Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment

Version 1.6a

Prepared by Blair Nason

February 19, 2002

Table of Contents

Assignment 1 – Security Architecture

Overview

GIAC Enterprises is a small but growing company of 27 people in a rural city that deals in the sales of fortune cookie sayings. They have decided to upgrade their technology and go online to do e-business with their customers, suppliers, and partners and allow remote access. A two-phase plan was developed and a two-year time frame was set for completing this implementation due to budget restraints. Phase one involved the upgrading of the workstations and servers, purchasing additional server hardware, and upgrading the network infrastructure. Phase one has been completed. Based on both GIAC business and security needs, phase two (this assignment) involves the set up and configuration of security components for connectivity to the Internet.

Assumptions

- There are budget restraints associated with this GIAC design.
- Redundancy is not required but expandability needs to be considered
- Network design is for data only; no long term plans for VoIP.
- GIAC preferred vendors are Microsoft, Compaq, Cisco and RedHat.
- The ISP for GIAC Enterprises has assigned the IP address (142.166.0.192/28)
- The ISP service supports a maximum of a 1.5M download and 750k upload.
- The ISP handles external routing and routing protocols.
- The "giac.com" name is registered to GIAC Enterprises.
- Currently there is no requirement for remote access for GIAC employees.
- Partner / suppliers use VPN technology for connectivity to GIAC "common" environment.
- There is no dial-up or dial-out access within GIAC network.

Business Practices

With the use of definitions and business policies, GIAC was able to develop a security policy to meet their current and future business needs.

Customer

- The customer is an individual or company that buys the fortune cookie saying.
- A customer requires a 128bit capable web browser for accessing http://www.giac.com over http / https.
- A customer requires a unique user name & password. The user name and password has already been assigned to the customer before accessing GIAC web service.

Partner

- A partner is an individual or company who assists in both the translation and re-selling of the fortune cookie saying.

- Data is transferred between a partner and GIAC through a VPN tunnel to a "common" server in a DMZ environment.
- The protocol for transporting data is SSH using either SFTP (Secure File Transfer Protocol) or SCP (Secure Copy) within the VPN tunnel.
- Each partner has a dedicated user name & password (previously assigned) on the "common" server. Dedicated directories on the server are used for picking up and delivering fortunes.
- Partners place their orders for re-selling fortunes through the same web access used by the "customers" (https://www.giac.com).

Suppliers

- A supplier is an author of a fortune cookie saying.
- Bulk data transfers are made through a VPN connection to the "common" server in a DMZ environment.
- The protocol for transporting data is SSH using either SFTP (Secure File Transfer Protocol) or SCP (Secure Copy) within the VPN tunnel.
- A user name and password is required (previously assigned).
- Single entries can be made via https over the web (https://www.giac.com).

GIAC employees

- The employees on GIAC network are located behind an internal firewall.
- Domain and system passwords are used to control access to all GIAC resources.
- All traffic flow within the internal networks are restricted by access control lists (ACLs) on each vlan.
- There's no remote access into GIAC internal network.
- All Internet traffic is routed through a non-transparent proxy server.

The Internet community has access to GIAC public information over the web via http. GIAC company profile, products and services, contact information and other general information are displayed through http://www.giac.com.

Security Policies

Some examples of general security practices implemented by GIAC include:

- Physical Security.
  - Production and development systems are located in a secure environment(s).
  - Only authorized users have access to the secure environment(s).
  - Visitors are escorted at all times while on GIAC premises.

- Logical security.
  - Everyone has a unique user name. There are no generic or shared accounts.
  - Password policy specifies length, uniqueness, password aging, etc.
  - No sharing of user names or passwords.

- General practices.
  - Server builds are based on minimum installs for server functionality.
  - All servers use time synchronization.
  - Vulnerabilities are assessed as they are announced.
  - System patches are tested and applied as needed.
  - Logging capabilities are enabled.
  - Log reviews are completed daily.
  - Security policies are reviewed / compared against current system configurations.
  - All employees must go through a proxy server before accessing the Internet.
  - All inbound and outbound emails are scanned for viruses.
  - Syslog capabilities are enabled and logged to an internal syslog server.

Some examples of security policies implemented by GIAC include:

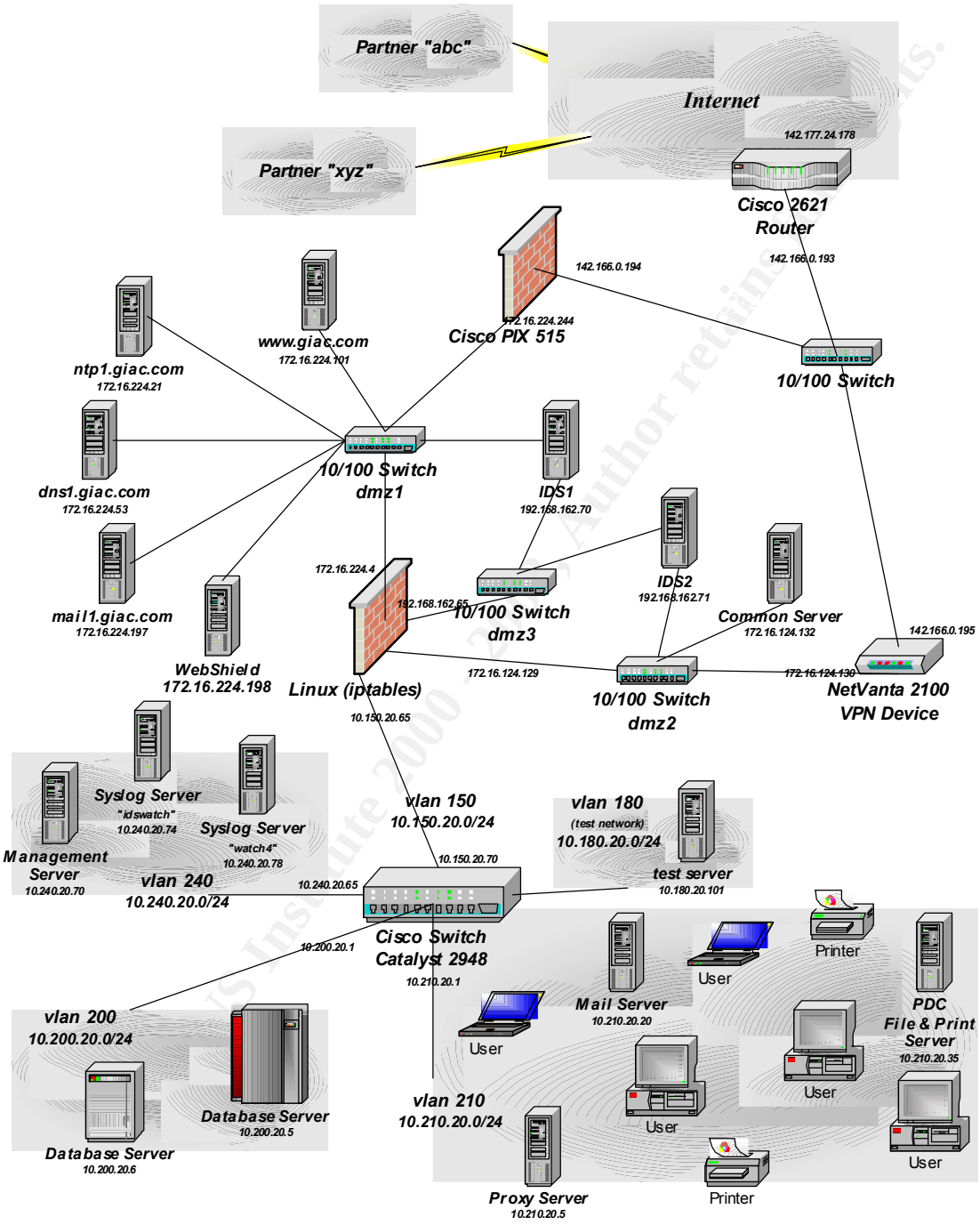
- The proxy server is restricted to port 80 and 443 for Internet access.
- The external DNS server will accept only UDP and TCP port 53.
- Only webshield can access the internal exchange server on TCP port 25.
- Only the border router can access GIAC management server on UDP port 69.

For a more detail list, see Appendix A.

IP Addressing

Device	*Host Name*	*IP Address*	*Public IP Address*
Cisco 2621 Router	outside	e0/0 – 142.177.24.178	142.177.24.178
		e0/1 – 142.166.0.193	142.166.0.193
Cisco PIX	control	outside – 142.166.0.194	142.166.0.194
		inside – 172.16.224.224	n/a
NetVanta 2100	special	WAN - 142.166.0.195	142.166.0.195
		LAN - 172.16.124.130	n/a
Linux Netfilter	rifraf	eth0 – 172.16.224.4	n/a
		eth1 – 192.168.162.65	n/a
		eth2 – 172.16.124.129	n/a
		eth3 – 10.150.20.65	n/a
Web Server	www	172.16.224.101	142.166.0.200
NTP Server	ntp1	172.16.224.21	142.166.0.203
DNS Server	dns1	172.16.224.53	142.166.0.202
External Mail Server	mail1	172.16.224.197	142.166.0.201
Virus Scan Server	webshield	172.16.224.198	n/a
Common Server	any1	172.16.124.132	n/a
Management Server	topgun	10.240.20.70	n/a
IDS #1 in “dmz1”	IDS1	192.168.162.70	n/a
IDS #2 in “dmz2”	IDS2	192.168.162.71	n/a
Syslog Server #1	idswatch	10.240.20.74	N/a
Syslog Server #2	watch4	10.240.20.78	n/a
Internal Mail Server	exchange	10.210.20.20	n/a
Proxy Server	proxy	10.210.20.5	142.166.0.205

Network Diagram



Device Description & Specification

Border Router (outside)

The border router is the first layer of security for the perimeter defence for GIAC. The Cisco 2621 is a good performance router with great scalability for this environment. The Cisco 2621 with the availability of the Hot Standby Routing Protocol (HSRP) could be used when redundancy is required. This Cisco 2621 has 16M flash / 40M RAM and is currently running Cisco IOS version 12.2 with IP feature set.

External Firewall (control)

GIAC decided to go with a Cisco 515 PIX as its stateful inspection firewall. The PIX is a hardware base solution that has performance, expandability and redundancy capabilities. Also, the PIX has built-in IDS capabilities (although limited), administration through command line (via ssh or telnet) and/or PIX Display Manager (https) and syslog capabilities for troubleshooting and logging.

VPN Solution (special)

The NetVanta 2100 for site-to-site and client-to-site applications adheres to IPSec standards and is interoperable with many other multi-vendor IPSec VPN solutions. Encryptions using DES and 3DES, stateful inspection firewall capabilities, Network Address Translation, and support of Internet Key Exchange makes the NetVanta a low cost all in one solution for VPN.

Demilitarized Zone (dmz1)

DNS Server (dns1)

For DNS within the GIAC network, "dns1.giac.com" will forward all DNS requests to the Internet and will act as the authority for the "giac.com" domain. This DNS server is running on a harden/patch RedHat 7.2 with Bind 9.1. There is no zone transfers between the internal DNS and dns1. Tripwire is installed and syslog is done locally and to a remote syslog server (watch4).

SMTP Mail (mail1)

The external mail server is another harden/patch RedHat 7.2 server running QMail. Its function is to send / receive SMTP traffic. This server is defined for only relaying SMTP messages from the internal servers to the Internet. "mail1" also has Tripwire installed and has its syslog sent locally and to a remote syslog server (watch4).

Virus Scanner (webshield)
WebShield 4.5 is running on a harden/patch Windows2000 standalone server and scans all SMTP emails and attachments for viruses. Mail is forwarded between mail1 and the internal exchange server through webshield. Virus scanning is done for both inbound and outbound messages. All virus updates are received from an internal system through a passive ftp connection so no direct connectivity to the Internet is required for webshield.

Web Server (www)
The web server is the gateway into GIAC Enterprises for information from the company profile to status on orders. A harden/patch RedHat 7.2 server is running Apache 1.3.20 but other than web pages, no data is stored on this server. For data, the correct credentials must be supplied and "www" will query the internal database server and forward the information back to the requester. Tripwire is installed and syslog is done locally and to a remote syslog server (watch4).

NTP Server (ntp1)
The NTP server is used for time synchronization for all servers within GIAC network to basically ensure time consistency in logged information. This system (a harden/patch RedHat 7.2) does its time synchronization with four external NTP servers to help protect it from incorrect or non-functional external NTP servers. Tripwire is installed and syslog is done locally and to a remote syslog server (watch4).

Intrusion Detection (IDS1)
In order to monitor activity within the demilitarized zone (dmz1), GIAC has decided to deploy a harden/patch RedHat 7.2 running snort 1.8. With two network interfaces in the server, the passive interface listens to "dmz1" traffic and the other interface can forward the information on to a management system. The "dmz1" switch is capable of scanning multiple vlans / ports allowing for the IDS to see all traffic. Tripwire is installed and syslog is done locally and to a remote syslog server (idswatch).

Internal Firewall (rifraf)
Internal firewall is a Compaq DL380 running Netfilter (iptables) on a harden/patch RedHat 7.2 OS. The Compaq DL380 was chosen because of its expandability and redundancy capabilities and Netfilter (a stateful inspection firewall) was selected for its detail logging capabilities and the ability to insert log-prefix extensions based on your own pattern definitions. Tripwire is installed and syslog is done locally and to a remote syslog server (watch4). One reason for choosing a different firewall technology (for the internal and external firewall) was to reduce the possibilities of platform vulnerabilities and human error in configuring rules between firewalls through copy / paste commands.

Internal LAN
GIAC internal network is focused around the Catalyst 2948 switch. With the capability of layer two switching and layer 3 routing, this device allows for isolation of the collision and broadcast domain and some level of security through the use of access control lists.

Vlan180
This is GIAC test and development network. This vlan is only accessible from the internal network and has no external connectivity (i.e. Internet or dmz's).

Vlan200
This network is where the database servers reside. With access control lists (ACLs), workstations are restricted based on IP addresses and port numbers. The database servers have user names and passwords defined, as do the databases themselves. The database server initializes a ssh connection to the "common" server in "dmz2" for pulling partner and supplier data as well as pushing partner data. A process is then run to verify format, content, etc. before inserting data into the production database.

Vlan210
This network is basically the internal network with desktop users. This is a mixed environment of Windows 98, Windows2000 Professional and Windows2000 server. This is the noisiest network with Exchange services, File/Print services, Proxy services, etc… This network has restricted access to vlan180, vlan200, vlan240 and externally.

Vlan240
Syslog server (watch4) – all systems with logging capabilities (with the exception of vlan210, vlan200 and IDS systems) push their logs here. This harden/patch RedHat 7.2 server has a large storage capacity with a CD-RW device. Logs are moved to CDROM on a regular basis with the storage of the media being offsite. Log analyzer tools are used daily to go through the large amount of data for interpretation.

Syslog server (idswatch) – both IDS systems push their logs to this harden/patch RedHat 7.2 server. Even with large storage capacity, a CD-RW device is used to move logs to CDROM on a regular basis with the storage of this media being offsite. Alerting is done through local scripts and log analyzer tools are used for data interpretation. The IDS logs are stored on a separate syslog server because of security reasons (not every one needs access to them), the volume of data generated and manageability.

Management server (topgun) – is a harden/patch RedHat 7.2 workstation mainly used for the access and configuration of rifraf, control, special, IDS1 and IDS2 through SSH. TFTP services are started / stopped as needed for IOS updates / backups for the Cisco equipment. Web browser functionality is used for administering the NetVanta VPN device.

Demilitarized Zone (dmz2)

"Common" Server
The partners and suppliers use this server as a drop off / pick up point for the fortune cookie saying. It's a harden/patch RedHat 7.2 platform designed for accepting SSH connections only. Tripwire is installed and syslog is done locally and to a remote syslog server (watch4).

Intrusion Detection (IDS2)

In order to monitor activity within the demilitarized zone, GIAC has decided to deploy a harden/patch RedHat 7.2 running snort 1.8. With two network interfaces in the server, the passive interface listens to "dmz2" traffic and the other interface can forward the information on to a management system. The "dmz2" switch that the IDS connects to is capable of scanning multiple vlans / ports allowing for the IDS to see all traffic. Tripwire is installed and syslog is done locally and to a remote syslog server (idswatch).

The overall design provides protection by isolating GIAC key segments and applying multiple layers of security. The border router with its packet filters in place, will cut down on unnecessary traffic before it passes to the firewall or VPN device. The PIX firewall (with NAT and stateful inspection) restricts access to / from the Internet and NetVanta device provides VPN capabilities. The Netfilter firewall is to protect the internal network from all other networks (dmz1, dmz2 and Internet). Since traffic flow between each segment is specific, each firewall device would have a different set of rules for permitting connectivity. The rules in the PIX firewall wouldn't be the same as the rules in the Netfilter or VPN device. Human error would less likely be a factor in opening something up all the way through to the internal network. Even the Catalyst switch with its access control lists (ACLs) would provide some packet filtering capabilities.

Assignment 2 – Security Policy

Configuration of Border Router

The border router is the first line of defence to keep some unnecessary traffic from entering GIAC network. As part of assignment #2, detailed instructions are provided in the configuration of the border router after the initial set-up has been completed (see Appendix B for initial configuration). ACL syntax was taken from:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#1001235

outside> enable

- Enters the user into privileged EXEC mode.

outside#conf t
Enter configuration commands, one per line. End with CNTL/Z.

- Enters the user into the global configuration mode for making system wide changes.

Syntax for creating Standard ACLs

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]

outside(config)#access-list 1 permit 10.240.20.70

- This is for creating a Standard Access Control List (ACL). This rules permits access for the system with IP address of 10.240.20.70 on any port. The "1" is a means of referencing this specific access list.

outside(config)#line vty 0 4

- Allows the user to do configuration changes associated with the remote console access (vty - Virtual terminal).

outside(config-line)#access-class 1 in

- This applies the access control list "1" to the inbound interface of ***vty 0 4***. This means that only the IP address of 10.240.20.70 can telnet to the router and have the router accept the connection.

outside(config-line)#exit

- Returns the user to global configuration mode.

outside(config)#
outside(config)#service password-encryption

- This will encrypt (a weak encryption algorithm) any clear text passwords within the configuration file.

outside(config)#no ip source-route

- This will disable source base routing options (Record Route, Loose Source Route and Strict Source Route), which could be misused to facilitate IP address masquerading or address spoofing.

outside(config)#no ip bootp server

- To disable bootp service available from hosts on the network.

outside(config)#no service tcp-small-servers

- This disables TCP services (echo, discard, daytime, chargen, and time). This is disabled by default on Cisco's IOS 12.0 and newer.

outside(config)#no service udp-small-servers

- This disables UDP services (echo, discard, daytime, chargen, and time). This is disabled by default on Cisco's IOS 12.0 and newer.

outside(config)#no service finger

- Disables the finger service, which is used by attackers to gather information about the target.

outside(config)#no cdp run

- This disables the Cisco Discovery Protocol (cdp). An attacker could use this information to identify Cisco network components and map out the network.

outside(config)#interface FastEthernet 0/0
outside(config-if)#no ip unreachables
outside(config-if)#no ip redirects
outside(config-if)#no ip proxy-arp
outside(config-if)#exit

- This disables ICMP host unreachable messages, ICMP redirect messages and proxy ARP from being sent to the originator through interface FastEthernet0/0. These are methods to discover if systems or ports are up and available.

outside(config)#interface FastEthernet 0/1
outside(config-if)#no ip redirects
outside(config-if)#no ip proxy-arp
outside(config-if)#exit

- This disables ICMP redirect messages and proxy ARP on FastEthernet0/1.

outside(config)#logging 10.240.20.78

- Defines a server IP address who's receiving syslog messages.

outside(config)#logging trap 6

- Defines the syslog level where level 6 is informational messages.

outside(config)#service timestamps log datetime msec

- Defines the timestamp of the syslog to include milliseconds in the date and time values.

outside(config)#banner /
Enter TEXT message. End with the character '/'.

***** WARNING: Authorized Access Only *****

This site is currently being monitored
/

- This places a login message that is displayed upon remote logins.

Syntax for creating Extended ACLs

access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [*precedence precedence*] [*tostos*] [*established*] [**log** | **log-input**] [*time-range time-range-name*]

outside(config)#access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
outside(config)#access-list 101 deny ip 224.0.0.0 7.255.255.255 any log
outside(config)#access-list 101 deny ip 255.0.0.0 0.255.255.255 any log

- This is to block and log loopback, multicast and broadcast addresses.

outside(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
outside(config)#access-list 101 deny ip 172.16.0.0 0.0.255.255 any log
outside(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

- This is to block and log private network addresses.

outside(config)#access-list 101 deny ip host 0.0.0.0 any log

- This is to block the invalid address.

outside(config)#access-list 101 deny ip 142.166.0.180 0.0.0.15 any log

- This is to block and log spoofed GIAC addresses.

outside(config)#access-list 101 permit ip any any

- This accepts all other traffic on the external interface.

outside(config)#access-list 121 deny tcp 142.166.0.192 0.0.0.15 any range 135 139 log
outside(config)#access-list 121 deny udp 142.166.0.192 0.0.0.15 any range 135 139 log
outside(config)#access-list 121 deny tcp 142.166.0.192 0.0.0.15 any eq 445 log
outside(config)#access-list 121 deny udp 142.166.0.192 0.0.0.15 any eq 445 log

- This blocks Windows related traffic generated from within the network from leaving the GIAC network.

outside(config)#access-list 121 permit ip 142.166.0.192 0.0.0.15 any

- This allows all other traffic from the GIAC network.

outside(config)#interface FastEthernet 0/0
outside(config-if)#ip access-group 101 in

- This applies access list "101" to the inbound interface of Ethernet 0/0.

outside(config-if)#interface FastEthernet 0/1
outside(config-if)#ip access-group 121 in

- This applies access list "121" to the inbound interface of Ethernet 0/1.

outside(config-if)#exit

outside(config)#exit

- Returns the user to privileged EXEC.

For complete configuration without comments, see Appendix C.

To verify that "***no cdp run***" actually disabled the Cisco Discovery Protocol, from the EXEC mode, type:

outside#sh cdp

The response will be:

- % CDP is not enabled

outside#

To verify that "***access-list 1 permit 10.240.20.70***" was applied to "***line vty 0 4*** " with the banner message; use the workstation with IP address 10.210.20.70 (topgun) and telnet to the router (142.166.0.193). The following message will be displayed for accepted connections.

[root@topgun root] telnet 142.166.0.193
Trying 142.166.0.193…
Connected to 142.166.0.193.
Escape character is '^]'.

***** WARNING: Authorized Access Only *****

This site is currently being monitored

User Access Verification

Password:

To verify that other workstations can't connect, use a workstation from the Internet and telnet to the router's external IP address (142.177.24.178). The following message will be displayed.

[root@localhost root]#
Trying 142.177.24.178…
telnet: connect to address 142.177.24.178: Connection refused
[root@localhost root]#

To verify the following rule within an "access list 101":

access-list 101 deny ip 172.16.0.0 0.0.255.255 any log

Using a workstation on the Internet, send a spoofed ICMP packet to the router (142.177.24.178) with the source address of 172.16.224.194. The syslog server will log a similar response:

Apr 2 16:05:23 142.177.24.178 33: *Apr 2 16:05:23.819: %SEC-6-IPACCESSLOGDP: list 101 denied icmp 172.16.224.194 -> 142.177.24.178 (0/0), 1 packet

You will also see that the "matches" will increase by one if one did a "sh access-list 101" before and after the ICMP command. This is assuming that no other traffic was sent and was denied by this rule during this test.

Configuration of External Firewall

The following are some highlights from the Cisco PIX configuration. For the detailed configuration file, refer to Appendix D.

The PIX is providing both static Network Address Translation (NAT) and Port Address Translation (PAT).

global (outside) 1 142.166.0.205
nat (inside) 1 10.210.20.0 255.255.255.0 0 0

In this configuration, all internal addresses of 10.210.20.0 network are being translated to the outside world as 142.166.0.205. An access control list (acl_inside) on the interface "inside" is used to restrict access to only the proxy server for outbound connections from the 10.210.20.0 network. With no general NAT defined for the 172.16.224.0 network (dmz1), no server on this network can establish a connection to the outside world unless defined by the static NATs.

The following are static NAT translations:

This maps "mail1" internal address to an external IP address (142.166.0.201),

static (inside,outside) 142.166.0.201 mail1 netmask 255.255.255.255 0 0

This maps "dns1" internal address to an external IP address (142.166.0.202),

static (inside,outside) 142.166.0.202 dns1 netmask 255.255.255.255 0 0

This maps "ntp1" internal address to an external IP address (142.166.0.203)

static (inside,outside) 142.166.0.203 ntp1 netmask 255.255.255.255 0 0

This maps "www" internal address to an external IP address (142.166.0.200)

static (inside,outside) 142.166.0.200 www netmask 255.255.255.255 0 0

Access lists are used to permit or deny traffic to each interface on the PIX. Access list "acl_inside" is applied to the "inside" interface with "acl_outside" applied to the "outside" interface. The rules are as follows:

1. ***access-list acl_inside permit tcp host 10.210.20.5 any eq www***
2. ***access-list acl_inside permit tcp host 10.210.20.5 any eq 443***
3. ***access-list acl_inside permit tcp host 10.210.20.5 any eq ftp***
4. ***access-list acl_inside permit tcp any host dns1 eq domain***

5. ***access-list acl_inside permit udp any host dns1 eq domain***
6. ***access-list acl_inside permit tcp any host mail1 eq smtp***
7. ***access-list acl_inside permit udp any host ntp1 eq 123***
8. ***access-list acl_inside permit tcp host topgun host 142.166.0.193 eq telnet***
9. ***access-list acl_inside permit udp host topgun host 142.166.0.193 eq tftp***
10. ***access-list acl_inside deny ip any any***

Rule 1 - The proxy server can access the Internet on TCP port 80 (http).
Rule 2 - The proxy server can access the Internet on TCP port 443 (https).
Rule 3 - The proxy server can access the Internet on TCP port 21 (ftp control).
Rule 4 - DNS services are permit with "dns1" on TCP port 53.
Rule 5 - DNS services are permit with "dns1" on UDP port 53.
Rule 6 - SMTP is permit on TCP port 25 with "mail1".
Rule 7 - Time synchronization is permit with "ntp1" on UDP port 123.
Rule 8 - "topgun" has telnet access to border router on TCP port 23.
Rule 9 - "topgun" can tftp to border router on UDP port 69.
Rule 10 - Deny all other traffic.

1. ***access-list acl_outside permit tcp any host www eq www***
2. ***access-list acl_outside permit tcp any host www eq 443***
3. ***access-list acl_outside permit tcp any host mail1 eq smtp***
4. ***access-list acl_outside permit tcp any host dns1 eq domain***
5. ***access-list acl_outside permit udp any host dns1 eq domain***
6. ***access-list acl_outside permit udp host 142.166.0.193 host topgun eq tftp***
7. ***access-list acl_outside deny ip any any***

Rule 1 - This allows TCP port 80 (http) to GIAC web server.
Rule 2 - This allows TCP port 443 (https) to GIAC web server
Rule 3 - This allows the outside world to access "mail1" on TCP port 25 (SMTP).
Rule 4 - This is for DNS queues to "dns1" on TCP port 53
Rule 5 - This is for DNS queues to "dns1" on UDP port 53.
Rule 6 - TFTP access to border router on UDP port 69.
Rule 7 - Deny all other traffic

Even though "***deny ip any any***" is implied, coding this rule in both the "acl_inside" and "acl_outside" gives a visual representation in the access control lists and allows for a "hit counts" to be displayed when doing a "sh access-list". It will also help ensure that the rule will remain intact, if in future PIX IOS releases the implied rule is removed.

To help control remote access to the PIX:

ssh topgun 255.255.255.255 inside
http topgun 255.255.255.255 inside

The PIX supports ssh (Secure Shell) connections as well as telnet connections for remote administration. Even though the PIX is using ssh protocol 1 with RSA and "DES" for its encryption method, it provides better security than using telnet with clear text. To configure the PIX for accepting ssh connections:

domain-name giac.com
ca generate rsa 1024
sh ca mypubkey rsa
ca save all

The "domain-name" command sets the domain for the PIX. If the domain name is not configured, the PIX will use "ciscopix.com" as a default domain. For the RSA key, the bit size can be 512, 768, 1024 or 2048 with 768 as its default. The "sh ca mypubkey rsa" just displays the public key of the PIX which is saved in Flash memory.

It also has a HTTP server associated with PIX Display Manager (PDM). The PDM allows for administration through a web browser on https but not all commands are supported under this. In the above syntax, "topgun" is being allowed access to both services.

The PIX "service resetinbound" command is used to return a RST flag in the TCP header to the source so a packet doesn't get dropped. IDENT is a service associated with email that is waiting for a reply. By just dropping this packet, the outside host keeps sending SYN packets until the IDENT times out. This may slow down performance.

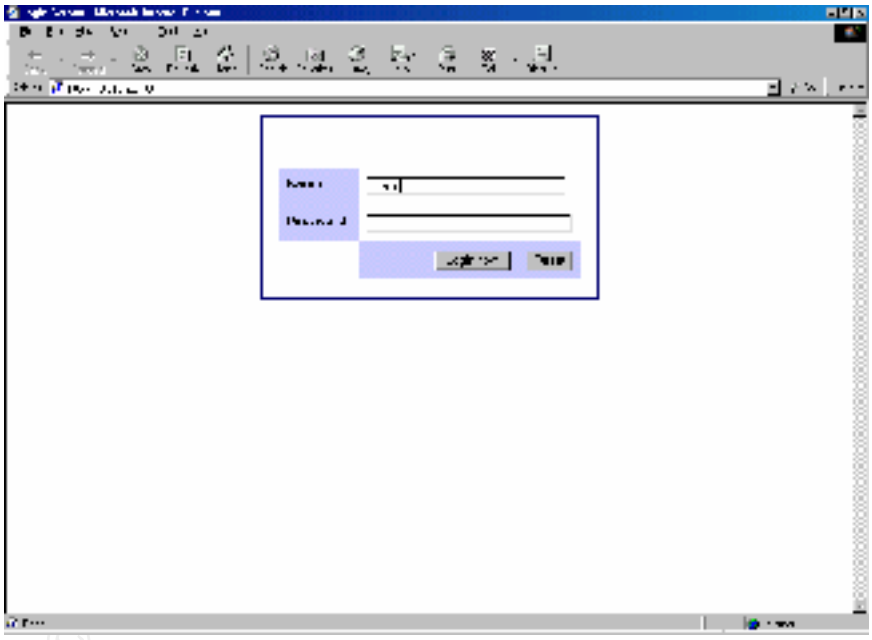
service resetinbound

Configuration of VPN Solution

The VPN solution is using an Adtran NetVanta 2100 in a site-to-site configuration but has the ability for client-to-site connectivity using client software from www.safenet-inc.com. The NetVanta is an IPSec (Internet Protocol Security) compliant device that supports both ESP and AH and can support up to 10 private encrypted tunnels.

The following screen shots are just a few of the many user-friendly web interfaces used in configuring the NetVanta. For more configuration options, refer to Appendix E.

The NetVanta comes with the "LAN" interface pre-configured with an IP address of 10.10.10.1 and a network mask of 255.255.255.0. Configure a workstation with a 10.10.10.x address (i.e. 10.10.10.50 with a network mask of 255.255.255.0) and using a cross-over cable, connect it to the "LAN" interface. Using a web browser on the workstation, connect to http://10.10.10.1 and logon to the NetVanta. The user name is "admin" and the password field is blank by default. Be sure to set a password.



Note: The NetVanta should be configured with no network connectivity except for the cross-over cable from the workstation. This limits the risk of exposure until the initial set-up is completed.

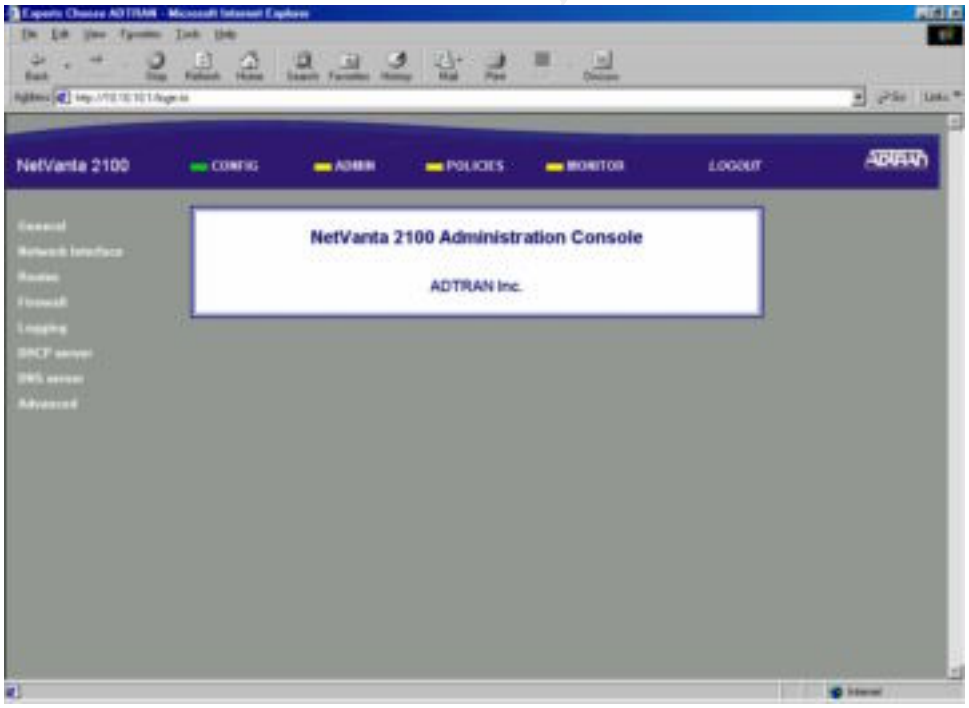
The NetVanta 2100 Administration Console contains a main menu bar with four areas of configuration (CONFIG, ADMIN, POLICIES, and MONITOR) and a menu list with applicable options.

CONFIG – the CONFIG menu contains the basic configuration parameters for setting up IP addressing for the Network Interface, Route and routing information, Firewall settings, Logging capabilities, DHCP parameters, DNS server options, and Advanced configurations.

ADMIN – the ADMIN menu allows system administration changes such as Change Password, Rebooting the NetVanta, Save Settings permanently, Factory Defaults, and Upgrading Firmware.

POLICIES – the POLICIES menu allows for Manage List (which include Users, IP Addresses, Services, Schedule and NAT policies), LAN Inbound for inbound VPN rules, and LAN Outbound for outbound VPN rules, and VPN policies.

MONITOR – the MONITOR menu contains information in regards to Policy Statistics, User Accounting and Access Logs.

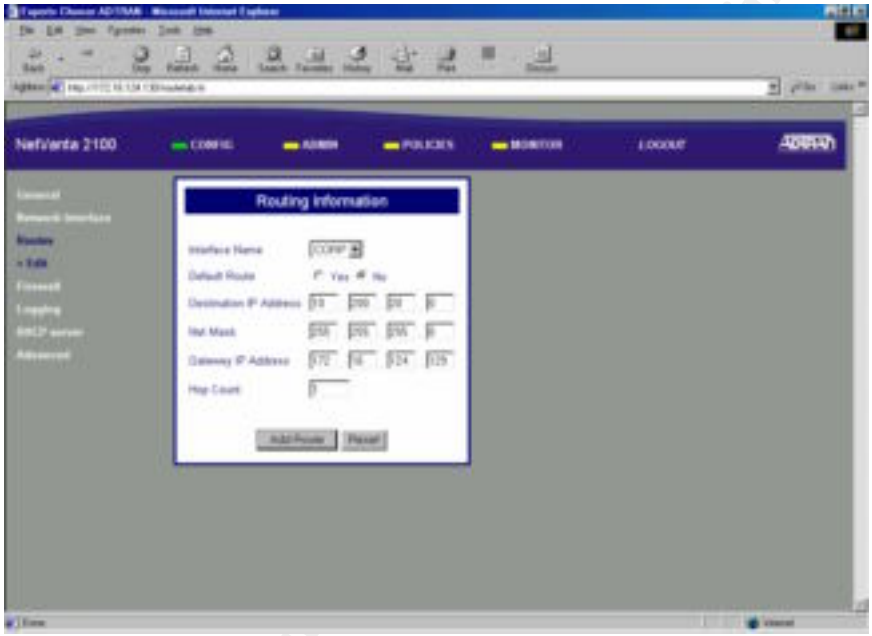


A couple of items worth noting. For a change to take effect, the "Submit" button must be clicked. If the overall configuration is not saved (ADMIN > Save Setting), the running configuration will be lost after the next power up or reboot.
To began the configuring of the NetVanta 2100, start with:

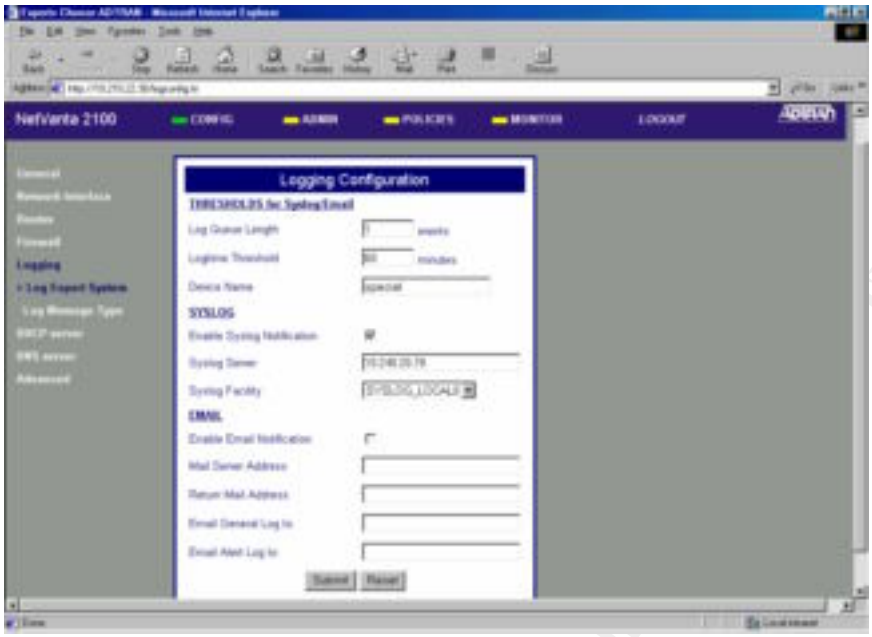
CONFIG > DHCP server > DHCP Server Configuration and disable DHCP because the "Common" server has a static address. Nothing in dmz2 requires DHCP and therefore it's one less service to be concerned with.

CONFIG > Network Interface > RIP config > RIP Configuration for LAN Interface and disable RIP. All routing is done statically.

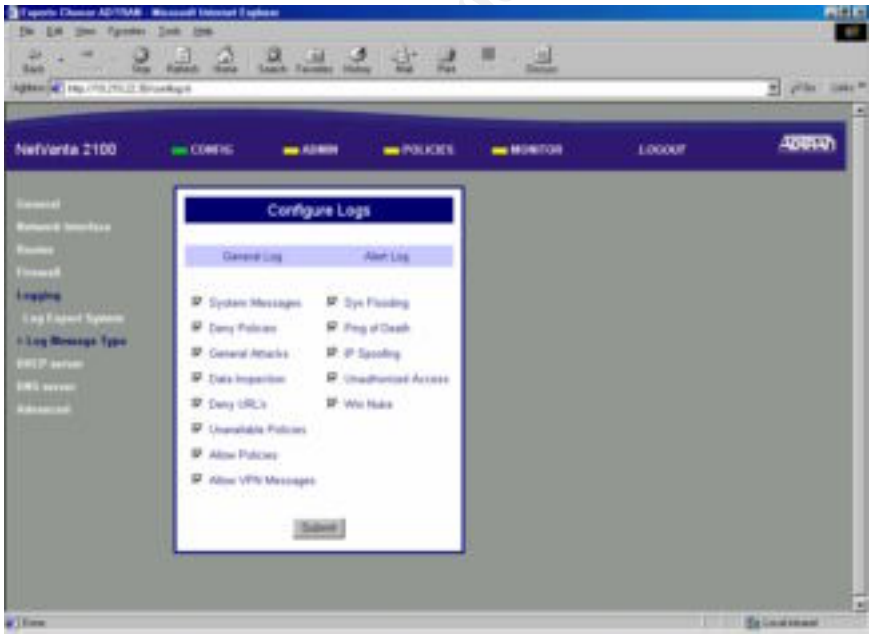
CONFIG > Routes, add a route for the networks 10.200.20.0, 10.240.20.0 and a default route to the Internet. The 10.240.20.0 route is needed for remote management of the VPN device and the 10.200.20.0 route is needed for return connectivity to the database server. The interface name "CORP" refers to the "LAN" interface.



CONFIG > Logging > Log Export System >Logging Configuration, logging is set-up through syslog and is directed at "watch4" with the syslog facility set to "Local0". Email could be used for logging notification but additional firewall holes would be needed and email could end up generating more traffic compared to syslog in GIAC environment. The "Log Queue Length" has been set to 1 event as its threshold with "Logtime Threshold" set to 60 minutes. An event is logged if 1 event happens within a 1-hour time frame. If these values are set too high, it's possible not to log any events.



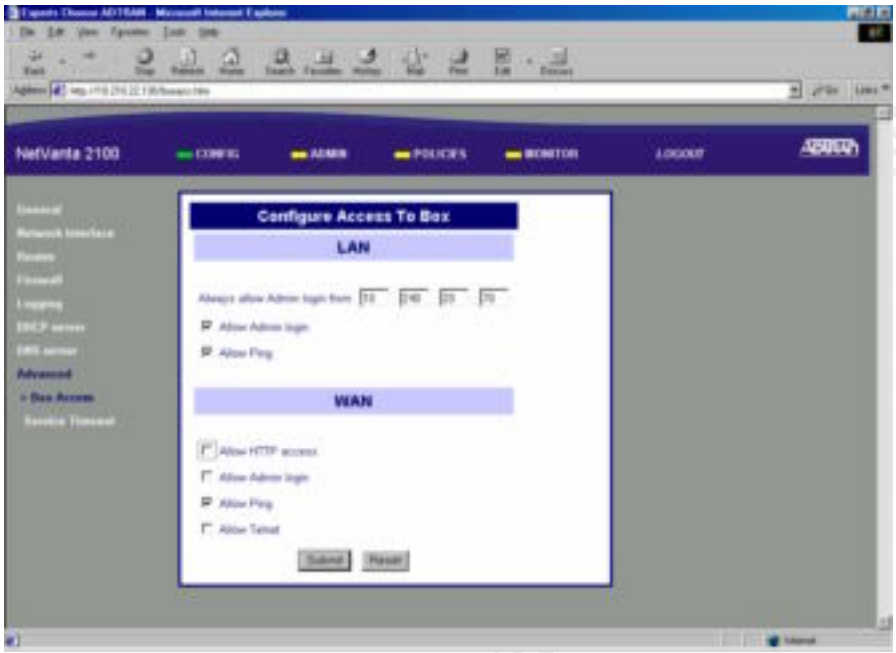
CONFIG > Logging > Log Message Type, all options get checked because GIAC wants to log all events.



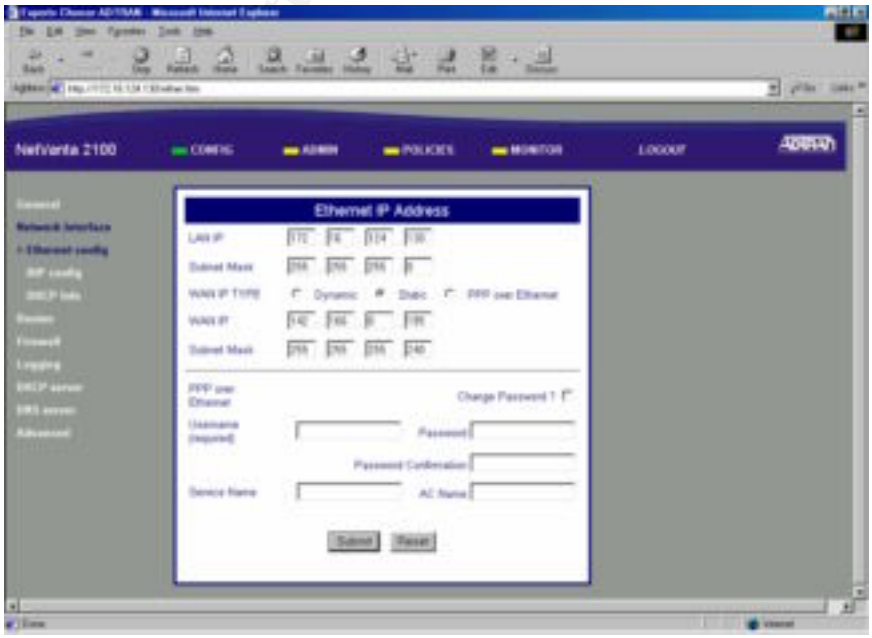
CONFIG > DNS servers, the NetVanta is configured to use the local ISP DNS servers.

CONFIG > Advanced > Box Access, uncheck "Allow HTTP access" and "Allow Admin login" for the "WAN" interface because remote administration through the WAN

interface is not required. The "Always allow Admin login from" is set to the IP address of "topgun".

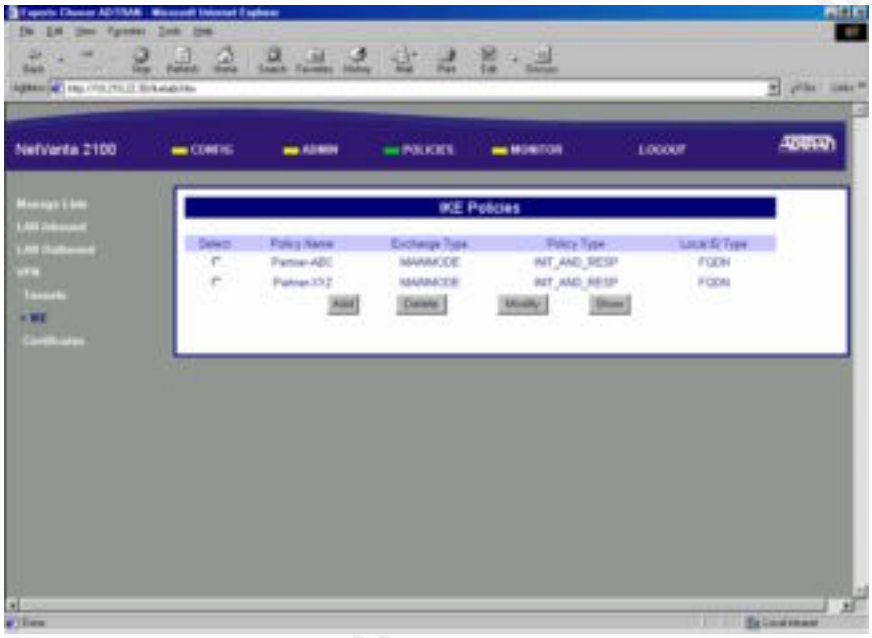


CONFIG > Network Interface > Ethernet config > Ethernet IP Address, configures the "WAN" interface to use a static IP address of 142.166.0.195. The NetVanta does support dynamic IP addressing if the ISP is using DHCP and PPP over Ethernet. For reliability and consistency, GIAC is using a static address since the suppliers and partners will be initiating the connection to GIAC. Change the "LAN" IP address to 172.16.124.130 and "Submit" the changes.

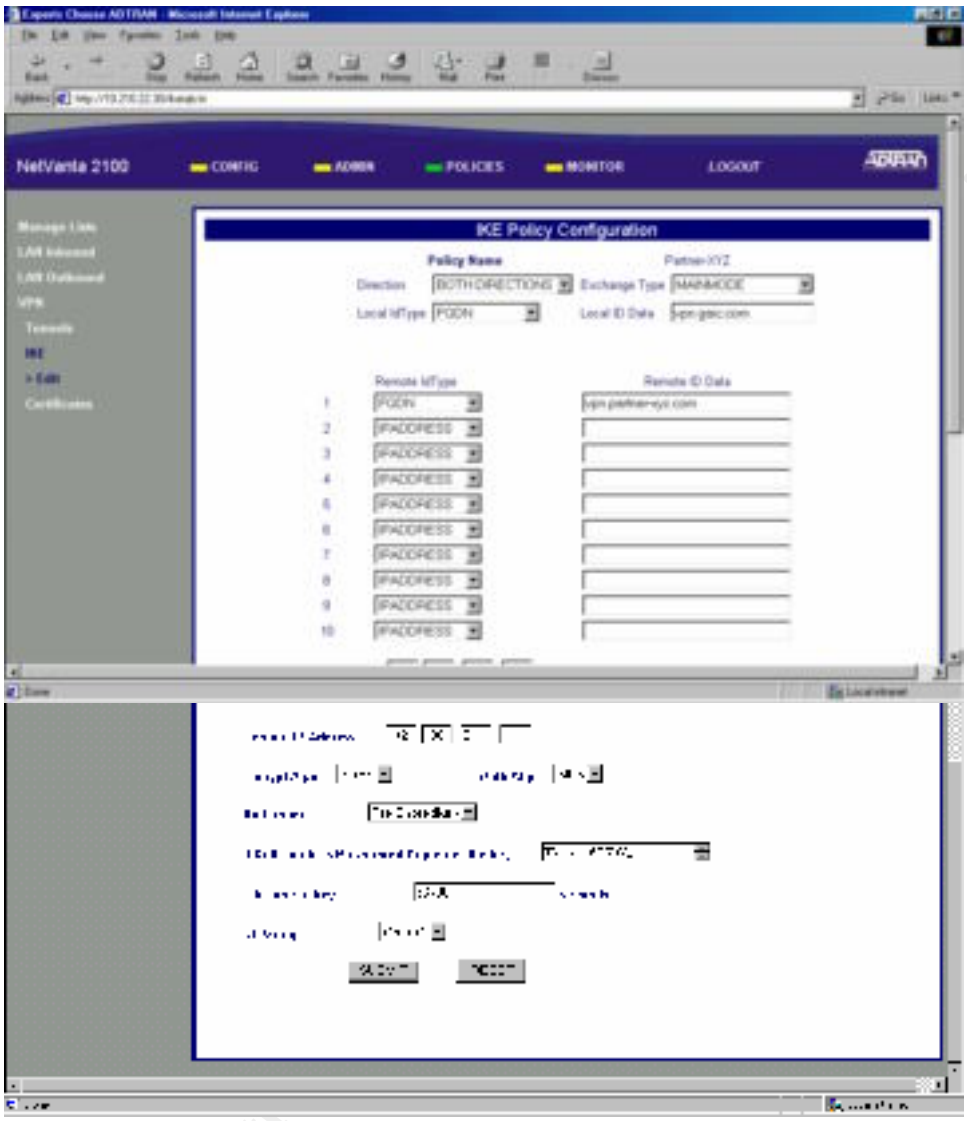


You will lose connectivity to the NetVanta because the new IP addresses are in place. To continue with defining the VPN policies, connect the NetVanta to the actual network. Using the web browser on "topgun", connect to the NetVanta device (http://172.16.124.130).

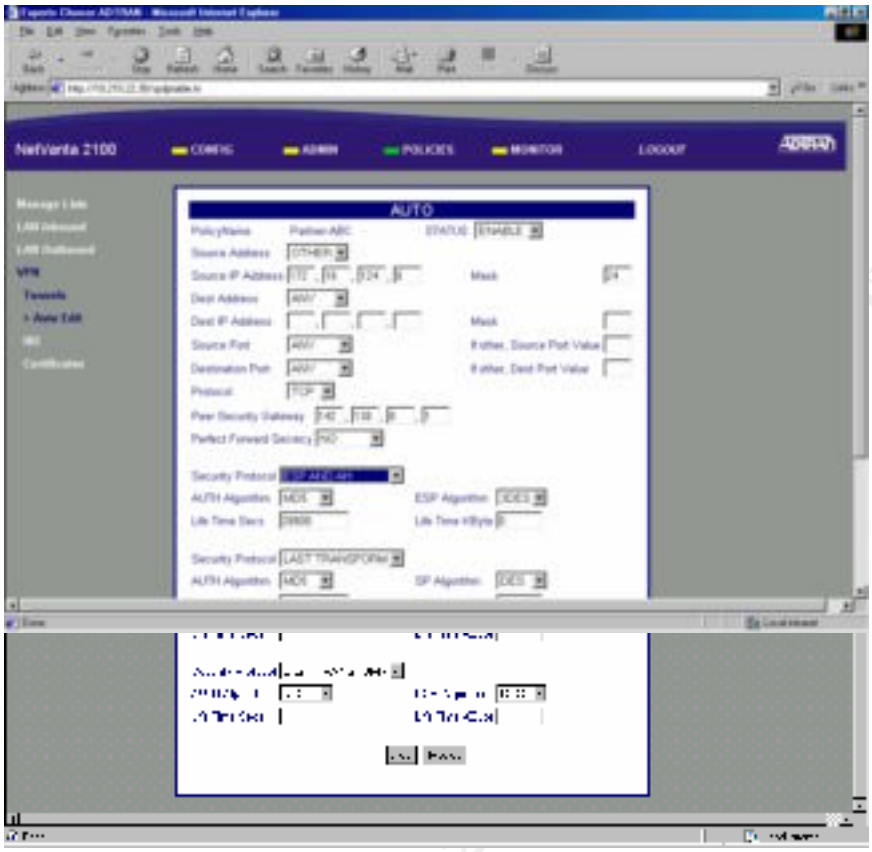
POLICIES > VPN > IKE, configuration of the IKE policies.

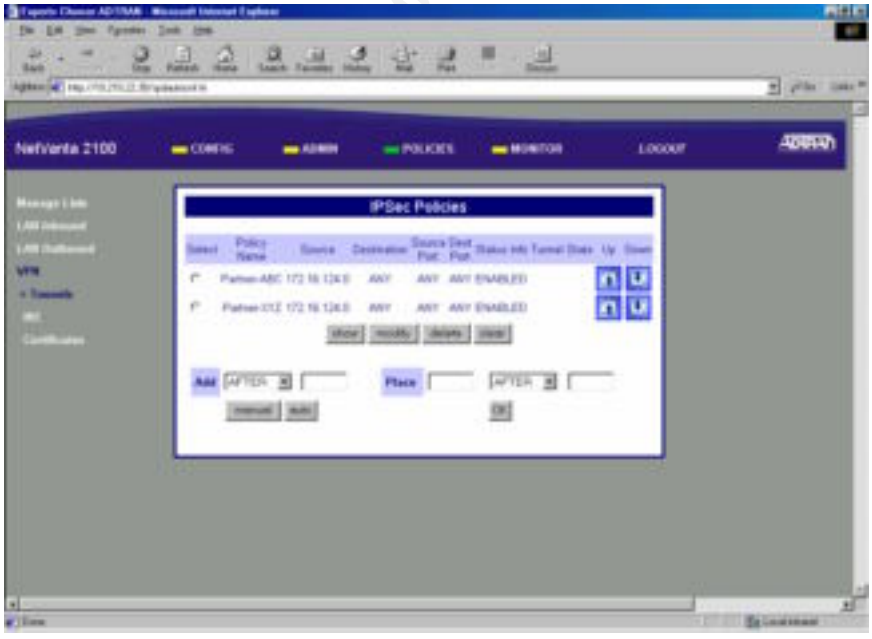


After clicking on "Add", begin creating a policy by defining a policy name. The policy name is an alphanumeric string to identify the policy (i.e. Partner-XYZ). The "Direction" is set to "BOTH DIRECTIONS" so the NetVanta can be a responder or initiator of a VPN connection. The "Exchange Type" is set to "MAINMODE" because both sites are using static addresses. The "Local Id Type" and the "Local ID Data" is in reference to this VPN device using the Fully Qualified Domain Name (FQDN) – vpn.giac.com. The "Remote Id Type" and "Remote ID Data" refers to the remote VPN device, which in this case is vpn.partner-xyz.com and the "Remote IP address" is the external IP address of the remote VPN device. The encryption is 3DES and the authentication algorithm is MD5 using pre-shared keys.

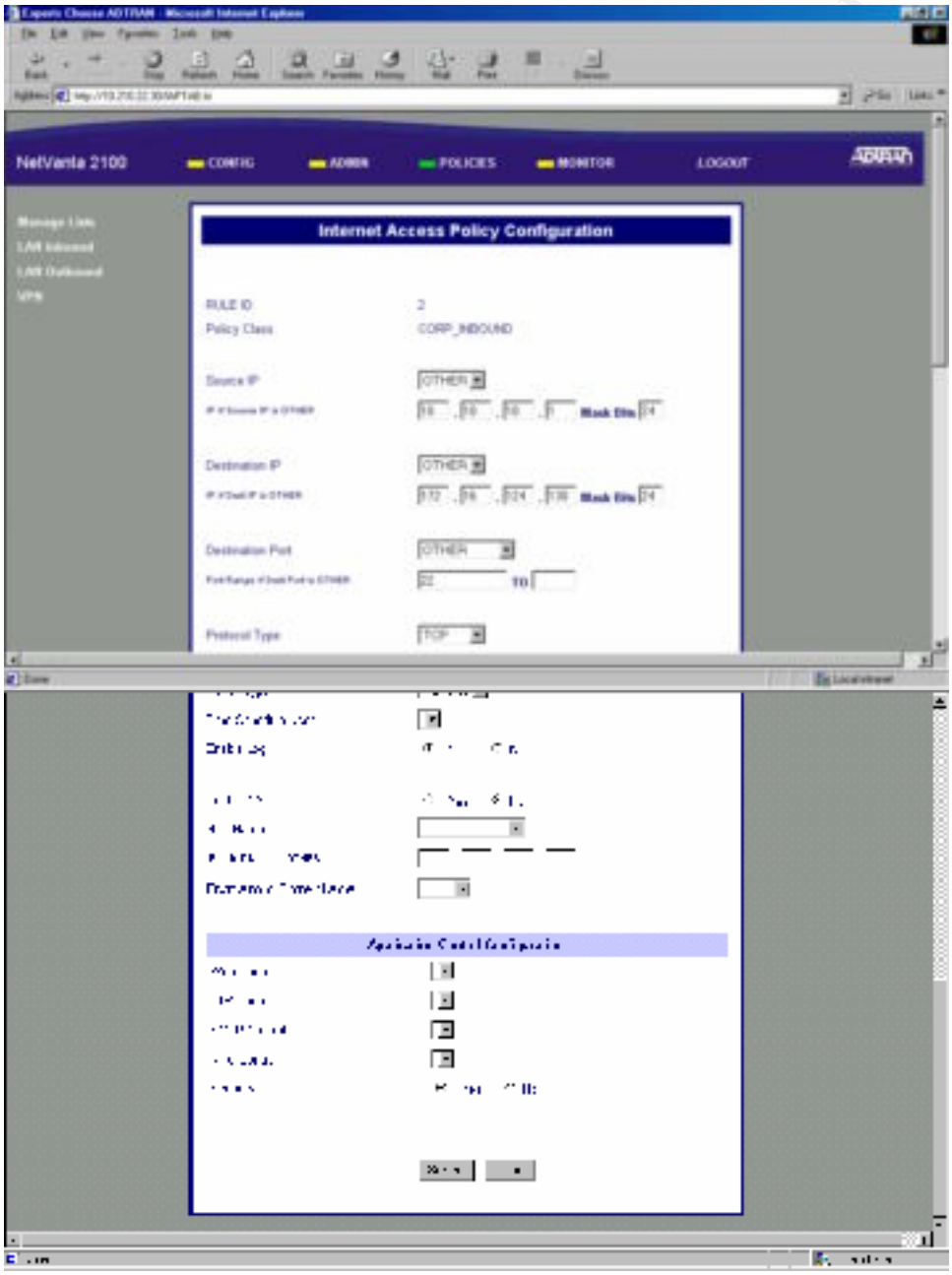


POLICIES > VPN > Tunnels > Auto Edit, to create the IPSEC policy for each remote VPN site. The Policy Name is an alphanumeric string used to identify the policy. The Status must be set to "ENABLE" to configure this as an active policy. With the "Source Address" set to "OTHER", use the local LAN IP address for the "Source IP Address". The "Peer Security Gateway" is the external IP address of the remote VPN device. The security protocol is set to ESP and AH. The auth algorithm is MD5, the encryption algorithm is 3DES and 28800 is the lifetime value of the key. It is recommended that a 3:1 ratio be used between the IKE and IPSec key lifetime values.

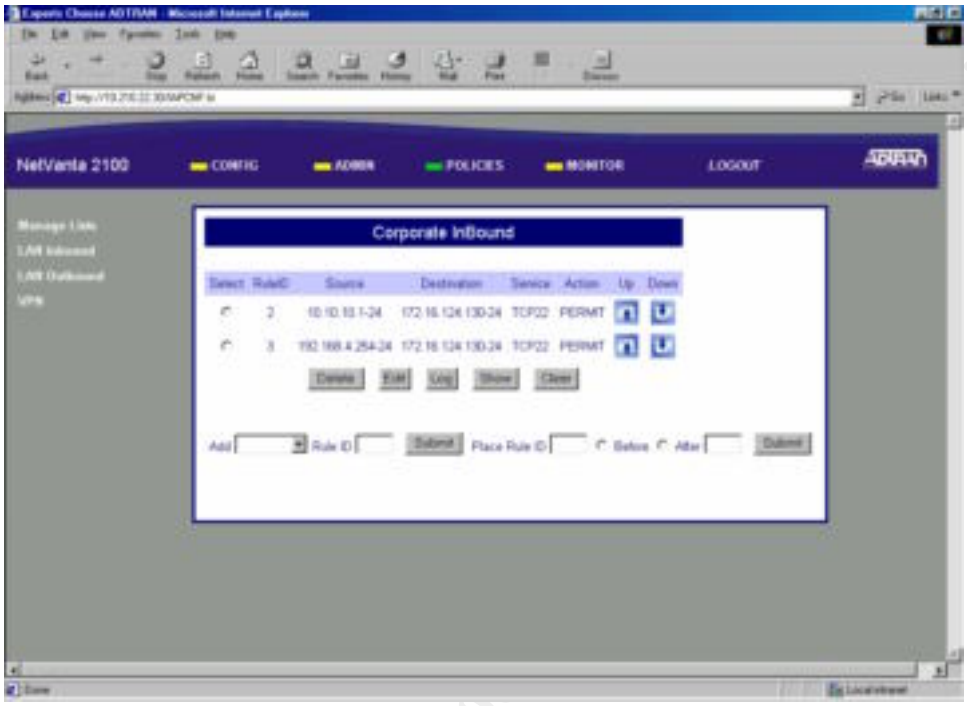


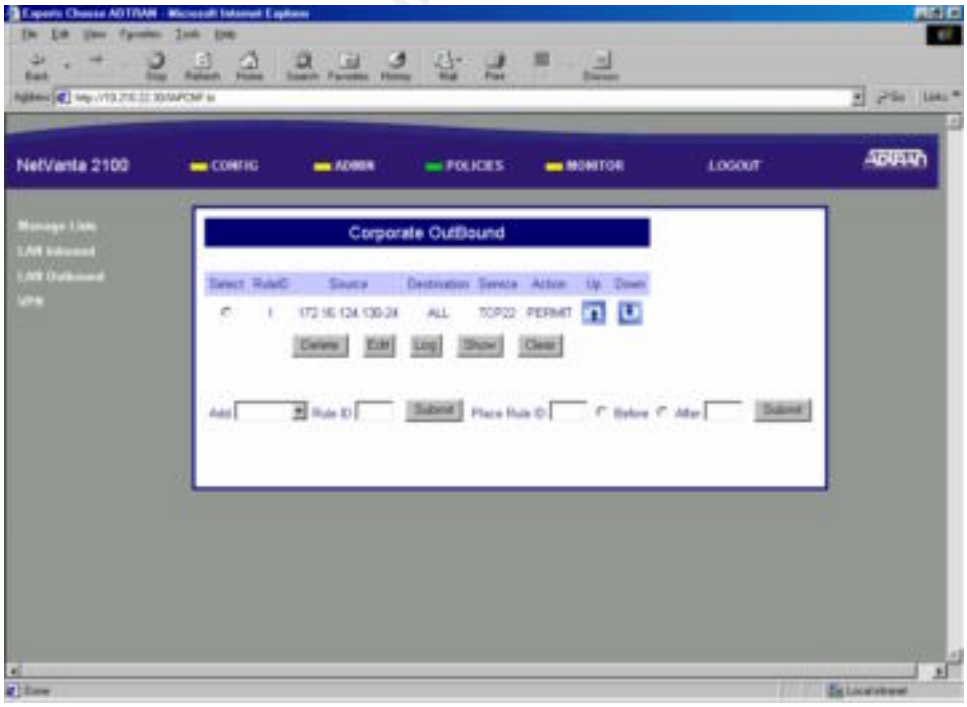


POLICIES > LAN Inbound and ***POLICIES > LAN Outbound*** are for defining rules for connectivity (protocol, port) allowed inbound and outbound from this NetVanta. For the Inbound policy, with "Source IP" set to "OTHER", the "IP if Source IP is OTHER" is the IP address of the internal address of the remote VPN device. GIAC has restricted connectivity to TCP on port 22 (Secure Shell), logging was enabled and NAT was disabled.



A summary of GIAC NetVanta Inbound and Outbound rules.





Configuration of the Internal Firewall

The following pseudo type rules are applied on the internal firewall. Note that these rules are considered as an inbound filter and the legend is as follows:

-i	the interface that the rule is applied too	***-p***	protocol
-s	source address	***-d***	destination address
-log	turns on logging function for that rule	***-dport***	destination port

- eth0 – dmz1 interface (172.16.224.0 / 24 network).

```
permit –i eth0 –p tcp –s 172.16.224.198 –d 10.210.20.20 –dport 25
permit –i eth0 –p tcp –s 172.16.224.101 –d 172.16.224.0/24 –dport 1521
permit –i eth0 –p udp –s 172.16.224.0/24 –d 10.240.20.78 –dport 514
drop –i eth0 –p ip –s 0/0 –d 0/0 –log
```

- eth1 – dmz3 interface (192.168.162.64 / 28 network).

```
permit –i eth1 –p udp –s 192.168.162.70 –d 10.240.20.74 –dport 514
permit –i eth1 –p udp –s 192.168.162.71 –d 10.240.20.74 –dport 514
drop –i eth1 -p ip –s 0/0 –d 0/0 –log
```

- eth2 – dmz2 interface (172.16.124.128 / 28 network).

```
permit –i eth2 –p udp –s 172.16.124.132 –d 10.240.20.78 –dport 514
permit –i eth2 –p udp –s 172.16.124.130 –d 10.240.20.78 –dport 514
permit –i eth2 –p udp –s 172.16.124.132 –d 172.16.224.21 –dport 123
permit –i eth2 –p udp –s 172.16.124.130 –d 10.240.20.78 –dport 123
drop –i eth2 –p ip –s 0/0 –d 0/0 –log
```

- eth3 – considered the internal interface to GIACs network.

```
permit –i eth3 –p tcp –s 10.210.20.5 –d 0/0 –dport 80
permit –i eth3 –p tcp –s 10.210.20.5 –d 0/0 –dport 443
permit –i eth3 –p tcp –s 10.210.20.5 –d 0/0 –dport 21
permit –i eth3 –p tcp –s 10.210.20.20 –d 172.16.224.198 –dport 25
permit –i eth3 –p udp –s 10.210.20.0/24 –d 172.16.224.21 –dport 123
permit –i eth3 –p udp –s 10.200.20.0/24 –d 172.16.224.21 –dport 123
permit –i eth3 –p udp –s 10.240.20.0/24 –d 172.16.224.21 –dport 123
permit –i eth3 –p tcp –s 10.240.20.74 –d 192.168.162.0/0 –dport 22
permit –i eth3 –p tcp –s 10.240.20.78 –d 172.16.124.0/0 –dport 22
permit –i eth3 –p tcp –s 10.240.20.78 –d 172.16.224.0/0 –dport 22
permit –i eth3 –p tcp –s 10.240.20.70 –d 0/0 –dport 22
permit –i eth3 –p tcp –s 10.200.20.0/0 –d 172.16.124.132 –dport 22
drop –i eth3 –p ip –s 0/0 –d 0/0 –log
```

Configuration of the Internal Catalyst Switch

The following are some highlights from the Cisco switch vlan / ACL configurations.

```
interface Vlan150
 description "VLAN 150 - Connection between rifraf and switch"
 ip address 10.150.20.70 255.255.255.0
 ip access-group 150 in

interface Vlan180
 description "VLAN 180 - Connection to Test Network"
 ip address 10.180.20.65 255.255.255.0
 ip access-group 180 out

interface Vlan200
 description "VLAN 200 – Production Database Network"
 ip address 10.200.20.1 255.255.255.0
 ip access-group 100 out

interface Vlan210
 description "VLAN 210 – Internal User Network"
 ip address 10.210.20.1 255.255.255.0
 ip access-group 110 in

interface Vlan240
 description "VLAN 240 – Management Segment"
 ip address 10.240.20.65 255.255.255.0
 ip access-group 140 in
 ip access-group 145 out

access-list 150 permit tcp host 172.16.224.198 host 10.210.20.20 eq 25
access-list 150 permit tcp host 172.16.224.101 host 10.200.20.5 eq 1521
access-list 150 permit udp 172.16.224.0 0.0.0.255 host 10.240.20.78 eq 514
access-list 150 permit udp 172.16.124.0 0.0.0.255 host 10.240.20.78 eq 514
access-list 150 permit udp 192.168.162.0 0.0.0.255 host 10.240.20.74 eq 514
access-list 150 permit udp host 142.166.0.193 host 10.240.20.78 eq 514
access-list 150 permit udp host 172.16.224.244 host 10.240.20.78 eq 514
access-list 150 permit tcp host 142.166.0.193 host 10.240.20.70 eq 69
access-list 150 deny any any
!
access-list 180 permit tcp 10.210.20.0 0.0.0.255 any
access-list 180 permit tcp host 10.200.20.6 any eq 22
access-list 180 deny any any
!
access-list 100 permit tcp host 172.16.224.101 host 10.200.20.5 eq 1521
access-list 100 permit tcp 10.210.20.0 0.0.0.255 any eq 1521 1526
access-list 100 permit tcp 10.210.20.64 0.0.0.7 any eq 22
access-list 100 permit tcp host 172.16.124.132 host 10.200.20.6 eq 22
access-list 100 deny any any
!
```

```
access-list 110 permit tcp host 10.210.20.5 host 172.16.224.21 eq 123
access-list 110 permit udp host 10.210.20.20 host 172.16.224.21 eq 123
access-list 110 permit udp host 10.210.20.35 host 172.16.224.21 eq 123
access-list 110 permit tcp host 10.210.20.5 any eq 80
access-list 110 permit tcp host 10.210.20.5 any eq 443
access-list 110 permit tcp host 10.210.20.5 any eq 21
access-list 110 permit udp host 10.210.20.5 host 172.16.224.53 eq 53
access-list 110 permit tcp host 10.210.20.5 host 172.16.224.53 eq 53
access-list 110 permit tcp host 10.210.20.20 host 172.16.224.198 eq 25
access-list 110 permit tcp 10.210.20.64 0.0.0.7 any eq 22
access-list 110 permit tcp 10.210.20.0 0.0.0.255 any eq 1521 1526
access-list 110 deny any any
!
access-list 140 permit tcp host 10.240.20.70 172.16.224.0 0.0.0.255 eq 22
access-list 140 permit tcp host 10.240.20.70 172.16.124.0 0.0.0.255 eq 22
access-list 140 permit tcp host 10.240.20.70 host 142.166.0.193 eq 23
access-list 140 permit tcp host 10.240.20.70 host 172.16.224.244 eq 443
access-list 140 permit tcp host 10.240.20.70 host 172.16.124.130 eq 80
access-list 140 permit tcp host 10.240.20.70 host 142.166.0.193 eq 69
access-list 140 permit tcp host 10.240.20.70 host 172.16.224.244 eq 69
access-list 140 deny any any
access-list 145 permit udp 172.16.224.0 0.0.0.255 host 10.240.20.74 eq 514
access-list 145 permit udp 172.16.124.0 0.0.0.255 host 10.240.20.74 eq 514
access-list 145 permit udp 192.168.162.0 0.0.0.255 host 10.240.20.78 eq 514
access-list 145 deny any any
```

Assignment 3 – Audit for Security Architecture

Audit Plan

An effective security strategy is a combination of the security architecture and design, as well as the evolving standards and procedures in preparation of an intrusion and/or a disaster. Understanding both combination will provide for an effective firewall solution.

1) *General Information*.
   After the scope of the audit has been defined, request any high-level documentation, network diagrams, flowcharts and procedures followed by GIAC. Reviewing this information should provide a baseline for establishing normal activity.

2) *Scanning*.
   Scanning from multiple access points would provide verification of the baseline and identify any other possible concerns. For the primary firewall, this would mean scanning from all directly connected network segments which in this case is the inside (dmz1) and outside interface. Since the primary firewall isn't the only potential access point into the GIAC network, scanning the VPN device should be included in the evaluation.

3) Interviews.
   Interview a number of employees of GIAC to understand their responsibilities, procedures and processes in doing their job. This would include helpdesk support, firewall administrator, developers, team leaders and IT managers.

   General questions asked to all interviewees:
   - Describe your role?
   - Are you aware of any security policies?
   - Are you aware of any change control processes for making changes?
   - Are you aware of any standards?
   - What type of background do you have? What type of training?
   - What would you like see changed?
   - Any known issues?

   More detailed questions are asked to individuals based upon their role. For example, questions about backup procedure, monitoring/alerting, system access, password policies, logging abilities, etc, would be for a firewall administrator.

4) *System Review*.
   Complete a detailed review of each system configuration. For both the primary firewall and the VPN device, this would include reviewing the system OS and firmware version, current configuration, reviewing security bulletins for any known issues with the devices or configuration of, and verifying scan results.

5) *Draft Report*.
   The draft report is based on all the information collected by documentation, scanning and interview processes. A discussion with the system owner(s) on the draft report gives them an opportunity to clarify or answer any questions before the final report.

6) *Final Report*.
   Present the final report with any observations and recommendations to GIAC. This would include suggestions for documentation, policies and processes, and general security awareness.

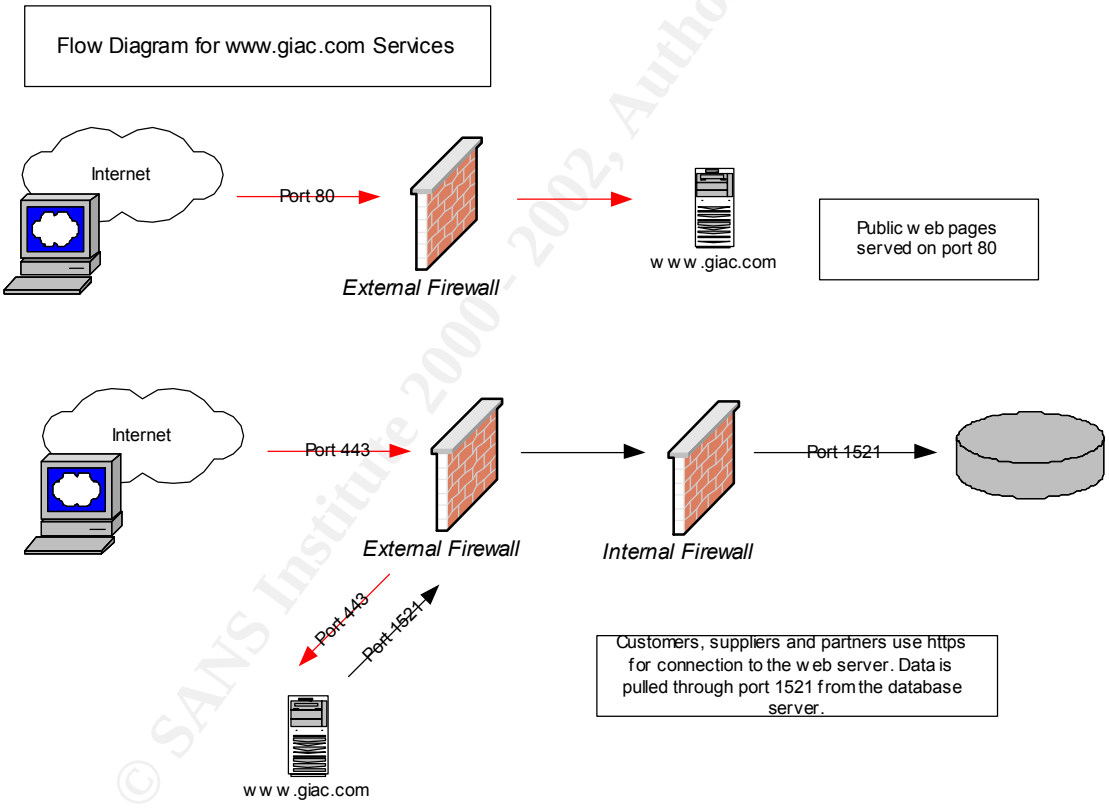
Estimated Cost for the Security Audit

	Estimated Hours	Estimated Cost
Planning and Defining Scope	.5 days	$500.00
Collection/Review of High Level Documentation	.5 days	$500.00
Technical Assessment (Scans)	.5 days	$500.00
Interview Process	1 days	$1000.00
Technical Assessment (System Reviews)	1 days	$1000.00
Draft Report and Discussion	2 day	$2000.00
Presentation of Final Report	.5 days	$500.00
Total	***6 days***	***$6,000.00***

Conduct the Audit

1) *General Information*.
   - ✓ The network diagram is documented (assignment #1).
   - ✓ The external firewall rule set is documented (assignment #2).
   - ✓ VPN policies (assignment #2).
   - ✓ Documented policies are place for:
     a. Basic server installation and configuration.
     b. Security policies
     c. Daily tasks based on roles and responsibilities.
     d. Escalation procedures.
     e. General flow diagrams (Appendix F for all diagrams)

GIAC Logical Flow Diagrams



2) *Scanning*.

To verify the system and network configuration, scans were done using a freeware tool nmap (http://www.insecure.org/nmap). The scanning schedule was coordinated with GIAC management to be performed at various times through out the day to test the logging and alerting processes with system administrators. The risk and impact of scanning with normal network traffic was waived to get a true evaluation of the network infrastructure under realistic conditions. The following targets were selected for scanning:

142.177.24.178	border router
142.166.0.194	outside the PIX firewall
142.166.0.195	outside the NetVanta VPN device

A brief description of a few nmap options used:

-sT TCP SYN scan, completes a full TCP connection.
-sS TCP stealth scan (or "half-open" scan), doesn't open a full TCP connection.
-sU UDP port scan
-P0 Don't ping host
-p for specifying a port range
-sF Stealth FIN scan, sends FIN flag set.
-sX Xmas Tree scan, sends FIN, URG, PUSH flag set.
-sN Null scan, no flags set in packet
-sA ACK scan, sends ACK flag set
-oN *filename* log output to a file.

3) *Interviews*.

Interviews were conducted with several employees from GIAC Enterprises. This included the two firewall / system administrators, the database administrator, the owner / manager and several general users. All employees seem to have a good understanding of:

- Their role and responsibilities.
- General security practices and policies for GIAC.
  - The change management process.
  - Standards and business practices within GIAC.

Being a small company, training is either provided through self-study with CBTs or through on the job training. A few people indicated that they would prefer instructor base training.

4) *System Reviews*.

Systems were reviewed against the documentation supplied on the configuration and setup. This review confirmed that the documented system configuration is accurate.

5) Draft Report

A draft report was compiled to summarize the findings in this audit. As agreed in the scope, this draft report was reviewed by the owner / manager of GIAC Enterprises.

Evaluate the Audit

1) *General Information.*

Physical security is a vital part of any critical environment. As part of the general information process, a physical security audit was conducted to verify:

- Server room doors were locked,
- Server cabinet was locked,
- Servers were on a UPS power source,
- Backup media wasn't in public view and was secured,
- Access codes were locked up.

2) Scanning.

A few of the scanning results were as follows:

A few scan results of the border router's external interface:

[root@localhost /root]# ***nmap 142.177.24.178***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0

[root@localhost /root]# ***nmap -sS -P0 -p 1-1024 142.177.24.178***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
All 1024 scanned ports on (142.177.24.178) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1270 seconds

Direct connections to the border router are being dropped as defined by class-list ACL. Scan targeted for GIAC public network where able to pass through the router as defined in "access-list 101".

A few scan results of the VPN's external interface:

[root@localhost /root]# ***nmap –sA -v 142.166.0.195***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Host (142.166.0.195) appears to be up ... good.
Initiating ACK Scan against (142.166.0.195)
The ACK Scan took 166 seconds to scan 1549 ports.
Interesting ports on (142.166.0.195):
(The 1547 ports scanned but not shown below are in state: filtered)

Port	State	Service
23/tcp	UNfiltered	telnet
80/tcp	UNfiltered	http

Nmap run completed – 1 IP address (1 host up) scanned in 166 seconds
[root@localhost /root]# ***nmap 142.166.0.195***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
All 1549 scanned ports on (142.166.0.195) are: closed

Nmap run completed – 1 IP address (1 host up) scanned in 1 second.

The general UDP and TCP scans showed that all ports scanned on the NetVanta were closed. The ACK scan turned up two services, telnet and http. To verify that, the telnet port was filtered:

[root@localhost /root]# ***telnet 142.166.0.195***
Trying 142.166.0.195…
telnet: Unable to connect to remote host: Connection refused
[root@localhost /root]#

A few scan results of the PIX and systems protected by it:

[root@localhost /root]# ***nmap -sT -v -P0 -p 1-1024 142.166.0.194***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Host (142.166.0.194) appears to be up ... good.
Initiating Connect() Scan against (142.166.0.194)
The Connect() Scan took 823 seconds to scan 1024 ports.
All 1024 scanned ports on (142.166.0.194) are: filtered

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 823 seconds

[root@localhost /root]# ***nmap -sX -p 1-1024 142.166.0.200-203***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
All 512 scanned ports on (142.166.0.200) are: closed
All 512 scanned ports on (142.166.0.201) are: closed
All 512 scanned ports on (142.166.0.202) are: closed
All 512 scanned ports on (142.166.0.203) are: closed

Nmap run completed -- 4 IP addresses (4 hosts up) scanned in 73 seconds

[root@localhost /root]# ***nmap -sS -v 142.166.0.194-204***

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Host (142.166.0.194) appears to be up ... good.
Initiating SYN Stealth Scan against (142.166.0.194)
The SYN Stealth Scan took 130 seconds to scan 1549 ports.
All 1549 scanned ports on (142.166.0.194) are: filtered
Host (142.166.0195) appears to be up ... good.
Initiating SYN Stealth Scan against (142.166.0.195)
The SYN Stealth Scan took 0 seconds to scan 1549 ports.
All 1549 scanned ports on (142.166.0.195) are: closed

```
Host  (142.166.0.196) appears to be down, skipping it.
…

Host  (142.166.0.200) appears to be up ... good.
Initiating SYN Stealth Scan against  (142.166.0.200)
Adding open port 80/tcp
Adding open port 443/tcp
The SYN Stealth Scan took 7 seconds to scan 1549 ports.
Interesting ports on  (142.166.0.200):
(The 1547 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open         http
443/tcp    open        https
…
```

The scan results from the PIX were as expected.

3) Interviews.

Highlights from the interview process:

- All GIAC employees interviewed understood the security polices / practices in place.
- Roles and responsibilities were well defined and documented.
- Physical security was in place.
- Logical security was documented.
- Concerns were raised that redundancy is required.

4) System Review.

During the system reviews, questions were raised about:

- Review if the border router should include in its ACL, "deny" any IP addresses known for generating attacks.
- Review if the border router should include in its ACL, "deny" any IP addresses that haven't been assigned to anyone.
- Review if the NetVanta needs ICMP enabled on the external (WAN) interface?
- Review if the PIX needs ICMP enabled on the external interface (142.166.0.194)?
- Review if the PIX needs syslog level set for "debugging"?
- Review the IDS configuration for the PIX?
- Review PIX options like "DNS Guard", "Frag Guard" and other "sysopt" commands.

5) Final Report.

Over all, GIAC has demonstrated a balance between the business requirements vs. the security requirements as identified within this audit scope. Documentation, network diagrams, flow charts and system configurations are kept up to date. The interviews, network scans and system reviews did not reveal anything that was unexpected. A few comments from the assessment summary:

Assessment: Documentation of Change Management Process.
Risk: Low
Recommended Action: Create a formal "Change Management Process" to address all changes being applied to the border router, NetVanta and the PIX firewall. This process should be expanded to include changes to the other network components (i.e. internal firewall, switch, etc.) and GIAC servers.

Assessment: Regular Audits
Risk: Low
Recommended Action: Conduct regular audits and scan for vulnerabilities and unexplained open ports. This should be done from all segments inside and outside the GIAC network. This should include not only network components but also servers themselves.

Assessment: Firewall / System Logs
Risk: Low
Recommended Action: Separate the PIX and the border router syslog messages from other server system syslog messages by directing them to separate files on "topgun". This would allow for an easier visual view when doing quick scans through the file. More automation could be done in reviewing the log files.

Assignment 4 – Design Under Fire

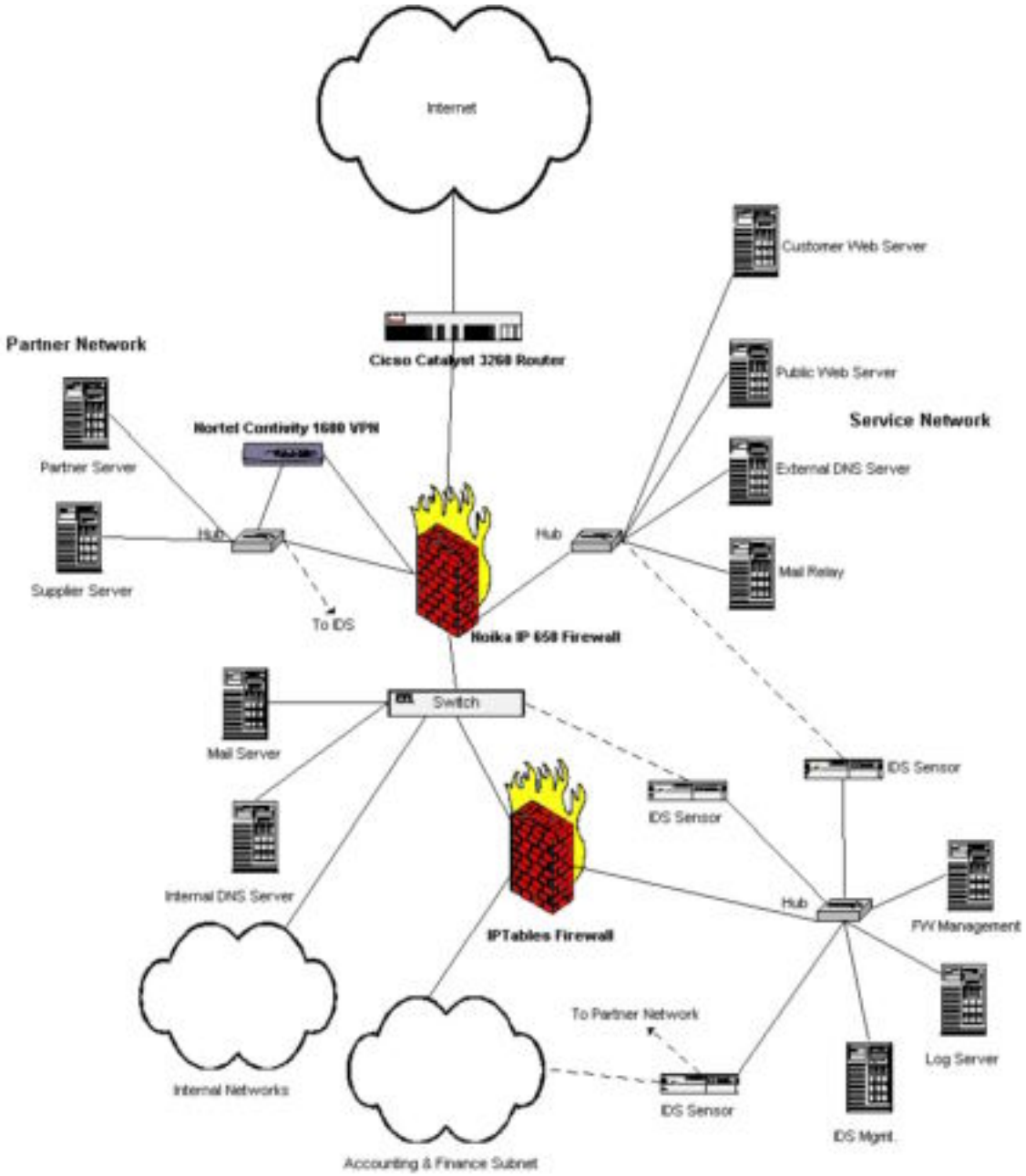


Figure 3-1

For my "Design Under Fire", I have chosen Kenneth Swingle design from

http://www.giac.org/practical/Kenneth_Swingle_GCFW.zip .

Research Vulnerabilities

In order to stage a successful attack on a target, vulnerabilities for the target device need to be identified. A few good sources of current information include:

- http://www.securityfocus.com/
- http://www.securiteam.com/
- http://www.incidents.org/
- http://www.cert.org/
- http://cve.mitre.org/

Some sites for hacking and vulnerability tools:

- http://hackpalace.com/
- http://www.nessus.org/
- http://www.sans.org/
- http://www.securiteam.org/

Attack of an Internal System

I've decided to attack the "Public Web Server" within Kenneth's GIAC network. Using the Internet with a few common tools, a general reconnaissance of the GIAC network was done.

First an nslookup was done to determine the IP address or addresses of the web server(s):

nslookup for www.giac.com

Server: opal.nbnet.nb.ca
Address: 198.164.30.2

Non-authoritative answer:
Name: www.giac.com
Address: 188.1.1.10

With the IP address from the nslookup and using http://www.arin.net, a whois was done on the IP address. The results were:

GIAC Enterprises (NET-GIAC)
123 ABC Lane, PO Box 6000
Moncton, NS J3B 6H7
CA

Netname: GIAC
Netblock: 188.1.1.0 – 188.1.1.255
Coordinator:
Swingle, Kenneth (DI22-ARIN) Kenneth.Swingle@GIAC.COM
1 902 454 5322 (FAX) 1 902 454 5352
Domain System inverse mapping provided by:
MARS.CSD.UNB.CA 131.202.1.3
DNS1.GOV.NS.CA 198.166.215.2
Record last updated on 14-May-2001.
Database last updated on 2-Apr-2002 19:58:26 EDT.

Using a workstation connected to the Internet, a telnet was done to the public IP address of the web server to determine what web service was running.

```
[root@localhost root]$ telnet 188.1.1.10 80
Trying 188.1.1.10...
Connected to 188.1.1.10.
Escape character is '^]'.
GET / HTTP/1.0        <return>
                      <return>
```

The first few lines of results

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Wed, 03 Apr 2002 17:43:04 GMT
Connection: Keep-Alive
Content-Length: 1270
Content-Type: text/html
…
```

I now know the "Public Web Server" has an IP address of 188.1.1.10 and is running Microsoft's Internet Information Server (IIS) version 4.0. We also know that IIS runs on a Windows platform that could also possibly be used in an attack. To review for Microsoft vulnerabilities:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security

One example of IIS vulnerabilities is from August 15/2001:

Microsoft Security Bulletin MS01-044[1]

[1] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Technical description:

This patch is a cumulative patch that includes the functionality of all security patches released to date for IIS 5.0, and all patches released for IIS 4.0 since Windows NT® 4.0 Service Pack 5. A complete listing of the patches superseded by this patch is provided below, in the section titled "Additional information about this patch". Before applying the patch, system administrators should take note of the caveats discussed in the same section.

In addition to including all previously released security patches, this patch also includes fixes for five newly discovered security vulnerabilities affecting IIS 4.0 and 5.0:

- A denial of service vulnerability that could enable an attacker to cause the IIS 4.0 service to fail, if URL redirection has been enabled. The "Code Red" worm generates traffic that can in some cases exploit this vulnerability, with the result that an IIS 4.0 machine that wasn't susceptible to infection via the worm could nevertheless have its service disrupted by the worm.
- A denial of service vulnerability that could enable an attacker to temporarily disrupt service on an IIS 5.0 web server. WebDAV doesn't correctly handle particular type of very long, invalid request. Such a request would cause the IIS 5.0 service to fail; by default, it would automatically restart.
- A denial of service vulnerability involving the way IIS 5.0 interprets content containing a particular type of invalid MIME header. If an attacker placed content containing such a defect onto a server and then requested it, the IIS 5.0 service would be unable to serve any content until a spurious entry was removed from the File Type table for the site.
- A buffer overrun vulnerability involving the code that performs server-side include (SSI) directives. An attacker who had the ability to place content onto a server could include a malformed SSI directive that, when the content was processed, would result in code of the attacker's choice running in Local System context.
- A privilege elevation vulnerability that results because of a flaw in a table that IIS 5.0 consults when determining whether a process should in-process or out-of-process. IIS 5.0 contains a table that lists the system files that should always run in-process. However, the list provides the files using relative as well as absolute addressing, with the result that any file whose name matched that of a file on the list would run in-process.

In addition, this patch eliminates a side effect of the previous IIS cumulative patch (discussed in the Caveats section of Microsoft Security Bulletin MS01-026) by restoring proper functioning of UPN-style logons via FTP and W3SVC.

Mitigating factors:
URL Redirection denial of service:

- This vulnerability only affects IIS 4.0. IIS 5.0 is not affected.
- The vulnerability only occurs if URL redirection is enabled.
- The vulnerability does not provide any capability to compromise data on the server or gain administrative control over it.

WebDAV request denial of service:

- The vulnerability only affects IIS 5.0. IIS 4.0 is not affected.
- The effect of an attack via this vulnerability would be temporary. The server would automatically resume normal service as soon as the malformed requests stopped arriving.
- The vulnerability does not provide an attacker with any capability to carry out WebDAV requests.
- The vulnerability does not provide any capability to compromise data on the server or gain administrative control over it.

MIME header denial of service:

- The vulnerability only affects IIS 5.0. IIS 4.0 is not affected.
- In order to exploit this vulnerability, the attacker would need to have the ability to install content on the server. However, by default, unprivileged users do not have this capability, and best practices strongly recommend against granting it to untrusted users.

SSI privilege elevation vulnerability:

- In order to exploit this vulnerability, the attacker would need to have the ability to install content on the server. However, by default, unprivileged users do not have this capability, and best practices strongly recommend against granting it to untrusted users.

System file listing privilege elevation vulnerability:

- The vulnerability only affects IIS 5.0. IIS 4.0 is not affected.
- In order to exploit this vulnerability, the attacker would need to have the ability to install content on the server. However, by default, unprivileged users do not have this capability, and best practices strongly recommend against granting it to untrusted users.

Vulnerability identifiers:

- URL redirection denial of service: CAN-2001-0545
- WebDAV denial of service: CAN-2001-0508
- MIME header denial of service: CAN-2001-0544
- SSI privilege elevation: CAN-2001-0506
- System file listing privilege elevation: CAN-2001-0507

Up to this point, all the information gathering has been unannounced to the GIAC administrators. The next step is to launch an attack using the "nimda" worm to utilize this vulnerability on an unpatched system.

The following is a sample of the commands passed in the "nimda" worm as it attacks the web service.

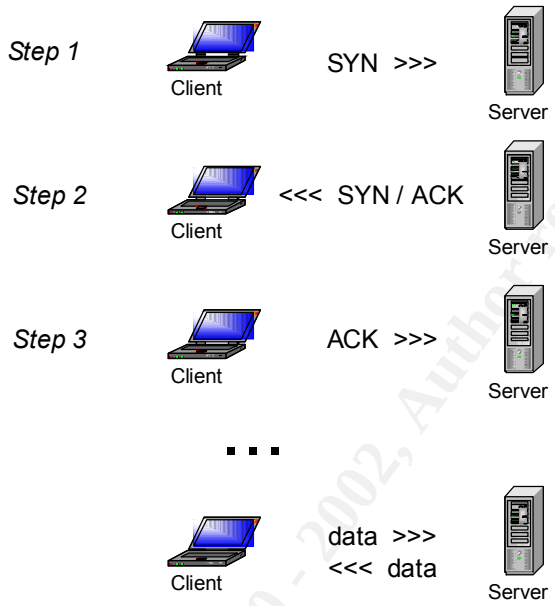
```
188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0"
404 292 0 "-" "-"
188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0"
404 292 0 "-" "-"
188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET
/scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 306 0 "-" "-"

…

188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET
/scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 289 0 "-" "-"
188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET
/scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 289 0 "-" "-"
188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 306 0 "-" "-"
188.1.1.10 - - [18/Sep/2001:10:52:03 -0300] "GET
/scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 306 0 "-" "-"
```

To reduce the risk of attacks like this, a number of steps should be taken:

- Ensure that the OS has been properly hardened.
- Ensure that the application (IIS) has been secured.
- Stay current with vendor patching / hot fixes for both the OS and application software.
- Follow news groups, mailing lists, security and hacker web sites on new vulnerabilities and fixes.
- Ban any IP address that is known for attacks with your border router.
- If the firewall is capable, inspect the content for known attack signatures and drop them.

Denial of Service Attack

For a Denial of Service Attack, I would utilize the 50 compromised systems using a TCP SYN flood against the "Public Web Server". Below is what a normal TCP connection would look like:



The first step is for the client to initiate a connection by sending a "SYN" to the server. In the second step, the server would acknowledge the client's "SYN" with an "ACK" and send its own "SYN" to the client. The final step of the three-way handshake is the client acknowledging the servers "SYN" with an "ACK". Normal data flow could now begin.

During a TCP SYN flood, each compromised client host would send multiple SYN packets to the target host. The server would send a "SYN / ACK" back for every "SYN" it received as part of the three-way handshake. To keep track of all its sessions, the server would allocate system resources and wait for the return "ACK" packet. The compromised client hosts would never send an "ACK" packet back to complete the three-way handshake. With enough of these half established sessions, the resources on the target host would be exhausted and would not have any resources left for legitimate users to access the target device.

In Kenneth's practical, I'm assuming a default install since no properties of the firewall were supplied. SYNDefender is a proprietary Firewall-1 feature that protects against denial of service. Check Point's SYNDefender intercepts the three-way handshake and replies on behalf of the internal host. The connection isn't handed to the internal host

until the handshake is completed. In a default installation of Check Point, SYNDefender is not deployed. Timeout values (how long SYNDefender waits for an acknowledgement before dropping the connection) and maximum sessions (the number of internal connections maintained by SYNDefender) could be set to help control SYN floods with SYNDefender.

Another option in the event of a SYN flood, the border router could be used to regain some internal functionality. Once the attacker's IP address has been identified, connect to the console port of the router and add an "ACL" rule to deny the attacker's IP address. By dropping the packets at the border router, the firewall and target host no longer are being directly attacked. Even though the Internet usage has been cut off by the denial of service attack, GIAC still has connectivity between their partners and "Service Network" with their internal network. The attacker's IP address should be forwarded to their ISP with a complaint about the activity and GIAC system admin should record the IP address in a list for "IP's to watch for in reviewing logs".

Appendix A

GIAC Security Policy.

Outbound Internet Policy

- The proxy server is restricted to port 80 and 443 for Internet access.
- The proxy server is restricted to port 21 for passive ftp access to the Internet.
- Only GIAC external DNS server can do domain name resolution with ISP DNS servers on both UDP and TCP port 53.
- Only GIAC NTP server can do time synchronization with 4 external NTP servers on UDP port 123.
- Only GIAC external STMP mail server can send SMTP message with Internet on TCP port 25.

Inbound Internet Policy

- Only http://www.giac.com will accept incoming http/https traffic on TCP port 80 and 443.
- Only GIAC external STMP mail server will accept external SMTP connections on TCP port 25.
- Only IPSec traffic going to the NetVanta VPN device will be accepted.
- The external DNS server will accept only UDP and TCP port 53.
- Only establish connections from the proxy server will be accepted back through.

DMZ1 Policy

- Only the internal exchange server can communicate with the WebShield server on TCP port 25.
- Only the GIAC external mail server can connect to webshield on TCP port 25.
- All network components and system servers can do time synchronization with GIAC NTP server on UDP port 123.
- Only the proxy server can do DNS requests against GIAC external DNS servers.
- Only a couple of internal workstation can access WebShield on TCP port 21 for Virus definition updates.
- Several internal workstations have access to systems (www, ntp1, dns1,mail1) in DMZ1 on TCP port 22 for administrations.
- Only GIAC management station can access external firewall on TCP port 22 for remote administration.
- Only GIAC management station can access internal firewall on TCP port 22 for remote administration.
- Only www can access the primary database server on TCP port 1521 for database queries.

DMZ2 Policy

- Several internal workstations can access systems (ftp server) in DMZ2 on TCP port 22 for system administration.
- Only GIAC management station can access VPN device on TCP 443 for remote administration.
- Only the secondary database server can access Secure FTP server on TCP port 22.

Policies for Catalyst 2948

- Only GIAC management station can access switch on TCP port 23 for remote administration.
- Internal users can access database servers on TCP ports 22, 1521.
- Only a couple of internal workstations can access GIAC management server and Syslog servers on TCP port 22.
- Only www can access the primary database server on TCP port 1521 for database queries.
- Only the secondary database server can access Secure FTP server on TCP port 22.
- Only webshield can access the internal exchange server on TCP port 25.
- Only GIAC management station can access dmz1 and dmz2 on TCP port 22.
- Only GIAC management server can access the border router on TCP port 23.
- Only GIAC management server can access the border router on UDP port 69.
- Only the border router can access GIAC management server on UDP port 69.
- All syslog capability devices send UDP port 514 to the Syslog #1 server.
- IDS #1 and IDS #2 send UDP port 514 to the Syslog #2 server.

Appendix B

Initial Configuration - Cisco 2621 Router

```
Current configuration : 663 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname outside
!
boot system flash:c1700-y-mz.122-4.T.bin
enable secret 5 $1$bK0D$Z1Rlu07jryIlOo2tRZPyj.
enable password !gcfw@00@
!
memory-size iomem 15
ip subnet-zero
!
!
!
interface FastEthernet0/0
 ip address 142.177.24.178 255.255.255.252
 speed 10
 half-duplex
!
interface FastEthernet0/1
 ip address 142.166.0.193 255.255.255.240
 speed 10
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 142.177.24.177
no ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
line aux 0
line vty 0 4
 password 1l0g0N
 login
!
end
```

Appendix C

Final Configuration - Cisco 2621 Router

```
Current configuration : 1914 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log datetime msec
service password-encryption
!
hostname outside
!
boot system flash:c1700-y-mz.122-4.T.bin
enable secret 5 $1$bK0D$Z1Rlu07jryIlOo2tRZPyj.
enable password 7 054A010C275B6E594925
!
memory-size iomem 15
ip subnet-zero
no ip source-route
!
no ip bootp server
!
!
!
interface FastEthernet0/0
 ip address 142.177.24.178 255.255.255.252
 ip access-group 101 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 speed 10
 half-duplex
 !
interface FastEthernet0/1
 ip address 142.166.0.193 255.255.255.240
 ip access-group 121 in
 no ip redirects
 no ip proxy-arp
 speed 10
 half-duplex
 !
!
ip classless
ip route 0.0.0.0 0.0.0.0 142.177.24.177
ip route 0.0.0.0 0.0.0.0 Null 0 255
ip route 10.240.20.0 255.255.255.0 142.166.0.194
no ip http server
!
```

```
logging trap informational
logging 10.240.20.78
access-list 1 permit 10.210.22.1
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.0.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log
access-list 101 deny ip 142.166.0.180 0.0.0.15 any log
access-list 101 permit ip any any
access-list 121 deny tcp 142.166.0.192 0.0.0.15 any range 135 139 log
access-list 121 deny udp 142.166.0.192 0.0.0.15 any range 135 139 log
access-list 121 deny tcp 142.166.0.192 0.0.0.15 any eq 445 log
access-list 121 deny udp 142.166.0.192 0.0.0.15 any eq 445 log
access-list 121 permit ip 142.166.0.192 0.0.0.15 any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
no cdp run
banner motd ^C

***  WARNING: Authorized Access Only  ***

  This site is currently being monitored
^C
!
line con 0
line aux 0
line vty 0 4
 access-class 1 in
 password 7 01420A545C5B28
login
!
no scheduler allocate
end
```

Appendix D

Cisco PIX Configuration

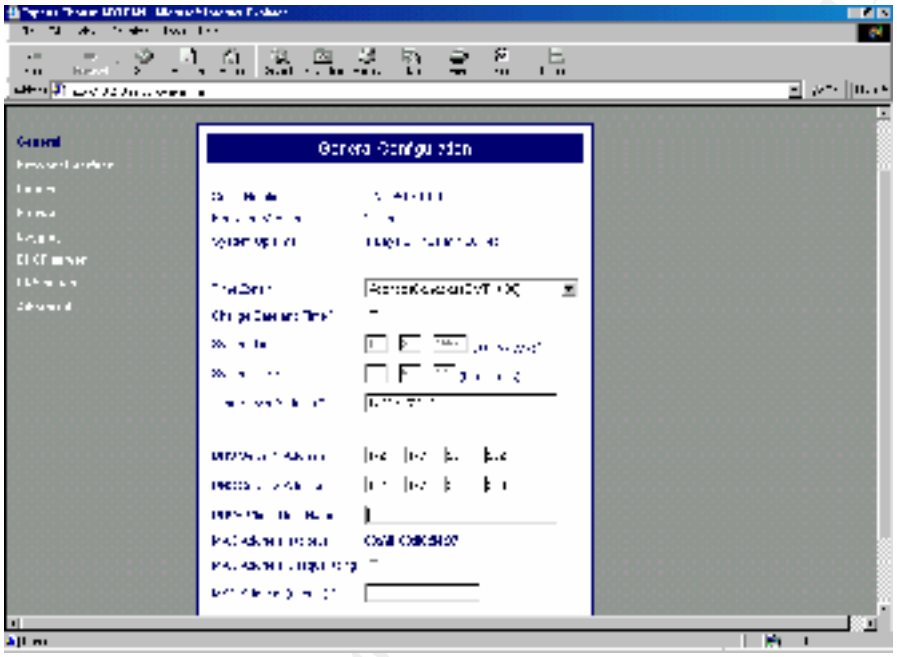
```
Building configuration...
: Saved
:
PIX Version 6.0(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password mzJisMbD.ttrRsBM encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname control
domain-name giac.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
name 172.16.224.101 www
name 172.16.224.197 mail1
name 172.16.224.21 ntp1
name 172.16.224.53 dns1
name 10.240.20.70 topgun
access-list acl_outside permit tcp any host www eq www
access-list acl_outside permit tcp any host www eq 443
access-list acl_outside permit tcp any host mail1 eq smtp
access-list acl_outside permit tcp any host dns1 eq domain
access-list acl_outside permit udp any host dns1 eq domain
access-list acl_outside permit udp host 142.166.0.193 host topgun eq tftp
access-list acl_outside deny ip any any
access-list acl_inside permit tcp host 10.210.20.5 any eq 21
access-list acl_inside permit tcp host 10.210.20.5 any eq www
access-list acl_inside permit tcp host 10.210.20.5 any eq 443
access-list acl_inside permit tcp host dns1 any eq domain
access-list acl_inside permit udp host dns1 any eq domain
access-list acl_inside permit tcp host mail1 any eq smtp
access-list acl_inside permit tcp host ntp1 any eq 123
access-list acl_inside permit tcp host topgun host 142.166.0.193 eq telnet
access-list acl_inside permit udp host topgun host 142.166.0.193 eq tftp
access-list acl_inside deny ip any any
pager lines 24
logging trap debugging
logging host inside 10.240.20.74
interface ethernet0 10baset
```

```
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 142.166.0.194 255.255.255.240
ip address inside 172.16.224.244 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm location topgun 255.255.255.255 inside
pdm location www 255.255.255.255 inside
pdm location mail1 255.255.255.255 inside
pdm location ntp1 255.255.255.255 inside
pdm location dns1 255.255.255.255 inside
pdm history enable
arp timeout 14400
global (outside) 1 142.166.0.205
nat (inside) 1 10.210.20.0 255.255.255.0 0 0
static (inside,outside) 142.166.0.201 mail1 netmask 255.255.255.255 0 0
static (inside,outside) 142.166.0.202 dns1 netmask 255.255.255.255 0 0
static (inside,outside) 142.166.0.203 ntp1 netmask 255.255.255.255 0 0
static (inside,outside) 142.166.0.200 www netmask 255.255.255.255 0 0
access-group acl_outside in interface outside
access-group acl_inside in interface inside
route outside 0.0.0.0 0.0.0.0 142.166.0.193 1
route inside 10.200.20.0 255.255.255.0 172.16.224.4 1
route inside 10.210.20.0 255.255.255.0 172.16.224.4 1
route inside 10.240.20.0 255.255.255.0 172.16.224.4 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
http topgun 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community 1d#f23AS0
no snmp-server enable traps
tftp-server inside topgun /pixconfig
floodguard enable
no sysopt route dnat
service resetinbound
telnet timeout 5
ssh topgun 255.255.255.255 inside
ssh timeout 5
terminal width 80
Cryptochecksum:9b51e43be6fe317f4e20d91692d8a9c5
: end
[OK]
```

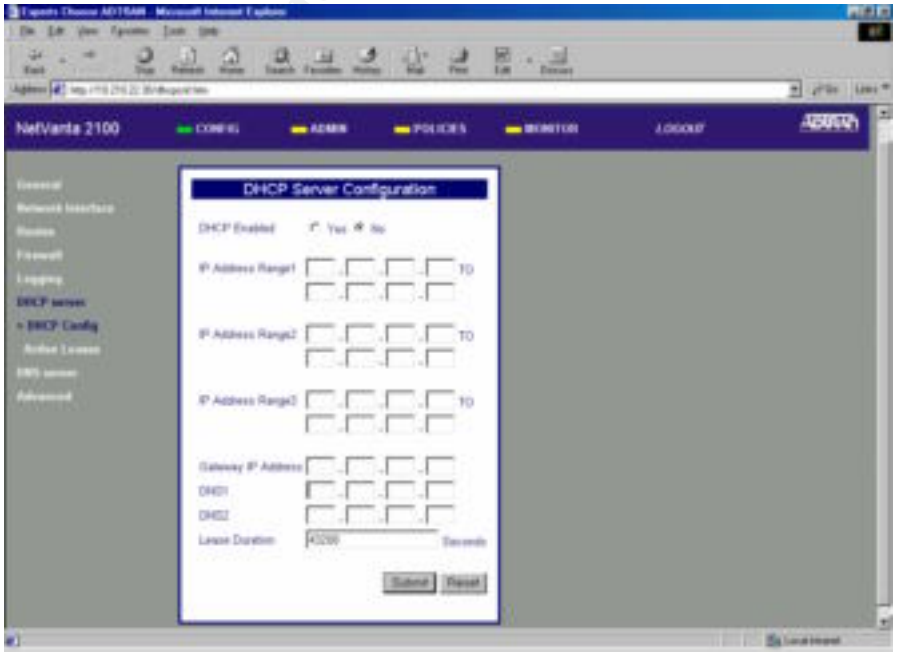
Appendix E

NetVanta 2100

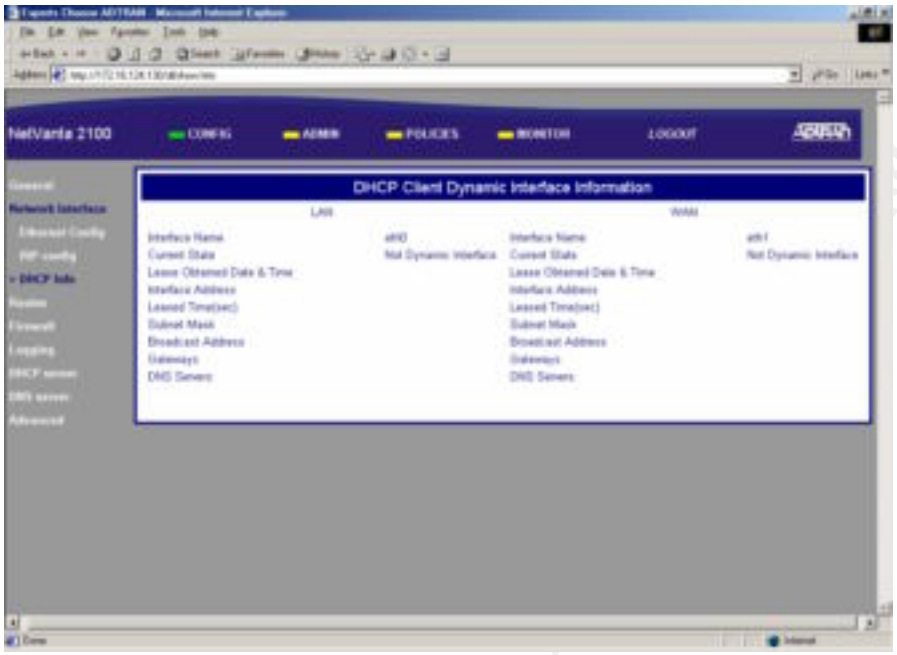
CONFIG > General > General Configuration – some general system information and the ability to define time zones, DNS servers, NTP server, etc.



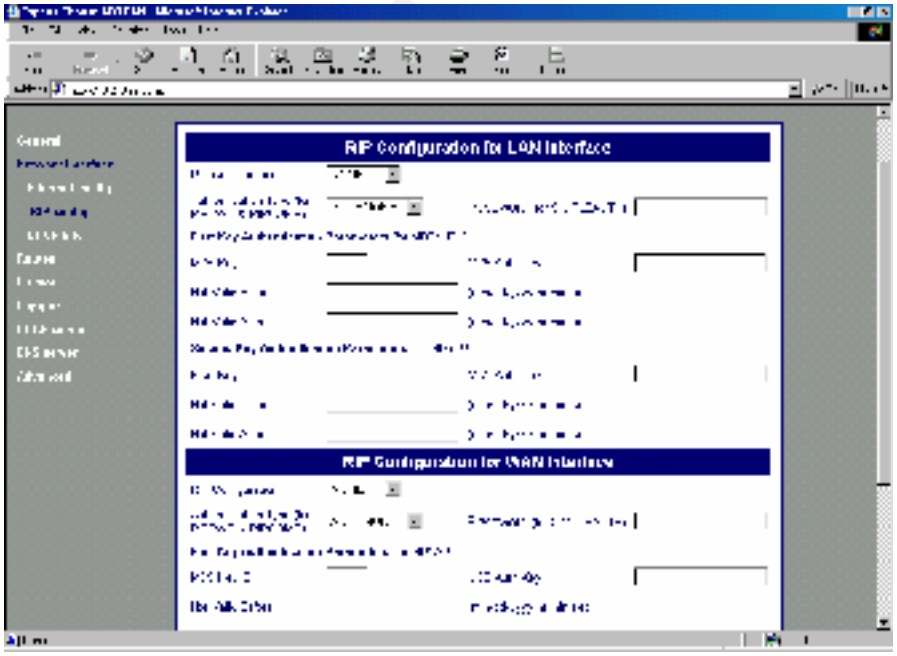
CONFIG > DHCP server > DHCP Server Configuration – for GIAC, disabling DHCP



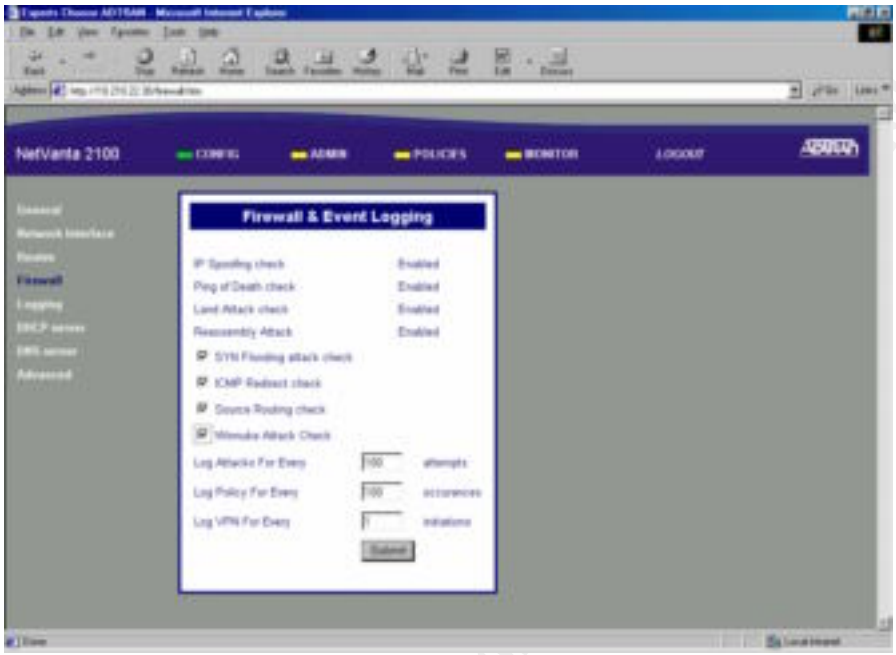
CONFIG > Network Interface > DHCP Info > DHCP Client Dynamic Interface Information



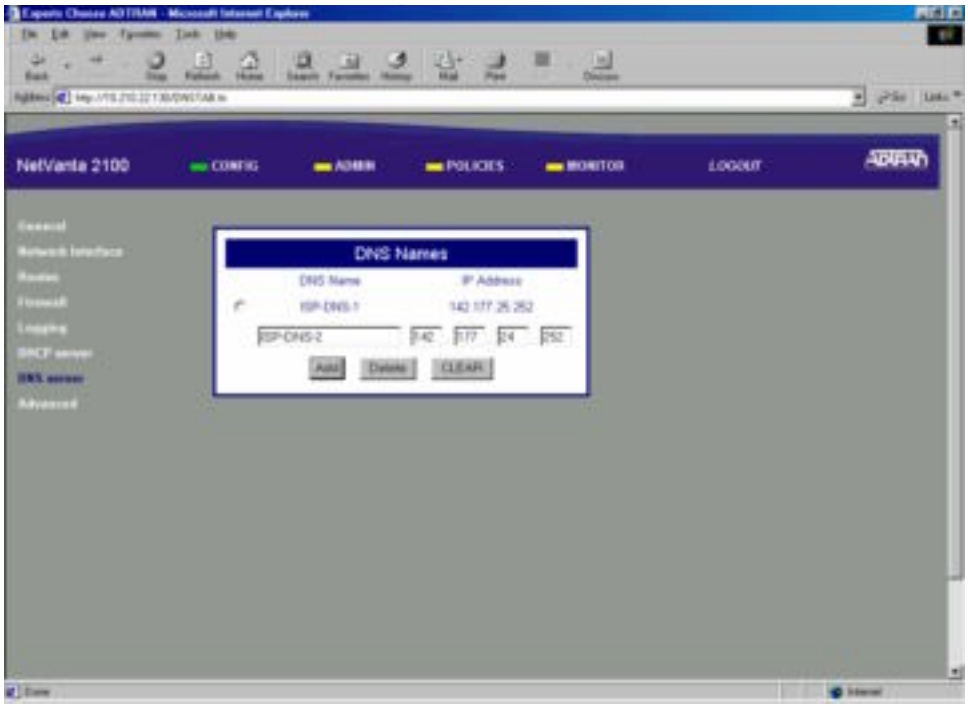
CONFIG > Network Interface > RIP config > RIP Configuration for LAN Interface – for GIAC, all RIP was turned off.



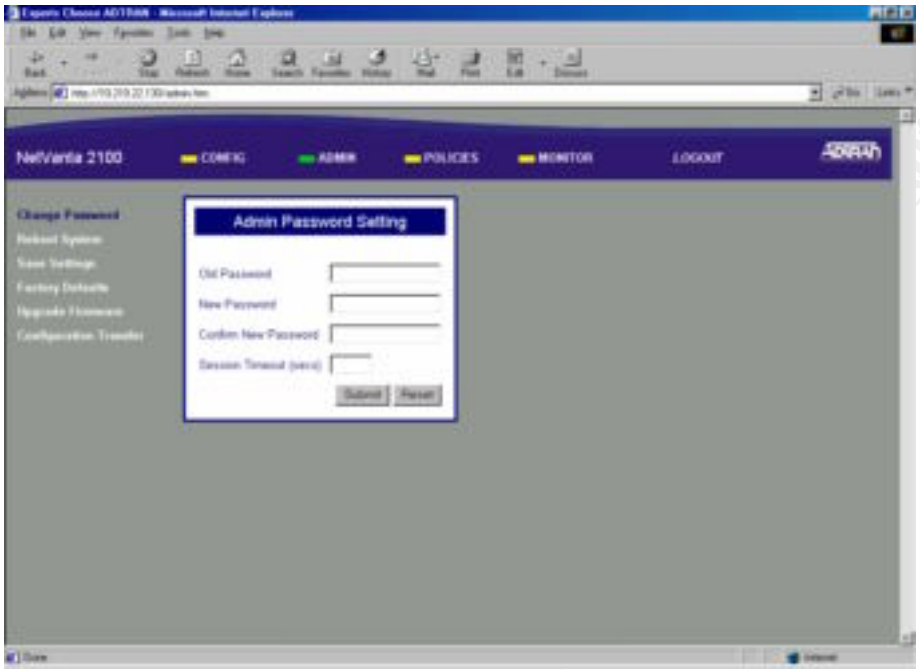
CONFIG > Firewall – for GIAC, all logging capabilities were enabled. Depending on "normal" Internet activities, the values for "Log Attacks For Every" attempts and "Log Policy For Every" occurrences will need to be adjusted.



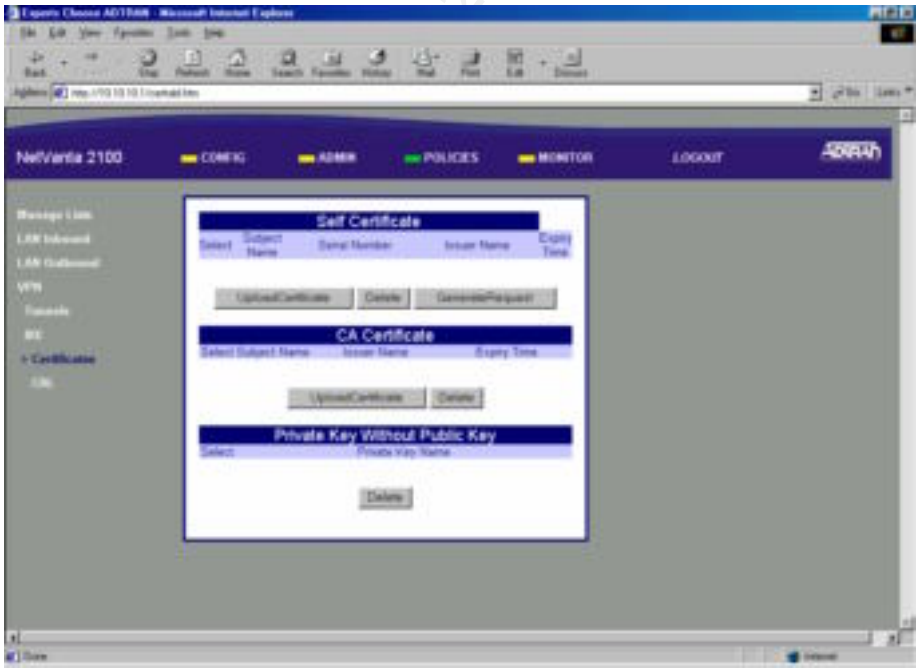
CONFIG > DNS server – for defining DNS services for the NetVanta.



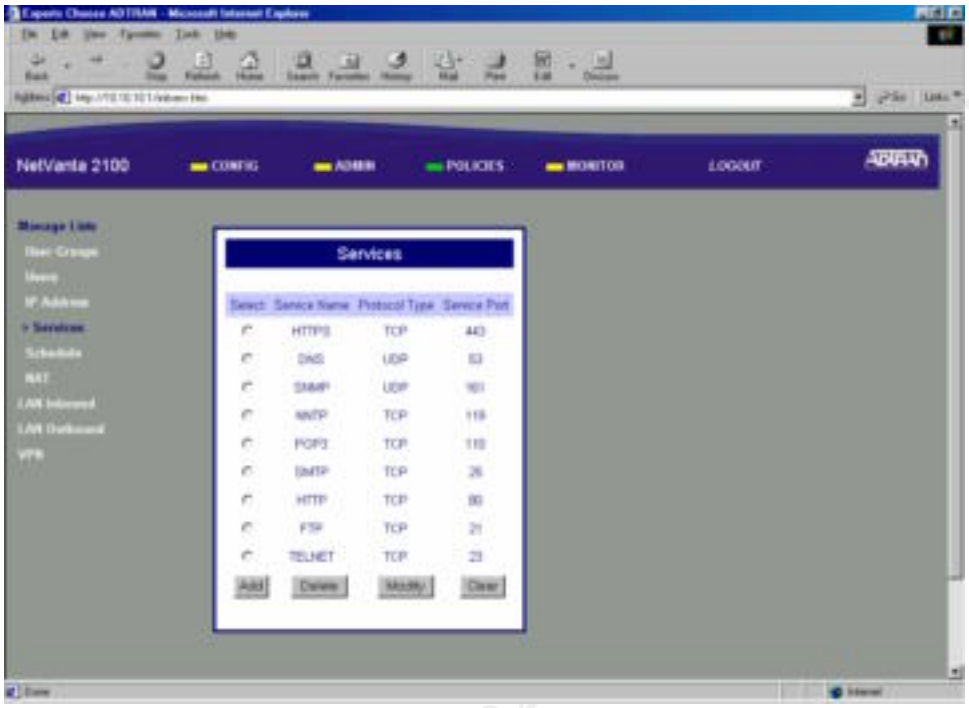
ADMIN > Change Password – for changing the administrator password.



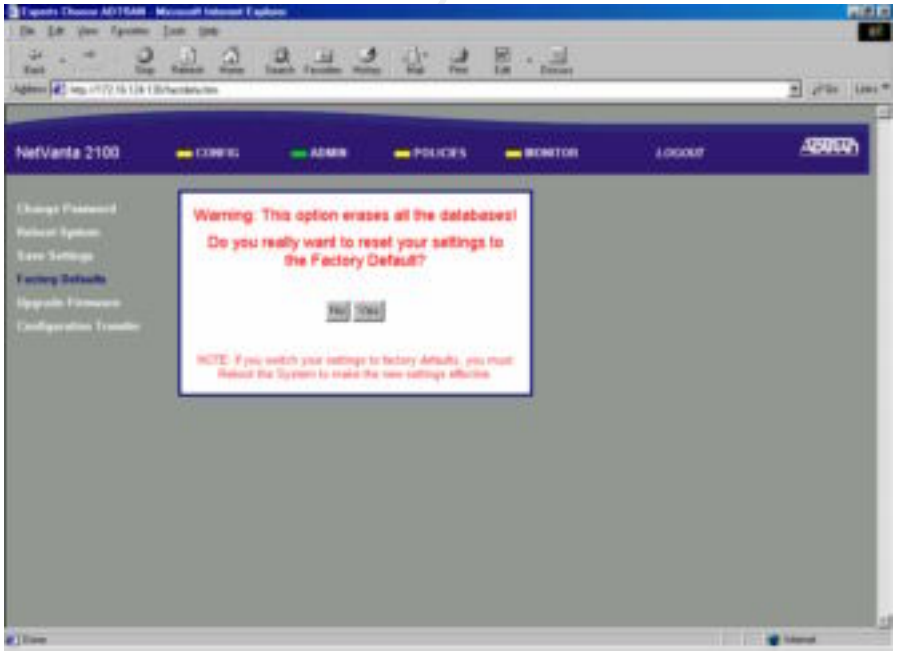
POLICIES > VPN > Certifications – for defining certificate policies.



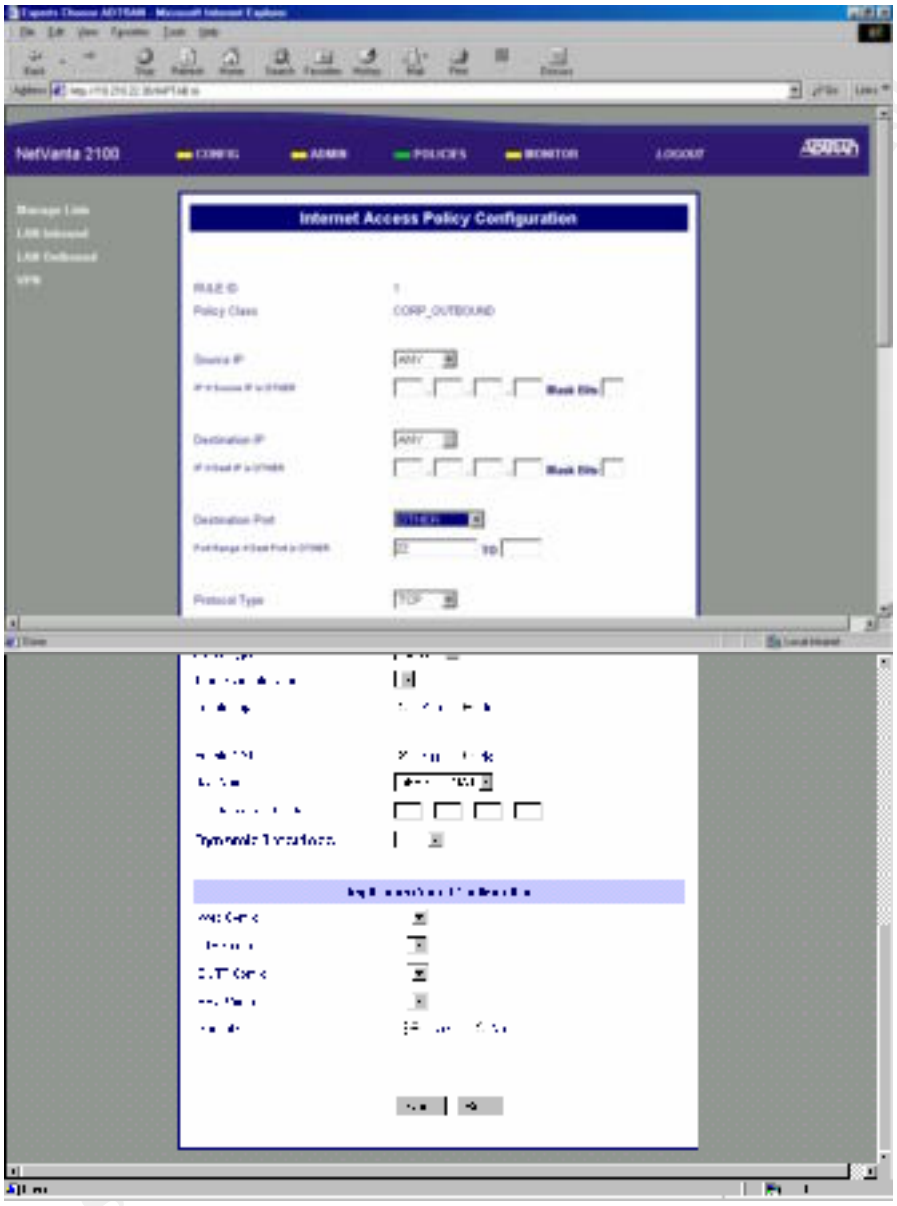
POLICIES > Manage Lists > Services – for defining services options.



ADMIN > Factory Defaults – for resetting the NetVanta back to factory defaults.

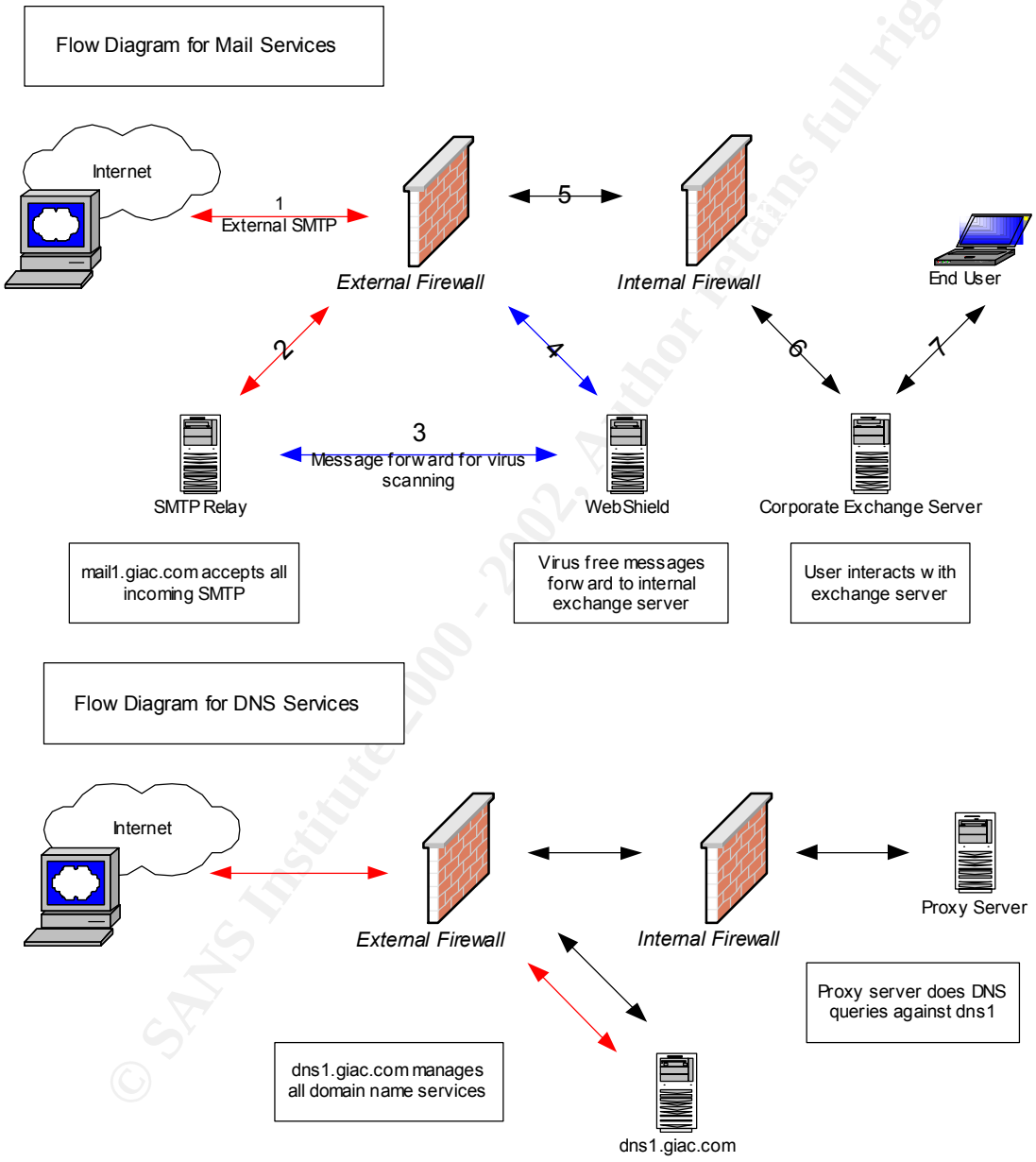


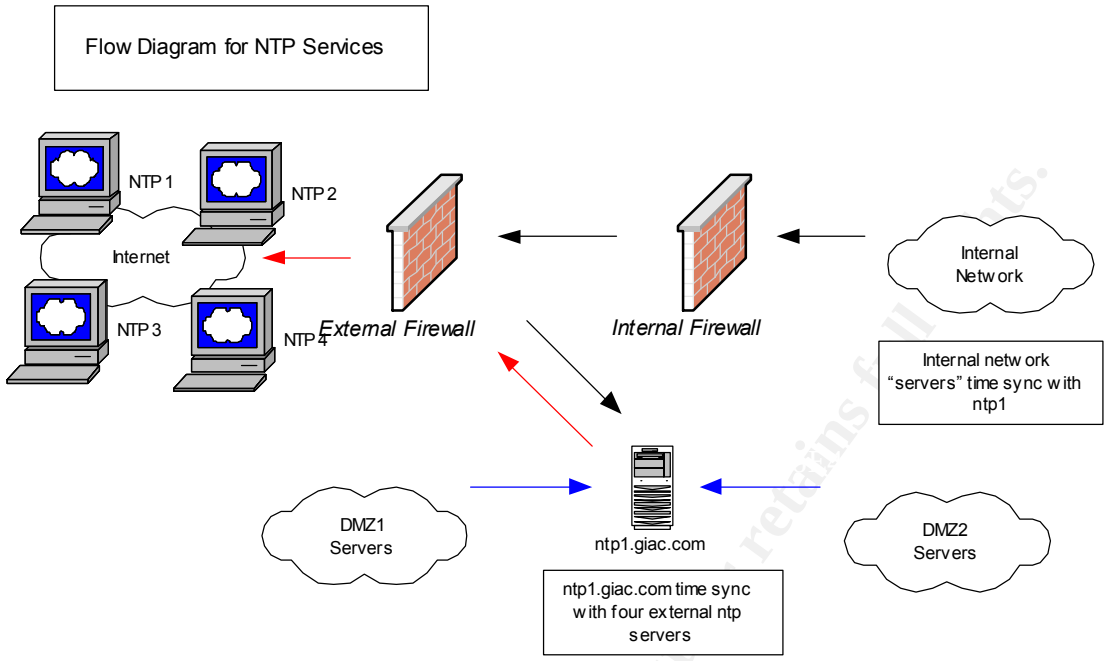
Policies > LAN Outbound > Internet Access Policy Configuration is created by default with full access to all partners on any port. As a good neighbour, a restriction has been put in place for TCP port 22 outbound.

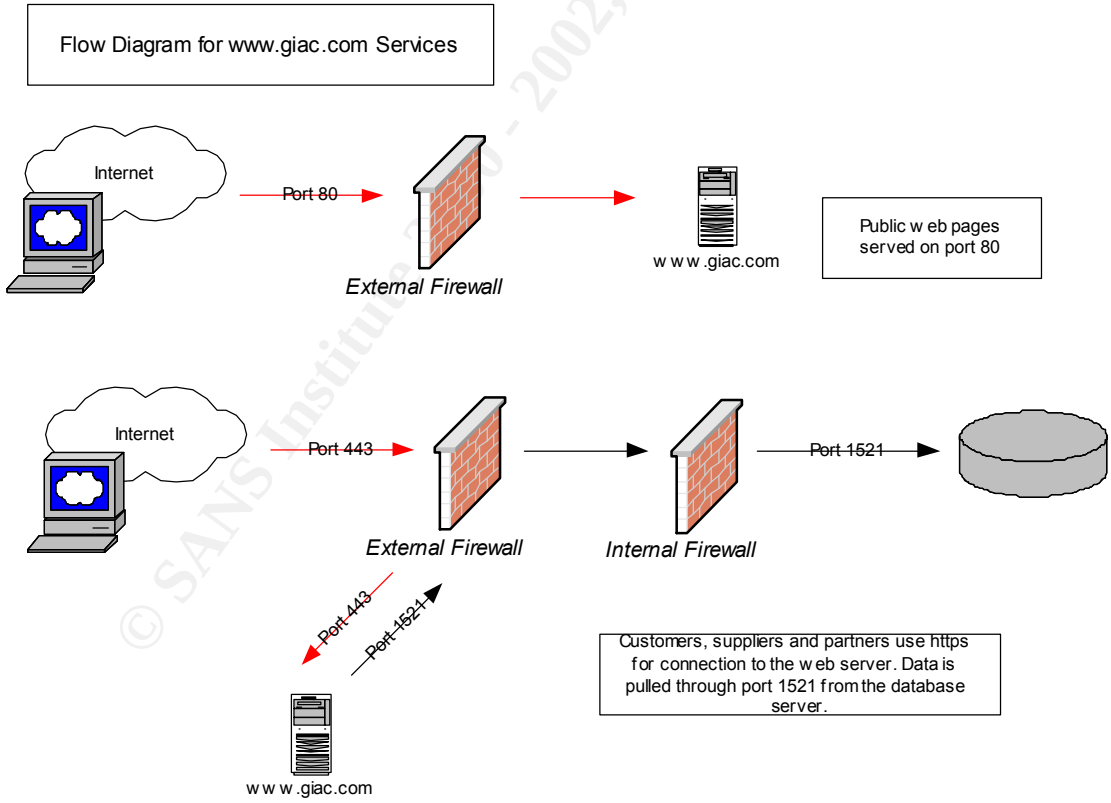


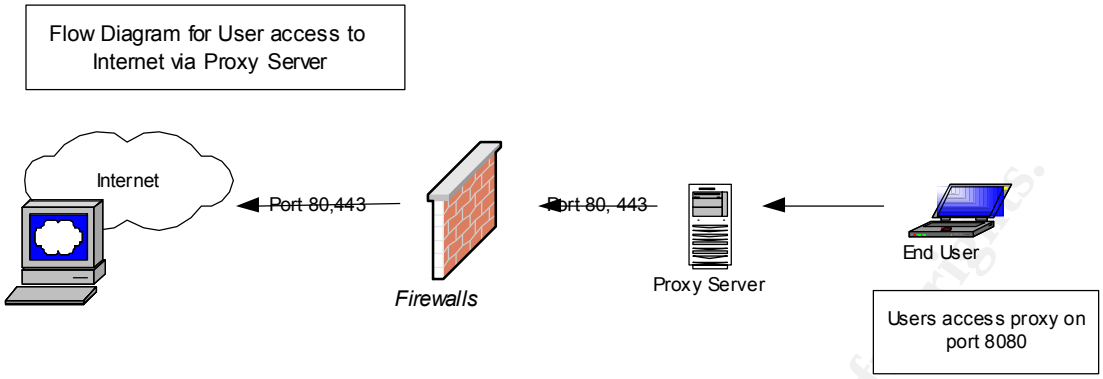
Appendix F

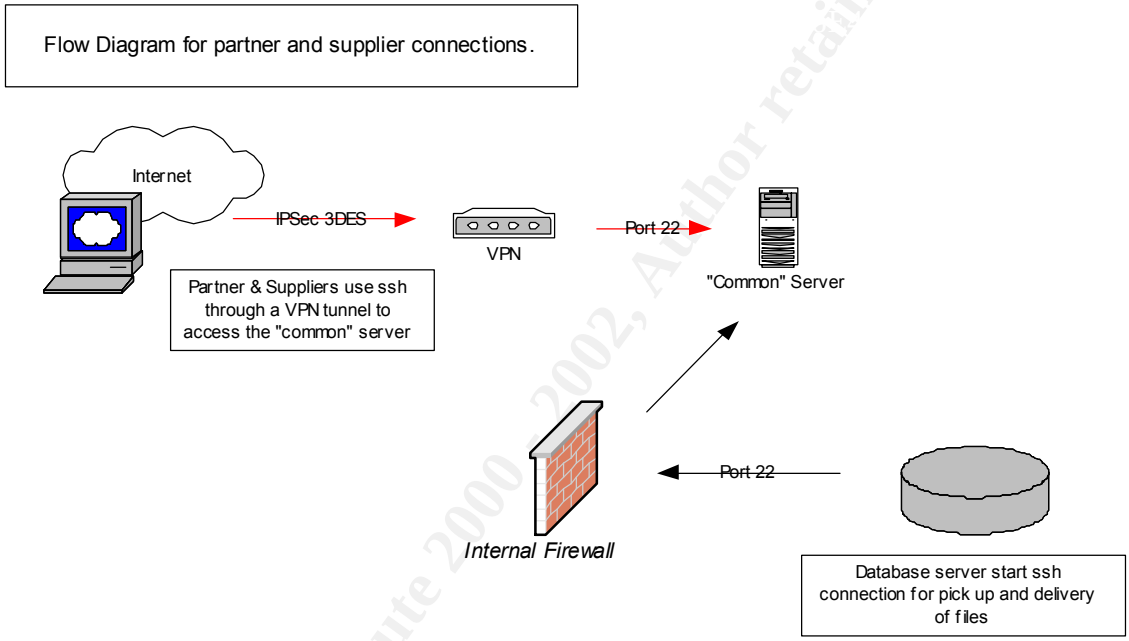
Logical Network Flow Diagrams











References

1) Brenton, Chris. 2.1: TCP/IP for Firewalls. SANS 2001 San Francisco, December 2001.
2) Brenton, Chris. 2.2 Firewalls 101: Perimeter Protection with Firewalls SANS 2001 San Francisco, December 2001.
3) Brenton, Chris. 2.3 Firewalls 102: Perimeter Protection and Defence In-Depth SANS 2001 San Francisco, December 2001.
4) Brenton, Chris. 2.4 VPN's and Remote Access SANS 2001 San Francisco, December 2001.
5) Brenton, Chris. 2.5 Network Design and Performance SANS 2001 San Francisco, December 2001.
6) URL: http://www.cisco.com/warp/public/707/21.html - routing
7) URL: http://www.linuxnewbie.org/articles/secureinstall.html
8) Pike, James. Cisco Network Security. Upper Saddle River, Prentice-Hall, 2002.
9) URL: http://www.pasadena.net/cisco/secure.html
10) URL: https://www.redhat.com/apps/support/errata/
11) URL: http://www.safermag.com
12) URL: http://www.checkpoint.com/techsupport/alerts
13) URL: http://www.securityfocus.com/advisories/2682
14) URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security
15) URL: http://www.cert.org
16) URL: http://www.sans.org
17) URL: http://www.incident.org
18) Swingle, Kenneth. GIAC Level2: Firewalls, Perimeter Protection, and Virtual Private Networks. September 2001
19) Will, Rita. Sans GIAC Firewalls, Perimeter Protection, and VPNs, July 19,2001
20) URL: http://www.adtran.com/all/public/