Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs GCFW Practical Assignment Version 1.6a

Brough Davis

2 Assignment 1 – Security Architecture

The following is the security architecture for GIAC Enterprises. GIAC Enterprises is an e-business which deals in the online sale of fortune cookie sayings.

2.1 Access requirements:

2.1.1 Overview

- Customers (the companies that purchase bulk online fortunes)
- Suppliers (the authors of fortune cookie savings that connect to supply fortunes)
- Partners (the international partners that translate and resell fortunes)
- GIAC Enterprises (the employees located on GIAC's internal network)

2.1.2 Customers

Customers will need to access GIAC Enterprises web servers via a secure connection in order to purchase the fortune cookies.
SSL should be the main method for customers to purchase fortune cookies. This allows an encrypted and scalable method for secure connections.

2.1.3 Suppliers

The suppliers work in a branch office that needs secure connections to the file servers at GIAC that contain all the fortunes.

Most suppliers are contracted out for their services for supplying fortunes. Since they are not employees a secure method was needed to protect how fortunes get sent to GIAC and at the same time not allow access to the GIAC employee resources.
Email is not an option. Using PGP to encrypt emails would cause confusion for the non-technical staff members to keep track of Key pairs. Email might also cause confusion when trying to archive all the fortunes in a central place.
A VPN remote access method would be more effective to provide the suppliers a secure met

2.1.4 Partners

The international partners have 2 different locations around the world (Berlin, Tokyo) for translating the fortunes into different languages and making sure

cultural differences are taken into account to limit the possibility of offensive translations. The partner locations need secure access to GIAC Enterprises file server in order to archive and update the translations to the fortunes. A VPN solution would be ideal between the partner locations and GIAC Enterprises.

2.1.5 GIAC Enterprises

The majority of the employees come in to the main HQ office to work. Most of the manufacturing and operations is done at the HQ office. A few employees such as the VP's are constantly traveling around the world to meet with the suppliers and partners. Those that are traveling need a secure method for accessing the fortune information along with the current supplier and partner information (orders, accounting books, etc.).
It was decided not to manage a RAS server for remote employee access to the GIAC Enterprise network. Even though a secure configuration might be effective this provides another possible hole that a hacker can use to bypass the firewall. A remote access VPN solution would be most effective to provide a one point of entry for all types of access.

2.2 Network Architecture

2.2.1 Services

Service/Protocol Name	TCP/UDP Port
SSL	TCP 443
SMTP	TCP 25
IMAP*	TCP 143
DNS queries	UDP 53
SMB** (MS File Sharing)	TCP/UDP 445

* IMAP is the preferred method for email. It allows the remote employees not to carry all sensitive data on their laptops. Of course they do have the ability to cache the emails locally when not connected to Internet/VPN connection.
** With windows 2000 file sharing can be implemented with out NBT and only using MS SMB ports.

2.2.2 Network Devices

Cisco 2621 IOS 12.2
The Cisco 2621 router will be the access router responsible for the "first line" of defense. The router will protect against spoof attempts and private/reserved space trying to be source-spoofed from both the public and internal sides.

Nokia IP330/Checkpoint FW1 IPSO 3.4.1 / (FW1/VPN1 4.1 SP5)
Two Nokia IP330 devices with Checkpoint Firewall Software will be used. The first IP330 will be used to protect the DMZ from the Internet.

The second IP330 will protect the internal networks from the DMZ and Internet traffic. It will also control the VPN tunnels for remote employees using internal systems for file sharing and email. Remote (mobile) Employees will use Checkpoint SecureRemote software as a remote access method for VPN access to access email and file sharing services. Partners will use a VPN gateway method using a Checkpoint FW at the Partner location to encrypt all email and file sharing into the internal network.

Snort SNORT 1.6 / FreeBSD 4.4
Snort will be used to alert the network administrator to any suspicious traffic destined for the DMZ or Internal Network. Centralized logging will be used to manage the information.

Foundry BigIron 4000 OS 7.1.24
The Foundry BigIron is a layer 3 switch. The BigIron has one of the highest port densities and lowest port costs of its kind in the industry. It also has a very similar Cisco-like configuration which makes this switch very easy to implement. Because the Foundry BigIron is very similar to Cisco switches it has had similar security holes that Cisco has seen such as HTTP and SSH vulnerabilities.

In the GIAC environment the BigIron plays two roles: Port Aggregation and Segmentation. The BigIron has 72 available 10/100 Ethernet ports that allows the internal network to scale well. The layer 3 capabilities of the switch allow internal networks to be even more segmented. In the current state the employee desktops are on a separate network than the management systems (monitoring, logging, TACACS). ACL's can further secure the internal networks from external sources and each other.

2.2.3 Host Devices

Device	IP Address
Web Server	199.0.5.2
Email Server	199.0.5.3
File/Print Server	199.0.0.2
RSA Server	199.0.1.2
Logging/Monitoring Server	199.0.1.3

2.2.4 Networks

Network Name	IP
Partners	200.0.0.0/24 Berlin 100.0.0.0/24 Tokyo
Suppliers	ANY
Customers	ANY

GIAC DMZ	199.0.5.0/27
GIAC Private (Employees)	199.0.0.0/24
GIAC Private (Network Mgmt)	199.0.1.0/24

2.2.5 Traffic Flow (pseudo rules)

PUBLIC (Customers)
Access to DMZ: Permit HTTP/HTTPS Traffic
Access to PARTNERS: Permit Return Session Based TCP Traffic
Access to REMOTE EMPLOYEES: Permit Return Session Based TCP Traffic
Access to SUPPLIERS: Permit Return Session Based TCP Traffic
Access to INTERNAL: Permit Return Session Based TCP Traffic

PARTNERS
Access to DMZ: Permit HTTP/HTTPS Traffic
Access to PUBLIC: Permit All
Access to REMOTE EMPLOYEES: No Access (Drop)
Access to SUPPLIERS: No Access (Drop)
Access to INTERNAL: VPN Encrypted Access for File Sharing and Email

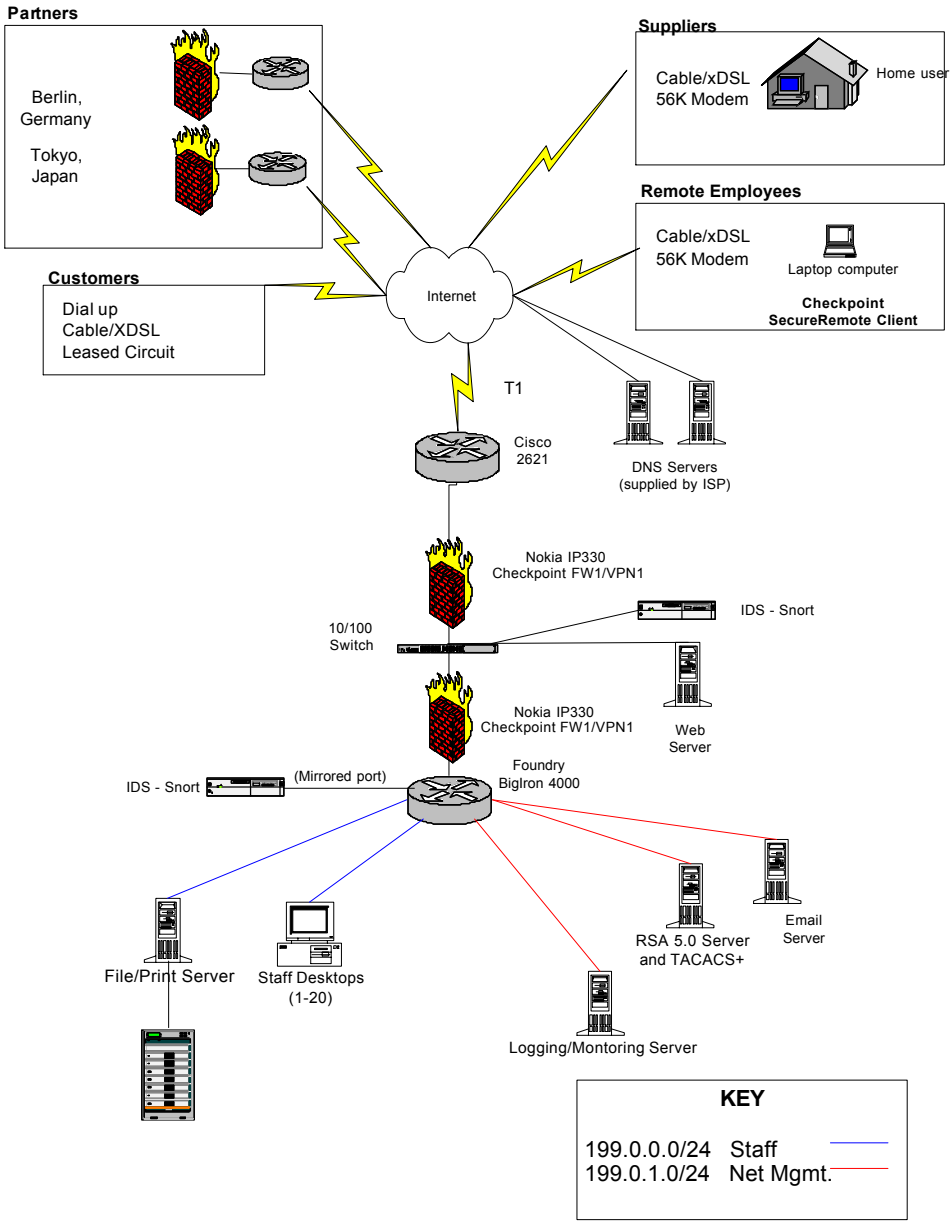
SUPPLIERS
Access to DMZ: Allow HTTP/HTTPS Traffic
Access to PARTNERS: No Access (Drop)
Access to REMOTE EMPLOYEES: No Access (Drop)
Access to PUBLIC: Permit All
Access to INTERNAL: No Access (Drop)

DMZ
Access to PUBLIC: Permit Return Session Based HTTP/HTTPS Traffic
Access to PARTNERS: Permit Return Session Based HTTP/HTTPS Traffic
Access to REMOTE EMPLOYEES: Permit Return Session Based HTTP/HTTPS Traffic
Access to SUPPLIERS: Permit Return Session Based HTTP/HTTPS Traffic
Access to INTERNAL: Permit Return Session Based Mgmt Traffic

INTERNAL
Access to DMZ: Permit Mgmt Traffic
Access to PARTNERS: No Access (Drop)
Access to REMOTE EMPLOYEES: No Access (Drop)
Access to SUPPLIERS: No Access (Drop)
Access to PUBLIC: Permit All

REMOTE EMPLOYEES
Access to DMZ: Permit HTTP/HTTPS Traffic
Access to PARTNERS: No Access (Drop)
Access to PUBLIC: Permit All
Access to SUPPLIERS: No Access (Drop)
Access to INTERNAL: VPN Encrypted Access for File Sharing and Email

2.3 Diagrams



3 Assignment 2 – Security Policy

3.1 Cisco 2621 Policy

The Cisco 2621 is the first level of defense from incoming threats. The following is a list of commands that will "harden" the router from attacks to itself as well as limit some basic DoS attacks.

! Disable http, bootp server, and small TCP and UDP ports
```
no ip http server
no ip bootp server
no service tcp-small-servers
no service udp-small-servers
```

! Enable tacacs+ for authentication and authorization
```
aaa new-model
aaa authentication login default tacacs+
aaa authentication login oob tacacs+ enable
aaa authorization exec tacacs+ if-authenticated
tacacs-server host 199.0.1.3
tacacs-server key G!@C
```

! Enable snmp read only string for MRTG and monitoring purposes.
! snmp queries only allowed from monitoring/logging server
```
snmp-server community m0n-G!ac RO 25
```

! enable password and max privilege level – make sure password is encrypted
```
enable secret 7 g!@c3nt3rpr!s3s
service password-encryption
```

! Only allow the secure workstations network to connect to the router
```
access-list 25 permit host 199.0.1.3
access-list 10 deny any log
    line vty 0 4
      access-class 10 in
      login authentication default
```

! login only tries tacacs for telnet but falls back to the enable password for login if tacacs+ server is unreachable
```
    line console 0
      login authentication oob
```

! Display a login warning banner
```
banner login /
*** WARNING ***
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system,
disconnect now.
Failure to do so may result in criminal prosecution, civil
penalties, or both.
By continuing beyond this point you attest under penalty of
perjury that you are an authorized user of this system, and
that you consent to monitoring of your activities.
If you do not agree with this statement, disconnect now.
/
```

! Enable logging to consolidated logging server
```
logging 199.0.1.3
```

!! Traffic Filtering

! In order to avoid disseminating information about the internal structure of the
! network, block all ICMP “unreachable” error messages.
```
no ip unreachables
```

! Block all IP directed broadcasts to prevent denial of service conditions on our network
! as well as prevent GIAC Enterprises from becoming a Smurf amplifier.
```
Interface s0/0 (as well as eth 0/0)
  no ip directed-broadcast
```

! Block all source routed packets
```
no ip source-route
```

Note: The policy outlined above should be implemented on all GIAC Enterprises routers. The following access controls are installed only on the perimeter router, however.

! Block all inbound traffic originating from private/non-routable address spaces

```
access-list 11 deny 192.168.0.0 0.0.255.255
access-list 11 deny 172.16.0.0 0.15.255.255
access-list 11 deny 10.0.0.0 0.255.255.255
access-list 11 deny 127.0.0.0 0.255.255.255
```

! Block all spoof attempts or forged packets with source address as the internal nets.

```
access-list 11 deny 199.0.0.0 0.0.1.255
access-list 11 permit any

interface s0/0
    ip address x.y.z.1 xxx.xxx.xxx.xxx
    ip access-group 11 in
```

! Block all outbound traffic that does not have source IP addresses in the GIAC
! Enterprises address space.

```
access-list 12 permit 199.0.0.0 0.0.1.255

interface e0/0
    ip address x.y.z.1 xxx.xxx.xxx.xxx
    ip access-group 12 in
```

3.2 Checkpoint FW1 Policy

3.2.1 Objects

Name	Description
Net-Business-Partners	200.0.0.0/24 Berlin 100.0.0.0/24 Tokyo
Net-Internal	199.0.0.0/23
Net-DMZ	199.0.5.0/27
RemoteEmployee	Employees assigned RSA Tokens
NM-WkStation	199.0.1.3
FW-Perim	FW Interfaces
Web	199.0.5.2
Email	199.0.5.3

3.2.2 External Firewall Rules

Rule	Source	Destination	Service	Action	Track	Comments
1	Any	FW-Perim	Any	Drop	Long	Do not allow anyone to connect to the firewall itself
2	Any	Web	Http Https	Accept	Long	Allow anyone to browse to the
3	Web	FileServer	NBT	Accept	Long	Allow backend web connection to dump to fileserver
4	Email	Any	Smtp	Accept	Long	Allow email gateway to send email to anyone
5	Net-Perim Net-DMZ Net-Remote Net-Internal	NM-WkStation	Syslog	Accept		Allow any system to syslog to the consolidated log server
6	Remote-Suppliers Net-Business-Partners Remote-Password-Users	Email DMZ	IMAP4	Accept	Long	Allow GIAC suppliers, business partners and employees to access the internal email system
7	RemoteEmployees	DMZ Internal Network	Any	Accept	Long	Allow a select group of employees unrestricted access to the network after they authenticate to the VPN via token
8	Any	Any	Any	Drop	Long	Drop everything that is not expressly permitted.

3.2.3 Internal Firewall Rules

Rule	Source	Destination	Service	Action	Track	Comments
1	Net-Business-Partners	Net-Internal	Email SMB	Encrypt	Long	VPN traffic from partners to GIAC internal net
2	RemoteEmployee@ANY	Net-Internal	Email SMB	Client-Encrypt	Long	VPN traffic from remote user to Internal Net

3	NM-WkStation	Net-Perim	SSH Firewall-1	Accept	Long	Allow Security Team to telnet, ssh, and remotely administer firewalls anywhere
4	Any	FW-Perim	Any	Drop	Long	Do not allow anyone to connect to the firewall itself
5	Internal	Any	Any	Accept	Long	Allow Staff out
6	Any	Any	Any	Drop	Long	Drop everything that is not expressly permitted.

3.3 Checkpoint VPN-1 Policy

SecureRemote and SecureClient

Authentication Protocol: Hybrid Mode IKE
Authentication Method: SecureID
Encryption: 3DES
Hash: MD5

Aggressive Mode: Enabled
Supports Subnets: Enabled

Groups: Suppliers, Partners, GIACEmployees
Client Authentication Scheme: SecureID
Cleint Encryption Method: IKE

IKE Properties:

Authentication: Set Password
ESP (Encryption and Data Integrity)
Encryption: 3DES
Data Integrity: SHA1

Rules:

1	Net-Business-Partners	Net-Internal	Email SMB	Encrypt	Long	VPN traffic from partners to GIAC internal net
2	RemoteEmployee@ANY	Net-Internal	Email SMB	Client-Encrypt	Long	VPN traffic from remote user to Internal Net

It is important to note that while the Business Partners can access email and file servers on the GIAC internal network the internal network can not access resources at the Partner location. The tunnel is only one way.

3.4 Foundry BigIron 4000 Policy

! Define ACL for management of the switch for SSH and SNMP
```
access-list 25 permit host 199.0.1.3
snmp-server community public ro 25
```

! Disable web server and telnet server
```
no web-management
no telnet server
```

! Enable tacacs+ authentication and authorization
```
aaa authentication login default tacacs+ enable
aaa authorization exec default tacacs+
tacacs-server host 199.0.1.3
tacacs-server key G!@C
```

! Enable SSH and SCP for secure management of the BigIron
! Mgmt ip must resolve in DNS for SSH to work properly
```
hostname bi4k-1
ip dns domain-name giacenterprises.com
crypto key generate rsa
ssh access-group 25
```

! Enable super user password
```
enable super-user-password g!@c3nt3rpr!s3s
```

Note: The passwords and snmp strings in the configuration are encrypted by default

! Enable Banner
```
banner /
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system,
disconnect now.
Failure to do so may result in criminal prosecution, civil
penalties, or both.
By continuing beyond this point you attest under penalty of
perjury that you are an authorized user of this system, and
that you consent to monitoring of your activities. If you do
```

```
not agree with this statement, disconnect now.
/


! Foundry comes with some handy DoS mitigation features
no ip directed-broadcast

! if for some reason ICMP makes it to the internal network the below statement
!   allows 5000 ICMP packets to sustain while it will allow a burst rate of 10000
!   before it drops all ICMP packets for 5 minutes
ip icmp burst-normal 5000 burst-max 10000 lockup 300

! Same as ICMP attack but for Syn floods
ip tcp burst-normal 10 burst-max 100 lockup 300
```

Since the BigIron is already behind the border router and main firewall it would be a little over kill to create specific filters for ingressing internet traffic.

3.5 Cisco 2621 Hardening Tutorial

Referring to the Cisco 2621 Policy the following is a step-by-step tutorial around implementing the commands.

Brief overview of commands:

```
no ip http server
no ip bootp server
no service tcp-small-servers
no service udp-small-servers
aaa new-model
aaa authentication login default tacacs+
aaa authentication login oob tacacs+ enable
aaa authorization exec tacacs+ if-authenticated
tacacs-server host 199.0.1.3
tacacs-server key G!@C
snmp-server community m0n-G!ac RO 25
enable secret 7 g!@c3nt3rpr!s3s
service password-encryption
banner login /
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system,
disconnect now.
Failure to do so may result in criminal prosecution, civil
penalties, or both.
By continuing beyond this point you attest under penalty of
perjury that you are an authorized user of this system, and
```

```
that you consent to monitoring of your activities.
If you do not agree with this statement, disconnect now.
/
logging 199.0.1.3
no ip unreachables

Interface s0/0 (as well as eth 0/0)
  no ip directed-broadcast
no ip source-route
access-list 11 deny 192.168.0.0 0.0.255.255
access-list 11 deny 172.16.0.0 0.15.255.255
access-list 11 deny 10.0.0.0 0.255.255.255
access-list 11 deny 127.0.0.0 0.255.255.255
access-list 11 deny 199.0.0.0 0.0.1.255 log
access-list 11 permit any
access-list 12 permit 199.0.0.0 0.0.1.255
access-list 12 deny any log
access-list 25 permit host 199.0.1.3
access-list 25 deny any log
interface s0/0
    ip address x.y.z.1 xxx.xxx.xxx.xxx
    ip access-group 11 in
interface e0/0
    ip address x.y.z.1 xxx.xxx.xxx.xxx
    ip access-group 12 in
line vty 0 4
      access-class 25 in
     login authentication default
line console 0
      login authentication oob
```

To implement configuration commands and access lists perform the following tasks:

Before configuring a border router make sure that you have some kind of out of band access either through a modem or terminal server attached to the console port. In the case you enter a command that disconnects the telnet session it is very helpful to use the out of band connection as a backup.

Login to the router via telnet.

```
telnet x.y.z.1

User Access Verification
Password:
```

You will be at the router> prompt, enter the enable command

```
Router> enable
```

You will be prompted for the enable password, enter it and you will be taken to the enable prompt.

```
Password:
Router#
```

Go into global configuration mode by entering the "conf t" command. Be very careful, while in configuration mode. It's possible to cause yourself some serious problems if you're not paying attention. Be especially careful when applying access lists to interfaces to make sure that you don't lock yourself out of the router. You also want to check your syntax to make sure you don't make typos if you can help it because editing numbered access lists can be a pain. If you make a mistake or you don't feel comfortable with the changes you've made to the configuration file and just want to get out of configuration mode without making any changes just hit control-c.

```
Router#conf t
Router(config)#
```

Now begin hardening the router

```
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers
Router(config)# snmp-server community m0n-G!ac RO 25
Router(config)#no ip http server
Router(config)#no ip bootp server
Router(config)#service password-encryption
Router(config)#enable secret 7 g!@c3nt3rpr!s3s
```

Now configure TACACS configuration for authentication and authorization

```
Router(config)#aaa new-model
Router(config)#aaa authentication login default tacacs+
Router(config)#aaa authentication login oob tacacs+ enable
Router(config)#aaa authorization exec tacacs+ if-authenticated
Router(config)#tacacs-server host 199.0.1.3
Router(config)#tacacs-server key G!@C
```

ACL Overview:

ACL 11 Allowing non-spoofed traffic from private/martian networks to come in (ingress) to the router from the internet. Applied to the internet facing router

interface
ACL 12 Allowing the internal network (only) to exit (egress) to the internet. Applied to the internal interface.
ACL 25 Allowing only trusted networks to Telnet to the router itself. This is applied to the VTY sessions

Now restrict login access to the router. Be sure that you define the access list before attempting to enable it, otherwise you may not be able to login to the router across the network. A good way of maintaining ACL's and to help prevent make mistakes is to keep the ACL lists on a TFTP Server. This allows a clean ACL lsit to be kept (one acl list per file). Once the file is double checked the following command can be entered to update the ACL:

```
Router#copy tftp running 199.0.1.3 acl25
```

However if a TFTP server is not available the following commands can be entered for inserting the ACLs. Make sure you are in global config mode ("conf t").

```
Router(config)#access-list 25 permit host 199.0.1.3
Router(config)#access-list 25 deny any log
Router(config)#line vty 0 4
Router(config-line)#   access-class 25 in
Router(config-line)#   login authentication default
```

Set the login Banner by entering "banner login" followed by the ending character you want to use such as "/". Then enter the lines of your warning banner followed by another the ending character you specified earlier.

```
Router(config)#banner login /
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system,
disconnect now.  Failure to do so may result in criminal
prosecution, civil penalties, or both.  By continuing beyond
this point you attest under penalty of perjury that you are
an authorized user of this system, and that you consent to
monitoring of your activities.  If you do not agree with
this statement, disconnect now.
/
Router(config)#
```

Enable logging to the syslog server, and block ICMP unreachable messages and source routed packets.

```
Router(config)#logging 10.10.100.14
Router(config)#no ip unreachables
Router(config)#no ip source-route
```

Block ICMP broadcast packets on the interfaces.

```
Router(config)#int e0/0
Router(config-if)#no ip directed-broadcast
Router(config-if)#int s0/0
Router(config-if)#no ip directed-broadcast
```

Create the ingress and egress filtering ACL's. The format of the standard ACL's we are using is as follows:

access-list <access list number> <action> [<source> <wildcard>] | [any]

Where:

<access list number> is a number between 1 and 99,
<action> is either permit or deny, and
<source><wildcard> specifies a source address to match against and a wildcard to specify how many bits of the source address to check in order to determine a match. In other words, in order for an address to match a source/wildcard pair every bit in the source address must match every bit in the address you are checking against, EXCEPT for those bits that are set to 1 in the wildcard. As an example, wildcard of 0.0.0.0 requires every single bit to match up, while a wildcard of 0.0.0.255 would require only the first 24 bits of the addresses to match up. The keyword "any" can be used to match any address in lieu of specifying a source/wildcard pair.

Order:

It is important to look at the order of how the ACL's are applied. When a packet is received on an interface with an ACL applied to it the packet will be compared against the very first ACL. This means the broadest rules should go first. For example:

```
access-list 50 permit any
access-list 50 deny 192.168.0.0 0.0.0.255
```

With this ACL all traffic will be accepted even if a packet from the 192.168.0.0 network is seen. The router prioritizes the first ACLs. Back to the ACL configs:

```
Router(config)#access-list 11 deny 192.168.0.0 0.0.255.255
Router(config)#access-list 11 deny 172.16.0.0 0.15.255.255
Router(config)#access-list 11 deny 10.0.0.0 0.255.255.255
Router(config)#access-list 11 deny 199.0.0.0 0.0.1.255
```

```
Router(config)#access-list 11 permit any

Router(config)#access-list 12 permit 199.0.0.0 0.0.1.255
```

If you mess up one of these commands you can remove it by issuing the "no" command in front of the incorrect line. For example if you incorrectly typed

```
Router(config)#access-list 11 deny 169.255.0.0 0.0.255.255
```

as the 4th line of access list 11 you could remove it by typing

```
Router(config)#no access-list 11 deny 165.255.0.0
0.0.255.255
```

You would then be free to re-add the line. Unfortunately, it will be added after the last line of access list 11, so if you didn't catch your error right away you would have to delete every line of access list 11 after the 4th line and re-add each one of the in order to maintain the correct ordering.

After you have your access lists correct, apply the ingress filter to the serial interface, and the egress filter to the Ethernet interface. It may be wise to issue a "wr t" command to display the configuration file so that you can verify that your access controls are correct before proceeding, just to be safe. "wr t" is synonymous with "show running-config" which shows the current configuration saved in volatile memory. It is important to know that if the running-config is different from the startup-config (which is in NVRAM) that after a reboot the running-config will be replaced with the startup-config and all changes to the running-config will be lost.

```
Router(config)#interface s0/0
Router(config-if)#    ip address x.y.z.1 xxx.xxx.xxx.xxx
Router(config-if)#    ip access-group 11 in

Router(config-if)#interface e0/0
Router(config-if)#    ip address x.y.z.66 xxx.xxx.xxx.xxx
Router(config-if)#    ip access-group 12 in
```

The access list restrictions will take place immediately upon the issuance of the "ip access-group" command. The other configuration commands will take place as soon as the configuration file is written to memory. This is accomplished by issuing the control-Z command.

```
Router(config-if)#^Z
```

The policy is now applied but in order to make a policy that will survive a power

down you will need to write the configuration to NVRAM with the "wr" command.

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

3.5.1 Possible Vulnerabilities

There were three ACL's in the perimeter firewall policy: access list 25 which restricted login access to the router, access list 11 which performed ingress filtering, and access list 12 which performed egress filtering.

Access list 10 helps secure the login connectivity to the router as well as snmp querying. Since the only host that can telnet and do snmp queries is behind the firewall it is more unlikely that any clear text passwords or snmp communitiy strings would be sniffed. However if one of the staff machines were compromised it is possible that the clear test password and/or strings could be sniffed. Even if the password was sniffed the hacker would need to spoof the trusted machine that can telnet to the router in order for the hacker to telnet to the router. This would get extremely more complicated for someone to access the router.

Access list 11 helps keep un-necessary traffic out whether it is intentional traffic from a hacker or not. Many DoS or Scanning attempts use spoofed private address space to hide the originating machines the hacker is using. This ACL helps keep this kind of traffic from getting past the border router.

Another type of common attack is the land attacks for windows machines. This attack utilizes spoofing the victim's host address or the loopback address. The windows machine ends up sending the receiving packet to itself which causes a loop that induces a system failure. Not allowing address space from the loop back range or the internal network to ingress through the router will prevent these attacks from happening.

Access List 12 prevents any malicious traffic from being generated from the internal network. By only allowing traffic out that is sourced from the internal network this prevents a compromised machine from sending out spoofed packets other than that of the internal network.

3.5.2 ACL Testing

ACL 25:
From a machine other than the host permitted to telnet to the router

Telnet to any of the interfaces on the router
If a login prompt appears the ACL is not working
If a login prompt does not appear and you are restricted attempt to telnet from the permitted host
If a login prompt appears the ACL is working properly.
If the login prompt does not appear make sure that the machine has connectivity to the router first before double checking the ACL for any syntax errors.

ACL 11:
From a machine other than a host on the internal subnet
Run the nmap command below
If the firewall logs pick up any of the IP addresses besides the real scanner IP than the ACL has failed.
If the only IP address in the firewall logs is the real scanner IP than the ACL is functioning.

```
nmap –D 10.0.0.50,192.168.0.50,172.30.0.50,
127.0.0.1,199.0.0.50,<real scanner IP> <Internal host IP>
```

ACL 25:
In order to test this ACL a machine on the internet must be running some firewalling services with logging turned on.
From a machine on a internal network
Run the below nmap command
If the internet firewall host logs is seeing IP addresses other than that of the internal networks the ACL is not working properly.
If the firewall logs are only picking up addresses from the internal networks than the ACL is working properly.

```
nmap –D 10.0.0.50,192.168.0.50,172.30.0.50, 127.0.0.1,
<Internal host scanner IP> <Internet firewall Host>
```

4 Assignment 3 – Audit Your Security Policy

4.1 Auditing the Firewall

The following Steps have been taken from Lance Spitzner guide, Auditing Your Firewall Setup, (Spitzer, 2000).

- Verify firewall OS Integrity
- Re-visiting the security policy that the firewall is implementing
- Verify firewall is enforcing security policy
- Evaluate results and propose corrective measures

Considerations:

Make sure that the scanning portion of the security audit is done during off hours so not to cause any un-necessary load during peak network traffic times. Scanning during off hours will also help in preventing the logs from getting extraneous data from other sources than your scanning machine. Some types of scans are classified as aggressive and may result in heavy network usage and even system down time if vulnerabilities are found in your network. If this is a current production network please make sure to schedule the times with the necessary personnel during the hours you will be scanning.

In order to make sure the scanning data is useful during analysis it is important to make sure the logs contain accurate date and time stamps.

Tests
A comprehensive firewall audit will include the following objectives:
port scans
vulnerability scans
log file review
OS configuration examination
data analysis
follow-up tests
documentation

Duration:
Even the small network and handful of firewall rules we are working with would take about a weeks worth of time to thoroughly complete the previous objectives. Depending on the number of firewall rules and how clear the security policies are depends on how long the audit will take. A firewall rule set may look simple at first but if the security policy needs to be re-written the audit can start turning into an overhaul effort. Just make sure you are billing hourly and have not committed to a short audit.

Tools:

Port Scanner	Nmap
Vulnerability Scanner	Nessus
Sniffer	tcpdump

4.2 Firewall OS Integrity

No matter what firewall software is loaded whether its Checkpoint or Netfilter the weakest portion of a firewall is the Operating system that is configured on it. Every default OS installation has security holes. Knowledge of the firewall software is not enough. The OS that is used must be "hardened". The SANS organization has useful step-by-step guides for "hardening" different operating systems. http://www.sansstore.org

Nokia offers a pre-hardened OS that comes with the checkpoint software. The operating system is hardened version of Unix (BSD) called IPSO. There are limited services running on the Nokia platform such as telnet. Other services can be configured depending on the application (ssh, ftp). As long as the IPSO version is not out of date Nokia will keep the newest version of OS's available with the latest security patches already built in. Installation is very simple compared to re-installing a new operating system.

To make sure the firewall is not running any services itself setup a scanner on the external side to the firewall. Make sure the scanning machine is not in any firewall rule sets and is treated as an external "Internet" host.

TCP SCAN

```
# nmap -sS –p 1-65535 192.168.10.1
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
All 65535 scanned ports on  (192.168.10.1) are:
filtered
```

UDP SCAN

```
# nmap -sU –p 1-65535 192.168.10.1
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
All 65535 scanned ports on  (192.168.10.1) are:
filtered
```

ICMP Echo requests

```
# ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1): 56 data bytes

--- 192.168.10.1 ping statistics ---
6 packets transmitted, 0 packets received, 100% packet
loss
```

There are no responses from the firewall. If there were any responses the firewall OS would need to be checked for any running services. If those services are not needed turn them off and remove the binaries for them. Rerun the port scans after this is done to verify that the services have been removed.

To verify that the firewall rules are not covering up any services that may be harmful shut down the firewall services with “fwstop”. After this is done rerun the scans. On a standard Nokia installation the scan should only come back with telnet and ICMP replies. Telnet and ICMP replies were found after shutting down the FW1 service. This should be an acceptable installation unless other applications or security policies requires this changed. If ssh is chosen to be installed this application must be maintained and all patches or upgrades should be followed closely.

4.3 Security Policy Evaluation

Verify if an existing Security Policy document was written. If there is one go through the document comparing it against the existing rule sets. Make sure the document does not contradict itself. Sitting down with the network/system administrator to go over the document may save a lot of time when a mistake was made in the original document. If this isn't verified the "correct" rule sets may be over ridden with the incorrect security policy translation.

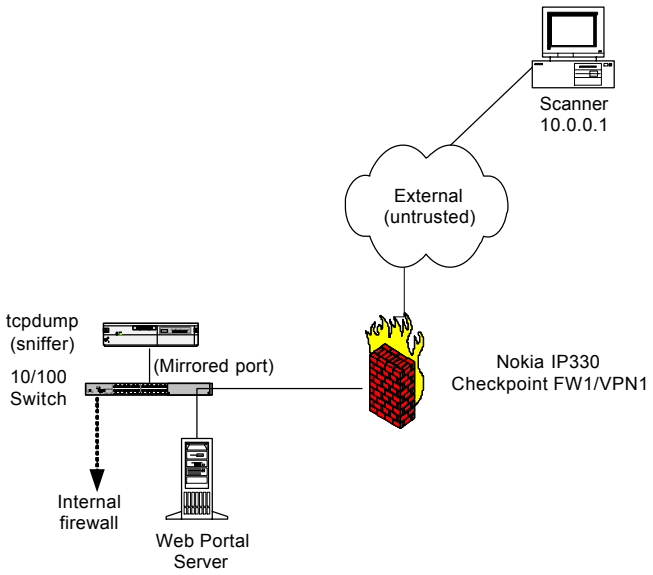
If a security policy document does not exist the network/system administrator and concerned parties need to sit down and go through a brief paraphrasing of the rule sets.

It was found after going through the rule sets one by one comparing to the security policies that some architectures may need to be changed in order to optimize the security architecture. In particular a CGI program was written on the web server to dump Fortunes into the file share on the file server via NBT. Since NBT is such a dangerous protocol to have in a network it was decided that a backend application server running Oracle could be used instead of the file share. The oracle machine could them be located on the DMZ away from the internal network. This is expanded upon more in the evaluation section.

4.4 Firewall Policy Testing

Scanning every possible variation across all protected systems would be too time consuming and costly. The best way to quickly test the firewall policies is to scan one host on each protected internal network from one external "un-trusted" host.

DMZ Network



Net-DMZ
199.0.5.0/27

TCP SCAN

The TCP scan can be accomplished with a simple nmap command. Let's scan the Web server (199.0.5.3) from an un-trusted host on the internal network (10.0.0.1):

```
# nmap -sS -P0 -p 1-65535 199.0.5.3
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (199.0.5.3):
(The 65534 ports scanned but not shown below are in
state: filtered)
Port        State       Service
80/tcp      open        http
443/tcp     open        https
```

From the nmap scan ports 80 and 443 seems to be open. When we compare this to our firewall rules this is exactly what we are allow through to this server.

UDP SCAN

Running a UDP scan to verify firewall rule sets is somewhat difficult. Since UDP packets are unreliable by design there is no certainty that the scanner can get a reliable response. The best way to see if UDP packets are getting through a firewall is to hang a sniffer off the other side near the victim hosts. This is seen in the diagram above. Since the hosts and sniffer are connected to a switch the switch had to be configured to monitor the victim host port. This topology allows UDP packets to be sent by the scanner and picked up by the sniffer if the UDP packets get through the firewall.

```
# nmap -sU 199.0.5.2
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (199.0.5.2):
All 65535 scanned ports on  (199.0.5.2) are: filtered

# tcpdump
Tcpdump: listening on pcn[x]
. . . (nothing)
```

As the above UDP scan shows nothing was allowed through the firewall. This is good!

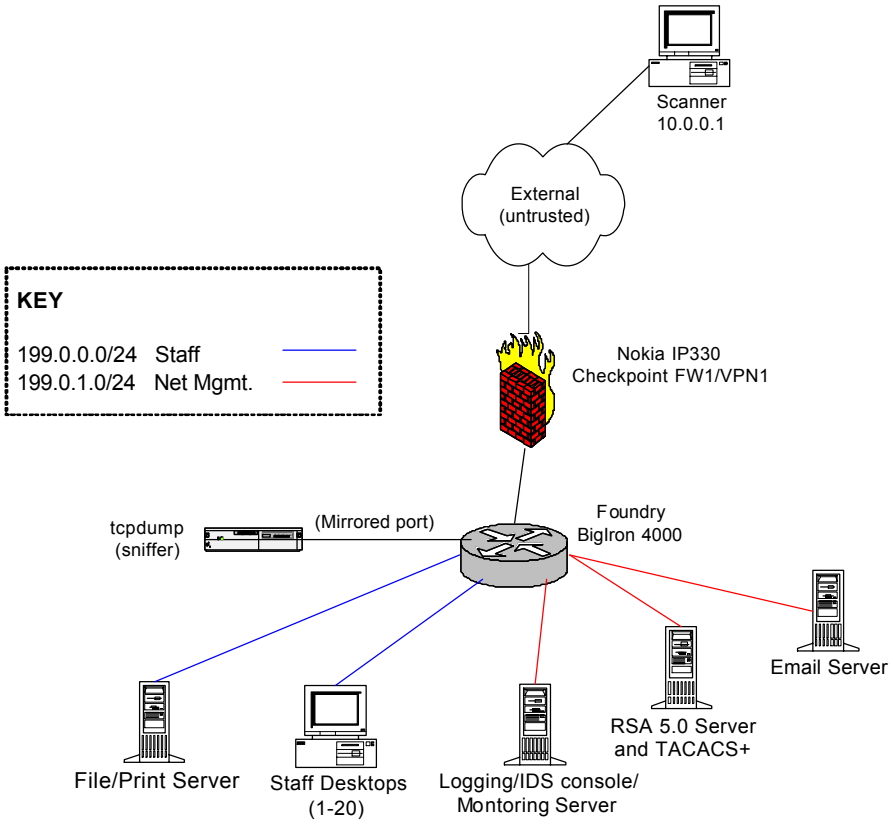
Vulnerability Scan

A very detailed audit calls for vulnerability scanning. Especially in the DMZ zone where applications like web or email may be vulnerable. This can become very dangerous if the DMZ has trusted relationships with that of the internal networks. The web server or email server can become compromised and used for a jump off point to compromise hosts on the internal networks.

Nessus was run and did find vulnerabilities on the Web server running IIS 5.0 on a Microsoft Windows 2000 Server. There was an indexing service that IIS uses that allows a hacker to run arbitrary code on the victim machine. This can ultimately give the hacker control of the web server. CERT CA-2001-13 http://www.cert.org/advisories/CA-2001-13.html

Knowing this and looking at the current rule sets the web server has NBT access to the file share. This can ultimately be disastrous to the whole internal network.

Internal Network



TCP SCAN

The TCP scan can be accomplished with a simple nmap command. Let's scan the File Server (199.0.0.2) from an un-trusted host on the internal network (10.0.0.1):

```
# nmap -sS -P0 -p 1-65535 199.0.0.2
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (199.0.0.2):
All 65535 scanned ports on  (199.0.0.2) are: filtered
```

The results of the TCP scan is understandable. There should be no access what so ever from an un-trusted machine to the intern networks.

UDP SCAN

```
# nmap -sU 199.0.0.2
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (199.0.0.2):
All 65535 scanned ports on  (199.0.0.2) are: filtered
```

```
# tcpdump
Tcpdump: listening on pcn[x]
. . . (nothing)
```

As the above UDP scan shows nothing was allowed through the firewall. This is good!

Vulnerability Scan

A vulnerability scan would not be as effective in this case since no services are running from the tcp or udp scan output. It can be run just for due diligence but don't expect much.

As expected after running a nesses scan from the "un-trusted" host to the internal networks nothing was able to be found.

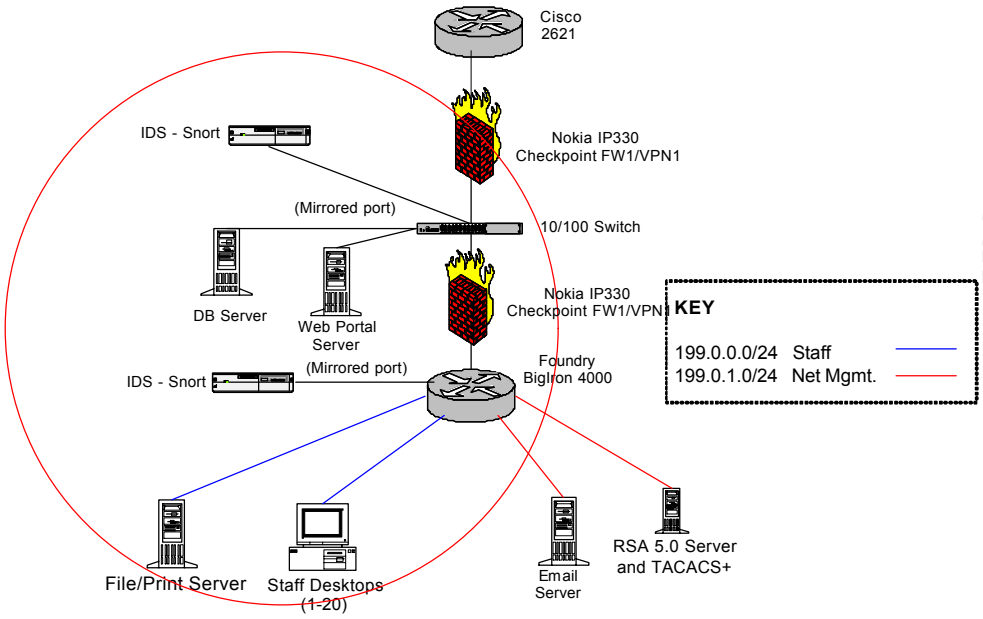
4.5 Evaluation and Recommended Corrective Measures

Noticing from looking at the security policy and scanning tests the following was found.

Web Server
From the vulnerability scan with nesses it was found that this web server needs to be patched. After this was done nesses was ran again and the vulnerability was not found again.

Security Policy and NBT
After going over the security policy it was found that allowing the web server in the DMZ to access file shares on the file server in the internal network was not a secure option. After rethinking the system architecture it was found that putting a database server on the DMZ would secure the internal network and allow a more robust relational data base architecture to keep the fortune data.

Recommended Changes



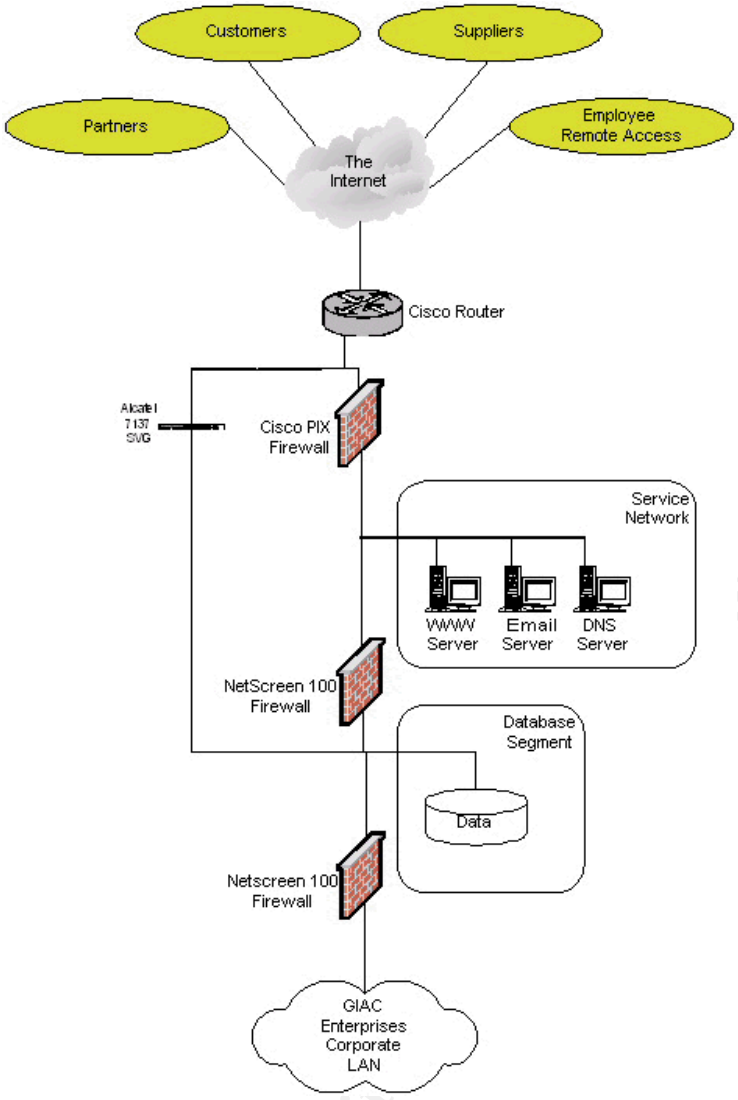
Removal of the following rule from the Checkpoint External Firewall Rule set.

Rule	Source	Destination	Service	Action	Track	Comments
3	Web	FileServer	NBT	Accept	Long	Allow backend web connection to dump to fileserver

5 Assignment 4 – Design Under Fire

5.1 Selected Network Design

The selected Network chosen to be “under fire” is the design from Brian Rickle.
http://www.sans.org/y2k/practical/Brian_Rickle_GCFW.zip



Border Router	- Cisco 4000
External Firewall	- Cisco PIX 525
Internal Firewall	- NetScreen 100
VPN	- Alcatel 7137 SVG's

5.2 Firewall Attack

After browsing through endless Cisco bug lists a few attacks were found to the Cisco PIX 525.

- **PIX SSH Vulnerability**
  Multiple SSH 3.0 attempts to the PIX can reload the PIX
  Cisco Bug# CSCdu89190
  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdu89190

- **URL Filtering Overload**
  There is a memory leak in the URL Filtering module of the PIX, which causes the PIX to consume all available memory when it is under heavy load, and the PIX is doing URL Filtering.
  Cisco Bug# CSCdr65680
  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdr65680

- **Heavy load and PAT usage**
  Under heavy usage with Port Address Translation the PIX may crash. Broadcast storms on the inside will also cause this problem.
  Cisco Bug# CSCdj22440
  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdj22440

5.2.1 PIX SSH Attack

Problem Overview

SSH Communications Client Version 3.00 for NT is not fully compatible with SSH
protocol 1.5, therefore it does not work with the PIX SSH server, which supports SSH v1.5. It fails to establish SSH connection with the PIX in both of the following scenarios:

When this client tries to connect to the PIX under the following conditions, the PIX will reload involuntarily:

- PIX is configured to allow the client host to establish SSH session with the PIX and
- PIX is configured to authenticate SSH users using AAA server(s) and
- at least one of the AAA servers configured for SSH is responsive, or

all of the AAA servers configured for SSH are down or unresponsive

Connecting to the PIX using other SSH clients, for example TeraTerm SSH, under the above conditions does not cause the PIX to reboot.

If the client host is not defined in the PIX SSH access list, the client will not reach the authentication stage.

Assessment

In order to see if the PIX is running SSH an nmap scan should be done. The design documentation details that the PIX should be accessible via SSH. No ACL's look like they were created for management access to the PIX so if ssh is running it should be accessible from anywhere.

TCP Scan

```
# nmap -sS <PIX IP>
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (PIX IP):
(The 65534 ports scanned but not shown below are in
state: filtered)
Port        State      Service
22/tcp      open       ssh
```

Attack

Now that ssh is confirmed reachable from the scanning workstation all that is left to do is download the SSH Communications Client Version 3.00 for NT. Once some simple tweaks have been made to script a sing session into a loop multiple ssh sessions can now be sent to the PIX. Even though the PIX will not be able complete the session the vulnerability lies in having a session started under a quasi-compatible protocol version of ssh. With multiple SSH sessions open the PIX starts to roll over on command.

Mitigation

In order to avoid this type of attack the ACL's for SSH access must be very specific. Making sure that only competent network admins can access the PIX via a standard SSH client (such as SecureCRT) will prevent any problems.

5.3 DDOS Attack

With 50 evil cable bots able to unleash a DDoS attack the main victim would

probably be the Cisco Pix or the Cisco 4500 via the T1 interface. The Cisco Pix 525 claims to maintain about 280,000 sessions in its state table. Approximating, 280,000 sessions can translate into around 70,000 connections of http, ssl, smtp, and dns queries. With a standard DDoS tool it may be possible to cause outages where the bandwidth capacity is the least, namely the T1 (1.544 mb) connection from the ISP. Both DDoS attempts can be tried.

DDoS Tool - Trinoo Explanation

The DDoS attack begins when the attacker connects (to masters) via telnet to top port 27665 and enters a password (the password was "betaalmostdone" in the case examined by Dittrich). Masters then pass command lines to daemons via UDP port 27444. These commands are password protected and are of the form: arg1 password arg2. Daemons respond to masters on UDP port 31335. Masters form a list of alive daemons by listening for the text "*HELLO*" in the data portion of UDP packets originating from daemons.

Attackers can send a number of commands to masters. Examples are:

```
quit - to logoff from the master
dos IP - to launch a DDos attack against the address IP
mdos <IP1:IP2:IP3> - to launch a multiple DDos attack
bcast -  to form a list of started daemons
```

Masters can send commands to daemons according to what the attacker has ordered. For example:

```
aaa password IP - Dos attack address IP by sending UDP packets to
random (0-65534) UDP ports.
bbb password N - Period of time in seconds to run Dos attack.
rsz N - Set size of UDP packets to N bytes.
d1e - Shutdown the daemon
```

Cisco PIX

To drive the number of connections to 70,000 you could configure
1/3 of the zombies to repeatedly attempt to connect to the web server on port 80, allow the 3 way handshake to complete and then just keep the connection open until it times out.
1/3 of the zombies to attempt the same thing over port 443 to the web server
1/6 to attempt the same thing over port 25 to the SMTP server
1/6 to run UDP DNS queries

Since the bots are creating a new connection attempt each time with a different source port, the firewall will have to build and maintain keep a separate entry in the state table until the session times out and gets reset.

Since there are 50 zombies and only room for 70,000 entries allowed in the

state table, each zombie only has to create and keep 70,000 / 50 or 1400 sessions.

100 bytes of upstream data to establish a single connection, that's 800 bits of data per connection.

Since each zombie needs to create 1400 of these connections at 800 bits per connection for a total of 1,120,000 bits of data. Let's call that 1.2 Mb.

Since most cable modems give you 256Kb/sec of upstream bandwidth it should take just a few seconds or possibly minutes (depending on latency issues) to fill up the state table and start causing all kinds of problems.

Many toolsets exist to implement this kind of attack. A standard DDoS exploit like Trinoo or mstream can be used. Since these tools usually come "pre-packaged" for sending UDP packets at random ports the source code would need to be tweaked to focus on the open TCP ports 80,443,25 and UDP port 53. Once this is done the attack command from Trinoo would look something like:

```
mdos <web server ip>:<dns server ip>:<email server ip>
```

Another method instead of tweaking the Trinoo source code would to utilize a Trojan such as Subseven in order to execute a simple script on all the zombies. The script would be written to open up TCP and UDP connections towards the 3 servers.

Cisco Pix Mitigation

There are several things you could try as a countermeasure:

- You could increase the number of connections allowed in your state table.
- You could block the source IP's at the perimeter router.
- You could try to get the ISP to block the activity or disable the user's cable modem connection since the source IP's are not spoofed.

Cisco 4500 Router

In order to saturate the T1 link connected to the Cisco 4500 the Trinoo exploit can be ran "off the shelf" as long as the traffic generated by the 50 zombies totals over 1.54 mb. Since the router is not configured for QoS for any vital services even if the total aggregate bandwidth from the zombies is 70% or more there will be noticeable decrease is service to the web, dns, and email servers.

A simple command to start a UDP flood across random ports using Trinoo would be:

Attacker command to Master:

```
dos <web server IP>
```

Master Command to daemons:

`aaa gi@c <web server IP>`	Sends UDP traffic across random ports (0-65534)
`bbb gi@c <1000>`	1000 sec attack duration
`rsz <1000>`	Sends 1,000 Bytes of per UDP packet

Cisco 4500 Mitigation

Several methods can be tried against this kind of "brute force attack". Finding out the zombie source IP addresses and service type ports via a sniffer or netflow collector can be a good starting point. With this information it can be seen that the Trinoo attack is using all UDP ports. Working with the upstream ISP to put UDP ACL's on their routing interfaces to only allow UDP port 53 can get rid of any saturation problems that the attack is causing. With the source IP's the ISP's that own the space (IP registrar lookup) can be notified of compromised zombie machines on their network.

Bibliography

Scambray, J., McClure, S., & Kurtz, G. (2001). Hacking exposed: Network security secrets & solutions (2nd ed.). Berkeley, CA: Osborne/McGraw Hill.

Deraison R. (2000). Nessus Documentation [Web Page] URL http://www.nessus.org/documentation.html

Fyodor. (2001). Nmap network security scanner man page [Web page] URL http://www.insecure.org/nmap/nmap_manpage.html

Sanford, Brad (2001). Practical Assignment For GIAC Firewall and Perimeter Protection [On-line Word Document] URL http://www.sans.org/y2k/practical/brad_sanford_gcfw.doc

SecurityFocus. (2001). Vulnerabilities - Check Point Firewall-1 [Web Page] URL http://www.securityfocus.com/cgi-bin/vulns.pl

Spitzner L. (2000). Auditing Your Firewall Setup [Web Page] URL http://www.enteract.com/~lspitz/audit.html