



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

**GIAC Training & Certification**  
**LevelTwo Firewalls, Perimeter Protection and VPNs**  
**GCFW Practical Assignment**  
**Version 1.5d**  
**By Greg Curless**  
**January 28 – February 2, 2001**

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

## Assignment 1 – Security Architecture (25 Points)

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

You must consider and define access for:

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

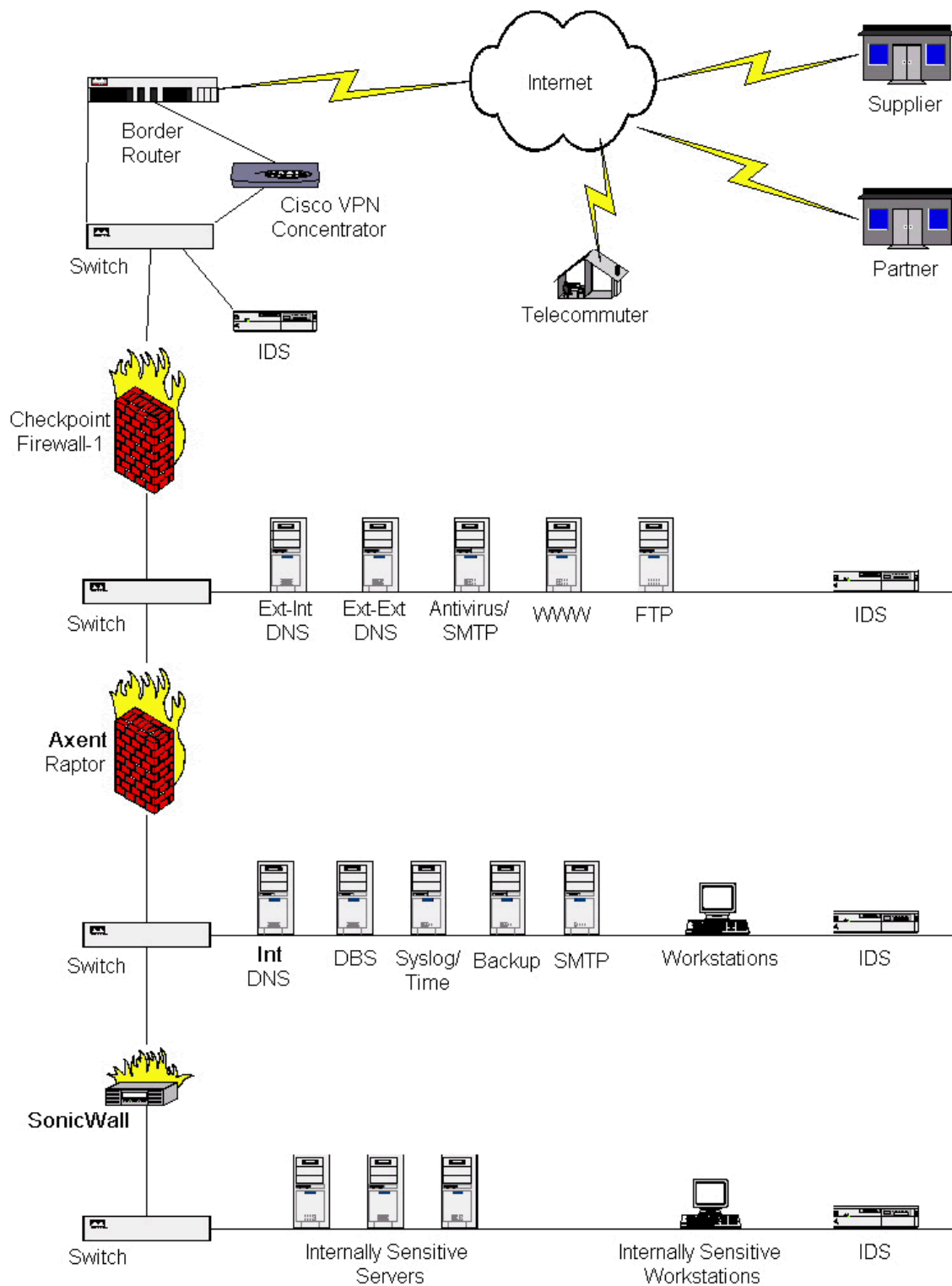
### Required access for GIAC Enterprises to do business

Customers will connect to our secure GIAC Enterprises Web server for their online purchase of fortunes and will also be able to send us email if they experience problems, have any questions, etc. Our customers, as well as any untrusted users, will have HTTP & HTTPS access to the Web server, SMTP access to the mail relay server, and DNS resolution access to the ext-ent DNS server.

Suppliers (in addition to the untrusted user access) will have list and put access to their individual directory of the FTP server via the VPN.

Partners (in addition to the untrusted user access) will have list and get access to their individual directory of the FTP server via the VPN.

Employees will only have access to the devices that their job responsibilities require. Telecommuters (any employee connecting from off site) will be required to connect through the VPN Concentrator from a pre-configured PC that has up to date anti-virus software, and an approved SOHO or host based firewall protecting it.



Having good security requires that security be considered at all levels. A firewall will not protect you against an internal user or even an external user that has compromised an internal box. While I won't go into detail on securing systems not required for this assignment, I will mention a few security practices that should be followed...

SANS securing step-by-step, and other guides, will be used to create a security profile for each type of system on the network. This will include setup of such things as anti-virus software, running only needed services, using Tripwire, etc.

New patches and service packs will be tested and installed in a timely manner.

Security advisory email lists will be monitored such as; The CERT Advisory Mailing List ([www.cert.org](http://www.cert.org)), Bugtraqs ([www.securityfocus.com](http://www.securityfocus.com)), Microsoft Security Notification Service ([www.microsoft.com/technet/security](http://www.microsoft.com/technet/security)), Security Alert Consensus ([www.sans.org](http://www.sans.org)), etc.

Security related sites will be monitored such as; [www.sans.org](http://www.sans.org), [www.searchsecurity.com](http://www.searchsecurity.com), [www.securityfocus.com](http://www.securityfocus.com), [www.cisecurity.org](http://www.cisecurity.org), [www.attrition.org](http://www.attrition.org), etc.

All devices will have logging enabled, and if supported, will log to the syslog server.

An NTP server will be used to sync date and time on devices.

All users will have unique usernames.

Passwords must be a minimum of 8 characters in length and include upper case, lower case, and numeric values. Passwords must be changed every 90 days and can not be repeated. A password cracking program will be used on a regular basis to check compliance.

Vendor default passwords must be changed to comply with the password standard.

Anytime a user leaves, be they fired or not, all passwords will be changed. An audit will be done of the accounts on all devices (includes servers and workstations). A full port scan of the entire network will be performed to check for back doors.

No modems will be allowed. Tonloc, TeleSweep Secure, or some other software will be used to check compliance.

Only approved software will be installed on computers (no pcAnywhere, America Online Instant messenger, ICQ, etc.).

All network communication will be done encrypted when possible (SSH instead of telnet, etc.).

A network wide port scan will be done on a regular basis to verify open ports are limited to those that should be open.

All networking devices and servers are in secured rooms.

### The security networking architecture

The Border Router is a Cisco 2621 running IOS version 12.1 and, with its ACL, will serve as our first tier of defense. It is fast enough to handle a full T3 and has two 10/100 ethernet ports, which are required for this setup. The border router will block some basic things such as spoofed IP addresses, telnet, SNMP, etc.

The VPN device is a Cisco 3030 VPN Concentrator running version 3.0.00 of the software. This device will handle up to 1500 simultaneous connections and has a throughput of 50 Mbps at 3DES-168 encryption. It can be upgraded to a 3060, which supports speeds of 100Mbps at 3DES-168, if needed in the future. By using a dedicated VPN device we lessen the load from the router or firewall that would have had to do it. Also, with this configuration, incoming VPN traffic will have been decrypted before going through the external firewall and therefore will be analyzed by the firewall. The VPN gives us encrypted traffic to and from our partner and supplier's networks as well as to and from our remote employees connecting from home. My preference would be no RAS but it is required in the assignment.

Switches are Cisco 3500 Series XLs. This gives us 100Mbps speed on the LAN as well as room for growth. They are scalable, stackable and support Gigabit speeds.

There is an Intrusion Detection (IDS) appliance on each segment of the network.

The external firewall is a Checkpoint Firewall-1 running version 4.1 service pack 3. It is on a SUN E220R running Solaris 2.6. Firewall-1 gives us ease of management, high configurability, OPSEC compatibility and stateful inspection. The E220R has dual 450Mhz Ultra SPARC-II CPUs, 4MB of E-cache, 2GB of ECC RAM and redundant power supplies. Solaris 2.6 is extremely stable which is very important for an E-Commerce business and can be a secure OS. This combination should give us a little over 200Mbps throughput, which should be more than enough to handle our needs. Firewall-1 sits between layers 2 and 3 and therefore looks at packets before they reach the system's OS. However, we will still harden the OS. The external, or parameter, firewall is used to only allow incoming and outgoing traffic that is approved based on its source, destination and service type.

The firewall protecting the corporate network is an Axent Raptor Firewall version 6.5. It will also be on a SUN box running Solaris 2.6. It is being used for its application layer protection and will serve as a proxy server and do NAT for the internal network. The use of different types of firewalls creates a heterogenous environment increasing the level of

security. As with the external firewall, the OS will be hardened. The final firewall protecting internally sensitive servers, workstations, printers, etc. is a SonicWall XPRS2 appliance. These devices are excellent for protecting departments from employees who might be tempted to look for sensitive company information such as payroll.

### Screened network

*Unless otherwise noted, all servers run a hardened Open BSD version 2.7 OS*

The Ext-Int DNS server resolves public DNS address for internal users only.

The Ext-Ext DNS server is used by the outside world to resolve the addresses of our public servers. It has only public server information on it.

All incoming and outgoing email will be relayed through the Antivirus/SMTP relay server where it will be scanned for viruses using something like Trend Micro's InterScan VirusWall.

The public web server runs Apache SSL version 1.3.14. This is the server that our customers connect to. This server works as a front end for the DBS server on the corporate network.

The FTP server has a directory set up for each supplier and each partner and they are limited to list/put and list/get access respectively in their own directory. Anonymous access is disabled. This server also uses TCP wrappers to add an additional layer of security.

### Corporate network

*Unless otherwise noted, all servers run a hardened Open BSD version 2.7 OS*

The Int-DNS server contains internal DNS information for internal users only. All external IPs are blocked from access.

The DBS server contains the database with fortune and customer information. The public web server is the only IP outside the corporate network that can access this server. The database is also encrypted and credit card data is deleted when no longer needed.

The syslog/NTP server is limited to syslog and network time protocol only. Network devices (routers, switches, VPN concentrator, etc) and servers log to the syslog server and do hourly time syncs to it. The reason you have all times synced to the same source is for forensics. This way the times in the syslog for all devices are correct in relation to each

other.

The backup server performs backups over SSH.

The internal SMTP server receives incoming mail from our SMTP server in the screened network and sends all outgoing mail through the same.

All workstations will adhere to strict hardening procedures. As with servers, only needed services will be loaded. All workstations must have antivirus software installed and configured to auto update.

#### Internally sensitive network

Servers and workstations are inaccessible from outside this network. Outgoing connections can be initiated but not incoming. They are hardened and have antivirus software configured to auto update. Physical access is also controlled.

#### Architecture Summary

This architecture gives us multi-tiered network security, or defense in depth. A hacker must get through several layers of security before getting to any servers with confidential information. While nothing is fool-proof, when you take into account the hardened OSes and things like the data on the DBS server being encrypted, it should prove to be a challenge to any external hacker.

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



## Assignment 2 - Security Policy (25 Points)

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

- Border Router
- Primary Firewall
- VPN

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

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

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

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

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

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

---

## **Border Router**

This is not a complete router setup. Only the security configuration of the border router will be covered.

Secure access to the router itself:

access-list 10 allow ip x.1.2.0 0.0.0.255 any log	- access from our IP range only
access-list 10 deny ip any any log	- deny and log
line vty 0 4	- virtual terminals 0 - 4
access-class 10 in	- apply the access list in the direction specified

Log to the syslog server:

service timestamps log datetime msec	- time-stamps log entries
no logging console	- not needed & gets in the way
logging trap notification	- level of events to log
logging facility local1	- facility to use on syslog
logging x.1.2.133	- syslog server's IP

Get time from the NTP server:

ntp broadcastdelay 10	- estimated delay in microseconds
ntp update-calendar	- updates the date and time
ntp server x.1.2.133 prefer	- NTP server's IP

Encrypt passwords and set enable password:

service password-encryption	- password encryption
enable secret xxxxxxxx	- MD5 hash on password

Stop some unneeded services from running on the router:

no service finger	- shows users logged in
no cdp running	- Cisco Discovery Protocol
no bootp server	- bootp protocol
no ip source-route	- used in some spoofing

These would be disabled if not off by default in IOS version 12.1:

no ip directed-broadcast	- used in smurf attacks
no service tcp-small-servers	- stop chargen, discard, echo
no service udp-small-servers	
no ip snmp	- could give up configuration
no ip http server	- not needed

To help protect the router from flood attacks we will use the following:

scheduler interval 500	- forces process-level task handling at least every 500 msecs
------------------------	---

Globally created access list for incoming traffic on the external interface:

access-list 101 deny icmp any any	- no ICMP
access-list 101 deny ip 0.0.0.0 0.0.0.0 any	- invalid address
access-list 101 deny ip 10.0.0.0 0.0.0.255 any	- private addresses
access-list 101 deny ip 127.0.0.0 0.0.0.255 any	- loopback address
access-list 101 deny ip 172.16.0.0 0.0.15.255 any	- private addresses
access-list 101 deny ip 192.168.0.0 0.0.255.255 any	- private addresses
access-list 101 deny ip 224.0.0.0 31.255.255.255 any	- multicast addresses
access-list 101 deny ip x.1.2.0 0.0.0.255 any	- our IP addresses
access-list 101 deny udp any any eq snmp	- no SNMP
access-list 101 deny tcp any any eq telnet	- no telnet (use SSH)
access-list 101 permit ip any any	- needed due to Cisco's implicit deny

Access list applied to the interface:

interface serial 0/0	- our WAN link
ip access-group 101 in	- applied to inbound

Globally created access list for outgoing traffic on the external interface:

access-list 102 permit ip x.1.2.0 0.0.0.255 any	- our IP range only allowed out
access-list 102 deny ip any any log-input	- logging includes MAC address

Access list applied to the interface:

interface serial 0/0	- our WAN link
ip access-group 102 out	- applied to outbound

### Test it

Telnet to the border router and other internal devices from an outside IP.  
 Perform an SMTP scan from outside.  
 Finger the border router.

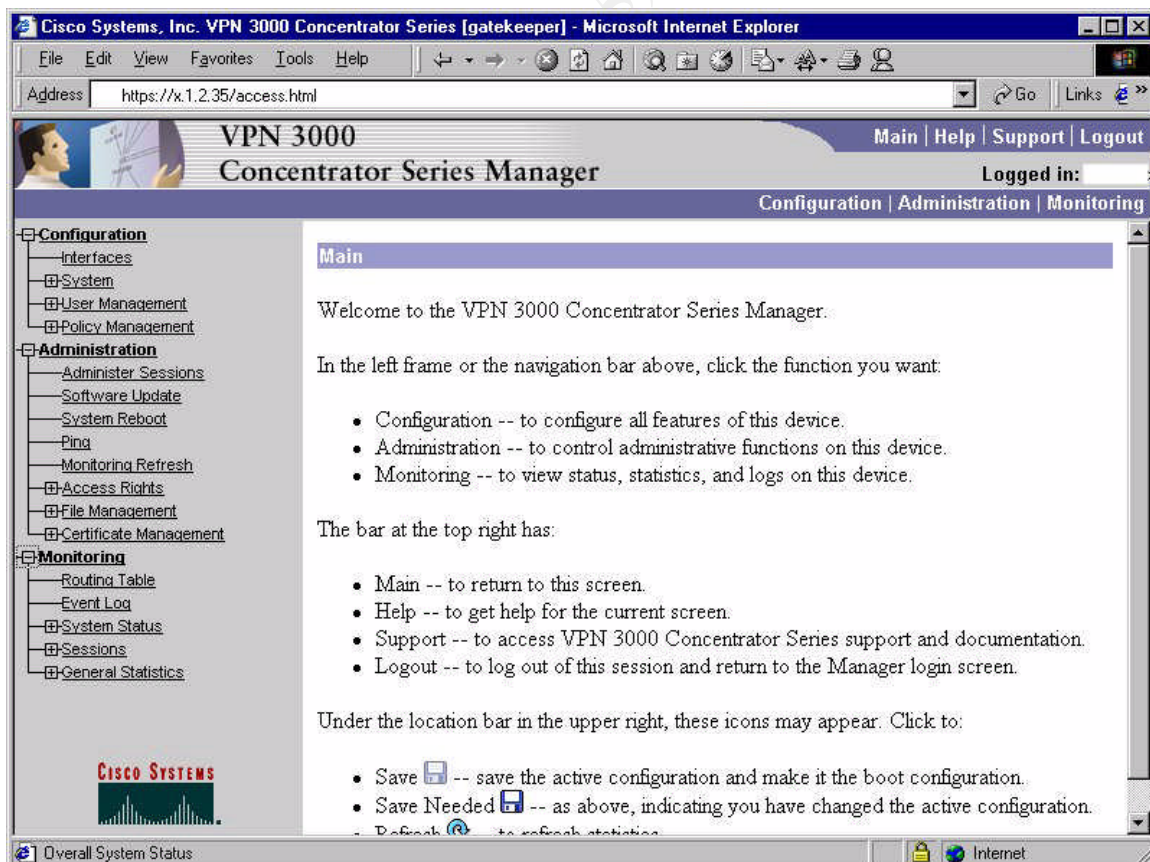
Ping an internal device from outside with a private IP address such as 192.168.3.3.  
Ping an external device from inside with a private IP address such as 192.168.3.3.  
Do a ping sweep of x.1.2.0.  
Set the date and time incorrectly on the border router and see if NTP sets it correctly.  
Check the syslog to see if the border router sent any data from these tests.

## The DMZ Switch

The switch between the border router and the firewall is layer 2 and will not have a management IP address. It is only manageable from the console.

## VPN Concentrator

The Cisco 3030 VPN Concentrator can be set up via console or a web interface. The complete setup of the concentrator will not be shown, only the security related LAN-to-LAN and RAS setup. Below is a full screen capture of the web interface.



NOTE – Be sure to click on “Save needed” when finished in order to save your changes to the configuration file.

## Access Control

One of the first things we want to do is limit which IPs can access the web interface. In the shot below a single IP is set up for group 1 access. We can have multiple single IPs as well as ranges of IPs. This screen is found under Administration/Access Rights/Access Control List/Add.

Administration | Access Rights | Access Control List | Add

Add a manager address to the access list.

IP Address	<input type="text" value="x.1.2.123"/>	
IP Mask	<input type="text" value="255.255.255.255"/>	The mask specifies the part of the address to match. Use 255.255.255.255 to match the whole address. Use 0.0.0.0 to match any address.
Access Group	<p><input checked="" type="radio"/> Group 1 (NetSec)</p> <p><input type="radio"/> Group 2 (config)</p> <p><input type="radio"/> Group 3 (isp)</p> <p><input type="radio"/> Group 4 (mis)</p> <p><input type="radio"/> Group 5 (user)</p> <p><input type="radio"/> No Access</p>	
	<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

## SSL

Next we set the level of SSL encryption to use. Here it is set at 3DES-168/SHA which is the strongest option. SSL Client Authentication is enabled. This requires a personal certificate on the browser and a trusted certificate on the concentrator. The default SSL version setting “Negotiate SSL V2/V3” is used. This will accept V2 only if the client can’t use V3. The strongest Generated Certificate Key Size of 1024 is used. This screen is found under Configuration/System/Management Protocols/SSL.

Configure SSL.



If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

<b>Encryption Protocols</b>	<input type="checkbox"/> RC4-128/MD5	Check the encryption algorithms to enable. Unchecking them all disables SSL.
	<input checked="" type="checkbox"/> 3DES-168/SHA	
	<input type="checkbox"/> DES-56/SHA	
	<input type="checkbox"/> RC4-40/MD5 Export	
	<input type="checkbox"/> DES-40/SHA Export	
<b>Client Authentication</b>	<input checked="" type="checkbox"/>	Check to enable client authentication. Client authentication requires an installed Certificate Authority and a personal certificate installed in your browser.
<b>SSL Version</b>	<input type="text" value="Negotiate SSL V2/V3"/>	Select the SSL version to use. Using a SSL V2 Hello provides compatibility with most browsers.
<b>Generated Certificate Key Size</b>	<input type="text" value="1024-bit RSA Key"/>	Select the key size used in the generated certificate.

### General Security settings

NTP – The Sync Frequency is set to every 60 minutes in Configuration/System/Servers/NTP/Parameters.

Configuration | System | Servers | NTP | Parameters

Configure NTP synchronization frequency.

**Sync Frequency**  (minutes) Enter the frequency to poll the NTP servers.

Apply

Cancel

The IP address for the NTP server (x.1.2.133) is set in Configuration/System/Servers/NTP/Hosts/Add.

Configuration | System | Servers | NTP | Hosts | Add

Add a new NTP host.

**NTP Host**  Enter the hostname or IP address of the NTP server.

Add

Cancel

Syslog – The syslog server's IP address, port number, and Facility to use are set in Configuration/System/Events/Syslog Servers/Add. We are using the default port of 514. Facility Local 2 is used for the VPN on our syslog server.

Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

**Syslog Server**  Enter the IP address or hostname of the syslog server.

**Port**  Enter the port used by the syslog server.

**Facility**  Select the syslog facility tag for events sent to this server.

Add

Cancel



Events – In Configuration/Systems/Events/General we set what events to log. We are logging to a syslog server so we don't need to Save Log on Wrap, nor do we care about Save Log Format and FTP Saved Log on Wrap. We are not sending email alerts so we have left the Email Source Address blank and have Severity to Email set to none. Syslog Format is set to Original. This includes all the information we need on one line. Severity to Log has been left at default. Console logging is also the default of 1-3 so that only critical information is displayed. Syslog logging is set to 1-5 so that it includes login/logout and above, but does not spam the syslog with useless information. We are not using SNMP so Severity to Trap is set to the default of none.

© SANS Institute 2000 - 2005. All rights reserved. Author retains full rights.

This section lets you configure default event handling.

<b>Save Log on Wrap</b>	<input type="checkbox"/>	Check to save the event log to a file on wrap.
<b>Save Log Format</b>	Multiline	Select the format of the saved log files.
<b>FTP Saved Log on Wrap</b>	<input type="checkbox"/>	Check to automatically FTP the saved log to a remote destination.
<b>Email Source Address</b>		Enter the email address that appears in the <b>From:</b> field.
<b>Syslog Format</b>	Original	Select the format of Syslog messages.
<b>Severity to Log</b>	1-5	Select the range of severity values to enter in the log.
<b>Severity to Console</b>	1-3	Select the range of severity values to display on the console.
<b>Severity to Syslog</b>	1-5	Select the range of severity values to send to a Syslog server.
<b>Severity to Email</b>	None	Select the range of severity values to send via email to the recipient list.
<b>Severity to Trap</b>	None	Select the range of severity values to send to an SNMP system.

IKE Proposal - IPSec negotiation begins with an Internet Key Exchange proposal. Based on the accepted proposal, the tunnel endpoints are authenticated and IPSec security parameters are negotiated. 3DES is the encryption algorithm and while it does not prevent sniffing, it makes the sniffed data useless if strong enough. Hashes, such as MD5, are used to verify data integrity. IKE Proposals are made active or inactive and placed in order of preference in Configuration/System/Tunneling Protocols/IPSec/IKE Proposals. The proposals are used when the concentrator is acting as a responder and are checked for compatibility in the order listed.

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate.

Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
IKE-3DES-SHA-DSA IKE-3DES-MD5-DH1 IKE-3DES-MD5	<< Activate	IKE-3DES-MD5-RSA IKE-3DES-MD5-RSA-DH1
	Deactivate >>	
	Move Up	
	Move Down	
	Add	
	Modify	
	Copy	

### LAN to LAN VPN to partner and supplier

LAN-to-LAN VPN connections are set up in Configuration/System/Tunneling Protocols/IPSec LAN-to-LAN/Add. Here we have the VPN connection to our partner shown. The Name used is Partner. If we had more than one partner, we would want to be more descriptive with our unique name in order to better distinguish them. The maximum name length is 32 characters. The Interface to use is Ethernet 2, which is our public interface. Peer is the IP address of the public interface of our partner's VPN concentrator. Because we are using a preshared key, we select none for Digital

Certificate. Our Preshared Key is a 4 to 32 character alphanumeric word that serves as a password when the connection is created. For Authentication we are using the default ESP/MD5/HMAC-128. Authentication is used to verify that a packet came from who we expected it to come from. For Encryption we are using 3DES-168. This is the default and is the most secure. Our IKE Proposal is IKE-3DES-SHA-DSA. This is not an active proposal by default, but is very secure. It uses 3DES-168 for the encryption algorithm, SHA/HMAC-160 for the authentication algorithm, DSA digital certificate for the authentication mode and group 2 Diffie-Hellman.

<b>Name</b>	<input type="text" value="Partner"/>	Enter the name for this LAN-to-LAN connection.
<b>Interface</b>	<input type="text" value="Ethernet 2 (Public)"/>	Select the interface to put this LAN-to-LAN connection on.
<b>Peer</b>	<input type="text" value="x.10.10.3"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
<b>Digital Certificate</b>	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
<b>Preshared Key</b>	<input type="text" value="secretpartnerkey"/>	Enter the preshared key for this LAN-to-LAN connection.
<b>Authentication</b>	<input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
<b>Encryption</b>	<input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
<b>IKE Proposal</b>	<input type="text" value="IKE-3DES-SHA-DSA"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.

*The next screen is a continuation from above.* Network Autodiscovery is unchecked. It would require RIP v2/v1 to be enabled on the private side of the VPN devices at each end of the connection. Local Network is used to tell the VPN device what addresses we are using. Our Local Network is our partner's Remote Network and vice versa. You can use a preconfigured Network List or you can enter a network address/wildcard mask. Here we have our class C network address and a class C wildcard mask. To figure out a wildcard mask from a subnet mask, swap the 0's for 255's and the 255's for 0's.

<b>Network Autodiscovery</b> <input type="checkbox"/>	discover networks. <b>Parameters below are ignored if checked.</b>
<b>Local Network</b>	
<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text" value="x.1.2.0"/>	<b>Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask.</b> A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
<b>Wildcard Mask</b> <input type="text" value="0.0.0.255"/>	

*The next screen is a continuation from above.* Remote Network is used to tell the VPN device what addresses our partner is using. You can use a preconfigured Network List or you can enter a network address/wildcard mask. Here we have our partner's class C network address and a class C wildcard mask.

## Remote Network

Network List

Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

Wildcard Mask

**Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example,  
10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**

Add

Cancel

## Supplier

The supplier VPN is set up in the same manner but with their information replacing our partner's information. Name is supplier, Peer is x.20.20.3, Preshared Key is secretsupplierkey, and Remote Network IP Address is x.20.20.0.

## RAS

There are several options that can be used for assigning IPs to our remote users. We are using an internal address pool. The IP address given to each user for each session is

recorded in the syslog, as well as login and logout times, for accountability. This is set in Configuration/System/Address Management/Assignment.

#### Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

- Use Client Address** ☐ Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
- Use Address from Authentication Server** ☐ Check to use an IP address retrieved from an authentication server for the client.
- Use DHCP** ☐ Check to use DHCP to obtain an IP address for the client.
- Use Address Pools** ☒ Check to use internal address pool configuration to obtain an IP address for the client.

Apply

Cancel

Set in Configuration/System/Address Management/Pools/Add, Range Start is the first IP address in the pool and Range End is the last.

#### Configuration | System | Address Management | Pools | Add

Add an address pool.

**Range Start**  Enter the start of the IP pool address range.

**Range End**  Enter the end of the IP pool address range.

Add

Cancel

The Base Group contains the default settings for all groups and users. Its parameters are set in Configuration/User Management/Base Group. Under the General tab we allow access at any time by choosing –No Restrictions- for Access Hours. Simultaneous Logins is set to the default of 3. A Minimum Password Length of 8 is set, which is also



the default. We don't check Allow Alphabetic-Only Passwords. This would violate our password policy. Idle Timeout is set to 30 minutes. Maximum Connect time is set to 0 which gives unlimited connection time. Filter is left at the default of -None-.

General Parameters		
Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input type="checkbox"/>	Check to allow alphabetic-only passwords for users in this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group

The next screen is a continuation from above. Primary DNS is set to our Ext-Int DNS server. Secondary DNS and WINS servers are left blank. SEP Card Assignment is set to the default of all four Scalable Encryption Processing modules. Tunneling Protocols is set



to use IPSec only.

<b>Primary DNS</b>	<input type="text" value="x.1.2.105"/>	Enter the IP address of the primary DNS server for this group.
<b>Secondary DNS</b>	<input type="text"/>	Enter the IP address of the secondary DNS server.
<b>Primary WINS</b>	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
<b>Secondary WINS</b>	<input type="text"/>	Enter the IP address of the secondary WINS server.
<b>SEP Card Assignment</b>	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
<b>Tunneling Protocols</b>	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	Select the tunneling protocols this group can connect with.

IPSec parameters for the Base Group are set under the IPSec tab. The IPSec Security Association is set to ESP/IKE-3DES-MD5. IKE tunnel authentication is MD5/HMAC-

128, IPSec authentication is ESP/MD5/HMAC-128, and both IKE and IPSec are encrypted with 3DES-168. Tunnel Type is set to Remote Access. We take the default of not locking users to the group. Authenticating is set to Internal. Mode Configuration is checked to enable the VPN concentrator to send several configuration parameters to the client.

IPSec Parameters		
Attribute	Value	Description
IPSec SA	ESP/IKE-3DES-MD5	Select the IPSec Security Association assigned to this group.
Tunnel Type	Remote Access	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
Remote Access Parameters		
Group Lock	<input type="checkbox"/>	Lock the users into this group.
Authentication	Internal	Select the authentication method for users in this group.
Mode Configuration	<input checked="" type="checkbox"/>	Check to use Mode Configuration for users of this group. Update parameters below if checked.

*The next screen is a continuation from above. We can set a banner that is displayed*

when the user logs in. It is limited to 128 characters and should be approved by the legal department. We obviously don't Allow Password Storage on Client. Split Tunneling Network List is set to the default of -None- to disable it. While split tunneling eases the load on the concentrator and PC by allowing traffic meant for other networks to go out unencrypted and by way of their normal route, it lessens the level of security. Default Domain Name is giacenterprises.com. IPSec through NAT is enabled to allow people running things like linux masquerading boxes at home to connect. *We are not using PPTP/L2TP so we don't need to set any parameters under that tab.*

<b>Banner</b>	<div></div>	Enter the banner for this group.
<b>Allow Password Storage on Client</b>	<input type="checkbox"/>	Check to allow the IPSec client to store the password locally.
<b>Split Tunneling Network List</b>	<div>-None-</div>	Select the Network List to be used for Split Tunneling.
<b>Default Domain Name</b>	<div>giacenterprises.com</div>	Enter the default domain name given to users of this group.
<b>IPSec through NAT</b>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to operate through a firewall using NAT via UDP.
<b>IPSec through NAT UDP Port</b>	<div>10000</div>	Enter the UDP port to be used for IPSec through NAT (4001 - 49151)

Groups are used to simplify management of users who have the same access requirements. Rather than setting parameters for each individual user, they are set in a group and the users are added to the group. Groups are created in Configuration /User Management/Groups/Add. Under the Identity tab we set the Group Name to `giac_users`. The Password needs to meet our password policy listed earlier. Type refers to where authentication is done. Ours is Internal. The client software must be configured with a valid group name and password before the concentrator will even request the username and password.

#### Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	<input type="text" value="giac_users"/>	Enter a unique name for the group.
Password	<input type="password" value="XXXXXXXXXX"/>	Enter the password for the group.
Verify	<input type="password" value="XXXXXXXXXX"/>	Verify the group's password.
Type	<input type="text" value="Internal"/> ▼	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator Series's Internal Database.

Under the General tab we find similar configuration options as under General in the Base Group. By checking Inherit, we have accepted the same settings as in the Base Group. If we wanted to change one, we would uncheck Inherit and enter the needed Value.

Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity	General	IPSec	PPTP/L2TP
<b>General Parameters</b>			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.

As with the General tab, under the IPsec tab we find similar configuration options as under IPsec in the Base Group. By checking Inherit, we have accepted the same settings as in the Base Group. If we wanted to change one, we would uncheck Inherit and enter the needed Value.

Uncheck the **Inherit?** box and enter a new value to override base group values.

<div>Identity</div> <div>General</div> <div><b>IPSec</b></div> <div>PPTP/L2TP</div>			
IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP/IKE-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPsec Security Association.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
		<input type="checkbox"/>	Select the authentication

Users are added in Configuration/User Management/Users/Add. Under the Identity tab we set the User Name, Password, Verify password, and Group. For some users, we might want to set a specific IP address. Each time the user logged in, they would get the same IP. For most users we will leave this blank. By not specifying an IP address, the user will get a random IP from the pool. This gives us more efficient use of our IP space as not everyone will be logged in at the same time and we still have accountability due to our logging. Subnet Mask only needs to be set if IP Address is.

#### Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity Parameters		
Attribute	Value	Description
User Name	John.Doe	Enter a unique user name.
Password	klaklaklaklak	Enter the user's password. The password must satisfy the group password requirements.
Verify	klaklaklaklak	Verify the user's password.
Group	qiac users	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add

Cancel



Under the General tab we take the Base Group defaults by checking the Inherit boxes.

Selected Group Values:

Identity	General	IPSec	PPTP/L2TP
<b>General Parameters</b>			
Attribute	Value	Inherit?	Description
<b>Access Hours</b>	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
<b>Simultaneous Logins</b>	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
<b>Idle Timeout</b>	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
<b>Maximum Connect Time</b>	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
<b>Filter</b>	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
<b>SEP Card Assignment</b>	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this user can be assigned to.
<b>Tunneling Protocols</b>	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.



As with General, under the IPsec tab we take the Base Group defaults by checking the Inherit boxes.

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity	General	IPSec	PPTP/L2TP
IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP/IKE-3DES-MD5	<input checked="" type="checkbox"/>	Select the IPSec Security Association assigned to this user.
Store Password on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.

Add

Cancel

### VPN Client Software

Client software is required to connect to the Cisco 3000 series VPN Concentrators. A configuration file can be created and used with the setup program to make installation simple.

Note – Be sure to set the MTU to 1400 or below or they will not be able to connect.

To get connected users just start the client, click on connect, and enter their username and password when prompted. They will then have an encrypted tunnel from their PC to the external interface of the VPN concentrator and an IP address from the VPN concentrator's pool. All traffic will go through this tunnel if set up as specified.

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



### **External Firewall**

Before setting up the rulebase on the firewall, we must know who needs access to what and from where. This will require input from the other departments to get it right. Security and customer access need to be the top two priorities.

TIP – A good firewall policy blocks everything that is not explicitly allowed.

Check Point Firewall-1 formats its rules as Source, Destination, Service, Action, Track, Install On, Time, and Comment.

Source is the initiator of the connection. It can be a computer, network, router, etc.  
Destination is the desired connection end point. It can be a computer, network, etc.

Service is the protocol and port of the Destination. It can be ICMP, TCP, UDP, etc.  
Action is what is to be done with the packet. It can be accept, drop, reject, encrypt, etc.  
Track is used for logging or alerting. It can be blank (no logging), short, long, etc.  
Install On is used to tell where this rule is enforced. It can be gateways, destination, etc.  
Time is used to set the time this rule is enforced. It can be set for time and day.  
Comment is a text field that can be used to help explain the rule.

TIP – If you have more than one person editing the rulebase, have each person include their name, or initials, and the date in the comment field whenever they make a rule change.

Here is an access list to base the external firewall's rulebase on:

No one remotely accesses the firewall. This is known as the stealth rule and should almost always be first.

Source = any, Destination = CPFirewall1, Service = any, Action = drop, Track = long.

For all our rules: Install On will be gateway, Time will not be set, and Comment will be a text description of the rule with the installer's name and the date.

TIP – It's generally better to use drop rather than reject. It gives a hacker less information.

Everyone should be able to access the web server via HTTP and HTTPS (ssl).

Source = any, Destination = web server, Service = HTTP & HTTPS, Action = accept, Track = long.

Everyone should be able to access the external-external DNS server for DNS resolution.

Source = any, Destination = ext-ext DNS server, Service = UDP 53, Action = accept, Track = long.

NOTE – While domain name resolution requests are generally UDP, they are not always. By limiting this to UDP port 53 we are taking a chance on blocking a customer from resolving our domain name. However, the percentage is quite low and we can have the few (if any) that can't, use the IP Address of the server. If this becomes a problem, we might have to open this up to TCP port 53 as well. The DNS servers should be set up to control zone transfers in either case.

The external-external and external-internal DNS servers need to get out to the internet for DNS resolution.

Source = ext-ext & ext-int DNS servers, Destination = any, Service = UDP 53, Action = accept, Track = blank. We are not logging most outgoing traffic. We can use content security software such as Surf Control or Web Sense on the corporate network firewall.

Internal users should be able to get out via web, FTP, and ssh.

Source = GIAC corp & screened networks, Destination = any, Service = HTTP, HTTPS, FTP, & ssh, Action = accept, Track = blank.

Everyone should be able to send us email via our email relay/antivirus server.

Source = any, Destination = SMTP relay server, Service = SMTP, Action = accept, Track = long.

Our email relay/antivirus server should be able to send email out.

Source = SMTP relay server, Destination = any, Service = SMTP, Action = accept, Track = long.

Our partner and supplier should be able to get to the FTP server.

Source = partner & supplier networks, Destination = FTP server, Service = FTP, Action = accept, Track = long.

RAS users should be able to get in via SSH.

Source = VPN network, Destination = any, Service = ssh, Action = accept, Track = long.  
While all RAS communications are encrypted due to the VPN, the users must use SSH because telnet is not allowed on any device.

RAS users should be able to access the external-internal DNS server for DNS resolution.

Source = VPN network, Destination = ext-int DNS server, Service = UDP 53, Action = accept, Track = blank.

The border router and VPN concentrator should be able to use the Syslog & NTP server.

Source = border router & VPN concentrator, Destination = Syslog/NTP server, Service = NTP & syslog, Action = accept, Track = blank.

Nothing else should be allowed, therefore it should be dropped.

Source = any, Destination = any, Service = any, Action = drop, Track = long. This is the clean up rule and it is logged.

TIP – As a general rule, have the most often used rules at the top of the rulebase. Once a rule matches, the packet is acted upon and doesn't have to be checked against the remaining rules. This can lessen the firewall load.

Now that we have the access list, we can begin configuring the firewall.

When you install Firewall-1, be sure to check control IP forwarding. IP forwarding has to be enabled on the system the firewall runs on. Once the firewall service is running, IP forwarding is controlled by the rulebase. However, during boot up, between the time the TCP/IP stack starts and the firewall service starts, the server will forward all packets.

Also, if the firewall is down for some reason, you don't want the network wide open to attack.

## Network Objects

Firewall-1 requires that network objects be defined for our sources and destinations. Using our access list, we can start creating our network objects. In the Policy Editor, click on Manage/Network Objects. The first object we will create is the firewall object which falls under the category of a workstation. From the Network Objects window, select New/Workstaion.

Below we find a screen capture of the Workstation Properties window. Each network object requires a unique name. This name should be descriptive enough so one can tell what it is based on the name alone. The firewall's external IP needs to be listed as the IP Address for licensing reasons. The Comment should help identify the object. Color is used to help pick out device types quickly. This helps when the network object list gets long and when you have a large rulebase. Location is relative to the firewall. Type is whether the object is multihomed (has more than one NIC or interface) or not. Host has one while Gateway has more than one. Modules Installed is if this is a Check Point Firewall-1 or Management Station for a Firewall-1.

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

**Workstation Properties**

General | Interfaces | SNMP | NAT | Certificates | VPN | Auth...

Name: CPMirewall1

IP Address: x.1.2.34 Get address

Comment: External Firewall

Color:

Location: ☒ Internal ☐ External

Type: ☐ Host ☒ Gateway

Modules Installed

☒ VPN-1 & FireWall-1 Version: 4.1 Get

☐ FloodGate-1 Version: 4.1

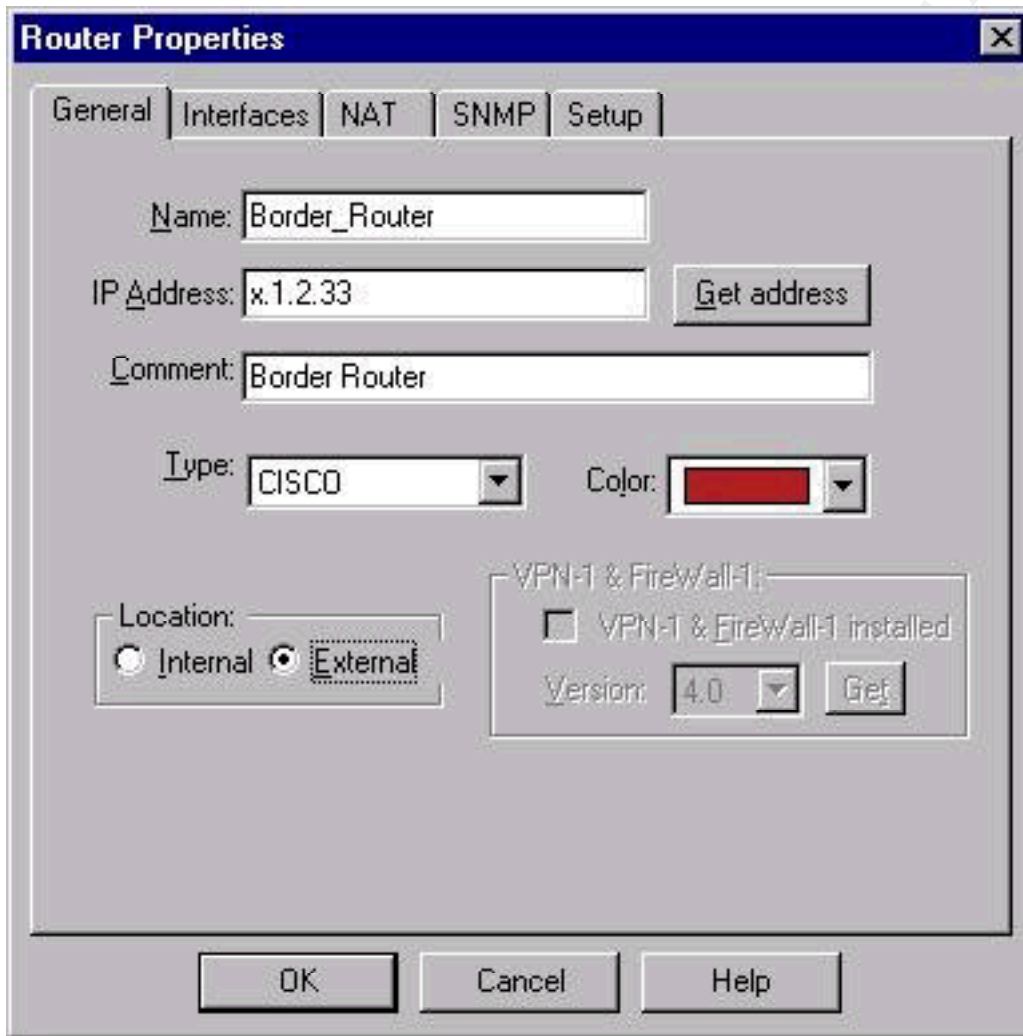
☒ Management Station

OK Cancel Help

The other workstation objects that need to be created are:

<u>Name</u>	<u>IP Address</u>	<u>Color</u>	<u>Location</u>	<u>Type</u>
VPN_Concentrater	x.1.2.35	maroon	External	Gateway
DNS_Ext_Ext_Serv	x.1.2.100	green	Internal	Host
DNS_Ext_Int_Serv	x.1.2.105	green	Internal	Host
SMTP_Relay_Serv	x.1.2.101	green	Internal	Host
Web_Serv	x.1.2.102	green	Internal	Host
FTP_Serv	x.1.2.103	green	Internal	Host
Syslog_NTP_Serv	x.1.2.133	green	Internal	Host

Next we create the border router object. From the Network Objects window, select New/Router. We are not going to set up the router ACL from the firewall so our router object configuration is similar to a workstation object. The Name is Border\_Router. IP Address is x.1.2.33. Comment is Border Router. Type is the maker of the router. Our's is a Cisco. Color is maroon. Location is External from the firewall.



The image shows a 'Router Properties' dialog box with a blue title bar and a close button. It has five tabs: 'General', 'Interfaces', 'NAT', 'SNMP', and 'Setup'. The 'General' tab is selected. The fields are as follows: 'Name' is 'Border\_Router'; 'IP Address' is 'x.1.2.33' with a 'Get address' button; 'Comment' is 'Border Router'; 'Type' is a dropdown menu showing 'CISCO'; 'Color' is a dropdown menu showing a red color swatch; 'Location' has two radio buttons, 'Internal' and 'External', with 'External' selected; and a section for 'VPN-1 & FireWall-1' containing an unchecked checkbox 'VPN-1 & FireWall-1 installed', a 'Version' dropdown showing '4.0', and a 'Get' button. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Field	Value
Name	Border_Router
IP Address	x.1.2.33
Comment	Border Router
Type	CISCO
Color	Red
Location	External
VPN-1 & FireWall-1 installed	False
Version	4.0



Looking back at the access list, we still need to define the networks referenced. From the Network Objects window, select New/Network. The first network we will define is Named Partner\_Net. The IP Address is x.10.10.0. Net Mask is 255.255.255.0. Location is External from the firewall. Broadcast is whether the broadcast address is considered part of the network when an accept rule is applied. Broadcast is set to Disallowed.

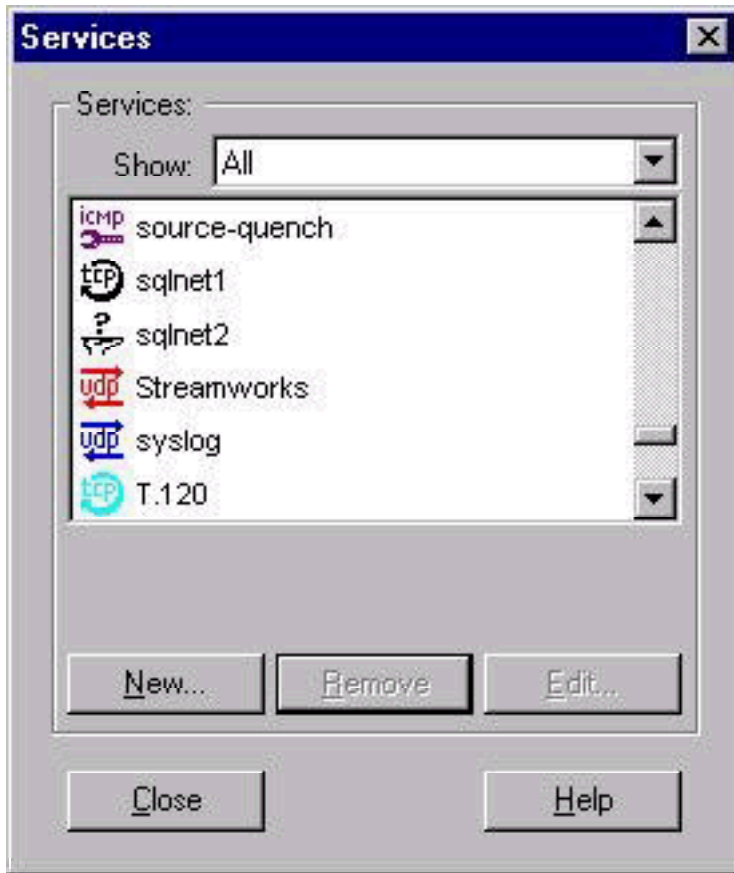
The screenshot shows the 'Network Properties' dialog box with the 'General' tab active. The 'Name' field contains 'Partner\_Net'. The 'IP Address' field contains 'x.10.10.0' and there is a 'Get address' button next to it. The 'Net Mask' field contains '255.255.255.0'. The 'Comment' field contains 'Partner's Network'. The 'Color' field is a dropdown menu showing 'Blue'. Under 'Location', the 'External' radio button is selected. Under 'Broadcast', the 'Disallowed' radio button is selected. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

The other network objects that need to be created are:

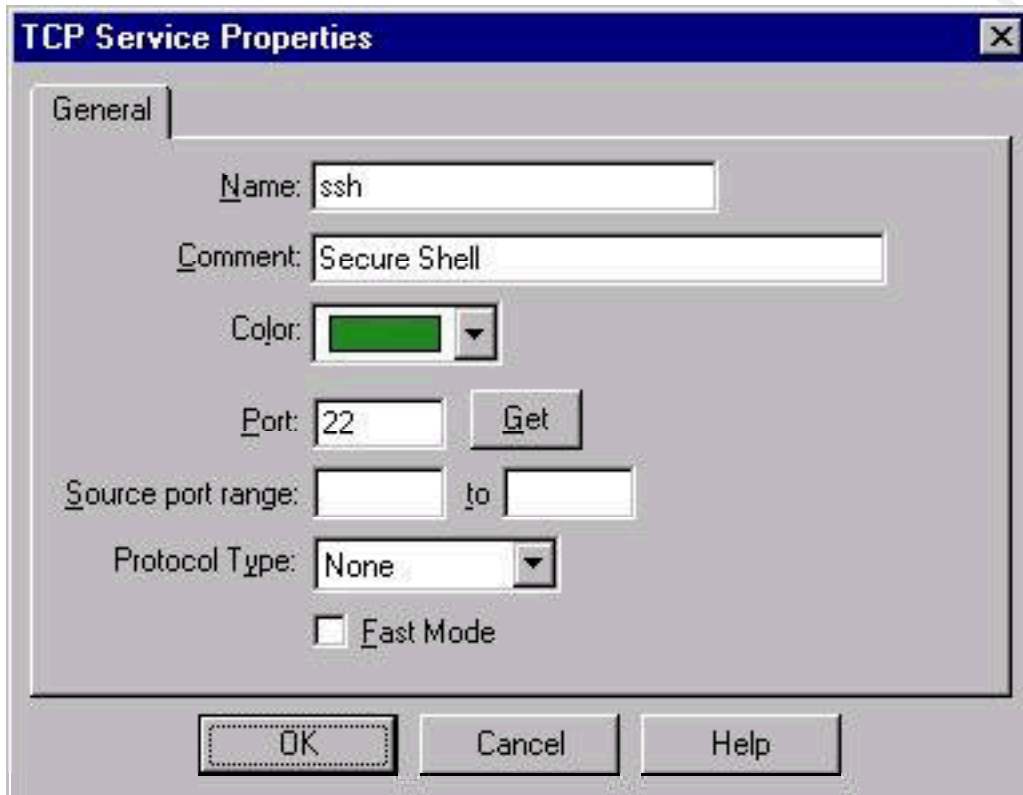
<u>Name</u>	<u>IP Address</u>	<u>Net Mask</u>	<u>Location</u>	<u>Broadcast</u>
Supplier_Net	x.20.20.0	255.255.255.0	External	Disallowed
VPN_DMZ_Net	x.1.2.32	255.255.255.224	External	Allowed
GIAC_Screened_Net	x.1.2.96	255.255.255.224	Internal	Allowed
GIAC_Corp_Net	x.1.2.128	255.255.255.128	Internal	Allowed

## Services

Firewall-1 comes with many pre-defined services. The only service not found was SSH (secure shell) so we need to add it.



To add a service click on Manage/Services. This brings up the window as seen above. Select New/TCP to get the window you see in the picture below, Name is ssh, Color is green, Port is 22. We leave the rest of the settings alone.

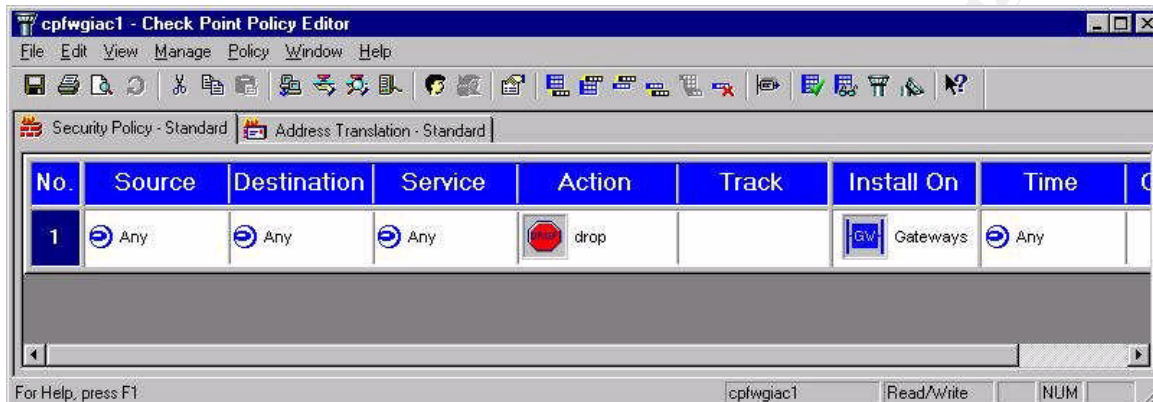


### Rulebase

Now that we have our network objects and services all defined, we can start adding rules to the firewall.

NOTE – Firewall-1 has an unseen last rule to drop everything. So, if the firewall is up with no rulebase, it will drop everything coming and going. This unseen rule does not log.

Still in the Policy Editor, click on Edit/Add Rule/Bottom. This will create a new rule with default settings at the bottom of our current rulebase as seen below. Because the rulebase is empty, it will become our first rule.

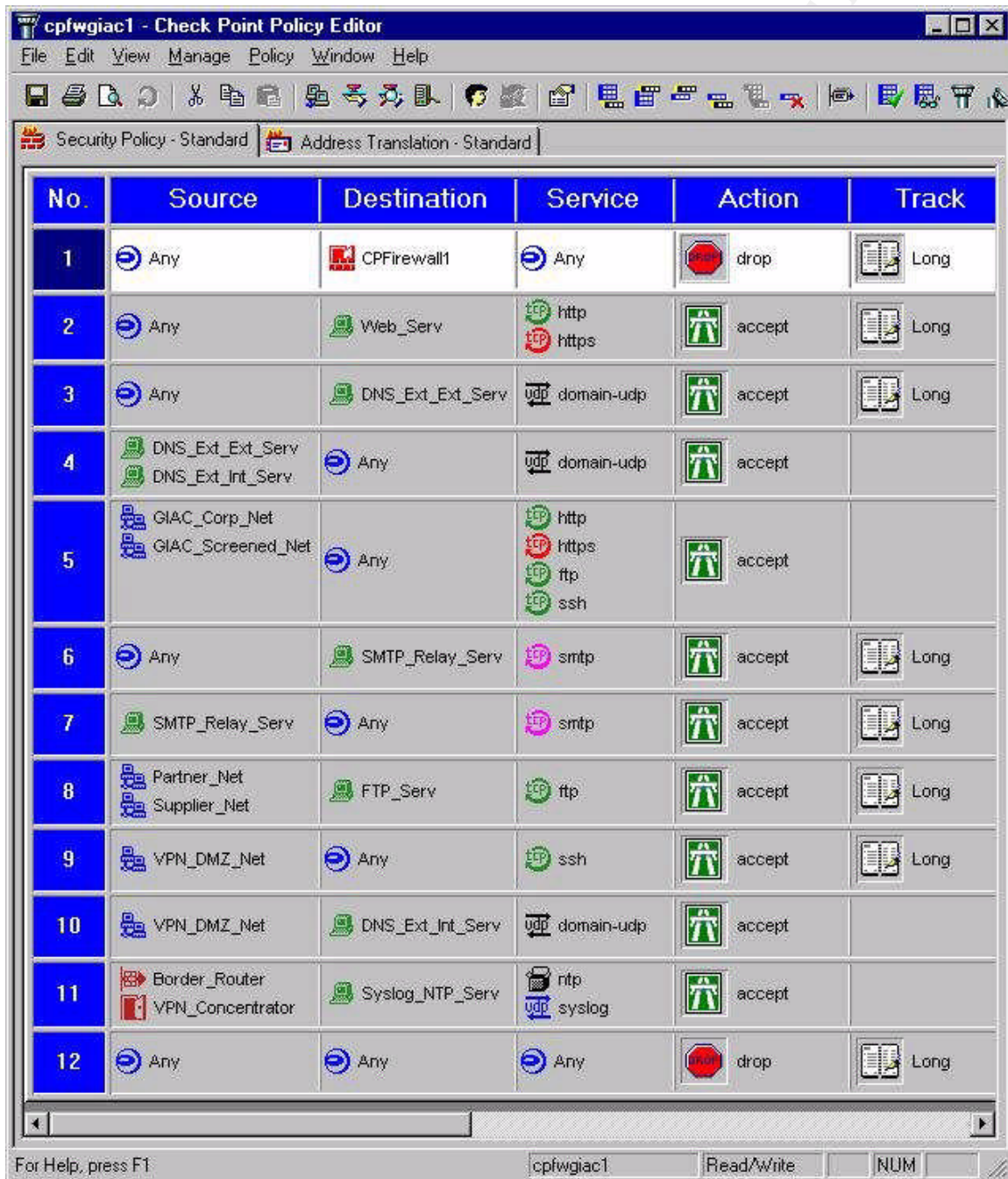


Our first rule was no one remotely accesses the firewall. Source = any, Destination = CPFirewall1, Service = any, Action = drop, Track = long, Install On = Gateways, Time = any, Comment = The stealth rule.

The Source will remain Any so we leave it alone. Right click in rule No 1's Destination field and choose Add from the menu that opens. This opens the Network Objects windows as seen below. Find CPFirewall1 in the list and double click on it. This changes the Any that was there to CPFirewall1. Service remains as Any. Action remains as drop. Track needs to be changed to Long so right click in the Track field of rule No 1 and select Long from the menu. Install On remains as Gateways. Time remains as Any. Comments need to be added so right click on the Comments field of rule No 1 and select edit. In the box that opens type "The Stealth Rule. GPC 4/20/01" and click on OK. Follow this same procedure for the rest of the rules.



When all the rules have been added, it should look like this:



TIP – In order to make management easier, try to keep your rulebase under 30 rules. Once it gets much more than that, it becomes easy to make a mistake and that could open major holes or cause customers to lose needed access.

### Implicite Rules

Firewall-1 has some other settings and implied rules that need to be considered also. In the Policy Editor, click on Policy/Properties to bring up the Properties Setup window.

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



**Properties Setup**

SYNDefender | LDAP | Encryption | ConnectControl

High Availability | IP Pool NAT | Access Lists | Desktop Security

Security Policy | Services | Log and Alert | Security Servers | Authentication

Apply Gateway Rules to Interface Direction: Eitherbound

ICP Session Timeout: 3600 Seconds

☒ Accept UDP Replies:

UDP Virtual Session Timeout: 40 Seconds

☐ Enable Decryption on Accept

**Implied Rules**

- ☐ Accept VPN-1 & FireWall-1 Control Connections: First
- ☐ Accept RIP: First
- ☐ Accept Domain Name Over UDP (Queries): First
- ☐ Accept Domain Name Over TCP (Zone Transfer): First
- ☐ Accept ICMP: Before Last
- ☐ Accept Outgoing Packets Originating From Gateway: Before Last

☐ Log Implied Rules

☐ Install Security Policy only if it can be successfully installed on ALL selected targets.

OK Cancel Help

NOTE - Implied rules don't show up in the rulebase by default so many people miss them.

We need to decide where we want the rules applied. Our choices are inbound, outbound, or eitherbound. Eitherbound has been chosen as it is a little more secure and it only adds a small amount of load. We have more than enough processor power.



TCP Session Timeout is left at the default 3600 Seconds. Accept UDP Replies remains enabled. UDP Virtual Session Timeout is left at 40 Seconds.

NOTE - Although UDP is connectionless, Firewall-1 maintains a “virtual session” in its state table so it can monitor the “connection”.

Enable Decryption on Accept is unchecked as we aren't using the firewall for VPN. All the Implied Rules are also unchecked. Accept VPN-1 & Firewall-1 Control Connections is unchecked because we are only using the management console on the firewall itself and we don't want the ports listening on the firewall. This is a dead give-away that it's a Firewall-1. The firewall has static routes so we don't want RIP. DNS is controlled in the rulebase and we don't want ICMP.

TIP – If you are using Firewall-1, be sure to check these implied rules! The “first”, next to the each DNS rule, means that they are checked before the rulebase. Any rule in the rulebase about DNS won't even get seen if these are enabled.

Accept Outgoing Packets Originating From Gateway is unchecked because no one should be using the firewall for any reason except managing the firewall. When updates need to be applied, we can enable it for that short period of time. Log Implied Rules and the Install Security Policy are both unchecked as we aren't using any implied rules and have only one Check Point Firewall-1 firewall.

### Applying rules

Firewall-1 lets you verify the rulebase before installing it. While it won't tell you if you have a hole open, it is useful for finding logic errors. Click on Policy/Verify to check the rulebase and save it. You should always verify the rulebase before installing it. Click on Policy/Install to have the rulebase installed. The rulebase must be installed before it can filter traffic.

## **Assignment 3 – Audit Your Security Architecture (25 Points)**

You have been assigned to provide technical support for a comprehensive information

systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

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

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

---

## **Planning**

Before performing our primary firewall audit we need to know what is expected as far as access to the firewall and through the firewall (both directions). The first part is easy - no one should be able to access the firewall remotely and therefore few if any ports should be listening. The second part is a bit more involved but can be worked out by looking at the rulebase.

To test these expectations we will use Nessus and nmap. Nessus is a vulnerability scanner that uses vulnerability plugins. These plugins are updated often and the new ones can be downloaded from their web site at [www.nessus.org](http://www.nessus.org). Some of the other benefits of Nessus include: tests vulnerabilities on known and unknown ports, incorporates nmap, has good reporting, and can even tell you how to fix some holes. Nmap includes stealth port scanning and several other nice features and can be found at [www.insecure.org/nmap](http://www.insecure.org/nmap).

We could also use ISS Internet Scanner. It is commercial so we would incur additional cost, but if this audit is going to be done often, it might be worth it.

Nmap Scans will be performed from every network (VPN/DMZ, screened, corp, sensitive) to every other network that is on the other side of the firewall being audited. A

scan will also be performed from the ISP coming in (we will of course have to work with them on this). Nessus will be used from the VPN/DMZ network against all networks behind the firewall.

The day and time for the tests is based on historically low traffic times and when we have the necessary support people. We want as little effect on our customers as possible and we need support people available incase a server is brought down, etc. We will not post on the customer web page that we are doing this as we don't want to give hackers that information. However, our supplier and partner will be informed as to when this will take place. Wednesday at 3:00am in the 3<sup>rd</sup> week of the month will be the start time and the scans will continue until completed that morning.

All departments will be made aware of the audit and have people on call in case there are any problems. A network engineer, firewall admin, and server admin will be on site.

Because this is a firewall audit, the firewall administrator will have the most time (besides myself) invested. Someone from each area will have a couple of hours in the planning stage and a couple of hours in the analysis stage. Those onsite during the tests will have about 5 hours in the implementation stage. If a knowledgeable outside consultant was to do this, you're looking at up to \$5,000 depending on the regen.

The major risks involved and the reason administrators and engineers are on site is in case a device is taken down by the tests. We want little or no customer down time.

### **Implementation**

The first tests we will perform are running nmap from the ISP against the whole GIAC Enterprises class C of x.1.2.0. The following command lines will be used:

```
nmap -sS -P0 -v x.1.2.0/24 >> sttcpisp.txt      - tcp stealth scan no initial ping
nmap -sU -P0 -v x.1.2.0/24 >> updisp.txt      - upd scan no initial ping
nmap -sP -P0 -v x.1.2.0/24 >> pingisp.txt      - ping scan no initial ping
```

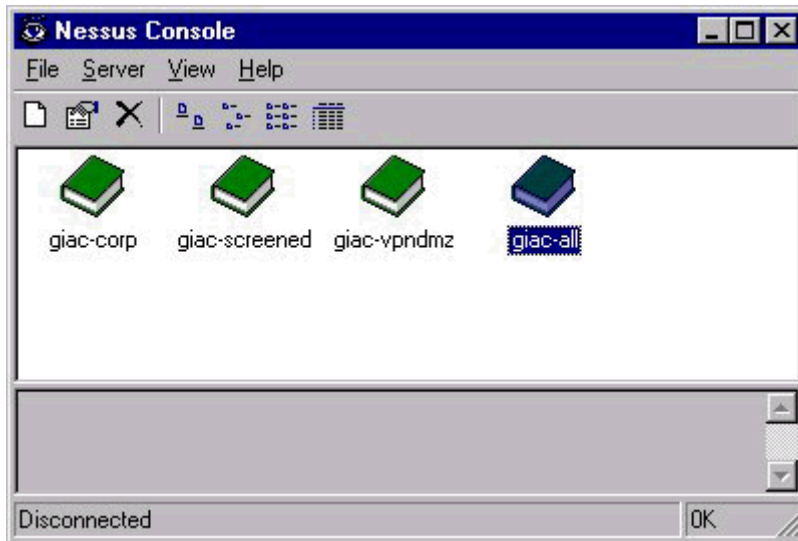
This will create three files containing the data that will be analysed later. The data should look something like this:

```
Host testbox.giacenterprises.com (x.1.2.x) appears to be up ... good.
Initiating SYN Stealth Scan against testbox.giacenterprises.com (x.1.2.x)
Adding TCP port 22 (state open).
Adding TCP port 7 (state open).
The SYN Stealth Scan took 33 seconds to scan 65535 ports.
Interesting ports on testbox.giacenterprises.com (x.1.2.x):
(The 65501 ports scanned but not shown below are in state: closed)
Port    State  Service
7/tcp   open   echo
```

22/tcp open ssh

The same three commands will then be run from the rest of the networks in front of and behind the firewall using appropriate network IPs and filenames.

The final test will be done using Nessus from the VPN/DMZ network going in through the firewall. Below we see the NessusWX Windows client with our networks defined. The client can be anywhere. It's the server that the tests run from so it needs to be temporarily connected to the switch in the VPN/DMZ network.



## Analysis

Analysis of the data consists of comparing what we got in our tests to what we expected to get. If they are not the same, we need to look at the firewall rulebase and configuration settings to see what needs to be changed. Also, the Nessus data may show us some holes either in the firewall or on the systems behind the firewall that need to be patched.

Our SAMPLE nmap output from above shows that only two ports are seen as listening from the network that we did the scan. Moving to another network could change that if there is a firewall or router ACL between our testing server and the server being tested. We expected to find 22/tcp (ssh) open but 7/tcp (echo) should not be. Now we know to look for a service allowing echo. Once found, we disable it if it's not required for some other reason. If it is not possible to disable it on the box, we might need to block it somewhere else, such as at a firewall or router. (The firewall would have blocked this but it shows how some analysis could be done)

Another example is: lets say that our ping scan showed several systems behind the firewall when performed from the VPN/DMZ network but not from the ISP. This would

indicate that the border router was blocking the ICMP packets as it should but the firewall was not. We would need to check the implied rules on the Firewall-1 firewall and verify that Accept ICMP was not checked.

If any vulnerabilities were found from Nessus, we need to inform the appropriate people so they will be fixed quickly. Nessus reports can be very helpful in patching systems. They can be extracted to Adobe Acrobat (.pdf) format for easy viewing also.

We need to check the IDS, firewall log, and the syslog to make sure that we see the activity from the tests. If we don't, we need to make some changes. This is also useful in showing us some things to look for in the logs that might indicate someone footprinting our network or even attempting an attack on a system.

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

## Assignment 4 – Design Under Fire (25 Points)

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

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

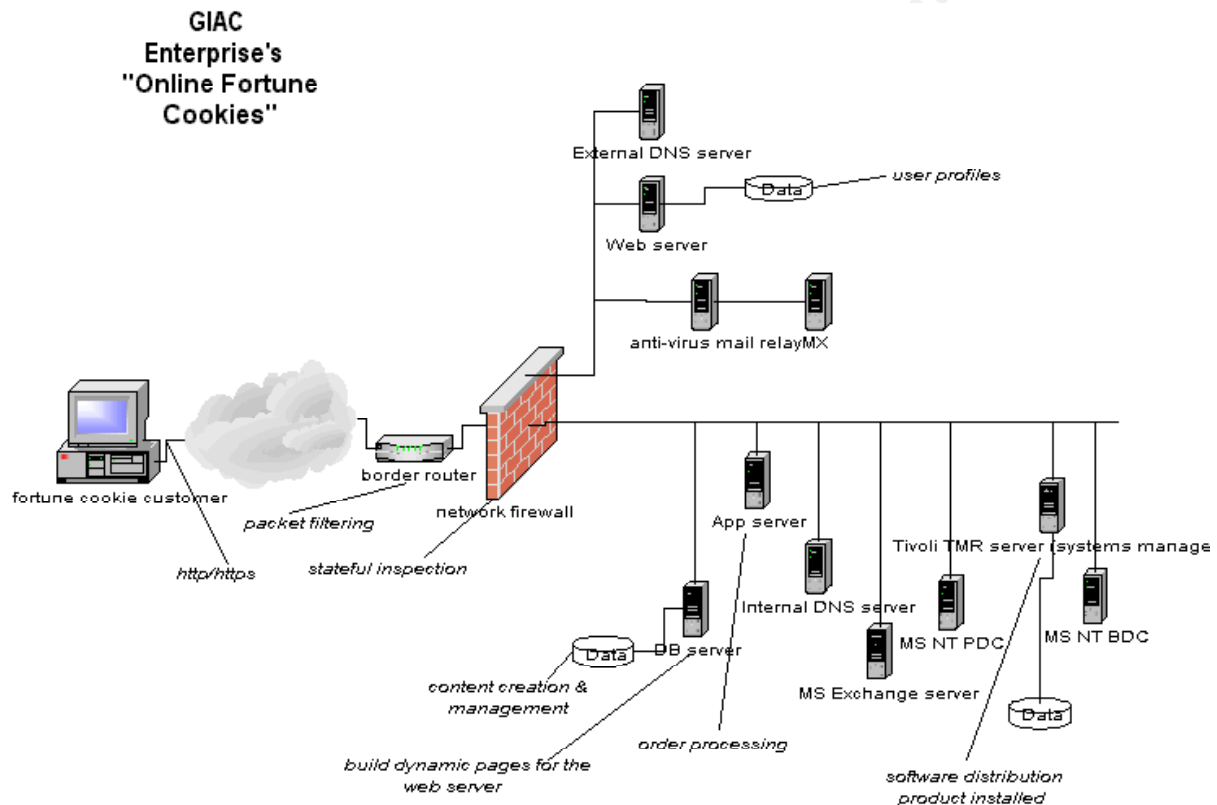
1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from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

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

---

For this assignment I have chosen Sinead Hanley’s design at:  
[http://www.sans.org/y2k/practical/sinead\\_hanley\\_GCFW.doc](http://www.sans.org/y2k/practical/sinead_hanley_GCFW.doc)

This design uses a Cisco 1600 series border router and a ConCeal PC Firewall as the perimeter firewall running on a Windows NT box. Not much information is given concerning the internal systems but only Windows NT is mentioned so we will assume an NT shop. It also uses static NAT on the firewall for the e-commerce servers. Below is the diagram from this practical:



### Attack against the firewall

The firewall is a ConSeal PC Firewall. This is a host based packet filtering firewall. It does not do stateful inspection. It may work okay as a personal firewall but it is not a good choice to protect an e-commerce site.

A quick trip to <http://www.candc1.com/conseal/knownissues.htm> and we see that there are two known issues that might affect this firewall. The first is that if the box goes into sleep mode, the firewall may shut down. If sleep mode has not been disabled, we can get through the firewall on just about any night or weekend for sure. There is a BETA patch for this on the site.

The second issue involves a conflict with Norton Anti-Virus, which is being used. Any time the firewall is opened or closed, or if the computer is rebooted, ConSeal will freeze for up to two minutes. During this time, the OS could still pass packets. If we caused the box to hang, and hence, require a reboot, we could get through the firewall for a short time unmolested and unlogged. We can accomplish this with a DoS attack as shown later.

The solution to this problem is setting Norton Anti-Virus to not scan the ConSeal directories. This solution does not always fix the problem but should at least shorten the duration of the freeze.

### **Denial of Service Attack**

The router does not appear to block anything but private IP addresses. A smurf attack could be used to overwhelm the firewall and possibly cause it to hang. This would require a reboot which, as mentioned above, would allow all traffic to go through the firewall unchecked and unlogged for a time.

Setting no ip directed-broadcast at the border router would prevent this.

Another DoS attack that could work on the web server is a SYN flood. The firewall is not stateful and can not protect the web server from this. A SYN flood is where you send a bunch of SYN packets from spoofed IP addresses to the server. The server responds with a SYN/ACK and waits for the ACK. The time it waits is generally a few minutes. If you can send enough SYN packets to the server, it will run out of resources and crash. Even if the server doesn't crash, it should get to a point where it ignores new connection requests.

There isn't much that you can do with this firewall to prevent this. You could reduce the timeout on the server itself.

The following rules look like they allow pings both ways:

2 Ping others.				Allow In Out All
Addresses 0.0.0.0	Ping Reply	My Address		
255.255.255.255 Ping Send	Always		100	F
32 Allow ICMP Echo Reply			Allow In	
Out All Addresses 0.0.0.0	Ping Send	My Address		
255.255.255.255 Ping Reply	Always		100	L

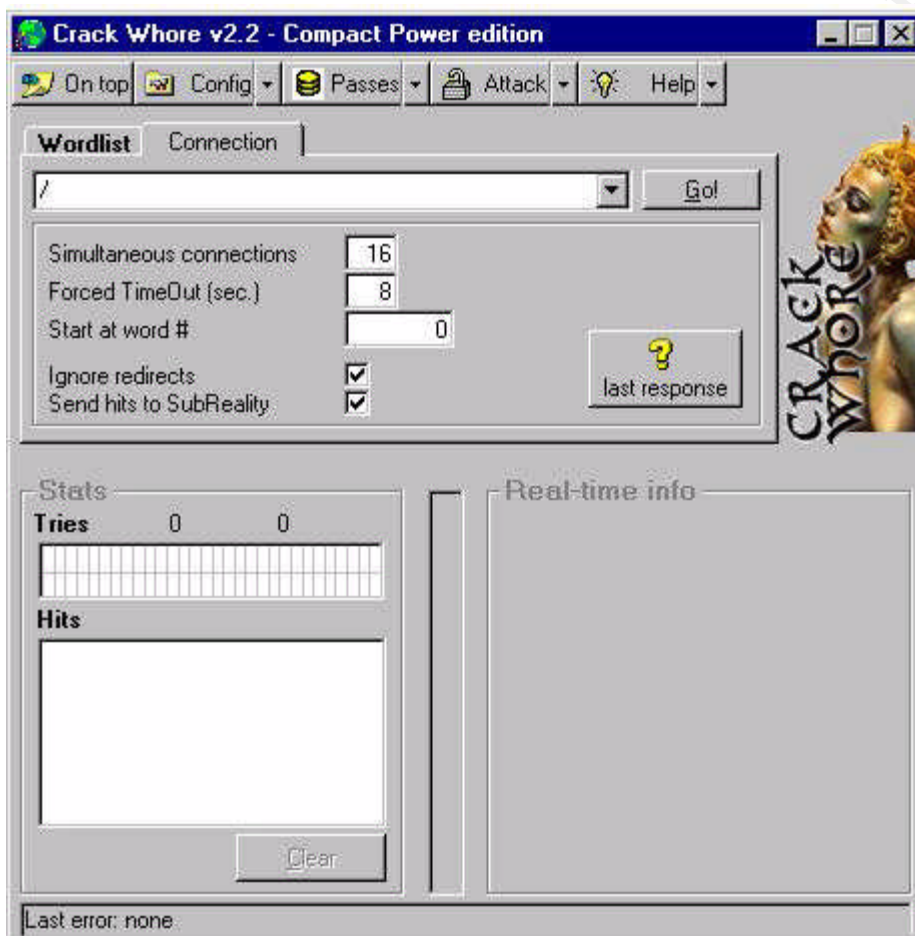
If this is the case, we have 50 compromised cable/DSL systems that we can use to launch a ping flood attack using trin00 or Tribe Flood Network. If we don't bring any systems down, we will certainly clog up the incoming link so badly that no one will get through.

You could block ICMP at the border router or at the firewall, but with a small incoming link, this isn't going to prevent a large DDoS attack.



## Compromise an Internal System

Let's say that our reconnaissance has shown that IIS is being used for their web server. There are a couple of things that point to this being a good target (besides it being IIS): "passwords must be at least six characters long" and "a username and password will protect confidential information on the webserver". CrackWhore ([www.subreality.net](http://www.subreality.net)) is a nice little program that will brute force a webpage login. (The screen capture below has been altered)



NOTE – Windows NT uses a 7 character hash for its passwords. Try running L0phtCrack against an NT SAM file. The eighth character in any eight character long passwords will be discovered quickly.

CrackWhore has a dictionary that can be used and works through a proxy server of your choice so it is much harder to track back to the real source. You might want to pick a proxy server in another country that uses a different language and is not on the best of terms with us. That way they may not be too helpful to anyone investigating the crack attempt.

The fix for this is to use stronger passwords and not use just username password to get to any confidential information. I also wouldn't store it on the webserver.

A new attack that should work is SMBRelay. SecurityFocus has a write up on their webpage about it. The following rule shows NetBIOS being allowed through the firewall:

45	TCP/IP				Allow	In	Out
10.90.24.250	255.255.255.255	Temp. Range	My Address				
255.255.255.255	NetBIOS	Always			100	*	F

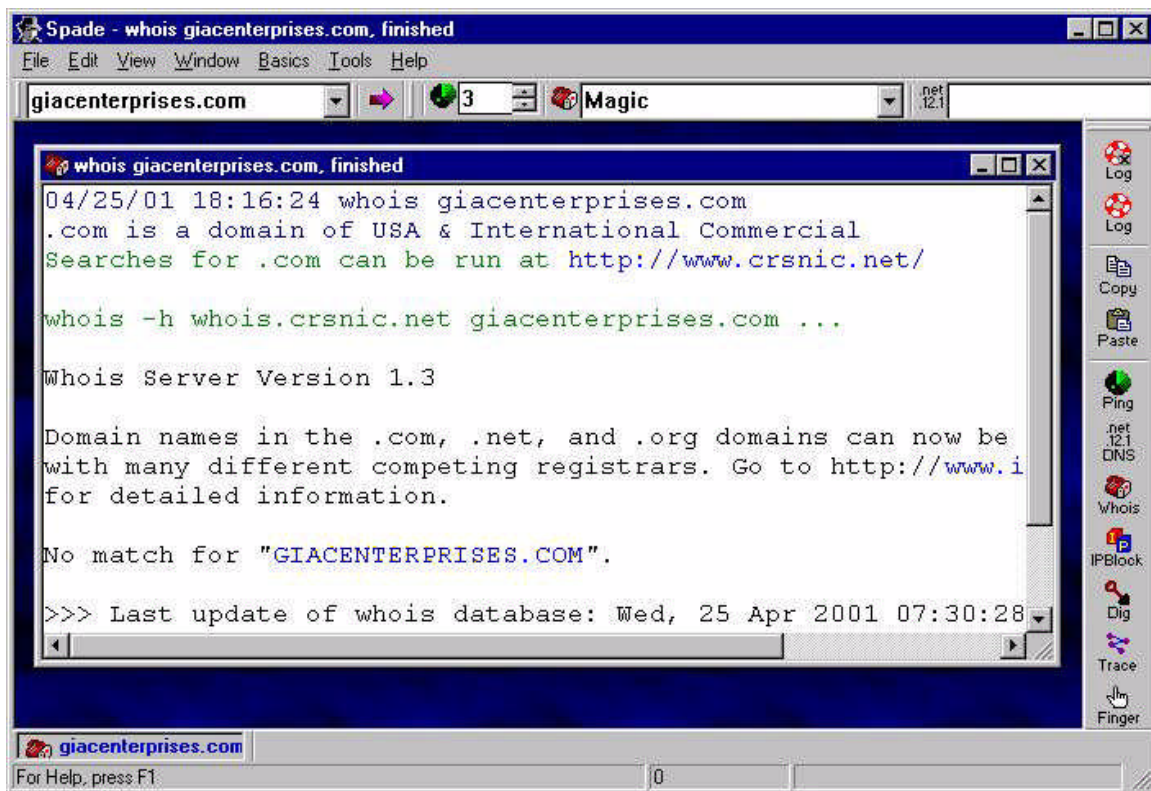
SMBRelay is a “man in the middle” attack that allows someone to hijack a connection. If the account used on the hijacked connection is admin level, they now have admin rights! All they have to do is create a few accounts of their own with admin privileges and they can come back whenever. Another feature of SMBRelay is that it grabs the password hashes. These can be used later by L0phtCrack ([www.securitysoftwaretech.com/lc3](http://www.securitysoftwaretech.com/lc3)) to crack the passwords.

The fix for this would be to block NetBIOS at the firewall. I'd also use NTLMv2 which has 128bit keys and should stop this internally as well.

#### What if we didn't know the architecture?

Although not technically required in this assignment, something else that should be talked about is how an outside hacker would get architecture information on your network.

A good tool for this is Sam Spade ([www.samspade.org/ssw](http://www.samspade.org/ssw)):



You start out running a whois against a domain name. You can then run ping, nslookup, dig, traceroute, finger, scan address, crawl website. Other things you can do include zone transfers and SMTP relay checks.

The basic procedure is to do a whois to get the DNS server names and addresses. You then do an nslookup to get several (hopefully) publicly available server names. You might try a zone transfer on the DNS servers. If it works, you should get a good list of several if not all their servers and could even get the OSes on them if they entered that information. By now you should have the general IP range for their network. Perform an nmap stealth scan on the network addresses to see what you can find out. You might even use the OS fingerprinting option.

Another thing that can be done is to telnet to a port. Try "telnet [www.giacenterprises.com](http://www.giacenterprises.com) 80" and see what happens. It may just tell you which OS they are running...