmitted.

B. HTTP- HyperText Transfer Protocol-

HTTP is the protocol used to exchange information over the Internet. It is called a transfer protocol because it transfers pages that you requested in your URL to your browser for you to view.

C. DNS-Domain Name System

DNS is the service that translates domain names into IP addresses. This is a wonderful service that saves us from having to remember all the IP addresses that we would ever want to access on the Internet. DNS allows the user to type in www.microsoft.com instead of the 32-bit IP address.

(RFC 1035 and RFC 1034)

D. SMTP - Simple Mail Transfer Protocol

SMTP is the protocol for sending mail between mail servers. Then, the mail clients (POP, IMAP) can retrieve the email messages from these servers. (port 25)

Access Group	Access Needed	Protocol / Port
Customer	Web, SSL, E-mail	HTTP:80 HTTPS:443 SMTP: 25 DNS:53
Supplier	Web, SSL, E-Mail	HTTP:80 HTTPS:443 SMTP: 25 DNS:53
Partners	Web, SSL, E-Mail	HTTP:80 HTTPS:443 SMTP: 25 DNS:53
Mobile Sales Force	Web, SSL, E-Mail VPN-IPSec	HTTP:80 HTTPS:443 SMTP: 25 DNS:53 IKE:- UDP/500
General Public	Web	HTTP:80 DNS:53
Local employees	Web, SSL, E-Mail, DNS	HTTP:80 HTTPS:443 SMTP: 25 DNS:53 POP3:110

1.4 Defense in Depth

Introduction

When I think of Defense in Depth I think of a football team. Depth on a football team means there is always someone behind the starter to come in and help out when needed. That substitute player could come into the game for special circumstances or special needs. In addition, sometimes depth on a football team could be a different zone that a particular player plays. You have the lineman, then the linebackers and finally the safeties. The safeties are there to catch anyone who gets through the first two zones.

Defense in Depth for a network is basically the same thing. You don't have one player (device) for a position; there are multiple devices or zones that play together as a team.

(GIAC Enterprises is going to implement their Defense in Depth in 2-3 phases. The first phase will include the components that will be discussed in this practicum and future considerations/phases will be listed when appropriate.)

Next will be an explanation of those devices and zones.

1.4.1 Routers³

Routers work at Layer 3 of the OSI model and route packets based on their IP address. They also maintain an IP routing table that improves the efficiency of the router. The router remembers the port to direct the traffic to the correct interface. This information is held in a route table. Routers are also used to filter traffic in and out of the network. This is called ingress and egress filtering. Ingress is filtering traffic inbound and egress is filtering traffic outbound. Filtering is accomplished through proper configuration which will be outlined in Section 2 during the router tutorial.

Routers can be used as a border router or an internal router:

1. Border Router

A. Purpose: The Border Router is the first and last line of defense in our Defense in Depth infrastructure. It is also the router that will connect GIAC Enterprises to the Internet. The Border Router will perform packet filtering based on IP address and also filter malformed packets. Since the Border Router will examine ALL traffic in and out of the GIAC Enterprises network, it will perform static packet filtering which is much quicker than a stateful inspection. Stateful inspection is critical but will be handled in a different layer after some of the traffic has been filtered. This way the stateful device will not have to examine every packet which could slow network performance. Also the router will only be configured locally.

B. EQUIPMENT^{4 5}

I have chosen to use the Cisco 1760 Modular Access Router using IOS 12.2 based on research and the “needs analysis” of GIAC Enterprises.

2. Internal Router- An internal router will not be utilized at this time. It will be added to the “future considerations” list. Internal routers can be placed strategically to defend against unwanted traffic.

A. Purpose-. It provides another layer of defense behind the primary firewall. It will strictly limit the access to and from the internal network.

- B. Equipment-The Cisco 1760 Modular Access Router would be recommended for the same reasons as mentioned above.

1.4.2 Firewalls ⁶

A firewall is a network appliance that inspects traffic as it passes through the appliance. The firewall will have a set of rules' very similar to the router; deciding what can be passed through and what should be blocked. There are many different types of firewalls including packet filters, proxies, and stateful inspection engines. Deciding which type of firewall to use should be dependent on the "needs analysis" that is conducted at the beginning of every project. A stateful packet inspection firewall has been determined as the best product for the GIAC Enterprises environment. Stateful inspection works at the Network Layer of the OSI model and looks at the "state" of the packet. As mentioned, routers work at layer 3 and make decisions based on the source/destination address. Stateful inspection does this as well as looking at the data portion of the packet. It also monitors the "state" of the connection and puts this information into a state table.

Primary firewall

A. Purpose: In our design, the primary firewall is the second line of defense behind the Border Router. The purpose of this device is to take a more comprehensive look at each packet as it passes. The Primary Firewall will also be performing as the DHCP server. All hosts on the Service Networks and the Intranet will be using NATed addresses. The addressing scheme is addressed in a later section.

The management console for all the firewalls will be located on the internal trusted zone of GIAC Enterprises and will be well protected behind an internal firewall accompanied by a Snort IDS. It will also be running Tripwire Manager for Servers for additional security

B. Equipment: Check Point VPN-1/Firewall-1 NG FP3 Hotfix-2 has been chosen because it performs stateful inspection with enterprise-wide security that can be managed centrally. FW-NG offers a single management console for multiple firewalls. Checkpoint Firewall-1/VPN-1 -NG will be installed on a box running Windows Server 2000. The Server 2000 will be hardened according to industry standards and will be maintained with the appropriate patches and updates.

Internal firewalls

A. Purpose: The internal firewall also adds another layer of defense and can help with network utilization. It can act as a router by keeping internal traffic internal. However, it can also keep external traffic out of the internal zone. Again, right now, GIAC Enterprises has decided to add this to the future considerations.

B. Equipment: Check Point VPN-1/Firewall-1 NG FP3 Hotfix-2

1.4.3 Network Address Translation (NAT)

As mentioned before, the primary firewall (Checkpoint VPN-1/FW1-NG) will also be the NAT server. NAT addresses will be used behind the primary firewall so that the IP addresses of the hosts will be hidden. NAT addresses will be assigned following RFC 1918.⁷ NAT translates non-routable (RFC 1918) IP addresses from the public domain into private addresses on the Internal network and Service Networks. It also assists in security by hiding the IP addresses of hosts on GIAC Enterprises. NAT can also assign static IP addresses for hosts that require static IP addresses. For example, servers and printers require a static IP address.

1.4.4 Service Network (DMZ)

The service network is a subnet that will be used to allow users to public servers, but deny that traffic to the internal network. It typically sits between the untrusted and trusted segments of the network. GIAC Enterprises will be utilizing two service networks.

Service Network #1

Web Server – GEWEB1

DNS Server- GEDNS1

Mail Relay Server- GEMail1

(There will also be a Snort IDS sensor on this segment)

Service Network #2

Saying Database Server- GEDB2

(There will also be a Snort IDS sensor on this segment)

1.4.5 Intrusion Detection Systems (IDS)

I compare an IDS system to a house alarm system. It can tell you when someone has gotten into the house, but doesn't stop them. It can also alert the police. A network IDS tells the network security administrators when there is unwanted traffic and then can alert them via pager, email, message, etc. There are network-based IDS systems that analyze traffic that is being traversed across

the media. In addition there are host-based IDS that analyze packets that are actually being processed by the host.

Intrusion Detection Systems can function in two different modes. The misuse model uses a rule base set. As traffic passes the IDS, it checks to see if the packet matches a rule or a signature set that triggers an alarm for “unwanted” traffic. Anomaly models use what has been identified as “normal” behavior/traffic. This model builds a “normal” traffic pattern over time and when something “unusual” happens then it triggers an alarm.

Snort sensors have been placed in strategic places throughout GIAC Enterprises. They have been noted in the architecture diagram. They will log to a syslog server for management purposes.

Network IDS

A. Purpose: Placement of the Network IDS is usually defined by security policy. This adds another layer of defense. At GIAC Enterprises several NIDS will be placed and outlined on the infrastructure diagram

B. Equipment: Snort⁸-

Snort is one the leaders of the industry for NIDS. It is open source, and performs real time analysis, and can be implemented with a number of Operating Systems. It can also be used for packet analysis and also has a mechanism for alerting security managers when a possible attack is taking place. It is a rule-based NIDS that installs with preconfigured rules that can easily be structured to your security policy. Also, many security personnel write their own rules and add them to the rule base.

1.4.6 Virtual Private Network (VPN)

A. Purpose: VPN sets up a secure tunnel for remote users to connect to GIAC Enterprises. It does this by encrypting data being exchanged between user/server. The type of encryption used is determined by the community membership and the topology. It is connected to the main firewall so that it is protected by the firewall.

B. Equipment - Check Point VPN-1/Firewall-1 (Build 53945_1)

Access Control for Checkpoint Firewall and VPN- some of the Access and Ports have been taken from Phoneboy at

<http://www.phoneboy.com/bin/view.pl/FAQs/PortsUsedByFireWall1NG>

Internet Key Exchange (IKE)	UDP/500
Encapsulating Security Payload (ESP)	IP/50
FW-1 Secure Client Verification	UDP/18233
Authentication Header (AH)	IP/51 – if used

Remote firewall module to send logs to a management console.	TCP/257
Client Authentication	TCP/259
Secure Client	TCP/264
HTTP Client Authentication	TCP/900
Encapsulation Mode	UDP/2746
Policy Editor/Smart Dashboard	TCP/18190

1.4.7 SERVERS

Dell PowerEdge⁹ servers with 4GB of RAM with Intel® Xeon™ processors 100 gig hard drive space.

1.4.8 Hardening of OS systems ^{10 11}

The servers will be installed on Windows 2000 (unless otherwise noted) with the latest upgrades and patches applied on a regular basis. It has been found to establish a schedule and assign personnel to perform this function. Also, strong passwords are recommended and should be identified in a separate password policy. Also, services should be turned off if they are not needed. Both internal and external vendors to help locate vulnerabilities should perform regular audit. Then diligence should be used to mitigate these vulnerabilities. It is a “best practice” to be proactive instead of reactive when it comes to vulnerabilities on your boxes.

1.4.9 Checkpoint Management Server

The Checkpoint Firewall-1/VPN-1 will be managed from this console server including all changes and configurations. This server will be solely used as a management console. No other services or applications should be installed. The log file will also be monitored from this server.

Policies can be installed from the Management Server and then it can be used to monitor network security using the SmartView Tracker.

In addition, SecurID will also be incorporated on the management server for verification of uses/uses. This will help to protect unauthorized access to the firewall.¹²

Checkpoint	CPD	Check Point Daemon Protocol - Download of rulebase from MM to FWM - Fetching rulebase, from FWM to MM when starting FWM - Download of rulebase from MDS/CMA to FWM - Fetching rulebase, from FWM to CMA when starting FWM	18191 /tcp
Checkpoint	CPD_amon	Check Point Internal Application Monitoring - Protocol for getting System Status, from MM or MDS/CMA to FWM	18192 /tcp

1.4.10 Token Authentication Server:

RSA ACE/Server 5.2^{13 14} will be used as our authentication server for VPN access. SecurID is a product from RSA Security, which is a proven global leader in the field of security and especially authentication and access control. SecurID uses a two-factor authentication: something you know and something you have. SecurID has also been chosen because of the flexibility it provides for all types of connections: wireless, PDA's, wireless phone, etc. In addition, Ace Server 5.2 offers more flexibility and lower administrative costs. It also has enhanced reporting allowing for more flexibility on the log files. Also, Ace Server has improved directory synchronization to allow for more information on group and user status.

SecureID	124
----------	-----

1.4.11 DNS Server^{15 16}

GIAC Enterprises will be using the split DNS technology. There will be two DNS servers. One will be located on the internal zone. This server will resolve all names within the local domain. The other DNS server will be placed in the Service Network #1. The purpose is to separate the general public from accessing the local domain for name resolution.

DNS- LDAP	TCP/UDP 389
DNS- Resolution	UDP/53

1.4.12 Logging Server

Purpose: The logging server is used as a collection point for the security logs. The logs could be pointed to a logging server. Kiwi Syslog Daemon is a freeware Syslog Daemon for Windows. It receives, logs, displays and forwards Syslog

messages from hosts such as routers, switches, and any other syslog enabled device. This server should be dedicated to just collecting log files. No other services or applications should be installed or utilized.

Software: Kiwi Syslog Enterprises 7.1.0

Kiwi Syslog	UDP/514
-------------	---------

1.4.13 Host Based Security- Tripwire Manager

Tripwire Manager/Server

Tripwire Manager 4.0

Tripwire Manager will manage all the Tripwire servers. It will also be used to distribute and display the status the policies created for Tripwire for Servers. Plus, it will tell us who made these changes and whether they were internal or external. It can also provide reports for IS team to analyze. Also, it is can be used with multiple platforms.

<http://www.tripwire.com/products/servers/index.cfm>

Tripwire Manager-SSL	TCP/1169
----------------------	----------

Tripwire for Servers

A. Purpose: Tripwire for Servers will be able to detect and pinpoint changes to system and configuration files. Tripwire for Servers enables IT staff to determine what changed, when it changed, how it changed, who changed it-and to roll servers back to a known good state if the change is not authorized or desired.

Tripwire can be placed on various hosts on the system to alert the security administrators when there is unwanted activity on that host.

1.4.14 E-Mail Server

GIAC Enterprises will be using Microsoft Exchange 2000 for their internal email server. This is a prior application they were using and will be kept in place, but it will be put into the “future considerations” for an upgrade to possibly Microsoft 2003. The Exchange Server will be located internally so that all internal email can be kept local and a mail relay will be placed in Service Network #1.

The mail relay will add another layer of protection because it keeps external email outside the internal zone. We will be using the Dell machines with Red Hat 9.0 installed to run Sendmail 8.12.11. The concept with internal/external email servers is similar to that of the split DNS. With this concept, local email can stay local and will not have to access the email server on Service Network #1. The email relay on the service network is to deliver email to local boxes after it has been scanned and also only allow local email to the internal network

Mail server- SMTP	TCP/25
-------------------	--------

1.4.15 Database Servers

The database servers will be running MS-SQL Server both internally and externally. The external database on Service Network #2 will only have a limited number of cookie sayings. This way if that machine is attacked, the attackers will only have access to a limited number of sayings and not the whole database. Each week the external database will be updated and the old ones will be archived on the internal database.

1.4.16 Web Servers

The web servers will be installed on the Dell machine running LINUX Red Hat 9.0 using Apache 2.0.49. The IT staff has agreed to research Fedora for an upgrade from 9.0. For many years, Apache has earned the reputation as being one of the most secure and efficient web server.

Web Server	HTTP/HTTPS
------------	------------

1.4.17 Workstations

The workstations are installed with Windows 2000 Professional (unless otherwise specified). They have been updated with the latest services packs and patches. Also they have been hardened according to National Security Agency.
17 18

1.4.18 Antivirus applications/ Personal firewall

A. Purpose: This adds another layer of defense. It is installed on the client machines.

B. Equipment

http://www.symantec.com/smallbiz/scs_sbe/index.html

This product has been chosen because of several reasons. First, Symantec has a reputation as a world leader for Internet Security and has won many industry awards. Client Security¹⁹ integrates antivirus, firewall, and intrusion detection technology for desktop.

1.4.19 Backup Policies

The backup policy will vary depending on the functionality of the host that is being backed up.

Service Network servers: full backup weekly (analysis to be completed to determine best time to complete a full backup because GIAC Enterprises is a 24/7 operation).

Fortune Cookie Sayings database- During the needs assessment this database was identified as a critical area for security. Usually a company's number one asset is their information and this is definitely the case for GIAC Enterprises.

Backup plan:

RAID array

Local backup- CD

Remote Backup- remote journaling to different geographical region

Additional Protection for Cookie Saying database for consideration:

Possibly a SAN appliance with Fibre Channel for data backup

1.4.20 Security Maintenance

Once the security infrastructure is set up, it should be sufficiently maintained. To summarize the requirements:

- Patching

Maintain current OS releases, up-to-date patches

- Backups

Regular backups of system files, system/monitoring logs, rule bases

- Log analysis/review

Besides the automated analysis tools, periodic human review is needed

- Virus and IDS signatures

Keep them up to date

- Regular audits of systems and processes

1.4.21 Internet Service Provider (ISP)

Through experience, it has been found to have a good working relationship with your ISP provider. There are many times when working in conjunction with the ISP can prove beneficial to both. For example, if someone is attempting a DOS against your network you can notify the ISP for assistance in filtering some of the unwanted traffic you have been alerted to. This DOS could possibly be affecting unaware clients using the ISP.

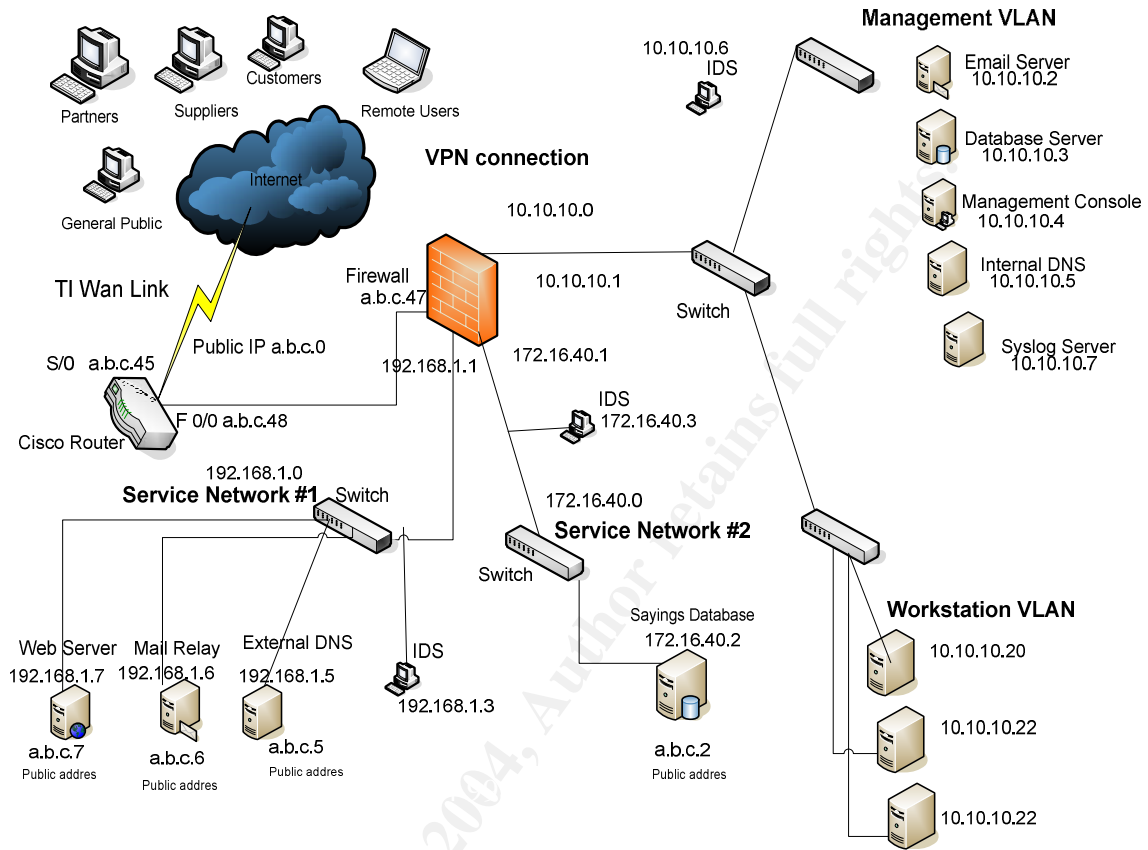
Encryption of data is an important detail in the configuration of the perimeter security for GIAC Enterprises. The goal is to ensure confidentiality, integrity and authentication by using SSL, 3DES, RSA. Also, during VPN connections we will be using AES.

1.5 ADDRESSING SCHEME

The addressing scheme for GIAC Enterprises will be comprised of one public IP for the WAN port on the router. The rest of GIAC Enterprises will be addressed using RFC 1918. (The names in our scheme are obvious to their function. In the real world, we would try to disguise this in some manner.

Device	Device Name	Function	Network ID	IP address
Untrusted				
Border Router	GE1	WAN Port-S/0	a.b.c.0	a.b.c.45
Border Router	GE1	Ethernet Port to Firewall FE/1	a.b.c.0	a.b.c.48
Border Router	GE1	Ethernet FE/2	a.b.c.0	a.b.c.49
Firewall	GEFW1	Router side port	a.b.c.0	a.b.c.47
Semi-Trusted				
Firewall	GEFW1	Service Network #1	192.168.1.0	192.168.1.1
Firewall	GEFW1	Service Network #2	172.16.40.0	172.16.40.1
Firewall	GEFW1	Trusted Port- to Internal Network	10.10.1.0	10.10.1.1
IDS	GEIDS1	Service Network #1	192.168.1.0	192.168.1.3
DNS Server	GEDNS1	Service Network #1	192.168.1.0	192.168.1.5
Mail Server	GEMAIL1	Service Network #1	192.168.1.0	192.168.1.6
Web Server	GEWEB1	Service Network #1	192.168.1.0	192.168.1.7
SecurID/VPN	GESECVPN1	Service Network #1	192.168.1.0	192.168.1.4
IDS	GEIDS2	Service Network #2	172.16.40.0	172.16.40.3
Ext. Database	GEDB2	Service Network #2	172.16.40.0	172.16.40.2
Trusted- Int. LAN				
E-Mail	INTEM	LAN	10.10.1.0	10.10.1.2
DataBase	INTDb	LAN	10.10.1.0	10.10.1.3
Management Console	INTMC	LAN	10.10.1.0	10.10.1.4
IDS	INTIDS	LAN	10.10.1.0	10.10.1.6
Syslog	INTSYS	LAN	10.10.1.0	10.10.1.7

1.6 TOPOLOGY/ARCHITECTURE of the GIAC Enterprises will be diagrammed using MS VISIO



© SANS Institute 2004, Author retains full rights

Security Awareness

Security Awareness and training is an area that many companies fail to address properly. User awareness training has to be as important an element to the total security policy as the router ACL and the firewall rule set. The tricky part is implementation of the Awareness Plan. There should be implementation policies: the technical staff and the users.

SANS offers a course that offers these benefits ²⁰.

- Educates your users about computer and Internet security risks.
- Conveys security best practices to help prevent damage due to avoidable mishaps.
- Most cost effective way to increase security across your organization.
- Empowers the individual to perform IT security best practices.
- Supports your organization security efforts and investments from the ground up.
- Aligns the security effort and supports the bottom-line.

Out of Scope Items –OTHER CONSIDERATIONS (not in order of priority)

Redundancy- routers/firewalls

Upgrade of Exchange 2000

Physical access within the GIAC Enterprises building

 Access into the building

 Access into the “server/device” areas

Patch management policy

2.0 Assignment – Security Policy and Tutorial

“A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of ‘what’ to do so that the ‘how’ can be identified and measured or evaluated.”²¹

(Stephen Northcut – Inside Network Perimeter Security)

This section will address the security policy for GIAC Enterprises. Perimeter Security and policy creation is a direct correlation to the Needs Analysis that should be thoroughly conducted at the beginning of ANY project. This entire process is cyclical in nature and is in a constant evaluation mode. Becoming static is possibly the number one reason for policy failures.

A security policy is actually a written statement that outlines what is acceptable or unacceptable in an organization. Organizations can have security policies written on various aspects of their organization. For example, there could be multiple policies in an organization ranging from strong passwords to user access.

Section 2 will discuss the security policy for the router, firewall, and VPN for GIAC Enterprises including a tutorial for the router.

2.1 ROUTER

The purpose of the router was explained in Section 1.

As mentioned previously, the border router is the first and last line of defense. The router policy locked down via configurations to disallow all unneeded traffic until a reason arises to allow certain traffic in. It is our policy to have a very tight policy and loosen it as the need arises.

Since GIAC Enterprises is a small e-commerce company, access to the router will only be permitted via the console port. The router will be in a secure room with limited access from employees.

The router provides secure access to network resources, and Internet services for all users. The border router will route traffic in and out of the GIAC Enterprises infrastructure based on packet filtering. It will examine packets based on the IP address of the packet and compare it to the Access Control Lists for both ingress and egress filtering. Based on this comparison it will either “permit” or “deny” the packet access to destination. By performing the function of a “filtering” router it will assist in distributing the security role between the router and the firewall.

Security Policy for Router

As all security policies, the security policy for the router is a “living” document that is constantly monitored for necessary changes as needed. It does not have to be lengthy. More importantly, it should be clear and specific. Also, there should be a metric in place to measure compliance with the security policy. This also will be used to keep the policy current.

The following items should be addressed in a router policy. Later, in this section, the tutorial will demonstrate how to implement the policy into the router configuration.

**The router configuration, including access control lists, will be reviewed as business needs arises.*

- All users must be authenticated and an encrypted password must be use.
- Filtering inbound and outbound traffic to the router
- Protecting against ICMP and SYN floods and other malicious traffic
- Protecting against malicious fragments
- Protecting against packets with IP options
- Preventing routers from being used as zombies
- Auditing for security- checking for unwanted traffic and malformed packets/traffic, and misuse and report to management
- Routing protocol events and errors
- Log of traffic being denied
- Use multiple security mechanisms in the architecture.-“Defense in Depth”
- Include a “warning” banner indicating appropriate use and consequences if used outside the scope of the policy.
- Disable unneeded services
- Disable remote configuration
- Disable servers on the router
- Properly configured backup configurations- TFTP

Border Router Tutorial.^{22 23}

The tutorial will now demonstrate how to implement the policy as described above.

Common Terms

a. Access Control List- kept by the router to control access of packets to and from the router – operates in a sequential order

b. Standard Access Control List- checks for source address only

Example of a Standard ACL- *access-list 1*

The number 1 indicates a standard ACL- if the number ranges between 1- 99 indicates a standard

- c. Extended Access Control List- allows for more thorough packet checking- checks the source/destination address, and port numbers, and protocols- the number would range from 100- 199
access-list 100
- d. Wildcard mask- is paired with an IP address – used to mask a single address or multiple addresses to permit or deny- looks like an inverted subnet mask- bits determine whether the corresponding bits in the IP should be checked. A “1” bit means do not check or ignore and a “0” bit means to check.

Configuration considerations:

Put rules that will be used frequently to the top of the configuration to improve the performance because once a rule is matched it does not move down the configuration file.

When making a change to the ACL it must be changed from the TFTP file in notepad. A standard or extended access-list cannot be modified on the router. Also, specific rules should be near the top of the ACL to filter more traffic than the general rules.

Interface assignment:

Serial 0/0 – connects to the Internet

Serial 0/1- not used at this time

Ethernet 0/0-connects to the firewall

Ethernet 0/1- not used at this time

Cisco routers are configured using a Command Line Interface (CLI). There are two modes or levels of access: user mode and privileged mode.

User mode (>) is used mainly for troubleshooting and no configuration changes can be applied while in this mode.

Privileged mode (#) is where actual configuration changes are made.²⁴

The next step is to configure router via the console port using a rollover cable, which is usually powder blue. This cable will connect the console port to COM1 on the computer you are going to use to configure the router. Routers can also be configured via telnet; however, a direct connection is more secure. The HyperTerminal utility will be used for configuration

Router> (note this is user mode)

At this command prompt, type “enable” and you will enter the privileged mode.

Router

At the privileged prompt (#), typing in configuration terminal (config t) will put the router in global configuration mode. Therefore, when you see a command “GE1(Config)#”, this indicates the router must be in configuration terminal mode. Global configuration mode is where changes that effect the entire router are made.

Once a command has been entered, the “show” command can confirm that command has been entered.

For example:

```
GE1# config t
Enter configuration commands, one per line. End with CNTL/Z.
GE1# (config)# no cdp run
GE1# (config)# exit
```

Then to verify the configuration use the “show” command

```
GE1#show cdp
% CDP is not enabled
GE1#
```

Naming a router

```
Router(Config)# hostname GE1
```

(Notice how the router has been renamed to GE1)

All passwords used on the router will be encrypted using Message Digest 5 (MD5).

```
GE1(Config)# service password-encryption
GE1(Config)# enable secret “password”
GE1(Config)# no enable password
```

The banner is used to alert intruders that their activities will be logged. This is an example of a possible banner.

```
GE1(Config)# Banner motd #Access to this device is logged and is also
prohibited except by authorized users. Violators will be prosecuted!#
```

SERVICES

Routers and Operating Systems are shipped with some services enabled by default. The first thing to secure the router is to disable unneeded services.

Disable this service so the router does NOT give out information about other Cisco equipment on the GIAC Enterprises network.

```
GE1# (config)#no cdp run
```


This command tells the router to not respond to a DHCP request.

```
GE1(config)#no service dhcp
```

This command will tell the router to not attempt to resolve domain names to IP addresses. This is helpful when the router administrator mistypes a command and the router attempts to resolve the incorrect information and sometimes this could take several seconds or even up to a minute or two.

```
GE1(config)#no ip domain-lookup
```

“Finger” allows a user to view users logged into a remote system. This is inappropriate for a router, and therefore disabled with the following:

```
GE1(config)#no ip finger
```

(Disable forcing a packet to take a specific route through the network)

```
GE1(config)#no ip source-route
```

Keep the router from DOSing itself if a hacker attacks the router. Also, during router administration it can be distracting and it can be turned on and off as needed.

```
GE1(config)#no logging console
```

This command will tell the router to not allow broadcast:

```
GE1(config)#no ip directed-broadcast
```

The following commands suppress ICMP Redirect, and ICMP Unreachable messages, plus this helps to prevent DOS attacks.

```
GE1(config)#no ip redirects
```

```
GE1(config)#no ip mask-reply
```

```
GE1(config)# no ip unreachable
```

Proxy ARP allows IP clients that do not understand a subnet mask to route properly when IP address spaces are subnetted. Modern IP stacks understand subnet masks, therefore proxy ARP should almost always be disabled with the following command

```
GE1(config)#no ip proxy-arp
```

Disable remote configuration

```
GE1(config) no service config
```

The service tcp-keepalives command clears hung telnet sessions so that a hacker cannot connect to a hung session:

```
GE1(config)#service tcp-keepalives-in  
GE1(config)#service tcp-keepalives-out
```

Log command- it is important to establish the router to log activity. This information can then be sent to the Syslog server for analysis.

```
GE1(config)#logging on  
GE1(config)#logging 10.10.1.7 255.255.255.0 (IP address of logging server)
```

SERVICES:

The following commands are used to disable services on the router. Shutting down unneeded services will also free up processor and memory utilization.

Disable HTTP router access, the only configuration changes will be done via serial

connection

```
GE1(config)#no ip http server
```

This disables all minor tcp and udp services running on the router.

```
GE1(config)#no service tcp-small-servers  
GE1(config)#no service udp-small-servers
```

GIAC Enterprises will **not** be utilizing SNMP at this time, so that protocol/utility should also be disabled.

```
GE1(config)#no snmp-server  
GE1(config)# no snmp-server enable traps  
GE1(config)# no snmp-server system-shutdown  
GE1(config)# no snmp-server trap-auth
```

This command will tell the router to **not** act as a bootp server

```
GE1(config)#no ip bootp server
```

Remote Access Ports – Configuration

Console

The router is managed via the console. The console port is enabled by default. It is configured to disconnect after 5 minutes idle.

```
GE1(config)# line con 0  
GE1(config-line)# exec-timeout 5 0  
GE1(config-line)# login local  
GE1(config-line)# transport input none
```

VTY

Telnet is a method of remote access. Routers can be configured via the telnet utility. In router terms is called the vty port. This needs to be disabled to prevent telnet connections.

```
GE1(config)# line vty 0 4
GE1(config-line)# transport input none
GE1(config-line)# exec-timeout 0 1
GE1(config-line)# no login
```

AUX

The auxiliary port is usually used for remote access via a modem. This should be disabled so hackers cannot war dial to the router.

```
GE1(config)# line aux 0
GE1(config-line)# transport input none
GE1(config-line)# no exec
GE1(config-line)# no login
GE1(config-line)# exec-timeout 0 1
```

Configuring Interfaces

```
Ethernet 0/0
GE1(config)# interface fastethernet 0/0
GE1(config-if)#ip address a.b.c.48 255.255.255.0
GE1(config-if)#description interface to firewall
GE1(config-if)#no shutdown
GE1(config-if)# no ip directed-broadcast
GE1(config-if)# no ip unreachable
GE1(config-if)# no ip redirects
GE1(config-if)# no ip mask-replies
```

Ethernet 0/1 is not being utilized at this time, so it will not be configured.

Now we apply these same rules to the Serial Interfaces.

```
GE1(config-if)# interface serial 0/0
GE1(config-if)#ip address a.b.c.45 255.255.255.0
GE1(config-if)#description interface to ISP
GE1(config-if)#no shutdown
GE1(config-if)# no ip unreachable
GE1(config-if)# no ip redirects
GE1(config-if)# no ip mask-replies
GE1(config-if)# no ip directed-broadcast
```

Serial 0/1 is not being utilized at this time, so it will not be configured.

ACCESS CONTROL LISTS (ACL'S)

The ACL on a Cisco router is a list of commands that list what traffic is permitted or denied. It also disables services that are not needed and should be denied access. Once an ACL is created it is then attached to the appropriated interface (internal/external). The order of the ACL is critical because as a packet hits an interface it processes through the ACL in the order the ACL is written. It is also recommended that the Access Control List be created in a utility such as Notepad so that changes can be easily made. Then use TFTP to transfer the ACL to the router. If a change is made to the ACL through HyperTerminal, it will add the change to the bottom of the ACL and placement of the rules is important as it was in the firewall rule set.

Ingress traffic

Interface Serial 0-Interface receiving traffic from the ISP/Internet

ip address a.b.c.45 255.255.255.0

ip access-group 101 in (this applies the access-list, outlined below, to this interface)

Do not allow IP traffic in from the addresses outlined in RFC 1918-

access-list 101 deny 10.0.0.0 0.255.255.255 any

access-list 101 deny 192.168.0.0 0.0.255.255 any

access-list 101 deny 172.16.0.0 0.15.255.255 any

Deny loopback and broadcast

access-list 101 deny 127.0.0.0 0.255.255.255 any log

access-list 101 deny 0.0.0.0 255.255.255.255 any log

Block protocols- these protocols will not be needed- therefore should be blocked

Systat, daytime, netstat, chargen, ftp

access-list 101 deny tcp any any eq 11 log

access-list 101 deny tcp any any eq 13 log

access-list 101 deny udp any any eq 13 log

access-list 101 deny tcp any any eq 15 log

access-list 101 deny tcp any any eq 19 log

access-list 101 deny udp any any eq 19 log

access-list 101 deny tcp any any range 20 21 log

Unallocated addresses will also be denied²⁶

access-list 101 deny ip 2.0.0.0 0.255.255.255 any log

access-list 101 deny ip 5.0.0.0 0.255.255.255 any log

access-list 101 deny ip 7.0.0.0 0.255.255.255 any log

access-list 101 deny ip 23.0.0.0 0.255.255.255 any log

```
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 0.255.255.255 any log
access-list 101 deny ip 59.0.0.0 0.255.255.255 any log
access-list 101 deny ip 85.0.0.0 0.255.255.255 any log
access-list 101 deny ip 86.0.0.0 0.255.255.255 any log
access-list 101 deny ip 87.0.0.0 0.255.255.255 any log
access-list 101 deny ip 88.0.0.0 0.255.255.255 any log
access-list 101 deny ip 89.0.0.0 0.255.255.255 any log
access-list 101 deny ip 90.0.0.0 0.255.255.255 any log
access-list 101 deny ip 91.0.0.0 0.255.255.255 any log
access-list 101 deny ip 92.0.0.0 0.255.255.255 any log
access-list 101 deny ip 93.0.0.0 0.255.255.255 any log
access-list 101 deny ip 94.0.0.0 0.255.255.255 any log
access-list 101 deny ip 95.0.0.0 0.255.255.255 any log
access-list 101 deny ip 96.0.0.0 0.255.255.255 any log
access-list 101 deny ip 97.0.0.0 0.255.255.255 any log
access-list 101 deny ip 98.0.0.0 0.255.255.255 any log
access-list 101 deny ip 99.0.0.0 0.255.255.255 any log
access-list 101 deny ip 100.0.0.0 0.255.255.255 any log
access-list 101 deny ip 101.0.0.0 0.255.255.255 any log
access-list 101 deny ip 102.0.0.0 0.255.255.255 any log
access-list 101 deny ip 103.0.0.0 0.255.255.255 any log
access-list 101 deny ip 104.0.0.0 0.255.255.255 any log
access-list 101 deny ip 105.0.0.0 0.255.255.255 any log
access-list 101 deny ip 106.0.0.0 0.255.255.255 any log
access-list 101 deny ip 107.0.0.0 0.255.255.255 any log
access-list 101 deny ip 108.0.0.0 0.255.255.255 any log
access-list 101 deny ip 109.0.0.0 0.255.255.255 any log
access-list 101 deny ip 110.0.0.0 0.255.255.255 any log
access-list 101 deny ip 111.0.0.0 0.255.255.255 any log
access-list 101 deny ip 112.0.0.0 0.255.255.255 any log
access-list 101 deny ip 113.0.0.0 0.255.255.255 any log
access-list 101 deny ip 114.0.0.0 0.255.255.255 any log
access-list 101 deny ip 115.0.0.0 0.255.255.255 any log
access-list 101 deny ip 116.0.0.0 0.255.255.255 any log
access-list 101 deny ip 117.0.0.0 0.255.255.255 any log
access-list 101 deny ip 118.0.0.0 0.255.255.255 any log
access-list 101 deny ip 119.0.0.0 0.255.255.255 any log
access-list 101 deny ip 120.0.0.0 0.255.255.255 any log
access-list 101 deny ip 121.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 122.0.0.0 0.255.255.255 any log
access-list 101 deny ip 123.0.0.0 0.255.255.255 any log
access-list 101 deny ip 124.0.0.0 0.255.255.255 any log
access-list 101 deny ip 125.0.0.0 0.255.255.255 any log
access-list 101 deny ip 126.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 187.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny IP 223.0.0.0 0.255.255.255 any log
```

(Also deny IP range 224.0.0.0- 239.0.0.0 – reserved for multicast and deny unallocated IP range 240.0.0.0 – 255.0.0.0)

DSshield- Top 10 Most Wanted Offenders²⁷ (Note- DSshield and other similar sites should be checked periodically for new offenders, but more importantly for accuracy)

```
access-list 101 deny ip host 152.30.203.88 any log
access-list 101 deny ip host 24.83.79.113 any log
access-list 101 deny ip host 80.185.111.116 any log
access-list 101 deny ip host 81.193.23.182 any log
access-list 101 deny ip host 80.125.239.177 any log
access-list 101 deny ip host 83.30.18.23 any log
access-list 101 deny ip host 138.88.176.158 any log
access-list 101 deny ip host 217.68.175.41 any log
access-list 101 deny ip host 210.22.141.90 any log
access-list 101 deny ip host 217.84.57.241 any log
```

```
access-list 101 deny tcp any any eq 3127 log
access-list 101 deny tcp any any eq 1433 log
access-list 101 deny tcp any any eq 1434 log
access-list 101 deny tcp any any eq 2745 log
```

This will be denied because tftp will be used internally and should not be allowed via the Internet.

```
access-list 101 deny udp any any eq tftp
access-list 101 deny tcp any any eq tftp
```

This is also denied because of known security risks with NetBIOS.

```
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 netbios-ss
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445
```

The following packets need to be permitted access because they correlate with a service that is being utilized.

```
access-list 101 permit tcp any a.b.c.0 0.255.255.255 established
access-list 101 permit udp any a.b.c.1 eq 53
access-list 101 permit tcp any a.b.c.6 eq 25
access-list 101 permit tcp any a.b.c.3 eq 80
access-list 101 permit tcp a.b.c.7 eq 443
access-list 101 permit tcp a.b.c.0 0.0.0.255 a.b.c.4 eq 80
```

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

Interface Ethernet 0/0

access-list on the E 0/0

```
access-list 110 deny tcp any any range 135 139
access-list 110 deny udp any any range 135 139
access-list 110 deny tcp any any 445
access-list 110 deny udp any any 445
access list 110 deny udp any any 514
access-list 110 deny udp any any range 161 162
access-list 110 deny icmp any any echo-reply unreachable
access-list 110 deny any any log
```

Assign the access groups to the interface e 0/0

```
interface Ethernet 0
ip access-group 110 in
ip access-group 102 out
```

In addition, many of the same commands from the Serial Interface 0 will also be applied here on the Ethernet interfaces.

EGRESS FILTERING- This is traffic that we do not want leaving our network-

Do not allow RFC 1918, multicast addresses, or loopback to leave our network

```
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 10.0.0.0 0.0.0.255 any log
```

Also, block all the unallocated IANA address spaces- no spoofed packets leaving.

```
access-list 102 deny ip 224.0.0.0 15.255.255.255 any log
access-list 102 deny ip 127.0.0.0 0.255.255.255 any log
access-list 102 deny ip 0.0.0.0 0.255.255.255 any log
```

TFTP does not need to leave the network- the TFTP server will be local for security purposes

```
access-list 102 deny udp any any eq tftp
```

```
access-list 102 deny tcp any any range 135 139
access-list 102 deny udp any any range 135 139
access-list 102 deny tcp any any 445
access-list 102 deny udp any any 69
access-list 102 deny udp any any 514
access-list 102 deny udp any any range 161 162
access-list 102 deny icmp any any echo-reply unreachable
```

```
access-list 102 deny any any log
```

(Note: the ACL's are not written in the proper order for implementation. As previously noted care must be taken when creating ACL's because as the traffic moves through the ACL the first match it makes is what is applied to that particular traffic.)

2.2 FIREWALL

Checkpoint Firewall-1/VPN-1 develops the firewall security policy based on individual rules programmed into the SmartDashboard. As the router policy, before the firewall configuration can begin it must be determined what is to allowed or denied access to GIAC Enterprises.

A Rule Base is an ordered set of rules that defines a specific Security Policy. A rule describes a communication in terms of its source, destination and service, and specifies whether the communication should be accepted or rejected, as well as whether it is to be logged.

There are implied rule and explicit rules for Checkpoint Firewall-1/VPN-1. The implied rules are defined in Global Properties. Implied rules use commonly used services such as RIP, domain names over UDP, and domain names over TCP. Checkpoint Firewall-1/VPN-1 has the capability for the user to add explicit rules. Explicit rules are rules that the firewall administrator creates. There are certain elements that must be contained in each of these rules:

Source- Where the traffic is originating?

Destination- where it is going?

Service- What kind of traffic?

Action- What action do you want the firewall to take against the service?

Track- Do you want the firewall to log the action?

Comment- good idea to add so you can remember why you added the rule

Both implied and explicit rules also have a configuration for placement. Ordering of rules is very important on a firewall. A firewall administrator should place high priority rules towards the top of the rule set. This will reduce processing as the rule moves down the list.

Typically the first rule on a Checkpoint Firewall-1/VPN-1 is considered the "Stealth" rule. This is used to hide your firewall.

The last rule is called the "clean-up" rule. This should be used in every rule base. Without the "clean-up" rule at the end of the rule set all the packets that didn't meet a rule would be dropped and no one would know this information. The "clean-up" rule makes the dropped packets logged so the log administrator is aware of the packets that were dropped. Finally there is an implied drop rule. Any rule that is not expressively permitted is dropped. This does not create a log entry. This is why the cleanup rule is created.

The rule base is a direct correlation of the security policy that has been established for the firewall. It is also a good idea to attempt to keep the rule base

as simple as possible as too many rules can easily become very confusing even for the most experienced firewall expert.

Placement of the rules is also a consideration. As packets enter the firewall they are matched against the rules. As soon as the packet hits a rule that matches, that rule is enforced. Therefore, it is important to place the rules that will be matched the most frequently at the top of the rulebase.

Checkpoint Firewall-1/VPN-1 NG has a defined rulebase order: ²⁸

IP spoofing/IP Options

Implied rules with "first" option

Rules before Stealth rule

Stealth rule

Rules after Stealth rule

Implied rules with "Before Last" option

Cleanup rule (Policy's last rule)

Implied rules with "Last" option

Implied Drop

Once the Checkpoint Firewall-1/VPN-1 software has installed, the next step is to add the network objects:

GEFW1- the Checkpoint Firewall-1/VPN-1 -NG firewall – a.b.c.47

GE1- Border Router- a.b.c.0

Service Network 1- 192.168.1.0

Service Network 2- 192.168.2.0

GEIDS1- 192.168.1.3

GEDNS1- 192.168.1.5

GEMAIL1- 192.168.1.6

GEWEB1- 192.168.1.7

GESECVPN1- 192.168.1.4

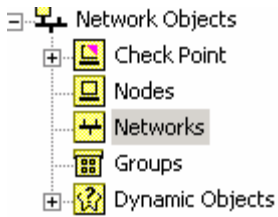
GEIDS2- 192.168.2.3

GEDB2- 192.168.2.2

This menu is located on the SmartDashboard and is a vital component. Some icons are described below:



Before beginning to build your rulebase, Network Objects need to be identified.



Checkpoint- Identifies the device where our firewall (GEFW1) is installed.

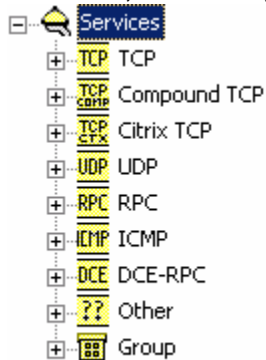
Nodes- Identifies the IP address

Networks- This will represent our services networks and internal (trusted) segment

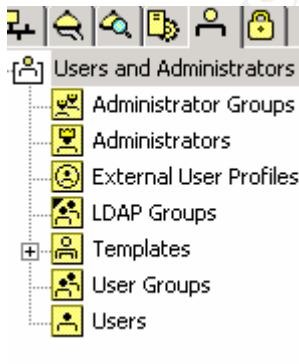
Groups- Identify our groups



Services- By default, Checkpoint has installed some specific, well-known services; however, it also provides the capability to add services as needed.



Users and Administrators- this icon allows the Checkpoint administrator to add users and administrators.



Now it is time to begin building our rulebase.

Rule Base definitions:

No.- number of rule

Source: source IP address- “from”

Destination: destination IP address- “to”

VPN: defines the VPN community the connection passes through

Service: protocols that should be checked

Action: what should the firewall do with the packet

Accept- sent to destination

Drop-connection is blocked

Reject- blocked and an ICMP unreachable is sent

User Auth- grants connection on a per connection basis

Client Auth- grants connection per host

Session Auth- grants connection per session

Track- what type of notification for each packet

None-

Log

Account

Alert

SnmpTrap

Mail

User defined

User defined 2

User defined 3

Install on: which firewalled object should this rule be installed on

Time: can define a time period- defaults to be constantly active

Comment: useful to help reason for rule and can help with troubleshooting

1	admin	fw-module	* Any Traffic	TCP CPD TCP FW1 TCP FW1_jca_push TCP FW1_CPRID	accept	- None
2	fw-module	admin	* Any Traffic	TCP FW1 TCP FW1_log TCP FW1_jca_pull	accept	- None

Rules 1 & 2- The first two rules allow for firewall administrator to access the firewall for admin purposes.

3	* Any	* Any	* Any Traffic	UDP bootp NBT UDP rip	drop	- None
---	-------	-------	---------------	-----------------------------	------	--------

Rule 3: The third rule in the firewall policy is to drop NetBIOS over TCP/IP and bootp protocols without logging. Windows servers and workstations often broadcast NetBIOS name announcements. NBT is not required across the firewall and can quickly fill the logs.

This rule is towards the top of the rule base because of the number of NetBIOS, NBT, and bootp traffic in the network. (Note: bootp is also being blocked at the router level)

4	* Any	GEDNS1	* Any Traffic	UDP domain-udp TCP domain-tcp	accept	- None
5	GEDNS1	* Any	* Any Traffic	UDP domain-udp TCP domain-tcp	accept	- None

Rules 4 & 5: The next two rules are to allow external users access for DNS resolution of addresses for GIAC Enterprises. It is early in the rule base because of the amount of traffic to the DNS Server. Traffic is also not logged for this reason.

stealth rule (Rule 6)						
6	* Any	gef1w1	* Any Traffic	* Any	drop	- None

Stealth Rule: The stealth rule should be in every rule set along with the cleanup rule. This rule drops any attempt to components. This rule protects and hides your Enforcement Point and logs it.

7	* Any	GEWEB1	* Any Traffic	TCP https TCP http	accept	- None
---	-------	--------	---------------	-----------------------	--------	--------

Rule 7: This rule allows traffic from “any” source to access the web server on Service Network #1 using either http or https. Internet users should be able to browse GIAC-P external web site.



Rule 8: This rule allows users in the admin group to access necessary devices and networks to perform administrative functions.



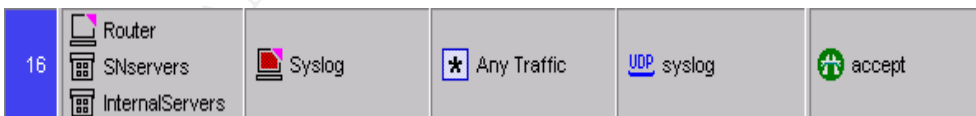
Rules 9-13: These rules are in place to allow Mail Traffic to and from the GIAC Enterprises intranet to access the mail relay. Rule 13 is important to deny any traffic to the internal mail server unless it has been specifically permitted.



Rule 14: This rule allows predefined external users to the fortune cookie database on Service Network #2. Only users listed under the external users can access this database.



Rule 15: Allows the Mobile users VPN access into GIAC Enterprises.



Rule 16: This rule directs the router and the servers on Service Network #1 & #2 to log traffic to the syslog server.

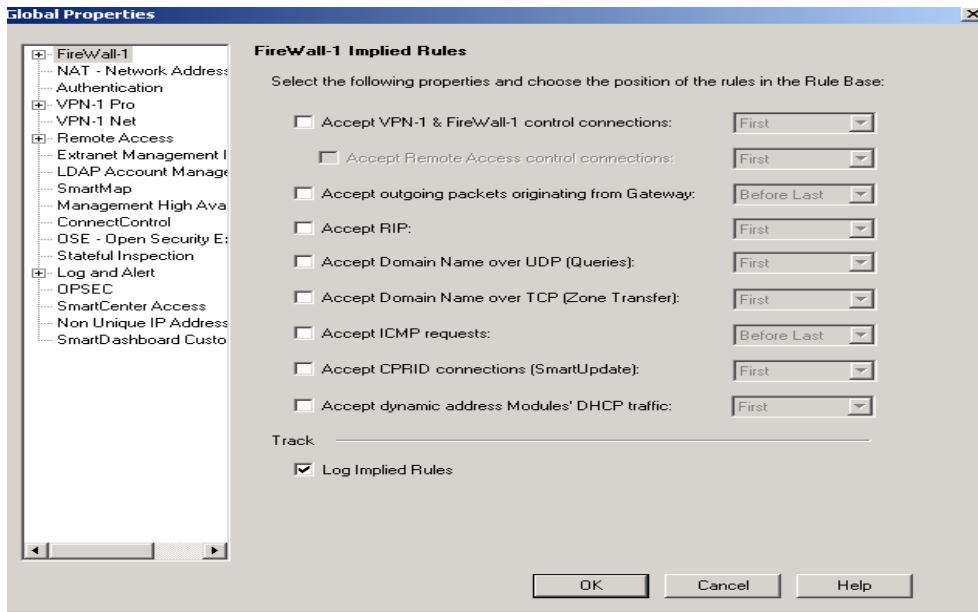


Cleanup Rule- Drops rule-rejects and logs all other communications.

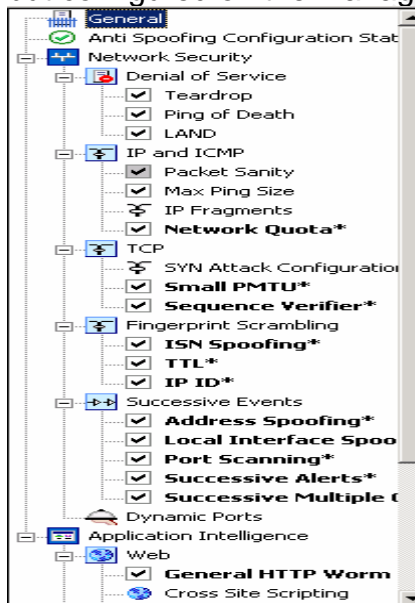
GEFW1- Global Properties-

Global Properties affect policies you create and there are some default configurations that are captured below.

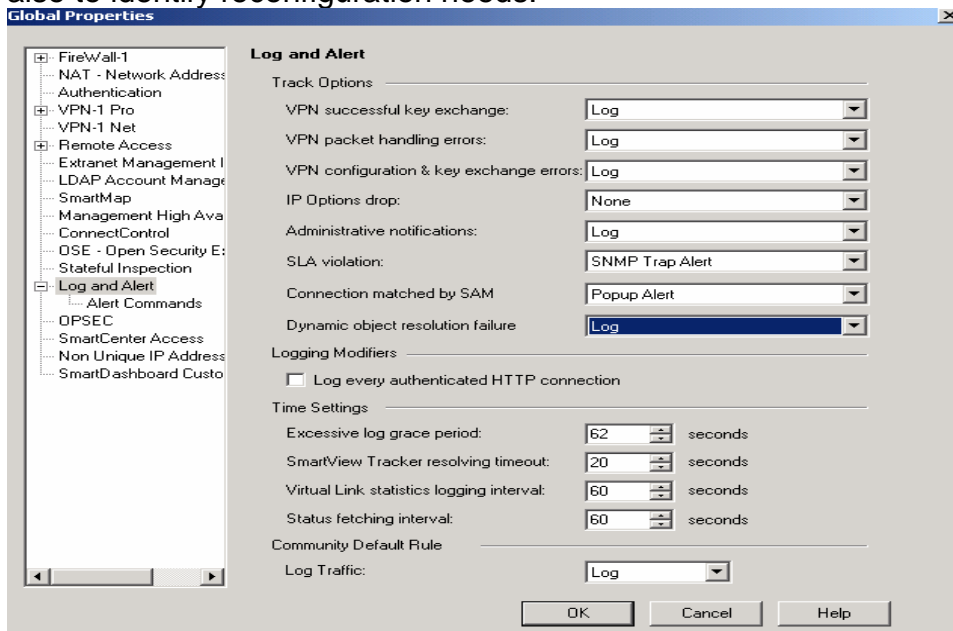
The following shows the Implied Rules for GIAC Enterprises Checkpoint firewall: Firewall implied rules are applied by the firewall; however, they will not appear in the rule base. The important item here is to “check” the “Log Implied Rules”



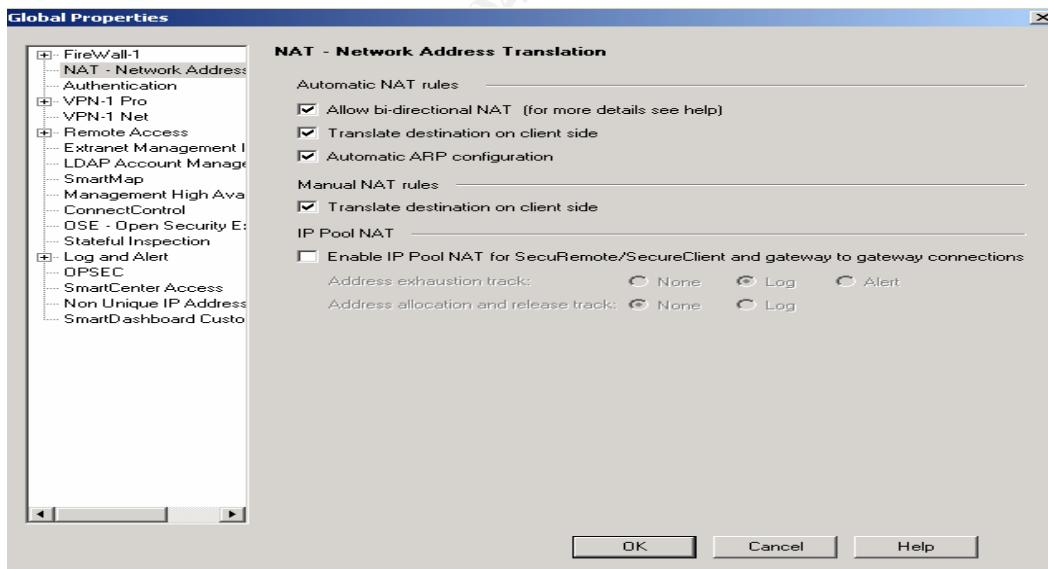
Smart Defense centralizes control for network and application level defenses. It also can alert and log possible attacks. It is deployed on the enforcement points, but configured on the management server.



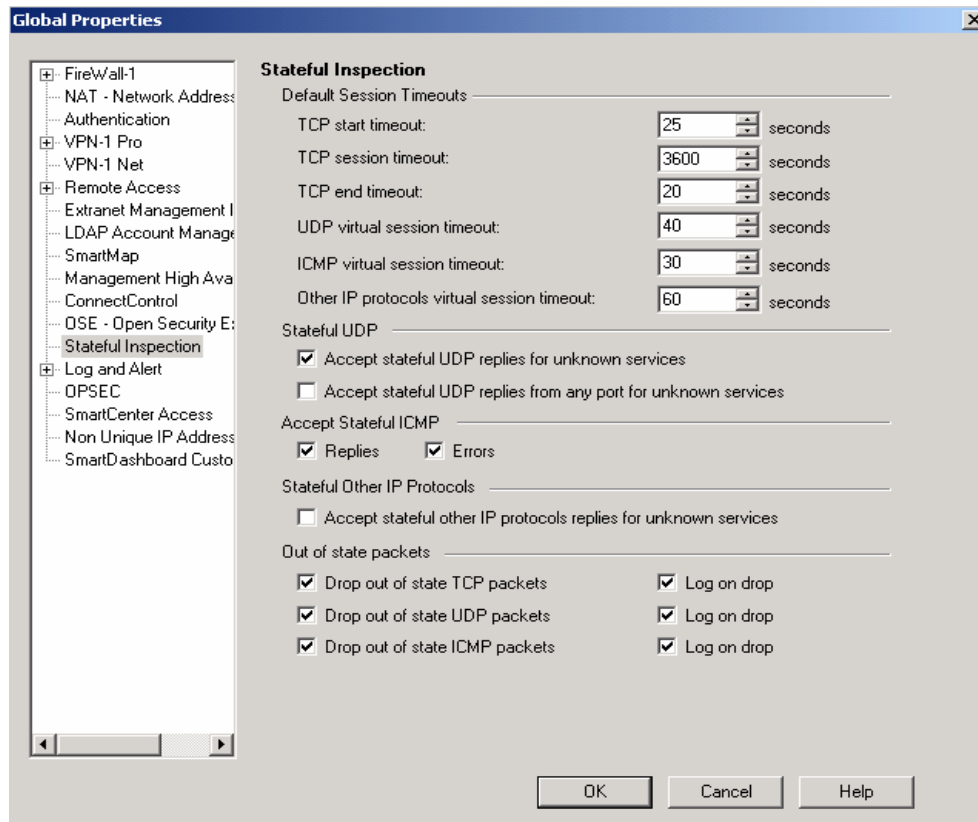
In the Global Properties- Log and Alert, is where we can configure certain functions to be logged. Logs are crucial to help identify attacks and trends, and also to identify reconfiguration needs.



NAT



This defines the timeout sessions and to log all “out of state” packets.



Once the rules have been written we can “verify” the policy by going to Policy-Verify

2.3 VIRTUAL PRIVATE NETWORK (VPN)

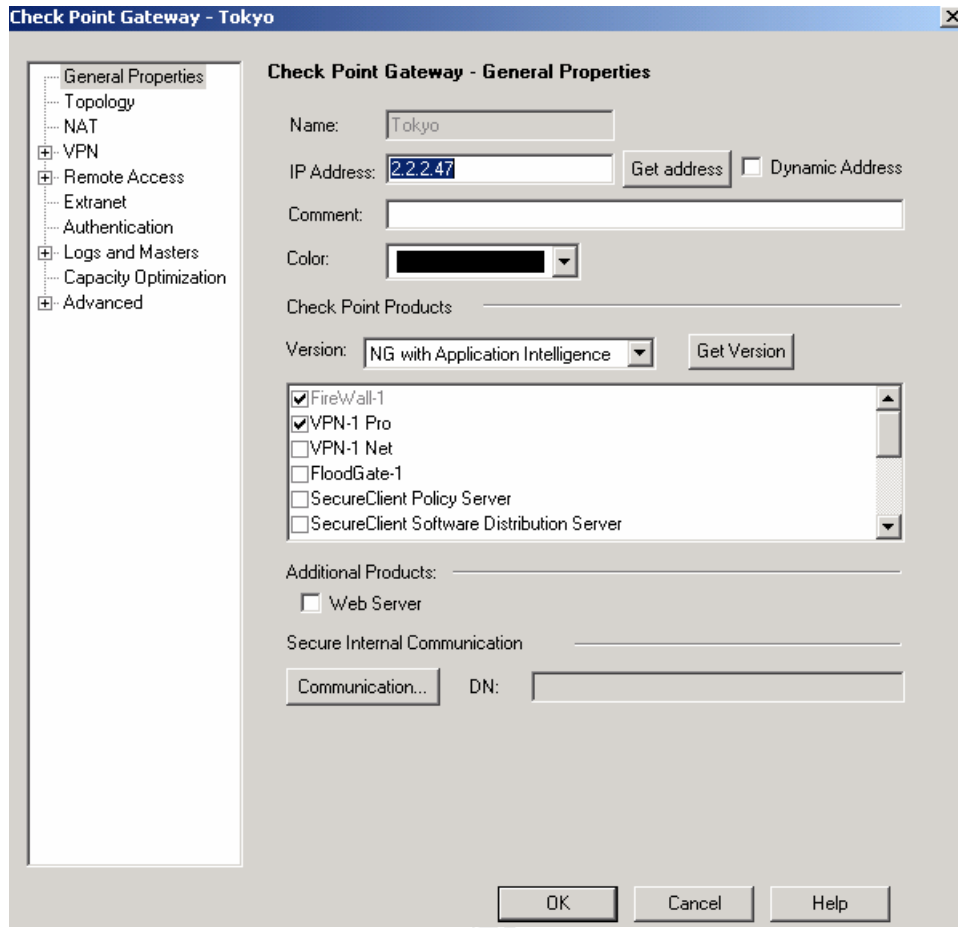
When establishing VPN policies, several items must be considered.

- Confidentiality- no one except the intended participants can view the data
- Integrity- no one has tampered or altered the data
- Authenticity- no one is sending false data

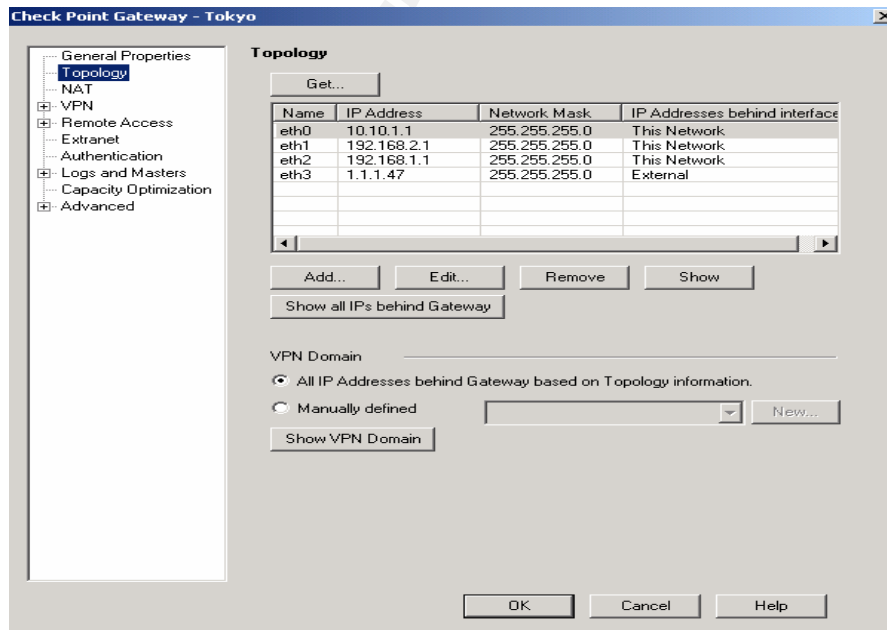
Checkpoint Gateway – General Properties

Step 1: Create a network object for Tokyo VPN gateway.

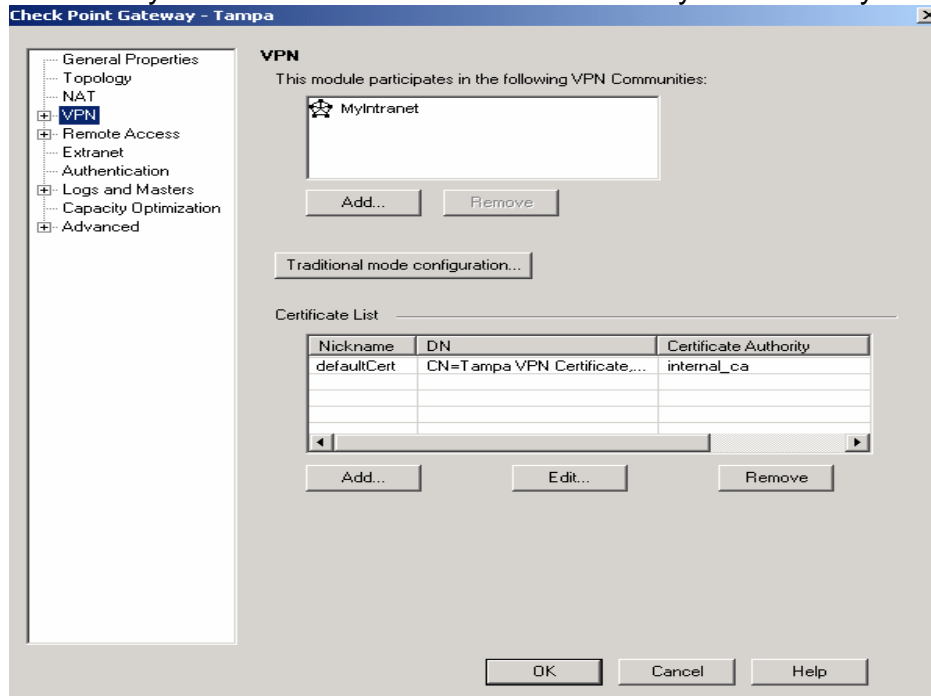
By creating the Tokyo network object we can now assign other properties. Also, assigns the IP address and other configurations for our Tokyo VPN partner



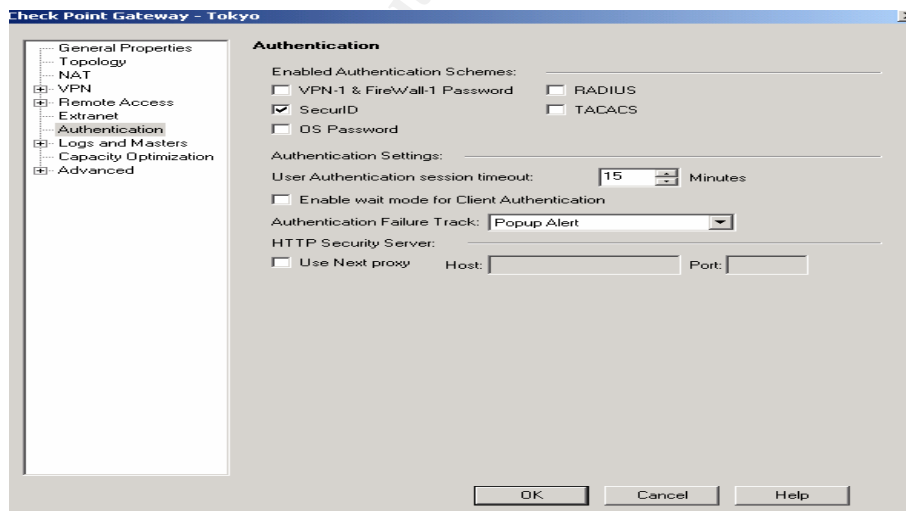
Now we identify the topology on Tokyo



The next step demonstrates TAMPA community to participate in the My Intranet community. We would do the same for the Tokyo community



The next step identifies authentication scheme for the communities. We will be using SecurID.

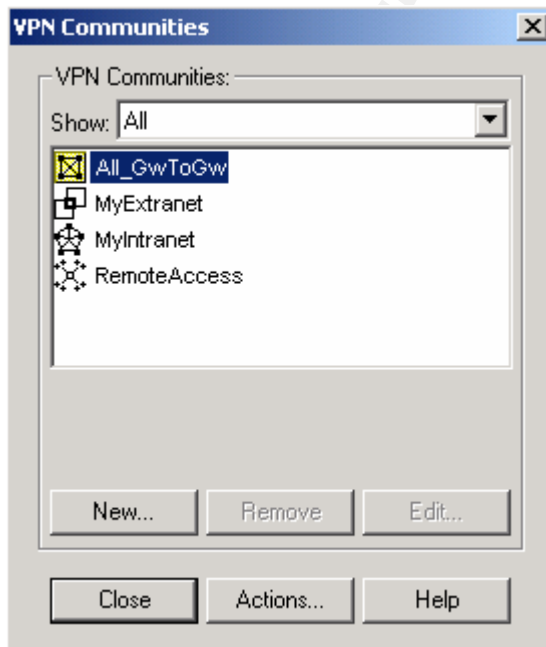
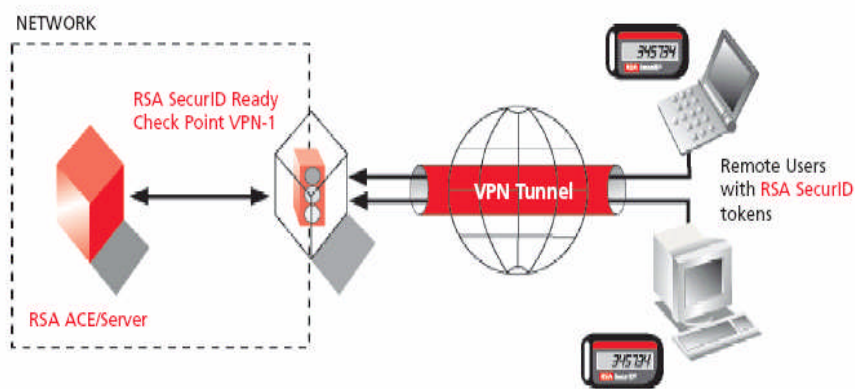


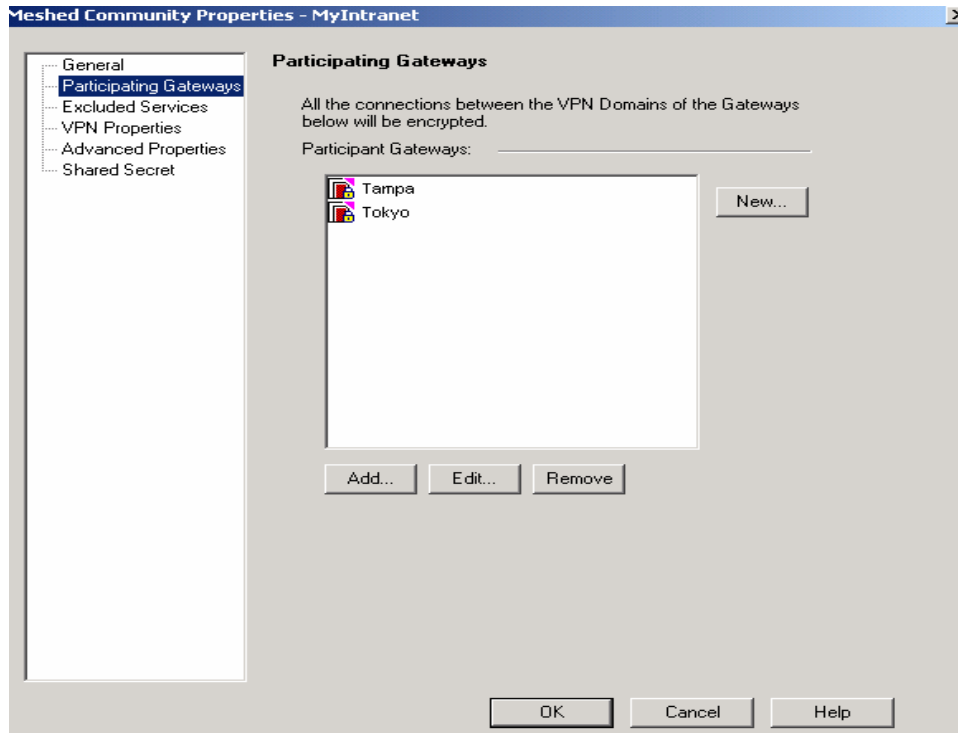
1. Explanation for incorporating SecurID

http://rsasecurity.agora.com/rsasecured/guides/solutions/Checkpoint_SB_0403.pdf

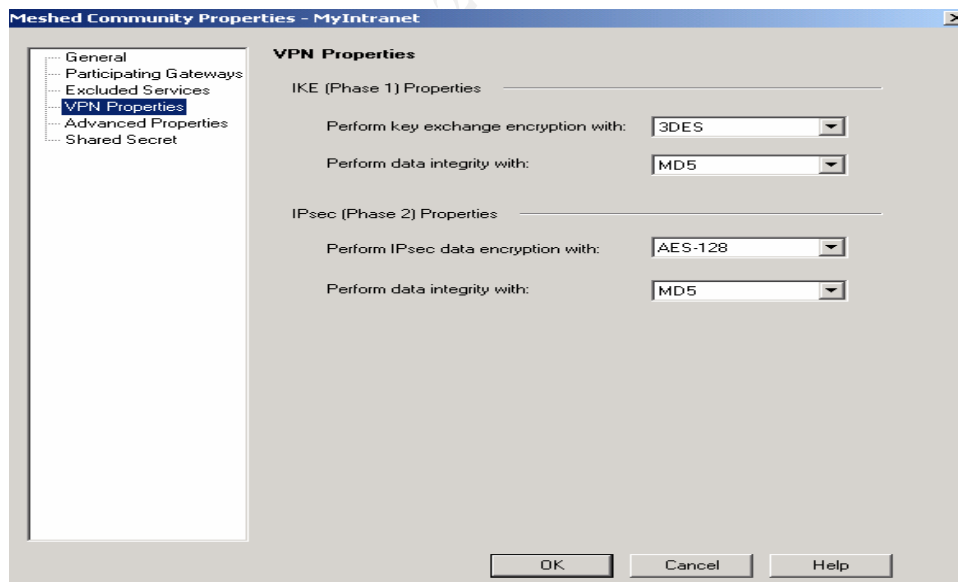
Solution Benefits- RSA

- Interoperates out-of-the-box with the Check Point VPN-1 solution
- Simplifies configuration and deployment with a detailed implementation guide
- Supports RSA ACE/Server (v5.0) automatic load-balancing and replication to meet enterprise disaster recovery and scalability needs
- Enables trusted access to critical information and transactions with end-user accountability
- Reduces risks and costs associated with intellectual property theft and security breaches
- Lowers costs associated with password related help-desk calls
- Increases remote user productivity without compromising security





This demonstrates the VPN communities of Tokyo and Tampa are installed in the Meshed Community.



This is a crucial configuration window. The IKE properties and IPsec properties must be consistent on all servers and clients for communication. AES is recommended for an encryption algorithm.

Internet Key Exchange- IKE

Internet Key Exchange is a key management protocol standard that is used with IPSec which adds authentication and encryption of IP packets as they are traversed across the media.

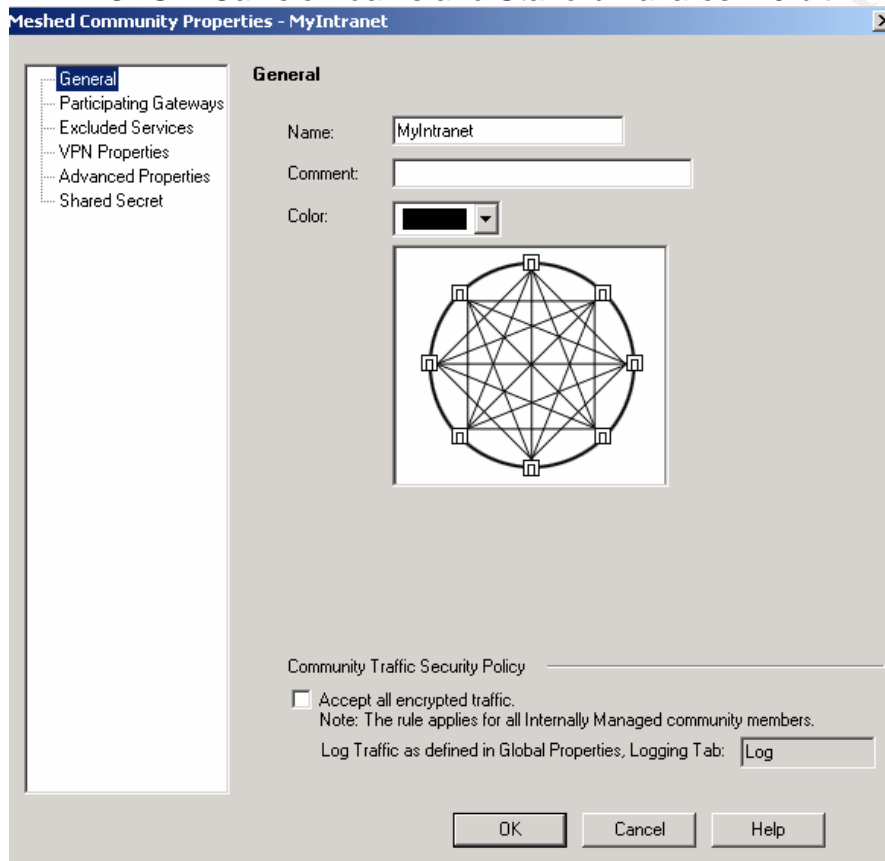
Symmetric Algorithms used by IKE:

DES- Data Encryption Standard- 56 bit

3DES- Triple DES- 168 bit

AES- Advanced Encryption Standard- 128/256 bit **(recommended)**

CAST- Carlisle Adams and Stafford Tavares- 40 bit



3.0 Verify the Firewall Policy

The goal is to verify the firewall policy and that the firewall policies are implemented correctly. Additionally, it should be noted that this is an initial audit of a “new” ruleset. More intrusive audits should be performed after the GIAC Enterprises has been using the security policy for a set period of time. Log files should be checked on a regular basis and sometimes can give the security personnel more information than an audit. Checking log files and a certain level of auditing is a constant process!!

A. Planning the validation:

- The first step in planning the validation will be to meet with management of GIAC Enterprises to explain to them the process of verification and the possible it could on production of the machines being targeted. We will also review the contract to perform the verification. This contract states that we will take every precaution to minimize disruption of service, but also that we are not liable for any down time or loss of data. We stress the importance of having all data backed up prior to starting the verification. We have explained to GIAC Enterprises that they might want to communicate the audit to the ISP in case they see/capture unusual traffic.

- We will also sign a Non-Disclosure Agreement (NDA) to verify that we will protect GIAC Enterprise’s confidential information.

- Verification during least productive time:

An analysis will be performed to determine the appropriate time of day and the day of the week to conduct the verification. The objective is to choose a day and time that will be least disruptive to business services. This can be a challenging task since GIAC Enterprises is a 24-7 company that conducts business globally. Also, it would be good policy to notify key support personnel (i.e. - partners, suppliers, local users) that access to certain resources could be affected during this audit/verification process.

This would also be an ideal time to stress to these key personnel that this action is to ensure proper security for GIAC Enterprises systems which would also protect them as they interact with

- Once the best time has been determined, the next task is to determine the technical approach to assess the firewall. Several tools/utilities will be utilized:
 - NMAP
 - ICMP-Ping
 - Firewall tracker (log file)
- Identifying Risks

1. Possible corruption or loss of data- therefore all critical information will be backed up properly.
 2. Disruption of Service- this is why it is critical to choose the best time to perform the analysis.
- Calculate the cost of the analysis-- based on Lance Spitzner's ³¹
 - Features
 3. Identify the Team
 4. Plan tools and tests to run
 5. Conduct the analysis
 6. Analyze the findings
 7. Report findings to GIAC Enterprises management

We have a 3-person team identified for GIAC Enterprises. They will be working in tandem. They are very experienced working together and very effective.

They will begin their analysis with Nmap by running several scans. They will analyze these scans and determine appropriate follow-up scans based on the findings from these scans.

They plan 4 hours to "inventory" the architecture of GIAC Enterprises. This is to check equipment and look for possible problem areas.

They estimate the initial scans to take 4-5 hours and an additional 3 hours to analyze the findings.

If additional scans are needed, it will be estimated for an additional 10 hours.

Reporting the findings to management generally averages 3-4 hours- so they will estimate with the 4 hours.

Total = Minimum 16 hours x \$150 per hour = \$2400
Maximum 26 hours x \$150 per hour = \$3900

- B. Conduct the validation- the audit will take place from 3 locations
 - a. from an internal machine on the intranet of GIAC Enterprises
 - b. from the Untrusted network
 - c. from a machine located on the service network

Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version)

they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.³²

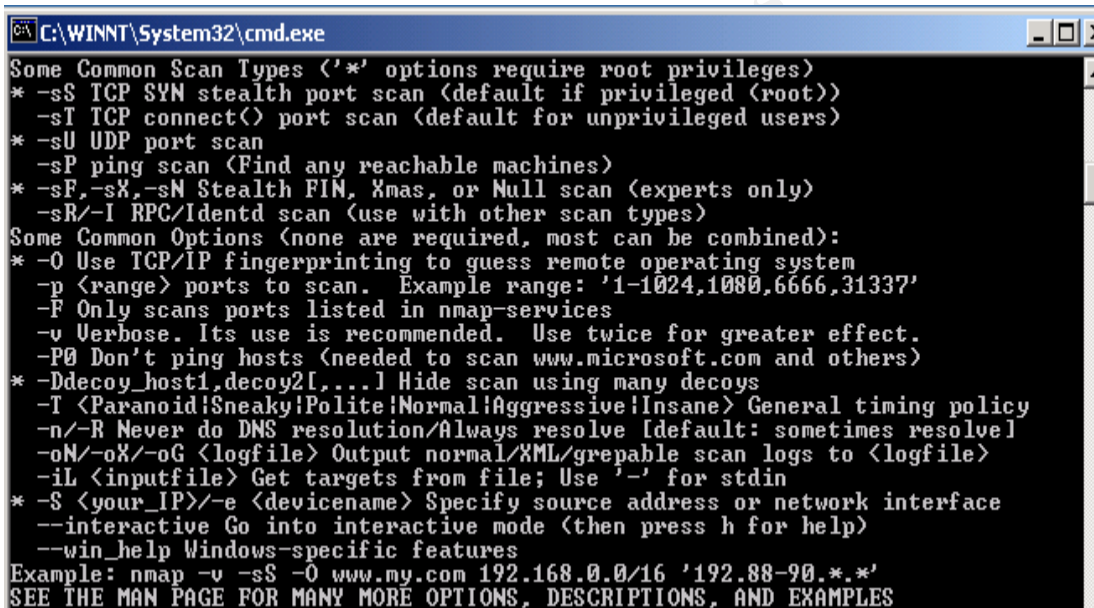
Nmap – When Nmap scans ports; it can report the ports to be:

Open- the port is open and listening.

Filtered- there must be a filtering device- and Nmap cannot determine the state of the port.

Closed- not listening.

The following figure demonstrates some of the possible commands used with Nmap.



```

C:\WINNT\System32\cmd.exe
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid!Sneaky!Polite!Normal!Aggressive!Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
  
```

1. Scans from the intranet of GIAC Enterprises with IP address – 10.10.10.5

Ping scan

```

D:\>ping 10.10.10.4

Pinging 10.10.10.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

This is the expected outcome of a Ping probe. Ping probes should be blocked and therefore return a 'Request timed out' response.

Note: All of our Nmap scans had to include the `-P0` command, because the host would appear down as it was blocking the PING command.

This SYN scan locally shows us that 1601 ports were scanned and all are filtered.

```
C:\NMapWin>nmap -sS -P0 10.10.10.4
Starting nmap V. 3.00 ( www.insecure.org/nmap )
All 1601 scanned ports on gefw1 (10.10.10.4) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 1719 seconds
```

SYN scan to the Mail Relay machine on Service Network #1.
This SYN scan locally show port 80 filtered.

```
C:\NMapWin>nmap -n -sS -P0 -p80 10.10.10.2
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on (10.10.10.2):
Port      State      Service
80/tcp    filtered   http
Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

This scan was performed to verify that port 25 for SMTP was available on the firewall and it was verified that it is open and being filtered.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host (10.0.0.6) appears to be up ... good.
Initiating SYN Stealth Scan against (10.0.0.6)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on (10.0.0.6):
Port      State      Service
25/tcp    filtered   smtp
Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

This scan also verifies that port 443 for https is open and filtered.

```
C:\Program Files\NMapWin>nmap -sS -P0 -p443 -vv 10.10.10.4
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host (10.10.10.4) appears to be up ... good.
Initiating SYN Stealth Scan against (10.10.10.4)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on (10.10.10.4):
Port      State      Service
443/tcp   filtered   https
Nmap run completed -- 1 IP address (1 host up) scanned in 44 seconds
```

SYN scan from remote machine on Service Network to an intranet machine and it was blocked from firewall.

```
D:\Program Files\NMapWin>nmap -sS -P0 10.10.10.4
Starting nmap U. 3.00 < www.insecure.org/nmap >
All 1601 scanned ports on <10.10.10.4> are: filtered
Nmap run completed -- 1 IP address <1 host up> scanned in 1724 seconds
```

55	27Apr2004	17:51:14	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
56	27Apr2004	17:51:19	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
57	27Apr2004	17:51:25	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
58	27Apr2004	17:51:31	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
59	27Apr2004	17:51:40	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
60	27Apr2004	17:51:46	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
61	27Apr2004	17:51:52	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
62	27Apr2004	17:51:58	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
63	27Apr2004	17:52:04	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
64	27Apr2004	17:58:13	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
65	27Apr2004	17:58:19	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
66	27Apr2004	17:58:25	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
67	27Apr2004	17:58:31	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1
68	27Apr2004	17:58:37	■■■	←	gefww1	■■■	⊗ TCP	http	VIC	gefww1

TCP connect scan

```
C:\Program Files\NMapWin>nmap -sS -P0 -O -T 4 10.10.10.4
Starting nmap U. 3.00 < www.insecure.org/nmap >
Skipping host <10.10.10.4> due to host timeout
Nmap run completed -- 1 IP address <1 host up> scanned in 301 seconds
```

This scan timed out- and the firewall logs proves that it was dropped.

76	28Apr2004	0:56:30	■■■	←	gefww1	■■■	⊗ TCP	http		
77	28Apr2004	0:56:35	■■■	←	gefww1	■■■	⊗ TCP	http		
78	28Apr2004	0:56:41	■■■	←	gefww1	■■■	⊗ TCP	http		
79	28Apr2004	0:56:47	■■■	←	gefww1	■■■	⊗ TCP	http		
80	28Apr2004	0:56:53	■■■	←	gefww1	■■■	⊗ TCP	http		

Plus, included is the Record Detail for Log 76. This proves useful information when analyzing the log file for Checkpoint.

Record Details	
Number	76
Date	28Apr2004
Time	0:56:30
Product	VPN-1 & FireWall-1
Interface	EL90BC0
Origin	gefww1 (10.10.10.4)
Type	Log
Action	Drop
Protocol	tcp
Service	http (80)
Source	VIC (10.10.10.5)
Destination	gefww1 (10.10.10.4)
Rule	
Source Port	42381
User	
Information	TCP packet out of state: First packet isn't SYN tcp_flags: ACK

2. Audit and results from untrusted port on the firewall Address of audit machine – a.b.c.8

ping 10.10.10.4

```
D:\>ping 10.10.10.4
Pinging 10.10.10.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This is the expected outcome of a Ping probe. Ping probes should be blocked and therefore return a 'Request timed out' response.

Note: All of our Nmap scans had to include the `-P0` command, because the host would appear down as it was blocking the PING command.

Although this is not the real output, it should look something like this:
Port 80 and 443 are filtered to allow for web access.
Port 25 is also filtered to allow for email communication.

3. Audit and results from a machine located on the Service Network #1 Audit address 192.168.1.7 to

ping 10.10.10.4

```
D:\>ping 10.10.10.4
Pinging 10.10.10.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This is the expected outcome of a Ping probe. Ping probes should be blocked and therefore return a ‘Request timed out’ response.

Note: All of our Nmap scans had to include the `-P0` command, because the host would appear down as it was blocking the PING command.

NOTE:

Just as an additional scan we tried to spoof a VPN machine and the results are demonstrated below:

The next 2 windows from Ethereal and FW log are interesting. I changed my scan machine to an IP address of one of the VPN gateways and the firewall log picked up packets as being spoofed.

Source	Destination	Protocol	Info
10.0.0.6	Broadcast	ARP	who has 10.0.0.5? Tell 10.0.0.6
10.0.0.2	10.0.0.6	TCP	[TCP Zerowindow] 18192 > 2757 [RST, ACK] Seq=0 Ack=0 win=0 Len=
10.0.0.2	10.0.0.6	TCP	[TCP Zerowindow] [TCP Dup ACK 2#1] 18192 > 2757 [RST, ACK] Seq=
10.0.0.2	10.0.0.6	TCP	[TCP Zerowindow] [TCP Dup ACK 2#2] 18192 > 2757 [RST, ACK] Seq=
10.0.0.6	Broadcast	ARP	who has 10.0.0.5? Tell 10.0.0.6
10.0.0.6	Broadcast	ARP	who has 10.0.0.5? Tell 10.0.0.6
10.0.0.6	Broadcast	ARP	who has 10.0.0.5? Tell 10.0.0.6
10.0.0.2	10.0.0.6	TCP	[TCP zerowindow] 18192 > 2763 [RST, ACK] Seq=0 Ack=0 win=0 Len=
10.0.0.2	10.0.0.6	TCP	[TCP Zerowindow] [TCP Dup ACK 8#1] 18192 > 2763 [RST, ACK] Seq=
10.0.0.2	10.0.0.6	TCP	[TCP Zerowindow] [TCP Dup ACK 8#2] 18192 > 2763 [RST, ACK] Seq=

gefw1	TCP	CPD_amon	gefw1	laptop	2698	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2698	message_info: Local interface address spoofing
VPN-1 & FireWall-1	TCP	CPD_amon	gefw1	laptop	2698	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2704	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2704	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2704	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2710	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2710	message_info: Local interface address spoofing
gefw1	TCP	CPD_amon	gefw1	laptop	2710	message_info: Local interface address spoofing

Summary of Results

During the initial analysis we have found that the ruleset on our firewall is functioning properly. Care must be taken to not assume that this initial evaluation of the rules is “all” inclusive!

Security personnel MUST stay current with updates and also with ‘new” attacks that are being created on a daily basis. These new attacks could indicate new rules or policies that must be implemented on either the firewall or the router to prevent attack.

Also, there are several suggestions to GIAC Enterprises for future expansion needs and as the budget allows.

1. Using two separate ISP’s
 - a. This will allow for redundancy and bandwidth
 - b. This will also assist in possible DDOS attack. GIAC Enterprises could to reroute needed traffic through another border router.
2. Implementing a second redundant border router. This will become necessary as the second ISP is implemented into the security policy.
3. Adding an addition internal router and firewall. This allows for additional security behind the initial border router and main firewall. Placement of these devices will be decided upon a further needs assessment at that time.

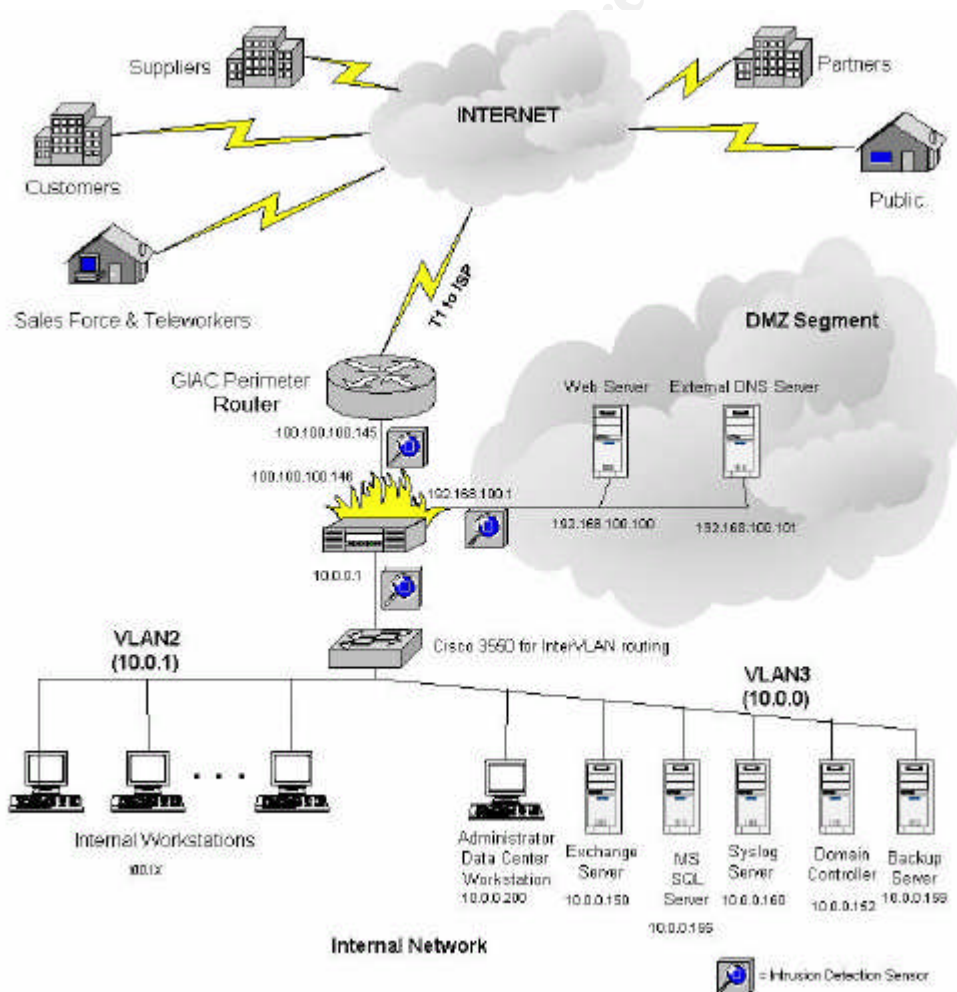
4.0 Designs Under Fire

Assignment 4, Design Under Fire, will consist of several components:

- Choose a GCFW practical that has been submitted within the last 6 months and include the URL and the network diagram.
- Design an attack against the firewall.
- Devise a distributed denial of service.
- Plan an attack to compromise an internal system

For this part of the assignment, I have chosen to attack the practical assignment by Brian C. Rudzonis submitted in February 2004. The practical assignment can be found at http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf.

The network diagram is displayed below:



I have chosen to attack giac.com because I received my “walking papers” because of their “new” business status (e-commerce) and increasing their security policies. They have hired some new IT staff with more experience that “fits” their new posture in the e-commerce field. They didn’t even give me a chance to show that I could manage their security infrastructure. So, I have decided that I will demonstrate my skills while I sit at home looking for a new job!!! I know they have made some changes since I left so I am going to have to start from scratch as if I don’t have any information about GIAC. “AKA- The Disgruntled Employee”

4.1 Attack against the firewall

During this phase, I am trying to gather as much information about the security at GIAC Enterprises as possible without penetrating the network. This is sometimes called footprinting. I like to call it “casing the joint”.

First, I must plan what information that I am trying to gather and the scope of my footprinting. Footprinting can gather several kinds of information for you:

- Locations
- Related companies
- Phone numbers
- Contact names and emails
- Links to other web servers, etc

Many times footprinting begins with the web page for a company and that is where we will begin also.

The source code for web page information can be buried in the html code that the public actually does not see. Plus, having the source code can allow you to search for information directly from the source instead of weeding through links, etc.

To countermeasure this activity, scan/analyze your source code and remove any unnecessary information.

I can also use the “ping” utility to gather some more information about GIAC Enterprises. I can “ping” IP addresses that I have gathered in previous tools to verify that they are live hosts.

To countermeasure against the “ping” utility block this request at the border router.

Using these tools will give me an idea of the address space for giac.com and then start probing with the information these utilities give me.

My next step is to conduct a domain query. This could possibly give me more information about GIAC Enterprises. The command is a “whois” query from <http://ws.arin.net/cgi-bin/whois.pl>

ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN. ARIN's database contains IP addresses, autonomous system (AS) numbers, organizations or customers that are associated with these resources, and related Points of Contact (POCs).

ARIN WHOIS Database Search

<http://ww1.arin.net/whois/>

Search for :

Enter IP address of “giac.com”- the IP address can be found by doing a Ping command for the host name of giac.com

This query can give me very useful information:

- Address/phone info
- Network address range
- CIDR

There are other query registers that can give me other information. For example, using the “whois” utility at Network Solutions provides the following information.

- Domain name
- Administrative contact
- Technical contact
- Domain servers “listed in order”
- Date of the domain registration

WHOIS information is used in several ways: (*Network Solutions*)

http://www.networksolutions.com/en_US/whois/index.ihtml

- Registrars (domain name providers) use it to validate requests to transfer a domain name registration to another domain name holder (registrant) or registrar.
- Many individuals and businesses use it to find out when a domain name registration they want is due to expire.
- Law enforcement agencies use it for investigations into illegal activities on the Internet.
- Intellectual property rights holders use it to contact individuals or companies that may be violating their intellectual property rights

How to use the information from the query:

The administrative contacts can be very useful information because many times that person might also be in charge of the security posture of the company (i.e. router, firewalls, etc). With this information I could then use social engineering to gather more information. Another useful tool is social engineering. I will call up GIAC Enterprises and talk to the receptionist that answers the phone. Since I am afraid that the receptionist might recognize my voice, I have a buddy is very willing to help me. There are many ways to social engineer information. We could pretend to be conducting a service call and just wanting to see how their firewall is performing. Hopefully, whoever answers the phone will give us some information about their equipment they are using if engineered properly.

Countermeasure for this information from *Network Solutions*:

“Network Solutions’ online Account Manager lets you assign multiple Administrative and Technical contacts for a single domain name account, and choose which of these contacts appears in the public WHOIS database. Account Manager also allows you to set up alternate contact information expressly for the public WHOIS database. These account permissions can be changed easily without sharing passwords or affecting your account. To designate an Account Contact to appear in WHOIS, you must first establish a Network Solutions User ID for the contact, using a valid e-mail address.”

Now that I have some useful information to start with, I have decided to check on GIAC Enterprises DNS configurations. “One of the most serious misconfiguration a system administrator can make is allowing untrusted Internet users to perform a DNS zone transfer. A zone transfer allows a secondary master server to update its zone database from the primary master”³³ The configuration should only allow the zones to be transferred between the primary and secondary DNS servers. However, if they are misconfigured the DNS server could possibly allow the information to be transferred to anyone who asks!

DNS information can be obtained by using the nslookup utility.

```
C:\>nslookup _
```

After the “nslookup” command just enter the domain name- giac.com

It could possibly return the following information:

Default server- many times this is the DNS server also
IP address of this server

The next step is to go into interactive mode with the following command:

```
> set type=any  
> ls -d giac.com. >> /tmp/zone_out
```

1. *set type= any* -This will allow us to pull any DNS records that are available.

2. `ls -d (domain name) >> /tmp/zone_out` -asks for any records for the specified domain.

To countermeasure against DNS queries, there are several options. The one that I am going to recommend is to configure either the router or the firewall to deny all unauthorized inbound connections to TCP and UDP port 53.³³ Name lookups are UDP and zone transfers are TCP.

Our query does not pull up any useful information, so we will move on to the next tool to footprint GIAC Enterprises.

The next utility we are going to try to pull information from GIAC Enterprises is tracerouting.

```
C:\>tracert giac.com_
```

Press "enter"

This utility will allow us to follow an IP packet from our source to the destination and show us the host path that it follows up to default maximum hop count of 30. The traceroute will end at our destination. Typically the last hop before the destination will be the border router. To countermeasure this utility, routers should be configured to deny source-routed packets. Since our last few hops "timed out" it is safe to say that Mr. Rudzonis has enable this option on the router.

IDServe from Gibson Research is another useful tool when doing a reconnaissance against a web site³⁴. This tool gives me information about the web server at GIAC Enterprises. With this information I can then look at vulnerabilities against the Internet server and possibly another route into GIAC Enterprises network.

A reconnaissance (footprinting) mission would not be complete without the use of Nmap.

Here are the scans we would use:

SYN scan: `nmap -sS -PT -PI -O -vv` - looking for open ports

FIN scan: `nmap -sF -PT -PI -O -vv`

UDP scan `nmap -v -sU -sR -O -P0-p1-65535 -n 192.168.100.1`

Once we have concluded the probing mission, we find that Mr. Rudzonis is using a Pix 515E 6.3(2) as his firewall. Huh, they told me they were going to make changes! The next thing we did is to start doing some research to find the vulnerabilities associated with the Pix firewall. Several were identified:

1. OpenSSL ASN.1 parsing³⁵

This vulnerability sends corrupt client certificates to the SSL server which will result in a possible crash of the system.³⁶

This information was researched at *Computer Associates- Vulnerability Information Center*.

<http://www3.ca.com/threatinfo/vulninfo/vuln.aspx?id=26160>

Impact: Remote attackers can cause a denial of service condition or possibly execute arbitrary code.

Root Cause: Software Vulnerability

OpenSSL contains multiple vulnerabilities that may allow remote attackers to cause a denial of service condition or possibly execute arbitrary code.

The first issue is due to improper deallocation of data structures holding ASN.1 encodings that are rejected by the parser. Remote attackers can exploit the vulnerability to cause a denial of service condition or potentially execute arbitrary code.

The second issue is due to insecure handling of improper ASN.1 tag values.

The third vulnerability is due to the way certificates with invalid public keys are processed. If the verify code is set to ignore all errors, such a certificate would cause a crash. Note that errors are set to be ignored only for debugging purposes. Attackers can exploit these issues to cause a denial of service condition. Additionally, due to an error in the SSL/TLS protocol handling, all client certificates are parsed by the server even when client authentication is not enabled. Note that the first issue does not affect OpenSSL 0.9.6.

Cisco PIX Firewall:

This vulnerability is fixed in software release 6.3-

Countermeasure for this attack is a software upgrade from Cisco

Since he has already upgraded to Cisco 6.3, this will not be vulnerability.

2. SNMPv3

The SNMP protocol in the Pix Firewall³⁷ has a known vulnerability that could allow for a Denial of Service attack on the firewall. The Pix will crash and then reload. This vulnerability can also be set from a remote source. If the Pix is continually having to reload, it can cause a DOS and possibly allow for other attacks during the vulnerability.

<http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.pdf>

Countermeasure: This could cause a Denial Of Service on the Pix and Cisco is offering free upgrades and patches to mitigate this vulnerabilities

3. TCP Vulnerability

http://cisco.com/en/US/products/products_security_advisory09186a008021bc62.shtml

This information was gathered from *Cisco - TCP Vulnerabilities in Multiple IOS-Based Cisco Products*

“A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain a TCP stack are susceptible to this vulnerability.”

As a general rule, all protocols where a TCP connection stays established for longer than one minute should be considered exposed

The only way to exploit these vulnerabilities is to see if the system has been patched. Since Mr. Rudzonis has been very thorough throughout his practicum it is assumed that he has patched these vulnerabilities especially since they are already publicized. The most danger from vulnerabilities is when they are exploited before the exploit and mitigation is announced. In addition, Mr. Rudzonis has denied SNMP at the router level, so this vulnerability will not affect his security policy.

4.2 A distributed denial of service (DDOS)

A DDOS is a type of denial of service where the denial of service is where the attacks come from many hosts.

http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt

There are several common components to carrying out a DDOS attack.

1. Client - an application that can be used to initiate attacks by sending commands to other components
2. Daemon - a process running on an agent responsible for receiving and carrying out commands issued by a client.
3. Master - a host running a client
4. Agent - a host running a daemon
5. Target - the victim (a host or network) of a distributed attack

The tool we will be using to conduct the DDOS will be Tribal Flood Network 2000 (TFN2K).³⁸

<http://staff.washington.edu/dittrich/misc/tfn.analysis>

This section will detail a method to compromise a 50 Cable/DSL system and subject the design to a DOS attack from the compromised systems. The first task is to identify a target of our 50 host (aka zombies) computers. This can be accomplished fairly easily. Since we are going to be using Cable/DSL users, they typically do not have the in-depth security policy that most enterprises incorporate nor do they usually keep regular updates and patches. Plus, even though ISP providers use DHCP servers to assign IP addresses to their users most end users maintain an IP for an extended period of time. With this knowledge, we can use scan utilities to find open systems to be hosts for our DDOS.

Ideally we would like to select targets from different ISPs, different geographic regions and several “hops” away from the target as this makes it harder to trace back to the origin.

I have decided to use spam mail to identify the 50 systems needed for the DDOS. In the email will be a Trojan to allow us access to the system once the Trojan has been installed. We are counting on some users still not “Internet” savvy and can be drawn into some kind of “great deal” sales ad. The Trojan will be configured to listen on port 80 and create a backdoor there to enter. There are many Trojans on the market but I have decided to use Sub7.

<http://netsecurity.about.com/cs/hackertools/a/aa032603a.htm>

“Installing Sub7 will open a backdoor (enabling a port that you are not aware is open) and contact the attacker to notify them that Sub7 is installed and ready to go. This is when the fun begins (for the hacker at least).” (*Netsecurity*)

Now that I have my list of IP addresses (zombies) to use with Trojan backdoor installed, I will begin to download the TFN2K program to these machines. When each machine restarts, the program will actually be installed.

“TFN2K uses a client/server mechanism where a client issues commands simultaneously to a set of TFN2K servers. http://vil.nai.com/vil/content/v_10535.htm

Once we have finalized the list of our 50 compromised hosts, we upload the Tribal Flood Network 2000 (TFN2K) client and agents to the systems using the Mydoom Upload/exploit code described above

TFN2K uses random TCP/UDP ports and/or ICMP Echo Replies. TFN2K will send multiple packets along with decoy packets making it difficult to track the source of each packet. We are going to launch TFN2K against the external DNS server. If we can successfully launch TFN2K against the DNS server it will possibly disrupt services. We found the DNS Server by using the “whois” record. Since the attack is against the DNS service the packets will need to traverse both the router and firewall to reach the DNS Server thereby possibly hampering their ability to analyze packets. If the attack is successful against the DNS server then GIAC Enterprises will possibly be unable to resolve names and thus not allowing Internet connectivity.

Commands that can be used for TFN2K-

<http://staff.washington.edu/dittrich/misc/tfn.analysis>

usage: ./tfn <iplist> <type> [ip] [port]

<iplist> contains a list of numerical hosts that are ready to flood

<type> -1 for spoofmask type (specify 0-3), -2 for packet size,

is 0 for stop/status, 1 for udp, 2 for syn, 3 for icmp,

4 to bind a rootshell (specify port)

5 to smurf, first ip is target, further ips are broadcasts

[ip] target ip[s], separated by @ if more than one

[port] must be given for a syn flood, 0 = RANDOM

We will be attacking TCP/UDP port 53 for the DNS attack.

The attack could also be directed at the ports commonly open: 80, 25, 443, 135-139 and 445.

Countermeasures:

Latest patches and update

Standard precautions against this DoS attack method: (Network Associates)

* implement egress and ingress filtering

* implement rate limit on ICMP packets

* implement rate limit on SYN packets

* become knowledgeable about the security breaches possible by reviewing the latest advisories for the systems you may be using

Common Mitigation/Countermeasures against DDOS³⁹

First, the router logs should be analyzed to determine the source IP addresses for this attack. Then the addresses can be added to the ACL.

Secondly at <http://www.packetstormsecurity.org/distributed/zombie/> there is a tool called Zombie Zapper v1.0⁴⁰. It is a free, open source tool that can talk to a zombie system and basically stop the flood of packets. It works against Trinoo, TFN, and Stacheldraht.

Thirdly, contacting the ISP and informing them of the attack on your system and asking for their assistance is stopping the attack with their systems. For example, implementing some form of filtering on the router that services your network.

It should be noted that Mr. Rudzonis mentions in his practicum that he has established a good relationship with his ISP with the specific purpose to halt DOS attacks. This is an excellent relationship to have when developing a “defense in depth” policy!

4.3 An attack plan to compromise an internal system

I have chosen to attack an internal workstation on VLAN2. Mr. Rudzonis mentions that they use Microsoft products internally. I didn't think they would change all the internal systems as well. So, I have decided to attack his workstation. Since Mr. Rudzonis was the person who gave me my “walking papers”, I think I will show him some of my skills in technology. I am going to assume that since they are undergoing all these changes, they are neglecting their updates and patches on individual workstations.

I again call on my “buddy” to help. He is going to call and ask for Mr. Rudzonis. Once we have him on the phone, he is going to tell him that he is with a firm that works with some of his main competitors and that his company XYZ has come up with a great tool for tracking Operations. He tells him that he knows he is busy, and will email him the information on the “tool” and attach a demo for him to review at a time that is convenient for him. He also tells him that he is going to ask for a “receipt” when he receives the email so that he knows he has received the tool. This will tell us that he has now installed the malware that is included in his “free” demo. I wait a few days and then I receive the receipt that he has read the email. I am now ready to execute the compromise of his system.

The first thing that I have done is implemented a backdoor to use into his system. This can be accomplished by a variety of utilities. I have chosen to use BackDoor.IRC.Flood.F because it is used for remote control of the compromised host. <http://iet.ucdavis.edu/whatsnew/news2.cfm?id=532>

When Backdoor.IRC.Flood.F is executed, it does the following: (Symantec) <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.irc.flood.f.html>

Creates the following files in the C:\Winnt\Inf folder:

- Conn.txt: This file is not viral itself, and Norton AntiVirus will not detect it.
- Explore.dat: This file is not viral itself, and Norton AntiVirus will not detect it.
- Network.dll: This file is a list of user names and is not viral.
- Nite.exe: This file is a Denial of Service (DoS) Tool, and Norton AntiVirus will detect it as Hacktool.DoS.
- Os32.dll: This is an IRC script.
- Vlxd.bat: This is a batch file that will attempt to launch the IRC client over network shares.
- Vlxd.exe: This is a dropper of the entire rootkit package.
- Vlxd.cfg: This is a configuration file, and Norton Antivirus will not detect this file.
- Winx.dll: This is an IRC script that is not detected.
- Psexec.exe: This file is not viral itself, and Norton AntiVirus will not detect it.
- Pnp11.exe: This file is not viral itself, and Norton AntiVirus will not detect it.
- Smss.exe: This is an IRC client that will connect to a server on port 6667.

When the Trojan is installed then, I will have a backdoor into his system. Now I can use this Trojan in a variety of ways. I could use it to collect information about his system. I could also reboot his machine. I could possibly find passwords or be able to access other systems on the network.

Mitigation:

Personal firewall

Update patches

Well, it appears that the “new” IT staff has done an adequate job of protecting GIAC Enterprises. Maybe I should be my time trying to accomplish more useful experiences and expand my own tool set and knowledge

REFERENCES

1. Online encyclopedia for computer technology
<http://www.webopedia.com/TERM/S/SSL.html>
2. Introduction to SSL
<http://developer.netscape.com/docs/manuals/security/sslin/contents.htm>
3. National Security Agency- Recommended Cisco Configurations
<http://www.nsa.gov/snac/cisco/>
4. Cisco Access Routers White Paper- Quick reference guide
http://cisco.com/application/pdf/en/us/guest/products/ps221/c1031/ccmigration_09186a008017f1d1.pdf
5. Cisco 1760 Modular Access Router
<http://www.cisco.com/en/US/products/hw/routers/ps221/ps227/index.html>
6. Firewall definition <http://www.commerce-database.com/firewall-definition.htm>
7. RFC 1918 - Address Allocation for Private Internets
<http://www.faqs.org/rfcs/rfc1918.html>
8. **The Open Source Network Intrusion Detection System**
<http://www.snort.org/about.html>
9. Dell PowerEdge 6650 Server Details
http://www1.us.dell.com/content/products/productdetails.aspx/pedge_6650?c=us&cs=04&l=en&s=bsd
10. National Security Agency Security Recommendation Guides
<http://nsa2.www.conxion.com>
11. Securing Windows 2000 Step by Step SANS Institute Version 1.5 July 1, 2001
12. Check Point VPN-1/FireWall-1 TCP and UDP Ports used by Next Generation
<http://www.fw-1.de/aerasec/ng/ports-ng.html>
13. The Power behind RSA SecurID Two-Factor Authentication
http://www.rsasecurity.com/products/secuid/whitepapers/AS51_SB_1103.pdf
14. <http://www.rsasecurity.com/products/secuid/>

15. Check Point Software Technologies LTD. FireWall-1Version 4.0 SecuRemote Split/Encrypted DNS Quick Reference Guide Revision 1.4
<http://support.fishnetsecurity.com/public/cppublic/sr-dns.pdf>
16. You Need to Create a Split DNS!- ISA Server
http://www.isaserver.org/tutorials/You_Need_to_Create_a_Split_DNS.html
17. National Security Agency – Central Security Service-Security Configuration Guides
<http://www.nsa.gov/snac/>
18. National Security Agency – Central Security Service-Security Operating Systems Guides- Microsoft Windows 2000 Guides
http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1
19. Symantec Client Security- Protect your business from viruses and hackers
http://www.symantec.com/smallbiz/scs_sbe/index.html
20. <http://www.sans.org/awareness/>
21. Inside Network Perimeter Security Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey, Ó New Riders Publishing 2003
22. NSA/SNAC Router Security Configuration Guide Executive Summary Card Version 1.1 I Executive Summary
<http://nsa2.www.conxion.com/cisco/guides/cis-1.pdf>
23. Router Security Configuration Guide- Principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers
<http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>
24. Cisco Press First-Year Companion Guide 2002 Cisco Press
25. <http://www.ntp.org/ntpfaq/NTP-s-def.htm>
26. INTERNET PROTOCOL V4 ADDRESS SPACE - The allocation of Internet Protocol version 4 (IPv4) address space to various registries
<http://www.iana.org/assignments/ipv4-address-space>
27. DShield- Top 10 Most Wanted Offenders <http://www.dshield.org/top10.php>
28. CCSA, CCSE, & NSA Book 1 Part 1, Vigilar 2004
29. http://www.giac.org/practical/GCFW/Jonathon_Berry_GCFW.pdf

30. <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp>
31. Auditing Your Firewall Setup <http://www.spitzner.net/audit.html>
32. Insecure.Org is pleased to announce the immediate, free availability of the Nmap Security Scanner version 3.50 from <http://www.insecure.org>
33. McClure, Stuart, Scambray, Joel, Kurtz, George Hacking Exposed- Fourth Edition, McGraw-Hill, 2003
34. ID SERVE Simple-to-use Internet Server Identification Utility <http://www.grc.com/id/idserve.htm>
35. OpenSSL ASN.1 parsing <http://securityfocus.com/bid/8732/discussion/>
36. Brute forcer for OpenSSL ASN.1 parsing bugs <http://downloads.securityfocus.com/vulnerabilities/exploits/ASN.1-Brute.c>
37. <http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.pdf>
38. Tribal Flood Network 2000- University of Chicago <http://security.uchicago.edu/seminars/DDoS/tfn2k.shtml>
39. Mitigation/Countermeasures against DDOS- <http://www.saic.com/healthcare/distributeddenial.pdf>
40. Packet Storm <http://www.packetstormsecurity.org/distributed/zombie/>
41. <http://www.nwinternet.com/~pchelp/bo/bo.html>
42. The Back Orifice "Backdoor" Program YOUR security is at risk. <http://www.cultdeadcow.com/tools/bo.html>

Additional References:

- Brenton, Chris. et al. TCP/IP, SANS Institute. 2003.
- Brenton, Chris. et al. Packet Filters, SANS Institute. 2003.
- Brenton, Chris. et al. Firewalls, SANS Institute. 2003.
- Brenton, Chris. et al. Defense in Depth, SANS Institute. 2003.
- Brenton, Chris. et al. VPNS, SANS Institute. 2003.
- Brenton, Chris. et al. Network Design and Assessment, SANS Institute. 2003.