Global Information Assurance Certification Paper

GIAC CERTIFIED FIREWALL ANALYST (GCFW)

Practical Assignment

Version 1.9

Robert Sorensen

March 28, 2003

Abstract

This practical assignment will demonstrate network and perimeter defense techniques needed to secure a successful on-line eBusiness called GIAC Fortune Cookie Sayings (eFortCS.) Part one will define eFortCS business requirements and a proposed network architecture. Part two will detail security policy for both the perimeter router as well as a high available firewall and other in-depth defense strategies. Part three will demonstrate an audit against the proposed eBusiness site, and finally, part four will explore a network design under attack.

Part One: SECURITY ARCHITECTURE

BACKGROUND

GIAC Enterprises e-business Fortune Cookie Sales ("GIAC eFortCS") is a very aggressive new on-line business that is taking the Internet by storm. They have entered into a marketing agreement with the National Basketball Association (TM) drawing on the popularity of one of its newest stars in Yao Ming. In fact, Yao Ming has consented to be the official spokesperson for eFortCS. Fortune cookies sales are expected to see a 50% increase in sales in the next four years.

EfortCS e-Business operations will consider the following components for the business plan:

	**Customers** EfortCS will have a worldwide customer base to include individual or companies. With the marketing prowess of the NBA, fortune cookie sayings will be very popular.
	**Suppliers** The Chinese Sports Federation will be contracted to provide fortune cookie sayings. The overall theme of the sayings will be sports. EfortCS will expand to other international sports federations in the near future.
	**Partners** The NBA will be a very important partner in this enterprise. The other partner will be a well-known translation service company located in Beijing, China. The sayings will be translated into 30 different languages. Since the NBA has international marketing arrangements, eFortCS will have a direct tie-in.
	**EfortCS Enterprise Employees** EfortCS core enterprise employees located on the eFortCS internal networks. They will insure the integrity and security of the fortune cookie sayings.
	**EfortCS Mobile Sales Force and Teleworkers** EfortCS mobile sales force will be located in cities where NBA teams are located. They will work closely with the marketing group of each team to formulate promotions. Given the high availability of broadband Internet connectivity, a small group of employees will be working from home to help with the accounting and financial aspects of the business.

Business Requirements

Customers

Customers will purchase bulk on line fortunes via the Internet using a web browser that supports128-bit SSL encryption. The eFortCS web portal uses an OpenSSL-enabled Apache web server that is interfaced with mySQL database. This configuration will allow customers to view samples, create accounts, purchase fortunes, and download bulk fortune cookie sayings.

All customer registrations and purchases will be conducted over a 128-bit SSL connection ("HTTPS"). Initial browsing of the eFortCS.com web site for pricing and information will be using the HTTP protocol.

Suppliers

All access for the Chinese Sports Federation will be conducted using a 128-bit SSL web portal to the mySQL database. They will be able to view accounting information, access the sayings database, and submit fortunes via the web portal. The portal will provide a means to mass load fortune cookie sayings. By allowing them to upload direct to the database, it will insure the fortune cookie sayings are current.

Partners

The business partner in Beijing will also have direct access to the web portal using 128-bit SSL encryption. The firm in Beijing is internationally well known with the ability to translate the sayings into 30 different languages. All translated sayings will be uploaded to the mySQL database through SSL encrypted tunnel via the web portal. All other correspondence via email will be encrypted using PGP.

Local Employees

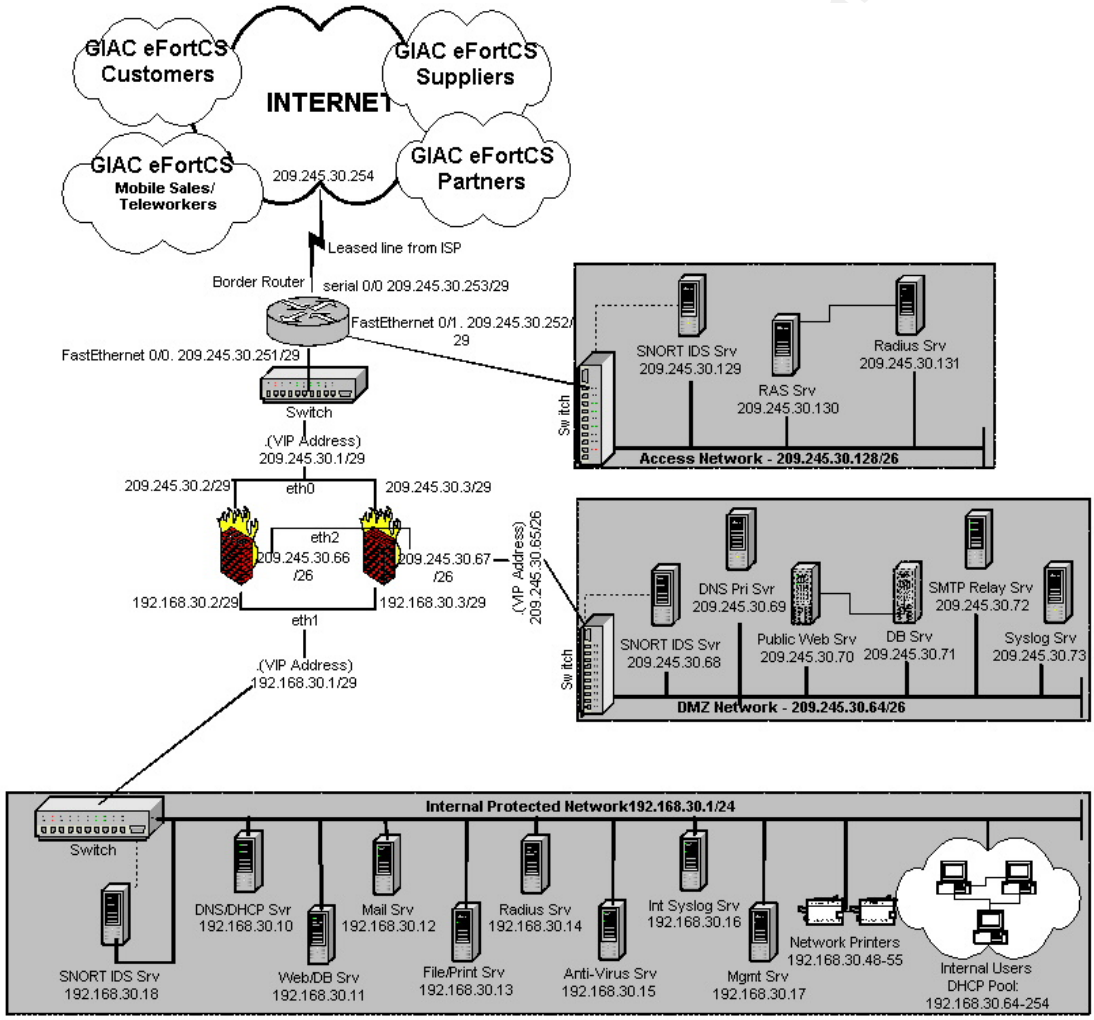
Local eFortCS employees will be allowed access for web (http/https), email, and ftp for file transfers. Internal access will be to the local file and print server. An Internet access usage policy will be read and signed. Sys admins will access local servers only through SSH. Internal users will access the web/DB servers on DMZ via SSH. All internal computers will have Norton Anti-virus software and ZoneAlarm Pro personal firewall software.

Remote Employees

Remote sales and telecommuting users will access the internal resources at eFortCS via SecuRemote VPN software that integrates with Check Point firewall. In addition to VPN software, all remote users will also have Norton AntiVirus software and ZoneAlarm Pro personal firewall software installed. Some remote users have Broadband Internet connectivity. Those employees who require dial-in access will be allowed to connect to a modem pool that will be set up on the access network. A toll-free number will be provided for the convenience of the employees. Authentication to either the modem pool or VPN will be by a hardware authenticator card that generates one-time passwords. All access to the internal network via modem pool is through SecuRemote.

Network Security Design/Architecture

The eFortCS network is shown below. The network will consist of one external network ("DMZ") tied to a High Available ("HA") firewall configured in hot-standby mode. This will provide the needed availability as well as the means to do system maintenance without bringing down the firewall.



Addressing Scheme

Non-routable addresses are used for the internal protected network. EFortCS has contracted with a leading ISP for its Internet connectivity. The ISP has provided eFortCS with a class C address. The following table outlines the network address allocation:

Network Segment	*Network Address/Mask*
External Network/Router	209.245.30.248/29
External Network/Firewall	209.245.30.0/29
Access Network	209.245.30.128/26
DMZ Network	209.245.30.64/26
Internal Protected Network	192.168.30.1/24

IP	*Description*
209.245.30.1	Virtual IP (VIP) address of external interfaces of firewall
209.245.30.2	Physical firewall external interface of node one
209.245.30.3	Physical firewall external interface of node two
209.245.30.65	Virtual (VIP) address of DMZ interfaces of firewall
209.245.30.66	Physical firewall DMZ interface of node one
209.245.30.67	Physical firewall DMZ interface of node two
209.245.30.68	DMZ SNORT IDS Server
209.245.30.69	Public DNS Server
209.245.30.70	Public Web Server
209.245.30.71	Public DB Server
209.245.30.72	SMTP Relay Server
209.245.30.73	External Sys Log Server
209.245.30.129	SNORT IDS Server
209.245.30.130	RAS/Modem Pool Server
209.245.30.131	Radius Server (Authenticate Modem Pool)
209.245.30.132-190	Reserved for modem pool (RAS Server)
192.168.30.1	Virtual (VIP) address of internal interfaces of firewall
192.168.30.2	Physical firewall internal interface of node one
192.168.30.3	Physical firewall internal interface of node one
192.168.30.10	DNS/DHCP Server

IP	Description
192.168.30.11	Internal Web/DB Server
192.168.30.12	Mail Server
192.168.30.13	File/Print Server
192.168.30.14	Radius Server
192.168.30.15	Anti-Virus Server
192.168.30.16	Syslog Server
192.168.30.17	Management Server
192.168.30.18	SNORT IDS Server
192.168.30.48-55	Network Printers
192.168.30.64-254	DHCP Pool for internal users

All internal networks will use (RFC 1918) non-routable IP addresses. The firewall will be configured to perform network address translation ("NAT"). The external interfaces of the firewall will be used for hidden NAT to the internal protected network. This will provide additional security through use of NAT.

Border Router

The border router is a Cisco 3660 running IOS 12.2. This router is very flexible and will accommodate expansion in the future if needed. The router will utilize the built-in Ethernet 10/100 ports for the internal and access networks and a T1 interface on the external side for WAN connectivity to our ISP. This router will allow for further expansion if the need for more broadband is required. Administrative access to the router will be restricted to SSH.

Firewall/VPN

The firewall design will use a traditional three-legged approach; i.e., external leg, DMZ or Public leg, and internal leg. Considering the importance of the eCommerce site, it was determined to purchase a HA firewall solution.

The firewall configuration selected was the Compaq SolutionPaq Ver 2.0. The two node HA firewall will run on Compaq ProLiant 320 rack mount servers with 2 GB of RAM memory, 36 GB SCSI hard drive, and a quad Ethernet card to provide a total of six 10/100 ethernet ports.

The Compaq SolutionPaq Ver 2.0 [1] is a pre-configured hardened version of RedHat Linux running kernel 2.2.19-7.0.12. This "Secured by Check Point" appliance has pre-installed, pre-configured, tested, and OPSEC certified software to ensure 'out-of-the-box' deployment as a single, fully integrated product. Checkpoint Firewall-1/VPN-1 version 4.1 SP6 with the Aggressive IKE Hotfix and OpenSSL Hotfix is installed. Even though end of life for Check Point 4.1 is eminent, it was decided to install version 4.1

and then upgrade to NG at an appropriate time in the future. This will provide eFortCS sys admins time to get up-to-speed on NG. Rainfinity Rainwall version 1.6 Build 31 will provide the HA solution. A hot-standby HA solution will be implemented. This will allow the flexibility of performing maintenance on individual nodes with no downtime. A guideline detailing how to install and configure this solution is included as Appendix A. Eth3 interface on both nodes will be used as a heartbeat connected via a cross-over cable.

Content Vector Protocol ("CVP") will be utilized to provide anti-virus and content filtering at the firewall for incoming email. Radius authentication using one-time passwords will be utilized.

The Check Point provided SecuRemote clients will be used for VPN support for remote sales and telecommuting workers. SecuRemote is very flexible to use and clients are available for Windows, Macintosh, and Linux (beta) users. To provide VPN support, SecuRemote clients will be utilized. A detailed configuration of the VPN is included as part of the tutorial.

When the need arises to establish a VPN tunnel to a partner or supplier site, Check Point can be used to establish this tunnel to other IPSEC compliant firewalls or VPN based routers.

IDS

There will be three strategic locations where SNORT IDS systems will be placed. Each SNORT box will have two 10/100 Ethernet ports installed with one port in stealth mode listening to the wire with no IP address assigned. The three locations are depicted on the network diagram. The first SNORT IDS will be listening to the spanning port of the switch associated with the access network. This will monitor all traffic that has passed through the modem pool. The second box will be connected to the spanning port on the switch supporting the DMZ. This will be able to watch for any malicious packets that pass through the firewall destined for the public net. The third box will be monitoring all traffic destined to the internal protected network. This will provide a robust ID umbrella monitoring malicious packets in front of and behind the firewall. Access to the servers themselves will be over SSH. Tcpwrappers will restrict access to these boxes only from the management server.

SNORT will run on Dell Poweredge 2500 servers on RedHat Linux 8.0, SNORT 1.9, mySQL 3.23.56 and ACID 0.9.6b23.

Virus/Content Filtering Protection

Considering all the recent news of viruses and trojans, it is imperative that eFortCS users are protected at the firewall for viruses and malicious attachments. In this regard, the firewall will be configured to use the smtp security server with CVP over to a Dell Poweredge 2500 server running on Windows 2000 SP3 with TrendMicro InterScan VirusWall 3.52 anti-virus and content filtering support [2]. TrendMicro will be configured to go out hourly to check for new virus definitions. Vendors have become very responsive to virus outbreaks and sometimes have new signatures available within

hours. This will insure that we have the most up-to-date signatures. Content filtering will be enabled and the industry recommended attachments will be stripped off. Microsoft provides a recommended list of file extensions [3], as follows:

Extension	File type
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.asx	Windows Media Audio / Video
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.isp	Internet Communication settings
.js	JScript file
.jse	Jscript Encoded Script file
.lnk	Shortcut
.mda	Microsoft Access add-in program
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.mdt	Microsoft Access workgroup information
.mdw	Microsoft Access workgroup information
.mdz	Microsoft Access wizard program
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	MS Win Installer transform; MS Visual Test src file
.ops	Office XP settings
.pcd	Photo CD image; Microsoft Visual compiled script
.pif	Shortcut to MS-DOS program
.prf	Microsoft Outlook profile settings
.reg	Registration entries
.scf	Windows Explorer command
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap object
.shs	Shell Scrap object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript Encoded script file
.vbs	VBScript file

Extension	File type
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

To add security in depth, a site license of Norton Anti-Virus corporate edition will be purchased and installed on all systems to include remote users. Norton will be configured to automatically go out daily to check for new virus definitions as well as a weekly in-depth scan of all hard drives. Users will also be instructed to use sound security techniques of scanning all removable media for viruses before attempting to access any files.

Web/DB Servers

eFortCS Web and DB Server is running on a hardened RedHat Linux 8.0 Dell Poweredge 2500 server. The latest version of Apache (Version 2.0.44) will be installed and integrated with MySQL Server (Version 3.23.56). The web server will be running on a separate server from the MySQL server. Access to the PHP based web portal will be controlled with strict user access controls. A host-based firewall will be installed on the database server and configured to allow access only from the web server. This will provide a separation between the web server and the important data contained on the DB server. Policy mandates that all security patches be applied immediately upon any known vulnerability. All clients will be required to have 128-bit SSL Encryption enabled in their web browser.

Tripwire will be used to monitor the integrity of the core operating system and application binaries.

An internal server will provide eFortCS employees with the needed web and database capability.

Remote Access Server (RAS)

A Cisco AS5400 with IOS version 12.2.2 will be deployed for remote access. Authentication will be required using a dedicated Safeword RADIUS server and hardware authenticators that generate one-time passwords. These will be located on a separate access network. This will provide a separation from the DMZ to reduce the risk to these resources. In order for the modem pool users to access the internal network, SecuRemote will be required. This will ensure a more complete security model for remote users.

Radius Server

The internal radius server running on a Dell Poweredge 2500 server will use Safeword Authentication server with Platinum hardware authentication cards employing a one-time password scheme. This will be used for SecuRemote and firewall authentication. The Radius server running on the access network will be used exclusively for authenticating modem pool users. This server will be running a host-based firewall and strict controls to only allow access from the RAS server.

SMTP Mail Relay

The smtp mail server will act as a gateway for all e-mail. The server will be running Sendmail (latest version) with strict spam filtering enabled. This server will run on a Dell Poweredge 2500 server with a hardened RedHat Linux 8.0 OS. OpenSSH 3.5p1 will be enabled to allow for administration of the box. TCPWrappers will be set to only allow connectivity from inside eFortCS computers.

DNS

eFortCS will deploy a split DNS with an external and internal server. The external DNS will only provide information on servers that are available on the public network (DMZ). The internal DNS server will also provide DHCP services for the internal network workstations. The Internet Software Consortium versions of Bind (9.2.1) and DHCP (3.0p2) will be installed and configured based on sound security practices. Again, Dell Poweredge 2500 servers will be deployed running RedHat hardened Linux 8.0 OS. OpenSSH 3.5p1 will be used for administration of the box.

Log Servers

The eFortCS log servers will be running on Dell Poweredge 2500 servers running RedHat Linux 8.0. The log server located on the DMZ will be configured to centrally capture all log events from the border router, and access and DMZ switches. An internal log server will support internal switches and other syslog generating devices. SWATCH will be configured to provide alerting capabilities [4].

File/Print Server

The file and print server the eFortCS will deploy will be run on a Dell Poweredge 2500 server running a hardened RedHat 8.0 Linux OS. Samba services will be enabled to provide full Windows compliant file/print services. OpenSSH3.5p1 will also be allowed on this server to provide file transfer capabilities using scp.

Management Server

A management server running Windows 2000 SP3 will be run on a Dell workstation that will be used mainly to remotely manage the firewall cluster HA software (Rainwall.) This station can also be used to manage other areas of the internal network servers to include DNS/DHCP, email server, tripwire, etc. A Win32 version of OpenSSH 3.5p1 will be installed in support of this management concept.

Part Two: Security Policy and Tutorial

The border router will be running Cisco IOS 12.2. Information gained from attending the SANS Firewalls, Perimeter Protection and VPNs class, SANS Inside Network Perimeter Security book [5] as well as the 'Router Security Configuration Guide' by NSA [6] will be utilized in developing policy for the protection of our border defense.

Logging will be important to this defense so all logging will be allowed to our Syslog server at IP address 209.245.30.73.

All access lists will be maintained on the internal management station located at 192.168.30.17. The router will be securely managed via SSH tunnel from internal management workstation, 192.168.30.17.

! This will setup the basic global configuration of the router and restrict services that are not needed

```
service password-encryption
service linenumber

hostname eFortCS
enable secret 5 %1223@Co&7942@Ut
enable password 7 lnS*x1aw&bJ1am

no service tcp-small-servers
no service udp-small-servers
no service finger
no snmp-server
no cdp enable
no ip http server
no ip bootp server
no boot network

! Disable source routing/ip-spoofing, broadcast amplifiyers

no ip source-route
no ip directed-broadcasts

! Limit ability of hacker to gain info

no ip proxy-arp
no ip unreachable
no ip redirect
no ip mask-reply
```

```
! Lets log!

logging on
logging console informational
logging server 209.245.30.73
logging facility local6

! Banner Info

Unauthorized access or use of this site, eFortCS.com, may subject violators to criminal
or civil action.  All information on this site may be intercepted, recorded, read, copied,
and disclosed by and to authorized personnel for official purposes, including criminal
investigation.  Access or use to eFortCS computers by any person whether authorized
or unauthorized, constitutes consent to these terms.

! Require vty to use SSH

line vty 0 4
login local
ip ssh time-out 90
ip ssh authentication-retries 2
transport input ssh

!Set up the router interfaces including IP address, services, and access lists

interface FastEthernet 0/0
description inside network connection
ip address 209.245.30.251 255.255.255.248
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet 0/1
description access network connection
ip address 209.245.30.252 255.255.255.248
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no ip mroute-cache
duplex auto
speed auto
```

```
! Will apply access lists to external serial interface of border router
interface serial0/0
description connection to ISP
ip address 209.245.30.253 255.255.255.248
ip access-group 101 in
ip access-group 102 out
no ip directed-broadcast
no ip redirects
no ip unreachables
no ip proxy-arp
no ip mroute-cache
no cdp enable

! Define routes
```
Default route to next hop of upstream ISP.
```
ip route 0.0.0.0 0.0.0.0 209.245.30.254
```

With the access network and internal network connected on physical interfaces, routing will be handled direct, however, the routes are added for clarity.
```
ip route 209.245.30.128 255.255.255.192 209.245.30.252
ip route 209.245.30.0 255.255.255.248 209.245.30.251
```

Inbound ACL

```
! Ingress filtering
! Deny any packets without an IP address

access-list 101 deny IP host 0.0.0.0 any log

! Deny packets that are sourced with eFortCS IP address in order to prevent spoofing

access-list 101 deny ip 209.245.30.0 0.0.0.255

! Deny Loopback
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log

! Deny Private addresses
```
Private addresses are non-routable.
```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
```

! Deny multicast, broadcast

access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log

! Deny reserved Class E addresses
access-list 101 deny ip 240.0.0.0 0.255.255.255 any log

! Unused IANA addresses.
This will prevent someone from spoofing an unused IANA address. This helps us be a good net neighbor. Will consolidate using supernetting to increase router performance.

access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 49.0.0.0 0.255.255.255 any log
access-list 101 deny ip 50.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 1.255.255.255 any log
access-list 101 deny ip 60.0.0.0 0.255.255.255 any log
access-list 101 deny ip 70.0.0.0 1.255.255.255 any log
access-list 101 deny ip 72.0.0.0 7.255.255.255 any log
access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
access-list 101 deny ip 84.0.0.0 3.255.255.255 any log
access-list 101 deny ip 88.0.0.0 7.255.255.255 any log
access-list 101 deny ip 96.0.0.0 31.255.255.255 any log

! Block untrusted services
It is critical to block Microsoft networking ports 135-139 and ports 445. There have been too many worms that have exploited these ports. There is no reason to allow Windows networking in from the Internet.

access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any range 135 139 log
access-list 101 deny tcp any any eq 445 log
access-list 101 deny udp any any eq 445 log

!
Again, block access to SunRPC ports 111. Many exploits are found to run against RPC services.

```
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 111 log

! Block inbound syslog
access-list 101 deny udp any any eq syslog log

! Block inbound SNMP
access-list 101 deny tcp any any eq 161 log
access-list 101 deny udp any any eq 161 log
access-list 101 deny tcp any any eq 162 log
access-list 101 deny udp any any eq 162 log

! Block inbound tftp
access-list 101 deny udp any an eq 69 log

! Permit everything else and log

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

Outbound ACL

```
! Only allow eFortCS routable IP addresses outbound – restricting everything else.

access-list 102 permit 209.245.30.0 0.0.0.255 any
access-list 102 deny ip any any log
```

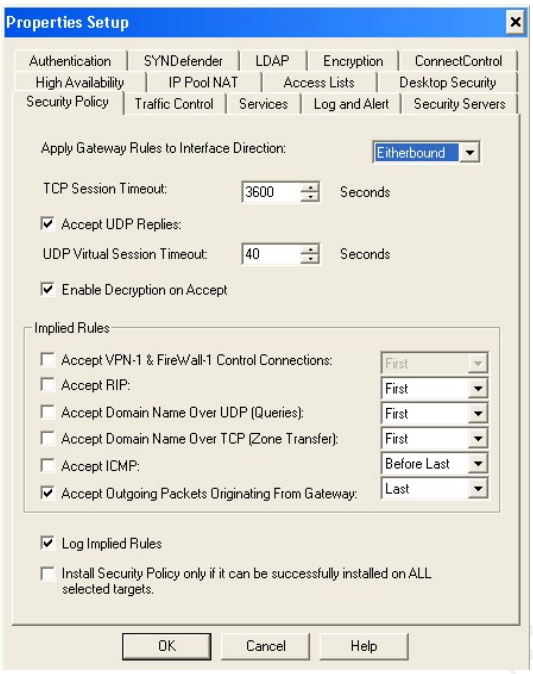
Firewall Policy

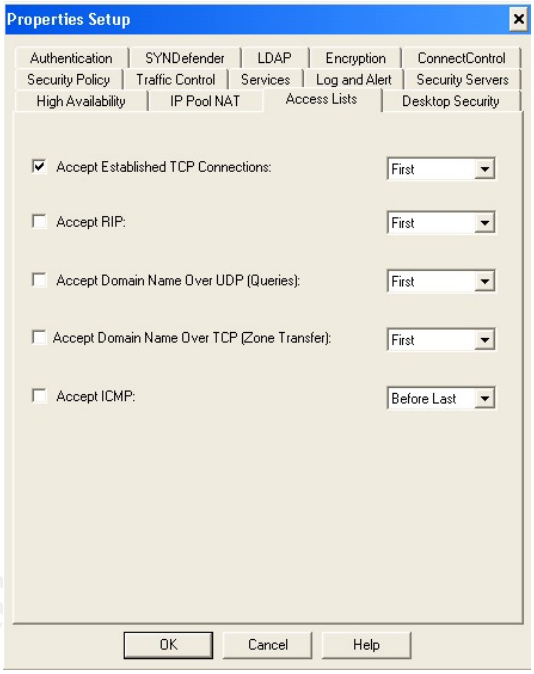
The firewall will be a clustered HA hot-standby solution running on the Compaq SolutionPaq Ver 2.0. This "Secured by Check Point" appliance has pre-installed, pre-configured, tested, and OPSEC certified software. Checkpoint Firewall-1/VPN-1 version 4.1 SP6 with the Aggressive IKE Hotfix and OpenSSL Hotfix is installed and integrated with Rainfinity Rainwall version 1.6 Build 31 which provides the HA capability. This solution will provide excellent management capability by allowing sys admins to perform maintenance on one node without bringing down the firewall.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	RainwallCluster	RainwallCluster	Rainwall_Stop	drop	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall rule to determine that firewall is operating properly.
2	RainwallCluster	RainwallCluster	Rainwall_Daemon	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rule permitting communication between the Rainwall cluster machines.
3	RainwallCluster mgmt_server	RainwallCluster	Rainwall_Status	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall status rule to permit communication between remote Management Console.
4	mgmt_server	RainwallCluster	Rainwall_Command	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows Rainwall Management GUI access to RainwallCluster.
5	Any	web_server	http https	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Public access to eFortCS Web/DB server
6	eFortCS_modem_pool NET-192.168.30.0	Any	http https ftp echo-request traceroute	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow internal and modem pool users access to authorized services
7	NET-192.168.30.0	external_dns_server	domain-tcp domain-udp	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows queries to external DNS server
8	NET-192.168.30.0	external_smtp_server	smtp	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows incoming SMTP traffic to external SMTP server
9	mgmt_server	eFortCS_Firewall_Cluster external_dns_server external_smtp_server web_server db_server	TCP-1169	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allow management server to monitor tripwire clients
10	sysadmin_workstations	eFortCS_Firewall_Cluster external_dns_server external_smtp_server web_server eFortCS_router db_server snort_servers	SSH	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allow sysadmins access to external servers via SSH
11	eFortCS_Firewall_Cluster	radius_server	RADIUS	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow access to Radius authentication server.
12	Any	eFortCS_Firewall_Cluster	ESP FW1_keys	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Needed for SecuRemote access.
13	SecuRemote@Any	Any	Any	Client Encrypt	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow remote and modem pool eFortCS employees access to intenal resources via SecuRemote
14	eFortCS_Firewall_Cluster	anti-virus_server	FW1_cvp	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow firewall cluster to talk to anti-virus scanner
15	Any	eFortCS_Firewall_Cluster	Any	drop	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Firewall stealth rule
16	external_smtp_server	internal_smtp_server	smtp->SMTP_scan	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Virus/content filtering on all incoming email traffic
17	eFortCS_router external_switch dmz_switch	dmz_syslog_server	syslog	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allow routers/switches access to syslog server
18	Any	NET-209.245.30.0	dest-unreach echo-reply time-exceeded	accept	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Allow replies back to pings/traceroutes.
19	Any	Any	icmp-proto	drop	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Deny all inbound icmp except those allowed above.
20	Any	Any	Any	drop	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Explicit drop rule for logging

Implied Rules

Looking at the property configuration of the firewall policy, all implied rules were disabled. Any access required will be provided by a specific rule as outlined in the breakdown by rules.



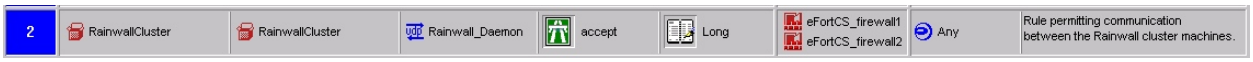


Finally, doing a view of the implied rules shows only the following:

This is exactly what we expected. The only implied rule allows outbound established TCP connections as held in the state table.

Breakdown by Rule

The first four rules deals with Rainwall configuration. The first rule blocks a specific packet type (Rainwall_stop (udp/6332)) used by Rainwall to determine that the firewall is operating properly. Short logging will be used initially. One might want to not log this rule once the firewall is up and operating since it will generate a lot of logs.



Rule two permits communication between the Rainwall cluster nodes. This provides the heartbeat between the two nodes to occur.

3	RainwallCluster mgmt_server	RainwallCluster	Rainwall_Status	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall status rule to permit communication between remote Management Console.

Rule three permits status communication to and from the remote management console (GUI) or from rwstat (a shell command used to collect data on Rainwall status).

4	mgmt_server	RainwallCluster	Rainwall_Command	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows Rainwall Management GUI access to RainwallCluster.

Rule four allows the management server to monitor and control the Rainwall daemon through a management interface. This interface provides firewall, Virtual IP address assignment, interface load status. Through this interface, one can also stop a node, switch to the other node and other administrative functions. This rule only allows access from the management server and no other system.

5	Any	web_server	http https	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Public access to eFortCS Web/DB server

Rule five is a very active process since it allows all traffic to the web/DB server. Since the most important function is the web portal, priority is given to this rule to allow the quickest processing through the rule base. Since we want to see all interaction with the web portal, account logging is enabled. Account logging allows for packet counts and number of bytes transferred in additional to the normal logging associated with Firewall-1/VPN-1.

6	eFortCS_modem_pool NET-192.168.30.0	Any	http https ftp echo-request traceroute	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow internal and modem pool users access to authorized services

Rule six allows eFortCS employees access outbound based on the policy defined. This rule covers not only internal users but users coming in through the modem pool. Again, account logging will be used to insure that full information is gathered. The above services should provide employees with the Internet access required to perform their jobs.

7	NET-192.168.30.0	external_dns_server	domain-tcp domain-udp	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows queries to external DNS server

Rule seven allows for access to the external DNS server from the Internet in general. Again, we anticipate there will be many requests to the DNS server in accessing eFortCS web portal information. Long logging will be implemented to insure auditing capabilities. A negate source on the protected network will prevent internal employees from using the external DNS server.

8	NET-192.168.30.0	external_smtp_server	smtp	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows incoming SMTP traffic to external SMTP server

Rule eight allows SMTP traffic to flow to the external smtp server. All inbound email will come to the external relay smtp server. This server will be configured to insure no SPAM email is allowed to be sent from eFortCS servers. Long logging will be implemented to provide auditing capabilities. A negate source on the protected network will prevent internal employees from using the external SMTP server

9	mgmt_server	eFortCS_Firewall_Cluster external_dns_server external_smtp_server web_server db_server	TCP-1169	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allow management server to monitor tripwire clients

Rule nine allows the internal tripwire management console access to each of the external servers. The tripwire console will be setup to monitor critical file system binary files and other files deemed critical. Hourly integrity checks will be setup to check binary and library files. In addition, a full integrity check will run four times a day. Sys admins will be responsible to insure tripwire database files are kept updated if they make any changes to the files being monitored by tripwire. A four-hour window will be established during the day for these changes. Long logging will be implemented to verify access from the tripwire management console.

10	sysadmin_workstations	eFortCS_Firewall_Cluster external_dns_server external_smtp_server web_server eFortCS_router db_server snort_servers	SSH	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allow sysadmins access to external servers via SSH

Rule ten allows access to all external servers via SSH protocol. Any administrative work on the external servers will only be performed through an encrypted SSH tunnel. Long logging will be implemented.

11	eFortCS_Firewall_Cluster	radius_server	RADIUS	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow access to Radius authentication server.

Rule 11 allows the SecuRemote users configured on the firewall cluster to authenticate with the internal radius server. Safeword one-time authentication will be used with hardware authenticator cards. Authenticator cards will be issued to all remote access employees to insure an additional layer of security when using SecuRemote.

12	Any	eFortCS_Firewall_Cluster	ESP FW1_keys	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Needed for SecuRemote access.

Rule 12 allows the required protocols needed for use by SecuRemote. This rule is necessary because we elected to turn off the default settings. It is expected to be used extensively so account logging is turned on.

13	SecuRemote@Any	Any	Any	Client Encrypt	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow remote and modem pool eFortCS employees access to intenal resources via SecuRemote

Rule 13 enables remote users access to internal resources through the use of SecuRemote VPN software. This provides client encryption for any remote employees or employees using the modem pool. Account logging will be utilized.

14	eFortCS_Firewall_Cluster	anti-virus_server	FW1_cvp	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow firewall cluster to talk to anti-virus scanner

Rule 14 allows the firewall cluster to communicate with the anti-virus server running TrendMicro InterScan VirusWall CVP version. All inbound email will run through the content manager and then checked for viruses. Account logging will be used.

15	Any	eFortCS_Firewall_Cluster	Any	drop	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Firewall stealth rule

Rule 15 is the firewall cluster stealth rule. Only permitted access to the firewall cluster is allowed in above rules. All other interaction with the firewall will be dropped and logged. This insures the integrity of the firewall. Long logging will be employed.

16	external_smtp_server	internal_smtp_server	smtp->SMTP_scan	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Virus/content filtering on all incoming email traffic

Rule 16 allows access from the external smtp server to communicate with the internal smtp server. Of course, all email will be sent through the anti-virus scanner before being delivered.

17	eFortCS_router external_switch dmz_switch	dmz_syslog_server	syslog	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allow routers/switches access to syslog server

Rule 17 allows syslog information to be passed to the DMZ syslog server from the border router and external switches. Long logging will be enabled.

18	Any	NET-209.245.30.0	dest-unreach echo-reply time-exceeded	accept	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Allow replies back to pings/traceroutes.

Rule 18 allows responses back in from pings and traceroutes. This rule is needed because we shut off the default icmp policy. By allowing destination unreachables (icmp type 3), we don't break MTU discovery. Logging is set to short.

19	Any	Any	icmp-proto	drop	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Deny all inbound icmp except those allowed above.

Rule 19 blocks all icmp that is not allowed in rule 19 above. Because the default icmp policy is not used, this rule is necessary. Logging is short.

20	Any	Any	Any	drop	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Explicit drop rule for logging

Rule 20 blocks everything not allowed by prior rules and logs it. Even though the rule is on be default, the need to log all dropped packets is very important. Account logging is used.

The rules are applied top down and thus the most used rules are set at the top. After having the site up and running for a period of time, the rules maybe reordered to ensure better firewall performance.

VPN Policy

As mentioned before, SecuRemote will be used to provide all VPN connectivity to eFortCS.com. This software will establish a VPN tunnel from the client desktop anywhere on the Internet to the firewall. The eFortCS employees will be required to have an account on the Radius server, a Safeword authenticator hardware card, and a PIN number to authenticate with the firewall. SecuRemote uses IPSEC with 3-DES

encryption and supports the SHA-1 algorithm. Client Mode will be setup to 'Transparent'. Split tunneling will be disabled.

Rules 12 and 13 helps define the VPN policy on the firewall.

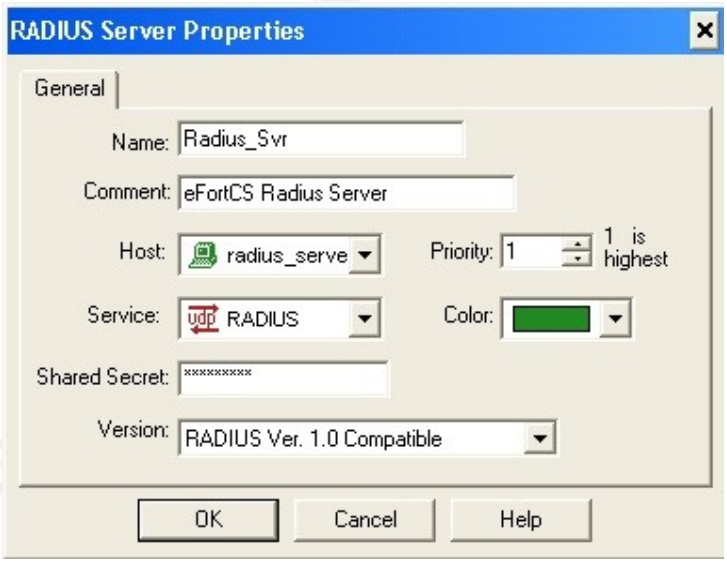
12	Any	eFortCS_Firewall_Cluster	ESP FW1_keys	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Needed for SecuRemote access.
13	SecuRemote@Any	Any	Any	Client Encrypt	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow remote and modem pool eFortCS employees access to intenal resources via SecuRemote

All remote eFortCS employees coming in from broadband connections from the Internet or through the modem pool will be required to use SecuRemote to provide for client encryption to internal resources. The details of the setup and configuration of SecuRemote VPN will be detailed in the tutorial that follows next.

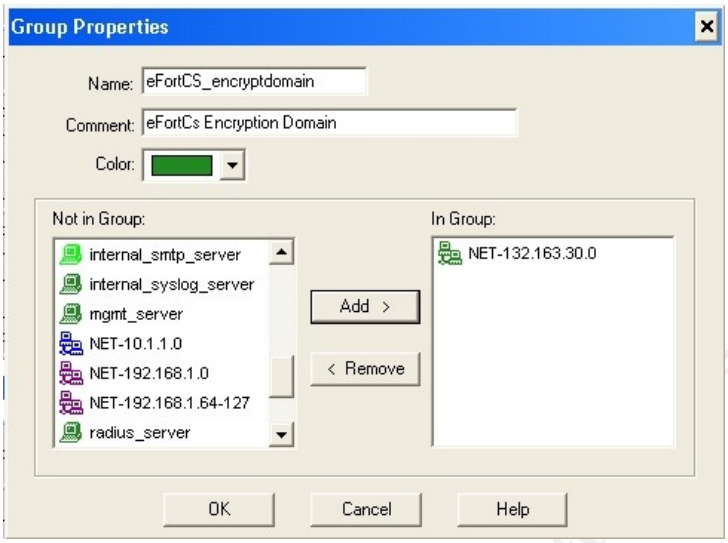
Checkpoint SecuRemote VPN Configuration Tutorial

This tutorial will detail how SecuRemote VPN is configured for use by eFortCS remote employees. It will cover the setup on the firewall and user definitions as well as the setup and configuration of SecuRemote on the client.

Since we are using SafeWord for radius authentication, we need to configure the Radius Server properties. Do this by selecting Manage=>Servers=>New=> Radius and configure it as below:

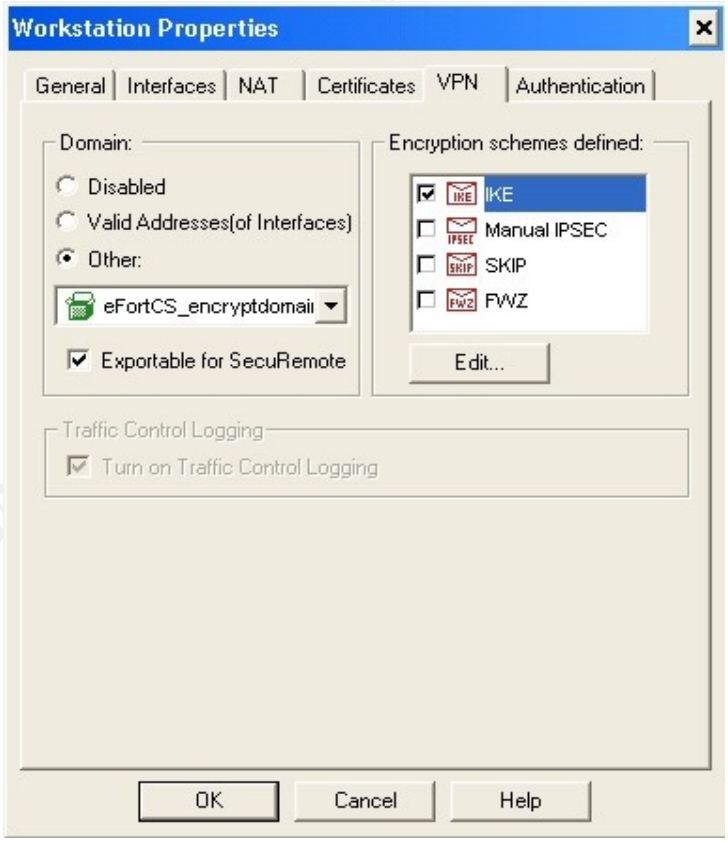


The 'Shared Secret' password will be used in configuring the Safeword Radius software. We next need to establish the encryption domain for use by SecuRemote. Select Manage=>Network Objects => New => Group and select the internal subnet.

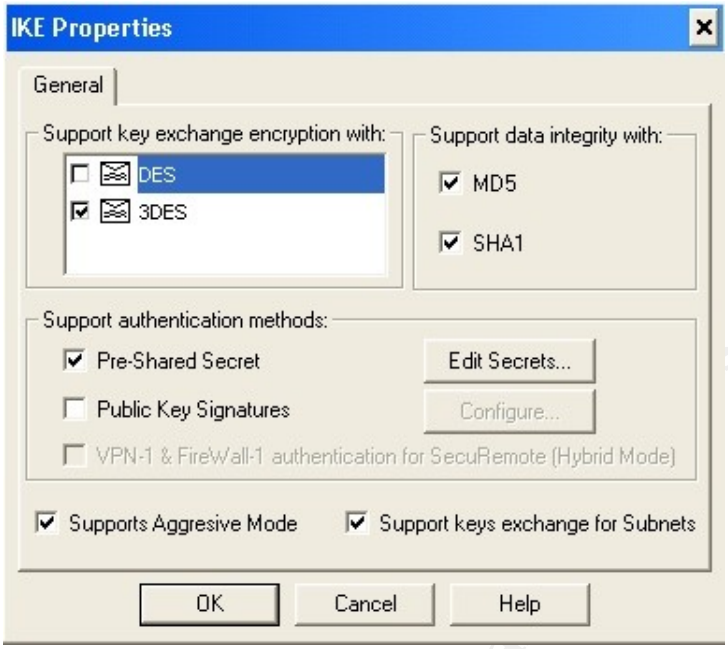


This encryption domain will represent the resources that will be accessible to the SecuRemote users. In our case, it will be the internal network.

We next need to update the firewall objects to reflect the encryption type and domain. Select Manage => Network Objects and select the eFortCS_firewall1. Add the encryption domain defined earlier as shown below:



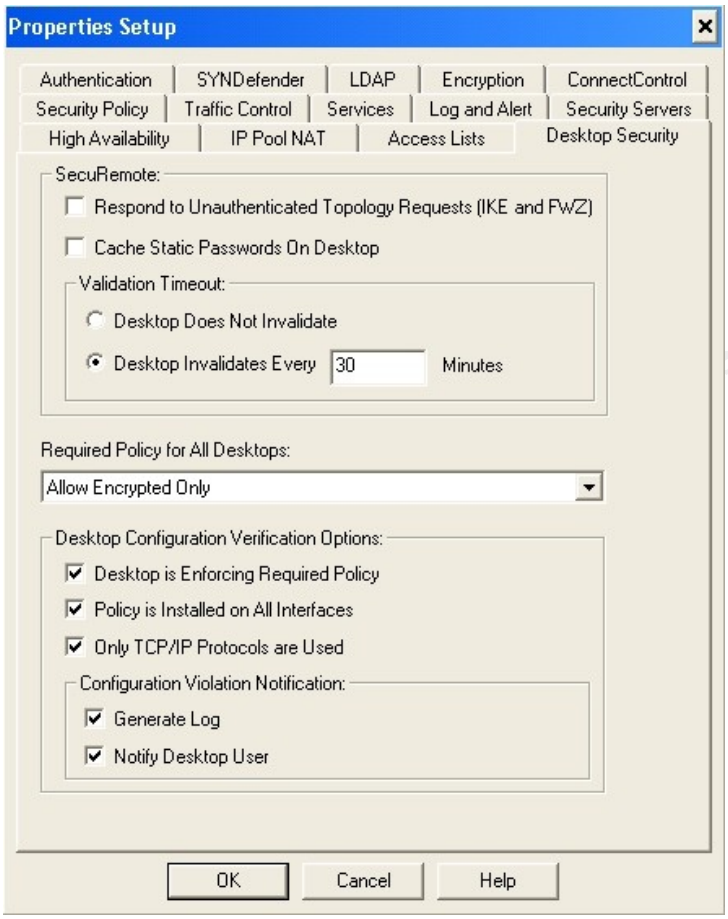
We chose IKE for the encryption scheme. We also made the encryption domain exportable for SecuRemote. Next, we need to define the IKE encryption scheme.



We got to the IKE Properties dialogue box by clicking edit. We will use 3DES for the key exchange encryption. Select Pre-Shared Secret for authentication method and will support data integrity with MD5 and SHA1. We will also select 'Supports Aggressive Mode' and 'Support keys exchange for Subnets'.

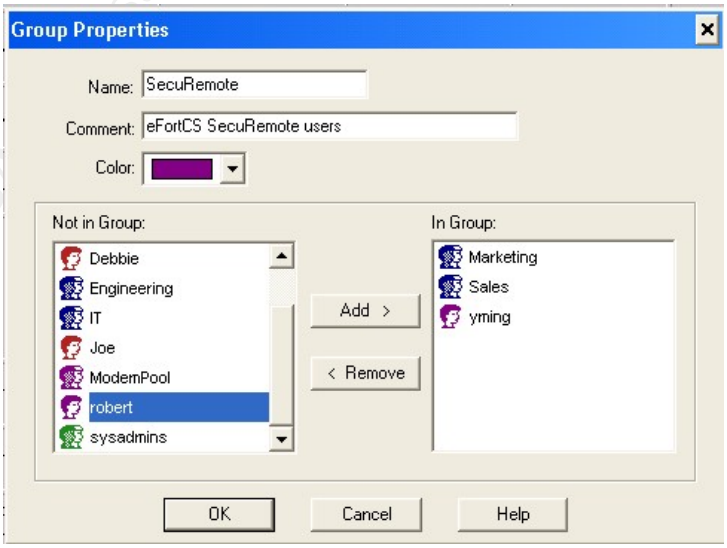
Do the same thing for eFortCS_firewall2 node. Since the configuration is the same, the screen shots will be spared.

Next, we want to ensure that authentication will be required to respond to topology requests. This is configured under the policy property dialogue box. Select Policy => Properties. Select the Desktop Security tab. The configuration for this is shown below:

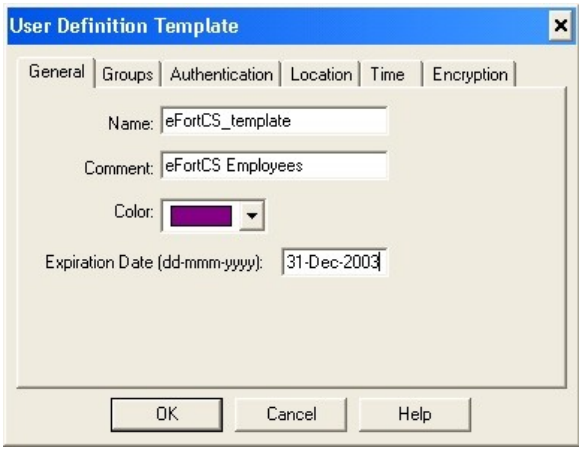


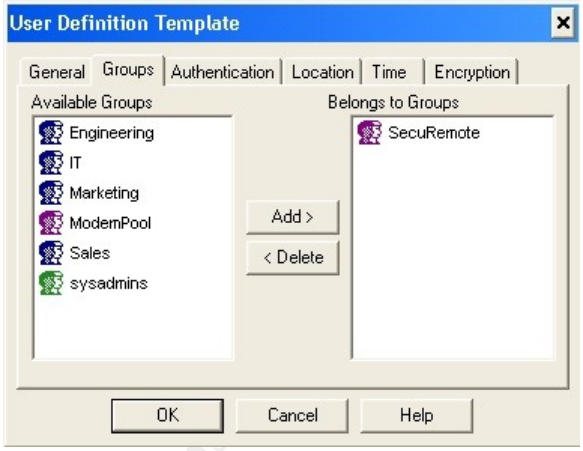
Deselect 'Respond to Unauthenticated Topology Requests (IKE and FWZ)'. Also, a validation timeout of 30 minutes was selected. We will disable split tunnel by selecting 'Allow Encrypted Only'.

We now create a group object for our SecuRemote users. Select Manage => Users => New => Group.

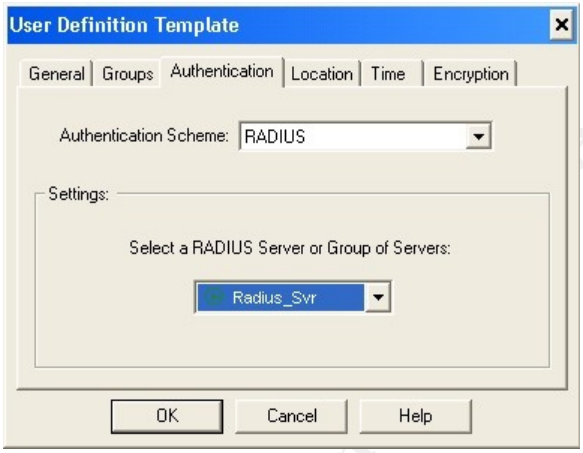


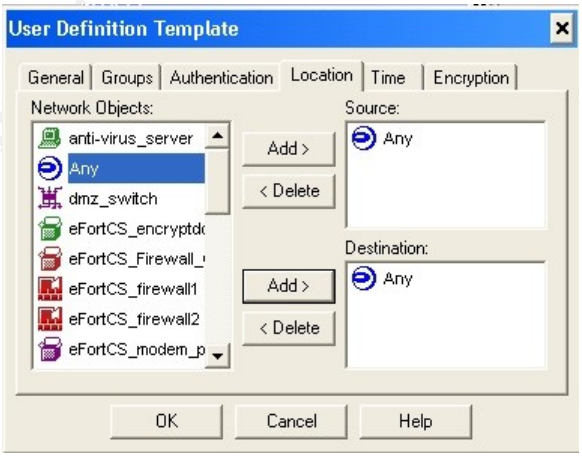
We now need to populate the SecuRemote group with a eFortCS users that are required to use SecuRemote. Since there are many users, a template will be built to accommodate the addition of users. Select Manage => Users => New => Template.



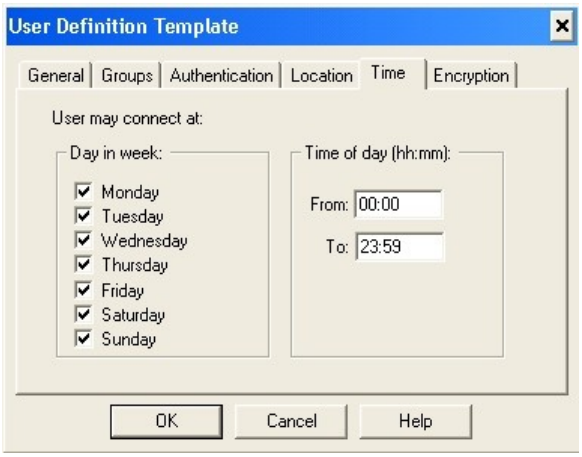


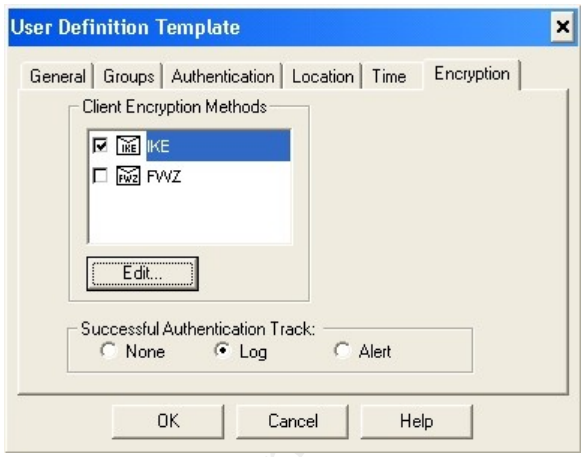
In the General Tab, an expiration date is defined as well as the name of the template. Under the Groups Tab, SecuRemote group is selected.



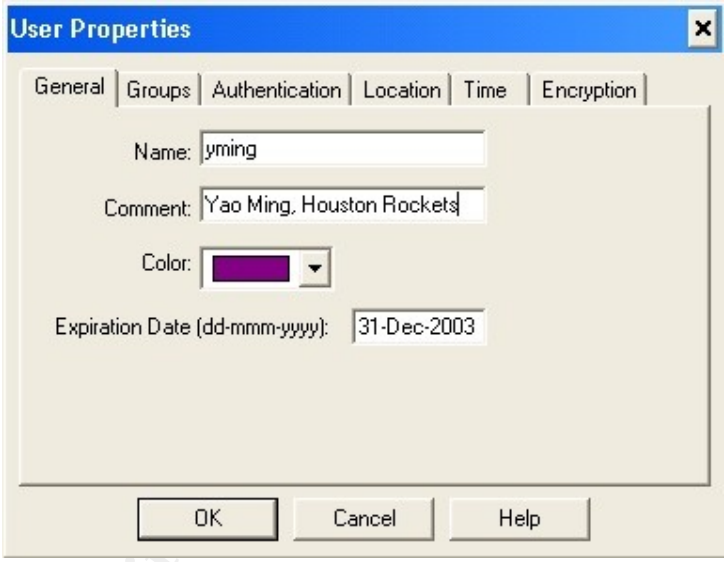


Under the Authentication Tab, Radius authentication scheme is selected with the appropriate Radius_Srv selected. No source or destination restrictions are placed on eFortCS users.





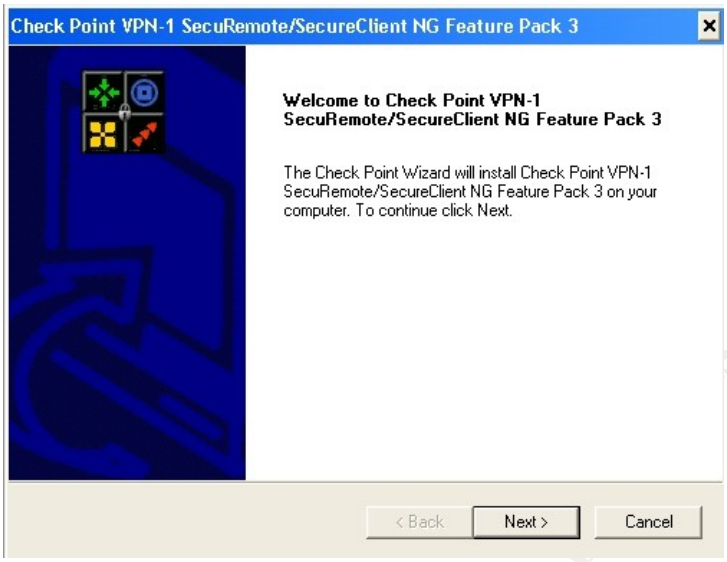
EfortCS users will have no time restraints placed on them. IKE encryption is selected.



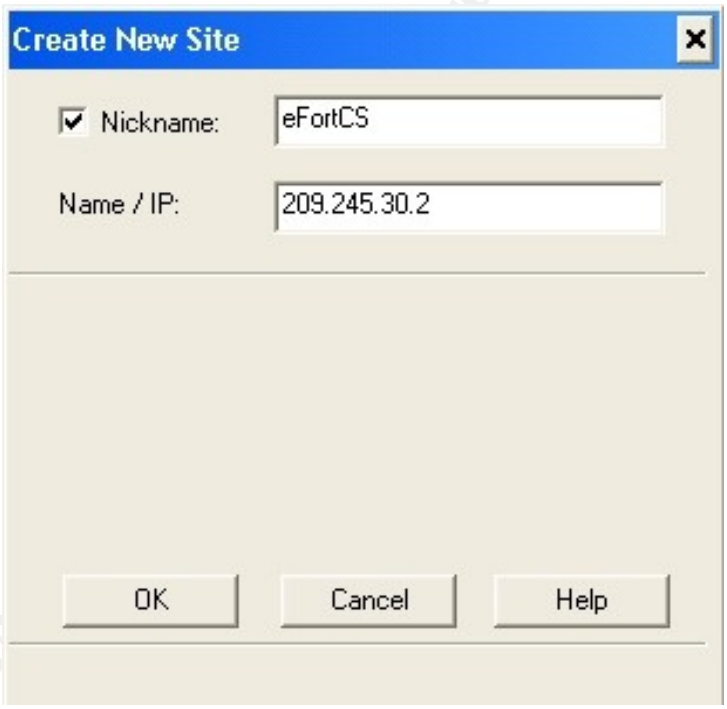
Yao Ming is given an account to access eFortCS resources!

The VPN rule is created as already detailed. Finally, we need to configure SecuRemote client.

Check Point VPN-1 SecuRemote/SecureClient NG Feature Pack 3 was installed.

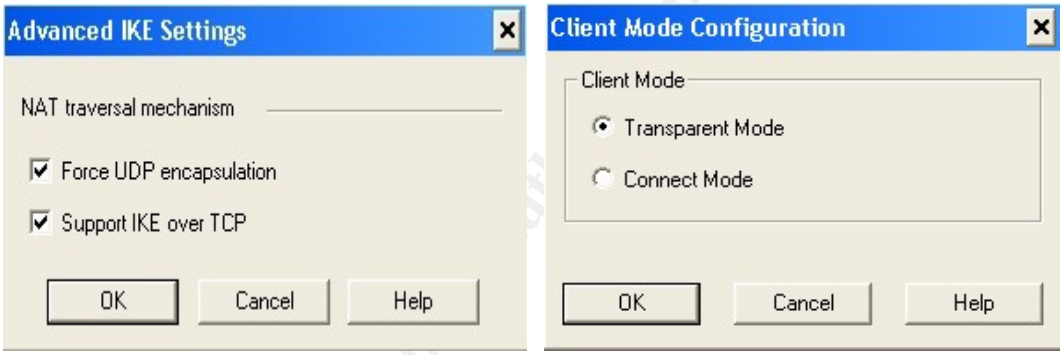


A Site was created by selecting Sites => Create New. The following site was created using the information below:



A Nickname of eFortCS was used with an IP address of 209.245.30.2. In order to create the site and download the topology, authentication was required as shown below:

The site was created successfully. The final step is to insure that IKE is configured properly. Verify that the default settings are as shown below by going to Tools => Advanced IKE Settings. Also, transparent mode is selected by default.



SecuRemote is memory resident on the client and is activated when one attempts to access resources within the encryption domain as defined in the firewall policy. The icon resides in the system tray as shown below:

Part Three: Verify the Firewall Policy

EfortCS is required to conduct an audit of its new firewall implementation and policy. It is critical to test the firewall policy to ensure that the policy is functioning properly. Since humans create and implement policy, mistakes can be made. This section will address three phases of verifying the firewall policy: 1) plan the audit, 2) conduct the audit, and 3) evaluate the audit.

Plan the audit

Now that the eFortCS web portal and network is up and functioning, an audit will be performed to test the firewall implementation and policy. An outside consulting firm will be contracted to perform the audit. The consulting firm, Packets'R'US, will use the testing methodology as outlined in the NIST DRAFT Guideline on Network Security Testing [7]. In particular:

- Specific IP addresses/ranges to be tested;
- Any restricted hosts (i.e., hosts, systems, subnets, not to be tested);
- A list of acceptable testing techniques and tools;
- Times when testing is to be conducted;
- Define a finite period for testing;
- IP address of the machines from which testing will be conducted so that administrators can differentiate the legitimate testing attacks from actual malicious attacks;
- Points of contact for both the testing team, the targeted systems and networks;
- Measures to prevent law enforcement being called with false alarms (created by the testing); and
- Handling of information collected by testing team.

Specific IP addresses/ranges

The following IP addresses/ranges will be part of the scope of this audit:

IP	*Description*
209.245.30.1	Virtual IP (VIP) address of external interfaces of firewall
209.245.30.2 209.245.30.3	Physical firewall cluster external interfaces
209.245.30.68	DMZ SNORT IDS Server
209.245.30.69	Public DNS Server
209.245.30.70	Public Web Server
209.245.30.71	DB Server

IP	Description
209.245.30.72	SMTP Relay Server
209.245.30.73	Syslog Server
209.245.30.129	Access Network SNORT IDS Server
209.245.30.251	Internal IP of Border Router
192.168.30.12	Mail Server (Internal)
192.168.30.14	Radius Server (Internal)
192.168.30.15	Anti-Virus Server
192.168.30.17	Management Server (Internal)

Restricted hosts

There are no hosts that are restricted from the audit. For the purpose of this audit, only selected internal hosts will be targeted. The internal hosts were selected because of the firewall policy allowing interaction between DMZ hosts and specific internal hosts.

Testing techniques and tools

Since the focus of this audit is to verify that the firewall policy is correctly enforced, a good scanning tool will be utilized. Probably the best tool available for this task is Nmap [8]. A description and usage (man page) of Nmap is included in Appendix B. Nmap will be the primary tool used in this audit.

Even though the audit is not intended to look for vulnerabilities, Nessus [9], an open source vulnerability scanner, will be used to audit the firewall.

To verify that the anti-virus scanner is working properly, the test file eicar [10] will be sent through the firewall.

Another important part of the audit will be to test the IDS capability. Results of the scans will be correlated with SNORT. This should help to confirm the scanning results as well as verify the IDS systems are placed strategically.

Testing Times

Packets'R'US will conduct the audit starting on a Saturday morning at 08:00 a.m. This will reduce the impact of the higher traffic seen during the work week. This will also allow eFortCS network/sys admins to be available in case the audit degregates the network. It will also provide them with an opportunity to verify the IDS. The auditors will correlate the scans against the IDS to provide further opportunity to improve the overall security of the network.

Testing Duration

The audit will be scheduled for six hours on the chosen Saturday between the hours of 08:00 a.m. - 2:00 p.m. This should provide the auditors plenty of time to conduct their testing. This will force the Packets'RUS to have a well thought out test plan.

IP address of the machines conducting test

Testing against the firewall itself will be coming from IP 209.245.30.5. A test workstation will be connected to the switch just inside the border router. Testing against the internal hosts will be conducted from both IP 209.245.30.5 as well as from a workstation positioned on the DMZ in place of existing servers. By placing the test workstation and configuring it as the same IP address as the existing server, a Nmap scan can be run to verify the firewall policy. Also, scans will be run from the management server at IP 192.168.30.17 to assist in verifying the firewall policy.

Points of contact

Packets'R'US point of contact will be Joe Sniffer Jones. His mobile number is (555) 248-3632.

eFortCS network team will be represented by Sam Slamdunk Smith. His mobile number is (555) 844-4827. All coordination with other Sys Admins will be handled by Sam.

Any risks associated with the audit will be handled by the above listed individuals. Sam will be working closely with the audit team and will have on hand key sys admins in case one of the key servers are knocked off-line due to any denial of service or other unforeseen events. Considering that the audit will be conducted on a Saturday morning, the risks should be minimal.

Measures to prevent false alarms being escalated to law enforcement agencies

Given that this will be a well-defined and pre-planned audit conducted at a specific date and time, there will be no need to involve any outside law enforcement agencies.

Handling of information collected by testing team

A formal agreement will be signed by both Packets'R'US and eFortCS management to include a Non-Disclosure statement. This will insure that any information gathered will be used only for the benefit of improving security. Any critical holes found in the implemented router/firewall policy by Packets'R'US team will be immediately shared with Sam Smith. His team will take whatever action is needed to insure that any vulnerability is taken care of. A formal report will be issued by Packets'R'US within 14 days of the audit. This report will include other findings of a not so critical nature, suggestions to improve security, and a proposal to provide an audit tool for future periodic testing.

Contract with Packets'R'US

Packets'R'US has submitted a proposal considering the requirements outlined above. They will employ a three-man team to conduct the audit. EfortCS has agreed to pay the going rate of $150/hr. Packets'R'US has estimated that the effort will take the following:

- Pre-audit planning – 5 Hrs
- Audit – 18 Hrs (3-man equivalents x 6 Hrs)
- Data analysis, formal report and recommendations – 25 Hrs

A contract for a cost of $7200 (36 Hrs x $150/hr) has been signed with Packets'R'US.

Audit and Analysis

Audit against Firewall

This is the most important part of the audit. Since the firewall is a hot-standby high available firewall, nmap scans were conducted against the VIP address as well as both physical interfaces.

We will first scan the VIP address. We would anticipate that there would be no ports open on the VIP address.

```
# nmap (V. 3.00) scan initiated Wed Feb 19 13:10:13 2003 as:
nmap -P0 -sS -O -p 1-65535 -oN firewall_vip.txt 209.245.30.1

Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
Interesting ports on eFort_firewall.eFortCS.com (209.245.30.1):

(The 65535 ports scanned but not shown below are in state: filtered)

Too many fingerprints match this host for me to give an accurate OS guess

# Nmap run completed at Wed Feb 19 15:25:26 2003 -- 1 IP address (1 host up) scanned in 8112 seconds
```

This produced exactly the results that we expected. A more interesting scan will be against the physical interfaces.

The next scan was against the physical external interfaces of the firewall nodes, as follows:

```
# nmap (V. 3.00) scan initiated Wed Feb 19 13:19:21 2003 as:
nmap -P0 -sS -O -p 1-65535 -oN firewall_phys.txt 209.245.30.2  209.245.30.3
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 209.245.30.2
(The 65533 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
264/tcp    open        bgmp
265/tcp    open        maybeFW1

Remote OS guesses: Linux 2.1.19 - 2.2.20, Linux 2.2.14
Uptime 55.269 days (since Thu Dec 26 07:53:25 2002)

Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 209.245.30.3:
(The 65533 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
264/tcp    open        bgmp
265/tcp    open        maybeFW1

Remote OS guesses: Linux 2.1.19 - 2.2.20, Linux 2.2.14
Uptime 14.318 days (since Wed Feb  5 07:45:10 2003)
```

Checkpoint uses port 264 for the exchange of public keys and port 265 for topology downloads in support of SecuRemote. This service is required to insure the proper functionality of our VPN connectivity. Authentication is required from the SecuRemote client before one can download the topology.

Port 25 is open on Check Point firewall as the SMTP security server. All inbound email from the external smtp server to the internal smtp server will pass through the firewall security server. The firewall accepts all smtp traffic in and passes it to the anti-virus scanner using content vector protocol (CVP). Once the message has been scanned and accepted or rejected based on content, etc., the firewall has another process that negotiates and sends the message on to the internal smtp server. This way, the external smtp server never actually opens up an connection directly with the internal smtp server.

As a second check against the firewall, Nessus was run. The results are below. Nessus was run against the VIP 209.245.30.1 as well as the two physical interface addresses 209.245.30.2 and 209.245.30.3.

Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which where alive and responding during test	3
Number of security holes found	0
Number of security warnings found	4

Host List

Host(s)	Possible Issue
209.245.30.3	Security warning(s) found
209.245.30.2	Security warning(s) found
209.245.30.1	Security warning(s) found

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
209.245.30.3	unknown (264/tcp)	Security warning(s) found
209.245.30.3	unknown (265/tcp)	No Information

Security Issues and Fixes: 209.245.30.3

Type	Port	Issue and Fix
Warning	unknown (264/tcp)	The remote host seems to be a Checkpoint FW-1 running SecuRemote. Letting attackers know that you are running FW-1 may enable them to focus their attack or will make them change their attack strategy. You should not let this information leak out. Furthermore, an attacker can perform a denial of service attack on the machine. Solution: Restrict access to this port from untrusted networks. Risk factor : Low For More Information: http://www.securiteam.com/securitynews/CheckPoint_FW1_SecureRemote_DoS.html

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
209.245.30.2	unknown (264/tcp)	Security warning(s) found
209.245.30.2	unknown (265/tcp)	No Information

Security Issues and Fixes: 209.245.30.2

Type	Port	Issue and Fix
Warning	unknown (264/tcp)	The remote host seems to be a Checkpoint FW-1 running SecureRemote. Letting attackers know that you are running FW-1 may enable them to focus their attack or will make them change their attack strategy. You should not let this information leak out. Furthermore, an attacker can perform a denial of service attack on the machine. Solution: Restrict access to this port from untrusted networks. Risk factor : Low For More Information: http://www.securiteam.com/securitynews/CheckPoint_FW1_SecureRemote_DoS.html

This file was generated by Nessus, the open-sourced security scanner.

Nessus validated our Nmap scan. In regards to the Denial of Service risk mentioned, Check Point was never able to confirm the DoS behavior and, therefore, deemed it nothing to worry about.

Finally, an ACK scan was run to test if the firewall is truly stateful. A nmap ACK scan was run against the web server on the DMZ as shown below:

```
C:\bin\nmap-3.00>nmap -P0 -sA -p 80-85 209.245.30.70

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.70:
Port       State       Service
80/tcp     filtered    http
81/tcp     filtered    hosts2-ns
82/tcp     filtered    xfer
83/tcp     filtered    mit-ml-dev
84/tcp     filtered    ctf
85/tcp     filtered    mit-ml-dev

Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Looking at the firewall produced the following log entries:

```
26Feb2003 13:19:31 drop   efortcs_firewall1 >eth0 proto tcp src 209.245.30.5 dst 209.245.30.70 service http s_port
63497 rule 0 reason: unknown established TCP packet
26Feb2003 13:19:31 drop   efortcs_firewall1 >eth0 proto tcp src 209.245.30.5 dst 209.245.30.70 service 81 s_port
63498 rule 0 reason: unknown established TCP packet
26Feb2003 13:19:31 drop   efortcs_firewall1 >eth0 proto tcp src 209.245.30.5 dst 209.245.30.70 service 82 s_port
63499 rule 0 reason: unknown established TCP packet
26Feb2003 13:19:31 drop   efortcs_firewall1 >eth0 proto tcp src 209.245.30.5 dst 209.245.30.70 service 83 s_port
63500 rule 0 reason: unknown established TCP packet
26Feb2003 13:19:32 drop   efortcs_firewall1 >eth0 proto tcp src 209.245.30.5 dst 209.245.30.70 service 84 s_port
63501 rule 0 reason: unknown established TCP packet
26Feb2003 13:19:32 drop   efortcs_firewall1 >eth0 proto tcp src 209.245.30.5 dst 209.245.30.70 service 85 s_port
63502 rule 0 reason: unknown established TCP packet
```

This demonstrates that the Check Point is a stateful firewall. ACK packets were sent through the firewall and dropped according to firewall protocol. When inspecting a non-SYN packet, Check Point checks its state table. Since no entry was present, it dropped the packet with the error "unknown established TCP packet."

Audit by Rule

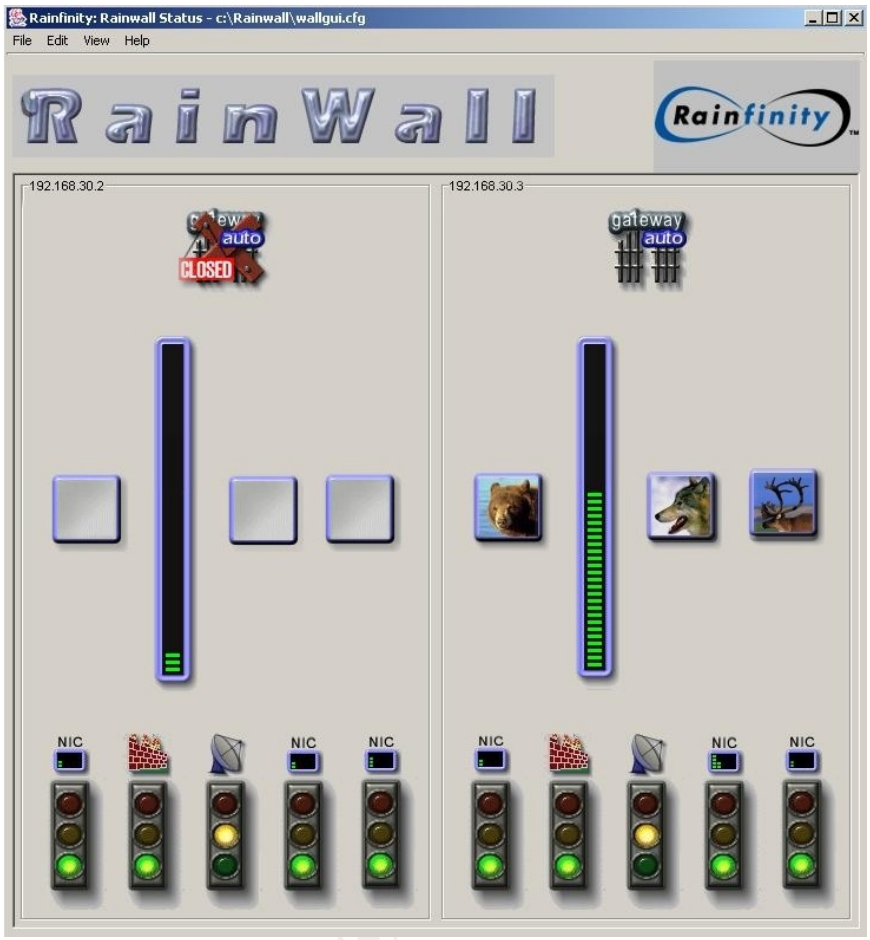
Rules 1 – 4

In order to truly audit and verify that the firewall policy is performing as advertised, each rule or groupings of rule will be tested. To start with, the first four rules deals with the Rainwall's hot-standby high availability cluster configuration.

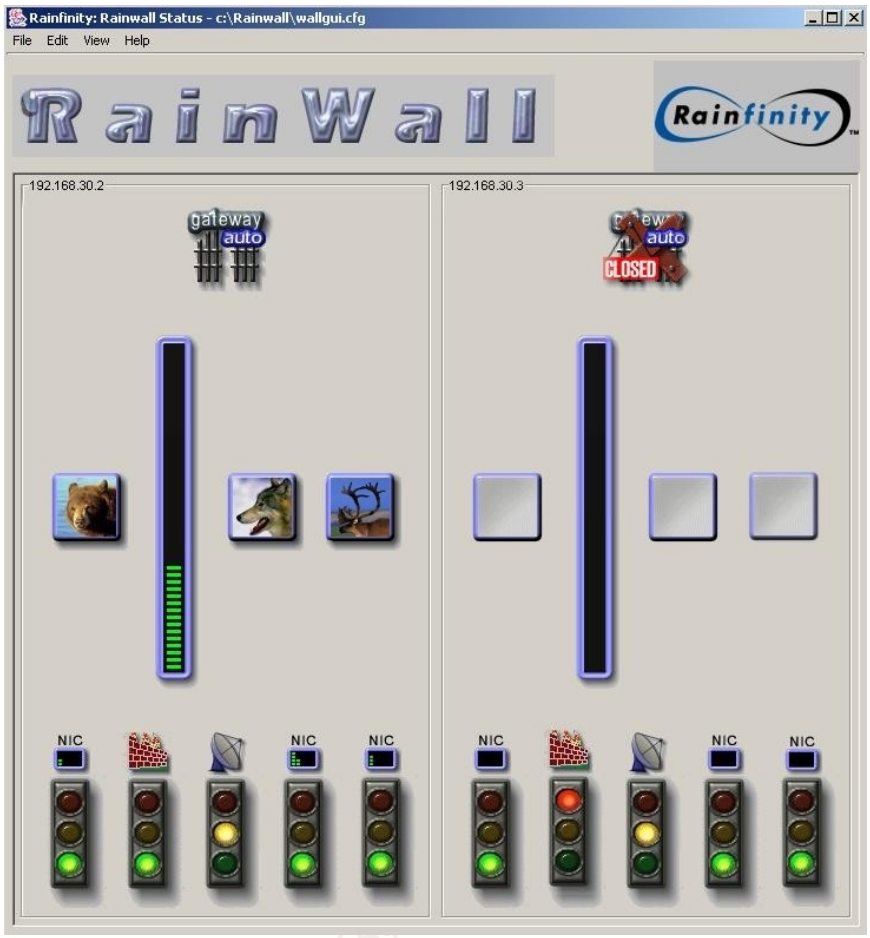
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	RainwallCluster	RainwallCluster	Rainwall_Stop	drop	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall rule to determine that firewall is operating properly.
2	RainwallCluster	RainwallCluster	Rainwall_Daemon	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rule permitting communication between the Rainwall cluster machines.
3	RainwallCluster mgmt_server	RainwallCluster	Rainwall_Status	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall status rule to permit communication between remote Management Console.
4	mgmt_server	RainwallCluster	Rainwall_Command	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows Rainwall Management GUI access to RainwallCluster.

In order to verify that the above rules are working properly, a test was conducted from the management server (192.168.30.17). The Rainwall management GUI was brought up and the first node was shutdown. Rainwall failed over to the other node automatically.

I right-clicked on the gateway icon and selected Disable Gateway. What is shown below is the effect of this action. The gateway shows it is a closed state and the VIPs moved over to the other node. Just before I disabled the active node, I started a ping from 192.168.30.17. Not one ping request timed out. The firewall was able to successfully switch over to the hot-standby node without missing a beat.



As a final test of the Rainwall ruleset, a fwstop was issued on the hot-standby node and the captured screen shot is below. The rule recognized the firewall had stopped.



I feel confident that the Rainwall ruleset is operating properly and according to policy.

Rule 5

5	Any	web_server	http https	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Public access to eFortCS Web/DB server

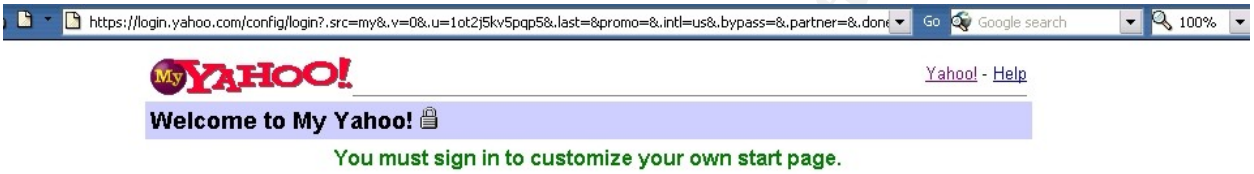
A nmap scan was run against the web server (209.245.30.70) from workstation located at 209.245.30.5.

```
#  C:\bin\nmap-3.00>nmap -P0 -sS -F 209.245.30.70

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.70:
(The 1146 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https

Nmap run completed -- 1 IP address (1 host up) scanned in 297 seconds
```

This is exactly what we want to see; only http/https in an open state. A scan from the internal management server at 192.168.30.17 produced the same results. Correlation of the firewall logs confirmed our results.

Rule 6

To confirm that rule six only allows the above services, the management server at 192.168.30.17 was used to attempt http, https, ping, and traceroutes out to yahoo.com. It was also confirmed that one could ftp out (microsoft.com).




```
C:\bin\nmap-3.00>ping yahoo.com

Pinging yahoo.com [66.218.71.198] with 32 bytes of data:

Reply from 66.218.71.198: bytes=32 time=111ms TTL=247
Reply from 66.218.71.198: bytes=32 time=113ms TTL=247
Reply from 66.218.71.198: bytes=32 time=99ms TTL=247
Reply from 66.218.71.198: bytes=32 time=45ms TTL=247

Ping statistics for 66.218.71.198:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 113ms, Average = 92ms
```

```
C:\bin\nmap-3.00>tracert -d yahoo.com

Tracing route to yahoo.com [64.58.79.230]
over a maximum of 30 hops:

  1    1 ms    1 ms    1 ms  192.168.30.1
...
 12    50 ms    51 ms    51 ms  64.58.79.230

Trace complete.
```

```
C:\bin\nmap-3.00>ftp ftp.microsoft.com
Connected to ftp.microsoft.com.
220 Microsoft FTP Service
User (ftp.microsoft.com:(none)):
```

All allowed services were confirmed to work from both internal and from the modem pool. The last test is to see if other services are not allowed. An attempt was made to connect to port 135 to yahoo.com. The result shows the port is filtered which confirms our policy.

```
C:\bin\nmap-3.00>nmap -P0 -sS -p 135 yahoo.com

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (64.58.79.230):
Port       State       Service
135/tcp    filtered    loc-srv

Nmap run completed -- 1 IP address (1 host up) scanned in 40 seconds
```

The firewall logs confirmed the above tests.

Rule 7

Two nmap scans (-sS for tcp and -sU for udp) was performed from workstation 209.245.30.5 and management server 192.168.30.17 to 209.245.30.69.

```
Scan from 209.245.30.5

C:\bin\nmap-3.00>nmap -P0 -sS -F 209.245.30.69

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.69:
(The 1147 ports scanned but not shown below are in state: filtered)
Port       State       Service
53/tcp     open        domain

Nmap run completed -- 1 IP address (1 host up) scanned in 242 seconds

C:\bin\nmap-3.00>nmap -P0 -sU -F 209.245.30.69

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.69:
(The 996 ports scanned but not shown below are in state: filtered)
Port       State       Service
53/udp     open        domain

Nmap run completed -- 1 IP address (1 host up) scanned in 1202 seconds
```

```
Scan from 192.168.30.17

C:\bin\nmap-3.00>nmap -P0 -sS -F 209.245.30.69

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.69:
(The 1148 ports scanned but not shown below are in state: filtered)

Nmap run completed -- 1 IP address (1 host up) scanned in 239 seconds

C:\bin\nmap-3.00>nmap -P0 -sU -F 209.245.30.69

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.69:
(The 997 ports scanned but not shown below are in state: filtered)

Nmap run completed – 1 IP address (1 host up) scanned in 1342 seconds
```

Results from 209.245.30.5 showed port 53 was in state ‘open’ while the scan from 192.168.30.17 provided the expected results due to the negate rule.

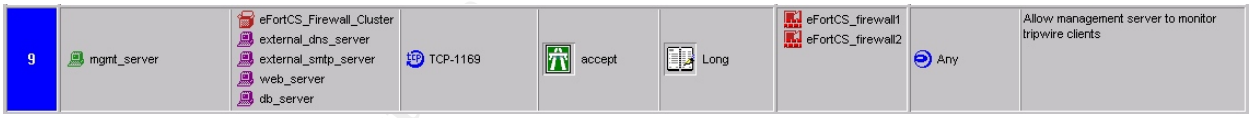
Rule 8

A nmap scan was performed from workstation 209.245.30.5 and management server 192.168.30.17 against 209.245.30.72. Again, the same results as from the domain scan above.

```
Scan from 209.245.30.5

C:\bin\nmap-3.00>nmap -P0 -sS -F 209.245.30.72

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.72:
(The 1147 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp

Nmap run completed – 1 IP address (1 host up) scanned in 209 seconds
```

```
Scan from 192.168.30.17

C:\bin\nmap-3.00>nmap -P0 -sS -F 209.245.30.72

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.72:
(The 1148 ports scanned but not shown below are in state: filtered)

Nmap run completed – 1 IP address (1 host up) scanned in 342 seconds
```

Rule 9



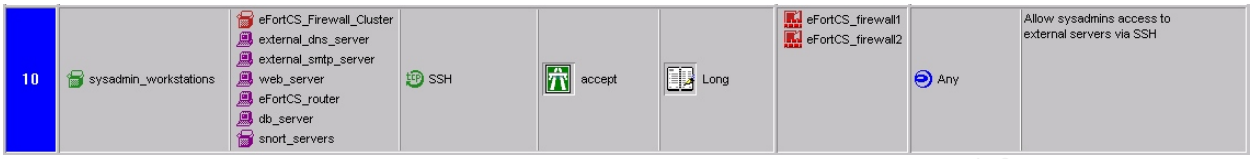
To confirm that only the management server at 192.168.30.17 is the only system allowed communication on tcp/1169, a nmap scan was performed against that port only. Another nmap scan was tried from workstation 209.245.30.5.

```
From 192.168.30.17
C:\bin\nmap-3.00>nmap -P0 -sS -p 1169 209.245.30.2 209.245.30.3 209.245.30.69 209.245.30.70 209.245.30.71
209.245.30.72

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.2:
Port       State       Service
1169/tcp   open   unknown

Interesting ports on 209.245.30.3:
Port       State       Service
1169/tcp   open   unknown

Interesting ports on 209.245.30.69:
Port       State       Service
1169/tcp   open    unknown

Interesting ports on 209.245.30.70:
Port       State       Service
1169/tcp   open    unknown

Interesting ports on 209.245.30.71:
Port       State       Service
1169/tcp   open    unknown

Interesting ports on 209.245.30.72:
Port       State       Service
1169/tcp   open    unknown

Nmap run completed -- 6 IP addresses (6 hosts up) scanned in 11seconds
```

```
From 209.245.30.5
C:\bin\nmap-3.00>nmap -P0 -sS -p 1169 209.245.30.2 209.245.30.3 209.245.30.69 209.245.30.70 209.245.30.71
209.245.30.72

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 209.245.30.2:
Port       State       Service
1169/tcp   filtered    unknown

Interesting ports on 209.245.30.3:
Port       State       Service
1169/tcp   filtered    unknown

Interesting ports on 209.245.30.69:
Port       State       Service
1169/tcp   filtered    unknown

Interesting ports on 209.245.30.70:
Port       State       Service
1169/tcp   filtered    unknown

Interesting ports on 209.245.30.71:
Port       State       Service
1169/tcp   filtered    unknown

Interesting ports on 209.245.30.72:
Port       State       Service
1169/tcp   filtered    unknown

Nmap run completed -- 6 IP addresses (6 hosts up) scanned in 198 seconds
```

For rule nine, only connections from the management console were allowed to communicate on the tripwire port 1169/tcp. The firewall logs also confirmed the results.

Rule 10



To verify Rule ten, a nmap scan was performed from the management server at 192.168.30.17 and another scan from our outside workstation at 209.245.30.5. Results are contained below. The scan will only target tcp/22 on the scan.

```
From 192.168.30.17
C:\bin\nmap-3.00>nmap -P0 -sS -p 22 209.245.30.2 209.245.30.3 209.245.30.68 209.245.30.69 209.245.30.70
209.245.30.71 209.245.30.72 209.245.30.129 209.245.30.251
Starting nmap V. 3.00 ( www.insecure.org/nmap )

Interesting ports on 209.245.30.2:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.3:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.68:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.69:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.70:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.71:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.72:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.129:
Port       State      Service
22/tcp   open       ssh

Interesting ports on 209.245.30.251:
Port       State      Service
22/tcp   open       ssh

Nmap run completed -- 9 IP addresses (9 hosts up) scanned in 19 seconds
```

```
From 209.245.30.5
C:\bin\nmap-3.00> nmap -P0 -sS -p 22 209.245.30.2 209.245.30.3 209.245.30.68 209.245.30.69 209.245.30.70
209.245.30.71 209.245.30.72 209.245.30.129 209.245.30.251

Starting nmap V. 3.00 ( www.insecure.org/nmap )

Interesting ports on 209.245.30.2:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.3:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.68:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.69:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.70:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.71:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.72:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.129:
Port       State      Service
1169/tcp   filtered   unknown

Interesting ports on 209.245.30.251:
Port       State      Service
22/tcp     open       ssh

Nmap run completed -- 9 IP addresses (9 hosts up) scanned in 238 seconds
```

The scan from the internal management server produces results consistent with the rulebase, the scan from outside on 209.245.30.5 did as well. The open port to the router makes sense due to the fact that the workstation scanning is between the firewall and the router.

Rule 11

In order to test Rule 11, the nmap scan will be coming from the firewall at addresses 209.245.30.2 and 209.245.30.3. Again, the management server at 192.168.30.17 and the workstation at 209.245.30.5 will demonstrate the rule is valid by filtering the scan.

```
From 209.245.30.2/209.245.30.3 (same results)

#   nmap -P0 -sU -p 1645 192.168.30.14
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on 192.168.30.14:

Port            State       Service
1645/udp    open        radius

Nmap run completed -- 1 IP address (1 host up) scanned in 37seconds
```

```
From 192.168.30.17 and 209.245.30.5

#   nmap -P0 -sU -p 1645 192.168.30.14
Starting nmap V. 3.00 ( www.insecure.org/nmap )

The 1 scanned port on 192.168.30.14 is: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 17seconds
```

Nmap verified that Rule 11 is functional. Only access to the internal Radius server is from the firewall for authentication purposes only.

Rules 12/13

12	Any	eFortCS_Firewall_Cluster	ESP FW1_keys	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Needed for SecuRemote access.
13	SecuRemote@Any	Any	Any	Client Encrypt	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow remote and modem pool eFortCS employees access to intenal resources via SecuRemote

Rules 12 and 13 are tied together in supporting SecuRemote. The best way to validate these rules is to attempt a SecuRemote session and capture the stream using tcpdump. A SecuRemote session was opened with workstation 209.245.30.5. Below is the results (note efortcs_firewall1 – 209.245.30.2 is the active node):

```
09:27:54.245663 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 1 I agg:(sa: doi=ipsec
situation=identity(p: #1 protoid=isakmp transform=4
(t: #1 id=ike (type=enc value=3des)(type=hash value=sha1)(type=auth
value=preshared)(type=group desc value=modp1024)(type=lifetype value=sec)(type=lifeduration
len=4 value=00003840))(t: #2 id=ike (type=enc value=3des)(type=hash value=md5)(type=auth
value=preshared)(type=group desc value=modp1024)(type=lifetype value=sec)(type=lifeduration
len=4 value=00003840))(t: #3 id=ike (type=enc value=1des)(type=hash value=sha1)(type=auth
value=preshared)(type=group desc value=modp1024)(type=lifetype value=sec)(type=lifeduration
len=4 value=00003840))
(t: #4 id=ike (type=enc value=1des)(type=hash value=md5)(type=auth
value=preshared)(type=group desc value=modp1024)(type=lifetype value=sec)(type=lifeduration
len=4 value=00003840))))
(ke: key len=128)(nonce: n len=20)(id: idtype=user FQDN protoid=0 port=0 len=8 ssmith2)(vid: len=40)
09:27:54.672400 efortcs_firewall1.isakmp > 209.245.30.5.isakmp: isakmp: phase 1 R agg:
(sa: doi=ipsec situation=identity(p: #1 protoid=isakmp transform=1
(t: #1 id=ike (type=enc value=3des)(type=hash value=sha1)(type=auth
value=preshared)(type=group desc value=modp1024)(type=lifetype value=sec)(type=lifeduration
len=4 value=00003840))))(ke: key len=128)(nonce: n len=20)
(id: idtype=IPv4 protoid=0 port=0 len=4 efortcs_firewall1)(vid: len=40)(hash: len=20) (DF)
09:27:54.911922 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 1 I agg:(hash: len=20)
09:27:55.005675 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 1 I agg:(hash: len=20)
09:27:55.115160 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 1 I agg:full rights.
Key fingerprint = DB27 EC46 4D42 664D ECB4 BC3D A8C4 E4C8 B245 7C37
Key fingerprint = DB27 EC46 4D42 664D ECB4 BC3D A8C4 E4C8 B245 7C37
(hash: len=20)
09:27:55.023514 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 2/others I oakleyquick[
E]: [encrypted hash]
09:27:55.326716 efortcs_firewall1.isakmp > 209.245.30.5.isakmp: isakmp: phase 2/others R oakleyquick[
E]: [encrypted hash] (DF)
09:27:55.432569 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 2/others I oakleyquick[
E]: [encrypted hash]
09:27:55.532571 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 2/others I oakleyquick[
E]: [encrypted hash]
09:27:55.634266 209.245.30.5.isakmp > efortcs_firewall1.isakmp: isakmp: phase 2/others I oakleyquick[
E]: [encrypted hash]
09:27:55.753491 209.245.30.5 > efortcs_firewall1: ESP(spi=0x0c5a0bbd,seq=0x1)
09:27:55.835419 efortcs_firewall1 > 209.245.30.5: ESP(spi=0x7b7eaa30,seq=0x1)
09:27:55.852077 209.245.30.5 > efortcs_firewall1: ESP(spi=0x0c5a0bbd,seq=0x2)
09:27:55.949266 efortcs_firewall1 > 209.245.30.5: ESP(spi=0x7b7eaa30,seq=0x2)
09:27:55.951572 efortcs_firewall1 > 209.245.30.5: ESP(spi=0x7b7eaa30,seq=0x3)
```

The tcpdump captured an IPSEC tunnel being set up with Phase1 and Phase2 negotiations, and ESP (protocol 50) packets kicking in for the actual encrypted data.

Rules 14 and16

14	eFortCS_Firewall_Cluster	anti-virus_server	FW1_cvp	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Allow firewall cluster to talk to anti-virus scanner
16	external_smtp_server	internal_smtp_server	smtp->SMTP_scan	accept	Account	eFortCS_firewall1 eFortCS_firewall2	Any	Virus/content filtering on all incoming email traffic

Rules 14 and16 will be discussed together as they are closely associated in the rulebase. To verify Rule 14, the test virus file, eicar.com, was sent through the firewall. Not only did the internal server communicate with the external smtp server, the anti-virus server did its very important function as well. Below is the message the sys admin received in response to this test:

From: InterScan@eFortCS.com
Sent: Wednesday, February 19, 2003 3:46 PM
To: hostmaster@eFortCS.com
Subject: Attachment Stripped in Transaction (Replaced with text)

********** eManager Notification **********

The eFortCS firewall has stripped the attachment because it may contain a virus or malicious code.

Source mailbox: "tester@test-isp.com"
Destination mailbox(es): "hostmaster@eFortCS.com"
Policy: Replaced with text
Attachment file name: eicar.com - application/octet-stream
Action: Attachment Removal

****************** End of message ******************

The anti-virus capability of the firewall is functioning properly as well as the exchange between the external smtp relay server and the internal smtp server.

Rule 15

As demonstrated in the section above, *Audit Against Firewall,* the stealth rule is working properly and preventing no connectivity to the firewall itself except what is allowed by the rulebase. The firewall logs substantiates this rule everyday due to scans performed against it.

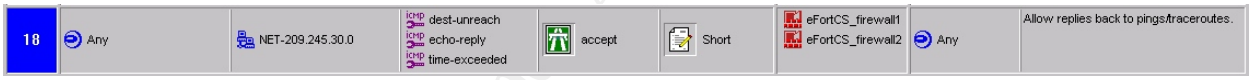
Rule 17

Tcpdump listened on the interface of the SNORT server on the DMZ switch. It captured the traffic below which was allowed through the firewall for syslog traffic:

```
21:14:32.224803 209.245.30.253.4086 > 209.245.30.73.514: udp 87
21:14:34.157466 209.245.30.251.56959 > 209.245.30.73.514: udp 158
21:14:34.157596 209.245.30.251.49785 > 209.245.30.73.514: udp 158
21:14:34.157789 209.245.30.251.56888 > 209.245.30.73.514: udp 158
21:14:45.625337 209.245.30.251.56959 > 209.245.30.73.514: udp 152
21:14:45.625476 209.245.30.251.49785 > 209.245.30.73.514: udp 152
21:14:45.625601 209.245.30.251.56888 > 209.245.30.73.514: udp 152
21:14:45.625731 209.245.30.251.56959 > 209.245.30.73.514: udp 149
21:14:45.625860 209.245.30.251.49785 > 209.245.30.73.514: udp 149
21:14:45.625981 209.245.30.253.56888 > 209.245.30.73.514: udp 149
21:14:58.429200 209.245.30.251.56959 > 209.245.30.73.514: udp 150
21:14:58.429342 209.245.30.251.49785 > 209.245.30.73.514: udp 150
21:14:58.429474 209.245.30.251.56888 > 209.245.30.73.514: udp 150
21:15:08.329150 209.245.30.253.56959 > 209.245.30.73.514: udp 157
21:15:08.329282 209.245.30.251.49785 > 209.245.30.73.514: udp 157
21:15:08.329451 209.245.30.251.56888 > 209.245.30.73.514: udp 157
21:15:31.357295 209.245.30.252.56959 > 209.245.30.73.514: udp 150
21:15:31.357426 209.245.30.252.49785 > 209.245.30.73.514: udp 150
21:15:31.357546 209.245.30.252.56888 > 209.245.30.73.514: udp 150
21:15:32.334470 209.245.30.253.4086 > 209.245.30.73.514: udp 87
21:15:34.588862 209.245.30.251.56959 > 209.245.30.73.514: udp 152
21:15:34.589001 209.245.30.251.49785 > 209.245.30.73.514: udp 152
21:15:34.589129 209.245.30.251.56888 > 209.245.30.73.514: udp 152
21:15:34.589266 209.245.30.251.56959 > 209.245.30.73.514: udp 149
21:15:34.589400 209.245.30.251.49785 > 209.245.30.73.514: udp 149
21:15:34.589525 209.245.30.251.56888 > 209.245.30.73.514: udp 149
```

The rule supporting syslog appears to working fine.

Rule 18



The test from *Rule 6* showed that pings and traceroutes worked from our internal network. Because the default ICMP rule was disabled, it became necessary to allow ICMP through the rulebase. The ICMP rule is functional.

Rule 19

The firewall logs confirms ICMP packets are being dropped.

Rule 20

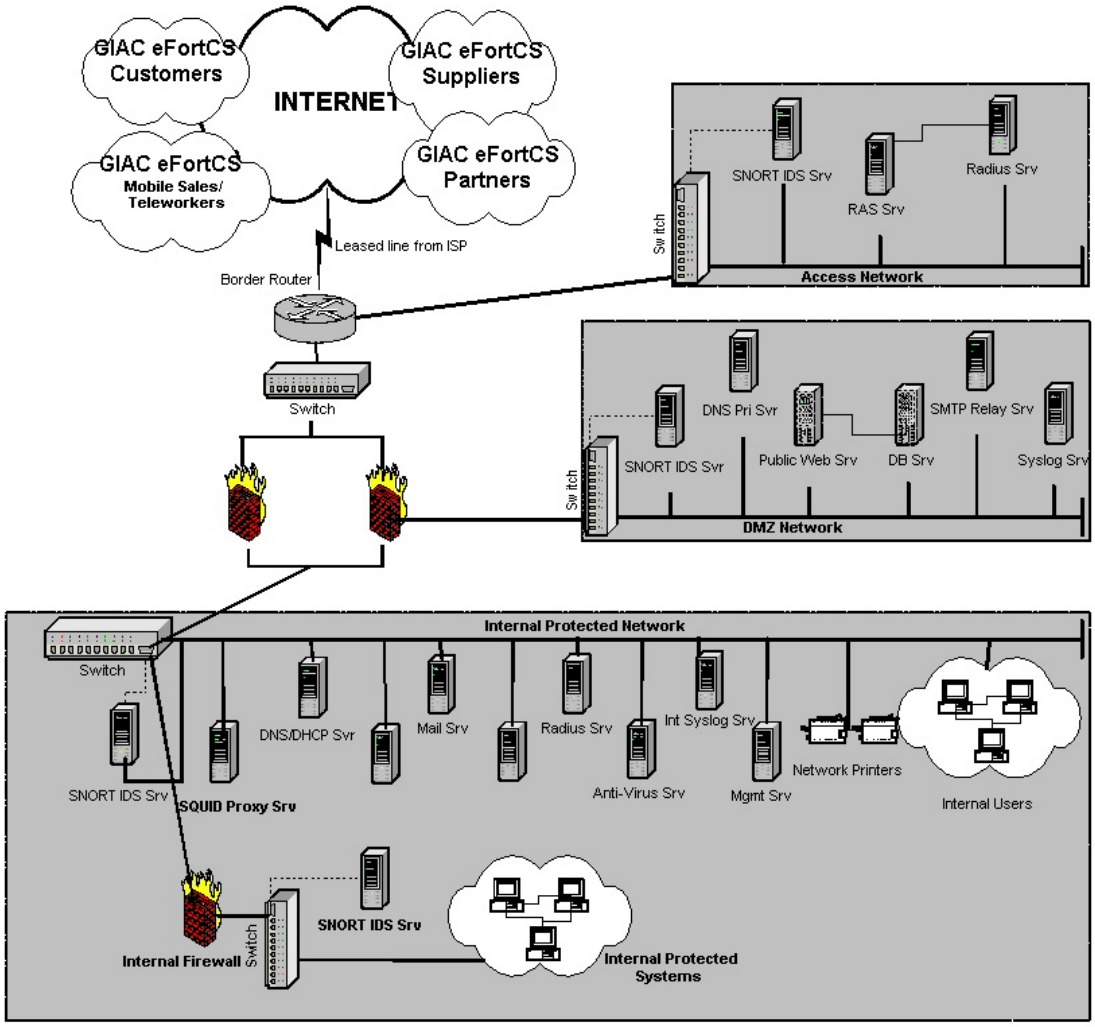
A quick look at firewall logs confirms this rule is functional. Also, the testing associated with the other rules have confirmed that packets are being blocked accordingly.

Evaluation and Recommendations

Packets'R'US did a great job in auditing the firewall policies. They were able to complete the task within the six-hour window that was originally scheduled. They found no major holes that needed immediate attention. Of course, no consultant is worth their salt if they don't find some shortcomings. Packets'R'US provided the following comments and recommendations in their report that was submitted within the 14 day period. Their specific comments/recommendations are:

1. They were pleased to see a HA firewall solution. Demonstration of switching nodes proved successful. The current HA is only a hot-standby solution. It is recommended that eFortCS the load through the firewall and possibly move to a true HA load balance active-active configuration. No additional software is required to support a true load balance scenario with Rainwall; only a software key and configuration changes to Rainwall. Of course, it will cost more money to obtain an active-active solution.
2. To mitigate the potential of a Denial-of-Service attack, configure Check Point with SYN Defender turned on.
3. Incorporate an outbound proxy web server into the network. It was felt that a proxy server like squid, would provide improved security as well as support management usage policy by restricting users access to certain offensive web sites.
4. Develop an automated log correlation tool. This tool should incorporate the firewall, SNORT IDS, and syslogs. Log checking, if done right, can be a time-consuming process. Provide a means to consolidate and correlate the logs that are important to eFortCS. Packets'R'US would be available to develop such a tool.
5. Documentation of Network Security can be improved. This report provides a good start to documenting the network. Recommend that this document be fleshed out.
6. In order to maintain and audit firewall and border router policy, develop a test audit application. It can be a custom tool that utilizes open source scanners, etc. This will provide a consistent check against perimeter routers and firewall. Insure that this tool be run every time a policy change is made and on a regular planned schedule of at least once a month. Packets'R'US will submit a formal proposal for management consideration.
7. Recommend that sensitive systems be placed behind an internal firewall. Currently, eFortCS has no restrictions on internal access. This would not necessarily have to be a Check Point solution but something as simple as an IPTables type of firewall.

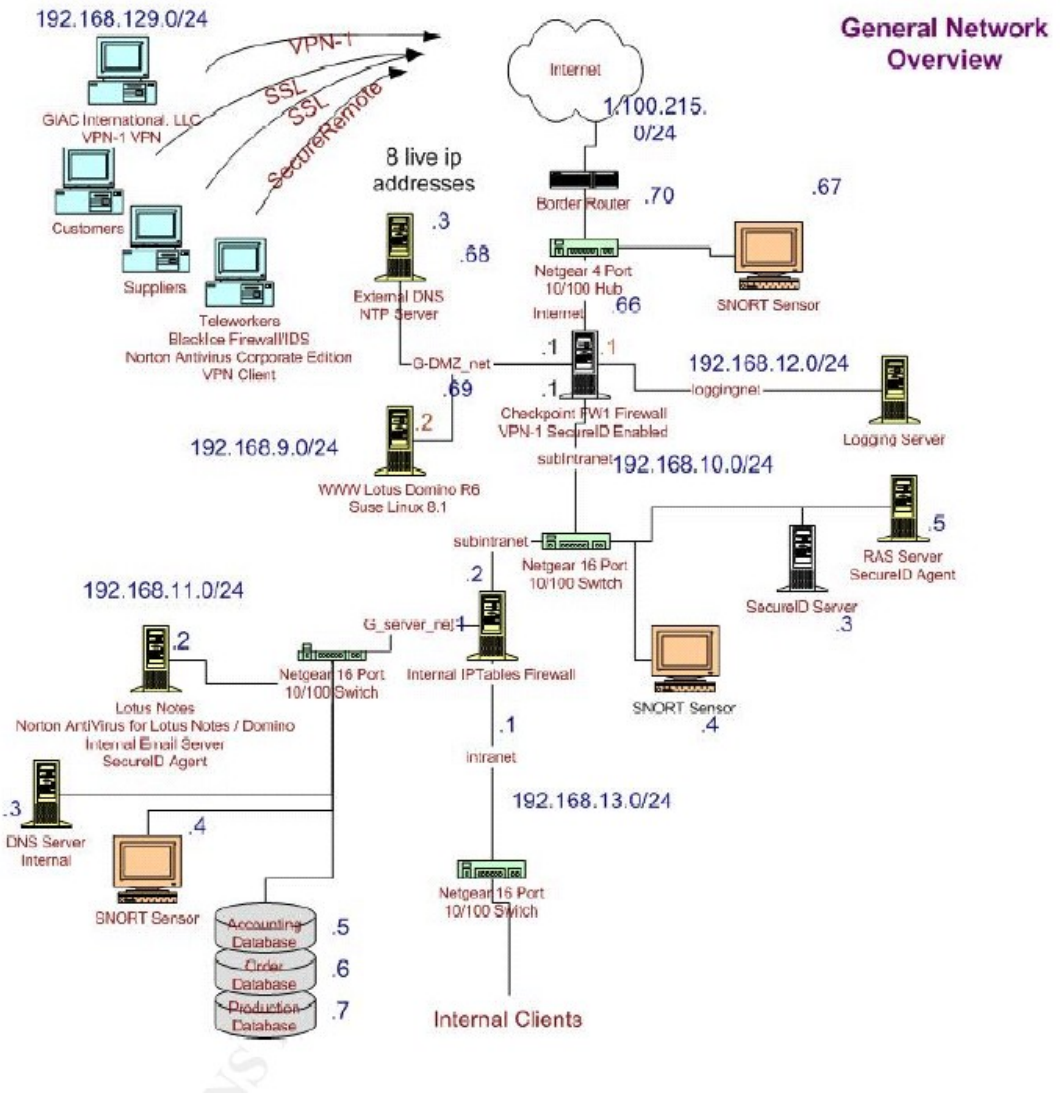
Recommended internal network changes are shown below:



Part Four: Design Under Fire

I selected Craig Duerr's (GWFC Analyst Number 0356) practical posted 31 December 2002. Reference can be found at: http://www.giac.org/practical/GCFW/Craig_Duerr_GCFW.pdf [11]

The network design uses Check Point Firewall-1/VPN-1 version 4.1. Below is the network diagram:

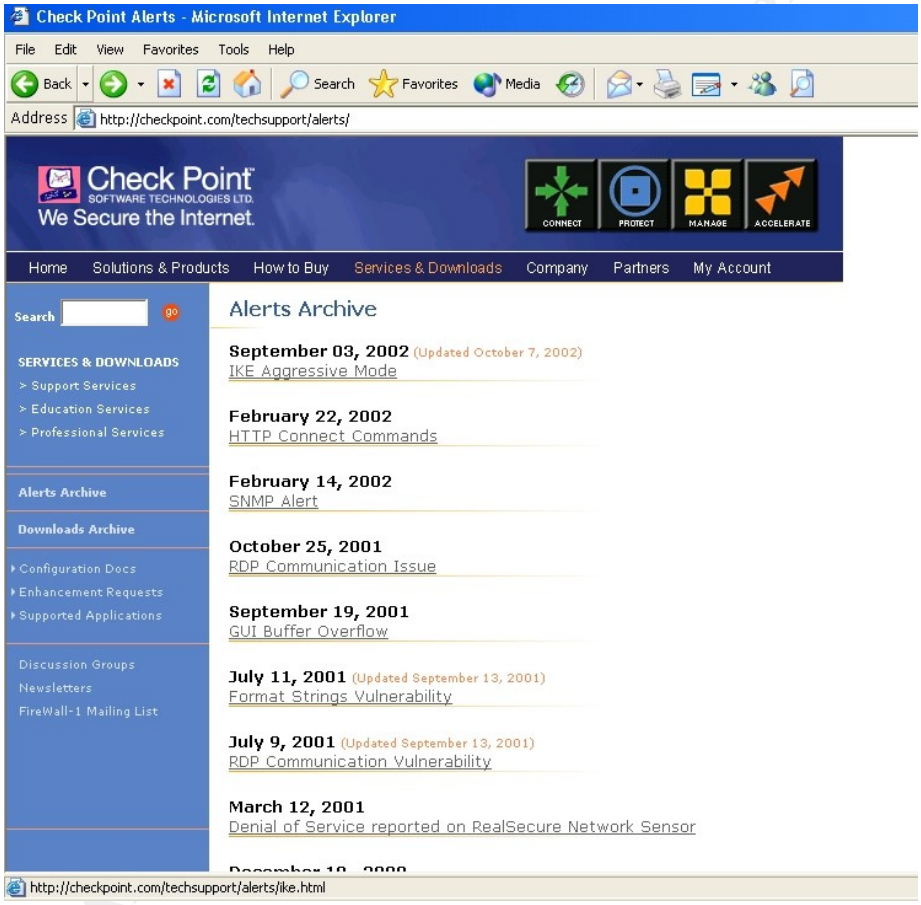


The design uses a Check Point firewall protecting the DMZ and an Internal IPTables firewall protecting critical internal network resources.

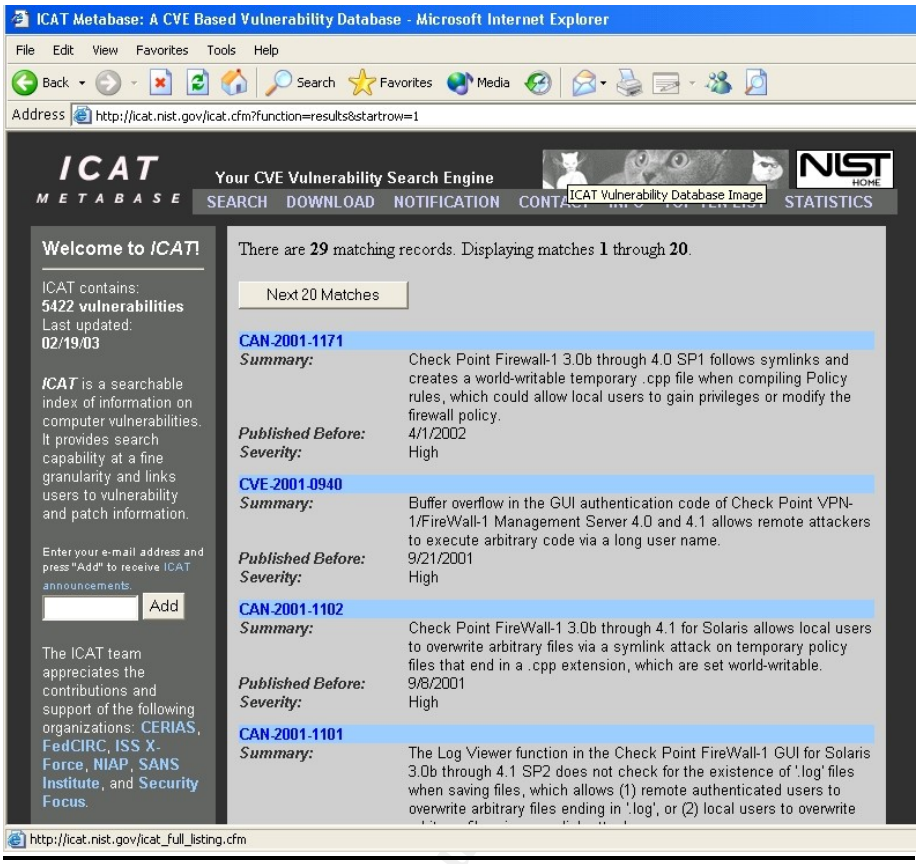
Attack against the Firewall

In order for an attacker to try to break into a firewall, it would be necessary to determine what type of firewall is deployed. Techniques, such as port scanning a potential firewall, might lead to clues, particular, in the case of a Check Point firewall. If tcp/259, tcp/264, tcp/265 are listening, it would be a great clue that it is a Check Point firewall. Without having to go through such steps, it was determined from the practical submission that Check Point Firewall Version VPN-1 and FW-1 Version 4.1 SP6 was being deployed.

The latest alerts were researched from the Check Point web site [12].



Also, NIST ICAT metabase was researched with 29 hits on Check Point [13].



Exploit Selection

Since it appears that this site is running SP6 with no mention of additional hot fixes, IKE aggressive mode was chosen since it is a fairly new vulnerability. Considering that if one could obtain permission via VPN through the firewall, they would have access to internal resources. This would then open up additional opportunities to exploit a more wide range internal hosts or obtain sensitive information via this privileged access.

Roy Hills, Technical Director from NTA Monitor, Ltd, discovered this vulnerability and disclosed the findings on the BugTraq mailing list [14]. He indicated the following in this posting on the NTA web site [15].

During the course of regular testing, NTA Monitor have discovered two serious flaws in Checkpoint Firewall-1, giving rise to both username guessing and sniffing issues.

Firstly, affected versions permit remote users to determine if a Firewall username is valid without having to know the associated password, enabling hackers to guess valid usernames using a dictionary attack. In tests of the flaw conducted by NTA Monitor, it took 2 minutes 30 seconds to check 10,000 usernames at a rate of 67 guesses per second using only 10% of a 2Mbps leased line. The guessing rate is mostly limited to by the Firewall CPU rather than by the Internet link speed. In effect, this means that companies using a hi-spec firewall server increase the speed at which an attacker can guess passwords.

In addition, VPN usernames are passed in the clear without encryption, allowing anyone who is able to sniff network traffic between VPN clients and the Firewall to observe usernames in transit. The flaws exploit the Internet Key Exchange (IKE) encryption scheme and affect all Checkpoint Firewall-1 systems of 4.0 or above.

This leaves the back door to the enterprise wide open to hackers. The biggest problem is that it is not necessary to send a password to obtain a reply from the Firewall. Given that both users and system administrators often chose weak passwords, it is likely that any attacker wil be able to guess at least one password and thus gain access to the VPN - and from there most configurations easily allow full access to the company's resources.

The correct approach would be to wait until both username and password are supplied, and if either is incorrect, send a generic error message. We were surprised to find this flaw when this is standard security practice in many other authentication mechanisms, including Unix logon.

This is a true brute force exploit of Firewall-1. One could go through a bunch of hoops and attempt to gather username information by covert or other means but with this sort of capability, one could build a dictionary of known usernames and "let 'er rip", so to speak. This could be a hit or miss type effort. It would still be more effective to attempt to obtain valid users to attempt the process. One could go to the web site and look for any contact info that might be found. With only finding as few as ten names, it would increase the odds of a successful attack attempt.

NTA web site provided the example [16]. A packet is crafted in IKE Phase-1 aggressive mode in the following format:

1. ISAKMP Header
2. SA - Containing one proposal with four transforms:
a) 3DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
b) 3DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
c) DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
d) DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
3. Key Exchange - DH Group 2 (MODP 1024)
4. Nonce

5. Identification - Type ID_USER_FQDN, Value is SecuRemote username as text string
The four transforms were selected to ensure that there would be an acceptable combination of encryption and hash algorithms for the Firewall. It would be possible to use just one transform if it were known which encryption and hash algorithms the Firewall supported.

NTA developed a script that performs the brute force attack using a dictionary of usernames. Script usage and examples of this program and results are listed below [16 ibid]:

```
# > fw1-ike-userguess --help
Usage: fw1-ike-userguess [options] <hostname>

<hostname> is name or IP address of Firewall.

Options:

--file=<fn> or -f <fn>  Read usernames from file <fn>, one per line.
--help or -h            Display this help message and exit.
--id=<id> or -i <id>    Use string <id> as SecuRemote username.
--sport=<p> or -s <p>   Set UDP source port to <p>.  Default 500.  0=random.
--dport=<p> or -d <p>   Set UDP dest. port to <p>.  Default 500.
--timeout=<n> or -t <n> Set timeout to <n> ms.  Default 2000.
--random=<n> or -r <n>  Set random seed to <n>.  Default is based on time
                        Used to generate key exchange and nonce data.
--version or -V         Display program version and exit.
--idtype=n or -y n      Use identification type <n>.  Default 3 (ID_USER_FQDN)
                        For Checkpoint SecuRemote VPN, this must be set to 3.
--dhgroup=n or -g n     Use Diffie Hellman Group <n>.  Default 2
                        Acceptable values are 1,2 and 5 (MODP only).

fw1-ike-userguess version 1.2 2002-08-30 <Roy.Hills@nta-monitor.com>
```

Results

```
Username guessing against Firewall-1 4.1 SP6
rsh@radon% fw1-ike-userguess --file=testusers.txt 172.16.2.2
testuser Notify message 9101 (User testuser unknown.)
test-ike-3des USER EXISTS
testing123 Notify message 9101 (User testing123 unknown.)
test-ike-des USER EXISTS
guest Notify message 9101 (User guest unknown.)
test-fwz-des Notify message 9101 (User cannot use IKE)
test-ike-cast40 USER EXISTS
test-ike-ah USER EXISTS
test-ike-hybrid Notify message 9101 (IKE is not properly defined for user.)
test-expired Notify message 9101 (Login expired on 1-jan-2002.)
Username guessing against Firewall-1 NG FP2
rsh@radon% fw1-ike-userguess --file=testusers.txt 192.168.124.150
testuser Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-3des USER EXISTS
testing123 Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-des USER EXISTS
guest Notify message 14 (NO-PROPOSAL-CHOSEN)
test-fwz-des Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-cast40 Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-ah Notify message 14 (NO-PROPOSAL-CHOSEN)
test-ike-hybrid Notify message 14 (NO-PROPOSAL-CHOSEN)
test-expired Notify message 14 (NO-PROPOSAL-CHOSEN)
```

Results of Attack

The potential use of this attack would be to obtain access with an obtained username. With a valid username, a password cracking dictionary could be utilized. Given the fact that there are users who still pick weak passwords, this could be considered a very likely possibility. If the overall attack was successful, one would have full authorization through the VPN to internal resources; in other words, Game Over! In our particular

attack against the referenced practical, the most likely scenario is that this attack was unsuccessful. Craig is utilizing SecurID which is an excellent means to prevent this attack. One can only hope that there are some administrative passwords directly on the firewall itself.

Counter Measures

The following steps are strongly recommended!

1.Apply the SP6- Aggressive IKE Hotfix.
2.Insure all accounts are using Firewall-1 Hybrid mode authentication with SecurID (or other strong authentication) server with one-time password authentication card.
3.Limit access to IKE to known authorized IP addresses.

Denial of Service Attack

50 cable modems/DSL hosts have been compromised with TFN2K (Tribal FloodNet 2K) servers installed. A vulnerability in Bind was reported in November 2002. Information concerning this can be found here http://icat.nist.gov/icat.cfm?cvename=CAN-2002-1219 [17]. Exploitation of this vulnerability could result in the execution of arbitrary attacker-supplied code with the privileges of the vulnerable BIND daemon. With the number of small businesses using cable modems/DSL, it would be very easy to find and compromise 50 DNS servers and install TFN2K.

TFN2K is a client-server tool that can be used to launch a distributed Denial-of-Service attack against a specific server. TFN2K is available from Packet Storm at http://packetstormsecurity.org/distributed/tfn2k.tgz. A detailed analysis of TFN2K was written by Jason Barlow and Woody Thrower [18]. A good description of TFN2K is provided from this paper.

> TFN2K is a two-component system: a command driven client on the master and a daemon process operating on an agent. The master instructs its agents to attack a list of designated targets. The agents respond by flooding the targets with a barrage of packets. Multiple agents, coordinated by the master, can work in tandem during this attack to disrupt access to the target. Master-to-agent communications are encrypted, and may be intermixed with any number of decoy packets. Both master-to-agent communications and the attacks themselves can be sent via randomized TCP, UDP, and ICMP packets. Additionally, the master can falsify its IP address (spoof). These facts significantly complicate development of effective and efficient countermeasures for TFN2K.

Usage of tfn client is broken down below:

./tfn <-f file | <-h host> -c <id> -i target host <options> -p target port

-f file contains list of compromised TFN2K servers

-h hostname of just one server

-c <id> consists of one of 10 different options.

ID 1 - Anti Spoof Level: The DoS attack commenced by the servers will always emanate from spoofed source IP addresses. With this command, you can control which part of the IP address will be spoofed, and which part will contain real bits of the actual IP.

ID 2 - Change Packet Size: The default ICMP/8, SMURF, and UDP attacks use packets of a minimal size by default. You can increase this size by changing the payload size of each packet in bytes.

ID 3 - Bind root shell: Starts a one-session server that drops you to a root shell when you connect to the specified port.

ID 4 - UDP flood attack. This attack can be used to exploit the fact that for every udp packet sent to a closed port, there will be an ICMP unreachable message sent back, multiplying the attacks potential.

ID 5 - SYN flood attack. This attack steadily sends bogus connection requests. Possible effects include denial of service on one or more targeted ports, filled up TCP connection tables and attack potential multiplication by TCP/RST responses to non-existent hosts.

ID 6 - ICMP echo reply (ping) attack. This attack sends ping requests from bogus source IPs, to which the victim replies with equally large response packets.

ID 7 - SMURF attack. Sends out ping requests with the source address of the victim to broadcast amplifiers, hosts that reply with a drastically multiplied bandwidth back to the source.

ID 8 - MIX attack. This sends UDP, SYN and ICMP packets interchanged on a 1:1:1 relation, which can specifically be hazard to routers and other packet forwarding devices or NIDS and sniffers.

ID 9 - TARGA3 attack. Uses random packets with IP based protocols and values that are known to be critical or bogus, and can cause some IP stack implementations to crash, fail, or show other undefined behavior.

ID 10 - Remote command execution. Gives the opportunity of one-way mass executing remote shell commands on the servers.
-i target hosts <options> <Example of option: "echo Wonder if your server is next to be slammed | mail -s 'a word of warning' webmaster@eFortCS.com"

The command I would use to send to the agents is:

./tfn -f tfn_agent.list -c 5 -i 1.100.215.1 -p 80

This command launches a Syn flood to destination port 80 of victim host 1.100.215.1 using the list of 50 compromised servers. Initially, the pipe from the ISP would be overwhelmed where legitimate packets would have a difficult time getting through. Next, the state table of the firewall would be consumed. Essentially, all traffic would stop under an intense DoS attack as described above.

Counter Measures

There is no real way to defend against this type of denial-of-service attack. However, there are some things that can be done to mitigate this attack.

1. Configure routers to do egress/ingress filtering, preventing spoofed traffic from leaving/entering the network.
2. Employ good IDS system to allow early detection of such an attack.
3. Increase the amount of memory on the firewall to allow for larger state tables.
4. Enable Check Points Syn Defender.
5. Perhaps adding some QoS features on the router to only allow a certain percentage of the bandwidth to the web server. This might still allow connectivity to other network resource.
6. Be a good net neighbor and insure that none of your systems are vulnerable to attacks that might allow the TFN2K agent being installed.

Attack against Internal System

Vulnerability

On March 17, 2003, Microsoft announced a vulnerability in IIS 5.0 web server. The details of the announcement can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-007.asp [18].

While this was a major concern to the Internet community as related to IIS 5.0 servers, the shocking news didn't come out until a week later when it was discovered that this vulnerability could be exploited in many other ways. According to TruSecure Corporation, the affected NTDLL.DLL could potentially provide other attack vectors. Quoting from the article found at http://www.trusecure.com/knowledge/hypeorhot/2003/tsa03006.shtml [19]:

> TruSecure Corporation discovered today that knowledge of other attack vectors against NTDLL.DLL (see TruSecure ALERT TSA 03-005 and 03-005a) are known to the Security Underground Community. We therefore expect attacks, potentially against W2K devices beyond just IIS servers. There are numerous additional attack vectors against NTDLL.DLL.
>
> It is therefore likely that within the near future multiple attacks attempting to exploit the vulnerability in NTDLL.DLL may surface and be used against your systems. Attacks may be network-based intrusion attempts, such as IIS or possibly FTP, NNTP, IMAP, etc... or within Email messages or Web Pages. Trojans may be built which include this attack method. They may come as attachments, or be found on public FTP servers. Further, publication of the details of the vulnerable applications may lead to internal attacks based on code being run by a malicious, although trusted, user.

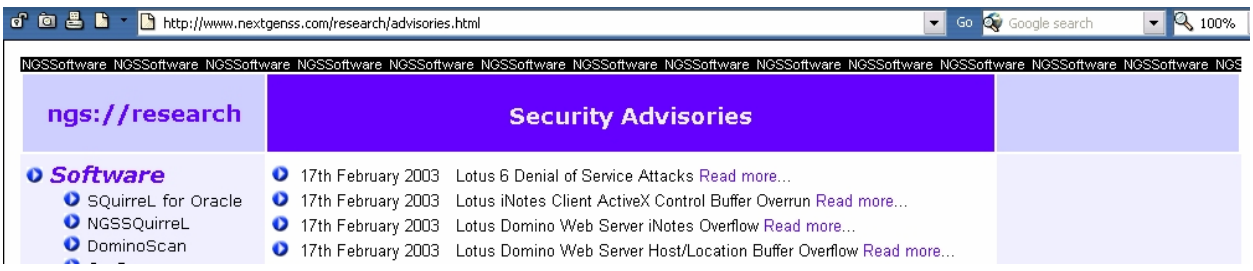
Also, David Litchfield from NGSSoftware concluded in a security research publication concerning the vulnerability found at http://www.nextgenss.com/papers/ms03-007-ntdll.pdf [20] as quoted below:

> Security researchers at NGSSoftware have already discovered several new attack vectors and believe there will be many that will come to light over the next few weeks. There are too many ways for an attacker to "access" the vulnerability. Likely areas will be Non-MS web and ftp servers, IMAP servers, Anti-Virus solutions and other MS Windows Services.
>
> Consequently, NGSSoftware believes that every Windows 2000 server or workstation should be patched, and patched as soon as possible – regardless of whether the box is running IIS or not.

Looks like we have found an attack vector to compromise an internal system. It is a fairly safe assumption that Windows 2000 systems are running at this site considering the dependence of Lotus Notes.

An exploit will be run against the Lotus Domino/Notes server. The impact of the vulnerabilities ranges from denial of service to data corruption and the potential to execute arbitrary code. CERT issued a detailed alert on March 26, 2003 as posted here http://www.cert.org/advisories/CA-2003-11.html [21].

I also searched and found the following Security Advisories at the Nextgenss.com web site [22]:



Attack Vector

Here is the attack vector that will be attempted to compromise an internal system:

1. An attempt will be made using the exploit listed in a security research advisory from NextGenss author Mark Litchfield as listed here http://www.nextgenss.com/advisories/lotus-hostlocbo.txt [23]. Quoting from the advisory concerning the vulnerability:

> Lotus Domino 6 suffers from a remotely exploitable buffer overrun vulnerability when performing a redirect operation. When building the 302 Redirect response, the server takes the client provided "Host" header and implants this value into the "Location" server header. By requesting certain documents or views in certain databases the server can be forced to perform a redirect operation and by supplying an overly long string for the hostname, a buffer can be overflowed allowing an attacker to gain control of the Domino Web Services process. By default these databases can be accessed by anonymous users. Any arbitrary code supplied will run in the context of the account running Domino allowing an attacker to gain control of the server.

If the exploit was successful, it would be possible to install a keystroke logger to collect passwords or install an IP proxy or tunnel to bypass the firewall, such as netcat [24], zebedee [25], or stunnel [26]. The goal here is to obtain account info and provide a hole through the firewall. Using netcat, the following command could be issued on the compromised server:

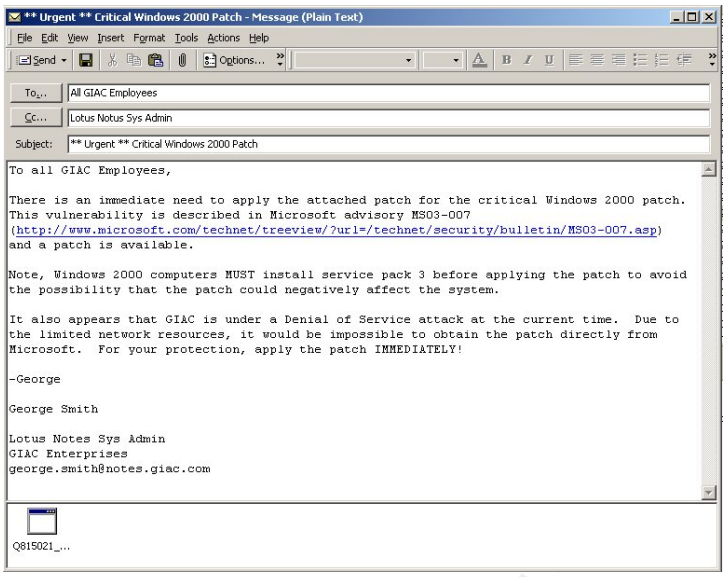
.nc –l p1080 –d –e cmd.exe –L

where:

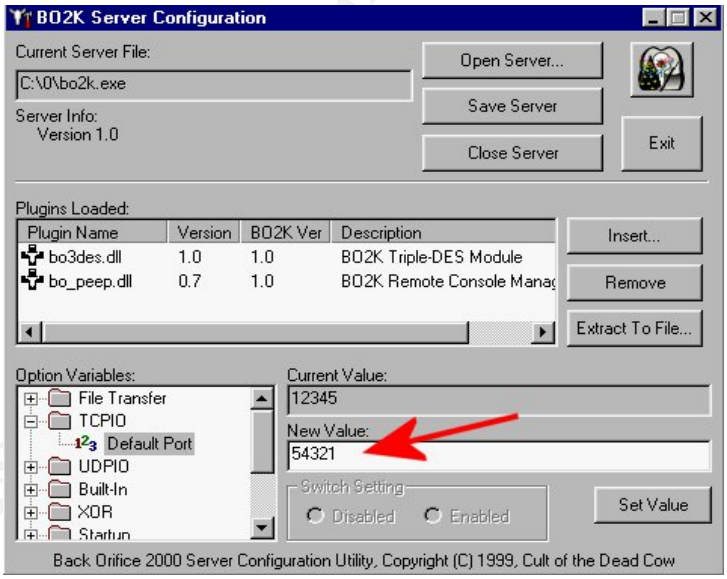
-l (listen mode)
-p 1080 (use port 1080)
-d (run detached from console)
-e cmd.exe (execute cmd.exe)
-L (restart netcat with same command line when connection terminated)

One could then attempt a connection to port 1080 on the compromised server.

2. Armed with a possible hole through the firewall or account info, it would be possible to now send a very convincing email from the Lotus Notes admin pleading for assistance in applying the critical Microsoft patch as mentioned above. However, the attached patch will be the killer app SubSeven or BO2K. The user, knowing the criticality of the patch, will more than likely run the attached 'Microsoft patch-☺'.



3. If this isn't successful, an attachment could be sent that might exploit the buffer overflow in NTDLL.DLL code that is common to many windows applications. Again, malicious code could be run against the Windows system that could install a DDoS zombie or an app like SubSeven or B02K. A B02K server would be configuration as shown below: Notice the change to the listening port.



After B02K is listening on port 54321, an attempt could be made to connect to it from an external client.

Results/Counter Measures

If the above attack were successful, many systems could possibly be compromised. The implications could be disastrous! The exploits could provide a means to bypass the firewall for further attacks through an IP proxy or remote control software like SubSeven or BO2K. It could also provide the means to sniff passwords as well as provide a platform for attacks on other internal or outside systems.

The following counter measures could be used:

1. Apply the latest maintenance release (6.0.1) to Lotus Notes/Domino Server [27].
2. Apply critical Microsoft patch MS03-007 [28].
3. Provide an authenticated means of applying critical patches to internal systems. This might include the use of software such as PatchLink [29].
4. Monitor IDS for any inappropriate activity from client systems such as scanning, or SubSeven/BO2K activity.
5. Insure that client systems are running up-to-date anti-virus software and signatures.

The Design Under Fire section was an eye opener. It really shows how critical it is to keep current on the systems and application software that your site is running. Just because you have installed and patched your firewall, for example, doesn't mean that you can ignore it. The Internet is an unforgiving creature, if you don't keep it caged, it will come back and bite you.

References

[1] Check Point, “Compaq and Check Point Deliver New Rapid Deployment, High Availability Internet Security SolutionPaq”, http://www.checkpoint.com/press/2001/solutionpaq041101.html

[2] TrendMicro, ‘‘InterScan VirusWall’’, http://www.trendmicro.com/en/products/gateway/isvw/evaluate/overview.htm

[3] Microsoft, “OL2002: You Cannot Open Attachments”, http://support.microsoft.com/default.aspx?scid=kb;EN-US;290497

[4] SWATCH, “The Simple WATCHer”, http://www.oit.ucsb.edu/~eta/swatch/

[5] Northcutt, Stephen, et al., ‘‘Inside Network Perimeter Security’’, New Riders, 2003, p. 143-159.

[6] NSA Router Security Configuration Guide v1.1 http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

[7] NIST, “DRAFT Guideline on Network Security Testing”, http://csrc.nist.gov/publications/drafts/security-testing.pdf

[8] Nmap, “Network Mapper”, http://www.insecure.org/nmap

[9] Nessus, “Vulnerability Scanner”, http://www.nessus.org

[10] TrendMicro, “Eicar Test File”, http://www.trendmicro.com/en/security/test/overview.htm

[11] Craig L. Duerr, “GCFW Practical Assignment”, Sans.org, 2002, http://www.giac.org/practical/GCFW/Craig_Duerr_GCFW.pdf

[12] Check Point, “Alert Archive”, http://www.checkpoint.com/techsupport/alerts/

[13] NIST, “ICAT Metabase”, http://icat.nist.gov

[14] BugTraq, “ SecuRemote usernames can be guessed or sniffed using IKE exchange“, http://online.securityfocus.com/archive/1/290202/2002-09-01/2002-09-07/0

[15] NTA, ‘‘NTA Monitor discovers Checkpoint FW-1 flaw...10,000 usernames guesses in 2 minutes 30 seconds.. ‘‘, http://www.nta-monitor.com/news/checkpoint/checkpoint-main.htm

[16] NTA, ‘‘Checkpoint FW-1 flaw technical details’’, http://www.nta-monitor.com/news/checkpoint/checkpoint-tech.htm

[17] NIST, ICAT CVE Vulnerability Search Engine,
http://icat.nist.gov/icat.cfm?cvename=CAN-2002-1219

[18] Barlow, Jason, and Thrower, Woody, "TFN2K – An Analysis",
http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt

[19] TruSecure Corp, "TruSecure Alert – TSA-03-006 – Hype or Not",
http://www.trusecure.com/knowledge/hypeorhot/2003/tsa03006.shtml

[20] David Litchfield, "New Attack Vectors and a Vulnerability Dissection of MS03-007",
http://www.nextgenss.com/papers/ms03-007-ntdll.pdf

[21] CERT, "Advisory CA-2003-11 Multiple Vulnerabilities in Lotus Notes and Domino",
http://www.cert.org/advisories/CA-2003-11.html

[22] NGS Software, "Security Advisories",
http://www.nextgenss.com/research/advisories.html

[23] NGS Software, "Lotus Domino Web Server Host/Location Buffer Overflow Vulnerability", http://www.nextgenss.com/advisories/lotus-hostlocbo.txt

[24] Zebedee.com, "Secure IP Tunnel", http://www.winton.org.uk/zebedee/

[25] @Stake Research Tools, "Network Utility Tools",
http://www.atstake.com/research/tools/network_utilities/

[26] Stunnel.org, "Stunnel – Universal SSL Wrapper", http://www.stunnel.org/

[27] Lotus, "Notes/Domino MR/MU Status ",
http://www-10.lotus.com/ldd/r5fixlist.nsf/Progress/601?opendocument

[28] Microsoft.com, "Windows 2000 Security Patch: IIS Remote Exploit from ntdll.dll Vulnerability",http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en

[29] Patchlink.com, "The Patch Management Experts™ ", http://www.patchlink.com

[30] Rainfinity, "Rainfinity High Availability Software for Check Point VPN-1/Firewall-1",
http://www.rainfinity.com/products/ds_rainwall.html

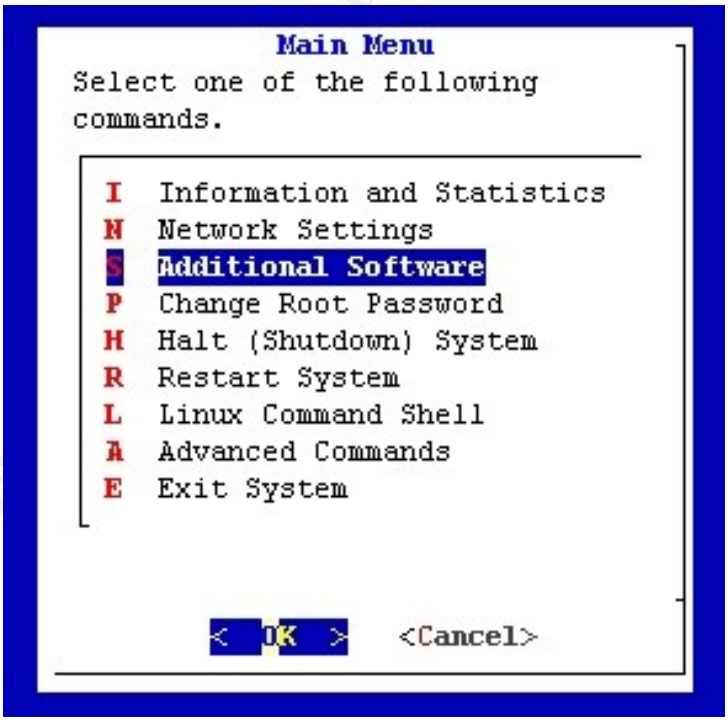
Appendix A

Rainfinity Rainwall Configuration Guide

This tutorial will cover the setup and configuration of Rainwall HA hot-standby firewall cluster software. There are two phases to implementing Rainwall: First, installation and configuration of Rainwall software on each firewall node. Included in this is the Checkpoint Firewall-1/VPN-1 synchronization feature. Second, the firewall policy needed to support Rainwall software. The last part of this tutorial will cover the Management GUI that provides status of firewall cluster as well as the ability to send management commands to the node. This includes the ability to stop a node, switch control from one node to another, and other management functions. Let's get started!

Rainwall provides a nice java based front-end to configure its software. I prefer to get to the heart of the matter and setup the config files direct. This helps one truly understand how the software works and not just be dependent on some GUI interface to configure the software. All config files are located under the /opt/rainwall/conf directory.

Step one involves installing Rainwall software. Do this from the Compaq *start menu* (/etc/Consoles/Console1).



From 'Additional Software' menu, select Install Rainwall. This installs rainwall under the /opt/rainwall directory.

Once the software is installed, the following will need to be performed to configure the system:

a: run /opt/rainwall/bin/rwadmin program. Following is the help command for rwadmin:

.

```
/rwadmin --help
Usage: ./rwadmin [options]
rwadmin is used to administer Rainwall on the local machine.
options:        -q, -quiet: do commands silently
        -p, -passwd [password]: Update Rainwall password. If no password
                is given on command line, you will be prompted for the new password
        -pf, -passwdfile <password file>: Specify the password file to use
                the default location is $RAINWALLROOT/conf/passwd
        -d, -dump : Shows the Rainwall driver information
        -d p, or -dump p: shows proxyarp IPs on the local node
        -query <query string>: send query string to driver
        -h, -help, --help, /? : show this usage listing
```

> ./rwadmin -p *password*

Run this on both firewall nodes.

b. Enter Rainwall-S license /opt/rainwall/conf/license.cfg file (sample license).

```
d11bbbc1-5a2a2a00-a0067bc8
```

Again, update the license.cfg on both nodes.

c. Configure the /opt/rainwall/conf/nodemap.cfg file on both nodes.

```
PRIMARY_IP {
 192.168.30.2
  192.168.30.3
}
```

These IP addresses provide the state synchronization between the two nodes. A cross-over cable between interface eth3 on both nodes provides the best connectivity for this function.

d. Configure VIP addresses of cluster in file /opt/rainwall/conf/vip.cfg on both nodes.

```
VIRTUAL_IP 209.245.30.0 {
  209.245.30.1
}
VIRTUAL_IP 192.168.30.0 {
  192.168.30.1
}
```

This sets up the two Virtual IP addresses associated with the external network/DMZ and internal network.

e: Configure Rainwall for hot-standby mode in file /opt/rainwall/conf/rainwall.cfg on both nodes.

```
RAINWALL {
 hotStandby(1);
}
```

This tells Rainwall that the configuration is hot-standby.

Setup of Check Point Firewall-1/VPN-1 state synchronization is required. This can be accomplished by the following steps:

Edit the /opt/CPfw1-41/conf/sync.conf file. The corresponding IP needs to be setup on each node. A fourth interface, eth3 will be used for this purpose. IP address 10.1.1.1 and 10.1.1.2 will be used.

Node 1:

```
10.1.1.2
```

Node 2:

```
10.1.1.1
```

Authentication is required between the Firewall-1/VPN-1 nodes to allow state synchronization traffic to flow. This can be accomplished by running the following:

Node 1:

```
fw putkey 10.1.1.2
    Enter Secret key:
```

Node 2:

```
fw putkey 10.1.1.1
    Enter Secret key:
```

Verify that Firewall-1/VPN-1 is exchanging state info. This can be accomplished this way:

#> /opt/CPfw-41/bin/fw ctl pstat.

```
Hash kernel memory (hmem) statistics:
  Total memory allocated: 33554432 bytes in 8191 4KB blocks using 1 pool
  Total memory bytes  used:   401080   unused: 33153352 (98%)   peak:  3240636
  Total memory blocks used:      138   unused:     8053 (98%)
  Allocations: 132800188 alloc, 0 failed alloc, 132793433 free
System kernel memory (kmem) statistics:
  Total memory bytes  used: 35120663   peak: 36078715
  Allocations: 6968 alloc, 1174 failed alloc, 6482 free, 0 failed free
Inspct: 738863063 packets, 1141177282 operations, 992015829 lookups, 135918970
record, -1654843488 extract
Cookies: 92382412 total, 0 alloc, 0 free, 35021 dup, 1323247016 get, 35362 put,
1009222281 len, 0 chain alloc, 0 chain free
Fragments: 32589 fragments, 11374 packets, 2998 expired, 0 short, 10 large, 314
duplicates, 0 failures
Encryption: 0 encryption, 0 decryption, 0 short, 0 failures
Translation: 0/2139824997 forw, 0/-2122929016 bckw, 0 tcpudp, 0 icmp, 0-0 alloc
sync old ver working
sync out: on  sync in: off
```

The 'sync out: on' status will be shown at the bottom of the output window. Verify this on both nodes. The last thing to check is whether the state table is sync. There will be a slight variance to this number but should be fairly close. Try to run the following command at the same time from both nodes:

#> /opt/CP-FW41/bin/fw tab -t connections -s

HOST	NAME	ID	#VALS
Node1	Connections	22	3717
Node2	Connections	22	3719

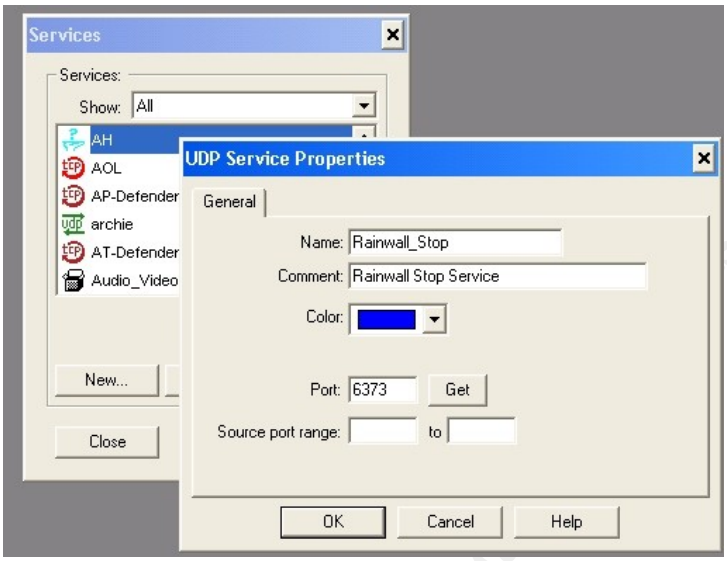
From the above output of the fw tab command, one can see that synchronization is occurring. The #VALS represent active sessions in the connections table.
This concludes phase one of the Rainwall configuration. Phase two will be configuring the firewall policy to support Rainwall.

There will be four rules needed to configure and make sure Rainwall is working properly. The summary of these rules are included below as well as a detailed description on the creation of the services required:

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	RainwallCluster	RainwallCluster	Rainwall_Stop	drop	Short	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall rule to determine that firewall is operating properly.
2	RainwallCluster	RainwallCluster	Rainwall_Daemon	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rule permitting communication between the Rainwall cluster machines.
3	RainwallCluster mgmt_server	RainwallCluster	Rainwall_Status	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall status rule to permit communication between remote Management Console.
4	mgmt_server	RainwallCluster	Rainwall_Command	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Allows Rainwall Management GUI access to RainwallCluster.

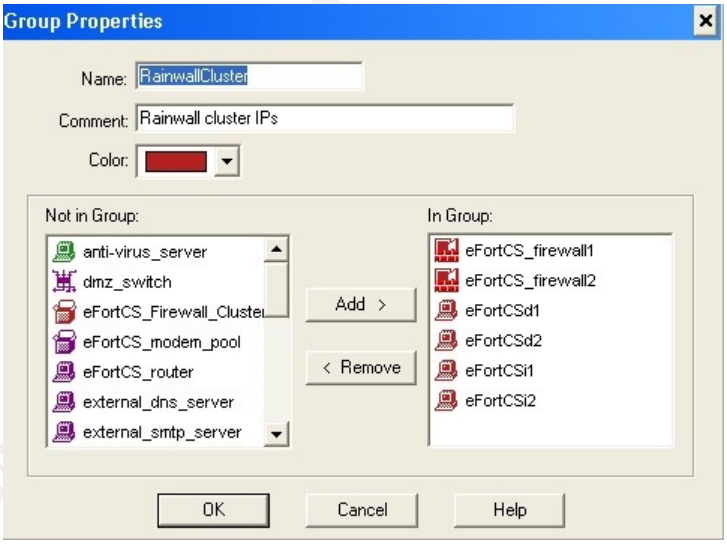
Let's set up rule one. The first rule blocks a specific packet type (Rainwall_stop (udp/6373)) used by Rainwall to determine that the firewall is operating properly. We

first need to create the Rainwall_stop service. This service will be created by going to Manage=>Services=> New => UDP



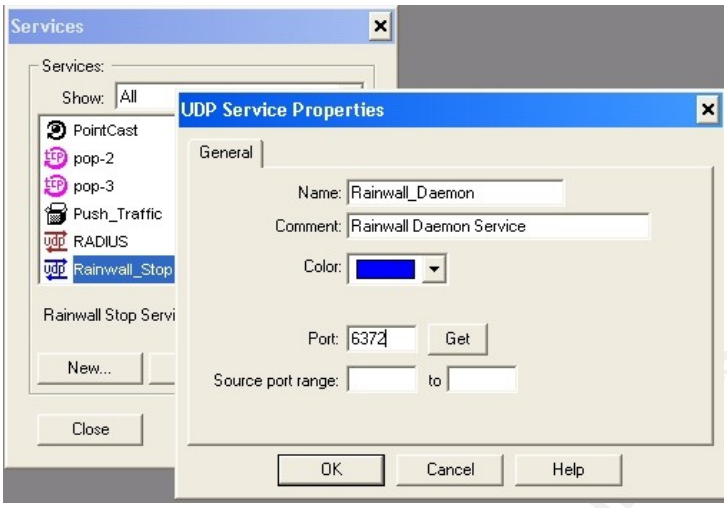
Name the service Rainwall_stop and assign udp/6373 to this service.

The next step is to define the RainWall Cluster group. I did this by selecting Manage => Network Objects => New => Group and include all firewall interfaces in a group.



Now create rule one as shown below:

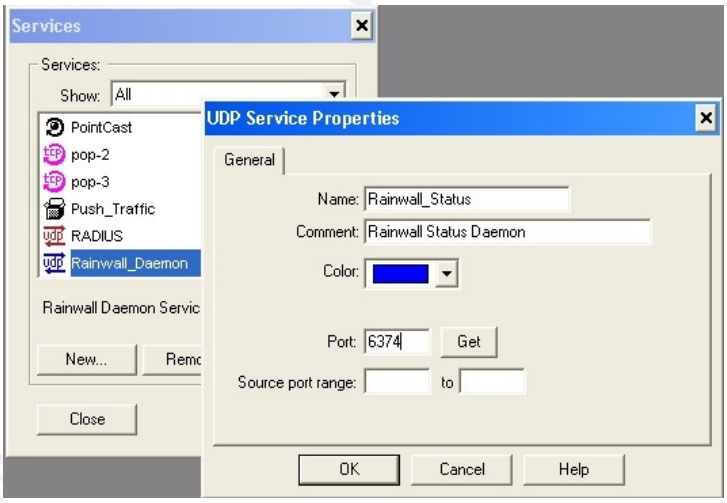
Rule two permits communication between the RainWall cluster machines. Communications run over udp/6372. Need to create the Rainwall_Daemon service. Manage=>Services=> New => UDP



Now create rule two as shown below:

2	RainwallCluster	RainwallCluster	Rainwall_Daemon	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rule permitting communication between the Rainwall cluster machines.

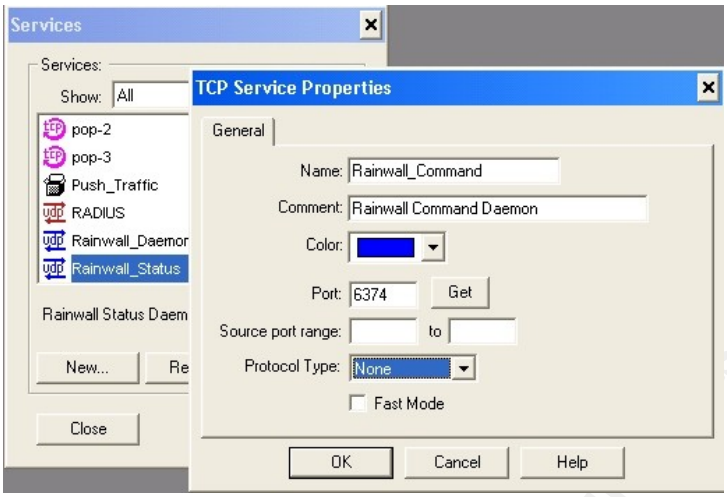
Rule three permits status communication to and from the remote management console (GUI) or from rwstat (a shell command used to collect data on Rainwall status). All status communication runs over udp/6374. Let's create the service by going to Manage=>Services=> New => UDP



Now create rule three as shown below:

3	RainwallCluster mgmt_server	RainwallCluster	Rainwall_Status	accept	Long	eFortCS_firewall1 eFortCS_firewall2	Any	Rainwall status rule to permit communication between remote Management Console.

Rule four allows the management server to monitor and control the Rainwall daemon through a graphical interface. This interface provides firewall, Virtual IP address assignment, interface load status. Through this interface, one can also stop a node, switch to other node and other administrative functions. Manage=>Services=> New => TCP



Now create rule four as shown below:

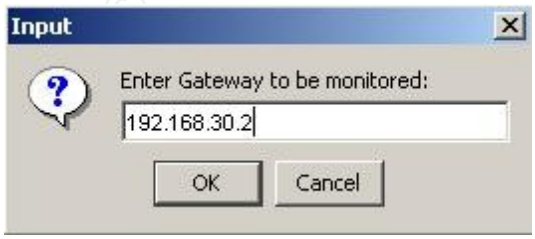
The final phase involves setting up and configuring the management GUI called Rainwall Management Console Version 1.6.0 build 17. This is a java based application so a java2 run-time environment is required. It will be run from the management server on the internal network at 192.168.30.17.

The first time the console runs, certain configuration parameters need to be set. Let's go through them.

a. The first thing that will pop up is a password dialogue box as shown below:

Enter in the same password that was created when installing Rainwall on each node. This will allow the GUI to interact with each firewall node.

b. From Edit => Add Gateway Monitor menu, add both nodes as shown below:



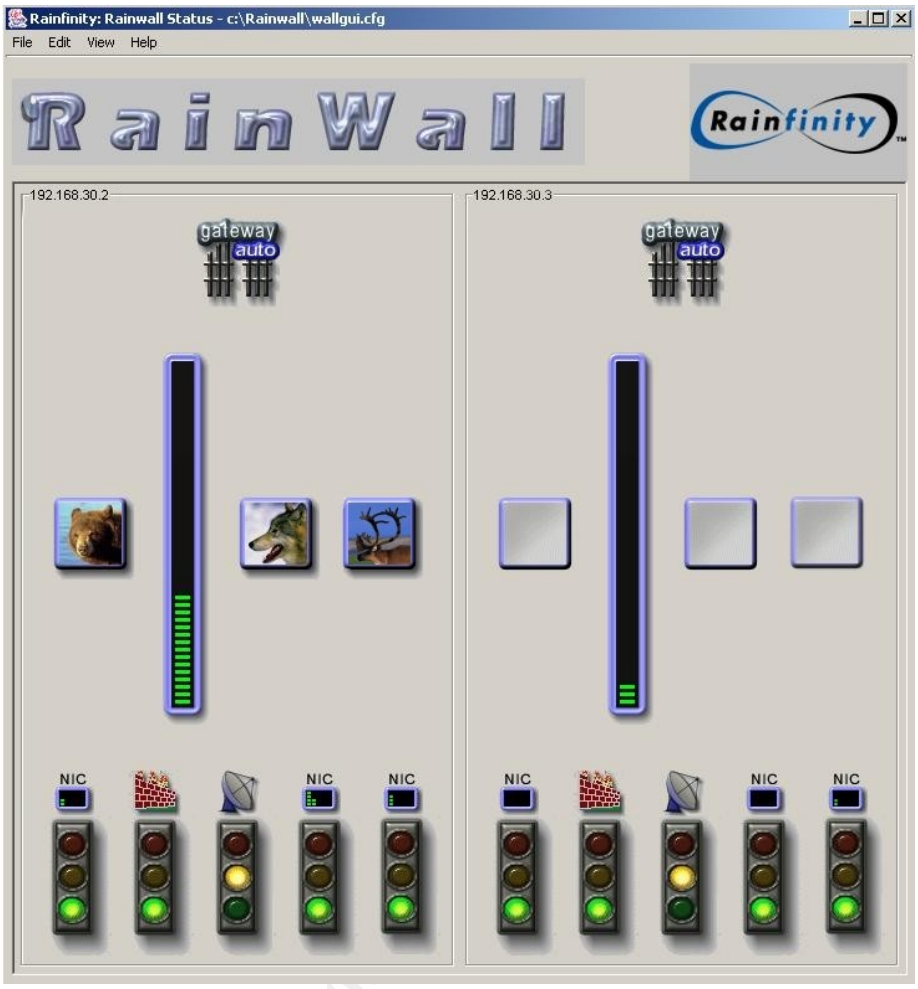
c. From the Edit => Set Number of Adapters as shown below:

Since we have external, DMZ, and internal adapters, this will satisfy our requirements.

d. From Edit => Set Size of VIP Pool as shown below:

This will allow us to see the Virtual IP assigned from the external, DMZ, and internal segments of firewall nodes.

Once the configuration changes are made, you will see a screen as shown below:



This represents all the different components of the firewall and Rainwall that the management GUI monitors. Let's break each part down. The gateway represents each node. The animal icons represent each VIP address and indicates which node is active. The other node is the hot-standby. The bear in our case is the external VIP of 209.245.30.1; the wolf is the internal VIP of 192.168.30.1 and the caribou is the DMZ VIP of 209.245.30.65. The stoplights at the bottom indicates the status of each interface and corresponds directly to the VIP above it. The firewall icon represents the health of the firewall. Green is good. The satellite icon can be configured as a ping monitor. Routers, switches, etc. can be included in a ping pool and this would show the health of the network.

The green indicator squares represent the throughput of the firewall or individual interfaces in Mbits/sec. This will be a dynamic indicator.

Finally, if one right-clicks on the gateway icon, a command menu appears as shown below.

From here one can control some functionality of the hot-standby cluster. By disabling the gateway, control immediately switches over to the other node (to include the animal icons) and this way, you can perform maintenance of a node and still have a fully functioning firewall.

More information concerning the integration of Rainwall with Check Point Firewall-1/VPN-1 software can be found at the Rainfinity web site [30].

Appendix B

Nmap Command Summary

Usage:

nmap [Scan Type(s)] [Options] <host or net list>

Scan Types:

-sT TCP connect() scan: Most common form of TCP scanning. Because it completes the full TCP handshake it is the most detectable.

-sS TCP SYN scan: Often referred to as "half-open" scanning, because this scan does not open a full TCP connection. Because this scan does not complete the TCP handshake, it is somewhat less detectable and is often referred to as a .stealth. scan. The user will need root privileges to conduct this type of scan.

-sP Ping scanning: Uses ICMP ping to detect active hosts. It does not conduct a port scan.

-sF Stealth FIN scan: Uses a bare FIN packet as the probe.

-sU UDP scan: This scan is used to determine which UDP ports are open on a host. UDP scanning can be slow due to the fact that some hosts limit the ICMP er-ror message rate.

Options:

-P0 With this option enabled, nmap will not attempt to ping the host prior to starting a scan. This is useful for scanning through firewalls that block ICMP echo re-quests.

-PT This option enables the use of TCP "ping" to determine active hosts. To set the destination port of the probe packets use **.PT <port number>**. This option is similar to the **.sP** option in determining active hosts except that it does not rely on ICMP which makes it useful for scanning through firewalls that block ICMP echo requests.

-F This option enables fast scan mode. With fast scan enabled, nmap will scan only for ports listed in the services file included with nmap.

-O This option activates remote host identification via TCP/IP fingerprinting.

-h This option displays a quick reference screen of nmap usage options.

-n/-R The option tells namp to never (**-n**) or always (**-R**) perform DNS resolution.

-v This option enables verbose mode. This mode provides additional information and can be used twice for greater effect (**-v -v)**

-oN <logfilename> Logs results of the scan in a .normal. (plain text) format to the file specified.

-oM <logfilename> Logs results of scan in a machine parsable form into the file specified.

--resume <logfilename> Resumes cancelled network scans. The log filename must be either a normal or machine parsable log from the aborted scan. Nmap will start on the machine after the last one successfully scanned in the log file.

Nmap Usage Examples:

nmap -v target.example.com

This example scans all reserved TCP ports (1-1024) on the machine target.example.com. The -v option activates verbose mode.

nmap -sS -O 192.168.10.1/24

This example launches a stealth SYN scan on all active hosts on the 192.168.10.x class 'C' network. This example will attempt to determine the operating system the scanned hosts are running. This scan will require root privileges due to the use of the SYN scan and the OS detection options.

nmap -n -v -sS -O -oN nmap-sS-O_172.30.100.20-31_230.N -oM nmap sS-O_172.30.100.20-31_230.M 172.30.100.20-31,230

A stealth SYN scan of addresses 172.30.100.20 through 172.30.100.31 plus 172.30.11.230. Verbose mode, **-v** and TCP/IP **-O** fingerprinting modes are enabled. The **-n** option configures nmap not to attempt any DNS resolution. Output will be in both human readable format (**-oN)** with filename nmap-sS-O_172.30.100.20-31_230.N and machine readable format (**-oM**) with the filename nmap-sS-O_172.30.100.20-31_230.M.