Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Firewall Analysis Certification Practical Assignment

Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks

Version 1.6

Perimeter Security using Check Point FireWall –1 4.1

By Glenn Brengel

SANS Institute Cyber Defense Initiative Washington, DC
December 3 – 8, 2001

A Perimeter Security Design for a Hypothetical Online Company

GIAC Enterprise Fortune Cookie Inc.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A Perimeter Security Design for a Hypothetical Online Company

GIAC Enterprise Fortune Cookie Inc.

"May your path to certification be paved with the knowledge gained"

© SANS Institute 2000 - 2002 Author retains full rights.

Assignment 1 – Security Architecture

1.1 Define a security architecture for GIAC Enterprises, an e-business that deals in the online sale of fortune cookie sayings.

The starting point for any security architecture should begin with proper planning. Before planning the security architecture, we need define what it is we are securing. We know upfront that we will have an e-business that is connected to the Internet. The Usage Policy is where we will start and from there begin to define the security architecture. The usage policy is not designed to restrict the GIAC workers, but is used in sure the security of the corporation as a whole.

Outbound or Internet access for the internal GIAC employees is not an open door policy. For example the corporate firewall blocks access to gotomypc.com and to AOL's IM servers.

In the interest of brevity, I will not take time and space to define the entire usage policy here, but I will mention a few of the major points. The usage policy will include a requirement for strong passwords on all of the corporate devices. The end user machines for example, will have password restrictions based on length, number of days, failed login attempts and reuse of old passwords. The strong password policy is of critical importance on all administrator or root accounts. The concept seems so obvious, but it is often overlooked or poorly enforced. The existence of a solid password policy can go a long toward addressing security weaknesses and preventing unauthorized access from both outside and inside the company.[1]

Modems will not be installed on internal corporate machines. Laptop machines do have modems that will be used for remote access, but these machines will also contain a personal firewall – which will be discussed in greater detail later in the paper.

*1.2 Your architecture **must** consider access requirements (and restrictions) for: Customers, Suppliers, Partners, and GIAC Enterprises.*

1.2.1Customers (the companies that purchase bulk online fortunes)

Customers: The customers are made up of numerous companies that buy bulk online fortunes for their fortune cookies. GAIC's largest customer is www.fancyfortunecookies.com, who

[1] Berhstein, Terry, et al., Internet Security for Business, New York, NY: John Wiley & Sons, 1996, page 33

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

claims to be the World's largest manufacturer of gourmet fortune cookies.[2] The customers connect to the web server in the GIAC Fortune Cookie Service Network via http and https (ssl) to buy the fortunes. Customers are limited to http and https access to the web servers on the service network. The customers can also make use of the dns services and mail server, as anyone can. Customers have do not have access to the ftp server or any access into the GAIC Enterprises internal networks.

While GIAC is interested in doing business with almost anyone, I will mention here that not quite everyone one on the Internet will have access to our Web server or Service Network. The known "Bad Guys" as listed on www.incidents.org will be blocked on our board router and firewalls as well as any would be hacker to our networks. There is also some consideration being made to block entire countries where Internet attacks commonly originate, like China for example. However, blocking the country of China would not be in the best interest of our business needs. GAIC will consider blocking other countries based on future analysis of hacking threats vs. sales data.

1.2.2 Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);

Suppliers: Confucius Say, Inc. supplies fortune cookie sayings to GIAC Enterprises, by connecting to the GIAC Fortune Cookie Service network FTP server to "put" new sayings. The supplier connects by way of a Gateway-to-Gateway VPN solution, in which their IKE firewall gateway is configured to form a VPN tunnel with the GAIC Fortune Cookie Firewall. Remote supplier employees have been granted access via SecuRemote and have the same ability to securely ftp files to the GFC FTP Server. While the supplier can and does access the web, mail, and DNS servers, they are restricted from all other access to the service and corporate networks of GIAC Enterprises.

1.2.3 Partners (the international partners that translate and resell fortunes)

Partners: The GIAC Fortune Cookie partners (including Chinese Translations, Inc., Great Wall Translations, Int. and Ming Fortunes Ltd.) are international companies that translate and resell the fortunes. The partners connect to the GIAC Fortune Cookie Service network web server and ftp server to get the fortunes authored by the Supplier and put the translations back on the ftp server. The partners connect via Firewall-to-Firewall solution that provides an encrypted tunnel. Remote users from the partner companies can access via SecuRemote. While the partner companies can, and do, access the web, mail, and DNS servers, they are restricted from all other access to the service and corporate networks of GIAC Enterprises.

1.2.4 GIAC Enterprises (the employees located on GIAC's internal network).

GIAC Enterprises: The company usage policy and the network design define the access of the GIAC employees. The internal network has, for the most part; unlimited access to the Internet, but the internal network only has limited access to the GIAC Fortune Cookie Service Network. The Network Operation Center (NOC) network has full access to the Service network, but does not have access to the Internet. The internal network extends into the NOC location to give the

[2] www.fancyfortunecookies.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

engineers the ability to connect to the Internet, but only from their laptops. Remote access is provided to the telecommuting and mobile GIAC employees via SecuRemote, but the access is limited. There is no remote access into the NOC network.

*1.3 You **must** explicitly define how the business operations of GIAC Enterprises will take place. How will each of the groups listed above connect to or communicate with GIAC Enterprises?*

GIAC Enterprises has formed a wholly owned subsidiary – GIAC Fortune Cookie Inc., also known as GFC. The GFC was created to provide, and profit from the, online sale of fortune cookie sayings. GIAC Fortune Cookie obtains the fortune cookie sayings from our supplier, Confucius Say, Inc. The majority of the fortune cookie sayings are in Chinese. Our partners then translate the fortunes and also assist in the resell of the fortunes. GFC uses the translated fortunes to make up the online or web content that is sold to our customers. Customers are companies, rather than individuals, that purchase fortune cookies sayings in bulk online. The customers browse and connect our web server (over http) and place their orders securely by ssl (over https). Order confirmations and business communications are, for the most part, handled by our mail server.

As mentioned above, the customers connect to the GIAC Fortune Cookie over the Internet to the web server. Customer communications begin with e-mails to and from our mail (Microsoft Exchange) server. While we try in encourage online communications, an 800 line is also offered to the customers. The aging practice of calling the customer is also used in some cases – particularly with our larger customers.

The Suppliers and Partner to GIAC Fortune Cookie ftp server over a Virtual Private Network (VPN). The suppliers "put" fortunes on the ftp server. The partners "get" the un-translated fortunes and "put" the translated fortunes on the ftp server. E-mail and the phone system are used to handle communications to and from GIAC.

1.4 How will GIAC employees access the outside world? What services, protocols, or applications will be used?

GIAC employees will connect to the world through the Internet, E-mail and as mentioned, the telephone. The GIAC Internet Usage Policy, which was designed with the assistance of upper management, governs Internet access. Employees can browse the Internet via http and https. Currently, employees can also make use of RealAudio. E-mail is used to a great extent to communicate with the outside world. GIAC employees are currently being denied access to other outbound services to the Internet such as ftp, telnet and ssh. This practice and policy is not being used to punish the GIAC employees, but rather to strengthen our perimeter defenses and protect our corporate assets.

*1.5 In designing your architecture, you **must** include the following components: filtering routers, firewalls, and VPNs to business partners.*

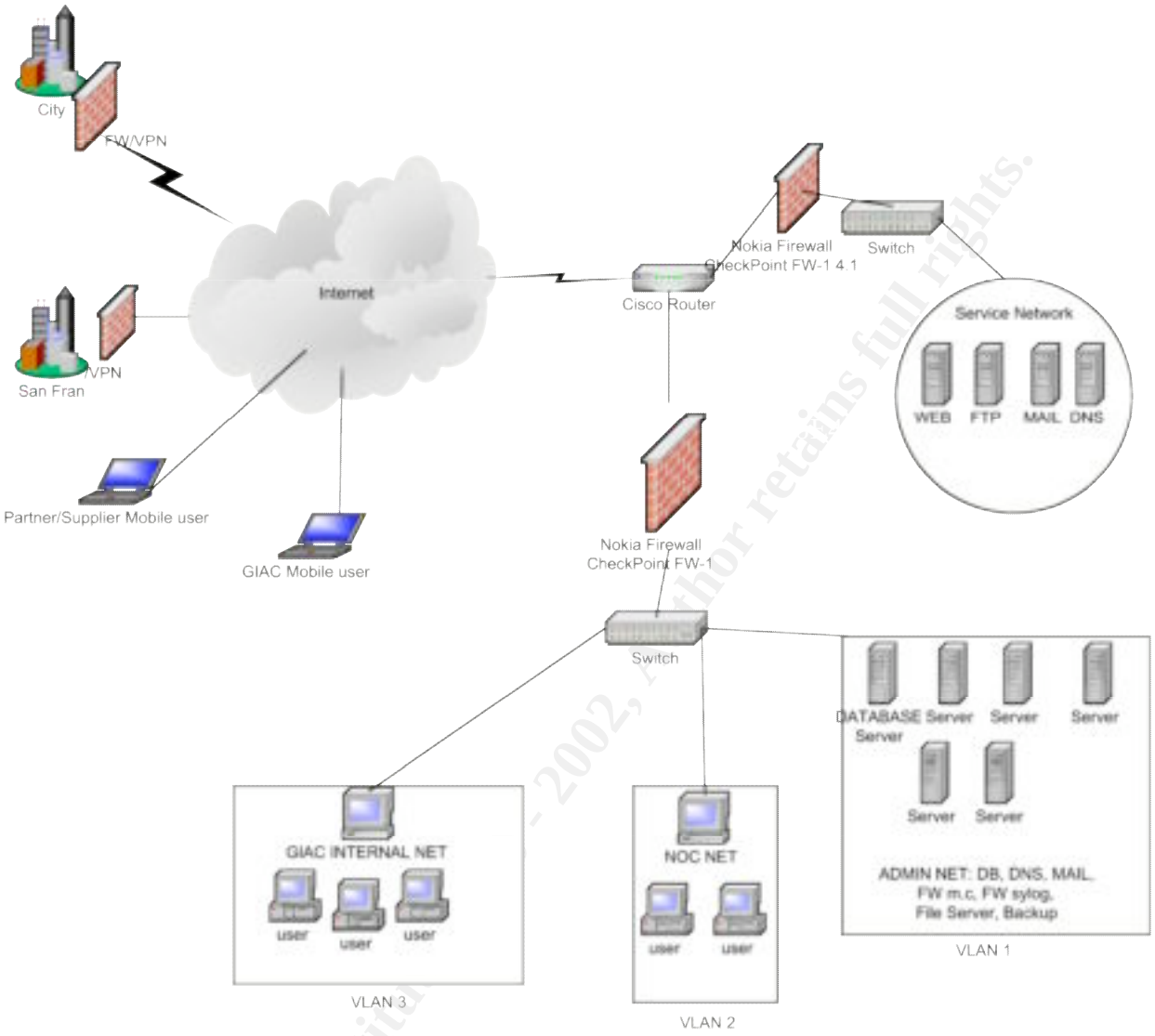
In designing the GIAC Enterprise's perimeter defense, we have chosen to create a number of separate networks. Having the separate networks will assist in our defense against both external

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and internal attacks. The GIAC Fortune Cookie Company (GFC) is driven by its online presence and as such will make up the GFC Service Network. GIAC Enterprises over sees the operations of the GFC and a number of other ventures that are not directly tied to the Internet. The GIAC Enterprises also referred to, as GE or GIAC Corporate, will make up another network. The IT solutions in the GFC and GE Networks will be implemented and administered by the GIAC Network Operations Center (NOC). The GIAC NOC is made up of a third network. The GFC and GE Network are connected the Internet by a boarder router. The boarder router also serves as a filtering router. The router forwards traffic to (and from) the GFC and GE network firewalls – which serve to protection their respective networks. The boarder router also forwards the GIAC NOC traffic to the GFC Service Network – but servers as a filter in not allowing the NOC traffic out on to the Internet. The router and firewalls are aided in the distributing the traffic by switches. Virtual Private Networks (VPNs) have been created off the GFC Firewall to form a secure link with our business partners and suppliers. In the case of our business partner we have formed a Firewall-to-Firewall VPN. In the case of our supplier we have formed a Gateway-to-Gateway VPN solution. The next section will provide an illustration of the network architecture. The filtering router, firewalls and VPNs mentioned above will be discussed in detail in the section following the network diagram.

1.6 Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above.

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



1.7 Provide the specific brand and version of each perimeter defense component used in your design. Include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

1.7.1 Filtering Router:

Build Info: Cisco 12000
IOS Version: 12.0(18)ST

The boarder router will be entry point into GIAC Enterprise through our T1 connection with our ISP UUNET. The router first job, as its name implies, is to route traffic. I n our case it will route traffic to the Service Network Firewall or the Corporate Network Firewall. In addition to routing traffic, our boarder router will be our first line of defense. The router will perform

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ingress and egress static packet filtering through Access Control Lists (ACL) to reduce traffic and threats to our networks. Static packet filtering, however, is weak security and can be fooled by crafted packets.[3] Also note that routers have also been known to leak traffic through when traffic levels are excessive. As mentioned above the routers first job is to route, and as such we now turn to our firewalls.

Cisco's marketing materials at www.cisco.com present the following about the Cisco 12000 router:

> The Cisco 12000 Series is the industry's premier next generation Internet routing platform featuring the capacity, performance, service enablers, and operational efficiencies service providers require for building the most competitive IP backbone and high-speed provider edge networks. With over 20,000 units installed, the Cisco 12000 Series Internet Router is the most broadly deployed high-end IP router in the industry today.[4]

1.7.2 Service Network Firewall

Firewall used to protect Web Server, External DNS Server, and External Mail Server
Nokia IP 440 http://www.checkpoint.com/products/security/platforms/nokiaip440.html
http://www.nokia.com/securitysolutions/platforms/440.html
Loaded with Checkpoint Firewall 4.1

1.7.3 Corporate Firewall:

Firewall used to Protect Internal Network
Nokia IP330 Firewall
Loaded with Checkpoint Firewall 4.1
http://www.nokia.com/securitysolutions/pdf/IP330_global.pdf

http://www.nokia.com/securitysolutions/platforms/330.html

Stateful Inspection Firewall

Check Point's stateful inspection firewall was chosen largely because of its ability to deal with FTP. Stateful inspection allows you to implement a tighter security policy because it able to inspect the packets rather than just the header. Through stateful inspection, the firewall is able to open data ports on the fly and when the session has been completed the ports are closed automatically. This prevents the need to configure the FTP rules by opening the common ports of 21 and 20 as well TCP-high- ports (>1023) as you would on a stateful filtering firewall.[5]

---

[3] SANS Institute Track 2 Firewalls, Perimeter Protection and Virtual Private Networks, 2.2 Firewalls 101: Perimeter Protection with Firewalls, page 67.
[4] www.cisco.com , most broadly deployed high-end IP router in the industry today
[5] SANS Institute Track 2 Firewalls, Perimeter Protection and Virtual Private Networks, 2.2 Firewalls 101: Perimeter Protection with Firewalls, page 101

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Check Points FireWall-1 architecture is based two components: FireWall-1 Inspect Engine and Stateful Inspection. The FW-1 Inspect engine module resides in an operating system's kernel on a driver between datalink and network layers of the OSI model – the lowest software level. The Inspection Engine intercepts and analyzes all packets before they reach the operating system, which saves system processing time and resources. A packet is not passed on to the next higher layer until FireWall-1 has verified that it complies with the security policy. The Inspection Engine stores and updates state context information in dynamic connection tables. These tables provide cumulative data against which FireWall-1 checks during subsequent communications. This is the concept behind Check Point's Stateful Inspection Technology, the key to FireWall-1.

1.7.4 VPNs to business partners

Virtual Private Network (VPN)

The GFC Firewall (Nokia IP 440) listed above is also configured with Check Point's VPN-1 software and serves as the end point of the encryption tunnel used by our Partner and Suppliers.

The Partner's VPN will be a Nokia IP330 IPSO 3.2.1 loaded with Check Point 4.1 VPN-1 / FW-1 SP-5.

The Supplier's VPN will be form through a Gateway-to-Gateway Solution on a Cisco PIX 535.

*1.8. "Options" Your architecture **may** also include the following optional components if they are appropriate to your design: secure remote access*

As mentioned above and listed in the network diagram, secure remote access is provided to mobile and telecommuting GIAC employees as well as our partner and suppliers.

Secure Remote Access is provided through Check Point VPN-1 SecuRemote.
VPN-1 SecuRemote Version 4.1 SP5
Build number: 4199

http://www.checkpoint.com/techsupport/downloads_sr.html

1.9 Additional Devices used in Design

A management console server will be used to remotely manage the Service and Corporate Network Firewalls.

Sun E 250
Solaris
SunOS 4.x/5.x Systems Management MIB, Concord Communications, Inc.
2 X UltraSPARC-II 296MHz
296 Mhz with 2.0 Mb Cache

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A dedicated Logging Server will be used for the Check Point Logging GUI.

Sun Netra t1 105
Solaris
SunOS 4.x/5.x Systems Management MIB, Concord Communications, Inc.
2 X UltraSPARC-II 296MHz
296 Mhz with 2.0 Mb Cache

Tiny Personal Firewall will be loaded on all GIAC Enterprise laptops.
Tiny Personal Firewall Build Info: Build 2.0.15 October 17, 2001 (1416KB), Win 9x, ME, 2000, NT & XP

1.10 Additional Notes and Information

Proxy servers were considered for the Service Network, but because of limitation related memory issues and processing time we chose not to implement them. GIAC Fortune Cookie predicts that business generate too much traffic for a proxy server solution, particularly for the web server.

The Cisco Pix firewall was strongly considered for both the Service Network and the Corporate Network, but we did not want to have all of our perimeter defense solutions to be manufactured by the same company – in this case Cisco. Having multiple platforms and operating systems should make penetration into our networks that much more difficult.

The GIAC Enterprise servers would be locked down by turning off all unnecessary services. Reference "How to Harden Internet Servers" on Stephen Northcutt's
http://www.happyhacker.org/defend/helpx.shtml

Assignment 2 – Security Policy

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components: Border Router, Primary Firewall, and a VPN.

2.1.1 Border Router

Packet Filtering through Cisco Routers
The boarder router will be entry point into GIAC Enterprise through our T1 connection with our ISP UUNET. The router first job, as its name implies, is to route traffic. In our case it will route traffic to the Service Network Firewall or the Corporate Network Firewall. In addition to routing traffic, our boarder router will be our first line of defense. The router will perform ingress and egress static packet filtering through Access Control Lists (ACL) to reduce traffic and threats to our networks. Note that routers have been known to drop packets or leak traffic through when traffic levels are excessive.

Extended IP access list:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The top ten attackers as listed on the www.inicidnets.org will be included on the access list.

```
access-list 101 deny host 131.234.192.11 any log
access-list 101 deny host 205.33.134.99 any log
access-list 101 deny host 204.34.192.18 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.15.0.0 0.240.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log
```

ACLs

To Permit our Partner / Supplier

```
access-list 102 permit icmp any host 205.233.23.125 echo
access-list 102 permit icmp any host 207.135.77.12 echo
access-list 103 permit tcp any 209.135.32.0 0.0.31.255 eq www
access-list 103 permit tcp any 209.62.144.0 0.0.15.255 eq www
access-list 103 permit tcp any 208.241.240.0 0.0.7.255 eq www


access-list 103 deny   ip host 255.255.255.255 any
access-list 103 deny   ip host 0.0.0.0 any
access-list 103 deny   icmp any any
access-list 103 deny   tcp any any eq ident
access-list 103 deny   tcp any any eq sunrpc
access-list 103 deny   tcp any any eq lpd
access-list 103 deny   tcp any any eq telnet
access-list 103 deny   tcp any any eq finger
access-list 103 deny   tcp any any eq login
access-list 103 deny   tcp any any eq cmd
access-list 103 deny   tcp any any eq nntp
access-list 103 deny   tcp any any eq exec
access-list 103 deny   tcp any any eq uucp
access-list 103 deny   tcp any any eq daytime
access-list 103 deny   tcp any any eq discard
access-list 103 deny   tcp any any eq pop2
access-list 103 deny   tcp any any eq chargen
access-list 103 deny   tcp any any eq gopher
access-list 103 deny   tcp any any eq irc
access-list 103 deny   tcp any any eq kshell
access-list 103 deny   tcp any any eq klogin
access-list 103 deny   tcp any any eq talk
access-list 103 deny   tcp any any eq hostname
access-list 103 deny   udp any any eq netbios-ns
access-list 103 deny   udp any any eq netbios-dgm
access-list 103 deny   udp any any eq ntp
access-list 103 deny   udp any any eq sunrpc
access-list 103 deny   udp any any eq snmp
access-list 103 deny   udp any any eq snmptrap
access-list 103 deny   udp any any eq tftp
access-list 103 deny   udp any any eq rip
access-list 103 deny   udp any any eq discard
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
access-list 103 deny   udp any any eq talk
access-list 103 deny   udp any any eq who
access-list 103 deny   udp any any eq xdmcp
access-list 103 deny   udp any any eq bootpc
access-list 103 deny   udp any any eq bootps
access-list 103 deny   udp any any eq dnsix
access-list 103 deny   udp any any eq time
access-list 103 deny   udp any any eq biff
access-list 103 deny   udp any any eq mobile-ip
access-list 103 deny   udp any any eq syslog
```

Note: For Cisco Command Usages refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/np1_r/1rospf.htm

2.1.2 Primary Firewall

The firewall solution to serve as the primary firewall is a Nokia IP440 loaded with Check Point FireWall-1 4.1. Check is a stateful inspection firewall that Check Point's stateful inspection firewall was chosen largely because of its ability to deal with FTP. Stateful inspection allows you to implement a tighter security policy because it able to inspect the packets rather than just the header. Through stateful inspection, the firewall is able to open data ports on the fly and when the session has been completed the ports are closed automatically.

For information about the firewall solution visit the following sites:
www.checkpoint.com
http://www.checkpoint.com/techsupport/
https://usercenter.checkpoint.com
www.phoneboy.com
www.nokia.com

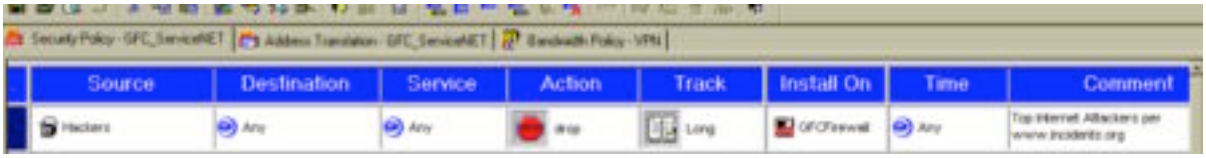
An in depth discussion of GIAC Service Network Firewall Rule Base:

One of the advantages of Check Point it their Policy Editor GUI, which make configuring the rules rather easy. But note that the order is which the rules appear is very important and is not necessarily easy. Additional information about the rulebase order will be present in another section.

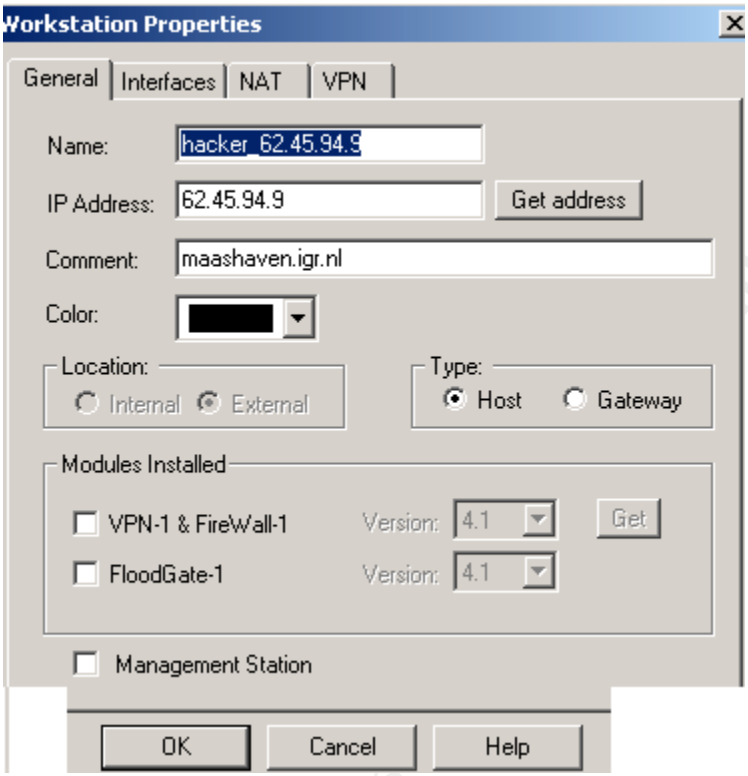
As mentioned in Assignment 1, the customers will not truly be "Any" and as such he first rule of our Service Network Policy will cover denial of access to a group, which shall be called "hackers". The list of hackers are the known "Bad Guys" as found on www.incidents.org.

Rule one: Drop Top Hackers

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



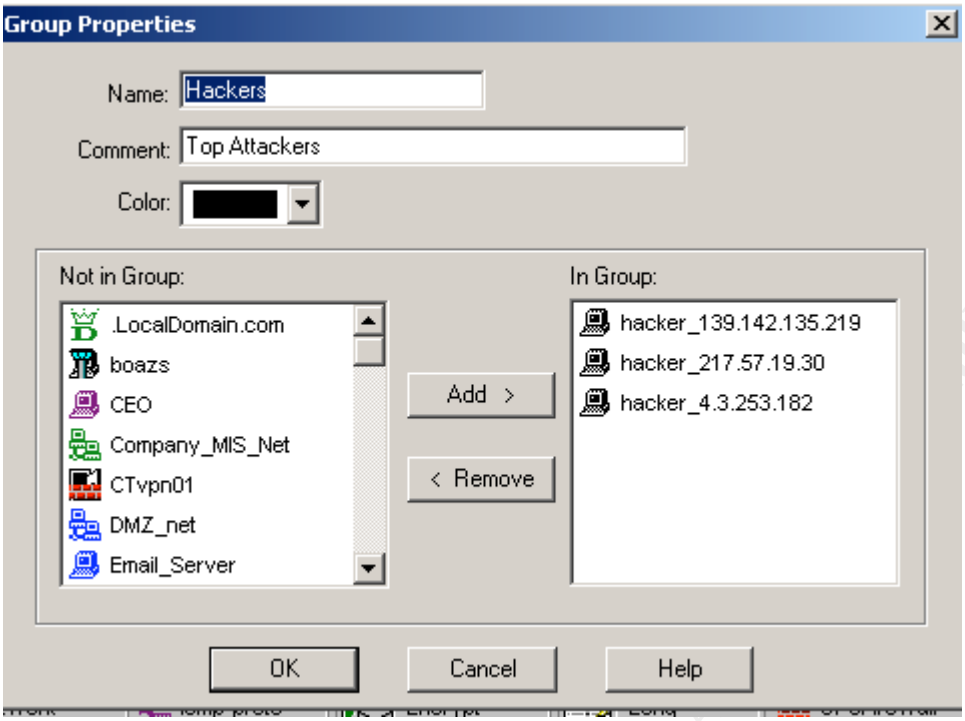
To create this rule, access the GFCFirewall Firewall Policy Editor on the management console. Under the manage tab select network objects and then select new. Next select workstation and enter the name, IP Address and a comment (for additional descriptive information). The location will default to external, as the GFC Firewall does not protect this IP.



Continue to create as many of these "hacker" workstations as need be. In our case we will add the top 10 attackers as listed on incidents.org web site, and this list will be updated once a week.

To ease administration of the firewall policy, a group will be created that contains the hacker workstations. To create a group, right click on the manage tab, select new and from the drop down list select "Group". On the Group properties tab create a name and comment. From the list of network objects in the "Not in Group" field select the previously created "hackers" and click the "add" button. As the hacker workstations are added they will appear to the right under the "In Group" field.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



After the hacker workstations and hackers group network objects have been created, the actual rule can be created. On the Policy Editor GUI, click on "Edit" and from the drop down list select "Add Rule". This will be our first rule, so select "Top" from the add rule options. Under the source column in rule one, right click and select "add". The list of "existing objects" will be shown. From here scroll down the "Hackers" group and click "ok" to add this object to the source of rule one. The rest of the rule is easily configured, much of it by default. By default, the Destination and Service will be "Any" and the Action will be "Drop". Under the "Install On" column select the relevant firewall on which this rule will be applied. The optional fields of Tracking and Comment will also be configured in our case - to log the hacker traffic and to add a narrative about the rule.

Note: The screen shot listed above is from an actual Check Point Policy Editor GUI. Each one of these screen shots make up of a file roughly 300 KB in size. In the interest of the reader and the reader's machine, the following screen shots of the rules will be simulated with the use of a word table.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
2	SercureRemoteUsers	GFC_Service_Net	ftp	Client Encrypt	Long	GFCFirewall	Any	SecuRemote access to GFC Service Net

Remote Users from the GIAC, the Supplier and the Partner Companies will have access to the GFC Service Network over a secure connection provided by Check Points SecuRemote product. SecuRemote is a free product that ships with Firewall-1. Additional information about the product and its installation as covered in the optional section – "Remote Access".

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
	CT_VPN	GFC Service Net	ftp	Encrypt	Long	GFCFirewall	Any	VPN between Partner Network

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3	Group	Group	http https smtp icho-proto					and GFC Service Net Encryption Domain

This rule is used to establish the VPN connection between the GIAC Partners and the GIAC Service Network. The VPN solution, which is described in greater detail in an upcoming section, creates an encrypted tunnel between the two locations. The services included ftp, http, https, smtp and icmp-proto, which covers icmp traffic to be used to trouble shoot network connectivity and to test the existence of the encryption tunnel. Seemingly ftp is the only service that truly needs to be included, but having http, https and smtp here makes it easier for our Partners to configure their routers, firewalls and VPNs.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
4	GFC Service Net Group	CT_VPN Group	ftp smtp icho-proto	Encrypt	Long	GFCFirewall	Any	VPN Tunnel back to Partner

Rule 4 creates the encryption tunnel from the GFC Service Network back to the Partner Network.

Note: You do not always have to create bi-directional rules when working in the Policy Editor, as the service/port is automatically bi-directional. The key point to consider is from where does the traffic originate. As we saw in Rule 2, the web server is the destination of the http and https traffic originating from the Internet or "Any".

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
5	Supplier VPN Grp	GFC Service Net Group	ftp http https smtp icho-proto	Encrypt	Long	GFCFirewall	Any	VPN between Supplier network and GFC Service Net Encryption Domain

Similar to the rule 3, this rule is used to establish the VPN tunnel from the Supplier Network to the GFC Service Network. Additional information about configuring the Network objects used to define the VPN Gateway, encryption domain and corresponding VPN rules is covered in the section on VPNs.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
6	GFC Service Net Group	Supplier VPN Grp	ftp smtp icho-proto	Encrypt	Long	GFCFirewall	Any	VPN Tunnel back to Supplier

Rule 6 creates the encryption tunnel from the GFC Service Network back to the Supplier Network.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
7	ANY	GFC Web Server	http	Accept	Short	GFCFirewall	Any	Internet traffic to GFC Web

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

			https					Server

To configure the web access to the fortune cookie web server, select the following on the firewall Policy Editor GUI: manage, network objects, new, and workstation. On Workstation Properties tab enter a name, the IP Address and comment that relate to the web server - 209.62.158.84 Web Server.

On the Policy Editor GUI, create a new rule. The source by default is "Any", which is exactly what we want in this case. Next define the destination by right clicking in the relevant cell, click add and from the drop down list of Existing Objects select the newly created Web Server. Right click in the cell under "Service", select add, under the drop down list of services select "Http" (port 80) and "Https" (port 443). Define Action as "Accept", Track "Short" to log the web site hits, Install On "GFCFirewall", Time as "Any" and add a descriptive comment about the rule.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
8	Any	External Mail Server	Smtp	Accept	Long	GFCFirewall	Any	Allow Mail to Ext Mail Server

Rule 8 allows the E-mail from the Internet into the Service Network to the External Mail Server. The Mail Server inspects the mail messages before passing them on to the corporate network.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
9	External Mail Server	Any	Smtp	Accept	Long	GFCFirewall	Any	Allow Ext Mail Server Out

Rule 9 permits E-mail communication from the External Mail Server back out onto the Internet. Routing the mail back out the External Mail Server protects the identity of the Internal Mail Server.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
10	Int Mail Svr Ext Mail Svr	Ext Mail Svr Int Mail Svr	Smtp Pop-3	Accept	Long	GFCFirewall	Any	Allow In / Ex Servers to communicate

The E-mail to and from the GIAC Corporate network is routed through external mail server, to strip the messages of any known viruses, trojans and to protect the identity of the internal mail server and its users. This rule allows Internal and external mail servers to communicate over smtp (25) and pop-3 (110).

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
11	GIAC Corp Network	GFC Service Net	ftp http https imcp-proto	Accept	Long	GFCFirewall	Any	Limited access from GIAC Corp Net to GFC Service Net

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Rule 11 allows for the GIAC Corporate network to connect to the GFC Service Network. As defined earlier, this access will be limited to protect the Service Network from internal attacks. The NOC engineers typically perform the administrative work performed on the service network servers. Employees who need to greater access to the service network servers will work from the extra workstations located in the back row of the NOC. The GIAC Corporate network has been natted on the GIAC Corporate Firewall using hide nat. This allows the private IPs of the Corporate network out to the Internet and protects the identity of the corporate networks private IPs. An explanation of how to use hide nat will covered during the discussion about the GIAC Corporate Firewall.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
12	GIAC NOC Network	GFC Service Net	ANY	Accept	Long	GFCFirewall	Any	Unrestricted access from GIAC NOC Net to GFC Service Net

As noted above, the GIAC NOC Network will have full access to the GIAC Service Network and therefore the service in this rule is "Any". The source is made up of the private IP network of the NOC (10.2.1.0/24) – which has not been natted on either the corporate firewall or GFC Firewall. The NOC Network does not have access to the Internet and therefore it does not require a public IPs.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
13	GFCFirewall manage Svr logging Svr	ANY	Firewall-1 Group	Accept	Long	GFCFirewall	Any	Allow remote management of Firewall

Rule 13 has been defined to allow for firewall administration. This will allow the network security engineers to access the firewall from the management console rather having to administer the policy from the Firewall directly. The will also allow the firewall traffic to be sent to a logging server – which reduce the load on the firewall itself. The service group of Firwall-1 has been selected to allow this functionality. Check Point Policy Editor GUI has a number of pre-defined service groups, including "Firewall-1". The FireWall-1service group is made up of the following:

FW1 - tcp 256
FW1_clntauth_http - tcp 900
FW1_clntauth_telnet - tcp 259
FW1_log - tcp 257
FW1_mgmt -tcp 258
FW1_snmp - udp 260
ISAKMP - udp 500
RDP - udp 259
snmp - udp 161

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
14	ANY	ANY	Silent Services Group	Drop		GFCFirewall	Any	Drop Network Pollution DO NOT LOG

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Rule 14 is a Check Point recommended rule used to drop unnecessary broadcast traffic. Check Point's pre-defined service group of the Silent Services has been selected in Rule 11. This service group is made up of UDP bootp, and the NBT services of nbdatagram, nbname, and nbsession. Notice that this rule, unlike all the other rules, does not have a selection for "Track". The omission means the rule will not be logged. Logging this rule is not recommended because it will capture a great deal of useless information and cause undue stress to the logging server.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
15	ANY	ANY	ANY	DROP	LONG	GFCFirewall	Any	Clean Up Rule to Log Dropped Traffic

Check Point drops all traffic that was not previously defined by default. Unfortunately, this traffic is not automatically logged – as it clearly should be for network security and trouble shooting. The cleanup or drop rules are not necessarily used to define what traffic to drop, but rather to capture this traffic in the logs. Rule 15 is simply the Any, Any, Any Drop Rule, which is used to log the undefined and unauthorized traffic. Note the network pollution dropped by Rule 14 never makes it to rule 15, and therefore that traffic is not logged.
If the order of the rules is important, include an explanation of why certain rules must come before (or after) other rules.

Implementing the firewall rule base is just as important if not more so than selecting the firewall products and defining the firewall architecture. Lance Spitzner, of the Honeypot Project, has written a whitepaper entitled *"Building Your Firewall Rulebase",* which uses Check Point FireWall-1as an example. In his whitepaper, last modified on January 26, 2000, Spitzner stated "Building a solid rulebase is a critical, if not the most critical, step in implementing a successful and secure firewall". The whitepaper emphasizes that simplicity is key and that a rule base should not contain more that 30 rules. Spitzner states, "Between 30 and 50 rules, things become confusing, the odds grow exponentially that something will be misconfigured. Anything over 50 rules and you end up fighting a losing battle." The rule order is also an important consideration in writing the rulebase. When the firewall receives a packet, it compares it against the first rule, then the second, then the third, etc. When it finds a rule that matches, it stops checking and applies that rule. If the packet goes through each rule without finding a match, then that packet is denied and dropped by the cleanup rule. It is important to understand that the first rule that matches is applied to the packet, not the rule that best matches. Based on this fact, the more specific rules should come first followed by the more general rules. This prevents a general rule from being matched before hitting a more specific rule, which helps avoid firewall misconfigurations. [6]

Dameon D. Welch-Abernathy, creator of www.phoneboy.com has posted the following regarding rulebase order:

[6] Spitzner, Lance, Whitepaper, Building Your Firewall Rulebase, January 26, 2000
http://www.enteract.com/~lspitz

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FireWall-1FAQ: What Order Does FW-1 Apply The Rulebase? [7]

So what is a good "rule of thumb" when ordering the rules in your rulebases? Here's how I typically order my rulebase based on action types:

SecuRemote Encryption rules
FireWall-to-FireWall Encryption rules
Incoming "accept" rules
Outgoing "accept" rules
Client Authentication rules
Session Authentication rules
User Authentication rules
Clean-up rule

Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
2	SercureRemoteUsers	GFC_Service_Net	ftp	Client Encrypt	Long	GFCFirewall	Any	SecuRemote access to GFC Service Net

Testing this rule serves a dual purpose of checking the SecuRemote and ftp is working properly. This rule will be tested from outside of the network. Use the following steps to test this rule:

• On a laptop, use the dialup modem to connect to the Internet through an ISP.
• Select the SecuRemote Icon in the lower left hand corner – and select the GFC Firewall.
• Select Passwords column and enter user name and password. Hit Ok.
You should now be authenticated on the firewall – to begin a SecuRemote session on the service network. Note: SecuRemote icon in lower right corner is now an opening and closing envelop.
• From a command line prompt type ftp 209.62.158.85.
• An acknowledgment back from the ftp server indicates a successful connection
• Additional testing of "get" or "put" will confirm the ftp service is working properly.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
7	ANY	GFC Web Server	http https	Accept	Short	GFCFirewall	Any	Internet traffic to GFC Web Server

Rule 7 is our Internet access to the Web Server Rule. This rule is easily tested through a web browser, but can also be test through the use of telnet. Although, telnet is not being used on the web server it can still be used to the test http and https.

From a command prompt type: C:\>telnet 209.62.158.84 80

[7] Welch-Abernathy, Dameon D. www.phoneboy.com , "FireWall-1 FAQ: What Order Does FW-1 Apply The Rulebase?"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

C:\>telnet 209.62.158.84 443

A successful attempt will bring up a blank command screen with a blink cursor. An unsuccessful attempt will respond back with a connection fail message.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
15	ANY	ANY	ANY	DROP	LONG	GFCFirewall	Any	Clean Up Rule to Log Dropped Traffic

Testing the clean up rule does not prove that particular service or application is working properly. However, testing this rule is very important to insure that the firewall is dropping unauthorized traffic and that the dropped traffic is being recorded in the firewall logs.

To perform this test, open a command prompt and attempt to telnet to a server on the service network over a random port, which you would assume to be closed. Below is an example were an attempt has been made to connect to the web server over port 10000.

C:\>telnet 209.62.158.84 10000
Connecting To 209.62.158.84...Could not open a connection to host on port 10000: Connect failed

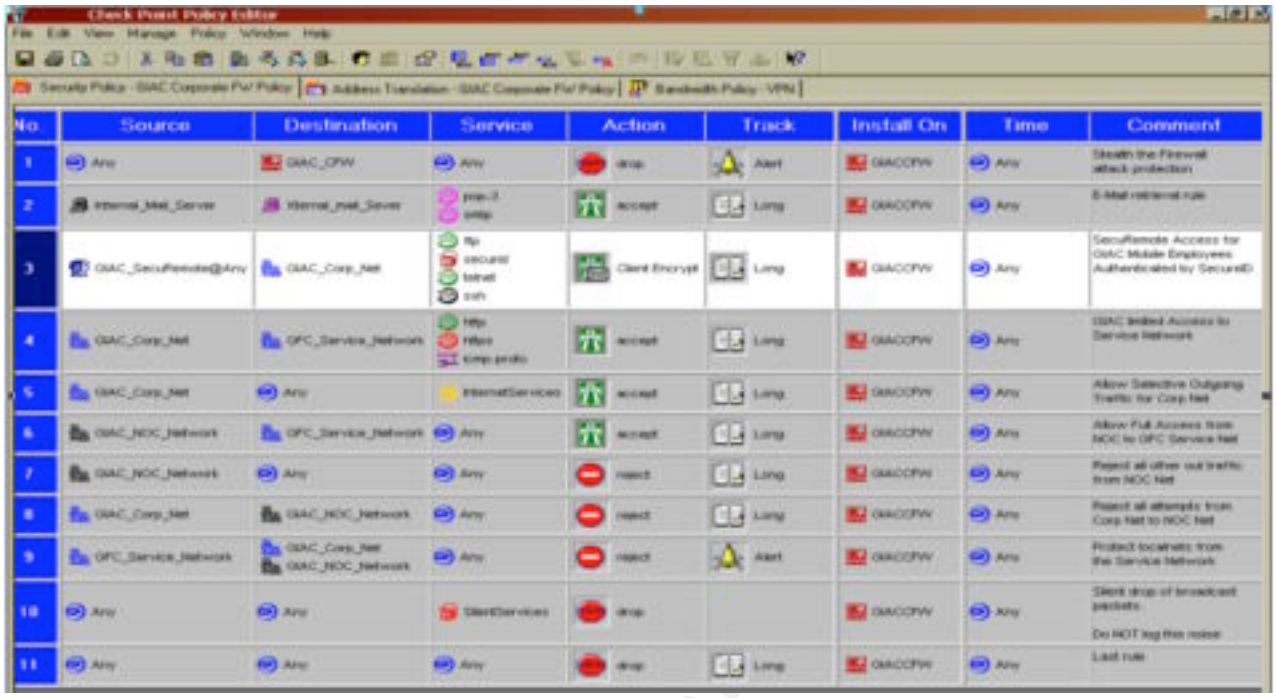
Access the Logging GUI to review the logs when testing each of the samples rules above. This practice will confirm the test findings and confirm that the firewall is working properly. With proper planning, you could design your network and firewall rules at the same time. The Logging GUI could help test to insure that each rule is working properly and as intended.

"How Can I Disable Everything in Rulebase Properties?" posted on www.phoneboy.com is a good source to learn more about how to protect the default property weaknesses.

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

The Corporate Firewall is connected to the Internet, although with limited access, and therefore it may not be considered a true internal firewall. However, the GIAC Corporate Firewall does help filter the traffic between our internal networks and does provide a "defense in depth" solution. As such, the GIAC Corporate Firewall Policy will be discussed in this section.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Listed above is the security policy that has been installed on the Corporate Firewall. Having gone through the Service Network firewall policy rule by rule, I will not repeat that process again. However, I will point out some of the things that are unique to the corporate firewall policy.

Rule one is designed to drop all traffic destined directly to the Firewall. This is a Check Point recommended rule, as it is included in the Policy Editor GUI rule wizard and templates.[8] The rule is useful for the Corporate Network to protect the Firewall, but it will not work on the GFC Service Network. The management console and logging server is within the same network as the corporate firewall. Because the management console and the logging server are on different network than the GFC Firewall, a separate rule is needed. Using Rule One on GFC Firewall would negate the ability to remotely manage the firewall – at least by having it any the top of the rulebase anyway.

Rule Three defines SecuRemote access for GIAC's mobile and telecommuting employees into the corporate network. Notice the SecurID service group is included with the other services. RSA's SecurID is being used to provide authentication on the firewall before allowing any further access to the corporate network.[9] This is a defense in depth solution that requires the end user to enter: a SecuRemote password, a SecurID password and a randomly generated number

[8] Check Point Firewall-1 4.1 Policy Editor includes a feature called "helpers" which are designed to assist in the creation of a security policy. Within the helper option are wizards and templates.

9 RSA SecurID two-factor authentication is designed to provide positive proof of user authenticity, protecting access to the key applications that are part of an enterprise's [Single Sign On] solution. Additional information about RSA SecurID can found at http://www.rsasecurity.com/.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

from the SecurID key in order to be authenticated. Note that the Supplier and Partner companies do not have SecuRemote access into the corporate network.
Note: It not necessary to configure firewall rules to allow communications between machines that reside on the same network – assuming the machines are behind the firewall.

As mentioned earlier, the GIAC Corporate Network (10.3.1.0 network) has been natted on the Corporate Firewall. This was done through the Policy Editor GUI by configuring the network properties of the object "GIAC_Corp_Net" – as seen in Rule Four. Select the NAT Tab, and in the "Values for Address Translation" box check "Add Automatic Address Translation Rules". In the Translation Method field select "Hide" from the drop down list. In the Hiding Address field enter the external IP for the GIAC Corporate Firewall - 209.62.158.99. Install on all is listed by default.

A number of the rules above list the Action of Reject rather than Drop. Drop is used to silently discard packets while reject is used to announce that the firewall has dropped the packet.

VPN – Firewall-to-Firewall Solution with Partner Company – Chinese Translations

GIAC's partner company, Chinese Translations, Ltd. (CT) is, as their name implies, in the business of providing translations. While they are brilliant, CT is not an Internet or IT savvy company and GIAC has therefore stepped in to assist. GIAC has provided the VPN solution between the CT and the GFC by installing a Nokia IP330 in a DMZ off the partners network. GIAC has essentially become an Application Solution Provider (ASP) in this partnership, which has created a "win, win" for both sides. GIAC and CT worked together to develop an acceptable security policy for the VPN.

The Nokia device is loaded with Check Point VPN-1/FW-1 4.1, similar to GIAC's own GFC Firewall. By design, GIAC does not have access into the CT network. GIAC can only access the VPN device in the DMZ and does so via an ssh connection coming out of the GIAC Corporate Network. In the same vane, CT does not have any special access into GFC Service Network. CT only has the access allowed by Rule 3 on GFC Firewall, as repeated here:

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
3	CT_VPN Group	GFC Service Net Group	ftp http https smtp icho-proto	Encrypt	Long	GFCFirewall	Any	VPN between Partner Network and GFC Service Net Encryption Domain

While the source and destination listed above seems quite clear, there is some additional configuration that lies beneath. Encryption domains must be formed in order for the encryption tunnels to be formed and for this rule to work properly. The encryption domains are created on the Firewall Gateway. In example above, the GFC Service Network has been defined as the encryption domain on the GFC Firewall and the Partner 1 Net (listed below as the CT Network) is the encryption domain on the CTvpn01 gateway. Note: You cannot set up multiple encryption domains for the same firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To configure the firewall, use the following steps on the Policy Editor GUI:

From the Manage link, Select Network Objects and from the drop down list select the GFC Firewall.

- Click Edit to access the workstation properties tab
- Select the VPN tab
- Under the Domain field, select "Other"
- From the drop down list of options, select the GFC Service Net
- In the Encryption schemes defined field, check IKE and hit edit
- On the IKE Properties Tab select the methods to be used for IKE encryption. 3DES encryption and the MD5 hash algorithm will be used.
- Select Pre-Shared Secret under Support authentication methods.
- Use the Edit Secrets button the configure the Shared Secrets
- Check the box for Supports Aggressive Mode
- Check the box for Support key exchange for Subnets

Note: The same steps would be used to configure the encryption domain on the CTvpn01.

The GIAC Network Security team implemented the security policy for the VPN – after being approved by CT. The rulebase installed on the Partner VPN device is listed below:

The security policy listed above is not very restrictive or complicated. The first two rules are used to establish the encrypted tunnel between the two networks. Rule three gives the CT unrestricted access to the rest of the Internet. Rule four also GIAC to administer the VPN remotely. Rules five and six drop unnecessary and undefined traffic.

VPN with Supplier via GATEWAY-to-GATEWAY Solution

Although Check Point does have the market share in firewall and VPN technology, obviously not everyone using Check Point for their VPN solutions.

A Gateway-to-Gateway solution will be use to provide and encrypted tunnel between the Supplier (Confucius Say, Inc.) and the GIAC Fortune Cookie FW (GFC FW). This solution is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

an IPSec VPN configuration between our FW-1/VPN-1 gateway, the GFC FW, and the supplier's Cisco PIX firewall version 535. Pre-shared secrets will be used to as the authentication method.

Below are guidelines to follow to implement this Gateway-to-Gateway solution on the GIAC Firewall side of the equation:

Note: As stated above, the GFC Firewall is running Checkpoint 4.1. If the GFC was only running Check Point 4.0, this option could still be used, but only if the remote gateway (the VPN on Partner/Supplier side) was also running Check Point VPN-1/FW-1. The Client gateway must be capable of encrypting using IKE and 3DES with pre-shared secret.

Configuration of VPN objects and Rules on GIAC Firewall through the Check Point GUI

The GCF VPN network objects were already covered in the section above. The focus here will be on the creating the supplier side VPN objects and rules.

Creating the Objects:

1. Create a network object for the supplier's network.
2. Create a workstation object for the Supplier's PIX Firewall.
3. On the VPN tab, under domain "other" select the Supplier Net – which will allow IPs in the network to access GFC through the encrypted tunnel.
4. Under the Encryption schemes, select IKE.
5. On the IKE Properties tab select the methods to be used for IKE encryption. 3DES encryption and the MD5 hash algorithm will be used in Supplier Network.

Note: Encryption Laws should be checked before selection the type of encryption. In our case 3DES is legal encryption.

6. Select "Supports Aggressive Mode" and "Support keys exchange for Subnets"
7. Select Pre-Shared Secret under Support authentication methods.

Note: When configuring the "Pre-Shared Secret" on the GIAC side FW, select the peer name Gateway (Supplier PIX Firewall) and enter the agreed upon secret/password. Obviously, this password should be exchange in the most secure method possible – (i.e. manually)
Once the network objects have been created as described above, the relevant rules can be created. The rule below shows that the Supplier Net can connect through the GFC Service Network via http, https, and ftp through the VPN tunnel. ICMP was also added to assist in trouble shooting network connectivity issues.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
5	Supplier VPN Grp	GFC Service Net Group	ftp http https smtp icho-proto	Encrypt	Long	GFCFirewall	Any	VPN between Supplier network and GFC Service Net Encryption Domain

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A bit more configuration is need, through use of the Policy Editor GUI, to insure the above encryption rules work properly. Use the following steps to complete the encryption configuration:

1. Select Encrypt under the relevant Rules under action column.
2. Edit properties – which takes you to the encryption properties tab.
3. Under encryption schemes defined select the relevant encryption type
(IKE in Supplier's case, although multiple selections could be made in cases where numerous encryption types are being used.
4. Then select edit which takes you to the IKE Properties Tab
5. Select the relevant properties, which will match those that have also been configured on the Suppliers PIX Firewall. Note: The properties from this tab relate to the phase two negotiations used to establish the IPSEC security association.

Credit for the steps and solution listed above goes to David Dietrich, who in wrote *"Check Point VPN-1 and Cisco PIX Gateway to Gateway IKE VPN Using Pre-shared Secrets"*.[10] Dietrich's paper also covers instructions on how to configure the Cisco PIX firewall and can be found at http://support.kcfishnet.com/public/cppublic/pixvpn.pdf. Additional information about Cisco PIX firewalls can be found at: http://www.cisco.com/univercd/cc/td/doc/pcat/fw.pdf

Optional

Remote Access Through Check Point's SecuRemote

Check Point's SecuRemote will be implemented to allow remote access for GIAC employees, partners and suppliers – although the access for each group will vary. SecuRemote provides a software VPN solution that is free with the Check Point VPN-1. Note: There is an additional license that is required to use SecuRemote but as mention this is a free upgrade. See the Check Point user center web page for details. Check Point provides a similar product called SecureClient that includes desktop security. This product insures that enforcing a desktop policy does not compromise remote access sessions. The desktop policy must be running before access is granted. Because of licensing costs and the varying needs of our end users, SecureClient will not be used in this environment. A personal firewall will be installed on all remote machines and more information about that will follow.

Please note that the Check Point's SecuRemote product is only available for Microsoft Operating Systems. This is a recognized shortcoming of the product from a UNIX and MAC perspective. Fortunately this is a non-issue in the GIAC Fortune Cookie environment, as all end users machines are using Microsoft.

The following is a guideline to install SecuRemote on the end users laptops/machine.

[10] Dietrich, David, "Check Point VPN-1 and Cisco PIX Gateway to Gateway IKE VPN Using Pre-shared Secrets", May 19, 2000 Version 1.0 2000 Check Point Software Technologies LTD.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SecuRemote Installation Guidelines:

Please Note: Installation of SecuRemote has been known to crash some machines. A thorough backup is recommended before installing SecuRemote.

The current standard is to use SecuRemote 4.1 SP-5 3DES build 4199 for Windows 2000. This can be obtained from Checkpoints website under software downloads.

The default settings should be used during the installation of SecuRemote **except** for the following options:

1. Chose Install SecuRemote without Desktop Security (that is for SecureClient)
2. Determine, which network adapters, you will be using. If SecuRemote will be used with a modem choose Install on dialup adapters only. If SecuRemote will be used over a LAN choose Install SecuRemote on all adapters.

The following covers detailed information using SecuRemote 4165, but please note that the others versions are very similar.

Phase One: Create a site for SecuRemote session.
Choose Site|
Create new
Enter the IP address of the firewall, press OK

Once the SecuRemote client is installed there is no additional configuration required as the default encryption is set to IKE.

Phase Two: Authentication

Authenticate to the firewall to download the site topology
Enter the assigned username and password in the appropriate fields. Click OK. Click OK once again.
The SecuRemote client will be displayed as active when the site has been created successfully as shown by the existence of the firewall icon. If the SecuRemote client has been properly installed, the user will note the SecuRemote Icon in the lower right corner of their screen. The icon is an open envelop with a key. When SecuRemote is in use, this icon will change to show the envelope opening and closing.

In the GFC environment, SecuRemote is being used exclusively for remote access through a dial-up connection. LAN Installation instructions are also provided for future needs and to provide a backup solution in the event that the VPN goes down. In order for SecuRemote to work properly over the GIAC or Partner/Supplier corporate LAN, the following ports must be opened bi-directionally on their firewall back to the GFC firewall: UDP 500, Protocol 94 (0x5e), Protocol 50 (0x32), Protocol 51 (0x33), TCP 264, and UDP 2746

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This completes the configuration of the SecuRemote client. After completing the above process a user can now access the servers remotely based the access define in the firewall policy rule(s). The firewall rulebase will be discussed next.

Configuring Check Point FireWall-1Rulebase for use of SecuRemote

Below is a screen shot of the SecuRemote rules on the GIAC Fortune Cookie Service Network Firewall.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
2	SercureRemoteUsers	GFC_Service_Net	ftp	Client Encrypt	Long	GFCFirewall	Any	SecuRemote access to GFC Service Net

To Create SecuRemote Users on the GFC Firewall, perform the following steps working from the Policy Editor GUI:

1. To ease the administration of the SecuRemote users, create a group by selecting manage, users, new and from the drop down list select Group.
2. In the Group Properties tab enter a name (SecuRemote) and comment.
3. Again from the manage tab select users, and new to create new users
4. General Tab: Used to define the user name, Additional comments (Department name for example) and Expiration Date, which can be used for temporary employees
5. Group Tab: To assign the users to a specific group or groups. Select the newly created SecuRemote group
6. Authentication Tab: Define the type Authentication to be used.
   In the GFC environment SecurID and the VPN-1 & FireWall-1Password will be used.
7. Location Tab: Used to further define the source(s) and destination (s) to which the SecuRemote users to have access to and from
8. Time Tab: Can used to further restrict access of a SecuRemote User.
9. Encryption Tab: Used to define the encryption method(s). In our case, IKE will be used.
10. IKE Properties Authentication Tab: Used to define password of public key authentication
11. IKE Properties Encryption Tab: Used to define ESP, AH, SHA1 or MD5 and the encryption algorithm of DES, DES-40CP or CAST-40

Screen shots on how to configure SecuRemote are included in the Additional Resources section of the end of the paper.
As stated above, the Check Point product with desktop security, SecureClient, was not selected for implementation for budgetary and flexibility issues. However, "personal firewalls are now a must for exposed hosts on the Internet. When home or remote user creates a VPN to the internal network, they have become an extension of that network – but without the benefit of perimeter security" [11]

GIAC employees, Partners and Suppliers working remotely through a SecuRemote connection are required to install a Personal Firewall. While there a numerous personal firewall available,

[11] SANS Institute Track 2 Firewalls, Perimeter Protection and Virtual Private Networks, 2.2 Firewalls 101: Perimeter Protection with Firewalls, page 161

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Enterprises uses Tiny Personal Firewall (Build Info**:** Build 2.0.15 October 17, 2001 (1416KB), Win 9x, ME, 2000 , NT & XP) Tiny is a free personal firewall that is easily to downloaded and configure. Go to www.tinysoftware.com and review the installation and use guidelines before installing the product. Educating the end users is the key to effective use of the personal firewall and the perimeter of our network security. It is import to stress to the end users that they should be using the personal firewall all the time, not just while they are connected to the GIAC environment.

Assignment 3 – Audit Your Security Architecture

3.1. Plan the Audit

The network security team has been given the task of auditing the "Primary" firewall of GIAC Enterprises, which is viewed to be the firewall protecting the GIAC Fortune Cookie Service Network. It is the revenue generated from the Service Network that makes GIAC a $200 million dollar online company, and such the firewall protecting that network is considered the "Primary" firewall. This firewall is affectionately known as the GIAC Fortune Cookie firewall or "GFC Firewall". The first goal of the audit is to not cause any harm to our business. Beyond that, the goal is to identify any and all vulnerabilities of the service network.

The audit will take place in phases. Phase one will be an internal audit, in which one the GIAC security engineers will work from within the GIAC Corporate network to assess the security of the Service Network. As mentioned in Assignment One, the corporate network will have limited access to the service network. GIAC employees making changes to service network to that need greater access levels are required to perform their tasks from the NOC Network. The phase of the audit will identify the vulnerabilities that the GIAC Fortune Cookie Network faces from its own internal employees. In 1996, Internet Security for Business reported "Significantly more threats come from a company's internal network – as much as 80 percent to 95 percent of the total number of incidents (according to various studies)." [12] These figures maybe a bit out of date, but the point that internal threats are a major issue is still valid today

Note: The audit will not include an assessment of the NOC networks access into the service network. As mentioned, the employees in the NOC network have full access to the service network as needed to perform their job functions.

Phase two of the audit is also an internal audit of GIAC perimeter.

Phase three of the audit will come from the outside the GIAC perimeter. It is often difficult to know exactly where the perimeter starts and ends or what it encompasses. This fact is particularly true when Virtual Private Networks (VPNs), and mobile users are added to the network design. In this phase of the audit will be truly outside the perimeter.

[12] Berhstein, Terry, et al., Internet Security for Business, New York, NY: John Wiley & Sons, 1996. Page 23

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Note: The task is to audit the "primary firewall" and as such this audit will be direct toward the Service Network only. However, the findings of this audit will be put to use to enhance the corporate firewall and project the internal networks as well.

3.1.1 "The How" *Describe the technical approach you recommend to assess the firewall.*

I recommend the auditor begin by attempting to access the service network over the common ports such as telnet (23), ftp (21), ssh (22) http (80), and https (443) and such and then move on to the less common service ports. Telnet could be used to perform a fairly non-intrusive test of the common ports (And telnet does not have be running on the target machine). From a command prompt on the auditing machine, attempt to telnet to the server IP over a given port number. For example,

```
C:\>telnet 209.62.158.85 22
Connecting To 209.62.158.85...Could not open a connection to host on port 22 : Connect failed

C:\>
```

The example above shows attempt to telnet from the GIAC Corporate Network to GIAC Fortune Cookie Web Server over port 22 – commonly used for ssh. As predicted, this connection failed because the GFC Firewall blocked it.

This type of testing was also used in Assignment Two to insure the firewall rule was working. In Assignment Three, the telnet testing will be used to insure that the firewall is not allowing unauthorized access or that the server has not been sufficiently locked down.

I also recommend the use of the scanning tools available such as nmap, snort, Nessus SARA and Cerberus.

The audit will include an analysis of the GFC Firewall of the Firewall Logs. A 24 hour period of logging data will be gathered for a through analysis prior to the start of the internal and external audit. Both the dropped and accepted traffic will be reviewed. There will also be an analysis of the firewall logs that have captured the activities of the audit. The firewall log viewer GUI will be reviewed "live" during the various audit phases – as listed above. The firewall logs will also be captured further review after the internal and external audits. Notations will be made regarding the audit activities that are not captured in the log.

Although Check Point does have limitations with it logging capabilities, it does have some nice options as well. The Logging GUI is very user friendly and it easy to customize – to narrow the scope of traffic you wish to view. To capture the traffic that is specifically being generated by the source machine in the internal and external audits, perform the following:

> Access to Logging GUI, right click on the "Source" column heading and from the drop down list, and click on "Selection". To the left is a drop down list of all the network objects entered on the management console – essentially all of the object that are protected by the firewall(s) or have been granted access through the firewall(s). In the

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

case of our audit, the sources IP will not be listed as a previously defined network object. Above the drop down list of network objects is an area called the "add data entry field". In this field enter the source IP that is being used to perform the audit and click add. The Logging GUI will now be focused on just the traffic that is coming from that source.

TIP: Turning off name resolution under the view tab will improve the performance of the logs. Clicking the down arrow button on the tool bar will place move you the bottom of the logs or most recently logged traffic. By using this feature, you can essentially view the traffic logging "live".

Note: To Reference port numbers go to: http://www.iana.org/assignments/port-numbers

3.1.2 "The When" *Be certain to include considerations such as what shift or day you would do the assessment.*

The internal audit will be conducted during normal business hours, in this case on a Wednesday between 9:00 AM and 5:00 PM, to simulate normal conditions. If an employee were going to attack the service network, they would likely do so during the day in hopes that their activity would go undetected. Although it is not uncommon for GIAC employees to work late or start early, their activities would that much more noticeable by the network security staff.

The external audit of the service network will take place at night during the hours when business activity on the service network servers is greatly reduced. Sunday 9:00 PM to Monday 5:00 AM has been selected. This time period was selected to reduce potentials risks (as noted below) and to isolate the audit activity for a more through analysis.

Note: It is understood by all that this audit is a not a test of the network security staff or the Network Operations Center (NOC) staff. The focus of the audit is to test the "Primary Firewall" and the network of servers it is designed to protect.

3.1.3 "The Cost" *Estimate costs and level of effort*

A Junior GIAC Security Engineer with an annual salary of $50,000 makes roughly $22 per hour.

Junior Security Engineer audit action items:

Inside and outside audit	12 hours
Preparation of audit results (i.e. reports, graphs, and printouts)	4 hours

Total = 6 hours x $22 = $352

The Senior GIAC Security Engineer with an annual salary of $75,000 makes roughly $33 per hour.

Senior Security Engineer audit action items:

Planning audit	4 hours

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Analysis of Firewall logs (a 24 hour sample period before audit)	4 hours
Assistance Jr. Engineer with audit	4 hours
Review and analysis of Jr. Engineer's findings	4 hours
Review of "independent auditor" findings	3 hours
Research of vulnerabilities found	4 hours
Write up of report, recommendations and meeting preparation	4 hours
Presentation and discussion of findings to CIO and CTO	2 hours
Preparation of post meeting memo on decisions and action items	1 hour

Total = 30 hours x $33 = $990

Network Operations Center (NOC) Engineer

An additional NOC engineer will be on shift during the audit to monitor the functionality of the Service Network servers, particularly the web server. If the NOC engineer observes any service degradation, beyond the previously measured baseline thresholds, the audit will be suspended. As stated above, the first goal of the audit to not cause any harm to our business. If at all possible, we do not want miss or interrupt a single e-mail, ftp session, or visit to our web site by one of our partners, suppliers, or customers. As such, this additional cost is easily justified.

In addition to monitoring service network servers, the NOC engineer will perform the task of running "netstat –an" on all machines in the service network to determine what ports are listening and what services are running. As discussed earlier, these boxes should have been hardened to have all unnecessary services turned off. This part of the audit will insure that the administrators of these machines are continuing to follow this policy.

The junior level NOC Engineer, making roughly $17.50 per hour, will work 16 hours outside of her normal shift. This will add an additional $280 toward the cost of the audit.

Junior NOC Engineer audit action items:

Monitor Service Network during audit	16 hours
Run "netstat –an" on each service network server and document findings	1 hour

Total 17 hours x 17.50 = $297.50

Estimated audit costs for GIAC Employees: $1,750.00

Additional Audit Resource, "The Independent Auditor"

The Chief Technology Officer's son, John, a Computer Science Degree seeking sophomore and notorious hacker, will augment the audit. John displayed a less than exemplary work ethic and attitude during his summer internship, and therefore will not be paid on an hourly basis. John will be given $100 each vulnerability he finds (and documents) on the service network, up to maximum of $1,500.00. John has been given strict instructions not to cause any damage or degradation of service to the Service Network. John will notify the GIAC network security team when he is performing his audit and will identify the source IP addresses he is using or spoofing.

Estimated cost of "Independent Auditor" $800.00

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Estimated Total cost of Audit $2,500.00

3.1.4 "Risks and Considerations" **Identify risks and considerations**

Risks -

The audit team will take every effort to minimize the risks involved as to not weaken the security or degrade service. The risks involved in the audit known from the planning stage include:

• The audit will increase the load on GIAC boarder router, which could allow potential hacking traffic to pass unfiltered.

• The increased CPU utilization on the firewall could cause a potential denial of service to the Service Network by blocking legitimate traffic, stopping the firewall daemon and theoretically could cause the firewall to crash.

• The increased load on the firewall could also allow potential hacking traffic to pass unfiltered (although there is no documentation that I have found, thus far, regarding Checkpoint or Nokia that states this to be true).

• The Service Network Servers (Web, Mail, FTP and DNS servers) could be at risk if the auditors are successful in gaining unauthorized access. As stated, above the audit team is under strict order not cause any harm, but none the less, the servers could be at risk. The scanning tools being used during the audit could also place the servers at risk by causing increased CPU utilization or some other disruption of the application/service.

Considerations -

The thought of having a completely independent audit performed was considered. GIAC look into hiring some network security consulting firms to perform the audit, before deciding to perform the audit in house. GIAC upper management agreed that the network security staff would gain a great deal of knowledge by working on the audit. Much more so than reading over security auditor report from a consulting firm. The audit may prove the security team is not doing an adequate job of protecting the GIAC Fortune Cookie Service Network and ultimately the GIAC Enterprises. Although that is unlikely, GIAC will consider bring in a consulting firm based on the results of the audit.

3.2. Conduct the audit.

Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

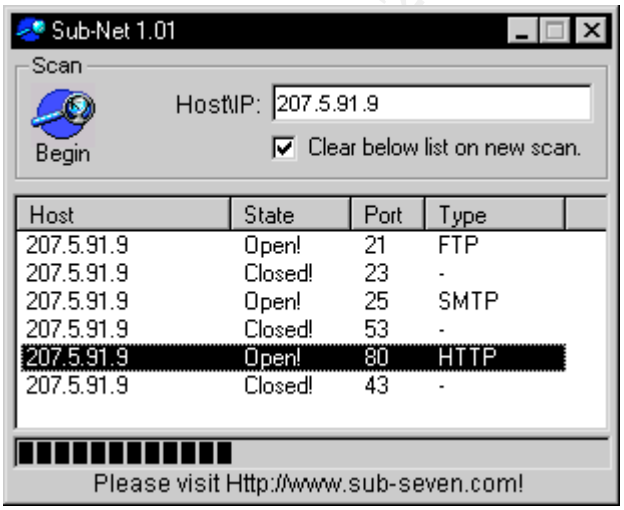
During the audit the GIAC network security team will make use of port scanners.

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

Here is article by http://www.islandnet.com/~cliffmcc/portscanner.html that lists a number of free port scanners:

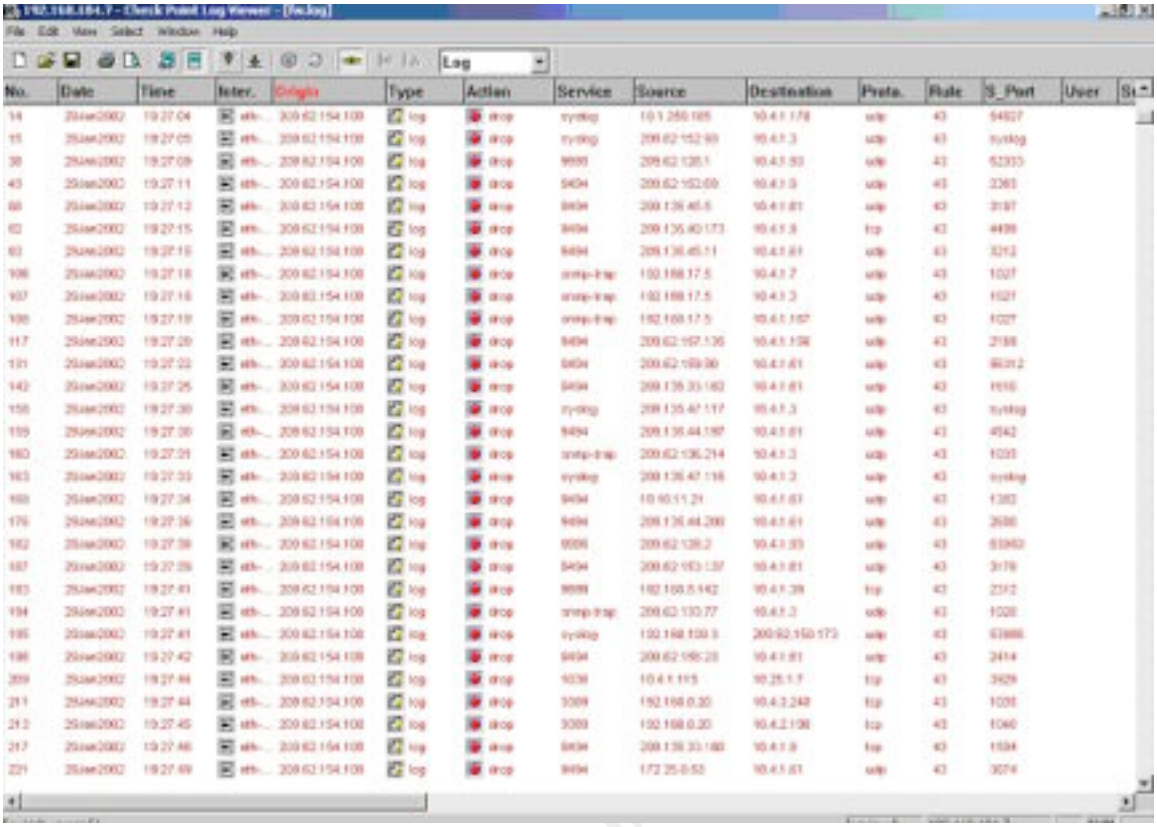
> To measure your computer's port vulnerability, you can download one (or more) of several freeware and shareware port scanners. Install these packages, let them scan, and read the results to determine potential problem areas. Blue Globe Software, for example, offers a program called Port Scanner http://www.islandnet.com/~cliffmcc/portscanner.html that is extremely simple yet effective enough if you want quick results.
>
> Atelier Web Security Port Scanner http://www.atelierweb.com has a more sophisticated look and better reporting, but essentially its functions are similar. Cyrosoft Software's Necrosoft NScan (Web site) offers Whois and Traceroute functions, as well as good flexibility in customizing scans. Similarly, Raw Logic Software's NetView Scanner (Web site) provides details about vulnerable ports and additional tools for detecting network clients that have Windows file and print sharing enabled. Sub Seven Software offers the freeware program Sub-Net (Web site), specializing in Trojan horse scanning on your ports. If you're working in Linux, go to Insecure.org's NMAP (Web site) to check out a comprehensive port scanner for large networks. Among other things, visiting the NMAP site and clicking Exploit World gives you an idea of how many ways a hacker can get at you.

From the options above we used the Sub Seven Software Sub-Net scanner to check the open ports on the Service Network. A sample of the reporting is shown below:



As mentioned, we viewed the firewall logs during the audit to confirm that security policy is working as intended. Below is a sample of the logging traffic during the audit.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



As shown, all of the traffic is being dropped. This screen is encouraging, but some of the scans into to our service network were successful.

When the Logging GUI is not available, you can use tcpdump to watch the traffic. While it is somewhat cryptic compared with the GUI, it does provide a great deal of information. Most importantly, it goes beyond just the initial syn / ack traffic the Check Point logs capture.

Tcpdump on outside interface of the GFC Firewall:

```
tcpdump: listening on eth-s3p1c0
07:21:34.100516 209.135.36.172.22 > 10.40.3.254.47351: P 2716292947:2716292999(52) ack 3483940651 win
16384 [tos 0x10]
07:21:34.144233 10.40.3.254.47351 > 209.135.36.172.22: . ack 52 win 9216 (DF)
07:21:34.880516 209.135.46.216.55772 > 208.241.240.12.53: 44564+ (34) (DF)
07:21:34.881689 208.241.240.12.53 > 209.135.46.216.55772: 44564 NXDomain* 0/1/0 (85)
07:21:34.883217 209.135.46.216.55773 > 208.241.240.12.53: 44565+ (38) (DF)
07:21:34.884157 208.241.240.12.53 > 209.135.46.216.55773: 44565 NXDomain* 0/1/0 (90)
07:21:34.885472 209.135.46.216.55774 > 208.241.240.12.53: 44566+ A? msuawi08. (26) (DF)
07:21:34.886368 208.241.240.12.53 > 209.135.46.216.55774: 44566 NXDomain* 0/1/0 (101)
```

Above we note the ssh connection from the NOC network to the ftp server. When you set up a tcpdump, you can define the traffic to provide for a more focused analysis. For example, tcpdump -i eth-s1p1c0 host 209.62.158.199 and port 80 is only listening on the inside interface for traffic to or from host 209.62.158.199 on port 80.
There is yet another option for viewing traffic. On the firewall itself, not the GUI, type:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"fw log –f" for real time traffic. But note that the traffic will likely scroll by so quickly that you will not be able to read it. To stop the traffic, hit CRTL C – many, many times to stop the logging. You can scroll up to view the captured traffic.

fw log can be configured a bit. Use fw log --help to check out the configuration options available.

```
fw log --help
fw log usage options: [-f[t]] [-l] [ -c action] [-h host] [-s starttime] [-e endtime] [-b stime etime]
[logfile]
```

During the audit, we ran netstat –an on the GFC Firewall to determine what port were listening. The results were somewhat surprising. Here is a result of netstat –an test.

```
GFCFW01 [admin]# netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  *.23                   *.*                    LISTEN
tcp        0      0  *.80                   *.*                    LISTEN
tcp        0      0  *.256                  *.*                    LISTEN
tcp        0      0  *.259                  *.*                    LISTEN
tcp        0      0  *.262                  *.*                    LISTEN
tcp        0      0  *.264                  *.*                    LISTEN
tcp        0      0  *.265                  *.*                    LISTEN
tcp        0      0  *.900                  *.*                    LISTEN
tcp        0      0  *.1026                 *.*                    LISTEN
tcp        0      0  *.1027                 *.*                    LISTEN
tcp        0      0  *.1028                 *.*                    LISTEN
tcp        0      0  *.1029                 *.*                    LISTEN
tcp        0      0  *.1030                 *.*                    LISTEN
tcp        0      0  *.1031                 *.*                    LISTEN
tcp        0      0  *.18183                *.*                    LISTEN
tcp        0      0  *.18184                *.*                    LISTEN
tcp        0      0  *.19190                *.*                    LISTEN
tcp        6      0  127.0.0.1.1032         127.0.0.1.19190        ESTABLISHED
tcp        3      0  127.0.0.1.1036         127.0.0.1.19190        ESTABLISHED
tcp        0      0  127.0.0.1.19190        127.0.0.1.1032         ESTABLISHED
tcp        0      0  127.0.0.1.19190        127.0.0.1.1036         ESTABLISHED
tcp        0      0  172.16.5.225.256       172.16.5.226.1045      ESTABLISHED
tcp        0      0  172.16.5.225.1038      172.16.5.226.256       ESTABLISHED
tcp        0    624  209.135.36.172.22      10.40.3.254.47351      ESTABLISHED
tcp        0      0  209.135.36.172.1061    192.168.185.71.257     ESTABLISHED
udp        0      0  *.259                  *.*
udp        0      0  *.260                  *.*
udp        0      0  *.514                  *.*
udp        0      0  *.500                  *.*
udp        0      0  *.1025                 *.*
udp        0      0  *.161                  *.*
GFCFW01 [admin]#
```

Of greatest concern is the fact that our firewall is actually listening on ports 80 and 23. These services clear should have been locked down during the configuration of our Nokia firewall. The Nokia device can be configured through voyager, which provides GUI / Web interface for administration, on port 80. SSH over port 22 is much more secure way to configure the firewall.

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

But if the voyager is used, it should only be turned on temporarily through the lynx connection via SSH. The telnet service (port 23) should be turned off.

Next we have a netstat –an report on our Web Server.

```
msuawi04{root}:/root: netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  209.135.45.52.63845    209.135.45.52.1221     TIME_WAIT
tcp        0      0  *.80                   *.*                    LISTEN
tcp        0      0  *.13783                *.*                    LISTEN
tcp        0      0  *.13782                *.*                    LISTEN
tcp        0      0  209.135.45.52.1305     208.241.240.50.36002   ESTABLISHED
tcp        0      0  *.1303                 *.*                    LISTEN
tcp        0      0  *.9494                 *.*                    LISTEN
tcp        0      0  *.1221                 *.*                    LISTEN
tcp        0      0  *.444                  *.*                    LISTEN
tcp        0      0  *.443                  *.*                    LISTEN
tcp        0      0  *.111                  *.*                    LISTEN
tcp        0      0  *.2121                 *.*                    LISTEN
tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  209.135.45.52.22       10.2.1.25.65148        ESTABLISHED
udp        0      0  *.514                  *.*
udp        0      0  *.111                  *.*
udp        0      0  *.*                    *.*
udp        0      0  *.49152                *.*
udp        0      0  *.123                  *.*
```

As predicted, we find that port 80 and 443 are listening and we see some established traffic (hopefully bringing in more $). We also see our own established ssh (port 22) connection from the NOC network. But there are a number of ports listening that maybe cause for alarm. These results will be researched and reviewed with the web server administrator.

3.3 Evaluate the audit. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures.

Note: This audit will be direct toward the Service Network only, although the findings of this audit will be put to use to enhance the corporate firewall and project the internal networks.

The networking security staff, as predicted, learned a great deal by performing the audit in-house. We learned that we are not quite as smart as we thought we were. The more research we did the more we found that we did not know. But we've learning and the security of the GIAC perimeter will improve it day.

Recommendations to improve the security of the Service Network:

Add a redundant firewall – The Nokia/Check Point firewall solution was chosen during the planning phase of the Fortune Cookie network design, because of its ability to provide a

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

redundant solution. We recommend that we move forward on implementing that high availability solution as soon as possible. Refer to Nokia's online posting on "High Availability to Ensure Continuous Internet Connectivity", which presents a good overview on how this solution works. [13]

The audit research lead me to a number of resources that suggest ways to improve the security and performance of Check Point Firewall-1. I will list among the best here: www.phoneboy.com posted entry for " FireWall-1FAQ: Improving Performance". [14]

> Q:
> What things can I do to improve performance for my FireWall-1box?
> A
> While not a complete list, here are some things I would do:
> Put the most commonly used rules at the top of the rulebase.
> Reduce the number of rules by combining similar rules.
> Reduce or eliminate the use of the security servers.
> Do not use Domain objects.
> Use "networks" instead of address ranges in address translation.
> If using Session Authentication, use the Implicit Client Auth trick.
> Where possible, do not use the Security Servers.
> Reduce logging.

I strongly suggest that we follow these recommendations for current and future configuration of our firewalls.

Add a multiple Web Servers – to provide redundancy and to serve more concurrent users - more customers. Load balancing would also be implemented as part of this upgrade. Adding additional web servers not only enhances our security, by limiting threats such as virus, Trojans and denial of service attacks, but it will also increase our business potential. This recommendation will likely receive the backing of many departments and ultimately be approved by upper management. Adding additional servers to the service network will give the network security team more to protect, which means more work, but the benefits will greatly out weigh those costs.

Being careful not to insult any department or GIAC employees, recommendations will be made that it is time to start running our company like a $200 million company – form a technology perspective. Expansion and growth were built into the design during the planning of the GIAC Fortune Cookie Company. It is time reinvest some of our $200 million to expand and improve GIAC's network security.

Additional Recommendations:

I strongly recommend additional training for the network security staff. Additional training will have the obvious benefit of expanding the knowledge of our staff, but will also assist in our goal of employee retention. Training suggestions include additional Cisco, Nokia, and Check Point

[13] http://www.nokia.com/securenetworksolutions/hot_standby.html
[14] Welch-Abernathy, Dameon D., www.phoneboy.com, "FireWall-1 FAQ: Improving Performance".

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

training to learn more about the perimeter defense products we are currently using. I will also recommend non-vendor specific training such as that SANS Institute – particularly their Intrusion Detection course. Intrusion detection is area were we are admittedly weak.
Audit the Corporate Firewall as soon as possible. I recommend that the secondary or redundant firewall be added to the service network first, and we will move on to the Corporate Network audit soon there after. I recommend that the corporate network audit included a check to insure that each machine has the corporate edition of Norton anti virus software loaded, being used properly and is up to date. [15]

When the network security team moves on the next audit, I recommend the plans outlined in Lance Spitzner's, "Auditing Your Firewall Setup" [16] be put into practice. After completing corporate network audit, I recommend that the network security team provide an in-house security-training seminar for all GIAC employees. Educating our end users on security will augment on our perimeter defenses and help will help secure our internal assets.

Assignment 4 – Design Under Fire

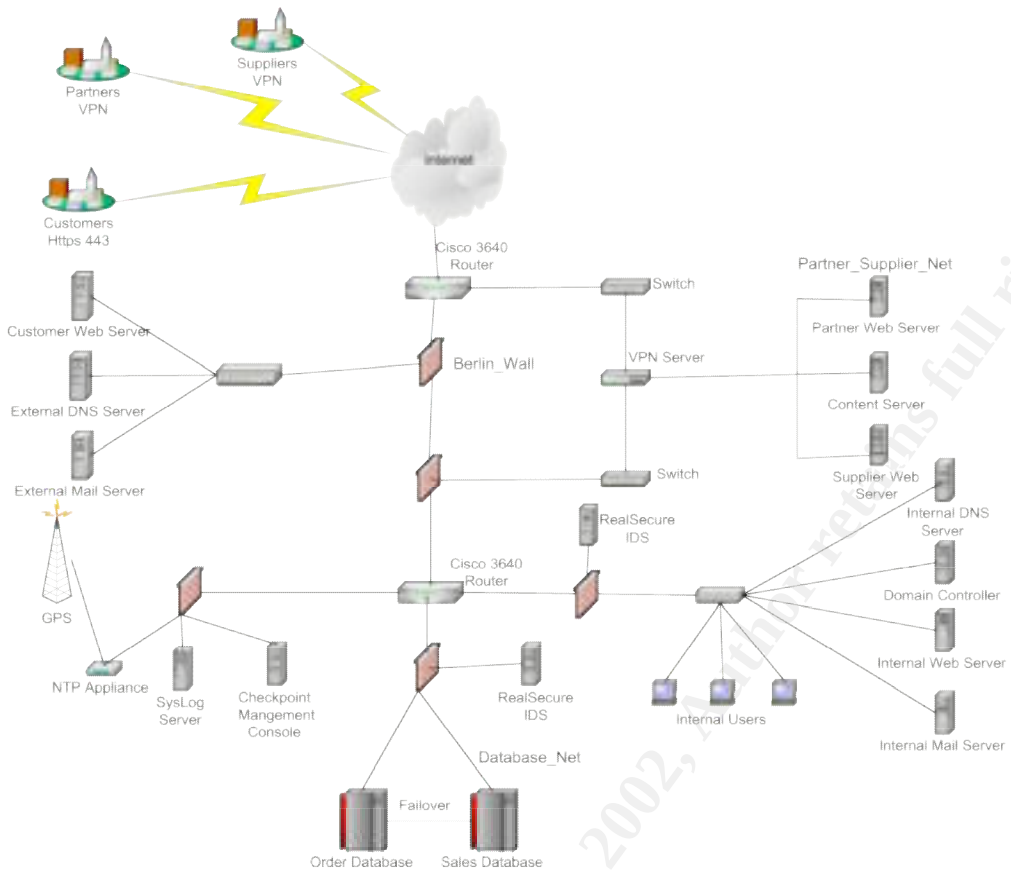
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design.

4.1 "Select a Target" *Select a network design from any previously posted GCFW practical (http://www.giac.org/GCFW.php) and paste the graphic into your submission. Be certain to list the URL of the practical you are using.*

I have select Brandon Board's network design submitted October 2001 as my target.[17] I have chosen Brandon design because it uses much of the same technology that I have used in my design. I felt that I would gain the most knowledge from researching (and attempting to exploit) the vulnerabilities in the design.

© SANS Institute 2000 - 2002 Author retains full rights.

[15] Norton AntiVirus™ Corporate Edition 7.6, http://enterprisesecurity.symantec.com
[16] Spitzner, Lance "Auditing Your Firewall Setup" http://www.enteract.com/~lspitz
Last Modified: 12 December, 2000
[17] Brandon Board's practical appears on http://www.giac.org/practical/Brandon_Board_GCFW.zip



4.2 "Attack Selection" *Research and design two of the following three types of attacks against the architecture: An attack against the firewall itself, a denial of service attack or an attack plan to compromise an internal system through the perimeter system.*

I have chosen to research and design an attack against the firewall itself and a denial of service attack. I made these selections because I feel from the outset that they will be out of the greatest benefit to me – at this time. Working these types of attacks will help me on focus on how to defend against threats to my network design as listed in Assignment Two and, more importantly, help me in my current position in "The Real World".

4.3 "The Firewall Under Review" *Research and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design.*

Research began with the posting on www.phoneboy.com, arguably the best single source of information about actually using Check Point. Found on the Phoneboy home page are the FireWall-1 Security Alerts:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FireWall-1 Security Alerts (Updated 14 October 2001)[18]

NOTICE: FireWall-1 4.1 SP5 (and earlier SPs) on IPSO has a problem with SYNDefender in Active Gateway mode with NAT that causes packets with untranslated addresses to leak out. A hotfix for 4.1 SP5 is available on Check Point's Software Subscription page.

NOTICE: All versions of FireWall-1 (up to version 4.1 SP4) allow the service RDP (UDP Port 259) through the firewall by default. A hotfix is available from here <http://www.checkpoint.com/techsupport/downloads.html>. More information <http://www.inside-security.de/advisories/fw1_rdp.html>.

NOTICE: If you're ***not*** running FireWall-1 4.0 SP7 (Solaris, NT, AIX, HPUX, Linux), FireWall-1 4.0 SP5 build 13 (IPSO), or FireWall-1 4.1 SP2 (all platforms) or later, you are vulnerable to a number of security issues. These issues were revealed at the Black Hat 2000 <http://www.blackhat.com> conference and are extremely serious in nature. You can read all about the vulnerabilities here <docs/bh2000/> .

NOTICE: A vulnerability in FAST MODE was found to exist, which people could use to get around the security policy. Note that this is not the default behavior, so you should only be vulnerable if you've explicitly enabled this feature for a TCP service. Either disable FAST MODE, upgrade to 4.1 SP3 (now available) or upgrade to 4.0 SP8 (available for all platforms except Nokia). Note that Check Point will remove this feature in the next major release since recent performance enhancements have reduced the effectiveness of this feature.

4.3.1 Check Point FireWall-1 RDP Bypass Vulnerability[19]

The latest version of this document is available at http://www.inside-security.de/fw1_rdp.html

The proof of concept code is available at http://www.inside-security.de/fw1_rdp_poc.html

Summary:
It is possible to bypass FireWall-1 with faked RDP packets if the default implied rules are being used. RDP (Reliable Data Protocol, but not the one specified in RFCs 908/1151, a Check Point proprietary one) is used by FireWall-1 on top of the User Datagram Protocol (UDP) to establish encrypted sessions. FireWall-1 management rules allow arbitrary eitherbound RDP connections to traverse the firewall. Only the destination port (259) and the RDP command are verified by FireWall-1. By adding a faked RDP header to normal UDP traffic any content can be passed to port 259 on any remote host on either side of the firewall. Implied rules can't be easily modified or removed (except all together) with the FireWall-1 policy editor.

Impact:
Given access to hosts on both sides of a firewall a tunnel to bypass the firewall could be built using this vulnerability. Such access could be gained with a trojan horse that uses this

[18] Welch-Abernathy, Dameon D. www.phoneboy.com FireWall-1 Security Alerts (Updated 14 October 2001)
[19] http://www.inside-security.de/fw1_rdp.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

vulnerability to connect from the inside back to the machine of the attacker. But also arbitrary connections from the outside to machines behind the firewall (even if they are supposedly totally blocked from the in- and outside by the firewall) can be established, for example to communicate with infiltrated programs like viruses.

Affected systems:
Check Point VPN-1(TM) & FireWall-1(R) Version 4.1

Releases tested:
Build 41439 [VPN + DES]
Build 41439 [VPN + DES + STRONG]
Build 41716 [VPN + DES + STRONG] (SP2)

Vendor status:
The vulnerability has been reported to Check Point and a fix is scheduled for today [2001-07-09]. We want to thank Check Point Software Technologies for their quick reaction.

Proof of concept code:
<http://www.inside-security.de/fw1_rdp_poc.html>

Suggested workarounds:
- Comment line 2646 of base.def (accept_fw1_rdp;)
- Deactivate implied rules in the Check Point policy editor (and build your own rules for management connections).
- Block UDP traffic to port 259 on your perimeter router.

Solution:
Apply the fix available from Check Point:
<http://www.checkpoint.com/techsupport/alerts/rdp.html>

Credits: This vulnerability was found and documented by Jochen Thomas Bauer <jtb@inside-security.de> and Boris Wesslowski <bw@inside-security.de> of Inside Security GmbH, Stuttgart, Germany.

4.3.2 Check Point FireWall-1 GUI Buffer Overflow [20]

I have made the assumption that Brandon's design is using a Check Point's Management Server on a Windows machine. If that is in fact the case the following vulnerability could be exploited. This vulnerability, however is only an issue in the hands of a malicious administrator or a very skill social engineer. Neither of these conditions is very likely, but researching the issue seems warranted none the less. The vulnerability list on http://www.checkpoint.com/techsupport/alerts/buffer_overflow.html follows below:

Check Point FireWall-1 GUI Buffer Overflow

[20] http://www.checkpoint.com/techsupport/alerts/buffer_overflow.html

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

Summary:
An issue exists in VPN-1/FireWall-1 Management Server running on Windows NT or Windows 2000. A malicious administrator can exploit a buffer overflow condition in the GUI authentication code to potentially impair management station functionality or to execute code. Any attack must come from an IP address explicitly defined as an authorized GUI client. Only management stations running Windows NT or Windows 2000 are affected. This includes any standalone VPN-1/FireWall-1 Gateways (with Management Server and enforcement points installed on the same machine), but does not include module-only (enforcement point) installations.
This issue affects VPN-1/FireWall-1 4.0, 4.1, and Next Generation systems. Hotfixes for VPN-1/FireWall-1 4.0 SP8, 4.1 SP4, 4.1 SP5, and Next Generation Hotfix-2 are available for immediate download at http://www.checkpoint.com/techsupport/index.html <../index.html>.

Solution:
Apply the relevant GUI Buffer Overflow Hotfix to the management station.

Who is affected:
All installations of VPN-1/FireWall-1 with Management Servers running on Windows NT or Windows 2000.

Immediate workaround:
Allow GUI connections only from trusted hosts.
Changes made in the Hotfix:
The buffer checking on the Management Server has been improved.

Download Information:
The GUI Buffer Overflow Hotfix is available for immediate download at the Software Subscription Download Site <../downloads/downloads.html> for the following versions:
VPN-1/FireWall-1 4.0 SP8
VPN-1/FireWall-1 4.1 SP4
VPN-1/FireWall-1 4.1 SP5
VPN-1/FireWall-1 NG HF2

NOTE: Management Servers with versions older than those listed above must be first upgraded and then have the GUI Buffer Overflow Hotfix applied.

4.3.3 "Denial of Service reported on RealSecure Network Sensor"

Brandon's design makes use of RealSecure so I did research on any known vulnerabilities.

http://www.checkpoint.com/techsupport/alerts/rsdos.html lists "Denial of Service reported on RealSecure Network Sensor" The listing on Check Point's Tech Support site follows:

March 12, 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NetSec, whose purpose for DOS testing was to advocate improved software quality, has kindly shared their paper, utility and testing configuration with ISS. ISS has thus been able to reproduce the tests.

Summary:
The "Stick" exploit creates a flood of attacks. When the Tribal_Flood_Network signature is checked on, all versions are susceptible to engine stoppage. Versions prior to Network Sensor 5.0, MicroUpdate 1.2 also encounter the same behavior when the Trinoo_Daemon signature is checked on. The engine must be restarted from the console.

As this exploit is not currently in the wild, ISS will deliver a fix for the Tribal_Flood_Network signature with the twenty plus new signatures scheduled for the next XPU, expected availability March 15. Should the exploit become available sooner, ISS will accelerate the fix.

Finally, as the NetSec paper states, a flood of events can obscure the true attack.

In conclusion, the RealSecure Network Sensor stops in certain conditions or receives a flood of events with the NetSec exploit tool. However, if this happens to a Sensor, the user will clearly know that there is malicious activity on the monitored network.

The NetSec report's premise is that "When a high number of false alarms occur, the shear [sic] number of alarms makes the alarm data useless in informing the decision makers of the real status of the network." The paper urges IDS technology to improve false positives and be more aware whether an attack is real or not. ISS is taking steps in this direction with plans to evolve our solutions to the next level of intrusion detection technology.

Details for the exploit called "Stick"

- All versions of Network Sensor with Tribal_Flood_Network signature
- Versions prior to Network Sensor5.0, MicroUpdate 1.2 with Trinoo_Daemon signature

The problem is defined as follows: If the signature is turned ON, the engine will stop running almost immediately after the Stick program fires. The Event Channel Status on the console will display "An error has occurred in an event channel. The Sensor Status is "Stopped". The engine must be restarted from the console.

Work-Around:
If it becomes necessary prior to the availability of MicroUpdate 2.2, you can protect yourself from it by ensuring that your RealSecure Network Sensor is at version 5.0 MU 1.2 or higher, and by turning off the Tribal_Flood_Network signature. If you continue to use versions prior to 5.0 MU 1.2, you would also turn off the Trinoo_Daemon signature.

The only other issue observed was an overflow of UDPBomb events during the Stick run. This was lessened by setting up an event filter in the Advanced section for the UDPBomb signature in the Policy Editor.

4.5.3 The Attack

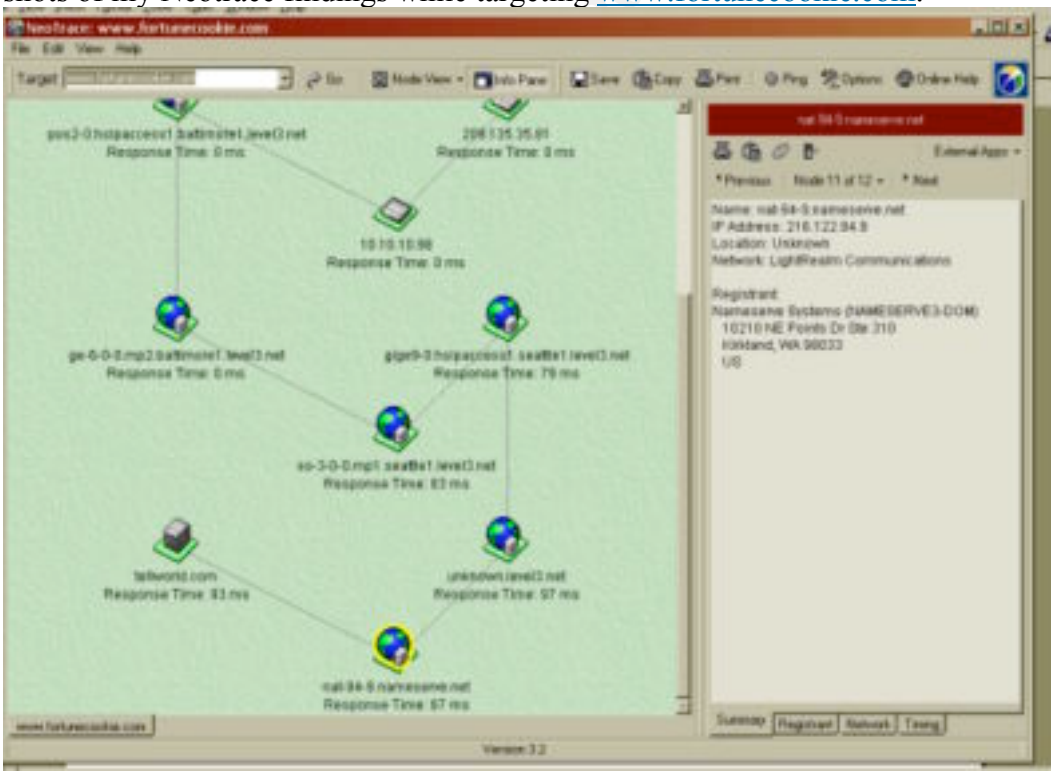
I have chosen the Check Point FireWall-1 RDP Bypass vulnerability as a potential way to attack Brandon's design. Testing my own firewall, I found that port 259 was open and listening, as also shown in my audit. Before trying to attempt to fake a RDP header linked to normal UDP

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

traffic, I will attempt to test the port 259 on Brandon's firewall "the Berlin Wall". First I need to try to learn the IP address of the Berlin Wall. This process will begin with simple traceroutes to the web customer web server followed by a Neotrace to the web server.[21]

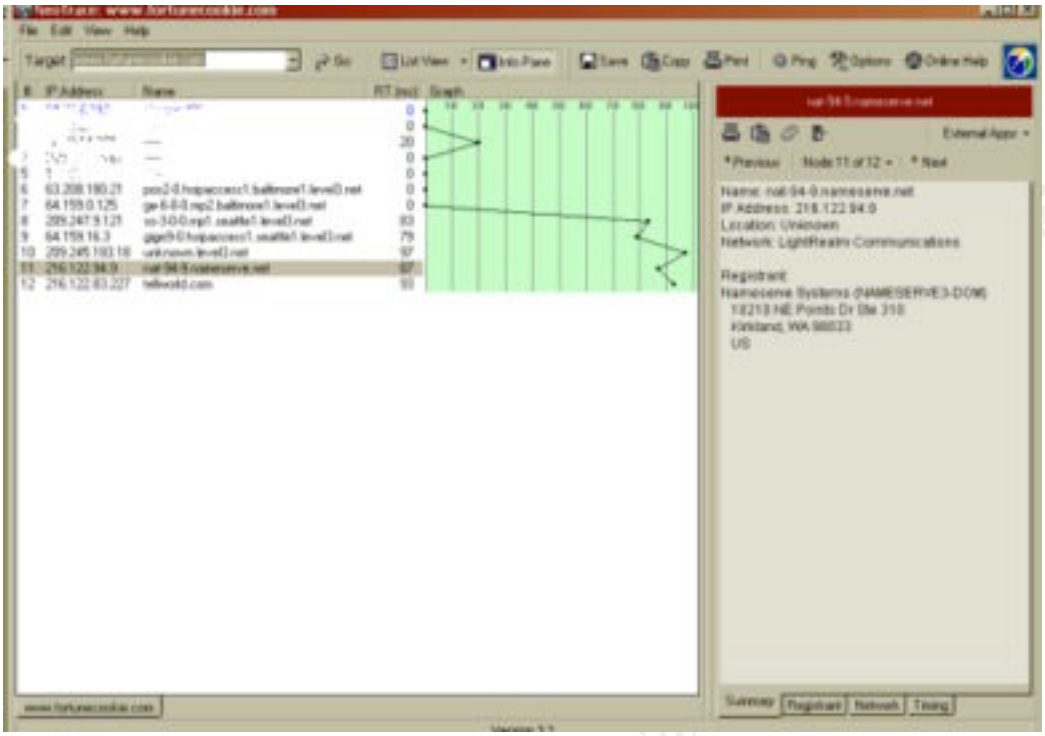
```
C:\>tracert 216.122.83.227
Tracing route to fortunecookie.com [216.122.83.227]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  1x.x.x
  2   <10 ms   <10 ms   <10 ms  1x.x.x.
  3   <10 ms   <10 ms   <10 ms  1.x.x.x
  4   <10 ms   <10 ms   <10 ms  1x.x.x.
  5   <10 ms   <10 ms   <10 ms  pos2-0.hsipaccess1.Baltimore1.Level3.net [63.208.180.21]
  6   <10 ms   <10 ms   <10 ms  ge-6-0-0.mp2.Baltimore1.Level3.net [64.159.0.125]
  7    60 ms    71 ms    70 ms  so-3-0-0.mp1.Seattle1.Level3.net [209.247.9.121]
  8    60 ms    70 ms    70 ms  gige9-0.hsipaccess1.Seattle1.Level3.net [64.159.16.3]
  9    70 ms    80 ms    80 ms  unknown.Level3.net [209.245.183.18]
 10   151 ms    80 ms    90 ms  nat-94-9.nameserve.net [216.122.94.9]
 11    70 ms    80 ms    70 ms  tellworld.com [216.122.83.227]

Trace complete.

C:\>
```

The information in Neotrace is very useful towards planning the attack. Listed below are screen shots of my Neotrace findings while targeting www.fortunecookie.com.



[21] Neotrace http://mcafeestore.beyond.com/Product/0,1057,3-18-SN107878,00.html
Product also used to provide Screen shots

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



The Neotrace provides us the IP of the Web Server, its location and the path leading to its door. I have confirmed that the Web Server IP by telnetting to the IP over port 80, which responded successfully. C:\>telnet 216.122.83.227 80

From the information in the Neotrace shows the hop prior to the web server is 216.122.94.9 – which may or may not be the Berlin Wall. I will not assume that this IP is in fact the Berlin Wall, but will attempt to telnet over 259. This attempt was unsuccessful, but I know I am close. While I am tempted to attempt some social engineering by call fortune.cookie.com posing as an employee of level3.net – likely their ISP in Seattle, I will be at bit more tactful. I will telnet over 259 from one of the compromised dsl systems. In time I will find a my target, and be prompted with a command line screen –

Check Point Fireall-1 Client Authenication Server running on berlinwall01
User:

From the this point, I will set up numerous telnet connection over port 259 from the 50 compromised cable modem systems. The CPU hit on the Berlin Wall during this attack, assuming the router is not deny the traffic, would likely be strong enough the bring the firewall to its knees if not crash it. At the very least the traffic to the Web server would be disrupted.

4.5.2 Conclusions

The researching the vulnerabilities of Check Point's FireWall-1, I found that there are many known weakness of the earlier versions. However, there are not that many documented vulnerabilities for the new versions – 4.1 SP3 and higher. This made attacking Brandon's design

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

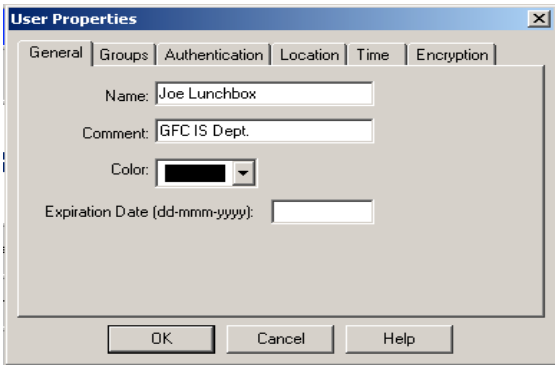
very difficult, and hopefully would make attacking my own system difficult as well. Many of the Internet attacks today are making use of exploits through http (port 80) and through mail messages carrying viruses (port 25). Having a presence on the Internet with a web and or mail server creates a difficult task for network security engineers. The need for a strong intrusion detection system is becoming increasingly important. It is not enough to have just a strong perimeter is not enough anymore. You need to employ defenses against the traffic you willing allow into your network – making use on content security servers, intrusion detection systems and virus protection systems. Protecting a network connected to the Internet is quite literally a "constant battle between good and evil". To stay head of the curve, you must continue to educate yourself and you users about Internet security.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

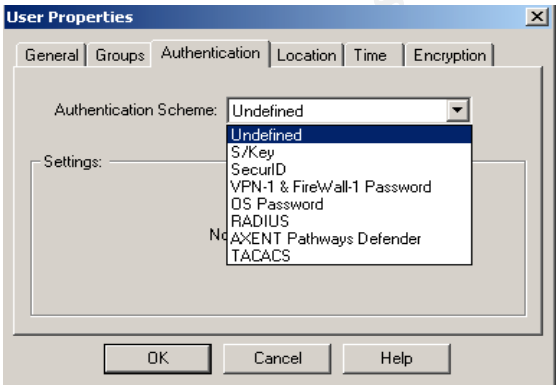
Additional Resources:

Installing SecuRemote Users :



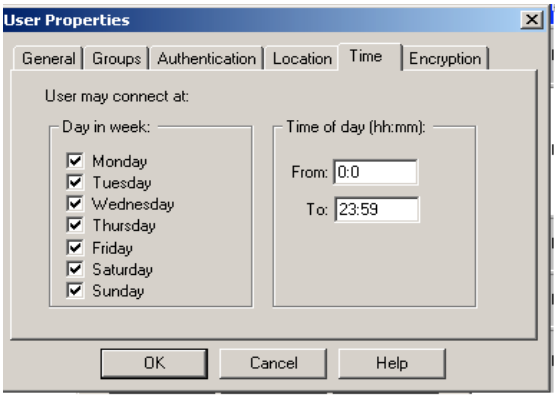
1. General Tab: Used to define the user name, Additional comments

2. Group Tab: To assign the users to a specific group or groups

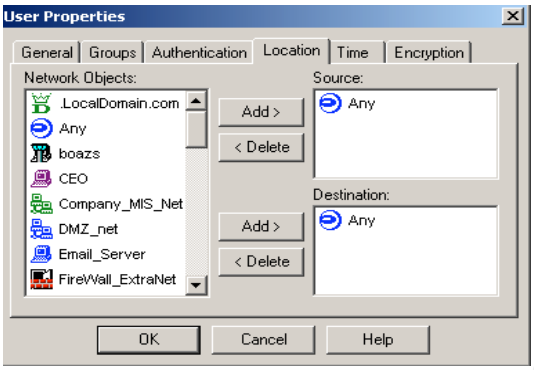


3. Authentication Tab: Define the type Authentication to be used. In the GFC environment SecurID and the VPN-1 & Firewall-1 Password will be used.

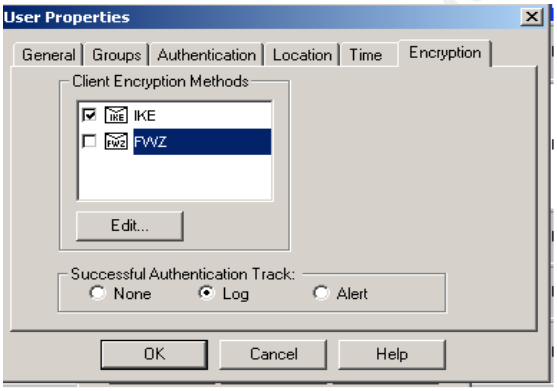
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



4. Time Tab: Can used to further restrict access of a SecuRemote User.



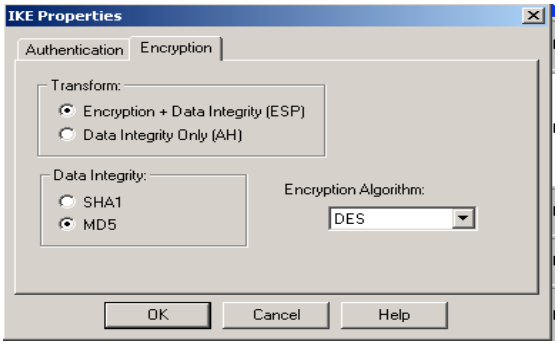
5. Location Tab: Used to further define the source(s) and destination (s) to which the secure remote users to have access to and from.



6. Encryption Tab: Used to define the encryption method(s). In our case, IKE will be used.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7. IKE Properties Authentication Tab: Used to define password of public key authentication



8. IKE Properties Encryption Tab: Used to define ESP, AH, SHA1 or MD5 and the encryption algorithm of DES, DES-40CP or CAST-40

References:

1. Berhstein, Terry, et al., Internet Security for Business, New York, NY: John Wiley & Sons, 1996

2. Dietrich, David
Check Point VPN-1 and Cisco PIX Gateway to Gateway IKE VPN Using Pre-shared Secrets May 19, 2000 Version 1.0 2000 Check Point Software Technologies LTD.

3. SANS Institute Track 2 Firewalls, Perimeter Protection and Virtual Private Networks, 2.2 Firewalls 101: Perimeter Protection with Firewalls.

4. Spitnzer, Lance
http://www.enteract.com/~lspitz/

5. www.checkpoint.com
6. www.phoneboy.com
7.www.securityfocus.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8. http://www.snort.org/

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