



# 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.

---

**Bringing good fortune to GIAC Enterprises**

**Or**

**"Man who leave door open get strange visitors"**

**Firewalls, Perimeter Protection, and VPN's GCFW  
Practical Assignment  
Version 1.5e  
SANS 2001 - May 2001**

**Garth Howe  
August 2001**

## Table of Contents

### Assignment 1 - Security Architecture

4	
1.1	Introduction to GIAC
4	
1.2	Design Philosophy 4
1.3	Guide to IP Addresses on the GIAC Network 5
1.4	Network Functional Overview
6	
1.5	Network Security Overview
6	
1.6	Hardware and Software Choices 8
	1.6.1 Cisco 1751 router - dual Ethernet interfaces
8	
	1.6.2 Firewalls - Netscreen Technologies Netscreen Firewall 8
	1.6.3 Ethernet Repeaters - Hewlett Packard Procurve 9
	1.6.4 Ethernet Switches - Hewlett Packard Procurve
10	
	1.6.5 Intrusion Detection - Network Ice Corporation ICEpac 10
	1.6.6 Host OS - Microsoft Windows 2000 11

### Assignment 2 - Security Policy 13

2.1	Defining Transparent Mode, and Introduction to Netscreen GUI
13	
2.2	Implementing the Accounting Firewall and Introduction to CLI
18	
	2.2.1 Defining the Address of a Host 19
	2.2.2 Setting up a Schedule 21
	2.2.3 Putting the Policy command line together
21	
	2.2.4 Policy Order - Importance and Reorganization 22
	2.2.5 Pulling it all together - CLI Configuration 23
2.3	Setting up the IT Firewall - Configuration gets more challenging
26	
	2.3.1 Defining Custom Services 26
	2.3.2 Custom Services Defined on the IT Firewall
27	
	2.3.3 Defining Custom Service Groups

27	2.3.4 Custom Service Groups Defined on the IT Firewall	
28	2.3.5 Defining Custom Group Addresses	28
	2.3.6 Custom Group Addresses Defined on the IT Firewall	
29	2.3.7 Time Scheduling Revisted	
30	2.3.8 Bringing the IT Firewall to life - creating the policies	
30	2.4 Setting up the External Firewall - The DMZ and Mapped IP	
33	2.4.1 Defining the Host Addresses, and Groups	34
	2.4.2 Setting a Time Schedule	34
	2.4.3 Defining and Implementing the External Firewall Policies	35
2.5	Setting up the VPN on the External Firewall	38
	2.5.1 Defining the VPN technology used	39
	2.5.2 Step by Step - Setting up Bob Thompson's VPN access	43
2.6	Securing the Netscreen Firewall	
	45	
2.7	Enabling Basic IDS Functionality with the Netscreen	
	45	
2.8	Tips regarding Netscreen documentation	46
2.9	Configuring the Cisco 1751 router	47
	2.9.1 Securing the Cisco router	47
	2.9.2 Filtering traffic with the Router - Access Lists Rules	49
	2.9.3 Blocking illegal addresses incoming to our network	50
	2.9.4 Allowing our Internal traffic Out	51
Assignment 3 - Auditing the External Firewall at GIAC Enterprises		
52		
3.1	Planning the Assessment	52
3.2	Time required for testing	53
3.3	Tools used for testing	54

3.4	Implementing the Assessment on the External Firewall	55
3.5	Perimeter Analysis	58
3.5.1	Multiple firewall OS's	58
3.5.2	Use of alternative firewall technologies	59
3.5.3	Implementing high availability for the firewall	59
3.5.4	An alternative "almost high availability" solution	59
3.5.5	Determining if there are attack patterns outside	59
Assignment 4 - Design Under Fire		60
4.1	Basic design flaw of network	60
4.2	Border routers configuration affects unprotected hosts	61
4.3	Intelligent Switch is itself a target of attack	61
4.4	An attack against the firewall itself	61
4.5	Denial of Service Attack	62
4.6	Attack plan to compromise an internal system through perimeter	63
List of References and Further Reading		65
Special Thanks		68

## Assignment 1 - Security Architecture

### 1.1 - Introduction to GIAC

GIAC Enterprises is a growing Internet startup expecting to earn \$200 million per year in online sales of fortune cookie sayings. As opposed to being a producer of these sayings, they purchase most of the sayings from independent authors. These sayings are then sorted, catalogued, and resold online to various fortune cookie manufacturers, who do their own printing. So GIAC functions as a clearinghouse for fortune cookie sayings.

Due to the structure of their business, they run a lean operation with only about 60 employees. They do however have a large number of remote "quasi employees" in all the independent authors they deal with. Combining these authors with GIAC's Customers, and Partners, means that several hundred more individuals need access to GIAC's network. So GIAC Enterprises may be a

physically small organization, but their network reflects the need to support many hundreds of users.

## 1.2 - Design Philosophy

The owners of *GIAC* acknowledge that security is a required component of their business. However, they do not feel that as a supplier of fortune cookie sayings, any hacker would spend a significant amount of effort on their site. To this end they have requested a safe design, which will not cost a fortune, nor require a small army of IT people to manage. Additionally they have requested that the design, and choice of products, allow for future expansion, without having to discard what is done today.

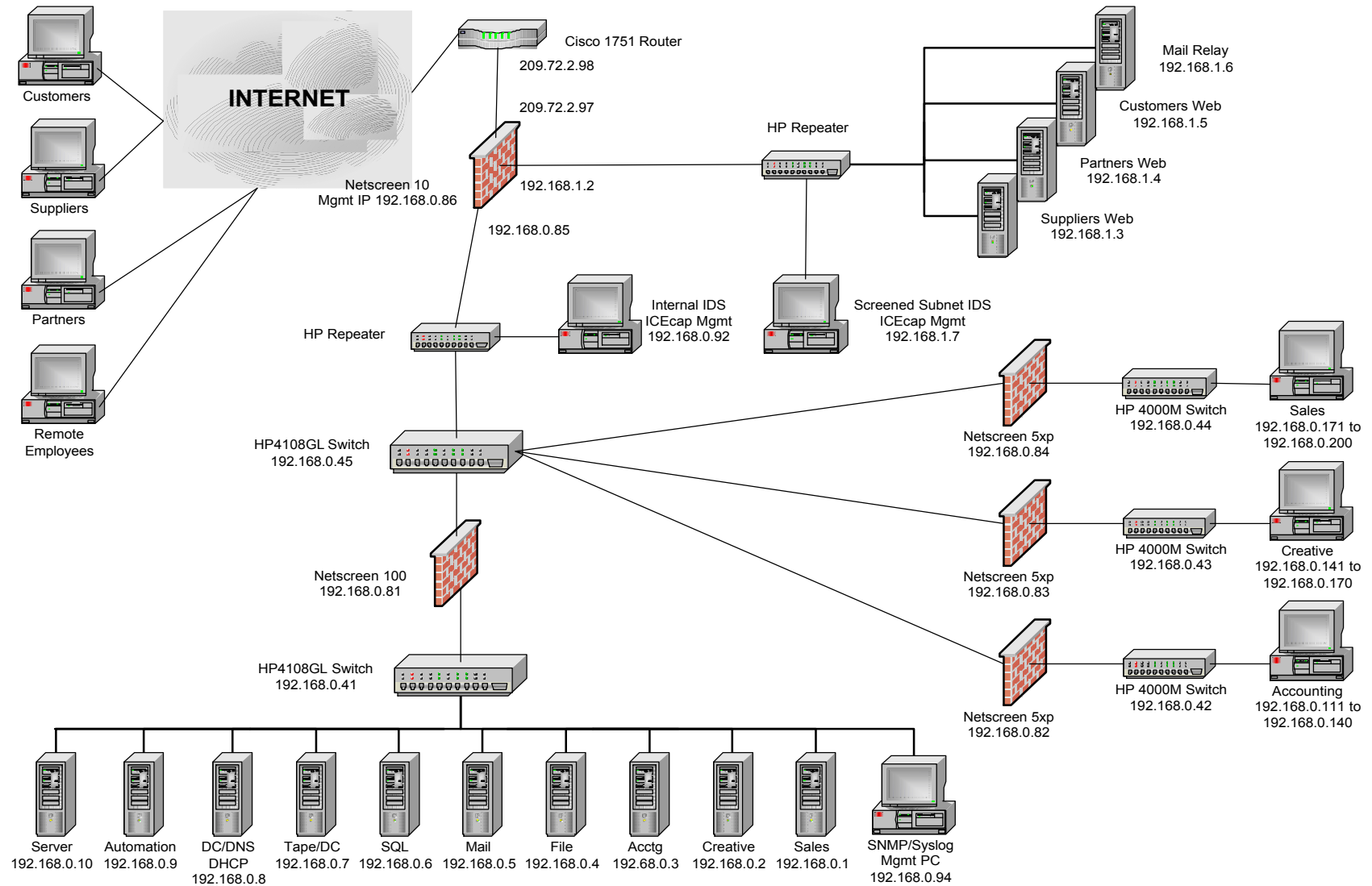
When wishing to protect physical premises from theft, it is common to divide your building into compartments, to slow down, and discourage the thief, hopefully stopping him from taking all of your assets. This network design reflects this same policy, by dividing it into compartments. Each compartment is isolated by a firewall and its policies.

Being a private company means you can dictate what services that staff are allowed to access. To this end, the network has been designed to allow only necessary traffic to pass between each compartment.

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

## Illustration 1 - GIAC Enterprises Network

### GIAC Enterprises Network Design



### 1.3 Guide to IP Addresses on the GIAC Network

Public IP addresses (Outside of External Firewall)

209.72.2.97 - 209.72.2.110      Mask 255.255.255.240

Screened Subnet Addresses (on External Firewall)

192.168.1.1 - 192.168.1.254      Mask 255.255.255.0

- Subnet addresses are NAT'd by the firewall

Internal Subnet Addresses (on External Firewall)

192.168.0.1 - 192.168.0.254      Mask 255.255.255.0

- Subnet addresses are NAT'd by the firewall

Hosts on the Subnet have Private IP address mapped to a Public IP Address

<u>Server Name</u>	<u>Public Address</u>	<u>Private Address</u>
Mail Relay	209.72.2.99	192.168.1.6
Customer Web	209.72.2.100	192.168.1.5
Partner Web	209.72.2.101	192.168.1.4
Supplier Web	209.72.2.102	192.168.1.3

For ease of administration, Internal IP addresses are allocated as follows:

Servers      192.168.0.1 - 192.168.0.40  
Switches    192.168.0.41 - 192.168.0.80  
Firewalls    192.168.0.81 - 192.168.0.91  
PC / Printer 192.168.0.92 - 192.168.0.254

### 1.4 - Network Functional Overview



At the logical centre of the network is the external firewall, a Netscreen 10 with three interfaces, the internal Trusted interface, the external NonTrusted interface, and the Screened Subnet, also known as the DMZ (DeMilitarized Zone). As you would expect, most of the companies hosts reside on the Trusted Interface. Three public web servers, and a mail relay server, reside on the DMZ. Customers, Suppliers, Partners, and Remote Employees all connect through the Internet to the Untrusted interface.

GIAC has designed a custom software solution in order to handle their unique business. When Customers, Suppliers, and Partners, wish to access data on the GIAC network, they connect via HTTPS to the appropriate web server on the DMZ. All data requests are then passed from the web server to the internal Automation Server. The Automation Server then makes a query to the SQL Server (also internal), and sends the response back up to the appropriate web server. This provides considerable isolation between an external user, and the corporate data.

Remote employees, when requiring network access, will connect via a VPN tunnel to the External firewall, and connect as a node on the internal network. If the remote employee, or any other internal employee, needs access to data contained in the corporate SQL Server, they connect directly to the Automation Server, and run their queries. The Automation Server will then return the response from the SQL Server to the user.

## **1.5 - Network Security Overview**

GIAC's network will use a Cisco filtering router to connect to the Internet. This will allow us to remove some of the traffic which we deem should not be entering, or leaving the GIAC network. By implementing filtering on the router, we are able to further improve overall security, and reduce unnecessary traffic.

Behind the router we will find our external firewall, a Netscreen 10, which provides us with a screened subnet for our public hosts, as well as a "trusted" interface for our internal network. At GIAC we will implement Network Address Translation (NAT), in order to obscure our host IP addresses, as well as minimize the number of public IP addresses required by the company. NAT is used on both the internal GIAC network, and the screened subnet. NAT is a great tool in helping to defend a network, as it is very difficult for someone outside of the firewall to determine what hosts you have, and what the

hosts IP address is.

Access to the public hosts on the screened subnet is provided by using "Mapped IP" on the firewall. Mapped IP, as the name suggests, allows us to use a private address on a host, but map the private IP address to a public IP address on the external interface of the firewall. As Mapped IP provides a "one to one" relationship between a host and an external IP address, it does not obscure the host to the same degree as NAT normally does. It does however still reduce the total information available about a host, which does help defend it.

As the Netscreen firewall implements most VPN functions in ASIC (Application Specific Integrated Circuit), it is a very fast VPN gateway. So all remote hosts requiring a VPN connection, will be configured, and terminate on the external firewall. This implementation simplifies the network by avoiding the use of a separate VPN gateway device.

Within the GIAC network we have five islands (groups), each isolated by a firewall, and its policies. These islands are Sales, Creative, Accounting, Information Technology (IT), and the Public Hosts. Through the configuration of the firewalls, we can precisely control what types of traffic are allowed from each group, and to which destinations.

Mail traveling to and from the GIAC network will pass through both the internal mail server, as well as the mail relay located on the DMZ. By using a mail relay, we deny any direct external access to our internal mail host, which stores the corporate mail. This reduces the ability of an external host being able to hack into our mail server.

## **1.6 - Hardware and Software Choices**

### **1.6.1 - Cisco 1751 router - dual Ethernet interfaces - IOS version 12.2**

A Cisco router was chosen as it is a common device, with a large number of networking professionals being familiar with its use, and configuration. Although this router is capable of some firewall, and VPN functionality, it will only be used as a router. The Netscreen firewalls described below are much better at being a firewall, and have better VPN performance.

The 1751 has been configured with two Ethernet interfaces, with one connecting to our External firewall, the Netscreen 10, and the other connecting with our ISP's interface to the Internet. Access Control Lists (ACL's) will be setup on the router to filter some of the traffic which should not be entering, or leaving, the GIAC network.

More detailed information is available from Cisco at:

<http://www.cisco.com/univercd/cc/td/doc/pcat/1750.htm> (25 July 2001)

### **1.6.2 - Firewalls - Netscreen Technologies Netscreen firewall - OS version 2.6.0**

Netscreen firewalls are solid state, appliance type, packet filtering firewalls. They run a proprietary operating system (Screen OS), with the most CPU intensive processes (Policy lookup, VPN encryption/decryption, etcetera) performed by a custom ASIC. Since these firewalls provide good VPN performance, the external firewall will be used as our VPN gateway device as well. This greatly reduces the complexity of the network, and eliminates the need for IT staff to learn about yet another device.

One of the advantages of solid state appliances, is should they ever "crash", the power only needs to be reset to restore the device to operation. Should the flash image become corrupted, these appliances can be fully restored in a few minutes including all custom configuration, by any I.T. person at GIAC. Contrast this with the time it takes to rebuild a firewall based on a general purpose PC platform. Looking at the total cost of ownership (TCO), and uptime requirements of GIAC, these types of devices have a great deal to offer.

Another advantage of these devices using purpose built OS's is that unlike many popular firewalls, you do not have to start by attempting to harden a general

purpose operating system (Windows, Linux, etc.) first, and then install your firewall application. Given the almost daily discovery of flaws in these general purpose operating systems, I think it is unlikely a small to medium business can maintain a secure firewall. It is perhaps unreasonable to expect that a small to medium IT group would have the time and expertise to keep on top of the necessary patches..... and why should they have to?

One additional feature of the Netscreen firewalls is the ability to set time schedules, and enable, or disable, individual policies based on the time of day. GIAC Enterprises has no employee, either local, or remote, which uses the network between the hours of midnight, and seven in the morning. During those times the external firewall has been configured to "tighten up" security by further restricting which traffic can pass through the external firewall. Since GIAC deals with International clients, the public web servers, and their internal connections, will remain open at all times. This scheduling functionality has also been implemented in the internal firewalls as well.

More detailed information is available from Netscreen at:

<http://www.netscreen.com/products/index.html> (25 July 2001)

### **1.6.3 - Ethernet Repeaters - Hewlett Packard Procurve 12 port Hubs - J3294A**

The trend towards pushing Ethernet switching to the desktop has provided many benefits, however it makes Intrusion Detection much more difficult. Most switches will support some form of port mirroring, which would allow us to forward data from one or more switched ports to our Intrusion Detection system. However, attempting to monitor many ports at once may cause congestion in the switch, and result in switch performance problems.

My solution is to place simple repeaters (hubs) at the two entry points into the networks of GIAC. One will be placed on the DMZ between the external firewall, and the hosts on the DMZ. This will allow us to use an IDS system to monitor all traffic on the DMZ.

The second repeater is placed between the external firewall and the Backbone switch for the network. This will allow a second IDS console to monitor all traffic entering, and exiting, the internal network of GIAC.

The choice of the make and model of the repeaters is dictated by two factors. It must be reliable, and secondly, as dumb as possible. By "dumb" I mean that it is preferable that it is a non-managed hub, providing no way for an intruder to modify its operation in any way. An intruder could theoretically instruct a managed repeater to shut down the port which the IDS console was on, effectively blinding it to further activities.

More detailed information is available from Hewlett Packard at:  
[http://www.hp.com/rnd/products/hubs/10\\_100hub/summary.htm](http://www.hp.com/rnd/products/hubs/10_100hub/summary.htm) (25 July 2001)

#### **1.6.4 - Ethernet Switches - Hewlett Packard Procurve 4108GL/4000M models**

Switches play a secondary, but important role related to network security, but of course an essential role in keeping GIAC up and running (and therefore in business). I have chosen two HP switch models which are reliable, can be configured with redundant power supplies, and provide the performance that GIAC needs.

The HP 4108GL has the power (36.6 Gbps switch fabric) to handle both the IT group at GIAC, as well as to be used as the Backbone switch for the company. The Sales, Creative, and Accounting groups do not generate the same high loads of traffic, so their needs are well served by the less expensive 4000M switch, with its 3.8 Gbps switch fabric.

Both models support "port security" which allows the switch to service only one MAC address, and lock out all others. Although this is not likely to be needed by GIAC, it could be very useful if you have physically insecure areas in the company.

More detailed information is available from Hewlett Packard at:  
<http://www.hp.com/rnd/products/switches/switch4108GL/summary.htm> (25 July 2001)  
<http://www.hp.com/rnd/products/switches/switch4000/summary.htm> (25 July 2001)

#### **1.6.5 - Intrusion Detection - Network ICE Corporation ICEpac Security Suite**

ICEpac is a suite of products designed to provide both Intrusion Detection,

and host firewalling. Each host (as required) would run the BlackICE Agent, which will act as a personal firewall, and will report suspicious activity back to a central ICEcap console.

Two PC's will be used as Intrusion Detection Systems (IDS) and reporting consoles. One PC will be placed on the internal network, and connected to the HP repeater at the entry point to the internal network. The second PC will be placed on the DMZ, connected to the HP repeater which is the through point to the public web and mail servers. The IDS PC located on the DMZ will **not** be connected to the internal network at any time. Then even if the DMZ is fully compromised by an intruder, the IDS PC will not be able to be used as an access point into the internal network.

Both IDS PC's will run the BlackICE Agent, to protect themselves from being compromised. They will also run BlackICE Sentry, which will monitor, and report on, all traffic going to and from their respective networks. The third component they will run is the ICEcap Management Console, which will consolidate the data from all of the BlackICE Agents, and BlackICE Sentry Agents on their monitored networks. The ICEcap console allows you to see any intrusion attempts across your network, and quickly check historical data looking for patterns.

As these two PC's will be important in providing us with information regarding an attack on our infrastructure, it is especially important that we harden their operating systems as best as possible. An intelligent hacker will wish to blind you, by first shutting down your IDS, and any logging, if possible.

More detailed information is available from Network ICE Corporation at:  
[http://www.networkice.com/products/icepac\\_suite.html](http://www.networkice.com/products/icepac_suite.html) (25 July 2001)

#### **1.6.6 - Host OS - Microsoft Windows 2000 - Professional/Server Editions**

GIAC Enterprises is a Windows environment, primarily Windows 2000. All internal hosts will be kept at a recent Service Pack level (currently SP2), providing that the Service Pack is supported by the relevant application vendors. Internal hosts will not normally have Hot-Fixes applied, as these are not fully regression tested, and can decrease the stability of a host. Due to our security precautions, the threat of an internal host being compromised is lower, so we will opt for the increased stability.

Hosts on the DMZ will however be subjected to a more rigorous routine of applying the relevant Hot-Fixes, as they are in the front line of assault. Unfortunately the exposure of these systems to the Internet means that the danger of being hacked is greater than the possible instability created by the use of Hot-Fixes.

Microsoft links to Windows 2000 Security include:

<http://www.microsoft.com/security/> (25 July 2001)

Microsoft's home page for security related links

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/bestprac/bestprac.asp> (25 July 2001)

One of Microsoft's better links to Practices and White Papers

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/tools.asp> (25 July 2001)

A good Microsoft link to Checklists, Tools, and Updates

<http://support.microsoft.com/support/servicepacks/Windows/2000/> (25 July 2001)

Microsoft's Windows 2000 Service Pack page

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp> (25 July 2001)

Microsoft's Security Bulletins!

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp> (25 July 2001)

Link to subscribe by email to Microsoft Security Bulletins - free

Further references are in the List of References

## **Assignment 2 - Security Policy**

In this section, I will discuss the configuration of the Cisco 1751 router (Border Router), the Netscreen 10 External Firewall (Primary Firewall and VPN device), the Netscreen 100 IT Firewall (Internal Firewall), and the Netscreen 5xp Accounting Firewall (Internal Firewall).

Fortunately, the Netscreen firewall models all share a common Operating System and command language, so the discussions of the firewalls are about the configuration differences for the different types of tasks they perform.

Although the complete configuration of either the Netscreen firewalls, or the Cisco router, are well beyond the scope of this document, I have tried to present the steps required to implement each feature we require. Additionally explanations have been provided for the various technologies, and terminology involved.

It would be useful if you were to print a copy of Illustration 1, the diagram of the GIAC Enterprises Network, if you have not already. It will help you to understand the relative positioning of all of the components involved in the GIAC network, and make the following explanations easier to follow.

The Netscreen firewall configuration is discussed first in this section, followed by the Cisco router.

### **2.1 - Defining Transparent Mode, and Introduction to Netscreen GUI**

In order to illustrate how the Security policies are implemented on the Netscreen firewalls, I will describe some of the features and how they function. I will show these through both screen shots from the GUI (Graphical User Interface) and examples of the CLI (Command Line Interface).

As mentioned previously, the IP addresses used internally at GIAC are private IP addresses, specifically the 192.168.0.0, mask 255.255.255.0 subnet. As



GIAC has approximately 90 hosts, including Servers, PC's, Switches, and Printers, a single subnet is the easiest to work with. The Netscreen firewalls used internally support "Transparent Mode". Transparent mode passes packets without modifying the IP header in any way, but still allow you to filter the packets.

This diagram illustrates the kind of IP addressing that Transparent Mode allows us, with hosts on both sides of the firewall being on the same subnet.

Illustration 2 - Transparent Mode

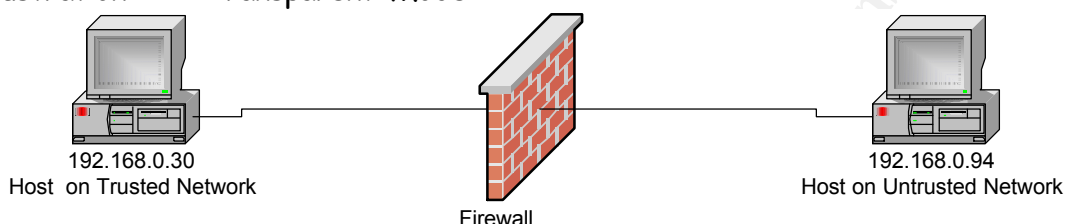


Illustration 3 - Default Outgoing Policy, Allow All

Incoming Outgoing											
ID	Source	Destination	Service	NAT	Action	Option					Configure
0	Inside Any	Outside Any	ANY	N/A							 <a href="#">Edit</a> <a href="#">Remove</a>

The Netscreen GUI for policies is very similar to other firewalls GUI's, and is easy to interpret. Here is a quick reference to the meaning of each column for policies.

#### ID

A number assigned to each policy that you define. The ID number is used when you wish to reorder the policies, and need some way to identify what policy, you want to move to where.

#### Source

An IP address, subnet address, or a label which has been defined as certain IP addresses. Since this is an Outgoing policy, the IP address in this field refers to hosts on the Trusted interface. The use of a label makes the policy easier to interpret.

## **Destination**

As above, an IP address, subnet address, or a label which has been defined as certain IP addresses. Since this is an Outgoing policy, the IP address in this field will reference either the Untrusted interface, or the DMZ interface of the firewall.

## **Service**

This essentially refers to the TCP and UDP port numbers of the Destination host(s). This field will also often have a label which defines a port instead, such as HTTP which has a default port of 80. Note: Other Protocol ID's can be defined, so we are not limited to TCP and UDP, but these are most common.

## **NAT**

This simply informs us whether Network Address Translation is being performed on the packets, or not.

## **Action**

This indicates whether the policy will block the kind of traffic we have defined, allow it, or allow it only through a VPN tunnel. A green circle with a checkmark indicates the traffic is allowed, a red circle with an "x" means it is blocked, and a padlock indicates a VPN tunnel will be used.

## **Option**

Multiple icons indicate whether many of the other options are enabled. These options are as follows:

- Authenticate - User must authenticate themselves to the firewall
- Log - Traffic is kept in a log and available to Syslog and Email, if enabled
- Count - Traffic is counted in bytes per second and can be graphed
- Alarm - An alarm will be sent when traffic exceeds a level you define
- Traffic Shaping - Bandwidth available to this policy has been defined
- Schedule - Traffic will be allowed according to a defined time schedule

## **Configure**

This is where you can move the policies position relative to other policies you have defined. Additionally you can enable and disable the features found under "Option"

Now looking at the GUI for the default Outgoing Policy (Illustration 3) we

see that packets originating from any IP address on the Trusted interface, can travel to any IP address on the Untrusted interface, using any service. This would be classified as an "allow all" policy. So if we were to Ping host 192.168.0.94 (Illustration 4), from host 192.168.0.30 on the other side of the firewall, we would expect to see the traffic pass through the firewall unhindered (Illustration 5)

Illustration 4 - Ping from host 192.168.0.30

```
E:\>ping 192.168.0.94

Pinging 192.168.0.94 with 32 bytes of data:

Reply from 192.168.0.94: bytes=32 time<10ms TTL=128
Reply from 192.168.0.94: bytes=32 time<10ms TTL=128
Reply from 192.168.0.94: bytes=32 time<10ms TTL=128
Reply from 192.168.0.94: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.0.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Illustration 5 - Windump output from host at 192.168.0.94

```
c:\windump>windump -n ip host 192.168.0.30
windump: listening on \Device\NPF{C97734CBC-BE4F-4533-A853-3AA5050674AD}
09:39:27.370941 192.168.0.30 > 192.168.0.94: icmp: echo request
09:39:27.370974 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:27.371010 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:28.363795 192.168.0.30 > 192.168.0.94: icmp: echo request
09:39:28.363838 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:28.363894 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:29.365129 192.168.0.30 > 192.168.0.94: icmp: echo request
09:39:29.365172 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:29.365232 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:30.366496 192.168.0.30 > 192.168.0.94: icmp: echo request
09:39:30.366538 192.168.0.94 > 192.168.0.30: icmp: echo reply
09:39:30.366595 192.168.0.94 > 192.168.0.30: icmp: echo reply



16 packets received by filter
0 packets dropped by kernel
```

So as we expected, the Ping (Echo Request) successfully crossed the firewall, elicited the Echo Reply from 192.168.0.94, and this reply came back to the originating host.

If we were now to modify the single policy to say that any host on the

Trusted interface can send packets to any host on the Untrusted interface, as long as the destination port is HTTP (port 80). The policy would look like Illustration 6 on the next page.

Illustration 6 - Outgoing Policy, Allow Only HTTP

Incoming Outgoing									
ID	Source	Destination	Service	NAT	Action	Option			
0	Inside Any	Outside Any	HTTP	N/A					<a href="#">Edit</a> <a href="#">Remove</a>

Now we repeat our Ping from host 192.168.0.30 on the Trusted interface, to host 192.168.0.94 on the Untrusted interface. Illustration 7 shows the Pinging host's screen, and Illustration 8 shows what traffic that host 192.168.0.94 sees through the firewall.

Illustration 7 - Ping from host 192.168.0.30

```
E:\>ping 192.168.0.94

Pinging 192.168.0.94 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.94:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Illustration 8 - Windump output from host at 192.168.0.94

```
c:\windump>windump -n ip host 192.168.0.30
windump: listening on \Device\NPF_{C9734CBC-BE4F-4533-A853-3AA5058694AD}

3 packets received by filter
0 packets dropped by kernel
```

So by changing our policy to only allow HTTP (port 80) traffic to pass through the firewall, we have blocked our Ping ( ICMP Echo Request).

## **2.2 - Implementing the Accounting Firewall and Introduction to the Command Line Interface (CLI) of the Netscreen Firewall**

The Accounting department is one of our "islands" that we have protected by a Netscreen 5xp firewall in transparent mode. Accounting is one group in the company which has network access needs which are relatively easy to define. These are the needs which were defined for Accounting:

1. Read and write files to the Accounting Server
2. Read and write files to the General File Server
3. Send and receive email to the Mail Server
4. Access the Win2K domain controller which also provides DNS and DHCP services
5. Access the Win2K Tape/DC server which is a secondary domain controller
6. HTTP and HTTPS Internet access

The accounting manager has expressed his concern that anyone outside of his group might gain access to any of their computers. Security is a priority for this manager! In illustration 9, and 10, you can see the GUI version of the policy that was implemented for the Accounting department's firewall. Following that is a tutorial of how we would implement this using the CLI (Command Line Interface).

Illustration 9 - Accounting Department Outgoing Policy

Incoming		Outgoing											
ID	Source	Destination	Service	NAT	Action	Option					Configure		
10	Inside Any	Accounting Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
11	Inside Any	Domain/DNS/DHCP Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
12	Inside Any	Mail Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
13	Inside Any	General File Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
14	Inside Any	Tape/DC Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
16	Inside Any	Outside Any	HTTP	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
17	Inside Any	Outside Any	HTTPS	N/A									<a href="#">Edit</a> <a href="#">Remove</a>

Illustration 10 - Accounting Department Incoming Policy

Incoming

Outgoing

ID	Source	Destination	Service	NAT	Action	Option	Configure
No policy available							

Upon first viewing the Outgoing policies (Illustration 9), you might wonder why we did not get more specific on the services that the accounting hosts are allowed to access on each external server. This was done to simplify administration of the firewalls. The Accounting firewall is in place to perform two major functions. The most important function is to block hosts outside of the accounting group from accessing the internal hosts. Illustration 10 shows that there is no Incoming Policy. Since the firewall has a default "deny all" policy, this means that the firewall will block all packets that are not a response to a packet sent from a Trusted host.

The secondary function is to primarily restrict the accounting hosts to specific servers, as a backup to the security which should be implemented within Windows 2000. We could analyze the traffic to each of their servers, and open just the required ports, but would this really improve our security stance

significantly? I don't believe so.

If we were to restrict access to specific ports, then each change in software in the company could require changes to the firewall policies. It is important to realize that we have to balance our security efforts against the amount of time required to maintain that security. If it is too intricate, some frustrated technician trying to get an application to work will simply enter a firewall policy that allows all traffic, and the firewall will truly be transparent!

### 2.2.1 - Defining the Address of a Host

So let us now look at how we would build these policies using the CLI in the Netscreen firewalls. In order to more easily understand the policies, in both the GUI and CLI interfaces, we first assign a label to hosts which are significant to our policies. When we are trying to evaluate how a collection of policies will effect packet flow, it is much easier to look at names such as "Sales Server" and "Accounting Server", than "192.168.0.1" and "192.168.0.3".

To define this label, what Netscreen calls an Address, we use one of these three formats:

Set address trust (label) (ip address) (mask) (optional description)  
Set address untrust (label) (ip address) (mask) (optional description)  
Set address dmz (label) (ip address) (mask) (optional description)

"label" is the name we wish to call the host, or subnet

"ip address" is the address of the host, or subnet

"mask" is a decimal representation of the bits we wish to count as significant when evaluating the address. If the mask is 255.255.255.255, it means that all bits are significant, and so for the expression to be true only one IP address will match.

If we wish to test for a subnet, then we will use a mask such as 255.255.255.0

Netscreen has already pre-defined the following Addresses.

**Inside Any** - any host on the Trusted interface of the firewall

**Outside Any** - any host on the Untrusted interface of the firewall

**DMZ Any** - any host on the DMZ interface of the firewall

**Dial-Up VPN** - any host connecting to the Untrusted interface by VPN

So to define the Addresses for a couple of our servers, we would use the following lines:

```
Set address untrust "Sales Server" 192.168.0.1 255.255.255.255
Set address untrust "Mail Server" 192.168.0.5 255.255.255.255
```

These hosts are on the Untrusted interface of the Accounting firewall, and have been defined as belonging to only one IP address, not a subnet, by using the mask of 255.255.255.255.

### 2.2.2 - Setting up a Schedule

To further enhance the security of the Accounting department, we have implemented schedules for their policies. To define a schedule we use this syntax:

```
Set scheduler (label) (type of schedule) (day if "recurrent") start (date if "once")
(time) stop (date if "once") (time)
```

"label" is the name of our schedule

"type of schedule" "once" for a one time event, or "recurrent" for a repeating event

"day" name of the weekday, if this is for a recurrent event

"date" date in the format mm/dd/yyyy if this is a one time event

"time" in 24 hour format like hh:mm

Each day of the week is a separate entry, so for an entire work week we created this schedule, which enables a policy between the hours of 7:00 am and 6:00 pm.

```
set scheduler "Business Hours" recurrent monday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent tuesday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent wednesday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent thursday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent friday start 7:0 stop 18:0
```

### 2.2.3 - Putting the Policy command line together



We have defined the Addresses of the hosts for our policies, and the schedules, now we need to bring these together to form a policy for each host. For this we use the Set Policy command. There are many variations on the Set Policy command, and the full usage of it is beyond the scope of this document. Here is the most common usage:

Set Policy id (number) name (name) outgoing (Source) (Destination) (Service)  
Permit schedule (schedule name)

So to grant the Accounting department users on the Trusted interface access to the Accounting server, we would use the following line:

```
set policy id 10 name "Acctg Server" outgoing "Inside Any" "Accounting Server"  
"ANY" Permit schedule "Business Hours"
```

The meaning of this policy line is as follows:

- Our policy ID number is 10 (just a sequentially picked number, could be another)
- We call this policy line "Acctg Server" for convenience
- This policy controls packet flow going from the Trusted to the Untrusted interface
  - Outgoing
- Packets can come from any host on the Trusted interface ("Inside Any")
- Packets can only be addressed to the Accounting Servers IP address, which we previously defined as 192.168.0.3 ("Accounting Server")
- Packets can have any destination port ("ANY")
- Packets matching the above criteria are permitted to pass (Permit)
- This policy is in force during the scheduled time called "Business Hours". This was defined earlier as from 7:00 am to 6:00 pm (18:00 hours). Outside of those hours the packet will be compared to other policies below this one.

#### **2.2.4 - Policy Order - Importance and Reorganization**

Policies are executed from the top of the policy list, to the bottom, and order is very important. First off, comparing a packet's characteristics to a policy takes CPU (Central Processing Unit) time, which slows the firewall down. If the

majority of the traffic from the Accounting department goes to the Accounting Server, and they only occasionally use the Internet, then it makes sense to test for the Accounting Server traffic first. There would be no sense always checking to see if every packet from the Accounting department is going to the Internet, if they rarely do.

Additionally, the order of the policies can affect the security you are trying to implement. Say you wished to allow all traffic, except packets destined for the Internet, HTTP service (port 80). You would create two policy lines like this:

```
set policy id 10 name "All Access" outgoing "Inside Any" "Outside Any" "ANY"  
Permit schedule "Business Hours"  
set policy id 11 name "No Internet" outgoing "Inside Any" "Outside Any" "HTTP"  
Deny schedule "Business Hours"
```

If this was the order the policies were in, users would be allowed to access the Internet, as well as anything else! Why? When our packet arrives at the Trusted interface, it will be compared to each policy, from the top down, until a match is made. So a packet addressed to a web server, port 80, will be compared to the first policy line. That policy says that a packet coming from anywhere on the Trusted interface, can have a destination anywhere on the Untrusted interface, with any destination port, and it will be permitted. Our HTTP destined packet matches this criteria, and so it is permitted. It will not even be evaluated by the second policy.

In order to make our policies work the way we intended, we need to put policy 11 in front (or on top) of policy 10. This is accomplished quite easily by the following command entered on the command line.

```
Set policy move 11 before 10
```

Our packet destined for the HTTP service on port 80 will now first be evaluated by policy 11, which will then deny the packet, disallowing our user access to the web server.

## 2.2.5 - Pulling it all together - CLI Configuration of the Accounting Firewall Policies

First, give the internal hosts we wish to access friendly names

```
set address untrust "Sales Server" 192.168.0.1 255.255.255.255
set address untrust "Creative Server" 192.168.0.2 255.255.255.255
set address untrust "Accounting Server" 192.168.0.3 255.255.255.255
set address untrust "General File Server" 192.168.0.4 255.255.255.255
set address untrust "Mail Server" 192.168.0.5 255.255.255.255
set address untrust "SQL Server" 192.168.0.6 255.255.255.255
set address untrust "Tape/DC Server" 192.168.0.7 255.255.255.255
set address untrust "Domain/DNS/DHCP Server" 192.168.0.8 255.255.255.255
set address untrust "Automation Server" 192.168.0.9 255.255.255.255
```

Second, setup the schedules to control access to these hosts

```
set scheduler "Business Hours" recurrent monday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent tuesday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent wednesday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent thursday start 7:0 stop 18:0
set scheduler "Business Hours" recurrent friday start 7:0 stop 18:0
```

Third, define our policies, and ensure the order is correct

```
set policy id 10 name "Acctg Server" outgoing "Inside Any" "Accounting Server"
"ANY" Permit schedule "Business Hours"
```

```
set policy id 11 name "Domain Controller/DNS/DHCP" outgoing "Inside Any"
"Domain/DNS/DHCP Server" "ANY" Permit schedule "Business Hours"
```

```
set policy id 12 name "Mail Server" outgoing "Inside Any" "Mail Server" "ANY"
Permit schedule "Business Hours"
```

```
set policy id 13 name "General File/Print Server" outgoing "Inside Any" "General
File Server" "ANY" Permit schedule "Business Hours"
```

```
set policy id 14 name "Tape/Secondary DC" outgoing "Inside Any" "Tape/DC
Server" "ANY" Permit schedule "Business Hours"
```

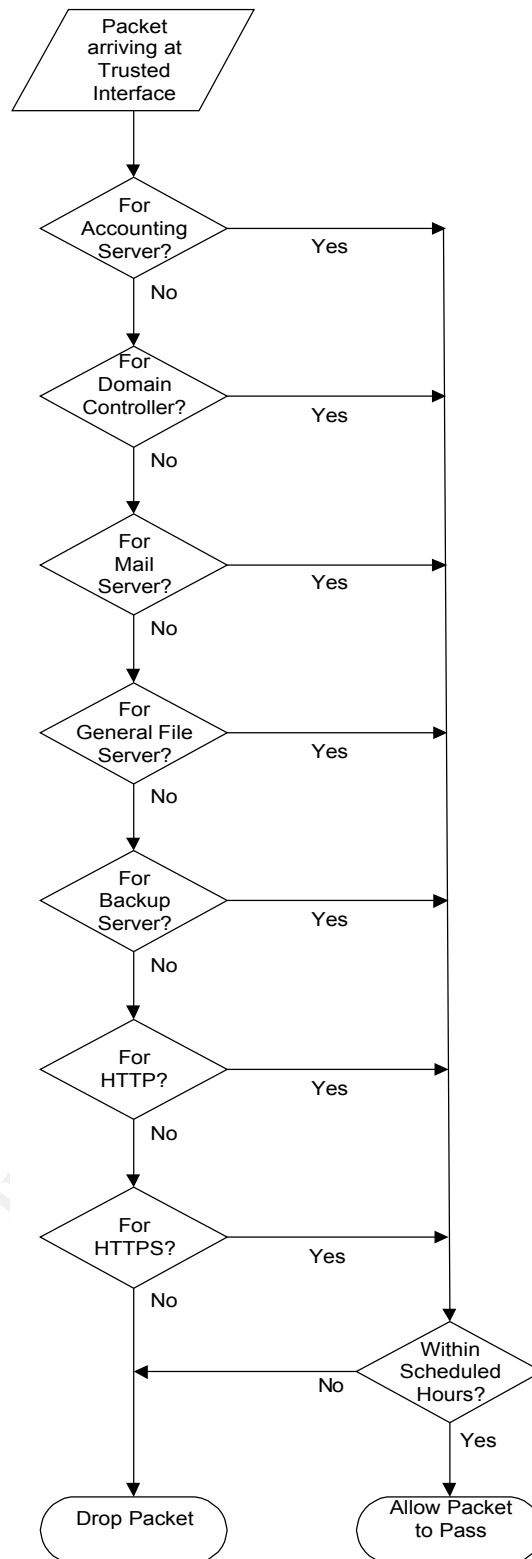
*set policy id 16 name "Web traffic" outgoing "Inside Any" "Outside Any"  
"HTTP" Permit schedule "Business Hours"*

*set policy id 17 name "Secure Web Traffic" outgoing "Inside Any" "Outside Any"  
"HTTPS" Permit schedule "Business Hours"*

The following flowchart shows the logical decision making that the policy that we just defined will follow. From top to bottom, each decision will either pass the packet onto the "schedule" question, or allow it to drop down to the next decision.

Illustration 11 - Accounting Firewall Outgoing Policy flow of logic

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



## 2.3 - Setting up the IT Firewall - Configuration gets more challenging

The Netscreen 100 (IT firewall) also runs in Transparent mode in the GIAC network, but the configuration is somewhat more difficult. Unlike the Accounting firewall, it is not sufficient to only allow packets to originate from the Trusted interface, but we must also allow some connections to be initiated from the Untrusted interface. For example, users throughout the internal network of GIAC will need to access the DNS server, and the Mail server. Additionally since our management workstation runs an SNMP application, as well as a Syslog service, we must allow the various agents in the network to be able to push data to it.

As the configuration becomes more complex, it becomes valuable to be able to group servers together which we will apply a common policy to. Netscreen calls these Group Addresses.

Additionally Netscreen has some predefined Services which make configuration easier, such as HTTP for TCP port 80, and MAIL for TCP port 25. We are however allowed to define our own services, and group these into Group Services. As with the addresses, we often have a common group of services we offer to users, so instead of assigning them one policy at a time, we can assign them as a group. This makes both configuration and long term management much easier.

### **2.3.1 - Defining Custom Services**

For defining custom Service entries, we use the Set Service command. The basic syntax is as follows:

Set service (label) protocol (protocol) src-port (source port range) dst-port (destination port range)

"label" is a friendly name for the service we are defining, in quotes

"protocol" can be TCP, UDP, or a protocol number

"source port range" is the port(s) the source host originates from and is represented by two numbers separated by a dash, like 80-80, or 135-139. Often this is 1024-65535.

"destination port range" is the port(s) the destination host runs the service on, and is represented the same way the source port range is

As an example, here is how I defined the Kerberos service:

```
set service "Kerberos 88 UDP" protocol udp src-port 1024-65535 dst-port 88-88
```

*set service "Kerberos 88 UDP"* - the name we call this custom service definition  
*protocol udp* - this service uses UDP

*src-port 1024-65535* - the ephemeral ports that clients use (expressed as a range)

*dst-port 88-88* - the port that the Kerberos service uses (expressed as a range)

### 2.3.2 - Custom Services Defined on the IT Firewall

These are the services that I defined, as they were not one of the pre-defined ones on the Netscreen.

```
set service "NetBIOS 137-138 UDP" protocol udp src-port 1024-65535 dst-port 137-138
```

```
set service "NetBIOS 139 TCP" protocol tcp src-port 1024-65535 dst-port 139-139
```

```
set service "RPC 135 TCP" protocol tcp src-port 1024-65535 dst-port 135-135
```

```
set service "SMB 445 TCP" protocol tcp src-port 1024-65535 dst-port 445-445
```

```
set service "Kerberos 88 UDP" protocol udp src-port 1024-65535 dst-port 88-88
```

```
set service "BOOTP 67/68 UDP" protocol udp src-port 67-67 dst-port 68-68
```

### 2.3.3 - Defining Custom Service Groups

I could define a policy for each of these services, but since there are so many services that everyone on the network needs, it is easier to manage them as a group. This is done by using the Set Group Service commands, with the following syntax:

```
Set group service (Group Name) add (service)
```

"group name" is the friendly name we assign to our new group

"service" is either a name I assigned to a custom service (above) or one of the predefined names

So if we wanted a group called "Network" and we wanted DNS and PING to be part of it, we would use the following two lines:

```
set group service "Network" add "DNS"  
set group service "Network" add "PING"
```

Now when setting up a policy with both DNS and PING, we can use the name "Network" instead.

#### **2.3.4 - Custom Service Groups Defined on the IT Firewall**

```
set group service "Network Services" add "DNS"  
set group service "Network Services" add "PING"  
set group service "Network Services" add "NetBIOS 137-138 UDP"  
set group service "Network Services" add "NetBIOS 139 TCP"  
set group service "Network Services" add "RPC 135 TCP"  
set group service "Network Services" add "SMB 445 TCP"  
set group service "Network Services" add "Kerberos 88 UDP"  
set group service "Network Services" add "BOOTP 67/68 UDP"
```

This is the group of services which is commonly assigned together in a Windows 2000 environment. DNS is needed to not only locate local hosts, but also Internet hosts. PING is our standard diagnostic tool, and also used by many utilities to locate active hosts. The NetBIOS, RPC, SMB, and Kerberos ports are all part of the operation of a Windows network. And finally BOOTP is what allows a client to obtain an IP address during the boot process.

#### **2.3.5 - Defining Custom Group Addresses**

Just as we grouped the services together to make it easier to create policies, we can group Addresses together. In the discussion of the Accounting firewall, I discussed how you could assign a friendly name to an IP address. In a similar fashion we can assign a friendly name to groups of hosts, using this syntax:

```
Set group address (interface) (label) add (Host)  
"interface" will be either Trust, Untrust, or DMZ  
"label" is the friendly name we wish to call our group by  
"host" is the name we assigned to a host IP address to make it easier to work
```



with

So if we have two servers named "Sales Server" and "Creative Server" we could put these in a group the following way:

First, create the group by assigning a name

```
Set group address trust "General Group"
```

Then assign the group members

```
Set group address trust "General Group" add "Sales Server"
```

```
Set group address trust "General Group" add "Creative Server"
```

We now have a group called "General Group" with two members. Any policies which we need to apply to both servers, can be applied to their group instead.

### **2.3.6 - Custom Group Addresses Defined on the IT Firewall**

```
set group address trust "General File Servers Group"
```

```
set group address trust "General File Servers Group" add "Sales Server"
```

```
set group address trust "General File Servers Group" add "Creative Server"
```

```
set group address trust "General File Servers Group" add "Accounting Server"
```

```
set group address trust "General File Servers Group" add "General File Server"
```

```
set group address trust "General File Servers Group" add "Automation Server"
```

```
set group address trust "Domain/DNS Server Group"
```

```
set group address trust "Domain/DNS Server Group" add "Tape/DC Server"
```

```
set group address trust "Domain/DNS Server Group" add "Domain/DNS/DHCP  
Server"
```

So for the IT Firewall we have created two group addresses, one called "General File Servers Group" and the other "Domain/DNS Server Group". This was done to make it easier to create the necessary policies, as you will see later.

### 2.3.7 - Time Scheduling revisited

We have already gone over how scheduling works, so I will not cover that again. However, since the IT group serves a wide group of users, we have defined a different time schedule to restrict access to some of the services. This schedule was defined as follows:

```
set scheduler "Extended Hours" recurrent sunday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent monday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent tuesday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent wednesday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent thursday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent friday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent saturday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent sunday start 7:0 stop 23:59
```

### 2.3.8 - Bringing the IT Firewall to life - creating the policies

Illustration 11 shows the GUI interface for the Outgoing Policy for the IT Firewall. Outgoing is easy in this case, as we can make these assumptions.

- The Mail server originates a call when contacting the Mail relay on the DMZ
- Our two domain servers, one of which is also our DNS, need to be able to contact the ISP's DNS, and also provide various "Windows" services
- Our Management PC needs to poll various SNMP devices

Illustration 11 - Outgoing Policy of IT Firewall

Incoming		Outgoing									
ID	Source	Destination	Service	NAT	Action	Option					Configure
16	Mail Server	Screened Subnet	MAIL	N/A							Edit Remove
17	Domain/DNS Server Group	Outside Any	Network Services	N/A							Edit Remove
18	Management Station	Local LAN	SNMP	N/A							Edit Remove

This Outgoing policy was easily created on the command line with these three lines:

```
set policy id 16 outgoing "Mail Server" "Screened Subnet" "MAIL" Permit
```

```
set policy id 17 outgoing "Domain/DNS Server Group" "Outside Any" "Network Services" Permit
```

```
set policy id 18 outgoing "Management Station" "Local LAN" "SNMP" Permit
```

The Incoming policy is somewhat more complicated, but still made fairly easy through the use of the various groups we created. Illustration 12 gives a clear overview of our Incoming policies. Here are the assumptions the policies were based on:

- Any host on our local network can access the "General File Servers" group, subject to time restrictions
- Any host on our local network can access our Mail Server, subject to time restrictions
- Any host on our local network can access our two domain controllers, one of which provides DNS and DHCP, using one of the allowed services, subject to time restrictions
- Any host on our local network can use SNMP to contact our Management workstation (for sending SNMP traps to our PC)
- Any host on the Untrusted interface can contact the Syslog server running on the Management workstation (for sending errors from firewalls to the PC)
- Any host on our local network can access the Automation server
- Any host on the DMZ can access the Automation server

Illustration 12 - Incoming Policy of IT Firewall

Incoming		Outgoing											
ID	Source	Destination	Service	NAT	Action	Option					Configure		
9	Local LAN	General File Servers Group	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
10	Local LAN	Mail Server	MAIL	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
11	Local LAN	Domain/DNS Server Group	Network Services	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
12	Local LAN	Management Station	SNMP	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
15	Outside Any	Management Station	SYSLOG	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
14	Local LAN	Automation Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>
20	Screened Subnet	Automation Server	ANY	N/A									<a href="#">Edit</a> <a href="#">Remove</a>

These Incoming policies can be created on the command line as follows:

*set policy id 9 name "General File Access Policy" incoming "Local LAN" "General File Servers Group" "ANY" Permit schedule "Extended Hours"*

*set policy id 10 name "Mail" incoming "Local LAN" "Mail Server" "MAIL" Permit schedule "Extended Hours"*

*set policy id 11 name "Network Services Policy" incoming "Local LAN" "Domain/DNS Server Group" "Network Services" Permit schedule "Extended Hours"*

*set policy id 12 name "SNMP Traps Policy" incoming "Local LAN" "Management Station" "SNMP" Permit*

*set policy id 15 incoming "Outside Any" "Management Station" "SYSLOG" Permit*

*set policy id 14 name "Automation Policy" incoming "Local LAN" "Automation Server" "ANY" Permit*

*set policy id 20 incoming "Screened Subnet" "Automation Server" "ANY" Permit*

## 2.4 - Setting up the External Firewall - The DMZ and Mapped IP

On the External firewall, the addition of a third interface, the DMZ, gives us a separate network to place hosts which are accessible by the public. In the case of the three Web servers, these hosts act as proxies. Customers, Suppliers, and Partners on the Internet can make requests to these servers, and if they are valid and authenticated, the Web servers will then contact the internal Automation server to fulfill their requests.

The Mail relay also acts as a type of proxy, as it will send and receive mail on the Internet, on behalf of the internal mail server. If this Mail relay host is compromised, it does not contain any company mail, other than that which might be in transit.

In order to further obscure information about our hosts, we will employ Mapped IP addresses for the hosts on the DMZ. Mapped IP allows us to have a Public IP address mapped to another internal IP address. For example our Mail relay on the DMZ has an IP address of 192.168.1.6 . By using a variation of the Set Interface command we can map this IP address to Public IP address 209.72.2.99 .

The format of this variation of the Set Interface command is as follows:

Set interface dmz mip (Public IP address) host (Host IP address) netmask (Mask)

"Public IP address" is the valid IP address that will appear to the public on the outside of your firewall

"Host IP address" is the true IP address assigned to your hosts interface

"Mask" is a decimal representation of the bits we wish to count as significant when evaluating the address. If the mask is 255.255.255.255, it means that all bits are significant, and so for the expression to be true only one IP address will match. If we wish to test for a subnet, then we will use a mask such as 255.255.255.0

For our external firewall, we used the following lines to setup our mapped IP addresses, one for each Web server, and one for the Mail relay

```
set interface dmz mip 209.72.2.99 host 192.168.1.6 netmask 255.255.255.255
set interface dmz mip 209.72.2.100 host 192.168.1.5 netmask 255.255.255.255
```

```
set interface dmz mip 209.72.2.101 host 192.168.1.4 netmask 255.255.255.255
set interface dmz mip 209.72.2.102 host 192.168.1.3 netmask 255.255.255.255
```

#### **2.4.1 - Defining the Host Addresses, and Groups, on the External Firewall**

As we did on the Accounting, and IT firewalls, one of our first steps is to define friendly names (Addresses) for individual hosts which we need to control traffic flow to and from. This is done with the Set Address command, but now besides defining hosts on the "Untrust" and "Trust", we can define hosts on the "DMZ".

```
set address dmz "Suppliers Web" 192.168.1.3 255.255.255.255
set address dmz "Partners Web" 192.168.1.4 255.255.255.255
set address dmz "Customers Web" 192.168.1.5 255.255.255.255
set address dmz "Mail Relay" 192.168.1.6 255.255.255.255
set address trust "Mail Server" 192.168.0.5 255.255.255.255
set address trust "Domain/DNS/DHCP Server" 192.168.0.8 255.255.255.255
set address trust "Automation Server" 192.168.0.9 255.255.255.255
set address untrust "External NTP Server" 209.87.233.53 255.255.255.255
set address untrust "ISP DNS Server" 209.72.1.100 255.255.255.255
```

We then define only one group, the "Screened Subnet Web Svrs" group. This is done with the Set Group Address command, as we did on the other firewalls. First we define the Group Address name, and then we add the Web hosts to the group.

```
set group address dmz "Screened Subnet Web Svrs"
set group address dmz "Screened Subnet Web Svrs" add "Suppliers Web"
set group address dmz "Screened Subnet Web Svrs" add "Partners Web"
set group address dmz "Screened Subnet Web Svrs" add "Customers Web"
```

#### **2.4.2 - Setting a Time Schedule for the External Firewall**

As we did with the other firewalls, we will make use of the Scheduling feature on the External firewall to control some of the network access. Working with International Customers, Suppliers, and Partners, means that we cannot completely close down our network at night. We can however restrict some access, which will enhance our security. Using the Set Scheduler command, we setup a daily schedule which runs from 7:00 am to 11:59 pm.

```

set scheduler "Extended Hours" recurrent sunday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent monday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent tuesday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent wednesday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent thursday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent friday start 7:0 stop 23:59
set scheduler "Extended Hours" recurrent saturday start 7:0 stop 23:59

```

### 2.4.3 - Defining and Implementing the External Firewall Policies

The company policy regarding specific host access for the external firewall was defined as follows:

- Web servers on DMZ will need a policy for external access, and to the Automation server on the Trust network
- Mail Relay on DMZ will need a policy for Untrust network access
- Mail Server on Trust will need to access the Mail Relay on the DMZ network
- Domain/DNS on Trust will need to access an external DNS server
- Automation server on Trust will need access to Web servers on DMZ
- Explicitly define the address of a NTP (Network Time Protocol) server on the Untrust network
- Explicitly define the address of a DNS server at GIAC's ISP (Internet Service Provider) on the Untrust network
- Hosts on Trust network can access HTTP, HTTPS, and FTP on the Untrust network

As the External firewalls rules are the most important, as they are the frontline defense for GIAC, I will step through each policy rule, explaining the function of the rule. Each rule is defined using the Set Policy command.

```

set policy id 1 outgoing "Inside Any" "Outside Any" "HTTP" Permit schedule
"Extended Hours"

```

This rule would be met by the majority of data flowing out of the GIAC network. Simply put, any host on the Trusted interface can make a connection to any Web server on the Untrusted interface using the normal HTTP protocol, between the hours of 7:00 am to 11:59 pm.

*set policy id 2 outgoing "Inside Any" "Outside Any" "HTTPS" Permit schedule "Extended Hours"*

This rule is identical to the first rule, except that it allows only secure HTTP connections (HTTPS).

*set policy id 5 outgoing "Inside Any" "Outside Any" "FTP" Permit schedule "Extended Hours"*

This rule allows anyone on the Trusted interface to send and receive files using the FTP (File Transfer Protocol) protocol, between the hours of 7:00 am to 11:59 pm.

*set policy id 3 outgoing "Domain/DNS/DHCP Server" "ISP DNS Server" "DNS" Permit*

Now we get to the more specific rules. This rule allows only our DNS host on the Trusted interface to make a connection to the DNS service on our ISP's DNS server. There is no time restriction on this function.

*set policy id 4 outgoing "Mail Server" "Mail Relay" "MAIL" Permit*

As mail can be sent and received at any time of the day, this rule allows our Mail server on the Trusted interface to make a connection to the SMTP service on our Mail relay, located on the DMZ. The Mail relay is the only host that our internal Mail server can make an SMTP connection to.

*set policy id 6 outgoing "Automation Server" "Screened Subnet Web Svrs" "ANY" Permit*

*set policy id 7 fromdmz "Screened Subnet Web Svrs" "Automation Server" "ANY" Permit*



Policy ID's 6 and 7 are complementary policies. Since the Automation server is a key link between the SQL database, and those who are seeking data, it needs to be able to make a connection to the Web servers on the DMZ. And then of course, the Web servers need to be able to make a connection to the Automation server as well. Once the programmers of the Automation server have finalized their software, it would be prudent to determine which Services/Ports are required for transactions between the two parties, and then modify this rule to allow only those Services to pass.

```
set policy id 8 outgoing "Inside Any" "External NTP Server" "NTP" Permit
```

Many of our hosts, as well as the Netscreen firewalls, rely on having the correct time. This rule allows any host on our Trusted interface to make a connection with the defined NTP server, using the NTP service.

```
set policy id 9 todmz "Outside Any" "Mail Relay" "MAIL" Permit  
set policy id 12 fromdmz "Mail Relay" "Outside Any" "MAIL" Permit
```

Since a Mail relay is not of much use if the outside world cannot connect to it, we must define this rule which allows any host on the Untrust interface to connect to our Mail relay on the DMZ, and communicate via the SMTP service. Then we have the complementary policy which allows the reverse, so that our Mail relay can connect to other mail hosts.

```
set policy id 10 todmz "Outside Any" "Screened Subnet Web Svrs" "HTTP"  
Permit  
set policy id 11 todmz "Outside Any" "Screened Subnet Web Svrs" "HTTPS"  
Permit
```

In order to allow our Customers, Suppliers, and Partners, to access the Web servers, we set this policy to allow any host on the External interface, to access the Web servers on the DMZ, using either the HTTP or HTTPS protocols.

```
set policy id 13 fromdmz "Screened Subnet Web Svrs" "Outside Any" "FTP"  
Permit
```

```
set policy id 14 todmz "Outside Any" "Screened Subnet Web Svrs" "FTP"  
Permit
```

Our last pair of complementary policies allows hosts on the External interface to send and receive files, using the FTP protocol, to our Web servers on the DMZ. These policies will also allow the Web servers to initiate a transfer.

## **2.5 - Setting up the VPN on the External Firewall**

Employees who are offsite and need access to the GIAC network are required to use a VPN connection. Partners of GIAC are recommended to use a VPN connection, but can alternatively use an HTTPS connection to the Partners Web server.

VPN provides a very secure method of communication, but requires separate client software be loaded on the host who wishes to establish the connection. Alternatively, if there is a close working relationship with the two parties, and they both have VPN gateways of some type, a VPN tunnel may be established between the gateways, eliminating the need for a separate client.

Partners are offered the alternative of an HTTPS connection, as the use of client software may not be allowed by their corporate policies. Additionally there may be some restrictions placed on the use of such encryption software by the Federal authorities in their country.

Fortunately, a "secure" HTTPS session can be established using any popular browser, without the requirement of additional software, or reconfiguration of the Partners hosts, or firewall.

GIAC has chosen to implement what Netscreen calls "Dialup-to-LAN VPN's". The term "dialup" may be a bit confusing, as it really refers to any host that will connect across the Internet, and may not have a fixed IP address. For example you may be connecting via a cable modem at home, but like a dialup user, the IP address is likely unknown to the user, and changes over time (although perhaps a long period of time in the case of a cable modem). The point here is that the IP address for many connection types is not fixed, and therefore will not be used as part of the authentication of the user.

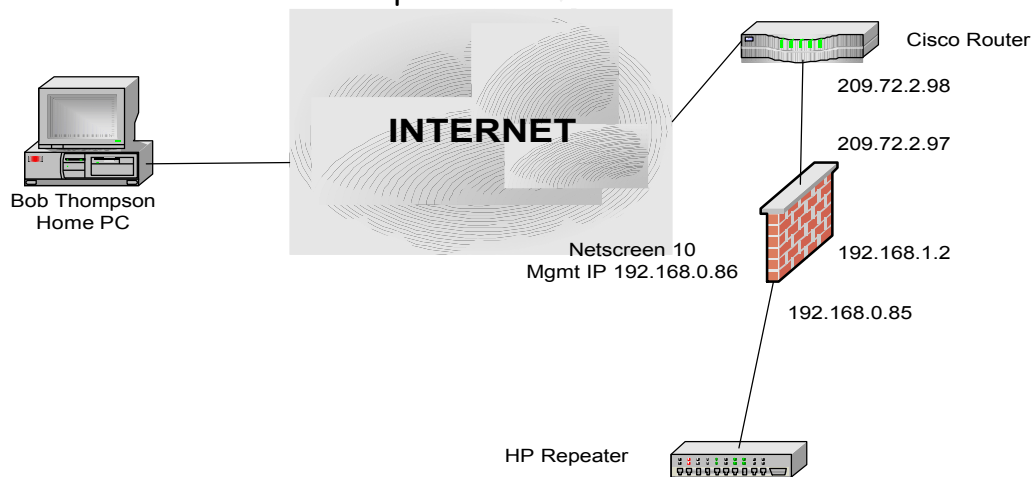
The first step, as with all security related components of the GIAC network, is to determine what, in plain English, our security policy is for the VPN, and the business requirements. GIAC determined these needs for their VPN service.

- The VPN must provide access to remote employees and Partners
- All data must be encrypted as well as the authenticated
- User must have minimal involvement in the setup and maintenance of their VPN tunnel
- IT group should be able to minimize the amount of effort required to maintain the VPN tunnels, for all parties

These requirements are straight forward, and make a lot of sense. The choice was made to go with what Netscreen refers to as "Dialup-to-LAN VPN, AutoKey IKE tunnel with a preshared key. The best way to show the configuration of this type of VPN tunnel is to go through the configuration needed for our first remote user, which in this case will be Bob Thompson, Senior Account Manager for GIAC Enterprises ([Bthompson@giac.com](mailto:Bthompson@giac.com)). For remote employees, a further requirement was added, that employees can only access the Automation server!

The components we are interested in look like this (Illustration 13):

Illustration 13 - Critical components for VPN access to the GIAC network



Setting up a VPN involves a number of decisions regarding the protocols, and encryption algorithms we choose to implement. Additionally VPN requires that each end of the VPN tunnel have a key, a type of password, to encrypt and decrypt the data. Just as each user on the network has a unique password (we hope), each VPN tunnel should also use unique keys.

### 2.5.1 - Defining the VPN technology used

Dealing with VPN's means having to face an onslaught of acronyms, and choices of algorithms. For companies such as GIAC, these choices are not massively important, they just need to be consistent. Since the Netscreen firewall does the encryption/decryption in ASIC, we might as well choose the algorithms which are considered more secure. At the remote end, these choices will require a bit more CPU muscle, but most PC's are quite capable these days. So let us look at the choices that GIAC made, and what they mean.

### **AutoKey IKE**

As mentioned earlier, we need to have each end use a password, or key, to encrypt and decrypt the data. Just as you should change your passwords regularly, it is more secure if we change the keys used regularly. But having to regularly change the keys on your firewall, and getting users to change them, would create a lot of grief for the IT staff.

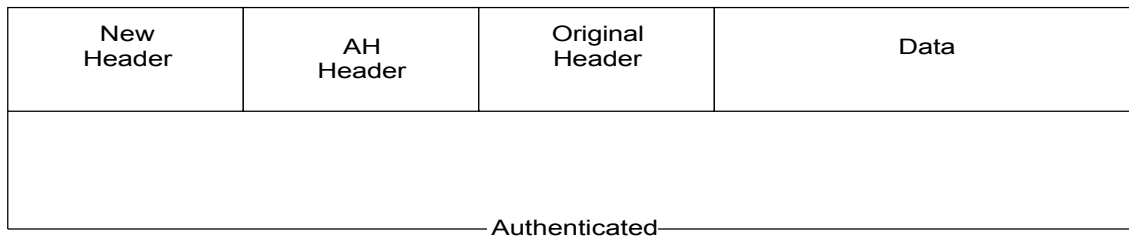
There is a standard for the automated generation and negotiation of new keys called IKE (Internet Key Exchange) protocol. Netscreen calls their implementation AutoKey IKE. AutoKey IKE will allow you to initially setup a VPN tunnel using preshared keys which are entered at both ends of the VPN tunnel during setup, but then it will automatically change the keys used, keeping the data transmissions more secure.

### **Authentication Header (AH) and Secure Hash Algorithm (SHA-1)**

AH is a protocol which allows us to verify the source of the packet (authenticity) and that the contents have not been altered (integrity). SHA-1 is an algorithm which takes our packet, and using a 20 byte key, creates a 160 bit hash. This hash is packaged within the AH, which is placed inside the IP packet, along with a new header.

When the packet arrives at the destination, the AH is removed from the packet, the receiving system calculates the hash the same way, and compares it to what was in the packet. If both hashes are the same, it is reasonable to assume the packet has not been altered. Note that this does not encode the data in any way, it simply ensures that it came from who you expected, and that the data was not changed

Illustration 14 - Authentication Header packet



### Encapsulating Security Payload (ESP ) and Triple DES Encryption Algorithm

ESP is a protocol which allows us to not only authenticate a packet, and verify its integrity, but encrypt the data within the packet, making it extremely difficult for anyone to determine the packet's contents. Triple DES is an algorithm which takes our packet, and using a 168 bit key, encrypts the data. Our packet is then given an ESP header which contains the authentication data. A new header is then pre-pended onto our packet.

When this packet arrives at the destination, the information in the ESP header is used to authenticate the packet, and it's contents. Once authenticated, the original packet (in its entirety) will be decrypted using the Triple DES algorithm.

Illustration 15 - Encapsulating Security Payload packet



Note: There are some differences in VPN as to how the headers are arranged, and pre-pended onto the packet. The method described above is used with Tunnel mode VPN, which is what GIAC is using. This is a requirement of a VPN tunnel when one of the termination points is a gateway device.

### Diffie-Hellman Group

No, not a blues band, Diffie-Hellman is an algorithm which allows the two ends of the VPN tunnel to generate a secure key together, over an unsecured connection, without ever transferring the key over the connection. There are different numbered Diffie-Hellmann groups depending on the length of the modulus used by the algorithm. Netscreen supports Group 1 (768 bit), Group 2 (1024 bit), and Group

5 (1536 bit). GIAC has chosen to use the Group 2 modulus.

### **Main Mode and Aggressive Mode**

In Phase 1 of the VPN tunnel negotiation (discussed below) there are two different methods that can be used. Main mode sends six messages to setup the tunnel, and Aggressive mode sends only three messages. Main mode is slightly more secure, but the Netscreen only supports Aggressive mode for "dial-up" users. Therefore GIAC must use Aggressive mode.

### **Security Association (SA)**

An SA is an agreement on the protocols and algorithms that will be used to setup and maintain a VPN tunnel. The SA must be agreed upon for each direction individually, so one SA from Bob to the firewall, and another from the firewall to Bob.

### **Phase 1 Tunnel Negotiation**

When the VPN tunnel first starts to set itself up, it goes through what you might call a "hand shaking" process, using the information prescribed in the Security Association (SA). In Phase 1, the two ends establish a secure tunnel for communications. The key pieces of information that will be communicated in Phase 1 are:

- Encryption algorithm to use - we chose Triple DES
- Authentication algorithm - we chose SHA-1
- Diffie-Hellman group - we chose group 2
- Preshared key - Any ASCII sequence that both sides know

### **Phase 2 Tunnel Negotiation**

Once Phase 1 completes, we now have a secure communications tunnel, the two sides have to negotiate the Security Association (SA), the agreement of what protocols and algorithms will be used to secure the data. The key pieces of information that will be communicated in Phase 2 are:

- use Perfect Forward Secrecy, or not - we chose not
- use ESP, or AH - we chose ESP
- Authentication algorithm - we chose SHA-1
- Encryption algorithm to use - we chose Triple DES

Note: The authentication, and encryption algorithms, do not have to be the same in

Phase 1 and Phase 2.

## 2.5.2 - Step by Step - Setting up Bob Thompson's VPN access

### Step 1

The first step is to define the address of the host that Bob will need access to. This would be defined by the following line:

```
set address trust "Automation Server" 192.168.0.9 255.255.255.255
```

As this host is already defined on our External firewall, this line would not be required. Remember the mask of 255.255.255.255 specifies one specific host, and not a subnet. Should you wish to grant Bob access to the entire subnet, you could create a new address entry with a different friendly name, any inside IP address (such as the one above), but use the mask of 255.255.255.0 . Bob's access would then be valid for any 192.168.0.x address on your network

### Step 2

We now create a user in the firewall's internal database.

```
Set user bob ike-id bthompson@giac.com
```

This sets up Bob Thompson as the user "bob", and identifies him as an IKE user. IKE then just needs an identity for the user. This is typically their email address.

### Step 3

Now we setup the VPN gateway for Bob, with the Phase 1 information

```
Set ike gateway bob_gw dialup bob aggressive preshare mysecretphrase proposal  
pre-g2-3des-sha
```

This is worth tearing apart a bit to understand what is happening here:

```
Set ike gateway bob_gw - Name our VPN gateway "bob_gw"  
dialup bob - Gateway is for Dial-up user named "bob" in address book
```

*aggressive* - Aggressive mode will be used for Phase 1  
*preshare mysecretphrase* - Our preshared secret key is "mysecretphrase"  
*proposal pre-g2-3des-sha* - For Phase 1 we propose to use a pre-shared key, Diffie Hellmann group 2 modulus, Triple DES encryption, and SHA-1 authentication

#### Step 4

Now we setup the information for the Phase 2 negotiations

*Set vpn bob\_vpn gateway bob\_gw tunnel proposal nopfs-esp-3des-sha*

Tearing this line apart we see the following information has been setup:

*Set vpn bob\_vpn* - Name the VPN tunnel "bob\_vpn"  
*gateway bob\_gw* - name of the gateway we setup in Phase 1  
*tunnel* - this is tunnel mode, because a gateway device is at one end  
*proposal nopfs-esp-3des-sha* - For Phase 2 we propose to use No Perfect Secrecy, Encapsulated Security Payload (ESP), Triple DES encryption, and SHA-1 authentication

#### Step 5 (the end is near)

The last step in configuring the firewall is to setup an Incoming policy

*Set policy id 16 incoming "Dial-Up VPN" "Automation Server" any tunnel vpn bob\_vpn*

And the breakdown of this line is as follows:

*Set policy incoming* - This is a policy for an incoming connection  
*"Dial-Up VPN"* - Source Address is the "Dial-Up VPN"  
*"Automation Server"* - Destination Address is the Automation Server  
*any* - Any service can be used, assuming the host supports it  
*tunnel vpn bob\_vpn* - The connection will be by a VPN tunnel named bob\_vpn

#### Step 6

Now we will need to supply Bob Thompson with a VPN client, and the same sort of configuration information that was used on the firewall. Bob will need to know the Preshared key, and the appropriate choices for authentication and encryption



protocols.

## 2.6 - Securing the Netscreen Firewall

There are a considerable number of items that need to be checked in order to verify that you have secured your firewall correctly. To be quite honest, coverage of all of the options is well beyond the scope of this document, so here are the first steps only.

### Administrative Accounts

The first step is to add a new administrative user to the firewall. I would recommend that each person who has responsibility for the firewall (hopefully not many) has their own administrative account. This is done by entering the following:

```
Set admin user bob password mysecret
```

So Bob is now an admin user on the firewall, with a password of "mysecret"

The second step is to rename the default administrative account "netscreen" , and to change the password. This information should then be stored away in a safe place, and not used unless necessary. This is done in two steps as follows:

```
Set admin name tarzan  
Set admin password jane
```

We now have a firewall admin called "tarzan", password of "jane"

## 2.7 - Enabling Basic IDS Functionality with the Netscreen

There are a number of features built into the Netscreen firewall which can provide some basic IDS (Intrusion Detection System) functionality, as well as a blocking mechanism, for some of the basic network attacks. By entering the following in the command line of the Netscreen, it will determine if one of these attacks is occurring, log the event, and where necessary, take steps to neutralize the attack.

*Set syn-threshold 200*  
*Set firewall tear-drop*  
*Set firewall syn-flood*  
*Set firewall ip-spoofing*  
*Set firewall ping-of-death*  
*Set firewall src-route*  
*Set firewall land*  
*Set firewall icmp-flood*  
*Set firewall udp-flood*  
*Set firewall winnuke*  
*Set firewall port-scan*  
*Set firewall ip-sweep*

A concise description of these attacks, and how the Netscreen responds to them is available on page 2-2 to 2-10 of "Netscreen Concepts & Examples, ScreenOS Reference Guide" version 2.6.0 available in .PDF form from Netscreen's website.

<http://www.netscreen.com/support/manuals.html> (25 July 2001)

### **Setting the Default Deny Policy**

Perhaps the single most important configuration line is this one:

*Set firewall default-deny*

This line is what sets the default "deny all" policy for the firewall, so the last policy for each interface does not have to explicitly block all traffic. This can save you a lot of grief from an incorrectly configured firewall.

### **2.8 - Tip regarding Netscreen documentation**

One last note regarding setting up a VPN tunnel on a Netscreen firewall, the documentation for software version 2.6 is truly terrible. Specifically the documentation contains a great deal of examples of how to configure the firewall for different scenarios. Upon first look they appear to be one of the best set of documents you have ever seen. However there are so many errors in the syntax and usage, that they will frustrate you a great deal.

I would suggest that the documentation is a good place to find the order of steps required, and the basic command(s) required. Then using the CLI you can type the basic command, followed by a space, and then a question mark. The CLI will respond back with suggestions for the next word required on the command line. Although this is a bit painstaking, I found the CLI help, as basic as it is, to be correct at all times.

Downloadable copies of the Netscreen manuals are available here:  
<http://www.netscreen.com/support/manuals.html> (25 July 2001)

## 2.9 - Configuring the Cisco 1751 router

When configuring the security on a Cisco router, there are two different aspects of configuration that require our attention. The first is that we must secure the router itself, disabling unneeded services, and doing our best to ensure the router itself will not be the victim of a successful attack. Secondly we wish to use the packet filtering abilities of the router to reduce the amount of incoming traffic the firewall must analyze, and also filter the outgoing traffic to ensure our site is not a source of illegitimate or forged traffic on the Internet.

### 2.9.1 - Securing the Cisco router

The following are command line snippets to disable services we do not need on the GIAC router. The full syntax, and justification for what we are doing, would require a several manuals otherwise. I have provided the commands to shut down each service individually for clarity. In reality, these commands would be "stacked" together with similar commands.

One word of advice. If you are not well experienced in configuring Cisco routers, it would be very unwise to configure one in a production environment.

Disable the Cisco Discovery Protocol (identify other Cisco routers)

```
config t
no cdp run
exit
```

Disable Small Servers (chargen, echo, etcetera)

```
config t
```

```
no service tcp-small-servers
no service udp-small-servers
exit
```

Disable the Finger Protocol (shows logged in users)

```
config t
no ip finger
no service finger
exit
```

Disable the Web based administration

```
config t
no ip http server
exit
```

Disable Bootp Server (used to remotely load Cisco IOS to another router)

```
config t
no ip bootp server
exit
```

Disable the ability of the router to load configuration from the network

```
config t
no boot network
no service network
exit
```

Disable Source Routing (used to route packets by specific routes)

```
config t
no ip source-route
exit
```

Disable routing packets with no clear route

```
config t
no ip classless
exit
```

Disable Directed Broadcasts (prevent your site from being part of a DOS attack)

```
config t
interface eth 0/0
no ip directed-broadcast
exit
```

Disable Proxy Arp (no reason for ARP to cross our router by proxy)

```
config t
interface eth 0/0
no ip proxy-arp
exit
```

Disable SNMP (Syslog instead, not quite the same, but safer)

```
config t
no snmp-server
exit
```

Disable various ICMP messages to reveal as little as possible to the outside world

```
config t
interface eth 0/0
no ip unreachable
no ip redirect
no ip mask-reply
end
```

Encrypt the router enable password

```
config t
enable secret "mysecretpass"
exit
```

### 2.9.2 - Filtering traffic with the Router - Access Lists Rules

The goal of filtering traffic on the Cisco router is to reduce the "noise" that is presented to the Netscreen firewall, not to replace the firewall in any way. All filtering on the GIAC router will be done using Extended Access Lists. The syntax for building these lists is as follows:

**access-list** access-list-number permit|deny protocol source destination source-mask destination destination-mask operator-operand log

where

access-list-number - is a whole number between 100 to 199

permit|deny - this describes data that we allow, or disallow with our rule

protocol - IP, TCP, UDP, ICMP, GRE, IGRP

source - source IP address

source-mask - masking to indicate which address bits are significant

destination - destination IP address

destination-mask - masking to indicate which address bits are significant

operator-operand - lt, gt, eq, neq (less than, greater than, equal to, not equal) and a port number or name

log - causes information about a packet which matches rule to be logged

All rules which have the same access list number are logically grouped together. They can then be applied to either the inbound, or outbound portion of any of the interfaces on the router.

### 2.9.3 - Blocking illegal addresses incoming to our network

We can build access-list 100 to block all IP addresses which cannot possibly be legitimate traffic, and allow the traffic destined for our screened subnet.

```
access-list 100 deny 10.0.0.0 0.255.255.255
access-list 100 deny 172.16.0.0 0.15.255.255
access-list 100 deny 192.168.0.0 0.0.255.255
access-list 100 deny 127.0.0.0 0.255.255.255
access-list 100 deny 224.0.0.0 0.0.255.255
access-list 100 deny host 0.0.0.0
access-list 100 permit TCP any any eq 80
access-list 100 permit TCP any any eq 443
```

```
access-list 100 permit TCP any any eq 25
access-list 100 permit IP any any established
```

The first three block the reserved Class A, B, and C network addresses. These should never be seen on the Internet, so if they are, they are either due to configuration errors, or malicious activity.

The fourth line blocks any traffic from the Loopback address. This should never be seen on any cable, as it is used only internally on your host.

The fifth line blocks the multicast addresses, and the sixth line the all-zeros address, none of which are valid destinations in GIAC.

Lines seven through ten, allow the HTTP, HTTPS, and SMTP traffic that our screened subnet servers need, while also allowing any traffic that is the result of an established session.

#### **2.9.4 - Allowing our Internal traffic Out**

When we designed the Outgoing Policies on the Netscreen firewall, the idea was to put the most frequently used rules at the top of the list. For example if most of the traffic coming out of GIAC is HTTP traffic, it makes sense to allow the firewall to successfully evaluate the rule, and pass the traffic, as quickly as possible.

The same goes for the border router. Access list rules are evaluated from "top" to "bottom", so ideally they should be in the same order as your firewall Outgoing Policies are.

```
access-list 110 permit TCP any any eq 80 - HTTP traffic
access-list 110 permit TCP any any eq 443 - HTTPS traffic
access-list 110 permit TCP any any eq 20
access-list 110 permit TCP any any eq 21 - FTP traffic
access-list 110 permit TCP any any eq 53 - DNS traffic
access-list 110 permit TCP any any eq 25 - SMTP traffic
access-list 110 permit TCP any any eq 123 - NTP traffic
access-list 110 deny IP any any - Deny everything else
```

## Assignment 3 - Auditing the External Firewall at GIAC Enterprises

### 3.1 - Planning the Assessment

The first step in assessing the External firewall at GIAC is to analyze the setup of the firewall. Special attention should be paid to the firewall policies, identifying the traffic which is permitted, or denied, and the order that the policies are applied. In order to determine whether these policies are correct, GIAC needs to provide a copy of their written Security Policy, detailing which services should be allowed to pass through the firewall. This will help to prevent overlooking what may seem like harmless services, but not allowed because of GIAC company policy.

One of the first steps in auditing the External firewall, is to identify the paths that packets can travel, and to match these paths to the policies that we have defined on the firewall. Since we have three interfaces, and packets can flow in two directions, these are the paths, and policies we need to examine.

From Trusted interface to the Untrusted interface

- policy id 1 outgoing "Inside Any" "Outside Any" "HTTP" Permit
- policy id 2 outgoing "Inside Any" "Outside Any" "HTTPS" Permit
- policy id 5 outgoing "Inside Any" "Outside Any" "FTP" Permit
- policy id 3 outgoing "Domain/DNS/DHCP Server" "ISP DNS Server" "DNS" Permit
- policy id 8 outgoing "Inside Any" "External NTP Server" "NTP" Permit

From Trusted interface to the DMZ interface

- policy id 4 outgoing "Mail Server" "Mail Relay" "MAIL" Permit
- policy id 6 outgoing "Automation Server" "Screened Subnet Web Svrs" "ANY" Permit

From DMZ interface to the Untrusted interface

- policy id 12 fromdmz "Mail Relay" "Outside Any" "MAIL" Permit
- policy id 13 fromdmz "Screened Subnet Web Svrs" "Outside Any" "FTP" Permit

From DMZ interface to the Trusted interface



- policy id 7 fromdmz "Screened Subnet Web Svrs" "Automation Server" "ANY" Permit

From Untrusted interface to the DMZ interface

- policy id 9 todmz "Outside Any" "Mail Relay" "MAIL" Permit
  - policy id 10 todmz "Outside Any" "Screened Subnet Web Svrs" "HTTP" Permit
  - policy id 11 todmz "Outside Any" "Screened Subnet Web Svrs" "HTTPS" Permit
  - policy id 14 todmz "Outside Any" "Screened Subnet Web Svrs" "FTP" Permit
- From Untrusted interface to the Trusted interface
- *policy id 16 incoming "Dial-Up VPN" "Automation Server" any tunnel vpn bob\_vpn*

Once we have determined that the Policies implemented on the External firewall, meet the objectives of GIAC's written Security Policy, we are ready to move onto the testing phase.

### 3.2 - Time required for testing

Testing GIAC's External firewall to verify that the policies are working correctly will take approximately one to two days. As this phase of testing involves simply scanning ports, the tests can be done during the day, unless of course GIAC has bandwidth problems already.

Once the port scanning is completed it would be highly advisable to perform further testing to see if the services that are available can be exploited. Since the purpose of an exploit is often to cause a Denial of Service (DOS), it would be prudent to perform this testing outside of the hours the host needs to be available to others. After completion of this testing, the host should be rebooted to ensure that the host is fully operational. Scanning for exploits is a large topic to itself, and so will not be covered further in this document. Two sources of products for doing this kind of scanning are:

Stealth HTTP Security Scanner 1.0 - freeware for HTTP vulnerabilities  
By Felipe Moniz - [www.hideaway.net/stealth](http://www.hideaway.net/stealth) (5 August 2001)

Various products by Internet Security Systems Inc.  
[www.iss.net](http://www.iss.net)

### 3.3 - Tools used for testing

All tools used for testing the firewall are available at no cost, or were included with my desktop operating system (Windows 2000). The tools used were:

Windump v3.52 by Politecnico di Torino

[www.netgroup-serv.polito.it](http://www.netgroup-serv.polito.it)

Windump is a great command line driven, packet capture program for Windows

The basic syntax is

*Windump* [Options]

NmapNT v2.53 by [ryan@eEye.com](mailto:ryan@eEye.com)

EEye Digital Security ( [www.eEye.com](http://www.eEye.com) )

Based on nmap by [fyodor@insecure.org](mailto:fyodor@insecure.org)

NmapNT is a command line driven, port scanning program for Windows NT/2000

The basic syntax for nmapNT is

*Nmapnt* [Scan Type] [Options] <Host Address>

SuperScan v3.00

Foundstone ( [www.foundstone.com](http://www.foundstone.com) )

SuperScan is a Windows based GUI application for scanning TCP ports

Telnet v5.00

Microsoft Corporation ( [www.microsoft.com](http://www.microsoft.com) )

Telnet is a command line terminal program

The basic syntax for Telnet is

*Telnet* <Host Address> [Port Number]

You may ask why would four different tools be used for port scanning. NmapNT is a highly configurable port scanner which can scan both TCP and UDP ports, however I find the Windows implementation to be fairly slow. Documentation is poor, however by searching the Internet you can find further examples of the correct usage.

SuperScan is a fast Windows based TCP scanner, which is very easy to use, with most options being very intuitive. I did find that when it is set to scan at the highest speed (default setting), it would miss ports which were known to be active, but did not respond quickly enough. This is easily remedied by using a sliding control button marked "Speed" to slow the scanning rate down.

Telnet is the preferred program for those of us who need a quick answer as to whether ports like FTP, SMTP, and HTTP are open. Most operating systems ship with a version of Telnet, so for those of us who are comfortable with command line programs, it is hard to beat the simplicity and speed of Telnet.

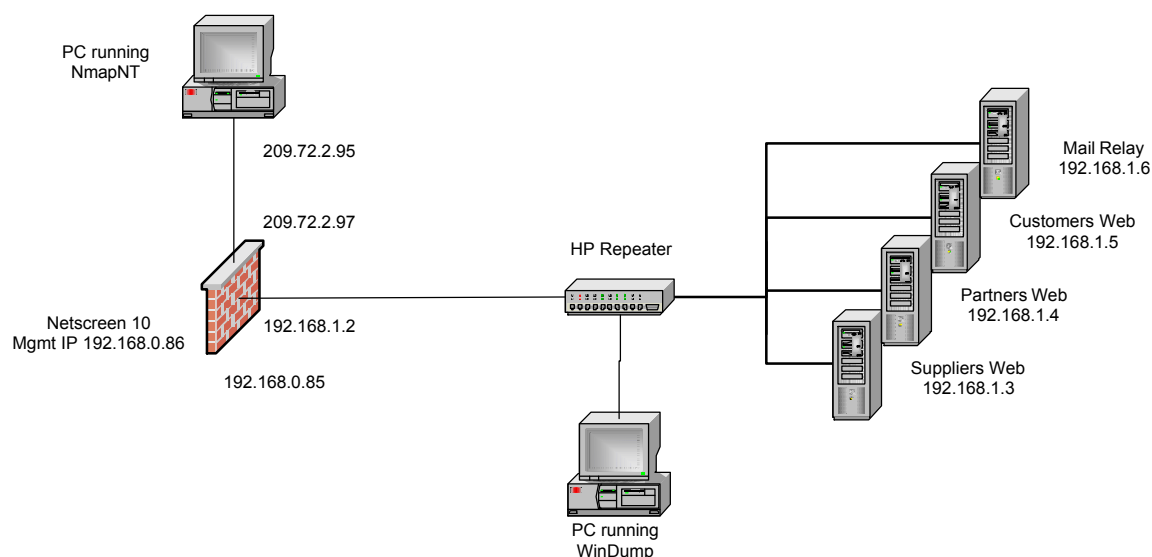
Windump is just a great little packet capture program which serves to verify whether traffic is actually present or not. As good as the port scanning programs are, they can only report on the response they receive back from the host in question. Windump allows us to see both the query, and the response, which goes a step further than a port scanner can.

### **3.4 - Implementing the Assessment on the External Firewall**

There is nothing difficult about testing whether the appropriate ports are open on the External firewall, but it does require that you be very methodical about it. As an example we can test for open TCP and UDP ports on the external interface's IP addresses. For example, we defined that our Mail Relay Server at 192.168.1.6 on the Screened subnet, should be mapped to an external IP address of 209.72.2.99. Using our incoming policies, we configured the firewall to only allow SMTP traffic to pass through from the Internet, to our Mail Relay.

So in order to verify whether this policy is working correctly we would setup our testing to look like this:

## Illustration 16 - Test Setup for Verifying External Firewall Policy



From our PC running NmapNT we would type the following line:

```
Nmapnt -sT 209.72.2.99 -p 1-1024 -PO -v
```

*-sT 209.72.2.99* - This initiates TCP scan on our hosts mapped IP address

*-p 1-1024* - Scan ports from 1 to 1024

*-PO* - Don't ping the host (we know that external Ping response is disabled)

*-v* - Use verbose output

NmapNT reported finding that "TCP port 25 (state open)", meaning that it received a response to its probe of port 25, where SMTP normally resides.

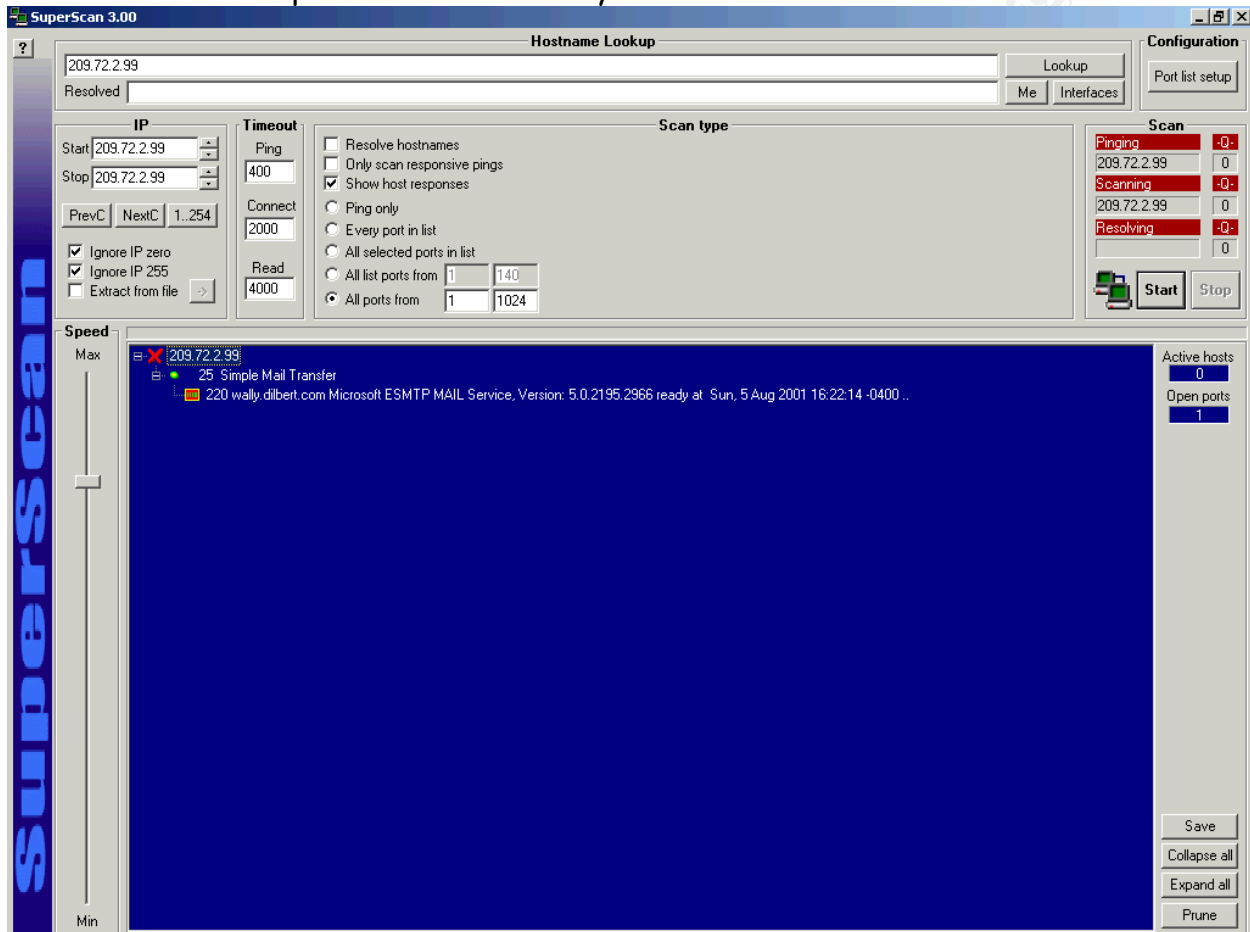
Our PC running Windump saw the following traffic, confirming that the NmapNT scan passed through the firewall, and that the host responded.

## Illustration 17 - Packet Capture of traffic on Screened Subnet during port scan

```
16:40:57.630620 209.72.2.95.2022 > 192.168.1.6.25: S 178030563:178030563(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
16:40:57.636051 192.168.1.6.25 > 209.72.2.95.2022: S 3127649278:3127649278(0) ack 178030564 win 17520 <mss 1460,nop,nop,sackOK> (DF)
16:40:57.636263 209.72.2.95.2022 > 192.168.1.6.25: . ack 1 win 17520 (DF)
16:40:57.637869 192.168.1.6.25 > 209.72.2.95.2022: P 1:120(119) ack 1 win 17520 (DF)
16:40:57.662084 209.72.2.95.2022 > 192.168.1.6.25: R 178030564:178030564(0) win 0 (DF)
```

Running SuperScan gave us the same results (Illustration 18), reporting that port 25, SMTP was open, and providing us with the response from port 25, which confirms that SMTP is the service running on this port.

Illustration 18 - SuperScan of Mail Relay host



The test is run again, but this time scanning for open UDP ports

Illustration 19 - NmapNT scan of UDP ports on Mail Relay host

```
d:\nmapnt>nmap -sU 209.72.2.99 -p 1-1024 -P0 -v

Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security < http://www.eEye.com >
based on nmap by fyodor@insecure.org < www.insecure.org/nmap/ >

Initiating FIN, NULL, UDP, or Xmas stealth scan against <209.72.2.99>
The UDP or stealth FIN/NULL/XMAS scan took 619 seconds to scan 1024 ports.
<no udp responses received -- assuming all ports filtered>
All 1024 scanned ports on <209.72.2.99> are: filtered
Nmap run completed -- 1 IP address <1 host up> scanned in 644 seconds
```

Our PC running Windump confirmed that no UDP ports were open/reachable, by not seeing any traffic on the Screened Subnet during our scan.

Each of the firewall policies can now be tested in the same way. The Windump PC is placed on the same segment as the host being tested, and the NmapNT PC is placed on the segment from which the traffic to the host would originate. NmapNT will report any responses it sees from the host, and Windump will confirm whether any packets passed through the firewall, and whether the host responded. For testing the TCP ports, SuperScan can be used instead of NmapNT, or as a double check of the scanning accuracy.

Once all of the IP addresses which are known to be in use have been scanned, the addresses which are not supposed to be in use should be scanned. The public IP space of GIAC consists of addresses from 209.72.2.97 to 209.72.2.110 inclusive. Our external firewall setup indicates that the firewall uses address 209.72.2.97, and the Screened Subnet hosts use 209.72.2.99 through 209.72.2.102. Scanning all other addresses should produce no responses.

### **3.5 - Perimeter Analysis**

#### **3.5.1 - Multiple firewall OS's**

One of the potential weaknesses is that all of the firewalls at GIAC are running the same operating system, ScreenOS. Potentially a fault found in the ScreenOS could be used to simultaneously defeat all of the firewalls at virtually the same time. If GIAC was a company which held some appeal to Black Hat hackers, it would be advisable to use a different firewall model for the External firewall versus the internal firewalls. My recommendation would be to go with another appliance type product, such as the Cisco Pix series.

For more information on Cisco Pix Firewalls:

<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/> (06 August 2001)

However, in smaller organizations, where technical knowledge is perhaps not as broad as in a larger company, staying with one make of firewall may be more secure. Why? It is difficult to know many products well. Staying with one make of firewall may decrease the chances of the administrator making an error in the configuration.

### **3.5.2 - Use of alternative firewall technologies**

An alternative firewall would be the proxy-type, which will further isolate GIAC's network from the Internet, and may provide some further defense against an exploit meant to cripple a host. The drawbacks to these types of firewalls are that they are CPU intensive, requiring a more powerful platform, and a limited number of proxies are available, providing limited protection to your services. Most proxy-type firewalls are based on general purpose operating systems, which introduce other vulnerabilities to the firewall.

### **3.5.3 - Implementing high availability for the firewall**

In order to enhance the availability of GIAC's hosts, the Netscreen 10 used as the External Firewall, could be replaced by two Netscreen 100's in a "high availability" configuration. One Netscreen 100 is active, while the secondary Netscreen 100 monitors the state of the active one. Should the active Netscreen fail, the secondary Netscreen will begin operating, while preserving all active sessions. All network operations will appear normal to the users, and the administrator can arrange for the replacement of the failed unit at a later time. This is an excellent solution for those concerned with maximum availability.

### **3.5.4 - An alternative "almost high availability" solution for the firewall**

A much less expensive alternative would be to keep a spare Netscreen 10 firewall, and ensure that the configuration of the current firewall has been saved to a text file on the network. Should the External Firewall fail, the replacement firewall could be up and running in as little as five minutes, especially if the standby firewall is kept configured the same as the one in use.

### **3.5.5 - Determining if there are attack patterns outside your firewall**

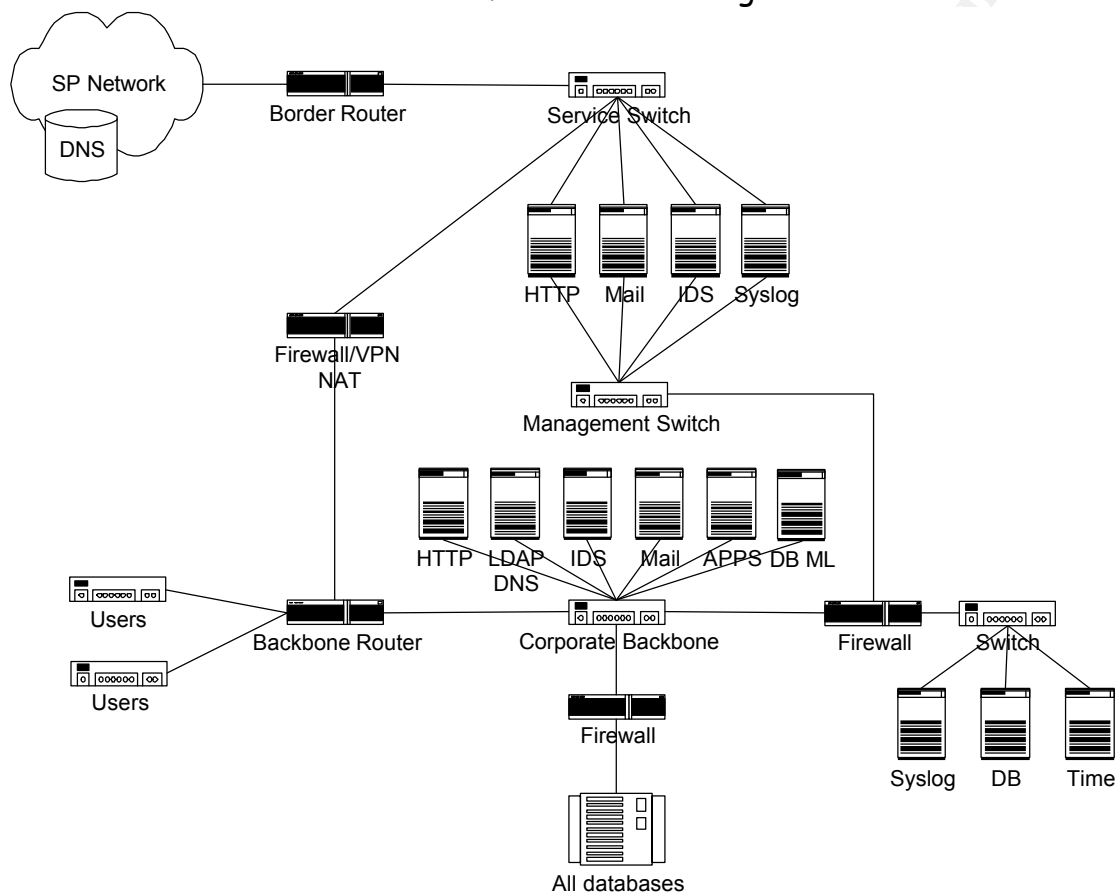
If the I.T. staff at GIAC have the time and resources available, they may wish to place an ICEcap IDS console on the outside of their firewall. By analyzing the attack patterns, they may be able to determine if there is an attacker who is determined to assault their firewall until they find a way in. This will give the GIAC staff an opportunity to double check their defenses, and consider filtering certain IP addresses. Additionally it would be a good idea to notify the party responsible for the source IP addresses of the attack, and request their help in stopping the activity.

## Assignment 4 - Design Under Fire

I have chosen the network design of Tim Kidder GCFW to analyze. His submission may be found at:

[http://www.sans.org/y2k/practical/Tim\\_Kidder\\_GCFW.zip](http://www.sans.org/y2k/practical/Tim_Kidder_GCFW.zip) (06 August 2001)

Illustration 20 - Tim Kidder's Infrastructure Design



### 4.1 - Basic design flaw of network

One of the problems I see with this design is that there are six targets which can be attacked, before we even reach either of the firewalls (seven if you include the Management Switch). These would be the following:

Cisco 3640 "Border Router"

Cisco 2912XL "Service Switch"

Linux hosts "HTTP", "Mail", "IDS", and "Syslog"



#### **4.2 - Border router's configuration affects unprotected hosts**

In the section titled "IOS Pseudo configuration" (page 11) it shows that traffic destined to TCP ports 20,21,25,53,80, and 443, as well as UDP port 53, is allowed to go to any host inside the Border Router. Furthermore, in the section titled "Border Router", subtitle "Allowed Traffic" (page 10), it states that the router policy will also allow all TCP traffic destined to ports about 1023. This certainly gives an attacker a better opportunity to exploit weaknesses in the exposed hosts (including the Service Switch). It would be much more secure if only the appropriate traffic was allowed to go to each host. For example, the Mail host should only see port 25 traffic, and not be exposed to someone trying to make use of an HTTP, or FTP exploit. Additionally, if one of the Linux hosts is compromised, and a Trojan, or Back Door is installed, they can conveniently use one of the ports above 1023 for communication.

#### **4.3 - Intelligent Switch is itself a target of attack**

Tim's Service Switch, a Cisco 2912XL is a managed switch, running Cisco IOS, supporting SNMP, Telnet, and HTTP services(!). Since the Border Router allows port 80 traffic to any host, this opens the Service Switch up for attack. Cisco has issued a Security Advisory which describes the "IOS HTTP Authorization Vulnerability" which could give an attacker complete control over both the Service Switch, and the Border Router, a Cisco 3640 router.

<http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html> (06 August 2001)

#### **4.4 - An attack against the firewall itself**

Tim had prudently configured the Main Firewall, a Cisco Pix 525 with the current (at that time) version of software, version 6.0. Since that time Cisco has found that Secure Shell (SSH) traffic can be intercepted, and arbitrary commands can be inserted into an established session. This hack is described here:

<http://www.cisco.com/warp/public/707/SSH-multiple-pub.html> (06 August 2001)

So if SSH was enabled in an attempt to provide a very secure method of remotely managing the Main Firewall, the SSH vulnerability may allow an attacker to control the firewall. The consequences could include the attacker opening ports to allow them access to the internal network, or damaging the operating system so that the PIX would fail.

#### 4.5 - Denial of Service Attack

My chosen initial target for a Denial of Service (DOS) attack would be the Service Switch. As all access to and from the network is through this switch, and since switches are often not secured as well as the higher profile components (Router, Firewall) in a network, it may be an easy target. Since the Cisco 2912XL has a built in web server the first thing to try would be to go directly with a web browser to the switch, and attempt to login to it. If this is successful, you could simply trash the configuration, and shut everyone down.

Next we would setup our 50 cable modem/DSL zombies to send SYN requests to port 80 on the Cisco switch, attempting to overwhelm it with requests for TCP connections. This may cause the CPU on the switch to become so busy it cannot service legitimate requests to move traffic. Alternatively, we may be able to overwhelm the TCP stack, and crash the operating system.

My countermeasure would be to remove the Cisco switch and put in a dumb, non-managed repeater, eliminating this as an attack destination. As the Internet connection is at T1 speeds, any repeater is more than capable of handling the traffic. This solution makes the job of the IDS easier, as all traffic is immediately repeated out onto all ports.

My ideal countermeasure would include putting ALL hosts (other than Border Router) on this network behind a firewall, and configuring the firewall to pass only what traffic needs to be passed to each host.

Additionally, there is some configuration that can be done on the Border router to eliminate some DOS attacks, and reduce the effects of others. These include the following commands:

Ip verify unicast reverse-path

- Eliminates packets which have been source IP address spoofed

Filter all of the Private IP Address Spaces

- Eliminates traffic with illegal IP addresses

Rate-limit

- Limits the data per second for the traffic you define

For more information:

<http://www.cisco.com/warp/public/707/newsflash.html> (06 August 2001)

#### 4.6 - Attack plan to compromise an internal system through the perimeter

Since in my mind, the firewall is not in the correct position in this network, I would go after the "low hanging fruit", the four Linux hosts sitting in front of the firewalls. Tim has been vague about the specific operating system, and the Web software running on his public web server. Since Linux and the various Web server packages frequently have exploits published, this would probably be a good host to start with.

The first step is to identify the operating system and the web software being used. Some webmasters make this easy, and identify this information on their website. Some are even so kind as to provide you with detailed information about the hardware they are running it on. If you know the hardware, you may be able to take advantage of "holes" in software which is routinely installed on that manufacturers hardware. One example is found at:

[http://www.compaq.com/support/techpubs/customer\\_advisories/ES990604\\_CW01\\_0.html](http://www.compaq.com/support/techpubs/customer_advisories/ES990604_CW01_0.html) (06 August 2001)

This advisory identifies that if someone can access port 2301 on Compaq Servers running older versions of their management agents, they can read files on the server. As the Border Router in this configuration allows inward access to ports above 1023, this type of vulnerability would be of concern.

Note: This advisory does not appear to be relevant to a Compaq Server running Linux. It is presented only as the kind of vulnerability that can be researched should you be able to identify the hardware platform.

Once you have identified the software running on the server you can then use the web to research the vulnerabilities. Common sources for this information include the Developers websites, Security websites, and Hacker websites. Although the Developer and Security websites will do a fine job of reporting the problem, and the cure, if you are looking for an exploit, you will wish to spend more time researching the Hacker websites.

An example of a vulnerability would be a Linux web server running Chilisoft ASP software. If a default installation of this software is performed (don't most

people pick "default"? then a default username and password will be setup. If this username and password are not changed, someone could remotely connect to the server with root privileges. For more information:

<http://www.chillisoft.com/security/3NIX.asp> (06 August 2001)

## List of References and Further Reading

"Router Security Configuration Guide". ver 1.0g. 20 April 2001. URL:

[http://nsa1.www.conxion.com/cisco/r1/router\\_security\\_configuration\\_guide.pdf](http://nsa1.www.conxion.com/cisco/r1/router_security_configuration_guide.pdf)  
(9 Aug 2001)

Brenton, Chris. Firewalls 101: Perimeter Protection with Firewalls. SANS 2001.  
May 2001. 19-23

Stevens, Richard W. TCP/IP Illustrated Volume 1. Reading. Addison Wesley. 1994.  
215-219

Chappell, Laura. Introduction to Cisco Router Configuration. Indianapolis. Cisco  
Press. 1999. 313-323

#### **Cisco 1751 Router**

<http://www.cisco.com/univercd/cc/td/doc/pcat/1750.htm> (25 July 2001)

#### **Netscreen Firewalls**

<http://www.netscreen.com> (06 August 2001)

#### **Hewlett Packard Switches, and Hubs**

<http://www.hp.com/rnd/products/switches/switch4108GL/summary.htm> (25 July  
2001)

<http://www.hp.com/rnd/products/switches/switch4000/summary.htm> (25 July  
2001)

[http://www.hp.com/rnd/products/hubs/10\\_100hub/summary.htm](http://www.hp.com/rnd/products/hubs/10_100hub/summary.htm) (25 July 2001)

#### **Network Ice ICEpac**

[http://www.networkice.com/products/icepac\\_suite.html](http://www.networkice.com/products/icepac_suite.html) (25 July 2001)

#### **Windows 2000, and Windows 2000 Security**

<http://www.microsoft.com/windows2000/professional/default.asp> (06 August  
2001)

Main webpage for Windows 2000 Professional product information

<http://www.microsoft.com/windows2000/server/default.asp> (06 August 2001)

Main webpage for Windows 2000 Server product information

<http://www.microsoft.com/security/> (25 July 2001)

Microsoft's home page for security related links

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/bestprac/bestprac.asp> (25 July 2001)

One of Microsoft's better links to Practices and White Papers

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/tools.asp> (25 July 2001)

A good Microsoft link to Checklists, Tools, and Updates

<http://support.microsoft.com/support/servicepacks/Windows/2000/> (25 July 2001)

Microsoft's Windows 2000 Service Pack page

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp> (25 July 2001)

Microsoft's Security Bulletins!

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp> (25 July 2001)

Link to subscribe by email to Microsoft Security Bulletins - free

### **Computer Security Organizations**

**SANS Institute** (You might have heard of them)

<http://www.sans.org/newlook/home.htm> (06 August 2001)

Excellent source of Security information, and training

### **National Infrastructure Protection Center**

<http://www.nipc.gov> (06 August 2001)

U.S. government site reporting on threats to critical infrastructure

### **Information Systems Security Organization - National Security Agency**

<http://www.nsa.gov/isso/index.html> (06 August 2001)

Great reference guides for securing systems

### **Computer Security Incident Handling**

Various Authors. Computer Security Incident Handling: Step-by-Step. SANS Institute

Information Security Reading Room - Incident Handling & Forensics

[http://www.sans.org/infosecFAQ/incident/incident\\_list.htm](http://www.sans.org/infosecFAQ/incident/incident_list.htm) (06 August 2001)

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

### **Special Thanks**

I would like to thank my wife Gayle, and my sons Jameson and Liam, who had to be very patient, and do without my presence for long periods of time during the preparation of this paper.

I would also like to thank Stephen Northcutt, and Chris Brenton, for their hard work, and humour, in presenting the GFCW curriculum at SANS 2001 in Baltimore. Not wishing to leave anyone else out, a big thanks to all of the people at SANS who put forth such a great effort preparing course materials, and staging the best technical conferences I have attended in about 20 years. Thanks everyone!

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