



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.



GCFW Practical Assignment

Version 1.6 – Parliament Hill SANS, August 2001

Curtis L. Blais

Table of contents

Introduction	3
Assignment 1 – Security Architecture.....	4
1. BACKGROUND	5
2. ARCHITECTURE DESCRIPTION	5
2.1. Layer 1 - Perimeter.....	7
2.2. Layer 2 - External DMZ	8
2.3. Layer 3 - Internal DMZ	10
2.4. Layer 4 - Core Network.....	12
2.5. Access Models	15
Assignment 2 – Security Policy	16
1. BORDER ROUTER POLICY	17
1.1. General Router Commands	17
1.2. Ingress Filter Commands	19
1.3. Egress Filter Commands	19
2. PRIMARY FIREWALL POLICY	20
3. VPN POLICY	22
3.1. PPTP Setup Description.....	22
4. POLICY TUTORIAL.....	40
4.1. ACL Syntax.....	42
4.2. General ACL Assembly.....	44
4.3. Applying an Ingress/Egress ACL.....	45
4.4. Detailed description of router ACL's and general security commands.....	47
Assignment 3 – Security Architecture Audit	54
1. AUDIT PLAN	55
2. AUDIT EXECUTION	56
3. AUDIT EVALUATION	61
Assignment 4 – Design Under Fire.....	63
1. CHOSEN DESIGN.....	64
2. THREE FIREWALL VULNERABILITIES.....	64
2.1.1. Vulnerability 1.....	64
2.1.2. Vulnerability 2.....	66
2.1.3. Vulnerability 3.....	66
2.1.4. Firewall Vulnerability Attack.....	67
3. DENIAL OF SERVICE ATTACK	67
4. INTERNAL HOST ATTACK PLAN	69
References.....	70

Introduction

This document is to fulfill the practical requirements for the GCFW certification. The instruction set for this specific practical is version 1.6. There are 4 assignments included in the practical itself that allow for the demonstration of perimeter security knowledge to be displayed.

The first Assignment is to build and describe a security architecture for a fictitious company GIAC Enterprises, which deals in the online sales of fortune cookie sayings. The architecture contains filtering routers, Firewalls, VPN's, secure remote access, and internal firewalls and will consider how customers, suppliers and partners will access the environment.

Assignment 2 requires the defining of a security policy for the border router, the primary firewall, and the VPN. This will list the specifics on how each of these devices is configured to meet GIAC Enterprises business needs. The second part of this section is to write a tutorial on how to implement a security policy from one of the items listed in this assignment.

The third assignment is to plan an audit, perform the audit and then evaluate the audit of the primary firewall from the previous two sections. This will demonstrate that the policy of the primary firewall is performing as expected and to help identify any configuration errors that may have taken place.

The fourth part of the practical is to design and undertake three attacks on a previously posted security architecture. The first attack is to search for vulnerabilities on the primary firewall. The second attack is to subject the design to a Ddos attack. Finally, plan the compromise of an internal system and describe the process.

Assignment 1 – Security Architecture

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

1. Background

The security architecture described within this document is designed for GIAC Enterprises (GIAC-E), the on-line fortune cookie sales company. This design also takes into account network security/redundancy, network management, and data backup. A description of how existing customers, suppliers and business partners communicate is included here, as well as solutions for the remote sales force and work at home users.

During the course of this paper, it may be appropriate to show GIAC-E Company policy on specific situations. These will be listed in a shaded box such as this one and labeled with "Company Policy Excerpt" to identify the contents.

2. Architecture Description

The security design for GIAC-E is divided into 4 sections. Beginning with layer 1 and progressing through each successive section the design becomes more secure. Layer 4 is the core of the environment and thus considered to be the most protected area.

Figure 1 on the next page encompasses the entire architecture. The rest of assignment 1 will describe each section in greater detail.

© SANS Institute 2000 - 2002
Author retains full rights.

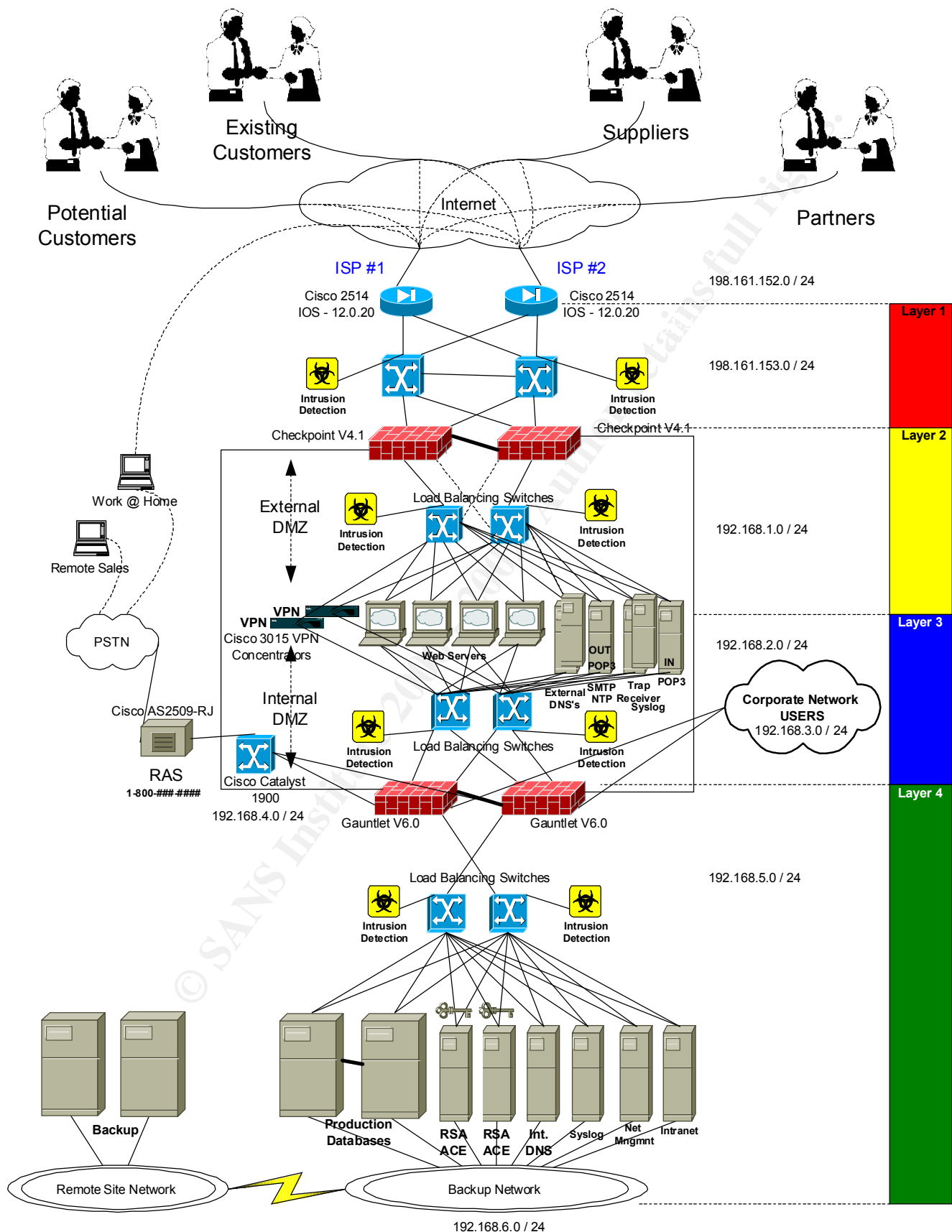


Figure 1 - GIAC-E Security Network Architecture

2.1. Layer 1 - Perimeter

Figure 2 shows the first layer of the security architecture for GIAC Enterprises. Dual connections to the Internet (via separate ISP's) utilize BGP for dynamic routing to allow for Internet redundancy. These two independent connections terminate on two separate Cisco 2500 Series Routers running Cisco Inter-network Operating System (IOS) version 12.0.20.

[Please Note: these low-end routers are used so that in section two of this report the configurations will match what is drawn here. Realistically, routers with a bit more horsepower would be used in this circumstance.]

These routers are the first measure of defense against hostile activity by utilizing the Access Control List (ACL) capability built in the IOS. It is possible to apply an inbound ACL and an outbound ACL on a single Cisco router interface to have some level of control over what will be allowed in or out of the perimeter. This is generally done at a high level to reduce the effectiveness of certain hacking or denial of service techniques. This level is meant to compliment the next level of security and not duplicate it. Assignment 2 of this paper will go into detail with respect to the actual ACL code lines.

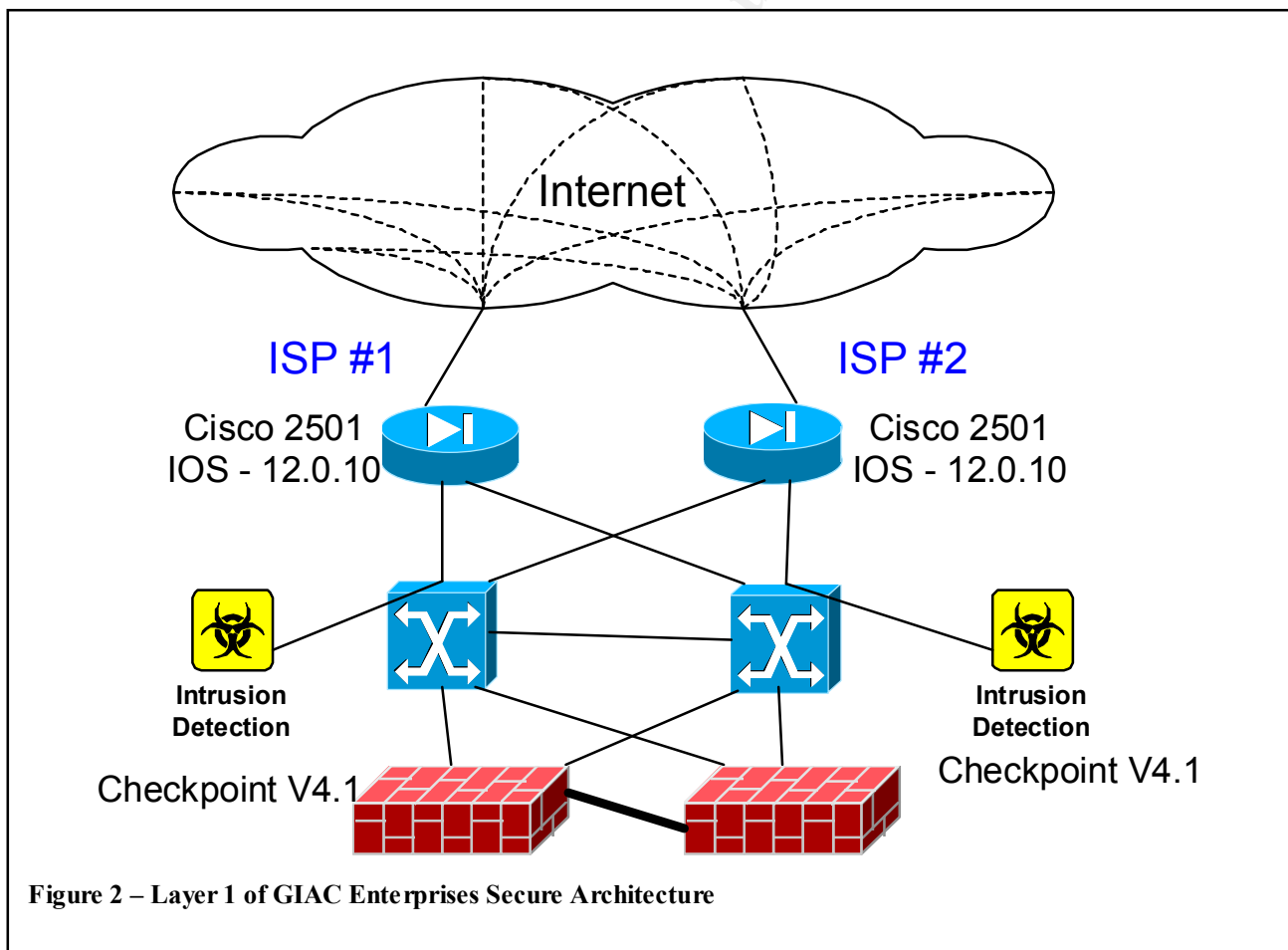


Figure 2 – Layer 1 of GIAC Enterprises Secure Architecture

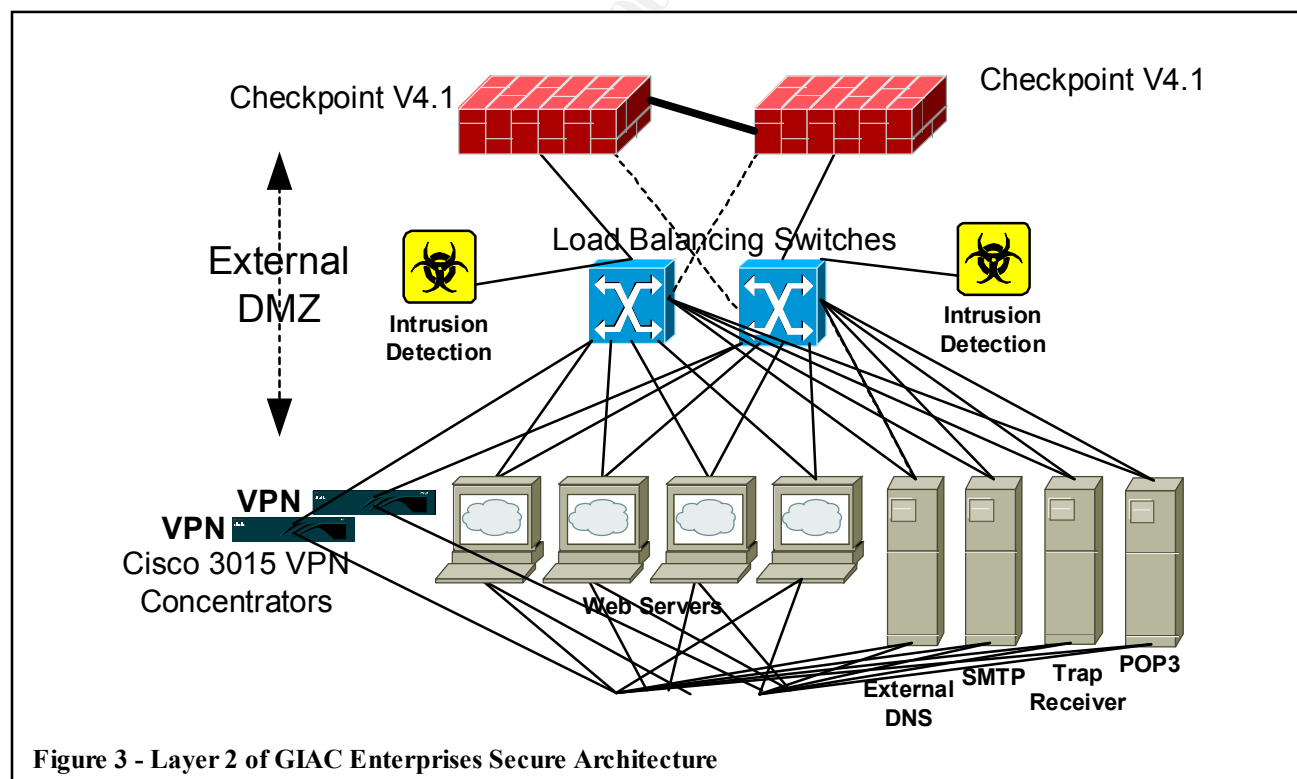
Following the routers is a set of two switches, which allow each router to have two connections on the inside. Some specific switches have built in load balancing and can provide for protection against TCP SYN attacks and monitor and track session flows to GCFW - V 1.6 Practical

guard against some denial of service attacks (for example see Foundry Networks ServerIron at the following link for a more detailed explanation → <http://www.foundrynetworks.com/products/webswitches/serveriron/datasheets.html>). A configuration for these switches will not be listed here but it is worth noting that some feature rich products can be used at this level to aid in securing the environment.

Layer 1 ends on the outside of the Checkpoint 4.1 state full inspection firewalls. These devices are also dual attached to the switches that connect them to the perimeter routers. Once again, this is done to provide for hardware redundancy and the possibility of load balancing to provide for a rich experience for the e-customers of GIAC-E.

2.2. Layer 2 - External DMZ

The second layer of the secure architecture can be seen in Figure 3. Dual Checkpoint firewalls are attached to a set of load balancing switches. This configuration allows for multiple simultaneous hardware failures and the continued operation of this environment. At this level the firewalls are keeping state of the connections that are originated from inside this area and providing access to specific services that are offered. The area between the firewalls and the service hosts is termed the “External Demilitarized Zone (DMZ)”. This area is where business partners, suppliers, customers, and the general public make their connection to GIAC-E.



Each of the devices in this section is configured to be single function. This is a method of securing the device so that it can only be attacked by the single service it is offering. It also is simpler to maintain patches for a single service.

The VPN devices chosen are the Cisco 3015 VPN Concentrators. In this configuration they can each sustain 100 simultaneous connections. Should the need arise to expand the capability, the devices can be upgraded to the 3030, 3060 or the 3080 respectfully with substantial increases in simultaneous sessions. A separate encryption accelerator card may also be added to increase throughput of the device.

The VPN concentrators have multiple uses. First, they provide the ability for work at home users to connect, via a broadband Internet connection at their residence, in a secure manner to the corporate environment. Windows 2000 comes with a client that will connect using Point-to-Point Tunneling Protocol (PPTP) to the Cisco concentrators. A separate client, one that is bundled with the Cisco VPN concentrator allows the configuration of an IPSEC connection.

Company Policy Excerpt:

... It is the policy of GIAC-E that employees will only connect to the corporate network with corporate computer facilities. Personal home computers are NOT to be used for business functions. This allows for a tighter control on the corporate computer environment.

Conversely, corporate computing equipment is NOT to be used in a personal manner. This could allow the compromise of a computer that would be brought to the inside of the environment and threaten the internal company resources

Employee's that are found in breach of this policy may expect disciplinary action including the possibility of dismissal...

Partners and suppliers could certainly make use of this connection via a limited number of users who would be given VPN access into the company. This way the partners and suppliers could access internal information on an "as required" basis. It would also be possible to use a site-to-site VPN for those partners and/or suppliers who require this type of connectivity.

This section also includes a separate DNS that is designed to provide name resolution explicitly for the External DMZ, two SMTP/POP3 servers, and a Trap Receiver. The incoming SMTP server will be the source of mail retrieval for the company and would contain a flavor of an E-mail scanning package. In this example let's say Trend Micro's version. As a crosscheck to this, each individual network station would be equipped with a virus scanner from a separate manufacturer. For the purposes of this description the host-based version will be VirusScan from McAfee/Network Associates. This difference is to provide from some overlap of virus detection, if one fails to detect a specific problem, there is a chance that the other manufacturer's product will catch it.

The receiving and sending SMTP servers are separate devices. This adds for a bit more security; a single function box. If the SMTP send service is running on the same device as the SMTP receive service and it is compromised, the perpetrator has access

to send and receive mail. In the single service model here – a perpetrator must compromise two separate boxes to control ingoing and outgoing mail.

The Trap receiver is a way to allow devices in layer 2 and layer 1 a place to report traps. This device will simply receive the traps. The network management station (located in layer 4) will retrieve these traps on a regular basis. This setup allows a centrally protected management system to still monitor devices in less protected areas. The network management station will be allowed to initiate contact to the trap receiver but the reverse will be denied by the firewall between these environments.

Syslog is also present at this layer to accept logs from the Layer 1 devices.

2.3. Layer 3 - Internal DMZ

This layer, as shown in Figure 4, is by far the most complex layer of the architecture. This is the layer that accommodates the requests that are generated from the External DMZ servers, allows connectivity from VPN users, provides the corporate users with their connection to the services offered internally and is the entry point for Remote Access Services (dial-up).

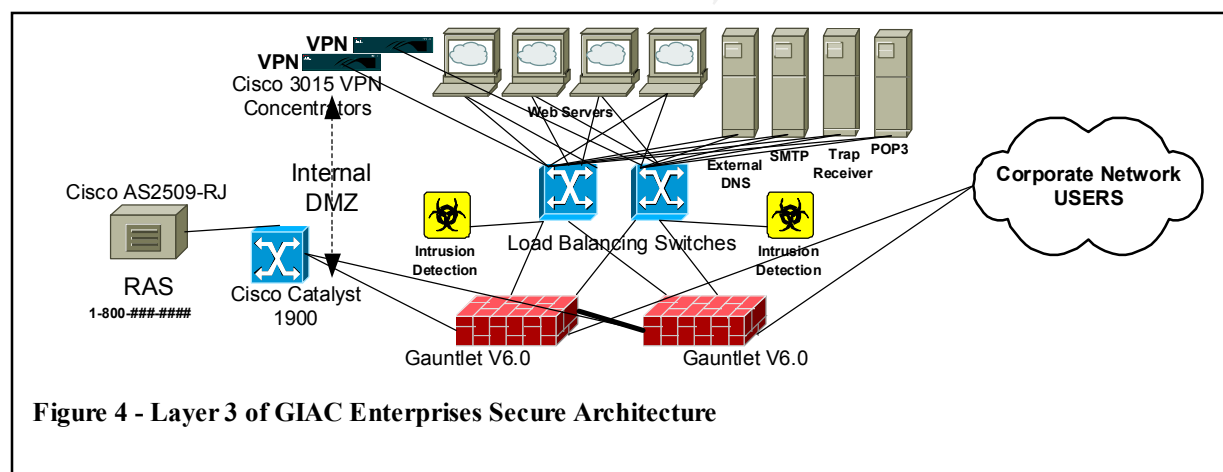


Figure 4 - Layer 3 of GIAC Enterprises Secure Architecture

The pair of Gauntlet V 6.0 firewalls that separate this layer from the next are key to protecting the final layer from un-authorized entry. This choice of firewall is completely different from the Layer 1-2 Checkpoint firewall product. In the case that a certain vulnerability is discovered in the Layer 1 firewall, it is prudent to choose a second type of firewall so that the same vulnerability cannot be exploited at the next layer. The Gauntlet firewall operates as a proxy, which operates differently than the State-full Inspection Checkpoint.

Proxy type firewalls always sit in the middle of a connection from the inside to the outside. This does not allow for a host on the internal network to directly connect to the outside world. Generally, Proxy type firewalls are considered to be faster and slightly more secure than their State-full Inspection counterparts. Thus, this firewall sits between layer 3 and 4 protecting the most sensitive part of the GIAC-E network. This firewall will control the following:

- General requests from the External DMZ
- Secure ID requests from External DMZ resources
- Corporate user access
- Remote User/Dialup user access
- VPN user access
- Network Management access

Requests from the External DMZ can be monitored and controlled down to specific types of service requests. In the case that an External DMZ host becomes compromised, the Gauntlet firewall will restrict the kind of access that is granted to the next level.

This architecture is designed to use Secure ID to provide for authentication for access. All devices would challenge for a Secure ID token before allowing the user access to the device. For example, a supplier who connects to the GIAC-E network via the VPN service would be prompted to enter the password and secure ID pin, which is a randomly generated 6 digit number. This number changes every 60 seconds making it extremely difficult for a would-be assailant to guess. More about Secure ID tokens can be found at the following link: <http://www.securid.com/products/securid/tokens.html>.

This mechanism gives excellent reliability in identifying that a legitimate user has made a connection. This same mechanism would be used to gain access to internal network equipment. In a December 2000 article in Information Security Magazine (written by M.E. Kabay and Lawrence M. Walsh) it is identified that internal security risks rose 42% and are much more of an issue than external threats:

“According to Information Security magazine's annual industry survey, published in September, the number of organizations reporting resource theft, destruction or sabotage increased by 42 percent from 1999 to 2000. Internal threats posed by disgruntled and careless employees continue to be a far more serious problem than external threats, where most companies focus their security budgets and resources.”

[Entire article: <http://www.infosecuritymag.com/articles/december00/features.shtml>]

Given the information from the article listed above, the corporate users are isolated from direct access to the core services. In this way, specific users can be identified for specific access through the Gauntlet firewall. Also, generic services can be allowed and at the same time, the firewall policy will disallow any access to “other” services as well as providing a choke point for logging.

As mentioned before, VPN access would be regulated through the Layer 3 firewall and authentication provided by Secure ID. This allows for exact controls as to what services VPN access is granted and also allows for logging of acceptable services.

Network Management is also controlled at this layer. The Trap Receiver would be queried for information that had been reported to it from layers above. This “step” type approach prevents a direct line of access from higher layers to lower ones.

The remote access device is also connected at this layer. This equipment provides dialup capability to the GIAC-E network and serves both the remote sales force and the work at home user. A 1-800 rotary line provides for access through the Plain Old Telephone System (POTS) and allows access to the GIAC-E environment from virtually any location. Remote sales can gain access from a client site or from their hotel room where 1-800 calls generally do not show up against your room charges.

The remote access system will also make use of the Secure ID service, to help positively identify the individual who is requesting access. This method is more desirable than having a remote sales person dial into a remote ISP and then use the VPN service to attach to the corporate environment. For one reason, using a 1-800 number connects the person directly to the GIAC-E environment through the point-to-point POTS system and immediately behind 3 layers of security. The alternative has the individual dialing a local ISP and first connecting to the raw Internet. Once connected, the initiation of a VPN session could take place. This traffic, although protected by the VPN tunnel and the encryption mechanism chosen to protect the data, is still travelling over an unprotected medium.

Work at home users have two options: they can dial-in to the RAS service and access the environment as described in the previous paragraph or if they subscribe to a broadband type of service, they could use the VPN facilities. Having two types of connections allows for an alternate access method to the environment in the case that one of the services is unavailable for whatever reason.

Company Policy Excerpt:

... It is the policy of GIAC-E that a single use tunnel will be used to connect from the user to the VPN service. This allows for the protection of the connection and helps prevent an attacker from accessing a split tunnel connection and gaining access to GIAC-E resources

...

2.4. Layer 4 - Core Network

The final layer of the Secure Architecture is shown in Figure 5. This layer is to be the most protected area of the GIAC-E network.

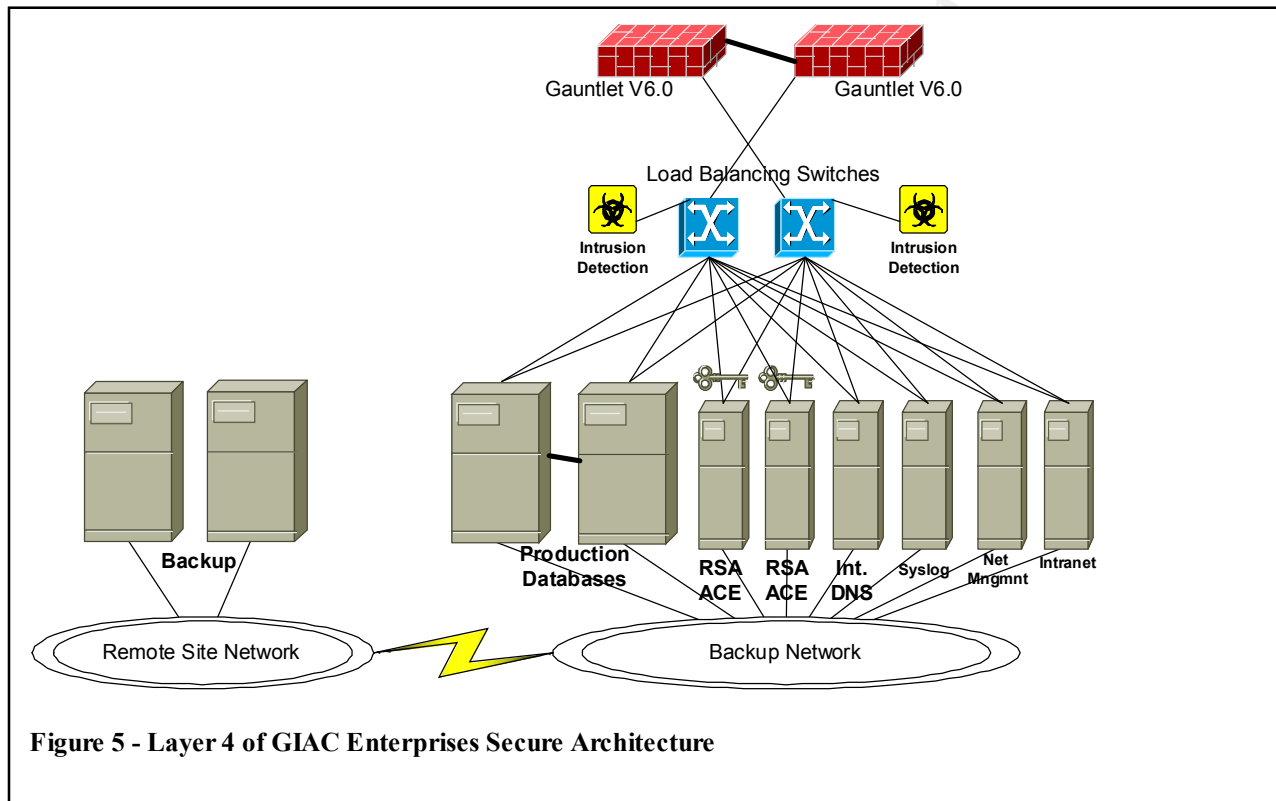
The Application Proxy firewalls that provide direct connectivity to this environment will be configured to allow only the expected type of access to the specific services. Each host included in this layer will be equipped with a host based intrusion detection system to allow for an extra level of security for the individual boxes.

Added to this will be a set of Intrusion Detection sensors that will be set to trigger an alarm for anything that appears to get through the existing perimeter and does not

GCFW - V 1.6 Practical

behave as expected. These logs will be sent to a common syslog server and analyzed on a regular basis to determine if any attempts have been made to breach system security. This will be done for all the IDS devices that are present in the Security Architecture at every layer.

The production databases are present here in a redundant fashion. And are equipped with automatic fail-over in the case that one of the database servers becomes incapacitated.



Dual RSA/ACE servers to provide for Secure ID redundancy are present. These devices will communicate with each other via the existing network and in the case of a failure, the secondary ACE server will assume the primary responsibilities.

The syslog server and Internal DNS are present here to protect them from access by unauthorized means and to allow for the contents to be backed up off site via the backup network.

The Network Management System (NMS) contains information about all the network elements that are being monitored. This information would be extremely valuable to an attacker, and thus needs to be protected from any unauthorized access.

The intranet server is located here to protect any internal information that will be delivered to the corporate users and to protect against attempts at tampering with this device.

The backup network could actually be considered layer 5 as the devices in layer 4 protect it in that they will not route between the two environments. Isolating the backup environment ensures that the backup traffic will be protected and not use corporate bandwidth. It also provides for an unobstructed restore path in the case that data needs to be recovered and isolates the traffic from any attempt to capture backup data.

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

2.5. Access Models

There are 5 models of access that can be applied to the customers, suppliers and partners (CSP) who require access to the GIAC-E network that include HTTP, HTTPS, Single user VPN, Site-to-Site VPN and Dialup. The solution will depend on the kind of access each requires from GIAC-E.

HTTP

Plain WEB access to the Layer 2 WEB servers is a possible solution for those who require access to data that is not sensitive. This would be the main mode of access for potential customers to browse the GIAC-E web page, find out what GIAC-E does and how to contact the company. It could also be used, in clear text, to provide a place for the CSP's to login (using secure ID) and having plain text access to reports or information that is deemed not sensitive.

HTTPS

Secure Access to the WEB services could be provided to the CPS's that are looking for data or access to WEB front-ended systems that is of a more critical nature. Generally, the 128-bit encryption is sufficient to protect this kind of data.

Single User VPN

This option may be reserved for existing customers. If only one person from the customer site requires access to place orders, a single user connection through the VPN service could be offered. The client would be given a Secure ID for authentication and would connect through the Internet. Once the session was established, the transactions can place in a secure manner. This is also one of the possible connections for the work at home user as well.

Site-to-Site VPN

The partners and/or the suppliers might best use this type of connection to the GIAC-E network. Partners work closely with GIAC-E to translate and re-sell the fortunes. The suppliers actually create the fortunes themselves. These two are good candidates to become "extensions" of the GIAC-E environment. A site-to-site VPN would allow these two groups to securely connect to GIAC-E from where ever they reside.

Dialup

The last case is the use for dialup - which could be used by any of the CSP's in the case that they did not have a permanent Internet connection, or their Internet site was not reliable and they needed to contact GIAC-E. This is used as a fall back position only. Remote Sales will use this as their connection back to the corporation from wherever they are at the time.

Assignment 2 – Security Policy

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

1. Border Router Policy

The border router policy was derived using the following four sources as guides and reference to increase the border security:

http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

<http://www.cisco.com/warp/public/707/21.htm>

<http://pasadena.net/cisco/secure.html> and

The GCFW course material Track 2 - Firewalls and Perimeter Protection, 2.3
Firewalls 102: Perimeter Protection and Defense in Depth.

The perimeter is built as is shown in Figure 6. Ethernet 0 is the External interface where the interface specific ACL's will be applied. The three areas that will be shown are: General router commands, Ingress Filter and Egress Filter.

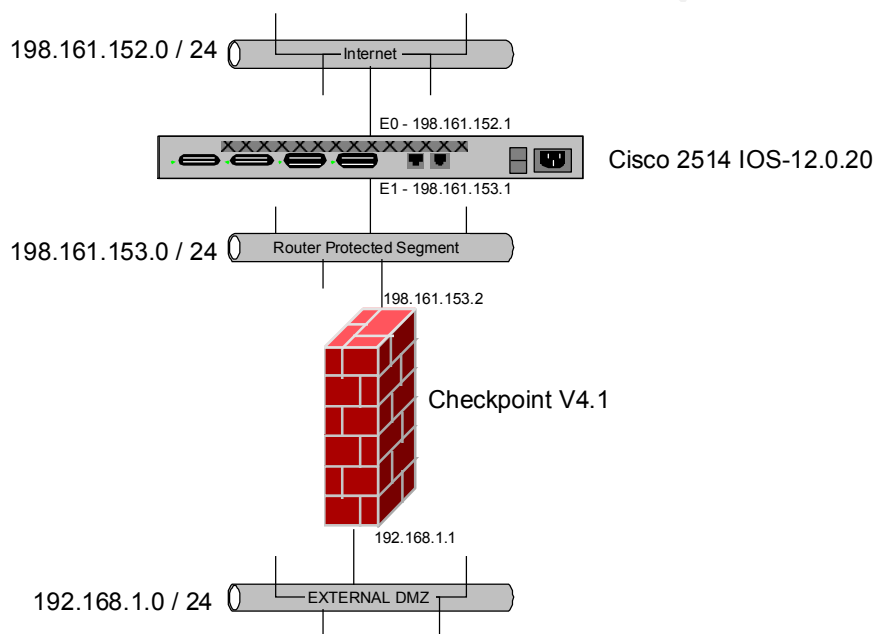


Figure 6 - Perimeter

1.1. General Router Commands

The router policy is listed in such a way that the statements contained here can simply be cut and pasted into a terminal session with a Cisco 2500 router. Items that are highlighted are default in 12.0.20 IOS but are included here as a precautionary measure.

```
service password-encryption
no cdp run
no service finger
no service udp-small-servers
no service tcp-small-servers
```

```
no ip source-route
no ip bootp server
no ip http server
no ntp master
no ip domain-lookup
no logging console
logging buffered
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
clock timezone MST -7
```

```
logging 192.168.1.29
```

```
snmp-server community c0vert RO 21
snmp-server trap-authentication
snmp-server tftp-server-list 2
snmp-server enable traps config
snmp-server enable traps snmp
snmp-server host 192.168.1.30 c0vert
```

```
access-list 2 permit host 192.168.1.30
```

```
banner motd &
```

```
*****
* THIS IS A CLOSED SYSTEM *
*****
```

DO NOT Proceed any further unless you have the expressed
written permission from the system administrators

All attempts to access are logged and will be used to
prosecute those who have not been granted the above stated
permission to the fullest extent of the law

```
*****
```

```
&
banner exec &
```

```
*****
* THIS IS A CLOSED SYSTEM *
*****
```

DO NOT Proceed any further unless you have the expressed
written permission from the system administrators

All attempts to access are logged and will be used to
prosecute those who have not been granted the above stated
permission to the fullest extent of the law

```
*****
```

```
&
banner incoming &
```

```
*****
* THIS IS A CLOSED SYSTEM *
*****
```

DO NOT Proceed any further unless you have the expressed
written permission from the system administrators

All attempts to access are logged and will be used to prosecute those who have not been granted the above stated permission to the fullest extent of the law

&

1.2. Ingress Filter Commands

Below is a list of the items that are present in the Ingress Filter for the GIAC-E perimeter. These items may be cut and pasted directly into an open configuration session on a Cisco router.

```
ip access-list extended ingress_filter
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 127.0.0.0 0.255.255.255 any log
deny ip 255.0.0.0 0.255.255.255 any log
deny ip 224.0.0.0 7.255.255.255 any log
deny ip host 0.0.0.0 any log
deny ip 198.161.153.0 0.0.0.255 any log
deny ip host 198.161.152.1 any log
permit tcp any host 192.168.153.2 gt 1023 established
permit ip any host 192.168.153.2
permit icmp any 198.161.153.0 0.0.0.255 3 0
permit icmp any 198.161.153.0 0.0.0.255 3 1
permit icmp any 198.161.153.0 0.0.0.255 3 3
permit icmp any 198.161.153.0 0.0.0.255 3 4
permit icmp any 198.161.153.0 0.0.0.255 3 13
permit icmp any 198.161.153.0 0.0.0.255 4
permit icmp any 198.161.153.0 0.0.0.255 11 0
deny tcp any any eq 113
deny ip any any log
interface Ethernet 0
ip access-group ingress_filter in
exit
exit
```

1.3. Egress Filter Commands

Below is a list of the items that are present in the Egress Filter for the GIAC-E perimeter. These items may be cut and pasted directly into an open configuration session on a Cisco router.

```
ip access-list extended egress_filter
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
deny ip any 192.168.0.0 0.0.255.255 log
deny ip any 172.16.0.0 0.15.255.255 log
deny ip any 10.0.0.0 0.255.255.255 log
deny icmp any any log
permit ip 198.161.153.0 0.0.0.255 any
```

```
deny ip any any log-input
Interface Ethernet 0
ip access-group egress_filter out
exit
exit
```

2. Primary Firewall Policy

The primary firewall in this architecture is a Checkpoint V 4.1 as previously shown in Figure 6. A brief description each of these rules is given here and a copy of the screen capture of the client session to generate Checkpoint policy rules is shown in Figure 7.

Rule #	Description	Log
1	To allow administrator(s) access to the firewall for maintenance	Long
2	To prevent any other persons, besides the administrators from accessin the firewall directly. Traffic is dropped.	Long
3	To drop any of the internal noisy Netbios traffic that would generate a lot of log information. Traffic is dropped.	Not Logged
4	To allow the switches and border routers to send traps and/or Syslog information to the Externl DMZ Servers.	Long
5	Allows both TCP and UDP DNS lookups from outside	Long
6	Allows Internal DNS's to make lokup requests to the outside world	Long
7	Allow outside users to connect to the Web cluster with either HTTP or HTTPS	Long
8	Allow Corporate Network users and RAS users access to the internet via HTTP or HTTPS	Long
9	Permit the Time Server to access information out on the Internet	Long
10	Allow the Mail Receiver to receive SMTP traffic from the Internet	Long
11	Permit the Mail Sender to sent SMTP mail out to the Internet	Long
12	Allow secure protocols to access either of the VPN concentrators	Long
13	Disallow any access from the Border Network to the External DMZ. This traffic is rejected	Alert
14	Final rule to drop anything that has not either been accepted or dropped already.	Alert

Table 1

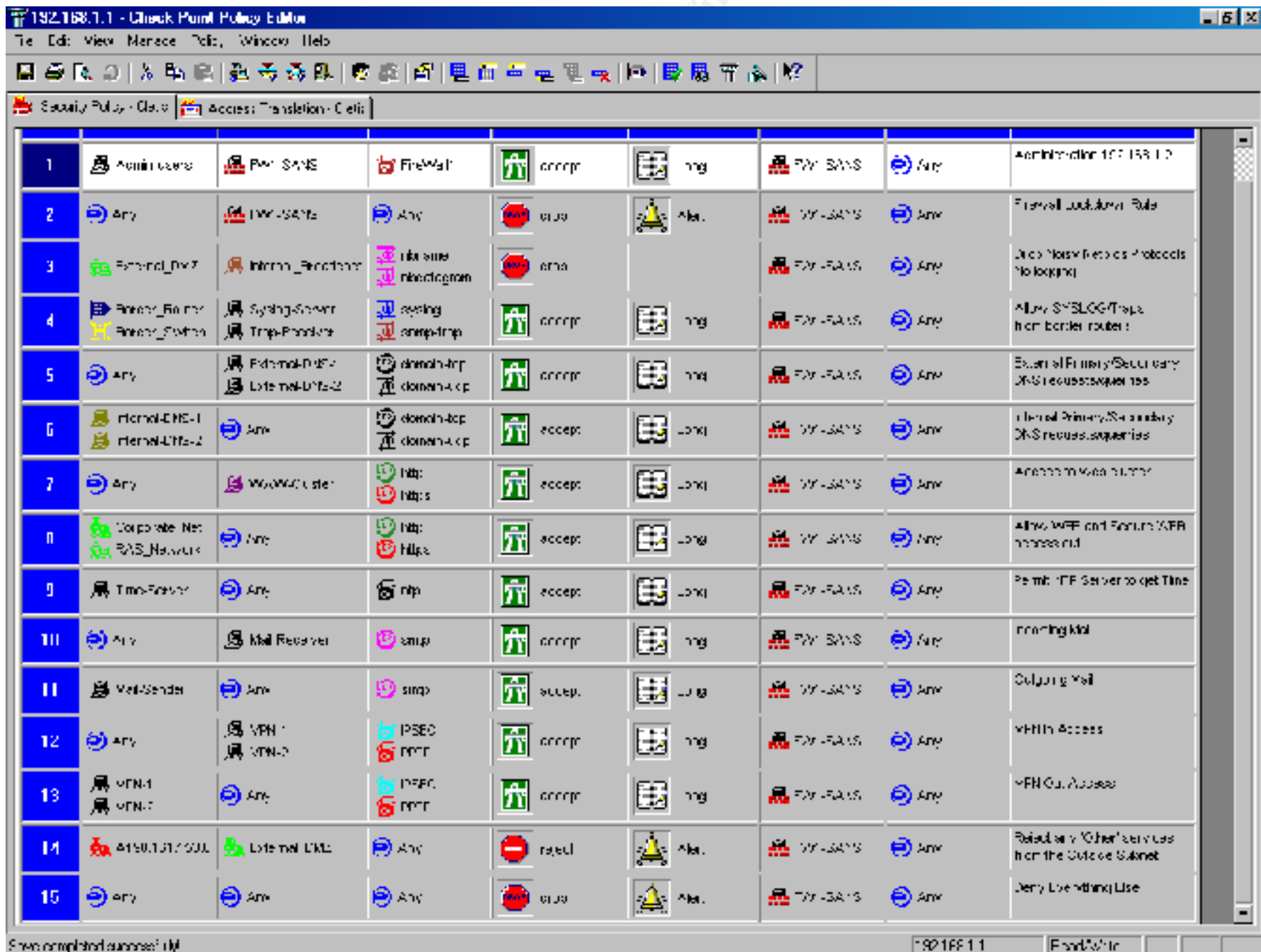


Figure 7 - Checkpoint Firewall 1 Policy

3. VPN Policy

The VPN policy for the GIAC-E architecture needs to take into consideration a few factors before the policy can be described.

First, NAT is being used at the Checkpoint perimeter firewall. This complicates things a little in that the Authentication Header protocol of the IPSEC Security Service cannot be used. The NAT process of FW1 will change the destination address and thus break the authentication header check that takes place at the VPN concentrator that is located behind the firewall. Moving the VPN concentrator to sit parallel with the firewall could alleviate this. However, an important assumption needs to be made to perform this step, which is assuming that the VPN concentrator security for all other types of access is nailed down. This is not the best alternative, and the concentrator should remain behind the protection of the firewall.

Second, no Cisco VPN hardware was available for this specific test. This means that an “actual” policy, directly from the Cisco hardware will not be produced here.

Third, the kind of data that will be transported here is not critical information, but fortune cookie sayings.

With this in mind, an attempt to satisfy the requirement of this section will be done as follows: a detailed description of the configuration of a PPTP solution for GIAC-E and what would need to be performed to make this choice function.

3.1. PPTP Setup Description

The first step here will be to create a user ID and account on the VPN Concentrator. The option to use Microsoft Challenge Handshake Authentication Protocol version 2 (MS CHAP v2) will be forced as the protocol of choice. As well, the maximum strength of encryption can be chosen (the standard is 40-bit but can be enhanced by the Microsoft “High Crypto” patch on the client to allow for a 128-bit encryption). In this example I will show the connection at 40-bit encryption. An option to use the RSA/ACE server for stronger authentication will also be chosen here.

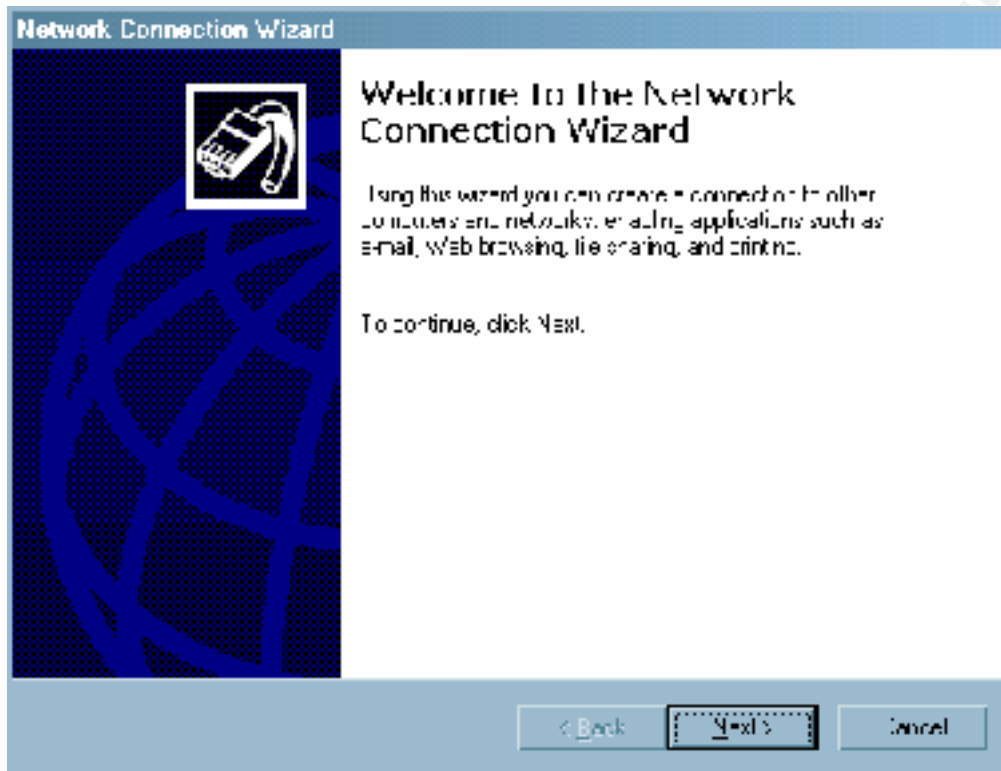
Once this is completed the Firewall requires two rules to aid in the setup of a PPTP both inbound and outbound. Generic Router Encapsulation (GRE), IP protocol 47, is required as well as the Point-to-Point Tunneling Protocol (PPTP) TCP port of 1723. Rule twelve in Figure 7 shows that any IP destined for either of the VPN concentrators, on service PPTP (which includes both GRE and PPTP) is accepted and logged. Conversely, rule thirteen allows either of the VPN concentrators to reply to any IP address with service PPTP (GRE and PPTP) and is logged. The IPSEC protocol suite is included as an allowable protocol but would need to be configured without

Authentication header as the firewall is performing NAT, which changes the header information.

The last step in the process is to configure the client on the end station. This is done with the following steps (Windows 2000):

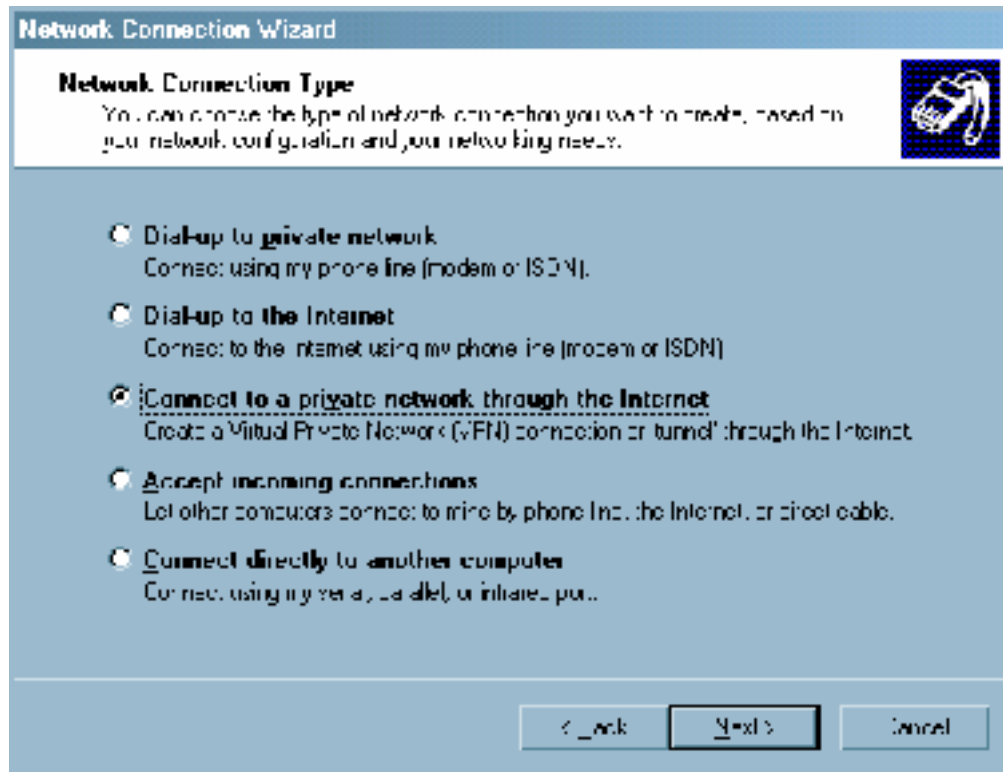
Step 1 - Left click on the "Start" button. Choose "Control Panel" and the sub-menu "Make a New Network or Dial connection"

You should now see the following popup on your screen:



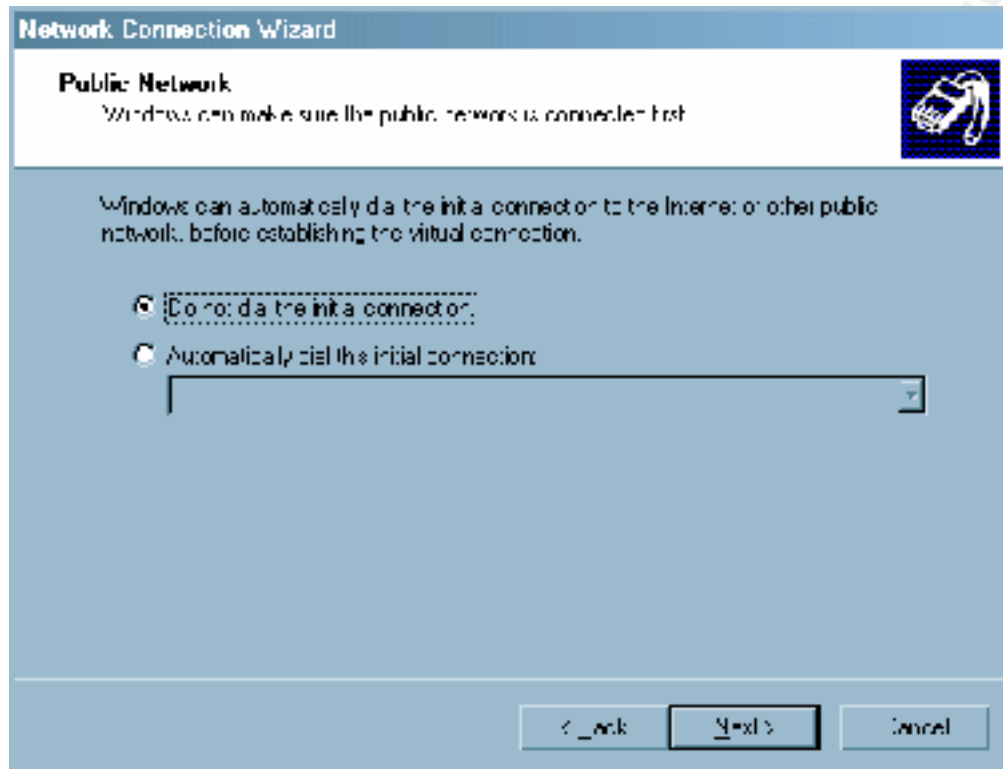
Please click on the "Next" button to move to the next screen.

Step 2 - You will need to choose the type of Network connection that you wish to create. It is assumed that you already have some sort of connection (dialup or ADSL/Cable Modem). Left click on the "Connect to a private network through the Internet" radio button.



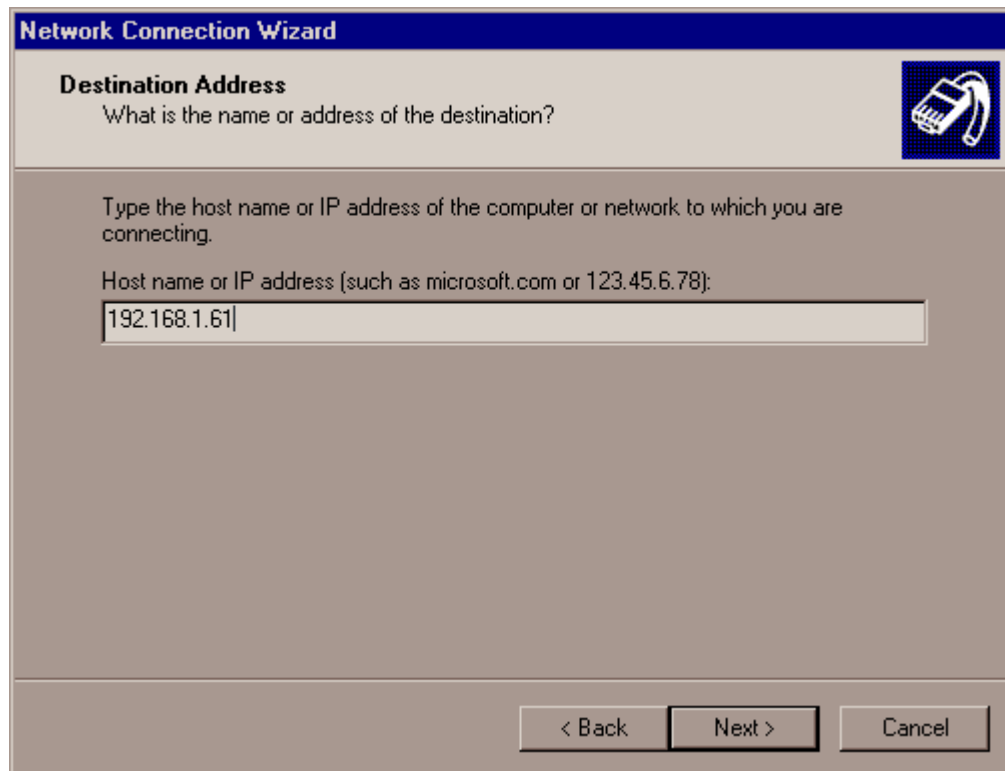
Please click on the "Next" button to move to the next screen.

Step 3 - If you are using an ADSL or cable modem connection you will need to select the "Do not dial the initial connection" radio button on the screen as shown below. If your connection is a dialup - you can choose the "Automatically dialup this initial connection" and then from the drop down box - select the appropriate dial connection. (NOTE - you do not need to select your dialup connection here - you can manually start your dialup connection each time you want to connect to the VPN concentrator. In this case select the "Do not dial the initial connection" option).



Please click on the "Next" button to move to the next screen.

Step 4 - The next screen allows you to put in the IP address of the VPN concentrator. Please type in the following IP address: **192.168.1.61** as shown on the screen capture below.



Network Connection Wizard

Destination Address
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

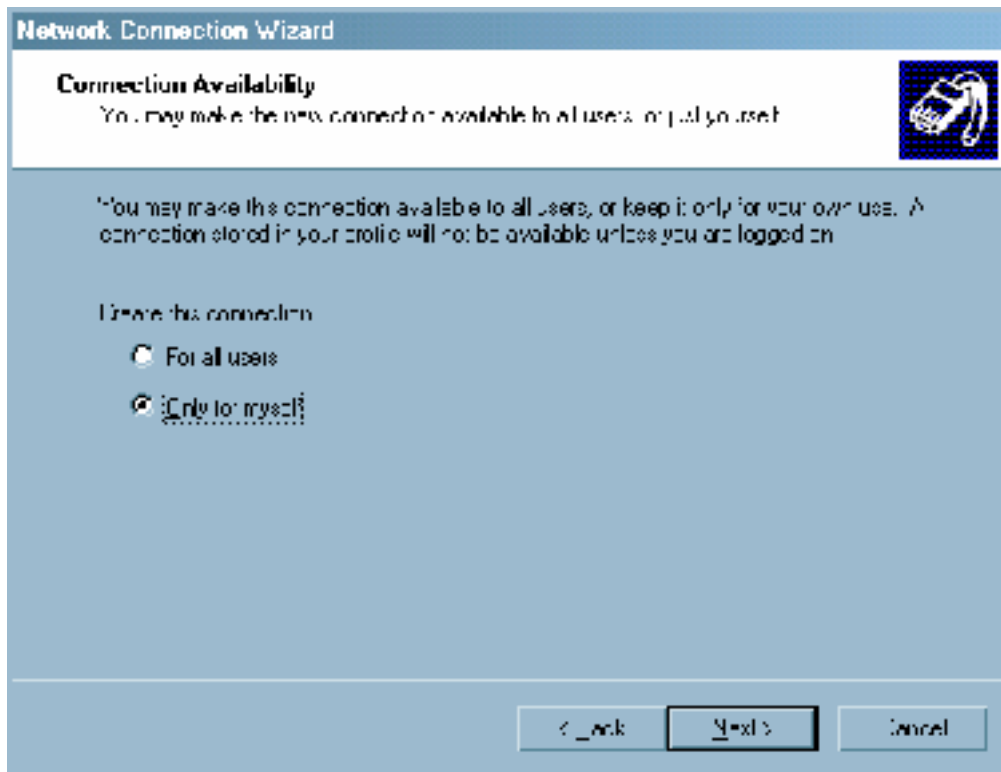
Host name or IP address (such as microsoft.com or 123.45.6.78);

192.168.1.61

< Back Next > Cancel

Please click on the "Next" button to move to the next screen.

Step 5 - This next screen allows you to make a choice if you want to make this connection available to all users of this specific computer. Unless the machine you are setting up is a community machine, say used for rotating support, then it is a good idea to select the "Only for myself" radio button as shown below.



Please click on the "Next" button to move to the next screen.

Step 6 - The next screen is the final screen of the Connection Wizard. In the blank space provided, type in the name by which you want to refer to your VPN connection. Also, if you want it to create a shortcut on your desktop - leave the "Add a shortcut to my desktop" selected as shown below.

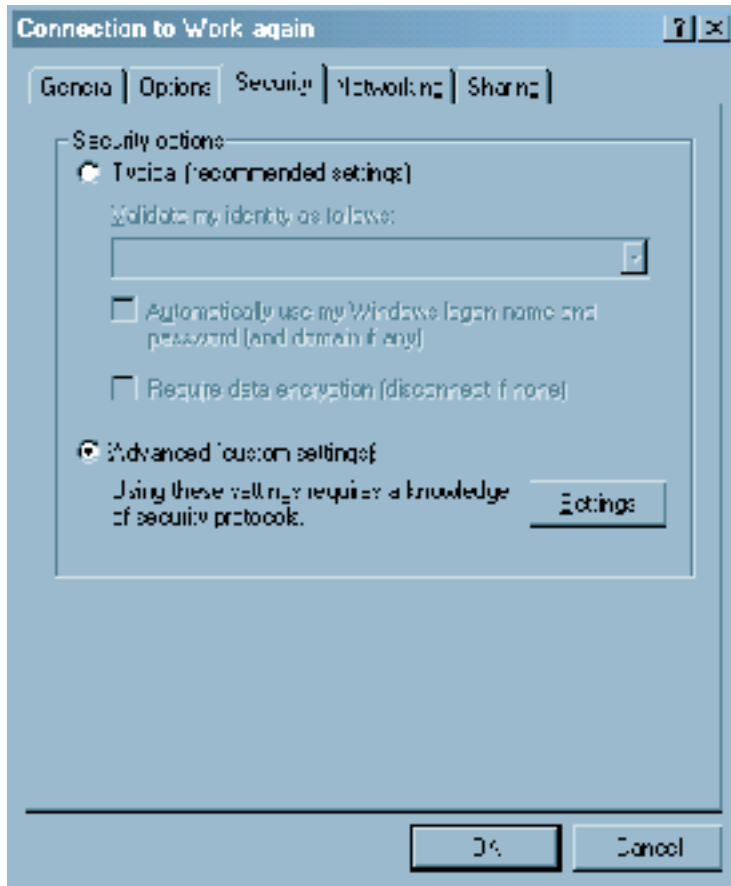


Left click on the "Finish" button.

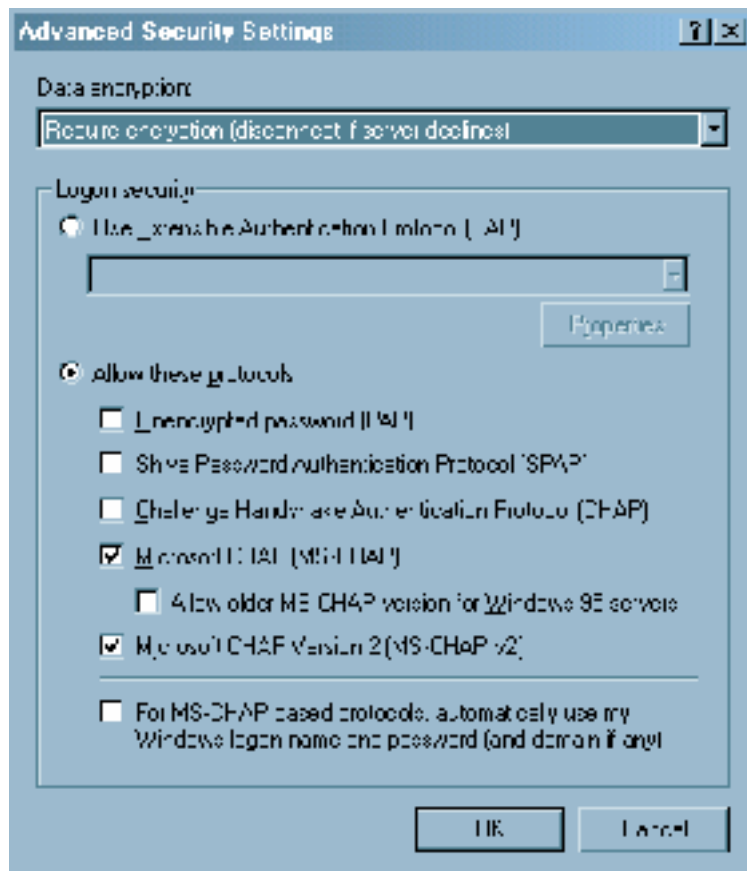
Step 7 - The next screen is the screen that you will normally see when you click on your VPN icon. The user name that you logged into the computer with will automatically appear in the "User name:" box. We are not quite ready to try and connect; there are a few properties that need to be set. Using the left mouse button, please click on the "Properties" button at the bottom of the panel.



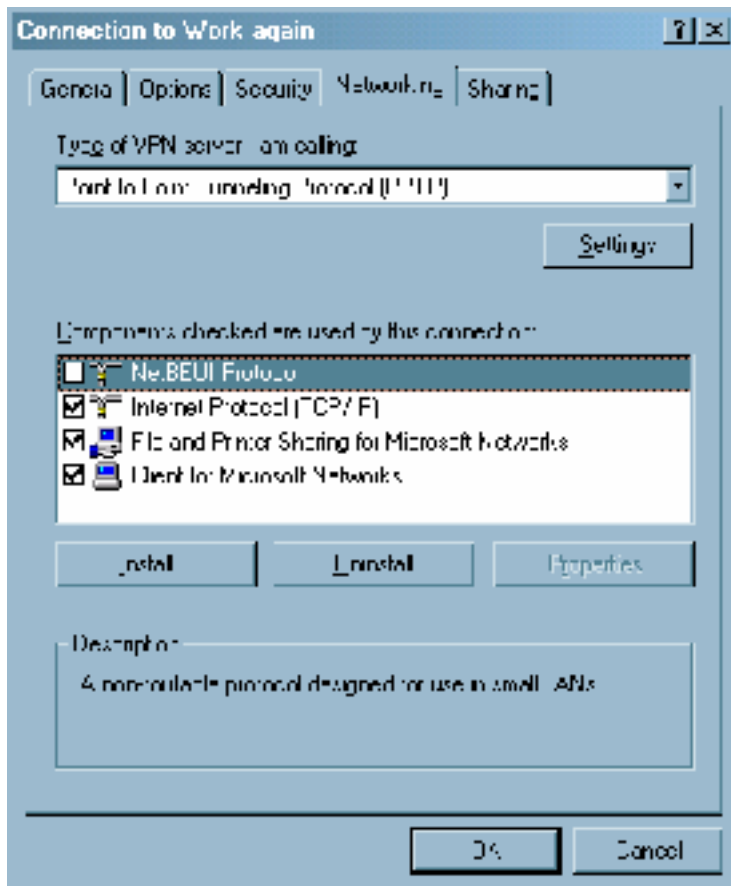
Step 8 - Using the left mouse button click once on the "Security" tab at the top of the panel. Choose the "Advanced (custom settings)" radio button as shown below. Next, click on the "Settings" button on the right side of the panel.



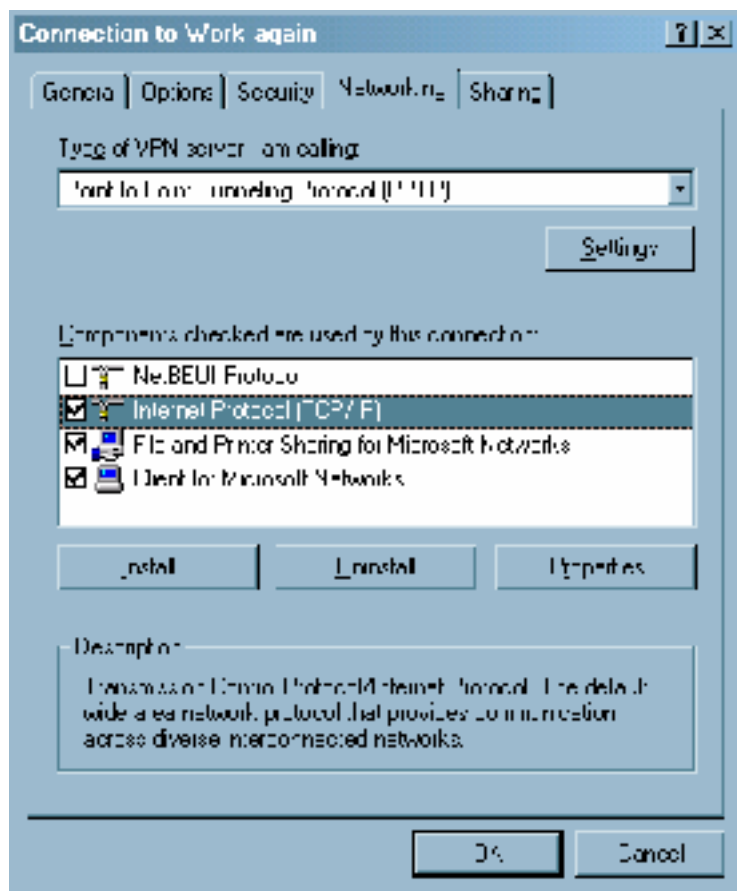
Step 9 - In the "Data encryption:" dialog box, please select the "Require encryption (disconnect if server declines)" option. This will ensure that your connection to the VPN concentrator is encrypted. Next select the "Allow these protocols" radio button to specify the protocol that will be used to create your session. Once that is done, ensure that there is a check mark beside "Microsoft CHAP" and "Microsoft CHAP Version 2" and no other protocols. Now click on the "Ok" button at the bottom of the panel.



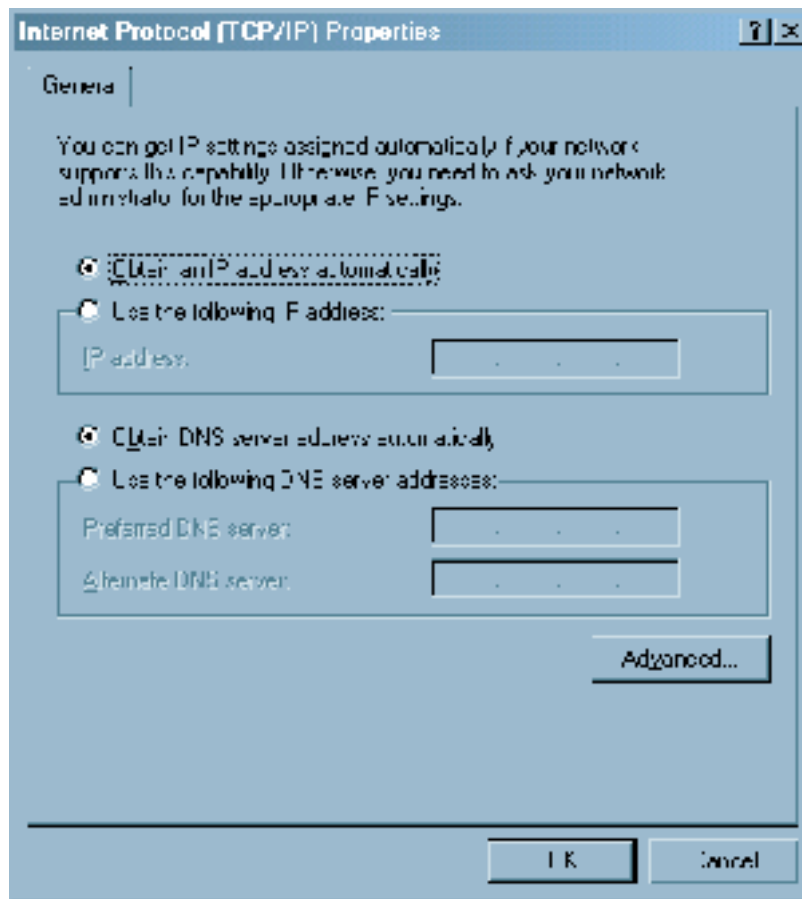
Step 10 - Using the Left mouse button, select the "Networking" tab at the top of the panel (shown below). In the "Type of VPN server I am calling:" dialog box choose the **Point to Point Tunneling Protocol** option. You can also UNCHECK the "NetBEUI Protocol" as it will not be negotiated correctly through the PPTP connection (if you leave this checked you will get a message when you try and connect that tells you it could not negotiate a connection for the NetBEUI protocol - you will still be able to connect).



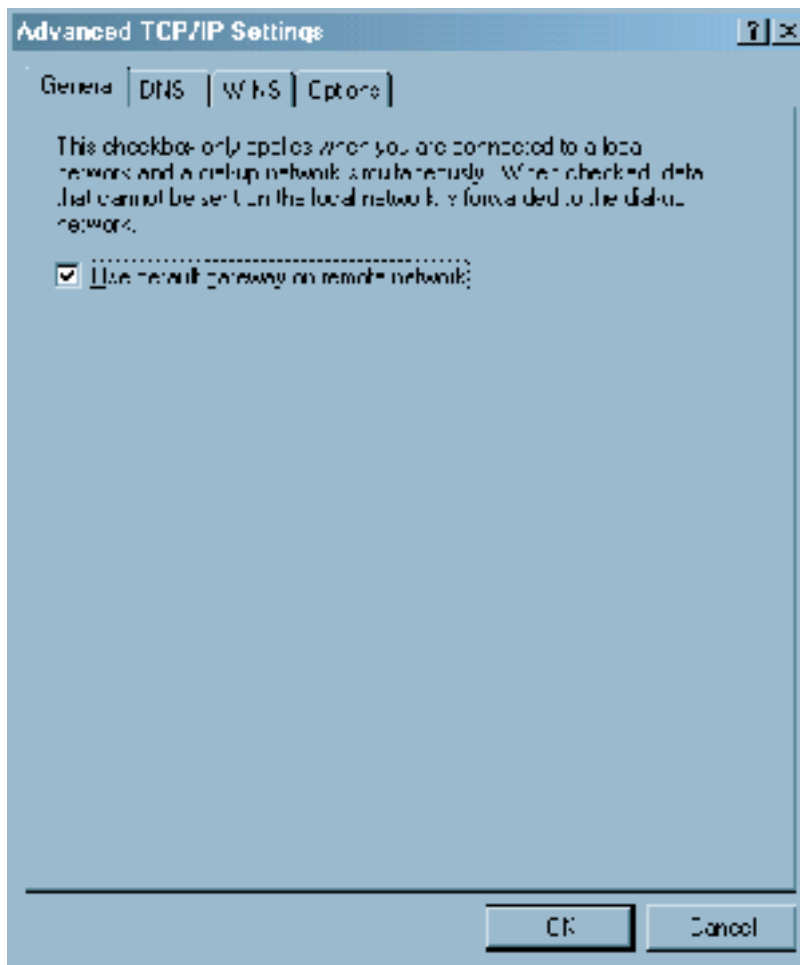
Step 11 - Now, highlight the "Internet Protocol (TCP/IP)" option in the components box as shown in the screen capture below. Then click on the "Properties" button.



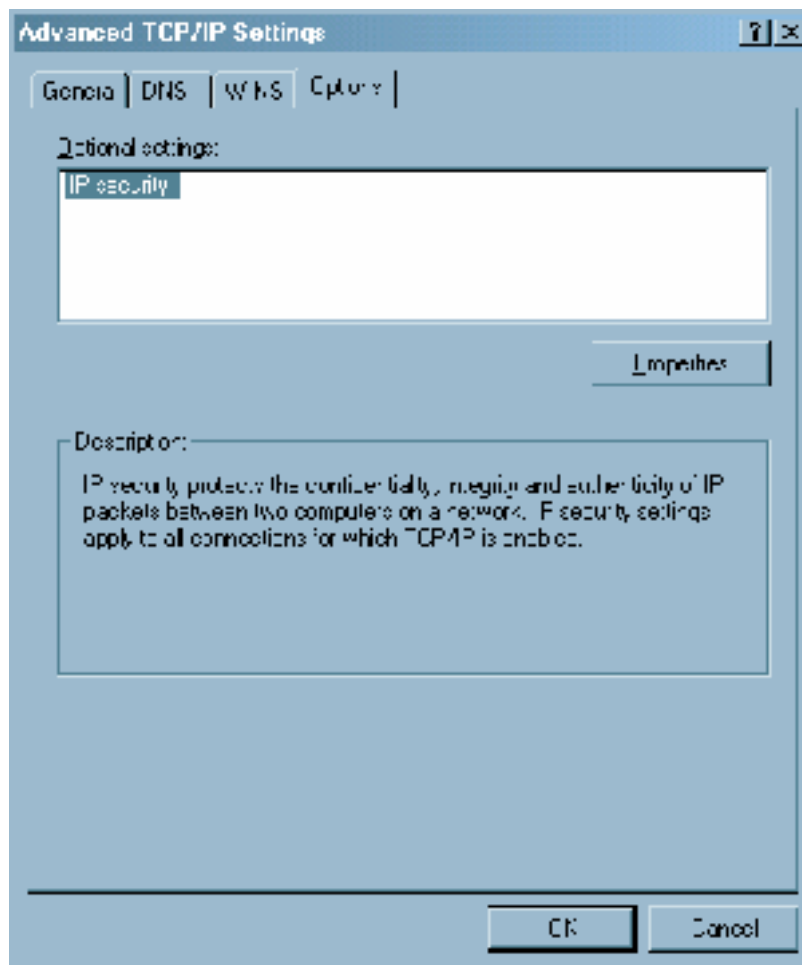
Step 12 - On the Internet Protocol (TCP/IP) Properties panel, both the "Obtain an IP address automatically" and "Obtain DNS server address automatically" should be selected. Press the "Advanced" button at the bottom of the panel.



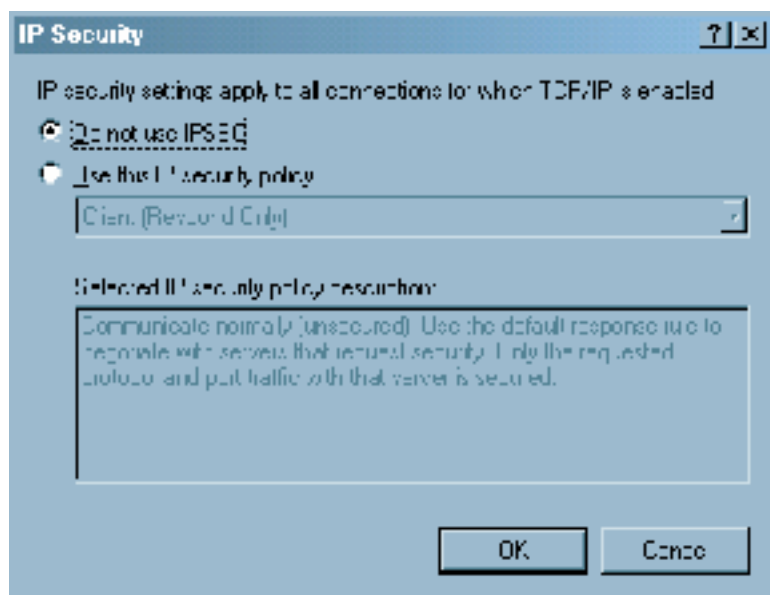
Step 13 - On the "Advanced TCP/IP Settings" click on the "Options" tab.



Step 14 - Ensure that the "IP security" optional setting was highlighted and click on the "Properties" button.



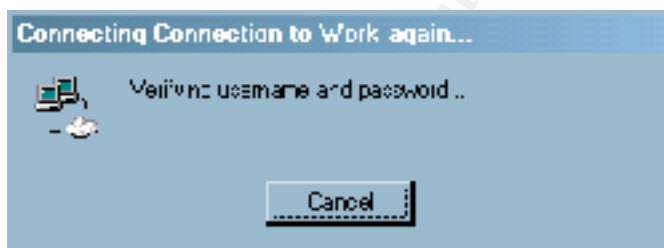
Step 15 - Ensure that the "Do not use IPSEC" option is selected. Press the "Ok" button.



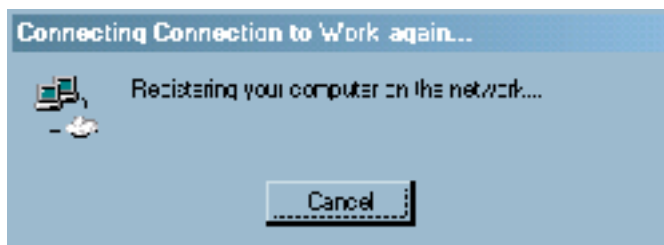
Step 16 - You will need to press the "Ok" buttons on the panels until to return to the screen shown below. You will need to type in your domain password in the "Password:" box. This is the password assigned to you on the GIAC-E network. The VPN Concentrator checks with the RSA/ACE server to ensure that you have the proper permissions and will prompt you for your pin and token combination before allowing you a VPN connection. Type in your password and press "Enter" or using the mouse left click on the "Connect" button.



Step 17 - You should now see the following panel appear. It will be on the screen for a few seconds as your user name and password are verified.



Step 18 - Next if you have made it though the user id and password authentication your computer will begin its registration on the GIAC-E network. A third panel will be displayed that indicates that your link is authenticated.

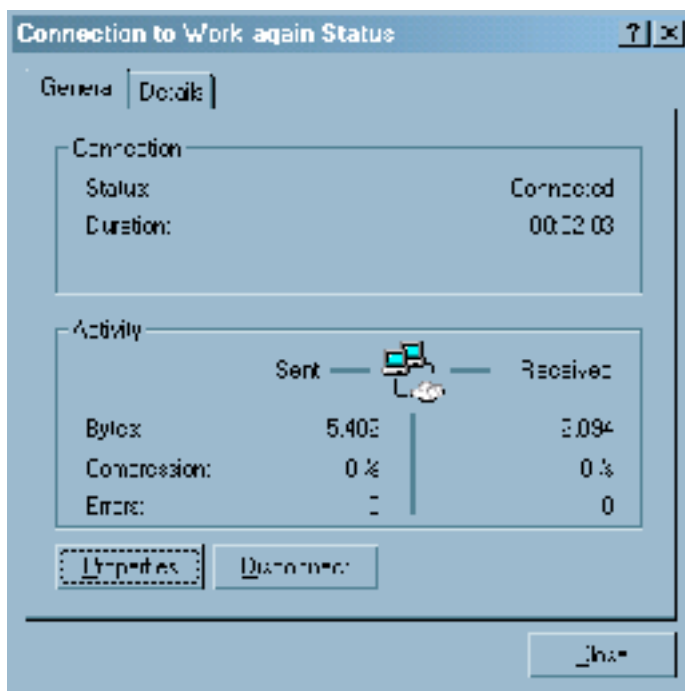


If you look at the bottom of your screen you should now see two little computer icons on the task bar. The first will be your network connection; the second will be your VPN connection. See here -----

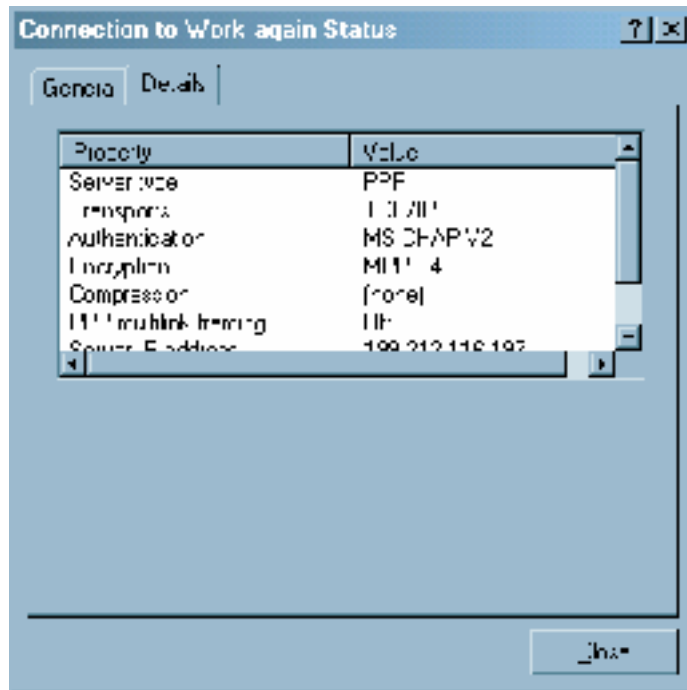


NOTE: This will only be displayed if you have the "show on Task bar" option selected in the protocol menu.

Click once on this icon and the following screen will appear:



This screen shows you the duration of your connection and the number of bytes that have been sent and received. By clicking on the "Details" tab you can verify that you are using 40-bit encryption by looking at the encryption line as shown below.



This concludes the PPTP workstation setup description for the GIAC-E environment.

4. Policy Tutorial

This tutorial will describe how to implement the policy built for the perimeter router. It is important to remember that the perimeter router will be used to enhance the security of the environment. This means that there are a few things that the router on its own can do to help protect the environment. By eliminating items into the network that are known to be inappropriate, we provide for better use of the resources between the perimeter router and the firewall and the firewall itself.

This is a "two-way-street", in that we can also eliminate things that should not be leaving our network to help protect the GIAC-E systems as well as possibly malicious traffic or noise.

The tutorial will be divided into 4 sections, general Access Control List (ACL) syntax, inbound ACL's, outbound ACL's and general router configuration steps.

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

4.1. ACL Syntax

The following example from the inbound access list will be used to describe the parts of an ACL

```
ip access-list extended ingress_filter
```

Before an ACL can be entered on a Cisco router, you must be logged in and changed to the enable mode. This will require administrative access to the router. You know you are at the enabled prompt of a Cisco router when after the name you see a '#' sign.

To allow you to input an ACL you can type in the line as listed above. This is like the title line of the ACL. The pieces of this line are described as follows:

Item	Description
ip	Internet Protocol, which is the kind of ACL you will be writing
access-list	Identifies that you will be writing an access list
extended	Indicates that this specific list will be an extended version which gives more options to configure than a 'standard' version
ingress_filter	This is the name or tag by which this specific ACL will be referenced and can be any name you choose. Remember to make the name somewhat descriptive

Table 2

Once this command has been entered, individual statements describing the rules that this ACL will contain will be added. The following is one rule of many that can be contained in a single ACL. A description of the parts of this rule follows on the next page:

```
deny ip 192.168.0.0 0.0.255.255 any log
```

Item	Description
deny	an ACL rule may be either a permit or deny rule. In this case we are going to deny something
ip	<p>This is the protocol that the rule will be applied against. The following is a list of the options for this field:</p> <ul style="list-style-type: none"> <0-255> An IP protocol number ahp Authentication Header Protocol eigrp Cisco's EIGRP routing protocol esp Encapsulation Security Payload gre Cisco's GRE tunneling icmp Internet Control Message Protocol igmp Internet Gateway Message Protocol igrp Cisco's IGRP routing protocol ip Any Internet Protocol ipinip IP in IP tunneling nos KA9Q NOS compatible IP over IP tunneling ospf OSPF routing protocol pcp Payload Compression Protocol pim Protocol Independent Multicast tcp Transmission Control Protocol udp User Datagram Protocol
192.168.0.0	<p>This is the network IP address from which this specific rule will be applied - or more commonly known as the "source" IP. The options allowed at this point in the rule are as follows:</p> <ul style="list-style-type: none"> A.B.C.D Source address any Any source host host A single source host
0.0.255.255	<p>The address mask that is applied to the source address. This allows for many IP addresses to be applied to this one statement. This specific mask makes this one rule effective for more than 65,000 IP addresses. The mask is the only option available at this point in the rule</p>
Any	<p>This is the network IP address to which the specific rule will be applied - or more commonly known as the "destination" IP. This key word means that it does not matter what the IP address of the destination is. The options allowed at this point in the rule are as follows:</p> <ul style="list-style-type: none"> A.B.C.D Destination address any Any destination host host A single destination host
log	<p>This key word indicates that if a packet matches this rule it will first be denied and then an entry to the router log will be made giving information from the packet. This is EXTREMELY useful information and need to be highly protected. The options at this point in the rule are as follows:</p> <ul style="list-style-type: none"> fragments Check non-initial fragments log Log matches against this entry log-input Log matches against this entry, including input interface precedence Match packets with given precedence value tos Match packets with given TOS value

Table 3

4.2. General ACL Assembly

Generally the ACL's of this nature are divided into three parts. The first part is to deny any of the traffic that we know is harmful or should not be entering the network. The second part is to explicitly permit the items that will be allowed further into the network. This does not guarantee that this item will be processed; it may be dropped at a further layer. Lastly, the final denies reminding us that anything that does not match a line in the ACL will be dropped. No rule is required for this to happen, it is how the ACL's work. To log these items, it is important to put an explicit deny at the end with a log parameter attached. See the following ingress filter as an example of general ACL assembly:

*

* Name and type of the ACL

*

ip access-list extended ingress_filter

*

* Denies

*

```
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 127.0.0.0 0.255.255.255 any log
deny ip 255.0.0.0 0.255.255.255 any log
deny ip 224.0.0.0 7.255.255.255 any log
deny ip host 0.0.0.0 any log
deny ip 198.161.153.0 0.0.0.255 any log
deny ip host 198.161.152.1 any log
```

*

* Items Permitted Further into the environment

*

```
permit tcp any host 192.168.153.2 gt 1023 established
permit ip any host 192.168.153.2
permit icmp any 198.161.153.0 0.0.0.255 3 0
permit icmp any 198.161.153.0 0.0.0.255 3 1
permit icmp any 198.161.153.0 0.0.0.255 3 3
permit icmp any 198.161.153.0 0.0.0.255 3 4
permit icmp any 198.161.153.0 0.0.0.255 3 13
permit icmp any 198.161.153.0 0.0.0.255 4
permit icmp any 198.161.153.0 0.0.0.255 11 0
```

*

* FINAL Denies

*

```
deny tcp any any eq 113
```

*

* Explicit Deny with Log parameter

*

```
deny ip any any log
```

4.3. Applying an Ingress/Egress ACL

Although ACL's can be applied in many places on a Cisco router, this section will demonstrate how to apply an Ingress and Egress ACL to the external interface of our perimeter router. This is the first point of contact that Internet traffic makes with the GIAC-E network – which is the reason, the perimeter specific ACL's are applied here.

Ingress implies that the ACL is written for incoming traffic. The following statements show how to apply the ACL called 'ingress_filter' to the outside interface of the Cisco router:

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

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

```
Router(config-if)#ip access-group ingress_filter in
```

```
Router(config-if)#exit
```

```
Router(config)#exit
```

```
Router#
```

To check that the ACL has been applied to the interface, we can show the running configuration and look for this command under the Ethernet 0 interface:

```
Router#show running-config
```

```
Building configuration...
```

```
Current configuration:
```

```
!
```

```
version 12.0
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
no service password-encryption
```

```
!
```

```
hostname Router
!
interface Ethernet0
ip address 192.168.152.1 255.255.255.0
ip access-group ingress_filter in
no ip directed-broadcast
no cdp enable
```

Notice the highlighted command, which is the one we just entered is applied to the Ethernet 0 Interface.

The same procedure is used to apply the Egress filtering, that filters out specific traffic from exiting the GIAC-E environment:

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface ethernet 0**

Router(config-if)#**ip access-group egress_filter out**

Router(config-if)#**exit**

Router(config)#**exit**

Router#

Notice the two changes highlighted here. The name of the filter is for the egress ACL and the filter is applied in the outward direction. Here's how the configuration on the Ethernet 0 interface looks now:

Router#**sh run**

Building configuration...

Current configuration:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
interface Ethernet0
ip address 192.168.152.1 255.255.255.0
ip access-group ingress_filter in
```

GCFW - V 1.6 Practical

```
ip access-group egress-filter out
no ip directed-broadcast
no cdp enable
!
```

The highlighted portion of the router configuration shows the egress filter applied in an outward direction.

4.4. Detailed description of router ACL's and general security commands

Next is a detailed description explaining what the lines of the ACL's and the general router commands are to perform.

Ingress Filter

*

* Name and type of the ACL identifying this particular one as Ingress

*

ip access-list extended ingress_filter

*

* Deny the RFC1918 values that should not be entering the GIAC Network – these are
*often used as spoofing addresses

*

```
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
```

*

* Deny the broadcast values that should not be entering the GIAC Network – these are
*often used to gather information or cause a number of replies with a single statement

*

```
deny ip 127.0.0.0 0.255.255.255 any log
deny ip 255.0.0.0 0.255.255.255 any log
deny ip 224.0.0.0 7.255.255.255 any log
```

*

* Deny packets without IP addresses

*

```
deny ip host 0.0.0.0 any log
```

*

* Deny packets from the outside with IP addresses that are used on the inside of the
*GIAC-E network

*

```
deny ip 198.161.153.0 0.0.0.255 any log
```

*

* Deny packets with IP addresses that are the same as that of the firewall

*

```
deny ip host 198.161.152.1 any log
```

*

* Permit any established TCP packets to the next security level (Checkpoint)

*

```
permit tcp any host 192.168.153.2 gt 1023 established
```

*

* Permit any IP packets that have not already been denied, to the next level

*

```
permit ip any host 192.168.153.2
```

*

* Permit in specific ICMP packets. These informational messages are useful for internal
* devices

*

```
permit icmp any 198.161.153.0 0.0.0.255 3 0 ** net-unreachable
permit icmp any 198.161.153.0 0.0.0.255 3 1 ** host-unreachable
permit icmp any 198.161.153.0 0.0.0.255 3 3 ** port-unreachable
permit icmp any 198.161.153.0 0.0.0.255 3 4 ** packet-too-big
permit icmp any 198.161.153.0 0.0.0.255 3 13 ** administratively-prohibited
permit icmp any 198.161.153.0 0.0.0.255 4 ** source-quench
permit icmp any 198.161.153.0 0.0.0.255 11 0 ** ttl-exceeded
```

*

* Deny Ident protocol. GIAC-E does not use it and it will add to the volume of log files
* so it is dropped and not logged. This may be modified as noisy protocols are
*discovered

*

```
deny tcp any any eq 113
```

*

- * Implicit Deny with a LOG to allow us to see what “else” is attempting to access the
- * GIAC-E perimeter

*

```
deny ip any any log
```

Egress Filter

*

- * Name and type of the ACL identifying this particular one as Egress

*

```
ip access-list extended egress_filter
```

*

- * Deny any RFC1918 source IP addresses from leaving the GIAC-E environment.
- * Helps prevent an internal resource becoming an amplifier.

*

```
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
```

*

- * Deny traffic from any internal station to an RFC1918 IP address

*

```
deny ip any 192.168.0.0 0.0.255.255 log
deny ip any 172.16.0.0 0.15.255.255 log
deny ip any 10.0.0.0 0.255.255.255 log
```

*

- * Deny any internal host the ability to respond with an ICMP message. Can give out
- * valuable information to a hacker

*

```
deny icmp any any log
```

*

* If the packet has not been dropped already and is coming from the External DMZ,
*permit it to leave the GIAC-E network.

*

```
permit ip 198.161.153.0 0.0.0.255 any
```

*

* Implicit deny of all other traffic – and log it using the MAC address of the machine that
*caused the deny. This will aid in identifying what machine has caused any log entries
*created by this rule.

*

```
deny ip any any log-input
```

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

General Commands

*
* Encrypt the service passwords on the router from being displayed.
*
`service password-encryption`
*
* Disable the use of Cisco Discovery protocol – will give out info to a hacker
*
`no cdp run`
*
* Disable the use of finger server protocol – will give out info to a hacker
*
`no service finger`
*
* Disable the use of small services for both TCP and UDP – Note this is off by default in
*this version of IOS, but it's a good idea to make sure these are off. Can be used to
*perform a denial of service attack
*
`no service udp-small-servers`
`no service tcp-small-servers`
*
* Do not permit any source to direct the routing
*
`no ip source-route`
*
* Do not permit the router to act as a bootp server
*
`no ip bootp server`
*
* Do not enable the WEB interface to the router
*
`no ip http server`
*
* Do not enable the Network Time Protocol server on the router
*
`no ntp master`
*
* Do not allow the router to look up names in the DNS
*
`no ip domain-lookup`
*
* Stop those unsightly console messages from showing up on the console
*
`no logging console`
*
* Send items that are to be logged to the buffer
*

```

logging buffered
*
* Include the current date/time with milliseconds and show the time zone. This is useful
* information if you are sending logging info to another sysadmin so that they know what
* time zone your logs came from and can translate that into their own time zone and thus
* pinpoint in their logs what might have happened. Do this for the logs and the debugs.
*

service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
*

* Set the time zone of the router
*

clock timezone MST -7
*

* Send all logs to a SYSLOG server with the listed IP – gets logs off of the router and to
* a place where they can be coordinated with other logs from other devices
*

logging 192.168.1.29
*

* Set the SNMP community string to something other than the default
*

snmp-server community c0vert RO 21
snmp-server trap-authentication
*

* Use a standard ACL to define who is a valid SNMP server. This stops others from
* using SNMP to gather info from SNMP the router
*

snmp-server tftp-server-list 2
*

* Identify the kinds of traps to send
*

snmp-server enable traps config
snmp-server enable traps snmp
*

* Identify the SNMP server to send the traps to
*

snmp-server host 192.168.1.30 c0vert
*

* ACL that defines who the valid SNMP device are
*

access-list 2 permit host 192.168.1.30
*

* Warning banners that identify this as a closed system and to direct them not to
* proceed unless they are specifically authorized to do so.
*

banner motd &

*****
* THIS IS A CLOSED SYSTEM *
*****

```

DO NOT Proceed any further unless you have the expressed
written permission from the system administrators

All attempts to access are logged and will be used to
prosecute those who have not been granted the above stated
permission to the fullest extent of the law

&

banner exec &

* THIS IS A CLOSED SYSTEM *

DO NOT Proceed any further unless you have the expressed
written permission from the system administrators

All attempts to access are logged and will be used to
prosecute those who have not been granted the above stated
permission to the fullest extent of the law

&

banner incoming &

* THIS IS A CLOSED SYSTEM *

DO NOT Proceed any further unless you have the expressed
written permission from the system administrators

All attempts to access are logged and will be used to
prosecute those who have not been granted the above stated
permission to the fullest extent of the law

&

Assignment 3 – Security Architecture Audit

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

1. Audit Plan

It is critical that once a firewall policy is created that it be checked to ensure that a configuration error will not leave the firewall, and thus those behind it, blatantly vulnerable to malicious activity. To audit the firewall policy it will be necessary to create a test to verify each rule. In this way it can be shown that the policy is acting as expected and will provide the level of security it was designed to perform. It would be ideal if a person other than the one who created the rule set audited the policy. This provides for impartiality and allows for another set of eyes to look over the work.

In a production environment it is likely that the newly created firewall/policy (this assumes that this firewall is a new install and not an upgrade to an existing policy) could be tested during normal business hours. For the most part another device (or possibly nothing at all) would be providing some sort of perimeter protection while this firewall was being installed. To that end, the use of security tools could be permitted at any time. A majority of the services could be mocked up and tested without disrupting production traffic.

An estimate of the cost of a this firewall audit would be as follows:

- | | |
|--|---------|
| ▪ review policy/creation of audit plan | 1 day |
| ▪ mock up services | 1 day |
| ▪ assemble/configure tools | .5 day |
| ▪ run tests | 1 day |
| ▪ create report | 1.5 day |

This puts the audit effort at approximately 5 man-days. Any services that need to be performed after hours would be charged for appropriately.

Once again the approach to this would be to first review the firewall policy as a paper review and identify if any errors exist. If an error is found it can be corrected and then a re-check of the paper policy would be performed. Once the paper review was completed a number of tests to verify each rule of the policy would be created which would include a number of rules that would exercise the "catch all" items of the policy. Then the actual running of the tests and tabulation of the results would provide a road map for any changes that would be required. The running of the tests and policy corrections may need multiple iterations to verify that the policy is functioning correctly. Once that auditor is satisfied that the policy is sound, it can be applied to the firewall and the firewall placed in service.

It is advisable to re-run the last test that was performed on the firewall on a regular basis (say every 3 months). By performing this step over time, any security holes that appear over time (via changes to the firewall policy) can be identified and corrected.

2. Audit Execution

The following is an example of the paper process that would be performed on the firewall policy:

Source	Destination	Service	Action	Track	Paper Check	Pass/Fail
Admin-users	FW1-SANS	FireWall1	Accept	Long	Permit a select few users to access the firewall using the firewall administration client	Pass
Any	FW1-SANS	Any	Drop	Alert	Deny any others from accessing the firewall and send an alarm if someone tries to access	Pass
External DMZ	Internal Broadcast	nbname nbdatagram	drop		Drop any netbios traffic that is floating around in the External_DMZ. This will just fill up the log and since it is already internal it can be ignored for the time being	Pass
Border_router Border Switch	Syslog-Server Trap-Receiver	syslog SNMP-trap	Accept	Long	Allow the Border router and switch access through the firewall to send traps and syslog information	Pass
Any	External-DNS-1 External-DNS-2	Domain-TCP Domain-UDP	Accept	Long	Permit any individuals to query the External DNS's	Pass
Any	WWW-Cluster	HTTP HTTPS	Accept	Long	Permit any individuals to use HTTP or HTTPS to the web cluster	Pass
Corporate_Net RAS Network	Any	HTTP HTTPS	Accept	Long	Permit the Corporate IP address range and the RAS IP address range access to the Internet	Pass
Time-Server	Any	ntp	Accept	Long	Permit the time server access to the internet for network time protocol	Pass
Any	Mail-Receiver	SMTP	Accept	Long	Allow incoming SMTP to the Mail receiver	Pass
Mail-Sender	Any	SMTP	Accept	Long	Allow outgoing SMTP from the Mail sender server	Pass
Any	VPN-1 VPN-2	IPSEC PPTP	Accept	Long	Permit any IP address using the IPSEC or PPTP suite of protocols to access the VPN servers	Pass
VPN-1 VPN-2	Any	IPSEC PPTP	Accept	Long	Permit the VPN server access to any IP when using the IPSEC or PPTP suite of protocols (only used when initiating a connection from inside)	Pass
A198.161.153.0	External DMZ	Any	Reject	Alert	Reject any attempts to access the external DMZ from the subnet that is proximal to the Checkpoint Firewall	Pass
Any	Any	Any	drop	Alert	Universal - drop everything else - REQUIRED	Pass

Table 4

Now that the paper check is satisfactorily completed, the mechanics of the physical audit of the firewall can begin.

Tool Selection

My preference would be to use tools from three different categories. The first category would be a commercially available perimeter-scanning tool like ISS's Internet Scanner or E-eye's Retina. The research team behind the products and their ability to find security holes is what is gained when one of these products is purchased. The second category of tool I would employ would be some freeware tools like SuperScan or Sam Spade. These tools are freely available and can provide good information when probing a perimeter. The third category of tool that would be useful here is items listed under the GPL. Things like NMAP, SATAN, SAINT, and NESSUS. These tools tend to have a large base of support to keep the code current and the vulnerabilities they can probe on the leading edge. Using tools from these three categories and comparing the results will help to eliminate false positive tests that a single product might show.

Another option would be to design tests using regular workstations and services to see how the firewall responds. For example, since rule 1 of the firewall policy allows a single user access to the firewall using the GUI application I configured my workstation with another IP address and attempted to access the firewall with the program. At the same time I ran a quick port scan against the internal address to see what might be available. Here are the log entries from that attempt:

0	15-Oct-01	16:50:39	FW1-SANS	control	ctl						
1	15-Oct-01	16:51:08	FW1-SANS	log	accept	FW1_mgmt	Admin-users	FW1-SANS	tcp	0	2932
2	15-Oct-01	16:51:37	FW1-SANS	log	accept	FW1_mgmt	Admin-users	FW1-SANS	tcp	0	2933
3	15-Oct-01	16:51:44	FW1-SANS	log	accept	FW1_mgmt	Admin-users	FW1-SANS	tcp	0	2934
4	15-Oct-01	16:52:01	FW1-SANS	log	accept	FW1_mgmt	Admin-users	FW1-SANS	tcp	0	2935
5	15-Oct-01	16:54:53	FW1-SANS	alert	drop	nbdatalogram	10.10.3.101	10.10.3.255	udp	15	nbdatalogram
6	15-Oct-01	16:55:09	FW1-SANS	alert	drop	snmp-trap	10.10.3.1	10.10.3.255	udp	15	7206
7	15-Oct-01	16:55:30	FW1-SANS	alert	drop		4692192.168.1.10	255.255.255.255	udp	15	1026
8	15-Oct-01	16:56:51	FW1-SANS	alert	drop	FW1_mgmt	192.168.1.10	FW1-SANS	tcp	2	1028
9	15-Oct-01	16:57:07	FW1-SANS	alert	drop	telnet	192.168.1.10	FW1-SANS	tcp	2	1030
10	15-Oct-01	16:57:27	FW1-SANS	alert	drop		192.168.1.10	FW1-SANS	icmp	2	
111	15-Oct-01	16:58:14	FW1-SANS	alert	drop		100192.168.1.10	FW1-SANS	tcp	2	1269
112	15-Oct-01	16:58:14	FW1-SANS	alert	drop	hostnames	192.168.1.10	FW1-SANS	tcp	2	1270
113	15-Oct-01	16:58:18	FW1-SANS	alert	drop	FW1_mgmt	192.168.1.10	FW1-SANS	tcp	2	1271
114	15-Oct-01	17:01:15	FW1-SANS	alert	drop		4692Admin-users	255.255.255.255	udp	15	1026
115	15-Oct-01	17:02:54	FW1-SANS	alert	drop	nbdatalogram	10.10.3.102	10.10.3.255	udp	15	nbdatalogram
116	15-Oct-01	17:02:56	FW1-SANS	log	accept	FW1_mgmt	Admin-users	FW1-SANS	tcp	0	1028
117	15-Oct-01	17:03:02	FW1-SANS	alert	drop	nbdatalogram	10.10.3.101	10.10.3.255	udp	15	nbdatalogram

Table 5

Line 1 to 4 of the log file listed above are examples of the single IP address that is allowed to access the firewall via the GUI (note this is configured at the command line and cannot be modified by the GUI). After changing the IP address to 192.168.1.10 I attempted to use the Policy Editor program and the result is shown in line 8. Rule 2

matched and the traffic was dropped. On the PC end I got no indication that the firewall was even present – the session just timed out.

Next I attempted to load up the Log Viewer and the result is shown on line 113, where the attempt was dropped and then an alert was logged. To make sure things were working correctly I changed my IP address back to the address that is allowed to use the software and re-connected to the firewall (see line 116 – about 4 min after trying the last failed attempt) to gather the logs. As is shown, I was accepted by the rule 1 and the login was recorded.

Author's note: During the course of this practical, I managed to acquire a Sun Ultra 1, with Solaris and a demo copy of Checkpoint V 4.1. The box came pre-configured with an internal IP address of 198.161.1.1/24 and a single IP address that the GUI would respond to (192.168.1.2). Normally this wouldn't be a problem because from the console, an additional address could be configured along with the external address of the Firewall. However, this specific device did not come with a monitor. Ok, shouldn't be a problem you say – just use a console cable, connect to the back of the device with a PC console and away you go. Well that's what I thought too, until I spent a tremendous amount of time attempting to get a console connection to no avail. It almost appears as though the console ports are disabled. I had 3 other people look at this and they couldn't get a console on the Ultra either.

Alright, what does this mean? Well, given that there is no external interface configured on my firewall and I am limited to the addresses that have already been assigned – I am unable to physically run tests from the outside of this device. My actual testing will only be done on the rules that are written to allow connections to the outside. This note is to inform the reader that a full range of test would be run from both inside and outside the firewall if it were configured to allow this using the model described in this assignment.

Listed below are the rest of the internal services tested to show that the specific services are nailed down to specific IP addresses and protocols.

Internal DNS to external query

25	16-Oct-01	10:20:52	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	nbname
26	16-Oct-01	10:20:57	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1027
27	16-Oct-01	10:21:27	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1028
28	16-Oct-01	10:21:33	FW1-SANS	alert	drop	nbdatalogram	10.10.3.102	10.10.3.255	udp	15	nbdatalogram
29	16-Oct-01	10:21:56	FW1-SANS	alert	drop	http	Internal-DNS-1	139.231.15.2	tcp	15	1029
30	16-Oct-01	10:22:41	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1030
31	16-Oct-01	10:22:59	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1031
32	16-Oct-01	10:23:02	FW1-SANS	alert	drop	http	Internal-DNS-1	139.12.24.3	tcp	15	1032
33	16-Oct-01	10:23:16	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1033
34	16-Oct-01	10:23:33	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1034
35	16-Oct-01	10:23:50	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1035
36	16-Oct-01	10:24:07	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1036
37	16-Oct-01	10:24:13	FW1-SANS	alert	drop	telnet	Internal-DNS-1	FW1-SANS	tcp	2	1037
38	16-Oct-01	10:24:48	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1038
39	16-Oct-01	10:25:16	FW1-SANS	alert	drop	ftp-data	Internal-DNS-1	12.3.4.5	tcp	15	1039
40	16-Oct-01	10:26:01	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	1040
41	16-Oct-01	10:26:18	FW1-SANS	alert	drop	nbname	Internal-DNS-1	192.168.5.255	udp	15	nbname
42	16-Oct-01	10:26:21	FW1-SANS	log	accept	domain-udp	Internal-DNS-1	199.185.220.36	udp	6	nbname
43	16-Oct-01	10:26:43	FW1-SANS	alert	drop	ftp	Internal-DNS-1	12.1.2.3	tcp	15	1041

Above is a list of log entries created by the Internal DNS device. As can be seen the firewall is allowing UDP name lookups from the Internal DNS. The lines in red represent a few services that were attempted from the Internal DNS that were disallowed by the firewall policy including http, telnet and ftp/ftp-data.

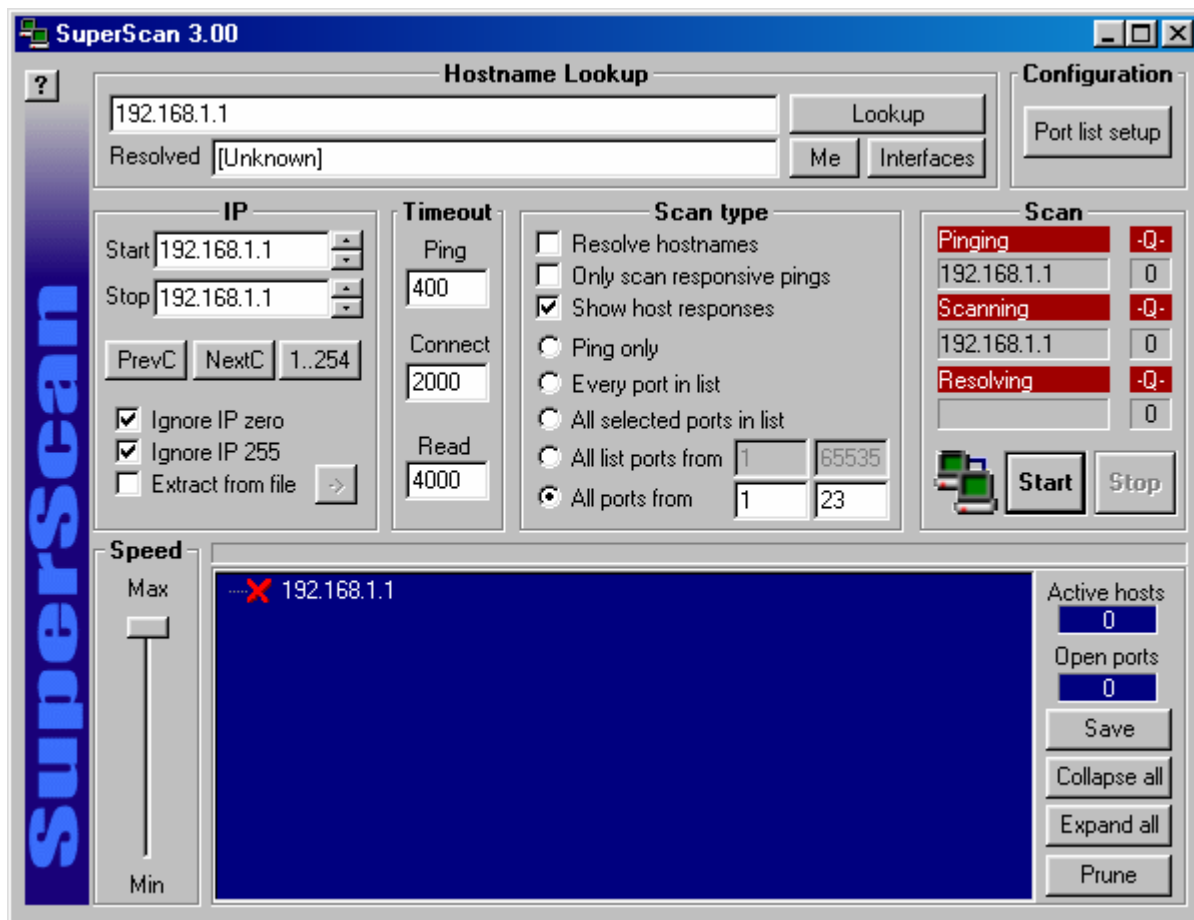
Corporate Network/RAS Network access to the Internet

13	16-Oct-01	10:35:45	FW1-SANS	log	accept	https	192.168.3.10	12.1.2.3	tcp	8	1028
14	16-Oct-01	10:35:55	FW1-SANS	log	accept	http	192.168.3.10	12.1.2.3	tcp	8	1029
15	16-Oct-01	10:36:07	FW1-SANS	alert	drop	ftp	192.168.3.10	12.1.2.3	tcp	15	1030
16	16-Oct-01	10:36:35	FW1-SANS	alert	drop	domain-udp	192.168.3.10	199.185.220.36	udp	15	1032
17	16-Oct-01	10:36:52	FW1-SANS	alert	drop	nbname	192.168.3.10	192.168.3.255	udp	15	nbname
18	16-Oct-01	10:36:54	FW1-SANS	alert	drop	domain-udp	192.168.3.10	199.185.220.36	udp	15	nbname
19	16-Oct-01	10:37:26	FW1-SANS	alert	drop	telnet	192.168.3.10	FW1-SANS	tcp	2	1033
20	16-Oct-01	10:38:29	FW1-SANS	alert	drop		192.168.3.10	FW1-SANS	icmp	2	
21	16-Oct-01	10:38:30	FW1-SANS	alert	drop	tcpmux	192.168.3.10	FW1-SANS	tcp	2	1034
22	16-Oct-01	10:38:30	FW1-SANS	alert	drop		2 192.168.3.10	FW1-SANS	tcp	2	1035
23	16-Oct-01	10:38:30	FW1-SANS	alert	drop		3 192.168.3.10	FW1-SANS	tcp	2	1036
24	16-Oct-01	10:38:30	FW1-SANS	alert	drop		4 192.168.3.10	FW1-SANS	tcp	2	1037
25	16-Oct-01	10:38:31	FW1-SANS	alert	drop		5 192.168.3.10	FW1-SANS	tcp	2	1038
26	16-Oct-01	10:38:31	FW1-SANS	alert	drop		6 192.168.3.10	FW1-SANS	tcp	2	1039
27	16-Oct-01	10:38:31	FW1-SANS	alert	drop	echo	192.168.3.10	FW1-SANS	tcp	2	1040
28	16-Oct-01	10:38:31	FW1-SANS	alert	drop		8 192.168.3.10	FW1-SANS	tcp	2	1041
29	16-Oct-01	10:38:31	FW1-SANS	alert	drop	discard	192.168.3.10	FW1-SANS	tcp	2	1042
30	16-Oct-01	10:38:31	FW1-SANS	alert	drop		10 192.168.3.10	FW1-SANS	tcp	2	1043
31	16-Oct-01	10:38:31	FW1-SANS	alert	drop	systat	192.168.3.10	FW1-SANS	tcp	2	1044
32	16-Oct-01	10:38:31	FW1-SANS	alert	drop		12 192.168.3.10	FW1-SANS	tcp	2	1045
33	16-Oct-01	10:38:31	FW1-SANS	alert	drop	daytime	192.168.3.10	FW1-SANS	tcp	2	1046
34	16-Oct-01	10:38:31	FW1-SANS	alert	drop		14 192.168.3.10	FW1-SANS	tcp	2	1047
35	16-Oct-01	10:38:31	FW1-SANS	alert	drop	netstat	192.168.3.10	FW1-SANS	tcp	2	1048
36	16-Oct-01	10:38:31	FW1-SANS	alert	drop		16 192.168.3.10	FW1-SANS	tcp	2	1049
37	16-Oct-01	10:38:31	FW1-SANS	alert	drop		17 192.168.3.10	FW1-SANS	tcp	2	1050
38	16-Oct-01	10:38:31	FW1-SANS	alert	drop		18 192.168.3.10	FW1-SANS	tcp	2	1051
39	16-Oct-01	10:38:31	FW1-SANS	alert	drop	chargen	192.168.3.10	FW1-SANS	tcp	2	1052
40	16-Oct-01	10:38:31	FW1-SANS	alert	drop	ftp-data	192.168.3.10	FW1-SANS	tcp	2	1053
41	16-Oct-01	10:38:31	FW1-SANS	alert	drop	ftp	192.168.3.10	FW1-SANS	tcp	2	1054
42	16-Oct-01	10:38:31	FW1-SANS	alert	drop		22 192.168.3.10	FW1-SANS	tcp	2	1055
43	16-Oct-01	10:38:32	FW1-SANS	alert	drop	telnet	192.168.3.10	FW1-SANS	tcp	2	1056

The logs above show that a user from the corporate network is allowed HTTP and HTTPS outbound from the network but has no access to telnet to the firewall or any TCP service from ports 1-25. Below are the logs for a RAS user. A short scan was run with SuperScan as is shown on the screen capture on the next page.

7	16-Oct-01	10:46:40	FW1-SANS	log	accept	http	192.168.4.10	12.3.2.1	tcp	8	1026 hme0
8	16-Oct-01	10:46:55	FW1-SANS	log	accept	https	192.168.4.10	12.4.3.2	tcp	8	1027 hme0
9	16-Oct-01	10:47:13	FW1-SANS	alert	drop	ftp	192.168.4.10	12.4.3.2	tcp	15	1028 hme0
10	16-Oct-01	10:48:00	FW1-SANS	alert	drop	nbdatagram	10.10.3.101	10.10.3.255	udp	15	nbdatagram hme0
11	16-Oct-01	10:48:00	FW1-SANS	alert	drop		192.168.4.10	FW1-SANS	icmp	2	hme0
12	16-Oct-01	10:48:01	FW1-SANS	alert	drop	nbdatagram	10.10.3.102	10.10.3.255	udp	15	nbdatagram hme0
13	16-Oct-01	10:48:01	FW1-SANS	alert	drop	tcpmux	192.168.4.10	FW1-SANS	tcp	2	1029 hme0
14	16-Oct-01	10:48:01	FW1-SANS	alert	drop		2 192.168.4.10	FW1-SANS	tcp	2	1030 hme0
15	16-Oct-01	10:48:01	FW1-SANS	alert	drop		3 192.168.4.10	FW1-SANS	tcp	2	1031 hme0
16	16-Oct-01	10:48:01	FW1-SANS	alert	drop		4 192.168.4.10	FW1-SANS	tcp	2	1032 hme0

17	16-Oct-01	10:48:01	FW1-SANS	alert	drop		5	192.168.4.10	FW1-SANS	tcp	2	1033	hme0
18	16-Oct-01	10:48:02	FW1-SANS	alert	drop		6	192.168.4.10	FW1-SANS	tcp	2	1034	hme0
19	16-Oct-01	10:48:02	FW1-SANS	alert	drop	echo		192.168.4.10	FW1-SANS	tcp	2	1035	hme0
20	16-Oct-01	10:48:02	FW1-SANS	alert	drop		8	192.168.4.10	FW1-SANS	tcp	2	1036	hme0



This tool can be found at: <http://www.foundstone.com/rdlabs/tools.php>

Time Server access to external time services

1	16-Oct-01	10:59:24	FW1-SANS	alert	drop	domain-udp	Time-Server	198.80.55.1	udp	15	1030	hme0	
2	16-Oct-01	10:59:51	FW1-SANS	log	accept	ntp	Time-Server	12.3.2.1	tcp	9	1031	hme0	
3	16-Oct-01	10:59:51	FW1-SANS	log	accept		FW1-SANS	Time-Server	icmp	0		hme0	
4	16-Oct-01	11:00:20	FW1-SANS	alert	drop	http	Time-Server	12.4.3.2	tcp	15	1032	hme0	
5	16-Oct-01	11:01:05	FW1-SANS	alert	drop	https	Time-Server	174.2.3.4	tcp	15	1033	hme0	
6	16-Oct-01	11:01:40	FW1-SANS	alert	drop		161	Time-Server	196.32.4.5	tcp	15	1034	hme0
7	16-Oct-01	11:02:27	FW1-SANS	alert	drop		162	Time-Server	194.2.3.4	tcp	15	1035	hme0
8	16-Oct-01	11:03:00	FW1-SANS	alert	drop	nbdatagram	10.10.3.101	10.10.3.255	udp	15	nbdatagram	hme0	
9	16-Oct-01	11:03:01	FW1-SANS	alert	drop	nbdatagram	10.10.3.102	10.10.3.255	udp	15	nbdatagram	hme0	
10	16-Oct-01	11:06:46	FW1-SANS	alert	drop	nbdatagram	10.10.3.101	10.10.3.255	udp	15	nbdatagram	hme0	
11	16-Oct-01	11:07:06	FW1-SANS	alert	drop	pop-3	Time-Server	23.4.5.6	tcp	15	1036	hme0	

The time server also showed that it was permitted to make an NTP request out and other services were not permitted.

Mail Sender access to SMTP outbound

2	16-Oct-01	11:11:29	hme0	FW1-SANS	log	accept	mail	Mail-Sender	203.4.5.6	tcp	11	1025
3	16-Oct-01	11:11:29	hme0	FW1-SANS	log	accept		FW1-SANS	Mail-Sender	icmp	0	
4	16-Oct-01	11:12:03	hme0	FW1-SANS	alert	drop	pop-3	Mail-Sender	203.4.5.6	tcp	15	1026
5	16-Oct-01	11:12:45	hme0	FW1-SANS	alert	drop	http	Mail-Sender	203.4.5.6	tcp	15	1027
6	16-Oct-01	11:12:58	hme0	FW1-SANS	alert	drop	https	Mail-Sender	203.4.5.6	tcp	15	1028
7	16-Oct-01	11:13:15	hme0	FW1-SANS	alert	drop	ftp	Mail-Sender	203.4.5.6	tcp	15	1029

The Mail-sender is also shown in the logs having the ability to use SMTP outbound but not permitted to do POP3, http/s, or ftp. The firewall policy makes this a single function device.

VPN server Access to PPTP services outbound

1	16-Oct-01	11:17:07	hme0	FW1-SANS	alert	drop		47 VPN-1	12.4.3.2	tcp	15	1025
2	16-Oct-01	11:17:35	hme0	FW1-SANS	log	accept	pptp-tcp	VPN-1	12.4.3.2	tcp	13	1026
3	16-Oct-01	11:17:35	hme0	FW1-SANS	log	accept		FW1-SANS	VPN-1	icmp	0	
9	16-Oct-01	11:28:40	hme0	FW1-SANS	alert	drop	ldap	VPN-1	12.4.3.2	tcp	15	1027
10	16-Oct-01	11:29:34	hme0	FW1-SANS	alert	drop		500 VPN-1	12.4.3.2	tcp	15	1028
11	16-Oct-01	11:30:06	hme0	FW1-SANS	alert	drop		50 VPN-1	12.4.3.2	tcp	15	1029
15	16-Oct-01	11:41:44	hme0	FW1-SANS	alert	drop		389 VPN-1	12.4.3.2	udp	15	1030
16	16-Oct-01	11:42:20	hme0	FW1-SANS	log	accept	IKE	VPN-1	12.4.3.2	udp	13	1031
17	16-Oct-01	11:42:20	hme0	FW1-SANS	log	accept		FW1-SANS	VPN-1	icmp	0	

The VPN server logs are interesting. At first it appears as though ESP, GRE and LDAP protocols are not operating correctly. But on further examination, these requests are for TCP port 50,47 and 389 respectively but, ESP is **IP** protocol 50, GRE is **IP** protocol 47 and LDAP uses UDP 389. Once this was determined the appropriate tools can be set up to check the correct protocols. For example, with a UDP port scanner WUPS, it can be seen that IKE (see: <http://ntsecurity.nu/toolbox/wups>) which is UDP port 500 is functional.

3. Audit Evaluation

The review of the firewall policy showed a couple of areas where the policy needed updating.

The first is that there is no rule to provide for the external DNS to make it's Domain requests. This would prove rather problematic in that nothing in the external DMZ would be able to lookup domain names. The recommendation here would be to add the External_DNS's to the source column of rule 6 that currently allows Internal_DNS access out for domain lookups.

The second thing that was found was that there was a much broader range of "noise" from the inside of the network than first expected.

18	16-Oct-01	11:42:46	hme0	FW1-SANS	alert	drop	Nbdatagram	10.10.3.101	10.10.3.255	udp	15	nbdatagram
----	-----------	----------	------	----------	-------	------	------------	-------------	-------------	-----	----	------------

With this traffic no being useful to determine problems, I would tend to broaden the filter that drops these frames and make sure not to log them.

Next, I realized that there was no provision for the corporate user community to be able to download (FTP) anything from the Internet. Now, this could be a good thing in that employees cannot accidentally download a malicious program and execute it from the inside. However, in reality, this is not very realistic. Many files on the internet need to use FTP, like PDF files, product updates, patches and the like. Therefore, another recommendation (or fix) would be to allow FTP to the Corporate Network and RAS networks.

Looking at the items discovered during the audit of the policy shows that even looking at it on paper, it may look correct, but until you actually attempt some of the services, you may not be aware of things you have missed.

As far as architecture changes, maybe because I was unable to run a physical check from the outside of the firewall, I was not able to come up with any compelling reasons to change the design. Overall, the architecture itself seems solid even though the policy requires an update or two.

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

Assignment 4 – Design Under Fire

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

1. Chosen Design

The following link will lead you to the GCFW practical for Mr. Keith Wilcox dated September 23,2000.

http://www.sans.org/y2k/practical/Keith_Wilcox.doc

[The diagram from this practical can be found on the next page]

2. Three Firewall Vulnerabilities

The following vulnerabilities were found for the Checkpoint Firewalls listed in this practical

2.1.1. Vulnerability 1

Spoofed UDP packer vulnerability URL:

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=1419>

A description from Security Focus is as follows:

If Checkpoint Firewall-1 receives a number of spoofed UDP packets with Source IP = Destination IP, the firewall (and likely the machine hosting it) crashes.

NOTE:

This vulnerability while being posted to Bugtraq is currently being denied as a problem by the vendor. The following text was sent to SecurityFocus.

"Checkpoint takes this and all other possible security issues very seriously. In this case, we have made every effort to work with the authors and reproduce the reported behavior. However, even after extensive testing we have been unable to reproduce this vulnerability. This testing was done both with and without IP Spoofing protection enabled, with the provided source code and other tools. The authors could not provide us with valid FireWall-1 version information, although 3.0, 4.0, and 4.1 are listed as vulnerable; please note that version 3.0 is no longer supported on non-embedded platforms.

At this time, Checkpoint does not believe this is an actual vulnerability. If anyone has successfully reproduced this condition or has further information, please contact SECURITY-ALERT@Checkpoint.com."

2.1.2. Vulnerability 2

Fragmented packet denial of service URL:

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1312>

Description of vulnerability from Security Focus:

By sending illegally fragmented packets directly to or routed through Checkpoint FireWall-1, it is possible to force the firewall to use 100% of available processor time logging these packets. The FireWall-1 rule base cannot prevent this attack and it is not logged in the firewall logs.

Code to test vulnerability:

<http://www.securityfocus.com/data/vulnerabilities/exploits/jolt2.c>

2.1.3. Vulnerability 3

FTPd vulnerability in Checkpoint URL:

<http://www.securityfocus.com/bid/979>

Description from Security Focus:

A vulnerability exists in the way that Checkpoint FireWall-1 handles packets sent from an FTP server to a connecting client. An attacker may be able to exploit this weakness to establish connections to any machine residing behind a FireWall-1 machine, or send packets in to a network protected by a FireWall-1.

FireWall-1 monitors packets from the FTP server to the client, looking for the string "227" at the beginning of each packet. If FW-1 finds a packet which matches this criteria, it will extract the destination address and port, verify that the specified destination address matches the source of the packet, and allow TCP connections through the firewall to the destination IP and port.

In FireWall-1 4.0, these TCP connections can only send data in one direction. Under FireWall-1 3.0 and prior, this limitation does not exist. In addition, under FW-1 4.0 the data cannot be travelling to a port that is defined in FW-1's list of well-known TCP services.

2.1.4. Firewall Vulnerability Attack

The nicest of the three vulnerabilities reported here is the first one. With the code supplied at: <http://www.securityfocus.com/data/vulnerabilities/exploits/cpd.c> this exploit could be tested on a local platform, if available, and then launched against this firewall. It assumes that the anti-spoofing mechanism has not been turned on.

What might be more interesting is to attempt the compromise of one of the WEB servers in the DMZ and then use this exploit against the internal firewall. It is interesting to note here that the external and internal firewalls are the same platform - which means if vulnerability is found on this specific product, it will be useable against two levels of this architecture.

It is also noted that there does not appear to be any work done on the external router that borders this environment. It may be possible to create a DOS condition using UDP small services directed at the router or using recent vulnerabilities on IOS.

3. Denial of Service Attack

I don't claim to be a white hat hacker, although I must admit that the more I learn about the workings of some of the security products, the more I realize how much you need to understand from the dark side to be successful in authoring some kind of compromise. Given that information, there are a few ideas I would use to deny the service at this specific site.

DDOS #1

I would gather information on sites that I could use as amplifiers (see <http://www.powertech.no/smurf/>) and with this information I would direct half of the 50 drones to send TCP SYN messages to various amplifiers while at the same time have the other half of the drones to send ICMP source quench messages with spoofed addresses from the amplifiers. This would create a large volume of traffic and at the same time would try and slow down the response with the ICMP messages.

I would make sure that the systems targeted in the subject network were alive and accepting information through the firewall.

DDOS # 2

Knowing that the Checkpoint firewall product has an anti-SYN flood mechanism built in, I would tend to use other protocols like UDP or ICMP and attempt to get them through the firewall by using fragmentation.

One example might be to have all of the drones attempt to walk the MIB tree of hosts that are allowed through the firewall. This would create large volumes of traffic and possibly flood the link out of the network with the responses.

DDOS # 3

Repeatedly send multiple port 80 requests (from each of the drones) with a spoofed address of the firewall's outside and inside interfaces. If the firewall policy does not drop these requests, or the perimeter router is not watching for this kind of packet, you might be successful in overloading the Internet connection.

Protecting against DDOS

There are a number of resources that describe ways to help protect against Denial of Service attacks. Unfortunately, they are extremely difficult to eliminate. The best method to help eliminate this kind of activity is to ensure that your specific environment is properly protected and patched to protect against becoming an un-willing participant in a DDOS attack on another system.

Rather than list all the different things that can be done, some resources are listed here for further reading to help minimize the effects as best as possible. Many of the suggestions in these documents are listed here as part of the security design.

<http://www.paraprotect.com/Resource/Security-Tips/Distributed-Denial-of-Service-Check-List.htm>

<http://www.cisco.com/warp/public/707/newsflash.html>

http://www.sans.org/ddos_roadmap.htm

<http://www.sans.org/dosstep/>

<http://www.networkmagazine.com/article/NMG20000512S0041>

4. Internal Host Attack Plan

Given the architecture listed here the host that I would attempt to attain control of is a WEB server.

The reasons include:

- Probably updated with new HTML code all the time and may not be checked for security holes on a regular basis
- It is open from the perimeter
- Use automated tools like Whisker <http://www.wiretrip.net/rfp/p/doc.asp/i2/d21.htm> to help identify what vulnerabilities may exist.
- Usually there is lots of traffic to a WEB server so my attempts may be hidden amongst all the other requests.

My plan for this would be:

- Target and perimeter investigation using automated tools
- Specific intelligence gathering on systems that appear interesting or have given up some information on previous attempts.
- Research on known vulnerabilities based on information gathered from the previous steps.
- Gather specific tools to accomplish the task.
- Possibly mock up the scenario in a lab and work at breaking in and finding a method of breach.
- Compromise a host on the @home network to use as the attacker
- Launch the attack.

References

Page 7 - Foundry Networks Server Iron Information

<http://www.foundrynetworks.com/products/webswitches/serveriron/datasheets.html>

Page 11 - RSA, Secure ID Token Information

<http://www.securid.com/products/securid/tokens.html>

Page 11 - 2000 YEAR-IN-REVIEW; The Year in Computer Crime*
BY M.E. KABAY AND LAWRENCE M. WALSH

<http://www.infosecuritymag.com/articles/december00/features.shtml>

Page 16 - Border Security Reference Material

http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

<http://www.cisco.com/warp/public/707/21.htm>

<http://pasadena.net/cisco/secure.html> and

The GCFW course material Track 2 - Firewalls and Perimeter Protection, 2.3 Firewalls
102: Perimeter Protection and Defense in Depth

Page 56 - SuperScan tool link

<http://www.foundstone.com/rdlabs/tools.php>

Page 58 - WUPS UDP Scanning tool link:

<http://ntsecurity.nu/toolbox/wups>

Page 60 - Practical for Mr. Keith Wilcox

http://www.sans.org/y2k/practical/Keith_Wilcox.doc

Page 61 - Firewall Vulnerability # 1

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=1419>

Page 62 - Firewall Vulnerability # 2

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1312>

Page 62 - Link to code for Vulnerability # 2

<http://www.securityfocus.com/data/vulnerabilities/exploits/jolt2.c>

Page 62 - Firewall Vulnerability # 3

<http://www.securityfocus.com/bid/979>

Page 63 - Code for Firewall Vulnerability # 1

<http://www.securityfocus.com/data/vulnerabilities/exploits/cpd.c>

Page 63 - List of Smurf amplification sites

<http://www.powertech.no/smurf/>

Page 64 – Links to Ddos protection reading

<http://www.paraprotect.com/Resource/Security-Tips/Distributed-Denial-of-Service-Check-List.htm>

<http://www.cisco.com/warp/public/707/newsflash.html>

http://www.sans.org/ddos_roadmap.htm

<http://www.sans.org/dosstep/>

<http://www.networkmagazine.com/article/NMG20000512S0041>

Page 65 - Link to Whisker web server scanning tool

<http://www.wiretrip.net/rfp/p/doc.asp/i2/d21.htm>

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