Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 1.9

GIAC Enterprise Fortunes
Spotlight on Remote Clients

Brian Stafford
7/2/03

TABLE of Contents

ABSTRACT

In the four aspects of this paper, I have attempted to build a secure perimeter network segment, with specific emphasis on the firewall and the remote users who attach to it. My attempt is to use GIAC Enterprises, Inc., a fictional company selling Cookie Fortunes, to demonstrate the perimeter security features of the network. The architecture is presented initially, followed by a tutorial in how to set up the Firewall and Remote Clients. Then an audit is done with a view to objectively analyzing the environment, looking for mistakes or weaknesses and recommending improvements. Finally, a recent GIAC practical is chosen to make an attack on. I have chosen to take a configuration involving remote access similar to my design, this to follow up on the theme of Remote Access with reference to common attacks.

1. Architecture

Overview

The diagram on page 8 will illustrate the architecture described here. GIAC Enterprises has a network with the following key aspects: (1) internal users, employees who will connect on the internal network using TCP/IP protocol to Windows 2000 Servers. They will also access the Internet through the perimeter network over a Frame Relay T1 connection provided by an ISP. (2) Remote GIAC Enterprises employees will access the internal network via a Virtual Private Network; using Checkpoint SecureClient software on company provided Laptop computers running Windows 2000, SP2. This group of remote users will include a Sales Force and Tele-workers who will use Online Data Entry, along with Support Personnel functions.

(3) Customers will access a secure Web Server residing in a Demilitarized Zone (DMZ) or Service Network on a separate interface of the external firewall as illustrated in the diagram. The Secure web server will be accessible from the internal network through an internal firewall via specific protocols. The On-line ordering software distinguishes distinct functions during the initial access to the web site. The distinction is whether the user is a Bulk-Buying partner business or individual, a first-time shopper or a user with an established user logon id. In this way we can take bulk orders on the same Web Server as regular online ordering from any shopper.

(4) Suppliers of Sayings and (5) Business partners who translate and resell, both national and international, have agreed upon requirements to use Virtual Private Networking (VPN). A secure VPN tunnel is set up between the customer's online computer and the external firewall at GIAC Enterprises. From there, based on the policy the customer is allowed to only the necessary resources.

Business Operations

1. How Internal Clients communicate to each other and the external World: Based on the illustration on pages 8 and 9, internal users or clients will connect on an internal Fast Ethernet segment, using Cisco 2900 Series switches[1], using TCP and UDP protocols. Their main connections will be to the internal Data Server, E-mail Server and SQL Database Servers (Microsoft Great Plains Solomon E-commerce for Small Business in this instance[2]). There will be automated script communication and support communication from the internal

[1] © 1992-2003 Cisco Systems, Inc. "Cisco Catalyst 2950 Series Switches" http://www.cisco.com/en/US/products/hw/switches/ps628/index.html (06/02/03)

[2] © 2003 Microsoft Corporation. "Microsoft Business Solutions Releases Solomon 5.5" (03/27/03): http://www.microsoft.com/presspass/press/2003/may03/05-27Solomon55pr.asp (06/02/03)

network to the external Firewall, Routers and DMZ. The web Servers will reside in the DMZ as shown in the illustration. The External e-mail Server and Anti-virus Server will reside on a separate DMZ on the external firewall.

The applications used for these communications will be Secure Shell, using Secure Copy and Secure FTP to move files. Also, Secure Shell will be used for management of the OS or command line access to the boxes on the external side of the Firewall. There will also be ports open for Browser applications, MS IE 5.5 SP2 will be used to and from the internal segments outgoing to the Web Server in the DMZ. Web and Proxy services will be provided in this way.

The services used will be ssh, scp, sftp, http, https, dns, MSSQL, RADIUS, IPSec, NTP, Checkpoint Management, as described below in Table 1, along with each application and protocol.

2. How Remote Tele-workers and Support Personnel Communicate:
Remote users will also use the Browser interface to place orders on line and will use Check Point SecureClient software[3] to initiate a VPN tunnel to the firewall. They will authenticate to the internal RADIUS Server[4], and attach to the network, thereby gaining access to a defined set of internal resources in order to do their work, such as file sharing and e-mail, browsing and Database work. They will use IKE/ISAKMP over TCP protocol to communicate and encrypt, while having their remote machines locked down by a personal firewall policy issued by the firewall upon connection. The applications used will be the same as above in that all functionality will be available as if on the internal network. The services will be the same also, with the exception that all communication will be encrypted in an IPSEC tunnel.

3. How Business Partners connect to Supply Sayings and Fulfill Orders, Translate and Resell our product:
Business Partners connect to the same front end Firewall as Customers but use SecureClient VPN and are challenged to log in as an authorized Vendor, at which point they must log in and authenticate with RADIUS and must use HTTPS with 128 bit encryption to our Vendor access. There they are allowed to view supply information for their orders and update Status and review invoices, but not change invoices. In this case, the protocol is TCP, the application being any compatible browser and the service HTTPS. Their access is limited to the DMZ where Partner information will also reside by way of Microsoft SQL replication of specific database information.

4. How Back End communication between DMZs and the internal network is handled:

---

[3] © *Check Point Software Technologies Ltd.* "VPN-1 SecuRemote & VPN-1 SecureClient" http://www.checkpoint.com/products/protect/vpn-1_srsc.html (6/02/03)
[4] © 2003 Vircom inc. "VOPRADIUS Server" http://www.vircom.com/Enterprise/Solutions/VOPradius/ (6/02/03)

The internal SQL Databases and E-Commerce application are housed internally and communicate using TCP protocol and MSSQL service for the purpose of using the Solomon E-commerce application. The application is based on Microsoft's SQL Server 7.0 Architecture, in order to process orders between the DMZ and the internal SQL databases. The internal Servers use RAID level 5 and are fail over Servers for redundancy.

5. How E-mail, Anti-Virus and Proxy Serving is handled for Internet traffic:
One Separate DMZ contains External E-Mail, Anti-virus and Proxy Web-Browsing services. The applications used are Microsoft Exchange Server[5], Trend Micro Anti-Virus Server[6] and Microsoft ISA Server Standard Edition[7]. These serve as a gateway before e-mail or browsing is delivered to the internal users. The Services are smtp, http, https, ftp and the Protocols are TCP, UDP and ESP. The Firewall is integrated using CVP with the Anti-Virus Server to scan the servers on the Web DMZ also. Internally, Norton Anti-virus definitions and scanning engines are installed on internal machines, updated by login scripts. Services and Protocols used for Applications:

Name	Protocol	Port	Application Usage
CPD	TCP	18191	Check Point Daemon Protocol
CPD-amon	TCP	18192	Check Point Application Monitoring
CPMI	TCP	18190	Check Point Management Interface
FW1	TCP	256	Check Point VPN-1 & FireWall-1Service
FW1-key	TCP	265	Check Point VPN-1 Public Key Transfer Protocol
FW1-ica-pull	TCP	18210	Check Point Internal CA Pull Certificate Service
FW1-ica-push	TCP	18211	Check Point Internal CA Push Certificate Service
FW1-log	TCP	257	Check Point VPN-1 & FireWall-1 Logs
FW1-pol-logon	TCP	18207	Policy server logon
FW1-pol-logon	TCP	18231	Policy server logon
FW1-topol	TCP	264	Topology Download
IKE	UDP	500	IPSEC Internet Key Exchange Protocol
IKE-tcp	TCP	500	IPSEC Internet Key Exchange Protocol
AH	51	N/A	Auth. Header Protocol for IPSEC
ESP	ESP	NA	Encapsul. Security Payload: for IPSec

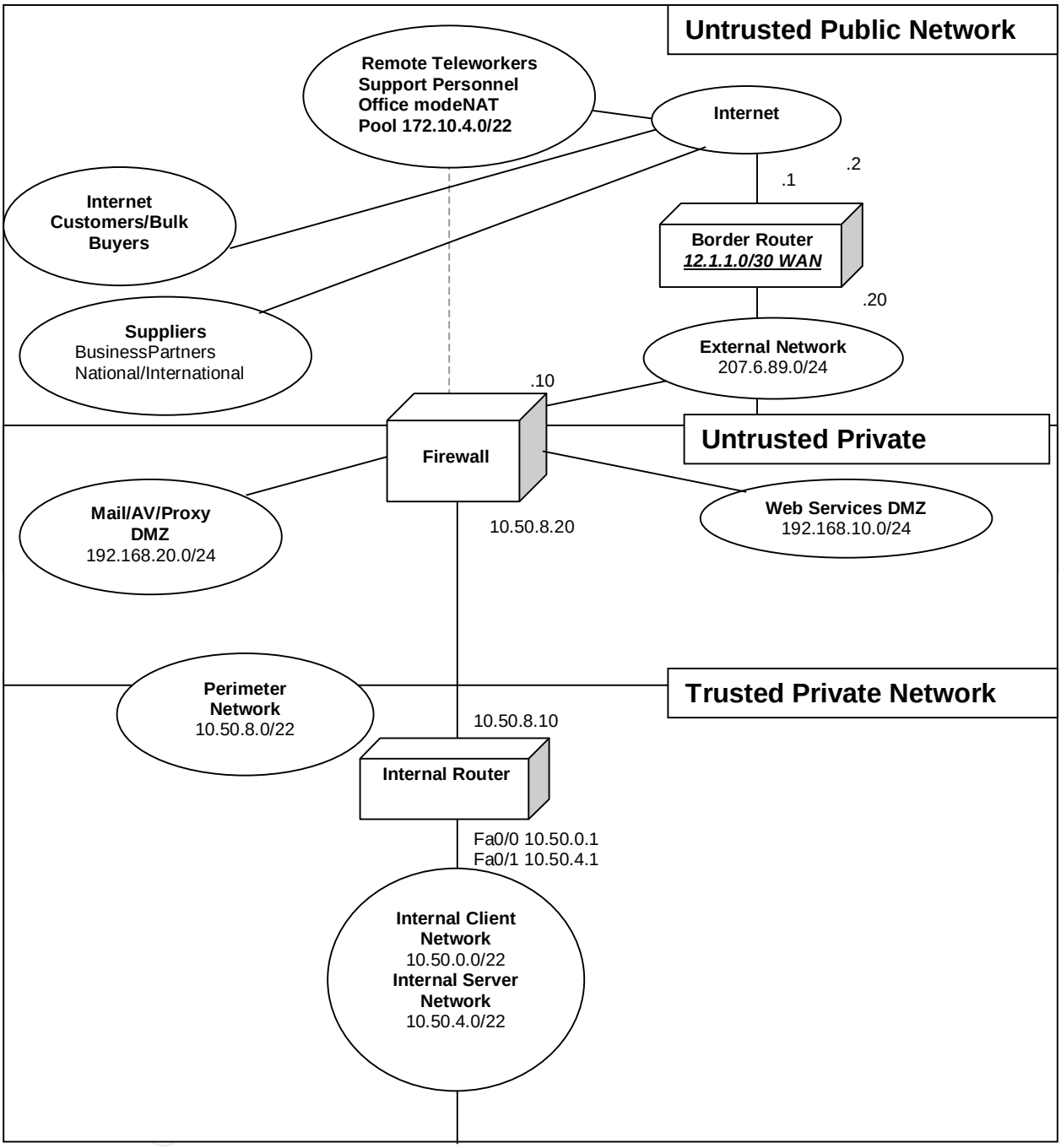
[5] **© 2003 Microsoft Corporation.** "Exchange 2000 Product Overview" (12/16/02) http://www.microsoft.com/exchange/evaluation/overview/default.asp (06/02/03)
[6] Copyright 1989-2003 Trend Micro, Inc. "InterScan VirusWall" http://www.trendmicro.com/en/products/gateway/isvw/evaluate/overview.htm (06/02/03)
[7] © 2003 Microsoft Corporation**.** "Choose Your Edition" (May 2001) http://www.microsoft.com/isaserver/howtobuy/choosing/default.asp (06/02/03)

IPSEC_encaps	UDP	2746	SecureClient IPSEC port
Tunnel-test	UDP	18234	VPN tunnel initiation check (Checkpoint)
HTTP	TCP	80	HTTP protocol
HTTPS	TCP	443	HTTP protocol over TLS/SSL
NTP-UDP	UDP	123	Network Time Protocol
Scp	TCP	21	Secure Copy Application
Sftp	TCP	21	Secure FTP Application
SSH	TCP	22	Secure Shell
RADIUS	UDP	1645	RADIUS Protocol
RADIUS-Acct	UDP	1646	RADIUS Accounting Info.
MSSQL	UDP	1433/34	Sql from internal Servers to access DMZ
Domain-tcp	TCP	53	Domain name system download
Domain-udp	UDP	53	Domain name system queries
NTP_TCP	TCP	123	Network Time Protocol

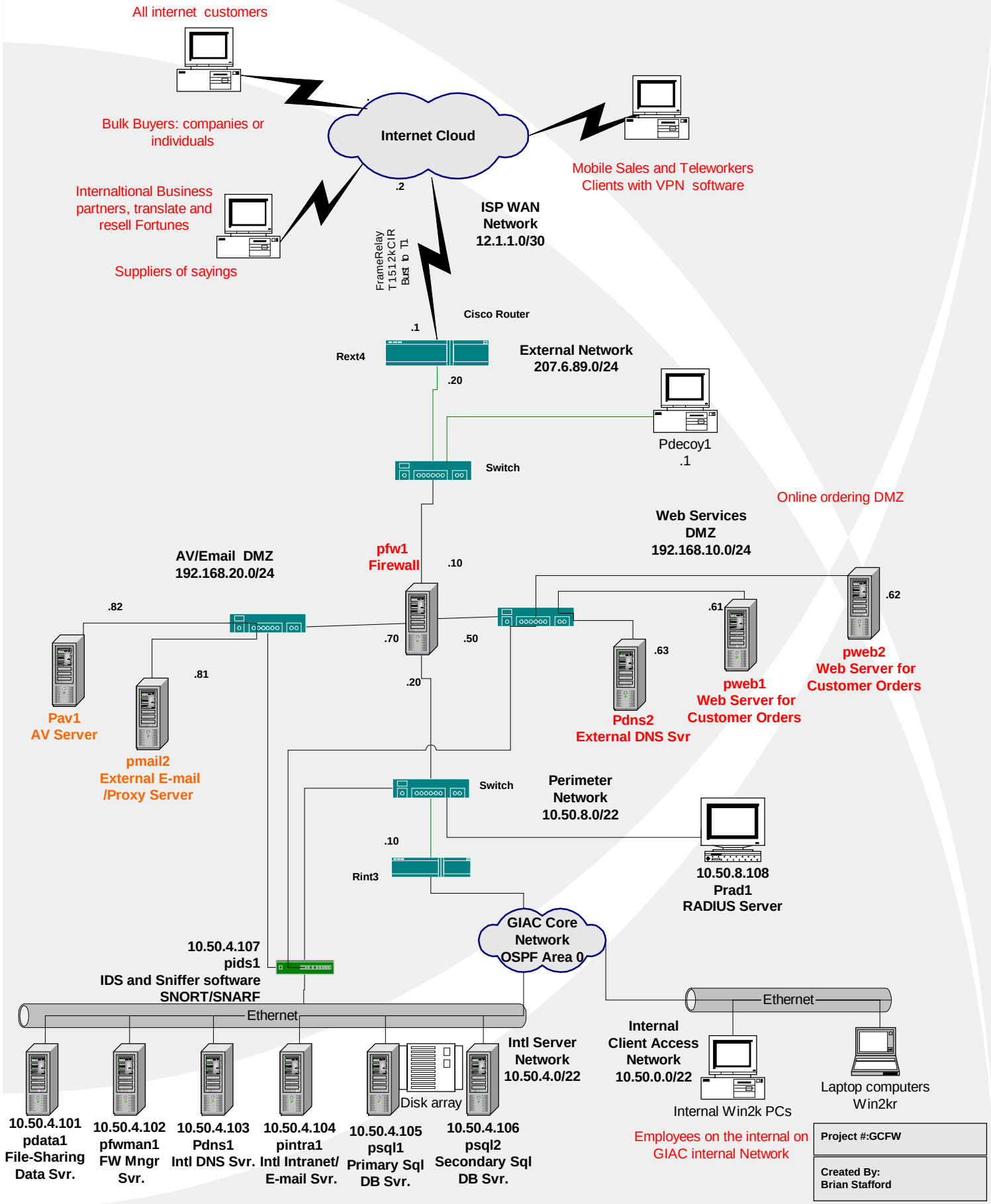
The above port number references are taken mostly from a public site, www.phoneboy.com[8], as well as many hours of personal experience on router logs and access lists and with Check Point documentation and support.

[8] *dwelchATphoneboyDOTcom.* "Issues pertaining to SecuRemote and Secure Client, Check Point's VPN client for Windows, Linux, MacOS, and others." 11/08/02 http://www.phoneboy.com/fom-serve/cache/13.html (06/03/03)

Logical Diagram:



Enterprises Network Architecture



2. Policy

Introduction to the Security Policy:

The security is enforced in four main places. Firstly, the configuration of the Border or External router, using an Access control List along with various hardening of the Cisco IOS. Secondly, a firewall permitting only specified traffic, which is running Checkpoint NG FP2 on Solaris 2.8. Thirdly, SNORT 2.0[9] will be operating primarily as an IDS system on segments of the network, with the potential to be used as a Sniffer at short notice. Fixes for recent vulnerabilities will be applied. Fourthly, authentication is required before use of resources, RADIUS is the chosen method and uses three pieces of information: User ID and PIN followed by a unique password for each use. In outlining the configurations and Policy Rules, I will refer to the Logical Diagram and Network Diagram on pages 8 and 9 above in order to reference addressing and devices. For clarity, a brief explanation of what is achieved by each entry in the security policy will be included after each entry. As a minor point, we have a decoy Linux P133 box with a generic Web Server running which we access physically to pull logs and look at activity. This provides some information on the threat volumes and types.

Router Hardening Commands and Interface Configuration

The following hardening commands are based on NSA recommendations[10], which will be deployed in general on the internal and border routers.

Below are some hardening commands on the External or Border router, Prtext1 in our diagram. There is a Brief Explanation of important NSA recommended commands in Parentheses with disguised password encryption and addressing etc:

Enable secret 5 $1jtripweoirjijgijwgtijr	(Password into non-reversible cryptographic function)
Service Password-Encryption	(Encrypts passwords, including varying user level Passwords)
Ip subnet-zero	(Allows use of entire subnet, including zero, for IP addressing)
no ip source-route	(Disable forcing a packet to take a specific route through the network)
no ip cef	(Disable Cisco Express Forwarding information to line cards)

logging buffered 3296000 debugging
no logging rate-limit
no logging console

[9] Brian Caswell and Marty Roesch "What is SNORT?" 6/4/03 http://www.snort.org/about.html (06/04/03)
[10] National Security Agency. "Router Security configuration Guide" 9/27/02 Version 1.1 http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (06/02/03)

```
no logging monitor
clock timezone EST -5
clock summer-time EST recurring
no ip bootp server
no ip domain lookup              (Control domain lookups on the network)
ip domain name giac.com
ip name-server 192.168.10.63
no ip directed-broadcast         (Disallow sending ip datagrams to the broadcast
                                  address of a  subnet to which the sending
                                  machine is not directly attached, then as
                                  unicast to destination subnet, then as link-layer
                                  broadcast, causing possible DOS attack)
no ip finger                     (Disallow inquiries as to who is logged in)

interface FastEthernet0/0
 ip address 207.6.89.10 255.255.255.0
 no ip route-cache               (Disables fast-switching of IP Unicast, allow
                                                debug messages)
 no ip mroute-cache              (Disables fast-switching of IP Multicast, allow
                                                debug messages)
 duplex full
no ip redirects                  (Disables directing of a node to use a specific
                                                router in it's path)
no cdp enable                    (Disable Cisco discovery protocol giving info. about
                                                other Ciscos on net)
no ip proxy-arp                  (Disables Router sending it's own ARP Request using
                                                it's own MAC)

interface serial0//0
 description ISP Internet Connection
 bandwidth 1536
 ip address 12.1.1.1 255.255.255.252
 ip access-group 106 in          (Referred to next section on ACLs)
 ip access-group 105 out         (Referred to next section on ACLs)
 encapsulation ppp
 no ip mroute-cache
 serial restart_delay 0
no ip redirects
 no cdp enable
no ip proxy-arp
!
router ospf 1
 log-adjacency-changes
 redistribute static subnets
 passive-interface FastEthernet0/0
 passive-interface serial0/0
```

```
 network 12.1.1.0 0.0.0.3 area 0
 network 207.6.89.0 0.0.0.255 area 0
 default-information originate     (Causes default route to be redistributed
                                                    into OSPF)
!
router bgp 12345              (Unique Autonomous ID for exterior gateway protocol)
 no synchronization
 bgp log-neighbor-changes
 network 207.6.89.0
 neighbor 12.1.1.2 remote-as 7018          (EBGP Neighbor)
 neighbor 12.1.1.2  description ISP access router
 neighbor 12.1.1.2 distribute-list 1 in
 neighbor 12.1.1.2 route-map ANYWORD out
 no auto-summary                    (Disables auto network number summary of
                                                    IGP into BGP)
!
ip classless                    (Uses best match route regardless of Class of
                                                    Destination Address)
ip route 192.168.20.0 255.255.255.0 207.6.89.10
ip route 192.168.10.0 255.255.255.0 207.6.89.10
no ip http server                    (Disables configuration by web browser)
no cdp run
banner motd ^C          (Acknowledges legal warnings visible to users  upon login)
This system is private property.
Unauthorized attempts to modify this system is unlawful,
It is our policy to prosecute.
^C
!
line con 0
 password 7 27839742738402834729347248 27
line aux 0
 password 7 23746702783467028402348232 34
line vty 0 4
 access-class 52 in
 password 7 15624951695814192354192735464
 transport input ssh
!
ntp clock-period 17178188
ntp server 128.4.40.12
ntp server 208.21.108.186
```

Router Access Lists

ACL (Access Control)
Access control is implemented on both the external and access routers to only permit required protocols access to the external firewall. The goal is to permit only specific traffic through the router to the external interface of the firewall and have the firewall process and verify traffic to it's ultimate destination. We will use allow HTTP, HTTPS, SMTP to the relevant DMZ coming in and out. Also, UDP is being used as the transport protocol for IKE, topology updates and policy server logons. This is required to support VPN Secure connections from Internet connections behind address-translated routers or firewalls.

```
access-list 105 permit udp host  128.4.40.12 any eq ntp
access-list 105 permit udp host  208.21.108.186 any eq ntp
access-list 105 permit tcp 207.6.89.0 0.0.0.255 any established
access-list 105 permit tcp 207.6.89.0 0.0.0.255 any eq www
access-list 105 permit tcp 207.6.89.0 0.0.0.255 any eq 443
access-list 105 permit tcp 207.6.89.0 0.0.0.255 any eq smtp
access-list 105 permit tcp 207.6.89.0 0.0.0.255 any eq ftp
access-list 105 permit udp 207.6.89.0 0.0.0.255 any eq domain
access-list 105 permit tcp 207.6.89.0 0.0.0.255 any eq domain
access-list 105 permit udp 207.6.89.0 0.0.0.255 eq domain any
access-list 105 permit tcp host 207.6.89.10 any established
access-list 105 permit udp host 207.6.89.10 any eq isakmp
access-list 105 permit udp host 207.6.89.10 any gt 1053
access-list 105 permit esp host 207.6.89.10 any
access-list 105 permit icmp any any
access-list 105 deny   ip any any log
access-list 105 remark Out to serial to ISP
access-list 106 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 106 deny   ip 172.0.0.0 0.255.255.255 any log
access-list 106 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 106 deny   icmp any any redirect
access-list 106 deny   icmp any any alternate-address
access-list 106 deny   icmp any any router-solicitation
access-list 106 deny   icmp any any router-advertisement
access-list 106 permit icmp host 12.1.1.2 any
access-list 106 deny   icmp any any
access-list 106 permit udp host 128.4.40.12 eq ntp host 12.1.1.2
access-list 106 permit udp host 208.21.108.186 eq ntp host 12.1.1.2
access-list 106 deny   ip any host 12.1.1.2 log
access-list 106 deny   ip any 192.168.20.0 0.0.0.255 log
access-list 106 deny   ip any 192.168.10.0 0.0.0.255 log
```

```
access-list 106 permit tcp 207.6.89.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 22
access-list 106 permit udp 207.6.89.0 0.0.0.255 192.168.20.0 0.0.255 eq 53
access-list 106 permit tcp any 207.6.89.0 0.0.0.255 established
access-list 106 permit tcp any 207.6.89.0 0.0.0.255 eq www
access-list 106 permit tcp any 207.6.89.0 0.0.0.255 eq 443
access-list 106 permit tcp any 207.6.89.0 0.0.0.255 eq smtp
access-list 106 permit tcp any eq ftp-data 207.6.89.0 0.0.0.255 gt 1053
access-list 106 permit udp any 207.6.89.0 0.0.0.255 eq domain
access-list 106 permit udp any eq domain 207.6.89.0 0.0.0.255 gt 1053
access-list 106 permit tcp any host 207.6.89.10 established
access-list 106 permit tcp any host 207.6.89.10 eq 264
access-list 106 permit udp any host 207.6.89.10 eq isakmp
access-list 106 permit udp any host 207.6.89.10 gt 1053
access-list 106 permit esp any host 207.6.89.10
access-list 106 deny   ip any any log
```

Firewall Security Layer and Tutorial

In Table 1 we will create the objects for inclusion in the Rule Base Policy. Most significantly the Firewall Gateway object itself has many of the configuration options we are interested in from the VPN and Firewall Policy Server perspective. We need to set up the firewall as a Gateway or Enforcement point, as well as a Policy Server for Client Access. During set up of the firewall object the following are some aspects of our configuration:

Authentication

User authentication is controlled by the VPN gateway. Only Tele-Workers and support personnel who have been authorized for remote access and issued RADIUS Password lists and PINS will be able to access the VPN. SecureClient prompts users for their 4 digit PIN, followed by a semi-colon and a one-time password. The external VPN firewall is configured to point to a RADIUS Server and allows or denies access based on the RADIUS Server response.

Encryption Scheme

An encryption scheme includes a key management protocol, an encryption algorithm and an authentication algorithm. IKE/ISAKMP will be the encryption scheme for GIAC VPN. Hybrid IKE will permit the use of a one-time RADIUS password instead of a certificate authority.

IKE is an industry standard protocol for VPN key management. It is used to negotiate Security Associations (keys) between two hosts. GIAC will be using Hybrid IKE, which does not require the initial sharing of Private/Public keys certificates or shared secret passwords.

IKE HMAC improves authentication security. The external firewall will support either HMAC-MD5 or HMAC-SHA-1 to ensure compatibility with SecureClient and vendor-to-vendor VPNs. SecureClient has been configured with HMAC-MD5 as the authentication algorithm to provide a high-level of security and performance.

SecureClient supports AES-128, AES-256, 3DES, DES and CAST as encryption algorithms. AES and 3DES encryption algorithms are enabled on the external firewall to enable proper encryption security for SecureClient and vendor-to-vendor VPNs. Office Mode is a Check Point feature which will allow us to create a network and translate the clients so that they are, virtually, a part of the internal network, getting routing information, DNS and WINS info for example as we will see below. The Principle is that we provide a NAT IP pool of addresses for the clients. In fact, the client has a virtual Ethernet device for this when connected.

Properties of the external firewall

On the NAT tab of the firewall properties we will select the option to "Use IP Pool "NAT" for SecuRemote/SecureClient" and select our IP NAT pool address network object from the Table 1 below. In the "Return unused addresses to IP Pool after:" box we select and extended day, such as 14 hours, and put in 840 in minutes.

On the "Topology" tab we have identified out internal, external and DMZ interfaces with addresses and subnet masks, and manually defined our encryption domain object as "VPN-Domain-GIAC" per Table 1 also.

On the "VPN" tab we check the IKE box and select "edit" to define IKE properties and advance IKE properties. With IKE properties we select 3DES and AES-256 to support both with key exchange encryption, also selecting "Public Key Signatures" and "VPN-1 & firewall-1 authentication for "SecureRemote/SecureClient (Hybrid Mode)". In the Advanced IKE properties we select UDP encapsulation and select the "VPN1_IPSEC_encapsulation" in the drop-down box. We also select "Group 2(1024 bit) Diffie-Hellman IKE phase 1. We will not select "support aggressive mode" in the "misc" area due to recent vulnerabilities.

On the "Remote Access" tab we select "Offer Office Mode to group" and select manual office mode method using the drop-down box to again select the network object name of our office mode pool of addresses. We also give an IP lease duration, such as 840 minutes in this case. In the "Optional Parameters" section we add the devices for DNS and WINS which we want Office Mode to dish out to the VPN clients after they connect, authenticate and get a topology download.

On the "Authentication" tab we select "RADIUS" to enable that authentication scheme, we give a user session timeout of 840 minutes, again to allow for someone using the client to work all day. We indicate how we want alerts in the drop-down box and select "Popup Alert". Finally we choose the group of users associated with the Policy Server, a drop-down box in which we select "iVPN".

On the "Logs and Masters" tab we identify Pfwman1, selecting the "Define Log Servers" button. On the "General Properties" tab we should see the IP address of the Gateway, with the version of Checkpoint and the modules installed, a check mark being on "Firewall-1", "VPN-1 Pro" and "SecureClient Policy Server". We will also see the Secure Internal Communication tab here with a DN reference.

Global Properties defined on the Firewall Manager

On the "NAT" tab of the Global Properties we have some selections in which we will check the "Enable IP Pool NAT for SecuRemote/SecureClient and gateway

connections. We will also check boxes for “Automatic ARP configuration”, “Translate destination on the client side” and “Allow bi-directional NAT”.

On “Remote Access” tab there are some topology update options where we will check “automatic update”. Also, there is an authentication validation timeout, which we will set pretty high again since we are using RADIUS one-time passwords and we want people to be able to work for long periods. We will not need to bother with Policy Server High-Availability but will want to check the “Enable Back Connections from Gateway to Client” so applications will work for the client.

On the “VPN” tab under Remote Access we select “Enable Office Mode”, the encryption algorithm of “AES-128” and data integrity of “SHA1”. We select the box “Force Encryption Algorithm and Data Integrity on all users”. For IKE advanced properties we select DH “Group 2” to tie back with our previous settings. We can also select that “Gateways support IKE over TCP”.

On the “Secure Configuration Verification” Tab under Remote Access we select the boxes that says, “Policy is installed on all interfaces” (ensuring the client is protected) and also, “generate log on client”, to help with troubleshooting clients.

On the “Stateful Inspection” tab, there are several timeout options and for TCP, ICMP and other IP protocols. We will keep the defaults there but check the box “Accept Stateful UDP replies for unknown services” to help with some applications which use high UDP ports to respond on.

We will use the following reference tables for the Tutorial:

In Table 1 we will create the objects for inclusion in the Rule Base Policy. Most significantly the Firewall Gateway object itself has many of the configuration options we are interested in from the VPN and Firewall Policy Server perspective.

Firewall Objects Created on Pfwman1 for use with Policy installed on Pfw1

Table 1

Name	Type	IP Address	Comment
Pfw1	Host	207.6.89.10	Ext. Interface of Firewall
Pfw1-Int	Host	10.50.8.20	Int. Interface on Firewall
Pfw1-webdmz	Host	192.168.10.50	Web DMZ Interface on Fw
Pfw1-emaildmz	Host	192.168.20.70	Email DMZ Interface of Fw
Pfwman1	Host	10.50.4.102	Firewall Manager
Pweb1	Host	192.168.10.61	Primary Web Server
Pweb2	Host	192.168.10.62	Secondary Web Server
Pdns1	Host	10.50.4.103	Internal DNS
Pdns2	Host	192.168.10.63	External DNS

Psql1	Host	10.50.4.105	Primary SQL DB Svr.
Psql2	Host	10.50.4.106	Secondary SQL DB Svr.
NTP-Server1	Host	128.4.40.12	Primary Time-Server
NTP-Server2	Host	208.21.108.186	Secondary Time-server
Prad1	Host	10.50.8.108	RADIUS Server
Int-Net	Net	10.50.0.0/22	Internal Network
Int-Data-Net	Net	10.50.4.0/22	Internal Data Center Net.
Perimeter-Net	Net	10.50.8.0/22	Perimeter Network
Ext-Net	Net	207.6.89.0/24	External Network
Web-DMZ-Net	Net	192.168.10.0/24	Web DMZ
Email-DMZ-Net	Net	192.168.20.0/24	Email DMZ
VPN-Domain-GIAC	Group	Int-Net, Int-Data-Net, Perimeter-Net	Contents of Encryption Domain
Office-Mode-IP-NAT-Pool	Net	172.10.4.0/22	IP NAT pool for Office Mode Clients

Desktop Policy pushed to the clients upon authentication

In Table 2 the principles at stake are a) the requirement for encrypted communication to the network and b) the requirement that as soon as the machine is connected to the corporate network and has established a Secure VPN tunnel, no other connections can be made to the Client.

The first inbound rule ensures that only encrypted traffic is allowed to the machine. The second rule denies connections to the machine to prevent hijacking of sessions or other secondary interface connections to the machine while connected. Tip: It is important to bind to all adapters during the installation of the client so that the machine is only deemed securely connected when all interfaces are accounted for during the establishment of the VPN. Although the third rule looks strange, it actually only applies a default condition when the machine does not have a VPN established and is therefore allowed to connect to other devices. One can restrict the activities of those in default mode also, if you want to control the Client when not connected. The complication here is that we would then have to disallow the client from having rights to stop the Client Software. We are then into the area of Client or user rights on the local machine.

The first outbound rule forces encryption from the Client to the Corporate Network. The second Blocks other traffic. The third permits access when not connected via VPN and is the Default mode for a machine not connected. The same area of discussion is open for this as in rule 3 of the inbound traffic.

Table 2

#	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
INBOUND RULES						
1	VPN-Domain-GIAC	iVPN@Any	* Any	Encrypt	Log	Encrypt from GIAC networks to desktops when connected to VPN.
2	* Any	iVPN@Any	* Any	Block	Log	Deny access from other networks to desktops when connected to VPN.
3	* Any	All_Users@Any	* Any	Accept	Log	Permit all access to desktops when not connected to GIAC VPN. Default rule.
OUTBOUND RULES						
4	iVPN@Any	* Any	* Any	Encrypt	Log	Encrypt from desktops to GIAC when connected to GIAC VPN.
5	iVPN@Any	* Any	* Any	Block	Log	Deny access to other networks from desktops when connected to GIAC
6	All_Users@Any	* Any	* Any	Accept	Log	See rule 3

User Setup

In Table three is an example of how to set up users and the options available based on our configuration.

Table 3

User	username
Authentication	RADIUS
Groups	iVPN
Expiration	31-dec-2005
Location	Source = Any Destination = Any
Time	All
Certificates	none
Encryption	IKE Encryption + Data Integrity(ESP)
Data Integrity	MD5
Encryption Algorithm	3DES

Rule Base on pfw1 (Firewall)

Table 4

In table 4 we address the most used rules first because the processing of rules begins with the properties, commonly called Rule 0, and then goes through the rules sequentially.

Table 4

#	SOURCE	DESTINATION	SERVICE	ACTION	Purpose
1	Ext-Net	Pweb1 Pweb2	https http	Accept	Allow web traffic to the Web servers
2	* Any	Pfw1	FW1_secureclient	Accept	Permit IKE key negotiation and Policy Server logon
3	IVPN@Any	VPN-Domain-GIAC	* Any	Client Encrypt	Encrypt all traffic from External VPN Domain
	Pav1	Pweb1,Pweb2	AV_SVC	Accept	AV Scanning
4	Ext-Net	Pav1 Pemail1	Smtp AV_Prot	Accept	Allow mail traffic to the external mail DMZ
5	Pdns1	Pdns2	domain-udp	Accept	Allow domain traffic to the dns servers
6	Pfwman1	Pfw1	CP Mgmt Svc Group ssh	Accept	Permit comm. And ssh between manager/log station and firewall.
7	Pfw1	NTP-Server1 NTP-Server2	NTP-UDP	Accept	Network Time Protocol for clock synchronization
8	Int-Net	Pweb1 Pweb2	MSSql	Accept	Allow sql traffic from the internal network to the Web DMZ
9	Pfw1	Prad1	RADIUS	Accept	Permit RADIUS Auth.
10					
11	* Any	* Any	* Any	Drop	Cleanup rule

SNORT Sniffer/IDS Layer

SNORT 2.0.3 Release with fixes applied will run as our primary Intrusion Detection System. As of 6/4/03 there are still CERT[11] alerts being sent about the preprocessor vulnerabilities, which affect heap overflow in the product. It will run on a hardened Windows 2000 Professional machine and be internally connected to the internal network segment as show in the diagram. The monitor probes will be connected to the Web Server DMZ, the external segment and the internal

[11]"CERT® Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors", 4/23/03 http://www.cert.org/summary/ (06/04/03)

segment. The normal operation will be in IDS mode but a configuration will be available for running the Sniffer mode as a cost savings option. For example, if alerts or other IDS rules are triggered, administrative staff can use the alert information to run the Sniffer looking at specific real-time activity. Jon Bull[12] suggests the following hardening tips for Windows 2000 machines in his Snort.org article.

* Uninstall IIS 5.0
* Strengthen you administrator accounts password
* Rename your administrator account
* Update to the latest service pack
* Apply "Hot Fixes" that deal with malformed packets
* Disable the services you aren't going to need

Due to cost restrictions for IDS we will run freeware SNORT as referenced above and IDSManager Pro[13], also for cost reasons, (http://www.activeworx.com), to allow us to run snort on multiple interfaces. This is not ideal in that some aspects of this require manual manipulation of files but we chose to spend most of our money on Firewall and client VPN licensing. Snort rules will send an alert to the Firewall Manager, which in turn has alerts enabled in the Data center, an audio beep and a text message on screen. Unfortunately, multiple instances of Snort must be running to monitor multiple interfaces due to constraints in the software. Some Linux versions do not require this. The latter is the reason we need IDSManager Pro, along with the ease of management it provides in the GUI. It manages SNORT IDS sensors in a distributed environment and allows ease of use in taking text configurations and rule files.

IDS Policy Manager was written to manage Snort IDS sensors in a distributed environment. This has the added ability to merge new rule sets, manage pre/post processors and scp rules to sensors.

The command to run SNORT and give instructions on where to log and where to find the rules is as follows:

c:\snort\bin\Snort -d -i <eth1> -l c:\snort\log -b –c c:\snort\etc\snort.conf

-log is the locations of the log file, the Default being ASCII format
-snort.conf[14] is the rules file (updated using current releases from snort.org
-d display packet data as well as well as header information (no -e option

[12] Bull, Jon. "Snort's Place in a Windows 2000 Environment" 4/15/02 http://snort.org/docs/snort-win2k.htm (06/05/03)

[13] Activeworx. "IDS Policy Manager Version 1.3.1 for Windows 2000/XP" 06/05/03 http://www.activeworx.com/ (06/05/03)

[14] Caswell, Brian and Roesch, Marty "Snort Signature Database" 06/05/03 http://www.snort.org/cgi-bin/needed.cgi (06/05/03)

for Data Link Layer headers)
-h precedes the home network indicating to SNORT what is internal
-I indicates the interface to use and is relevant to the use of multiple interfaces on win2k machines
-b using this we log everything to a binary file for later analysis
-r will replay from binary format to more normal tcpdump format

Here are some excerpts with annotations from the sample snort.conf. file available at http://public.lanl.gov/cpw/snort.conf.html [15] as referenced below:

```
##################################################
# Standard format
#  1) Set the network variables for your network
#  2) Configure preprocessors
#  3) Configure output plugins
#  4) Customize your rule set
##################################################
# Step #1: Set the network variables:
# You must change the following variables to reflect your local network
# You can specify it explicitly as:
#
# var HOME_NET 10.1.1.0/24
#
# or use global variable $<interfacename>_ADDRESS
# which will be always initialized to IP address and
# netmask of the network interface which you run
# snort at.  Under Windows, this must be specified
# as $(<interfacename>_ADDRESS), such as:
# $(\Device\Packet_{12345678-90AB-CDEF-1234567890AB}_ADDRESS)
#
# var HOME_NET $eth0_ADDRESS
#
# You can specify lists of IP addresses for HOME_NET
# by separating the IPs with commas like this:
#
# var HOME_NET [10.1.1.0/24,192.168.1.0/24]
# or you can specify the variable to be any IP address
# like this:

var HOME_NET any…….”

“# Step #2: Configure preprocessors
#
# General configuration for preprocessors is of
```

[15] Green, Chris. “snort.conf, v.110” 08/14/02
http://public.lanl.gov/cpw/snort.conf.html (06/05/03)

```
# the form
# preprocessor <name_of_processor>: <configuration_options>……"
preprocessor frag2

"# Step #3: Configure output plugins
#
# output <name_of_plugin>: <configuration_options>
# [Win32 can use any of these formats...]
# output alert_syslog: LOG_AUTH LOG_ALERT
# output alert_syslog: host=hostname, LOG_AUTH LOG_ALERT
# output alert_syslog: host=hostname:port, LOG_AUTH LOG_ALERT
#
include classification.config
#
# Include reference systems
include reference.config

# Step #4: Customize your rule set
#
# The rules included with this distribution generate alerts based on
# on suspicious activity. Depending on your network environment, your
# security policies, and what you consider to be suspicious
include c:\snort\bad-traffic.rules
include c:\snort\exploit.rules
include c:\snort\scan.rules
include c:\snort\finger.rules
include c:\snort\ftp.rules
include c:\snort\telnet.rules
include c:\snort\rpc.rules
include c:\snort\rservices.rules
include c:\snort\dos.rules
include c:\snort\ddos.rules
include c:\snort\dns.rules
include c:\snort\tftp.rules
include c:\snort\web-cgi.rules
include c:\snort\web-coldfusion.rules
include c:\snort\web-iis.rules
include c:\snort\web-frontpage.rules
include c:\snort\web-misc.rules
include c:\snort\web-client.rules
include c:\snort\web-php.rules
include c:\snort\sql.rules….."
```

3. Verify Firewall Policy

Audit Plan

An external resource was used to do the audit in order to give an objective flavor to the assessment. The technical approach will be as follows:

1. Scan for open ports from the external side of the router and Firewall to verify that External Router and Firewall policies are, in fact, applied.
2. Look at logs on the firewall to ensure that Accepts, encrypts, decrypts, drops and rejects are logged correctly based on the port scan and that the rule number corresponds to the expected action of the rule. Ensure that the Firewall is not receiving packets that should be blocked at the external router.
3. Ensure that authentication is using the one-time RADIUS mechanism by trying the same password twice in a row and ensure that authenticated client traffic is encrypted as the rule requires. Ensure Desktop Policy is in effect by attempting to connect to another interface on the Client while it is connected to the GIAC VPN network.

Costs and Level of Effort

The time of the audit and the shift on which it takes place are important since we could impede the Server's functions. We have assessed our least busy time and maintenance window to be Friday night and early Saturday morning. We would like to spend 12 hours verifying the configuration and are using 8pm Friday night to 8am Saturday morning. The external contractor has given us a 6-hour time-frame for preparing the audit and the tools as well as 16 hours to prepare analysis and reports. We estimate 40 hours of work afterwards for our staff to pursue the recommendations. We have emphasized that the objective is not a vulnerability assessment but is a verification that the Firewall Rules are operational.

Demonstrate Audit using Tools and Commands

1. Scan for open ports from the external side of the network to verify the Firewall and Router policies. *Nmap[16] is a common port scanning tool:* nmap v2.30Beta21 will be used for port scanning. The parameters are noted below:

nmap –sT –v –O –p 1-65535 207.6.89.10 –oN Pfw1_TCPInternet.txt

nmap –sU –v –O –p 1-65535 207.6.89.10 –oN Pfw1_UDPInternet.txt

nmap –sT –v –O –p 1-65535 12.1.1.1 –oN Prt1_TCPInternet.txt

nmap –sU –v –O –p 1-65535 12.1.1.1 –oN Prt1_UDPInternet.txt

[16] www.insecure.org. "Nmap 5/3/03 http://www.insecure.org/nmap/ (06/05/03)

-sT TCP connect Scan; unprivileged use, log succeed followed by shutdown

-sU UDP scans send 0 byte packets; icmp unreachable means port closed

-O some remote host fingerprinting

-v Verbose mode

-p port range

2. Look at logs on the firewall to ensure that Accepts, encrypts, decrypts, drops and rejects are logged correctly based on the port scan and that the rule number corresponds to the expected action of the rule. Ensure that the Firewall is not receiving packets that should be blocked at the external router.

3. Check that our configured options in checkpoint are operational. The option for successive events includes port-scanning defenses, which gives us alerting options for this type of scanning. Based on our nmap scan the administrator should have received a page indicating successive events. The SmartDefense module[17] has not been purchased with the firewall due to cost restraints. So we are depending on our own verifications that the Security Policy is working. Even though there are many functions built into the SmartDefense module which indicate the attempts interval, max logging attempts, successive events and the like. We can turn on anti-spoofing on the interfaces.

Using Checkpoint's Log Viewer from the Firewall Manager we can watch the log during the nmap scan and then do a quick export of the log to a Text and then Excel format. Then we can search for ports that should be blocked at the router and make sure they are not reaching the firewall log. We can search for a port that ought to be coming to the firewall and accepted and check against the rule, which accepts it to ensure it is the relevant rule. We can then search for ports, which reach the firewall but are disallowed to specific hosts and ensure they are dropped by the correct rule. Then we will use a client to login using the Secure Client VPN connection. We can follow the same process by doing the port scans in each of our two DMZs as follows. For TCP the most basic connect SYN Scan is used to generate as much information as possible in logs on the target host. We are not trying to be clandestine with this since the objective is to verify the Firewall Policy. We can also do a snoop or tcpdump at the OS level of the firewall to compare results.

nmap –sT –v –O –p 1-65535 192.168.10.50 –oN Pfw1_TCPWEB.txt

nmap –sU –v –O –p 1-65535 192.168.10.50 –oN Pfw1_UDPWEB.txt

nmap –sT –v –O –p 1-65535 192.168.20.70 –oN Pfw1_TCPEMAIL.txt

[17] © *Check Point Software Technologies Ltd.* "SmartDefense" http://www.checkpoint.com/products/downloads/smartdefense_datasheet.pdf (06/05/03)

nmap –sU –v –O –p 1-65535 192.168.20.70 –oN Pfw1_UDPEMAIL.txt

The end result of these two steps is that we now have a sense of whether the Rules are being applied on the firewall. We can also check the output of the NMAP to see if ports are accessible and weigh it against the firewall log. The following is an example of the output of the NMAP and the Log export.

NMAP Output
The following is an example but not an exhaustive list of the open ports found and should correspond with our services allowed on each interface of the firewall

Records	**Port**	**State**
1	22/tcp	Open
2	80/tcp	Open
3	18191/udp	Open
4	18192/udp	Open
5	18190/udp	Open
6	256/tcp	Open
7	18208/udp	Open
8	265/tcp	Open
9	18210/udp	Open
10	18211/udp	Open
11	257/tcp	Open
12	18207/udp	Open
13	18231/udp	Open
14	264/tcp	Open
15	500/tcp	Open
16	500/udp	Open

Firewall Log Viewer Output

I have taken a sample of some of the log entries, showing some NTP accepted traffic (records 109 to 111) along with some vpn session activity:

112	6-Jun-02	0:01:58	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	drop	RDP		10.50.8.10	12.1.1.1
113	6-Jun-02	0:02:02	VPN-1 & FireWall-1	hme0	10.50.8.10	log	accept	ntp-udp		10.50.8.10	10.50.4.103
114	6-Jun-02	0:02:02	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	drop	RDP		10.50.8.10	12.1.1.1
115	6-Jun-02	0:02:02	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	drop	RDP		10.50.8.10	12.1.1.1
116	6-Jun-02	3:33:33	VPN-1 & FireWall-1	hme0	10.50.8.10	log	accept	ssh		10.50.4.102	207.6.89.10
117	6-Jun-02	3:33:33	VPN-1 & FireWall-1	hme0	10.50.8.10	log	accept	ssh		10.50.4.102	207.6.89.10
118	6-Jun-02	3:39:03	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		62070	10.50.8.10	192.168.10.61
119	6-Jun-02	3:39:03	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		52113	10.50.8.10	192.168.10.61
120	6-Jun-02	3:39:03	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		63881	10.50.8.10	192.168.10.61
121	6-Jun-02	3:40:57	VPN-1 & FireWall-1	hme0	10.50.8.10	log	accept	domain-udp		10.50.8.10	10.50.4.103
122	6-Jun-02	3:40:57	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	domain-udp		10.50.8.10	10.50.4.103
123	6-Jun-02	3:49:38	VPN-1 & FireWall-1	daemon	207.6.89.10	log	keyinst			68.82.235.152	207.6.89.10
124	6-Jun-02	3:49:42	VPN-1 & FireWall-1	hme0	10.50.8.10	log	accept	ntp-udp		10.50.8.10	128.4.40.12
125	6-Jun-02	4:09:15	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		62070	10.50.8.10	192.168.10.61
126	6-Jun-02	8:22:21	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	decrypt	domain-udp		100.0.0.2	10.50.4.103
127	6-Jun-02	8:22:22	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	decrypt	domain-udp		100.0.0.2	10.50.4.103
128	6-Jun-02	8:22:22	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	domain-udp		172.10.4.1	10.50.4.103
129	6-Jun-02	8:22:22	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	domain-udp		172.10.4.1	10.50.4.103
130	6-Jun-02	8:22:26	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	domain-udp		172.10.4.1	10.50.4.103
131	6-Jun-02	8:22:26	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	domain-udp		172.10.4.1	10.50.4.103
132	6-Jun-02	8:24:35	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		49497	10.50.8.10	192.168.10.61
133	6-Jun-02	8:24:35	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		52635	10.50.8.10	192.168.10.61
134	6-Jun-02	8:24:35	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		63881	10.50.8.10	192.168.10.61
135	6-Jun-02	8:24:35	VPN-1 & FireWall-1	hme0	10.50.8.10	log	drop		51789	10.50.8.10	192.168.10.61
136	6-Jun-02	8:37:47	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	http		208.5.6.7	192.168.20.61
137	6-Jun-02	8:37:47	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	decrypt	http		100.0.0.2	192.168.20.61
138	6-Jun-02	8:43:27	VPN-1 & FireWall-1	qfe0	207.6.89.10	log	accept	IKE		207.25.45.55	207.6.89.10

Tip: For specific VPN traffic we will look at the logs for the attempted VPN client login, authentication to RADIUS and the subsequent “keyinst” action in the traffic. Although not seen in the above output table, Checkpoint’s distinctive blue/purple color of encrypted traffic logs is helpful is this respect.

Analysis and Recommendations regarding the Audit

Upon auditing the firewall, it seems that there is an inefficiency associated with having the email and anti-virus servers in a different DMZ to the Web Servers. We recommend moving the e-mail and anti-virus servers to the Web Browsing DMZ and having one untrusted Service Network between the external and internal segments. The anti-virus scanning engine has to pass through the firewall in the current environment.

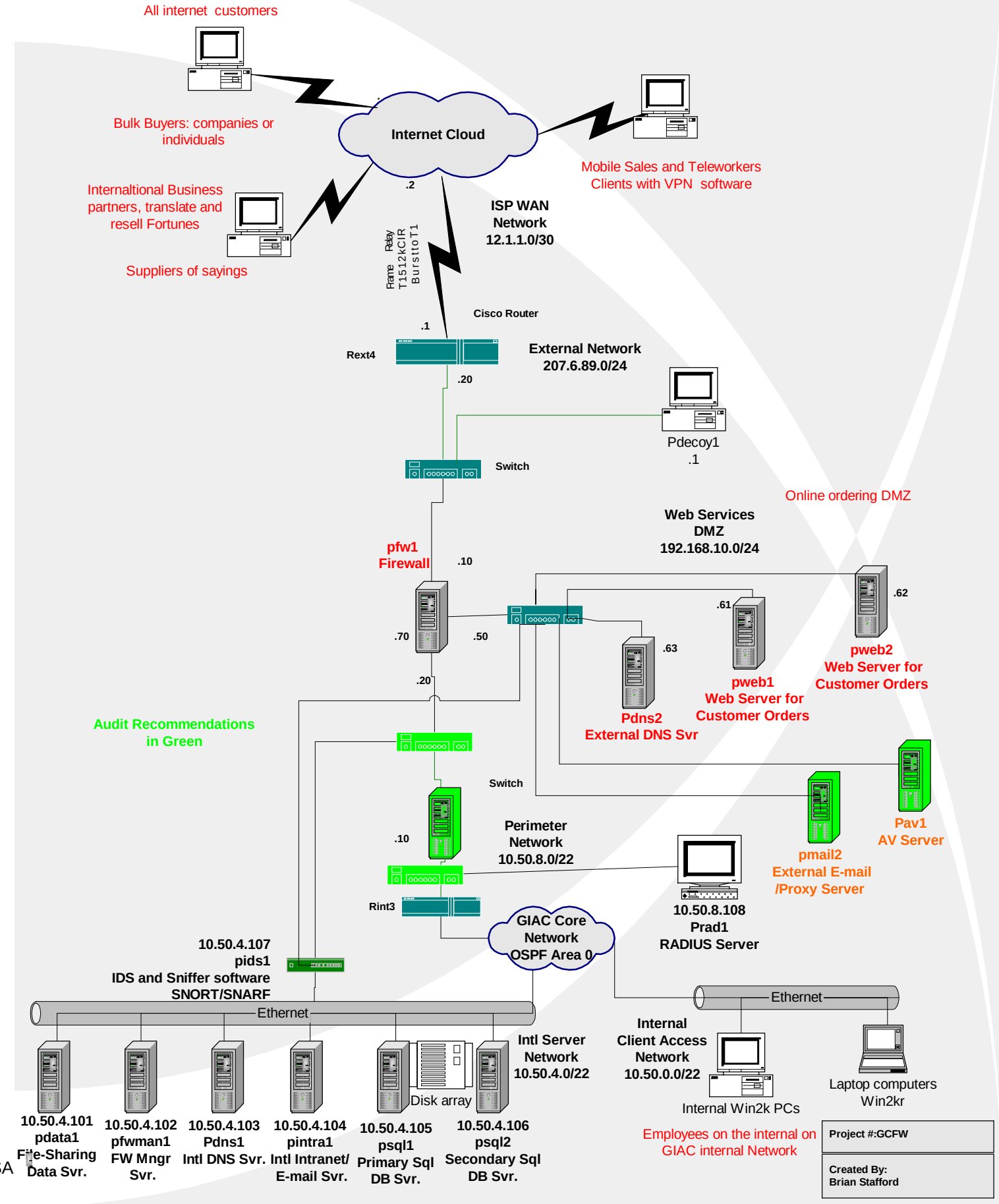
The rules seem efficiently placed with the exception that the Client-encrypt rule should be placed nearer the top of the Rule base in our opinion due to it's volume of use. Also, high udp ports are open on the Router access-list and any service is accepted to the Firewall interface. It is recommended to be as specific as possible regarding port access through to the firewall. Also, we would investigate some RDP traffic coming from the ISP, although we drop it.

Also, a practice in the industry is to place an internal firewall to separate the private to a semi-private zone, commonly called a "firewall sandwich" which can offer another layer of security if the service network or external DMZ is compromised.

On the positive side the decoy is something not as commonly used as it could be in the industry and we agree with a function like this. It can give clues as to threatening activity directed towards your address space.

The following will be a general recommendation for a re-architecture, should you choose to accept it.

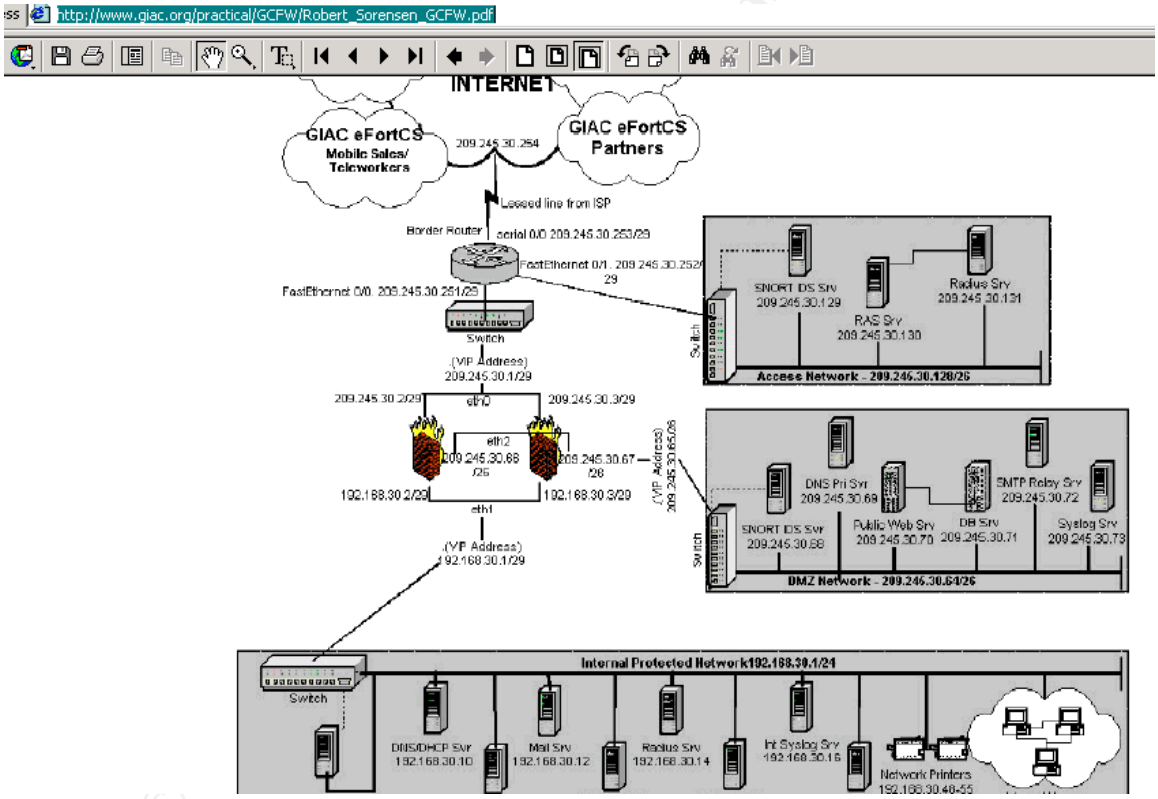
Enterprise Network Architecture



4. Attack

Design Under Fire

I have chosen Robert Sorensen's[18] design for a sample attack. Although time-consuming there are three approaches I would like to explore. Firstly, the personal firewall on the home users laptops is worth looking at to pursue my theme of Remote Access. Securemote is different from SecureClient and I'd like a stab at hijacking a session if I can sniff one out but it will require somehow breaking the Personal Firewall to **compromise an internal host.** Secondly, SNORT version 1.9 reminds me of a recent vulnerability and (although this is a recent paper from 3/28/03) may help **attack the Firewall.** Thirdly, use some compromised hosts to initiate a **Denial of Service** using a recent e-mail worm.



The Social engineering aspect requires some phone calls to see if I can get the external address to set up my SecureRemote Client, pretending to be a remote user. The e-mail addressing scheme will be easy enough to get. I can also do some DNS lookups on the resulting networks to get some clues on external addressing. I'll then do some sniffing of that network on the Checkpoint tunnel

[18] Sorensen, Robert. "GIAC Certified Firewall Analyst (GCFW)". Analyst #0391 3/28/03 Practical Assignment. Version 1.9, (06/07/03) http://www.giac.org/practical/GCFW/Robert_Sorensen_GCFW.pdf 6/07/03

setup ports and try to fish out some naming conventions and/or addressing of remote clients. Even if these fail the web presence will expose some addressing information about the public side of the network.

I have discovered through Web Services and port/address scanning that the Web server is 209.245.30.70. I really need the address with the high 18,000 ports open, like 18,191, also 2746 and 500 ports to identify the end point of the VPN tunnel. My gut tells me that if I can get a session on one of those VPN connections, that traffic to the inside the network might be open through the tunnel, with the user permissions only of course. It strikes me that it would be easier to exploit the network if I hijack a session rather than the hard way of DDOS and Brute Force attacks which don't get me any valuable information. I have decided to focus my primary effort on trying to compromise a remote user, with a secondary plan of a Denial of Service as a consolation prize if I fail.

The key to trying the Session Hijack is to find the remote VPN user's public IP address and since I have done some reconnaissance on the destination address of Web Servers and the VPN endpoint address of the GIAC network, I can sniff out some connections. The tools to do this are HUNT[19], SATAN[20], using finger, systat and rwho, who, or ps, which are freely available. I choose to use my Linux Redhat 8.2[21] machine to try the attack. Luckily, I note that an address of one of these connections is in the range of a large high-speed cable provider, the same nation-wide provider that I myself use for my cable connection. The following is the theoretical approach I use to try the hijack. The assumption here is that I could be lucky enough to find a support level type session and not just an online data entry session without any good privileges to attack the network systems. However, should I come across the latter I would attempt to put junk data into the data entry application. A third assumption is that, since the user is running Securemote and not SecureClient, Zone Labs ZoneAlarm Pro[22] is in use as personal firewall as referenced in the paper on page 4[23].

On the assumption that I identify the session and have identified the remote user's public address I decide to attack the host. I am interested in trying to stop the personal firewall from loading so that I can try to hijack the session. I am very interested in one of the latest strange virus traits. Bugbear is referred to by

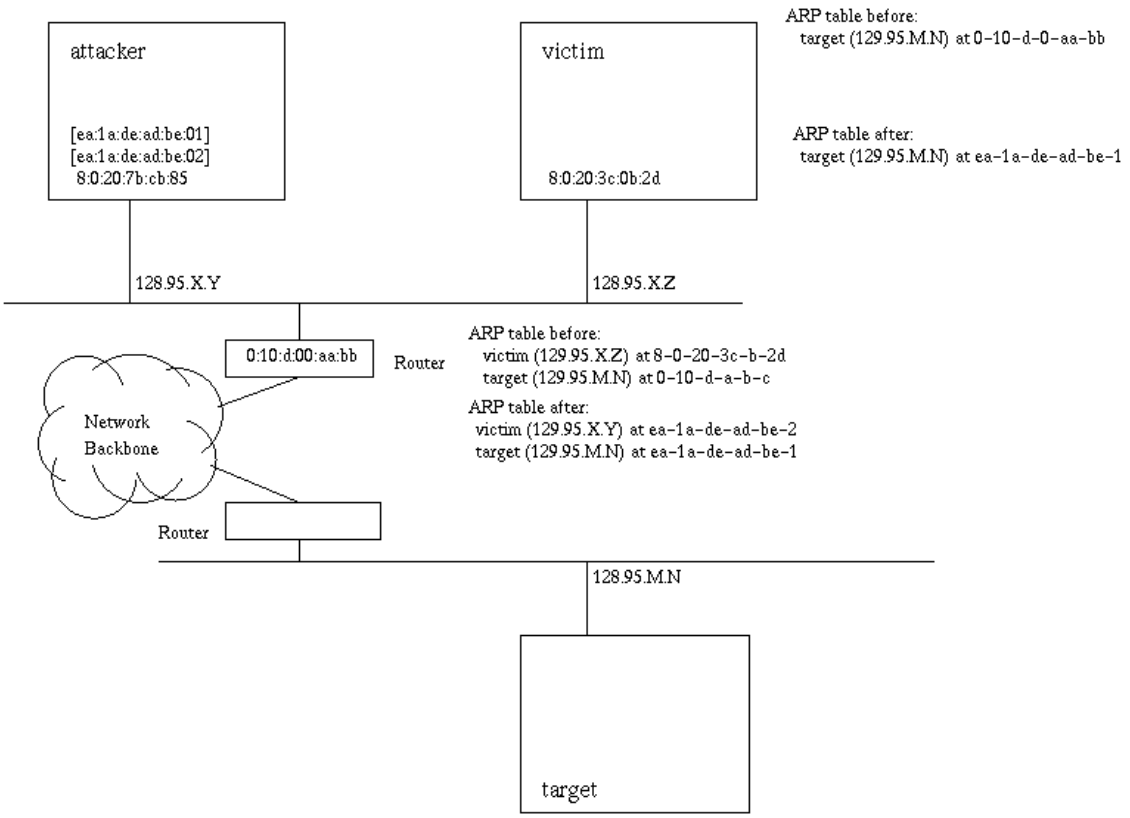
[19] Krauz, Pavel. "Pavel Krauz's Home Page", circa 2001 http://lin.fsid.cvut.cz/%7Ekra/index.html, (06/07/03)
[20] Staff of Wasington University. "Getting started" ???? http://staff.washington.edu/dittrich/misc/satan/docs/satan_doc.html (06/07/03)
[21] Copyright © 2003 Red Hat, Inc. , "Red Hat Linux 9", 06/07/03 http://www.redhat.com/software/linux/ (06/07/03)
[22] © 1999-2003 Zone Labs, Inc. "Zone Alarm Pro" http://download.zonelabs.com/bin/media/pdf/ZAP_datasheet.pdf (06/07/03)
[23] Sorensen, Robert. "GIAC Certified Firewall Analyst (GCFW)". 3/28/03 Practical Assignment. Version 1.9, (06/07/03)

CERT[24] and specifically tries to stop some security services.

“The CERT/CC has received reports of a variant of the BugBear mass-emailing worm, referred to as "W32/BugBear.B", "W32/Kijmo" or "W32/Shamur". It arrives as an attachment with a .pif, .scr, or .exe extension. Upon opening the attachment, the worm attempts to mail itself to all e-mail addresses it finds in the current inbox and in files with a .dbx, .eml, .mbx, .mmf, .nch, .ocs, or .tbb file extension. Additionally, this worm has a built-in keylogger, a backdoor that listens on port 1080/tcp, and attempts to terminate numerous security product processes on the system.” Our learned e-mail addresses come into play.

Should the attempt succeed in stopping the firewall service I would use the following diagram on page 33, as a well-known paper regarding session hijacking, written by the staff at Washington University[25]. We use HUNT as a tool to detect a new session and the prompt changes from “->” to “*>”. The paper refers to the following steps. Start the ARP relay daemon and prepare the RST daemon for use later. Log into the target using telnet. Turn on the RST daemon to prevent new sessions, wait to hijack a root session, looking for an ssu or pbsu to see a root login. Look for DNS server information to check around the network. Look at hosts file to get an idea of naming conventions. Set up back door, disable the command history, turn off the RST daemon. Wait till late evening or early morning to log on through the back door, install a rootkit and clean log files.

[24] CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office. , “W32/BugBear.B”, 06/05/03 http://www.cert.org/current/current_activity.html#bugbear (06/07/03)
[25] Staff of Washington University, “Session hijack Script” http://staff.washington.edu/dittrich/talks/agora/script.html (6/04/03)



To **attack against the Firewall** I will try to exploit the SNORT vulnerability just in case the fixes have not been applied:
"To exploit this vulnerability, an attacker must disrupt the state tracking mechanism of the preprocessor module by sending a series of packets with crafted sequence numbers. This causes the module to bypass a check for buffer overflow attempts and allows the attacker to insert arbitrary code into the heap"[26].

This vulnerability affects Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1, including Snort 1.9.1. Snort has published an advisory regarding this vulnerability; it is at the SNORT website also[27]. My logic is that enough arbitrary code will adversely affect the firewall OS. Then we can target the interface of the firewall with many large packets. The danger of this is that it will,
".. allow remote attackers to execute arbitrary code with the privileges of the user running Snort, typically root."

[26]CERT® and CERT Coordination Center®, (6/7/03)
http://www.cert.org/advisories/CA-2003-13.html (06/06/03)
[27] Snort(TM) Advisory: Integer Overflow in Stream4, (6/06/03)
http://www.snort.org/advisories/snort-2003-04-16-1.txt (06/07/03)

"..merely sending malicious traffic where it can be observed by an affected Snort sensor is sufficient to exploit these vulnerabilities."

The following is suggested to protect against this attack in the snort.conf file:
"To prevent exploitation of VU#139129, comment out the following line:
preprocessor stream4_reassemble
To prevent exploitation of VU#916785, comment out the following line:
preprocessor rpc_decode: 111 32771"

Having **compromised 50 cable modem** machines I decide to now flood the E-mail Server with a worm and, hopefully, deny service. The logic behind this attack is that I take the most recent information I have, in this case the "W32/Sobig.E". Hopefully, I can make my 50 "Zombies" send the e-mail virus to everyone in the address books I have crafted. The idea is that the more recent a virus I can find the more likely that the server is not updated. This update was submitted at "www.CERT.org"[28] on June 26, 2003

"The CERT/CC has received reports of a variant of the Sobig mass-emailing worm, referred to as "W32/Sobig.E." It arrives as an attachment with a .zip extension. Within that .zip file is a file with either a .scr or .pif extension. Upon opening the attachment, the worm attempts to mail itself to all e-mail addresses it finds in files with a .wab, .dbx, .htm, .html, .eml, or .txt file extension. Additionally, this worm spoofs the "From" address, therefore it is likely that the sender address is not that of the infected user.
Upon execution, the worm places the following files in the "%Windir%" directory:
winssk32.exe (copy of worm)
msrrf.dat (configuration file)
The following registry keys are created:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"SSK Service"="%Windir%\winssk32.exe"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"SSK Service"="%Windir%\winssk32.exe"
The worm also attempts to propogate by copying itself to the following folders:
Documents and Settings\All Users\Start Menu\Programs\Startup\
Windows\All Users\Start Menu\Programs\StartUp\ "

The recommendation here is that Anti-Virus software be kept up to date.

[28] CERT® and CERT Coordination Center® "CERT/CC Current Activity" (6/26/03) http://www.cert.org/current/current_activity.html#sobig.e (7/01/03)

List of References

1. © 1992-2003 Cisco Systems, Inc. “Cisco Catalyst 2950 Series Switches” http://www.cisco.com/en/US/products/hw/switches/ps628/index.html (06/02/03)
2. © 2003 Microsoft Corporation. “Microsoft Business Solutions Releases Solomon 5.5” (03/27/03): http://www.microsoft.com/presspass/press/2003/may03/05-27Solomon55pr.asp (06/02/03)
3. © Check Point Software Technologies Ltd. “VPN-1 SecuRemote & VPN-1 SecureClient” http://www.checkpoint.com/products/protect/vpn-1_srsc.html (6/02/03)
4. © 2003 Vircom inc. “VOPRADIUS Server” http://www.vircom.com/Enterprise/Solutions/VOPradius/ (6/02/03)
5. © 2003 Microsoft Corporation. “Exchange 2000 Product Overview” (12/16/02) http://www.microsoft.com/exchange/evaluation/overview/default.asp (06/02/03)
6. Copyright 1989-2003 Trend Micro, Inc. “InterScan VirusWall” http://www.trendmicro.com/en/products/gateway/isvw/evaluate/overview.htm (06/02/03)
7. © 2003 Microsoft Corporation**.** “Choose Your Edition” (May 2001) http://www.microsoft.com/isaserver/howtobuy/choosing/default.asp (06/02/03)
*8. dwelchATphoneboyDOTcom. “*Issues pertaining to SecuRemote and Secure Client, Check Point's VPN client for Windows, Linux, MacOS, and others.” 11/08/02 http://www.phoneboy.com/fom-serve/cache/13.html (06/03/03)
9. Brian Caswell and Marty Roesch “What is SNORT?” 6/4/03 http://www.snort.org/about.html (06/04/03)
10. National Security Agency. “Router Security configuration Guide” 9/27/02 Version 1.1 http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (06/02/03)
11. “CERT® Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors”, 4/23/03 http://www.cert.org/summary/ (06/04/03)
12. Bull, Jon. “Snort’s Place in a Windows 2000 Environment” 4/15/02 http://snort.org/docs/snort-win2k.htm (06/05/03)
13. Activeworx. “IDS Policy Manager Version 1.3.1 for Windows 2000/XP” 06/05/03 http://www.activeworx.com/ (06/05/03)
14. Caswell, Brian and Roesch, Marty “Snort Signature Database” 06/05/03 http://www.snort.org/cgi-bin/needed.cgi (06/05/03)
15. Green, Chris. “snort.conf, v.110” 08/14/02 http://public.lanl.gov/cpw/snort.conf.html (06/05/03)
16. www.insecure.org. “Nmap 5/3/03 http://www.insecure.org/nmap/ (06/05/03)

17. © Check Point Software Technologies Ltd. "SmartDefense" http://www.checkpoint.com/products/downloads/smartdefense_datasheet.pdf (06/05/03)
18. Sorensen, Robert. "GIAC Certified Firewall Analyst (GCFW)". Analyst #0391 Practical Assignment. Version 1.9, (03/28/03) http://www.giac.org/practical/GCFW/Robert_Sorensen_GCFW.pdf (6/07/03)
19. Krauz, Pavel. "Pavel Krauz's Home Page", circa 2001 http://lin.fsid.cvut.cz/%7Ekra/index.html, (06/07/03)
20. Staff of Wasington University. "Getting started" http://staff.washington.edu/dittrich/misc/satan/docs/satan_doc.html (06/07/03)
21. Copyright © 2003 Red Hat, Inc., "Red Hat Linux 9", 06/07/03 http://www.redhat.com/software/linux/ (06/07/03)
22. © 1999-2003 Zone Labs, Inc. "Zone Alarm Pro" http://download.zonelabs.com/bin/media/pdf/ZAP_datasheet.pdf (06/07/03)
23. Sorensen, Robert. "GIAC Certified Firewall Analyst (GCFW)". 3/28/03 Practical Assignment. Version 1.9, (06/07/03)
24 CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office. , "W32/BugBear.B", 06/05/03 http://www.cert.org/current/current_activity.html#bugbear (06/07/03)
25. Staff of Washington University, "Session hijack Script" http://staff.washington.edu/dittrich/talks/agora/script.html (6/04/03)
26. CERT® and CERT Coordination Center®, (6/7/03) http://www.cert.org/advisories/CA-2003-13.html (06/06/03)
27. Snort(TM) Advisory: Integer Overflow in Stream4, (6/06/03) http://www.snort.org/advisories/snort-2003-04-16-1.txt (06/07/03)
28. CERT® and CERT Coordination Center® "CERT/CC Current Activity"(6/26/03) http://www.cert.org/current/current_activity.html#sobig.e (7/01/03)