Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs

Practical Assignment

Version 1.6

For

Track 2 – GCFW SANS Parliament Hill

August, 2001

Submitted by: Dave Weir

Table of Contents

Assignment 1 – Security Architecture

Define a security Architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookies. Your architecture must include the following components:

- filering routers;
- firewalls;
- VPNs to business partners;
- secure remote access; and
- internal firewalls.

Your architecture must consider access requirements (and restrictions) for:

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

Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

Information Gathering

The very first step in any design process is to find out the exact requirements for the design. After meeting with the CEO, CIO, and Network Administrator for GIAC Enterprises I learned the following information:

- The Network Administrator is familiar with and has experience working with Cisco products;
- GIAC Enterprises are a relatively small company with a restricted budget but realize the importance of Information Security;
- GIAC Enterprises have a single office with approximately 60 employees of which about 20 people require remote access;
- The remote access users do not travel and only require access from their homes;
- GIAC Enterprises have three suppliers all of whom are located in North America;

- GIAC Enterprises suppliers need to connect to supply fortunes using a proprietary software package that uses TCP port 4004;
- GIAC Enterprises has four partners whom are all located in countries that allow DES to be imported and used;
- GIAC Partners need to connect to translate fortunes in order to resell them internationally;
- GIAC Enterprises has to provide web access to the public to provide general information to potential customers as well as provide secure web access to existing customers to allow them to purchase fortunes;
- GIAC Enterprises takes the privacy of their employees' personal information very seriously and wishes to insure that only the HR department has access to this information;
- GIAC Enterprises realizes the importance of their customer information and billing information which must only be accessible by people in the accounting department;
- All employees require the ability to send and receive e-mail;
- All employees require the ability to have both http and https web access;
- Both the CEO and CIO support the idea of limiting employees' access to non business related applications such as Real Audio and IRC to conserve bandwidth and limit risk.

Architecture Design

Vendor Selection

The first step in the design process is to select a hardware vendor for each of the required pieces of our design. I have decided to go with Cisco as the vendor for all our network infrastructure. While there is some risk associated with using similar products from the same vendor in all our layers where by a vulnerability could exist in all our hardware layers at the same time, it is outweighed by the advantages.

I acknowledge that it would be far more unlikely that the same vulnerability would exist in two firewalls using different technology and operating systems from two different vendors at the same time. However since the current Network Administrator has experience with Cisco hardware I feel the risk of introducing new hardware for him to have to manage increases the chance of making configuration errors which represent a much more significant security risk.

Also since the budget is tight I feel the limited budget would be better spent on hardware as opposed to increased training required by introducing hardware they have no experience with.

Standardizing on a single vendor will also decrease support requirements, sparing, and the time required to stay on top of new vulnerabilities.

Security Architecture

Your architecture must take all aspects of your network into consideration and mitigate the risks associated with your requirements. Security has to be a balance between business requirements and risk.

Based on the information that I learned from my meeting with GIAC Enterprises I will build a network model that balances security against their business requirements. The first step of building the architecture is to write a security policy and get agreement from upper management to enforce the policy. The policy must clearly indicate what is and is not acceptable as well as who is responsible for each item outlined in the policy.

While the implementation and details of many of the items in the security policy are outside the scope of this document I will mention the type of things that must be considered and addressed in the security policy. Some of these items also play a key role in the layout of the network. Many companies use the VISA "Twelve Commandments"[1] as a starting point for their security policies

Four common threats are vulnerable services, insider information, poor access control, and virus payload[2]. Your security policy should address these threats and take steps to mitigate them. You also must keep in mind that the security policy will be a living document and need to be maintained and updated as risks or business requirements change.

The security policy must address the following:

Firewalls

A firewall must be installed and maintained to protect data from the Internet. There must be clear definition of what traffic is acceptable and who is responsible for enforcing and maintaining the firewall rule set. The policy should also cover any other data that needs to be protected internally. We will look at this section of the policy in more detail in the firewall policy section. The policy should also indicate the punishment for internal attempts to bypass the firewall as well as the process for dealing with external attempts.

[1] VISA ***Cardholder Information Security Program*** consisting of 12 basic requirements for protecting Visa cardholder information.`http://www.visabrc.com/doc.phtml?2,64,932,932a_cisp.html`
[2] Firewalls 101: Perimeter Protection with Firewalls Page 1 - 6

Security Patches

The security policy should also consider the need to track patches and updates. It should name the people responsible for tracking patches and the means by which they are tracked. It should also define the process and time frame in which patches must be installed on all affected equipment.

.

Data Encryption

The security policy should also indicate the encryption required for any data that passes over public networks. It should also indicate any other data that must be encrypted and the minimum levels. We will look at this in more detail in the VPN section.

Anti-Virus Protection

The security policy should address the type of Anti-virus software to be ran and at what points it is implemented. It must also address who is responsible for insuring it is kept up to date.

Restrict Data Access

The security policy should restrict access to data on a need to know basis. It should indicate who is responsible for securing data by user or group. It should also detail the process by which someone is approved access to certain data.

User ID's

The security policy should state that everyone must have a unique ID and password. It should set minimum lengths and rules for passwords. It should define the process by which new ID's are approved and assigned. It also should set the process by which passwords are reset and given to the user. It should also define that vendor supplied passwords are changed.

Logging

The security policy should indicate the level of logging required and who is responsible for checking logs. Access to data must be logged to allow for accountability. It also must define what else needs to be logged in addition to access of data such as changes to security settings etc.

Testing and Auditing

The security policy should indicate the frequency and process for testing and auditing all systems and processes.

Physical Access

The security policy should indicate the physical security used to restrict access as well as defining the process by which people are granted access to equipment rooms, etc.

Server and Workstation Deployment

The security policy should indicate the process for installing new desktops and servers. It should detail what software is to be installed, patches to be applied, etc. It should also detail how to secure the box by listing what services are to be disabled, etc. There are several useful guides for securing different operating systems such as SANS Step by Step guides as well as "TSS/NSA Windows NT Security Guidelines"[3] and "Linux Administrators Security Guide"[4].

Backups

The security policy should indicate the process and timing for backups. It should cover when they are done, how long they are kept for, where they are stored, and who has access to them. It should also include the process for testing backups/restores and the frequency of the tests.

Infrastructure

Screening Router

For the first layer of defense for GIAC Enterprises I selected a Cisco 3620. This router is placed at the edge of GIAC's network and will be used to do stateful packet filtering. It is running Cisco IOS 12.2T and will be used to filter any packets that should not be entering our network. This will remove a large amount of traffic from ever having to be processed by their firewall.

Primary Firewall

For the primary firewall I have selected a Cisco PIX 515UR firewall running PIX OS 6.0. It is configured with five 10/100 interfaces and will be used to do stateful inspection to protect the service network, the supplier extranet, the partner extranet, and the corporate LAN.

[3] An NT security guide available at //www.trustedsystems.com/downloads.htm
[4] A Linux Security Guide available at //www.freek.com/lasg/lasg-0-1-7.pdf.

Internal Firewalls

I have selected two Cisco PIX 515R firewalls running PIX OS 6.0 with two 10/100 interfaces to protect internal segments of the corporate LAN. One is placed in front of the HR segment to protect HR information from anyone who is not a member of the HR department. The second is placed in front of the Accounting segment to protect accounting information from anyone who is not a member of the accounting department.

Secure Remote Access

Since users only need remote access from their homes and it has been determined that each lives in an area that can be serviced by high speed Internet access either with Digital Subscriber Line (DSL) from the Incumbent Local Exchange Carrier (ILEC) or cable modem from the Competitive Local Exchange carrier (CLEC). I have decided to use the primary firewall to terminate IPSEC tunnels from their homes to grant them remote access. Each user will be provided with a Cisco 806 Router which is designed for use with either access method to allow companies to standardize on a broadband router.

This increases security because the IPSEC tunnels are coming from specific predetermined IP addresses and because the hardware devices provide protection to the home machines thus preventing someone from hacking the home machine and tunneling in to the corporate LAN from it.

This also eliminates problems associated with having to install software on home machines and support issues that arise from supporting home machines.

Supplier / Partner VPN Access

I have selected to use the primary firewall to terminate IPSEC tunnels from suppliers and partners as well.

Suppliers will connect over an IPSEC tunnel between their IPSEC device and the outside interface of GIAC's primary firewall. Since all three suppliers are located in North America and are eligible to use 3DES that will be the encryption used. There will be a separate subnet for the Supplier Extranet which will allow GIAC to both log access and/or restrict access by suppliers to this network. They will be limited to the ports required for their proprietary software. Devices and data on the supplier Extranet will be limited to supplier required systems such as the server that runs the proprietary software that the suppliers connect to deposit fortunes. GIAC employees retrieve the fortunes from the supplier Extranet and enter them in the cookie database that resides on the internal GIAC network.

Partners will also connect over an IPSEC tunnel between their IPSEC compliant device and the outside interface of our primary firewall. Since all four partners are not eligible to use 3DES because of the countries they are in they will have to fall back to DES encryption instead of 3DES. There will be a separate interface and subnet for the partner extranet. Partners access will be logged but not restricted to this subnet. Devices and data on the partner extranet will be limited to systems and information required by partners. This extranet will be home to an Intranet server that provides information to partners, a file server which houses shares that GIAC employees will place fortunes for partners to download for translation on, and a file server with shares for partners to upload translated fortunes to. GIAC employees will retrieve translated fortunes from this Extranet and enter them into the fortune database on the internal network. Other tools and information for partners will also be located on this network segment.

Protected Service Network

Servers that the public are required to have access to are located on the service network which also has it's own interface off the primary firewall. This network will be home to a mail server, and the external DNS server which will be part of the split DNS implementation.

It will also be home to the web server which will provide web access to the general public and will provide secure web access using SSL to existing customers. Existing customers will place orders for fortunes by connecting to the web server using ssl and filling out online order forms. The online forms once completed send notification to a GIAC employee who retrieves and fills the order.

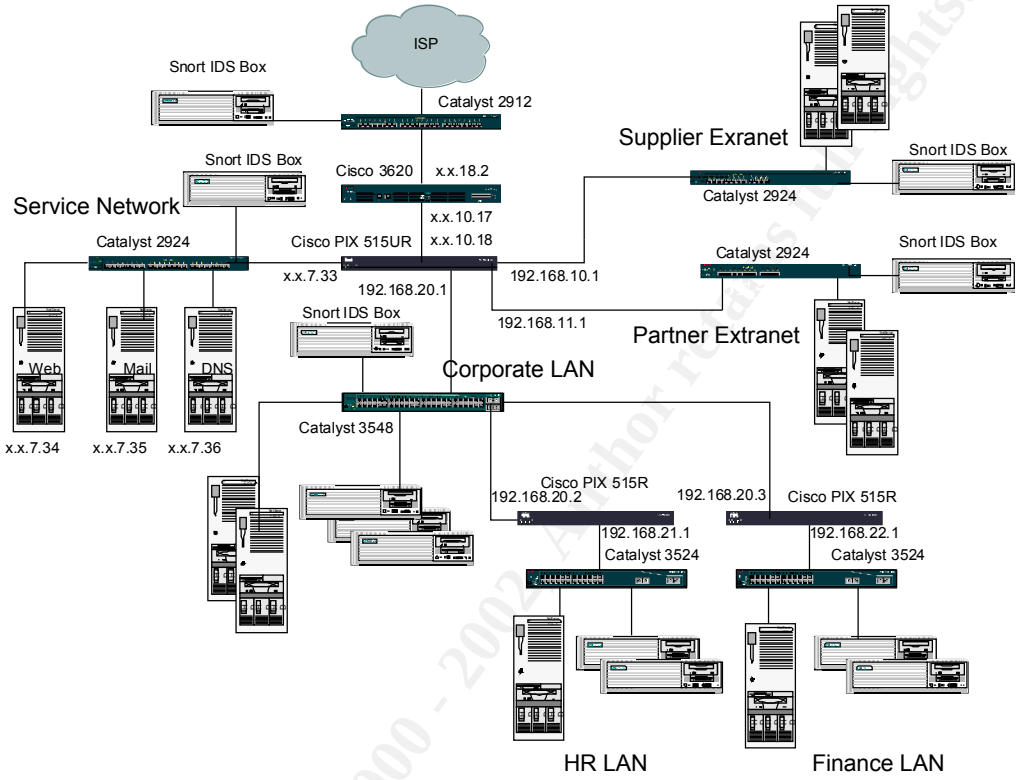
Internal Corporate Network

The Internal corporate network will be home to all internal GIAC servers and workstations and will be located on an interface off the primary firewall as well.

The internal corporate network will not be accessible from any other segments except for return traffic from sessions initiated from the internal network. It will contain the internal DNS servers, file servers, and the "Fortune Database". It will also contain all the workstations, printers, etc. that are used by GIAC employees.

GIAC employees will perform their day to day functions from this network segment including retrieving fortunes from the supplier network to be entered into the "Fortune Database", placing fortunes to be translated on the partner segment, retrieving fortunes that have been translated from the partner segment to be entered in the database, filling customer orders for fortunes, and other related duties such as answering mail messages, etc.

Network Diagram for GIAC Enterprises



Assignment 2 – Security Policy

Part 1 – Define Your Security Policy

Based on the security architecture that you derived in Assignment 1, provide a security policy for at least the following three components:

- Border Router
- Primary Firewall
- VPN

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

By 'security policy' we mean the specific Access Control List (ACL), firewall ruleset, IPSEC policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations,

customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners – you MAY NOT simply block everything.

You must include the complete policy (ACLs, ruleset, IPSEC policy) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" etc. The policies may be included in an Appendix if doing so will help the "flow" of the paper.

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

Part 2 – Security Policy Tutorial

Select one of the three security policies defined above and write a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. A general explanation of the syntax or format of the ACL, filter, or rule for your device.
2. A general description of each of the parts of the ACL, filter, or rule.
3. A general explanation of how to apply a given ACL, filter, or rule.
4. For each ACL, filter, or rule in your security policy, describe:

   • the service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.

   • any relevant information about the behavior of the service or protocol on the network.

   • if the order of the rules is important, include an explanation of why certain rules must come before (or after) other rules.

5. Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

Be certain to point out any tips, tricks, or potential problems ("gotchas").

Border Router

I will be using the border router to eliminate all traffic that GIAC Enterprises does not wish to allow into their network. By using our border router's built in stateful packet filtering we will prevent a large amount of unwanted data from ever reaching our

firewall. This will free up resources in our firewall to enable it to terminate our VPN tunnels in addition to it's firewall function.

The only inbound traffic that the policy will allow into GIAC's perimeter is:

- IPSEC traffic to the outside interface of the firewall;
- Zone transfers from the ISP's secondary DNS server;
- DNS queries from anyone to our external DNS;
- SMTP traffic to our external mail server;
- Web traffic to our public web site;
- SSL traffic to our secure web site;
- FTP-DATA traffic to any address. Since FTP does not behave as a typical protocol it is necessary to allow ftp-data port 20 into our network Otherwise data traffic would be blocked since there is no record of an existing session using port 20 in the state table. It will be the job of the firewall to insure only valid ftp sessions are allowed into the internal network, service network or extranets.
- Any traffic that originated from the inside and has an entry in the state table.

In order to be a good Internet neighbor and to help GIAC identify abnormal behavior on it's network the border router will also perform egress filtering.

Therefore the only outbound traffic that the policy will allow is:

- Traffic with a source address from valid GIAC address space

In addition the border router will have additional configuration to improve security. This additional configuration will take into consideration such things as:

- Password Management – Steps will be taken to set and encrypt password
- Warning Banners – A banner will be displayed when people connect to the router
- Management services – Steps will be taken to disable SNMP, restrict vty access to telnet sessions from inside GIAC's network and to disable the built in HTTP server.
- Logging – Steps will be taken to implement logging
- Anti-Spoofing – Steps will be taken to block addresses that are known to be invalid
- Directed Broadcasts – Steps will be taken to prevent directed broadcasts which can be used for Smurf like attacks on other networks
- IP source routing – Steps will be taken to prevent IP source routing
- ICMP Redirects – Steps will be taken to prevent ICMP redirects

- Packet Floods – Steps will be taken to prevent the router from spending so much time responding to interrupts that no other work gets done
- Unnecessary Services – Steps will be taken to eliminate unnecessary services because any service can become a vulnerability in the future and attacks exist currently for some services such as ports below 20 such as the echo service or chargen.
- ICMP error messages – Steps will be taken to prevent the router from providing to much information to people probing the network by silencing ICMP unreachable messages.

In order to configure the border router a console cable must be connected to the console port using a terminal application such as hyperterminal configured for 9600 bits per second, 8 data bits, no parity, and 1 stop bit. Once connected you must type "enable" and press enter to be placed in privileged mode, followed by typing "config t" to be placed in configuration mode. The following is the complete configuration file for the border router with each command preceded by comments explaining that line. The comments start with an exclamation mark which lets the router know to ignore it. Once in configuration mode you would enter these commands line by line to implement the desired policy or you could simply paste the entire config file into the terminal application window.

Border Router configuration:

```
version 12.2T
! Disables the parser cache which is on by default since 12.1(5)T This feature was
! designed to increase load time for large config files. Disabling it frees the resources it
! consumes in memory
no parser cache
! Disables the ability to reload a single line card only applicable on a 7500, off by
! default
no service single-slot-reload-enable
! helps alleviate congestion in large networks caused by small TCP packets off by
! default
service nagle
! all PAD and associated commands are disabled, they are enabled by default
no service pad
! disables finger service, unnecessary service that can be used to gain information about
accounts logged into the router
no ip finger
! disables small services tcp ports under 20, these are unnecessary services that may be
! exploited such as echo, and chargen, Off by default since IOS 12.0 but since it is
! difficult to track what default settings are for the various releases I enter all the
! settings I want instead of sorting out whether they are on or off for a particular
! release. It is also possible Cisco in the future may turn them back on
```

```
no service tcp-small-servers
! disables small services udp ports under 20, unnecessary services that there are known
! exploits for such as chargen, echo, daytime, etc, Off by default since IOS 12.0
no service udp-small-servers
! No timestamps by default, enables timestamps for debug and logging and includes
!  milliseconds the local time and the time zone
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
! encrypts the passwords scrambling them to prevent someone from reading them
! over your shoulder or reading them off a printed version of the config
service password-encryption
! Sets a hostname
hostname GIAC_Enterprises
! limits logging to the console to 10 per second except errors, no limits by default
logging rate-limit console 10 except errors
! indicates that process-level tasks are to be handled no less frequently then every 500
! milliseconds. Prevents too many interrupts to get any work done caused by packet
! floods
scheduler interval 500
! sets an enable secret password, stronger encryption then older enable password
enable secret 5 $1$yOkj$ofXuU1Rd8n7HIH18pe3.y.
! default setting, sets 25% DRAM for I/O leaving the other 75% for processor
memory-size iomem 25
! sets the timezone to Newfoundland Standard Time which has a minus 3 hour and 30
! minute offset from UTC
clock timezone NST -3 30
! sets daylight savings time to Newfoundland Daylight Savings Time using the US rules
clock summer-time NDT recurring
! disabled by default, enables the ability to configure and route to subnet 0
ip subnet-zero
! prevents source routing which prevents the packet from choosing the routed path
no ip source-route
! disables bootp server, unnecessary service which may be exploited. If a service is not
! running it can not be attacked and frees resources it would use if started.
no ip bootp server
! prevents the router from sending out dhcp requests to get DNS and netbios server
! information
no ip dhcp-client network-discovery
! Configure interface FastEthernet 0 in slot 0
interface FastEthernet0/0
! Displays the description “Internal LAN” for this interface
 description Internal LAN
! Sets the IP address and netmask for this interface
 ip address x.x.10.17 255.255.255.240
! disables the sending of icmp redirect messages
```

```
 no ip redirects
! disables the translation of directed broadcast to physical broadcasts which prevents
! you from becoming a smurf amplification site
 no ip directed-broadcast
! sets the speed to 100M
 speed 100
! sets the duplex to full
 full-duplex
! Configure interface FastEthernet 1 in slot 0
interface FastEthernet0/1
! Displays the description "Internet" for this interface
 description Internet
! Sets the IP address and netmask for this interface
 ip address x.x.18.2 255.255.255.240
! Applies the named access list "filtrin" to traffic entering this interface
 ip access-group filterin in
!Applies the named access list "filterout" to traffic exiting this interface
 ip access-group filterout out
! disables the sending of ICMP redirects
 no ip redirects
! disables the translation of directed broadcast to physical broadcasts
 no ip directed-broadcast
! disables the generation of ICMP unreachable messages which can be used to map
! your network and makes it harder for users to detect your router or devices behind it
 no ip unreachables
! Sets the speed to 10 M
 speed 10
! Sets the duplex to full
 full-duplex
! Disables Cisco Discovery Protocol, unnecessary service, may hand out useful
! information to attackers
 no cdp enable
! Prevents this interface from receiving NTP (Network Time Protocol) packets,
! unnecessary service which may be exploited
ntp disable
! Enabled by default since 11.3, allows for classless routing, required for VLSM
ip classless
! Sets the default route to be the ISP router's interface x.x.18.1
ip route 0.0.0.0 0.0.0.0 x.x.18.1
! Disables the HTTP server built into the router, unnecessary service and the router
! should only be configurable from the console via telnet from the internal network
no ip http server
! Disables SNMP, unnecessary service which can be exploited. It's only authentication
! method is an unencryped  community string. Attackers could use SNMP to gather
! information, change configuration parameters or shut down an interface remotely
```

```
no snmp-server
! Creates a named access list called "filterin"
ip access-list extended filterin
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-9
deny ip 1.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-2
 deny ip 2.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-5
 deny ip 5.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-6
deny ip 10.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-23
 deny ip 23.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-10
 deny ip 27.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-12
 deny ip 31.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-36
 deny ip 36.0.0.0 1.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-39A
 deny ip 39.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-41A
 deny ip 41.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-42
 deny ip 42.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA Block (Returned to IANA Mar 98)
deny ip 49.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA Block (Returned to IANA Mar 98)
deny ip 50.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-58 and
! NET-RESERVED-59
 deny ip 58.0.0.0 1.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-60
 deny ip 60.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-7
 deny ip 69.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-7
 deny ip 70.0.0.0 1.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-7
 deny ip 72.0.0.0 7.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-11
 deny ip 82.0.0.0 1.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-11
 deny ip 84.0.0.0 3.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-11
```

```
 deny ip 88.0.0.0 7.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-8 and
! LOOPBACK
 deny ip 96.0.0.0 31.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved RESERVED-3
deny ip 128.0.0.0 0.0.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved NET-TEST-B
deny ip 128.66.0.0 0.0.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-LINKLOCAL
 deny ip 169.254.0.0 0.0.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block IANA-BBLK-
! RESERVED
 deny ip 172.16.0.0 0.15.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-4
deny ip 191.255.0.0 0.0.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-2
deny ip 192.0.0.0 0.0.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-IANA-192
deny ip 192.88.99.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block IANA-CBLK-
! RESERVED
 deny ip 192.168.0.0 0.0.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! 13
 deny ip 197.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-DLW
deny ip 199.103.97.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-DLW
deny ip 199.103.98.0 0.0.1.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
!  FOR-DLJ-SAS
deny ip 199.103.109.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-DLJ-SAS
deny ip 199.103.110.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! 14
 deny ip 201.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-FOR-
! GE-FANUC
 deny ip 204.79.12.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-
! JOHNSON-CONT
```

deny ip 204.231.25.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-INFORMIX3-133
deny ip 204.231.133.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESERVED-
! ROUTE1
deny ip 204.231.141.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-RESFOR-
! NORTHERN-TRUST
deny ip 204.231.229.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-INFORMIX
deny ip 204.231.242.0 0.0.1.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-INFORMIX
deny ip 204.231.244.0 0.0.1.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-INFORMIX
deny ip 204.231.246.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-KYMMENE1
deny ip 205.248.0.0 0.0.3.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-RESERVED-
! FOR-KYMMENE1
deny ip 205.248.4.0 0.0.1.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-207-211-089-
! 000-24
deny ip 207.211.89.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-CF-D3-5F-80-
! 26-99026
deny ip 207.211.95.128 0.0.0.63 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-113
deny ip 209.197.196.224 0.0.0.31 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-170
deny ip 209.197.220.24 0.0.0.7 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-148
deny ip 209.197.212.192 0.0.0.31 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-151
deny ip 209.197.215.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-159
permit ip 209.197.218.0 0.0.0.63 any
permit ip 209.197.218.240 0.0.0.15 any
deny ip 209.197.218.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-163
permit ip 209.197.219.0 0.0.0.15 any
permit ip 209.197.219.216 0.0.0.7 any

```
deny ip 209.197.219.0 0.0.0.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-218B
permit ip 209.197.224.192 0.0.0.0 any
deny ip 209.197.224.192 0.0.0.15 any
deny ip 209.197.224.208 0.0.0.0 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-5
 deny ip 219.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-5
 deny ip 220.0.0.0 3.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block NET-MCAST-NET  and
IANA reserved
 deny ip 224.0.0.0 31.255.255.255 any
! Prevent spoofing, blocks traffic from IANA reserved Block RESERVED-1
 deny ip 0.0.0.0 0.255.255.255 any
! Prevent spoofing, blocks traffic from GIAC's own address space
deny ip x.x.10.16 0.0.0.15 any
deny ip x.x.7.32 0.0.0.31 any
! Permit ISAKMP packets to reach the outside interface of the firewall to allow key
! exchange and create tunnels for encrypted VPN access
 permit udp any host x.x.10.18 eq isakmp
! Permit ESP packets for IPSEC to reach the external interface of the firewall to allow
! the exchange of encrypted data between the VPN peers
 permit  esp any host x.x..10.18
! Permit DNS queries from any IP address to the DNS server on the service network to
! allow people to access the DNS servers for name resolution of GIAC public devices
 permit udp any host x.x.7.36 eq domain
! Permit the secondary DNS server to do zone transfers from the DNS server on the
! service network to allow it to stay synchronized with the primary when records are
! added, deleted or changed
 permit tcp host x.x.1.100 host x.x.7.36 eq domain
! Permit any IP address to access the Web server using http to allow the general public
! to browse the web site
 permit tcp any host x.x.7.34 eq www
! Permit any IP address to connect to the web server using SSL to allow any existing
! customers to connect using SSL to securely fill out online order forms to place orders
! for fortunes
 permit tcp any host x.x.7.34 eq 443
! Permit any IP address to access the mail server on port 25 to allow the general public
! to send mail messages to GIAC employees
 permit tcp any host x.x.7.35 eq smtp
! Permit any IP address to pass through the router on port 20. This is required because
! ftp does not behave like other tcp protocols. When a client connects to an ftp server on
! port 21 and sets up a control channel the ftp server responds from port 21 to the client
! port as per normal tcp interaction. However the server then tries to connect to the
! client from port 20. Without this rule this traffic would be discarded because there
```

```
! was no initiating traffic that went out to port 20 from the client
 permit tcp any any eq ftp-data
! Permit any traffic to pass through the router that has a corresponding entry in the
! state table named packets this allows any return traffic to sessions initiated from
! inside GIAC's address space
 evaluate packets
! Create a named access list called "filterout"
ip access-list extended filterout
! Permit all IP traffic from the service network to exit the router and enter it in the state
! table named packets to allow return traffic from this session back into GIAC's
! network
 permit ip x.x.7.32 0.0.0.31 any reflect packets
! Permit all IP traffic from the outside interface of the firewall to exit the router and
! enter it in the state table named packets to allow return traffic from this session back
! into GIAC's network
 permit ip x.x.10.16 0.0.0.15 any reflect packets
! Permit all IPSEC traffic using protocol 50 or esp from the firewall outside interface to
! anywhere which allows encrypted data from the firewall to it's remote VPN peers
 permit esp host x.x.10.18 any
! Implicit deny at end which drops all other traffic
! Creates an access list to limit who can telnet to the router
access-list 10 permit x.x.10.16 0.0.0.15
access-list 10 permit x.x.7.32 0.0.0.31
! Creates a banner to be displayed when people connect to the router required for legal
! reasons to be able to prosecute unauthorized people who attempt to connect
banner motd ^CCCCCC
---------------------------
STOP: Authorized access only!
---------------------------

This system is available only to authorized personnel of GIAC Enterprises
Please disconnect immediately unless you have been specifically authorized to
connect to this terminal by GIAC Enterprises

All connection attempts are logged
^C
! Configures the console port
line con 0
! sets a password for the console
 password 7 03034F34121C32
! require a login for console access
 login
! Configures the auxiliary port
 line aux 0
! sets a password for the auxiliary port
```

```
 password 7 050C1230355F5D
! require a login for auxiliary port access
 login
! Configure vty remote access
line vty 0 4
! restrict vty access to connections from GIAC address space by applying access list 10
 access-class 10 in
! set password for remote access
 password 7 1302032D1F1F17
! require a login for remote access
 login
!
end
```

When preparing your border router there are a couple of things to keep in mind. First, when configuring ACL's it is important to be careful of the order in which the lines occur. ACL's are processed in order, and once a match is encountered the packet is either permitted or denied based on that line, and no later lines are processed. Therefore placement becomes extremely important.

For example when blocking NETBLK-FAST-163 the block does not include all 255 addresses of 209.197.219.0. In this instance 209.197.219.1 – 15 and 209.197.219.216 – 223 are not part of a reserved block and therefore should not be denied. It is crucial in this case to permit these two ranges prior to denying the entire class c size block as follows:

```
! Prevent spoofing, blocks traffic from IANA reserved Block NETBLK-FAST-163
permit ip 209.197.219.0 0.0.0.15 any
permit ip 209.197.219.216 0.0.0.7 any
deny ip 209.197.219.0 0.0.0.255 any
```

By doing so it allows these IP addresses to match the permit rules first and be allowed into the perimeter without being matched against the deny rule. If these rules were reversed the packets from these addresses would be discarded after matching the deny rule and never reach the line that permits them. Therefore the ACL would actually block data that it should allow in. As you can see placement of the rules can drastically change the intent of the ACL and produce undesirable results.

Second you should never assume that something is configured properly without testing it. Before being implemented it should be tested to insure it is performing as expected. The following three rules have been chosen to demonstrate methods to test your rules to insure they are functioning properly.

```
! Permit any IP address to access the Web server using http
 permit tcp any host x.x.7.34 eq www
```

In order to test this rule you can use a tool called netcat which can be downloaded from http://www.infobro.com/anon-FTP/Security/Tools/netcat/nt/ . This is an extremely useful tool that can be used to make connections on any tcp port. In order to test this rule you can use netcat running on a device outside your perimeter to connect to the web server on port 80.

You do this by typing:

Nc –v x.x.7.34 80
GET / HTTP/1.0

Followed by a couple of enters.

If the rule is working you should be able to connect to the web server and see something similar to the following:

D:\net>nc -v x.x.7.34 80
www.giac.com [x.x.7.34] 80 (?) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 08 Nov 2001 01:29:16 GMT
Server: Apache/1.3.9 (Unix) PHP/3.0.12 mod_ssl/2.4.1 OpenSSL/0.9.4
Last-Modified: Fri, 22 Dec 2000 16:38:13 GMT
ETag: "d113-46-3a438375"
Accept-Ranges: bytes
Content-Length: 70
Connection: close
Content-Type: text/html

<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://www.giac.com/">

! Permit DNS queries from any IP address to the DNS server on the service network
permit udp any host x.x.7.36 eq domain

You can use nslookup from a device outside your perimeter to insure you can connect to the DNS server and resolve names. To do this you would use nslookup and set the server to be x.x.7.36 and set the type to any. You then would enter GIAC.com and you should get back records for giac.com. You can also enter www.giac.com and insure you get back the IP address for the web server. The following example shows typical results of using nslookup to confirm that you can connect to the DNS server and resolve names.

```
C:\>nslookup
Default Server:  dns1.roadrunner.nf.net
Address:  192.75.13.69

> server dns.giac.com
Default Server:  dns.giac.com
Address:  x.x.7.36

> set type=ANY
> giac.com
Server:  dns.giac.com
Address:  x.x.7.36

giac.com
        primary name server = dns.giac.com
        responsible mail addr = hostmaster.mail.giac.com
        serial  = 2001100301
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
giac.com        MX preference = 0, mail exchanger = mail.giac.com
giac.com        nameserver = dns.giac.com
giac.com        nameserver = dns.isp.com.com
mail.giac.com internet address = x.x.7.35
dns.giac.com      internet address = x.x.7.36
dns.isp.com.com      internet address = x.x.1.100
> www.giac.com
Server:  dns.giac.com
Address:  x.x.7.36

www.giac.com    internet address = x.x.7.34
giac.com        nameserver = dns.giac.com
giac.com        nameserver = dns.isp.com.com
dns.giac.com      internet address = x.x.7.36
dns.isp.com.com      internet address = x.x.1.100
```

```
! Permit any IP address to access the mail server on port 25
 permit tcp any host x.x.7.35 eq smtp
```

Finally in order to test to insure you can connect to the mail server you can again use netcat. You would once again from outside the perimeter type:

```
Nc x.x.7.35 25
```

If the rule is working properly you should be able to connect to the mail server and should see something similar to the following:

```
D:\net>nc x.x.7.35 25
220 mail.giac.com ESMTP Sendmail 8.11.6/8.11.6 (Wed, 7 Nov 2001 22:25:28 -033
0 (NST)) -- Throw down your headers and prepare to be judged
```

Once the connection is established you can either enter smtp commands to test sending a message or type quit to close the connection.

After testing all your rules, you should also keep in mind that things change rapidly so your configuration may need to be modified, updated, or changed as business needs change, new vulnerabilities are discovered, or new features are developed.

Other useful tips include using the tab key to complete commands and using the ? mark to find command options and syntax. Finally always remember to type "copy running-config startup-config" to save your configuration or else the next time the router reloads the changes will be lost.

Primary Firewall

I will be using the primary firewall to serve two roles it will restrict data into and out of GIAC's various networks as well as performing the role of terminating the IPSEC tunnels from remote users, suppliers, and partners.

The PIX by default blocks traffic from lower security interfaces to higher numbered security interfaces. Therefore the outside interface will be set to the lowest security level, followed by the service network, then the supplier, next the partner, and finally the corporate internal network will be set to the highest level. Doing this will prevent devices from lower security level segments from initiating connections to higher security segments. As a result it will only be return traffic from sessions initiated from the higher security level that will be allowed back into that segment.

GIAC trusts it's internal users and feels that there is no need to restrict them from accessing any devices on any of their network segments except for the human resources and accounting segments. Since all their systems are protected by file and directory permissions and require authentication they take no special precautions to limit the type of traffic allowed between the internal desktops and corporate servers etc. The only data that they consider confidential and restrict access to is the human resources and financial systems which reside behind internal firewalls. All data and systems on the extranet, and service networks are not considered confidential to internal employees and are not considered to be at risk from attack by internal users.

Also for the ease of maintenance and service it is considered to be more efficient if the IT staff have full access to systems on the various network segments from any PC or

device on the internal network. GIAC feels that since there is no confidential data on either of the extranets or service networks, and there is no risk of attack or malicious damage from users on the internal network that there is no need to restrict access to any of these segments from the internal segment. They feel doing so would only add complexity and load on resources without mitigating any risk and therefore is not required.

Finally GIAC feels that ftp, ssl, and http are required services from all segments. GIAC feels that the IT staff need to be able to initiate outbound connections over these protocols from any device on any of their network segments in order to efficiently download patches, updates, and other tools required to do their day to day support. GIAC feels that as long as access is restricted to these ports and initiated from inside that the benefit of timely access to needed resources out weighs the risk of allowing it. They also feel that telnet access to the router from all segments falls into this same category. They feel that restricting this access will be an impediment to the IT staff to trouble shoot and resolve issues that may arise on the varying segments. Forcing a staff member to go to a machine on the internal network to research an ongoing problem and download any relevant documentation or patch would result in costly delays to problem resolution.

As a result the PIX will be configured as follows.

The PIX will be configured to allow inbound:

- traffic from anyone to the web server on the service network using http which will allow customers and potential customers to access the public web site to learn about GIAC
- traffic from anyone to the web server on the service network using ssl which will allow customers a secure connection to place orders for fortunes
- traffic from anyone to the mail server on the service network using smtp which will allow users to send e-mail to GIAC employees
- traffic from anyone to the DNS server on the service network to do name lookups which will allow everyone to determine IP addresses for public resources such as the web server and mail server
- traffic from the secondary DNS server to the DNS server on the service network to do zone transfers which will allow the secondary DNS server to remain in synch with the primary as records are updated, added, or deleted
- traffic from anywhere that has a corresponding entry in the state table which will allow return traffic from sessions initiated from GIAC network segments
- IPSEC traffic from remote users, suppliers, and partners which will allow these users to have secure encrypted connections to their respective network segments

The PIX will be configured to allow outbound traffic from the corporate network as follows:

- http traffic from the corporate internal network to anywhere which will allow GIAC users to browse the Internet
- ssl traffic from the corporate internal network to anywhere which will allow GIAC users to browse secure web sites
- ftp traffic from the corporate internal network to anywhere which will allow GIAC users to upload and / or download files using ftp such as virus updates, software patches, etc.
- telnet traffic from the corporate internal network to the router to allow IT staff to connect to the router to troubleshoot or correct problems from any device on the internal network
- dns queries from the corporate DNS servers to anywhere which allows the corporate DNS servers to communicate with other DNS servers on the Internet in order to do name resolution for all corporate hosts
- nntp traffic from the corporate network to anywhere which allows GIAC users to read news groups
- all traffic from the corporate network to remote users network via IPSEC tunnel which allows remote users the same access to resources as if they were in the office
- all traffic from the corporate network to the supplier extranet which allows GIAC users access to all devices on this Extranet segment since GIAC feels it unnecessary to restrict this access
- all traffic from the corporate network to the partner extranet which allows GIAC users access to all devices on this Extranet segment since GIAC feels it unnecessary to restrict this access
- all traffic from the corporate network to the service network which allows GIAC users to use POP and IMAP to retrieve mail from the mail server, SMTP to send mail to the mail server, as well as any other access to any devices on this segment since GIAC feels it is unnecessary to restrict this access

The PIX will be configured to allow outbound traffic from the supplier extranet as follows:

- http traffic from the supplier extranet to anywhere which allows devices on this segment to browse the Internet
- ssl traffic from the supplier extranet to anywhere which allows devices on this segment to browse secure sites on the Internet
- ftp traffic from the supplier extranet to anywhere which allows devices on this segment to be able to upload / download files via ftp
- telnet traffic from the supplier extranet to the router allowing devices on this segment to be able to connect to the router
- dns queries from the supplier extranet to the ISP's resolver DNS servers which allows devices on this segment to resolve names to IP's for browsing, etc.
- any traffic from the supplier extranet on TCP port 4004 to suppliers via IPSEC tunnel which allows suppliers to remotely upload fortunes using GIAC's proprietary software

- any traffic from the supplier extranet to the corporate subnet that has a corresponding entry in the state table which allows return traffic to devices on the corporate segment

The PIX will be configured to allow outbound traffic from the partner extranet as follows:

- http traffic from the partner extranet to anywhere which allows devices on this segment to be used to browse the Internet
- ssl traffic from the partner extranet to anywhere which allows devices on this segment to be used to browse secure Internet sites
- ftp traffic from the partner extranet to anywhere which allows devices on this segment to be used to upload / download files via ftp
- telnet traffic from the partner extranet to the router which allows devices on this segment to be used to connect to the router
- dns queries from the partner extranet to to the ISP's resolver DNS servers which allows devices on this segment to resolve names
- any traffic from the partner extranet to partners via IPSEC tunnel which allows partners secure encrypted connections to devices on this segment. This segment contains only devices for use by suppliers such as a partner Intranet, and a file server containing shares for them to download fortunes from and upload translated fortunes to. GIAC trusts its partners and houses no information that should not be seen or used by partners on this segment and therefore logs traffic on this segment but does not restrict access. They do not believe there is any risk of partners being malicious
- any traffic from the partner extranet to the corporate subnet that has a corresponding entry in the state table which allows return traffic to the corporate segment

The PIX will be configured to allow outbound traffic from the service network as follows:

- http traffic from the service network to anywhere which allows devices on this segment to browse the Internet
- ssl traffic from the service network to anywhere which allows devices on this segment to browse secure Internet sites
- ftp traffic from the service network to anywhere which allows devices on this segment to be used to upload / download files via ftp
- telnet traffic from the service network to the router which allows devices on this segment to connect to the router
- dns queries from the service network to the ISP's resolver DNS servers which allow devices on this segment to do name resolution
- any traffic from the service network to the corporate subnet that has a corresponding entry in the state table which allows return traffic to the corporate network

- any responses from the service network to anywhere which allows the servers to respond to clients that are accessing their services
- smtp traffic from the mail server to anywhere which allows the mail server to send mail to all other companies
- traffic from the DNS server to the secondary DNS server to do zone transfers to allow them to stay synchronized when records are changed, added, and deleted

In addition the firewall will have additional configuration to improve security. This additional configuration will take into consideration such things as:

- Password Management – Passwords will be set and encrypted for telnet access and privileged mode access
- Management services – Steps will be taken to disable SNMP, and restrict telnet and ssh access to the firewall from the inside of GIAC's network
- Logging – Logging will be turned on to both a syslog server and to a buffer in memory.
- Packet Floods – Steps will be taken to protect against flood attacks
- Fragmentation – Steps will be taken to protect against fragmentation attacks such as teardrop
- Protocol inspection – steps will be taken to inspect protocols to insure only valid commands are sent

VPN on the Primary Firewall

The secondary function of the primary firewall is to terminate IPSEC tunnels for remote users, suppliers, and partners. It will be configured to use pre-shared keys via ISAKMP.

The supplier VPN will be configured as follows:

- each supplier will have it's own pre-shared key
- each supplier connection will have to match a set IP address
- they will use 3DES encryption
- they will use group 2 Diffie-Hellman which uses 1024 bit as opposed to 768 bit prime modulus which is stronger security but requires more cpu cycles
- they will use sha instead of md5 as it is has a larger digest for better security but is slightly slower
- encrypted traffic will be between the specified subnets only
- esp will be used since data confidentiality is critical

The partner VPN will be configured as follows:

- each partner will have it's own pre-shared key
- each partner connection will have to match a set IP address
- they will use DES encryption
- they will use group 2 Diffie-Hellman which uses 1024 bit as opposed to 768 bit prime modulus which is stronger security but requires more cpu cycles
- they will use sha instead of md5 as it is has a larger digest for better security but is slightly slower
- encrypted traffic will be between the specified subnets only
- esp will be used since data confidentiality is critical

The remote user VPN will be configured as follows:

- each remote user will have it's own pre-shared key
- each remote user connection will have to match a set IP address
- they will use 3DES encryption
- they will use group 2 Diffie-Hellman which uses 1024 bit as opposed to 768 bit prime modulus which is stronger security but requires more cpu cycles
- they will use sha instead of md5 as it is has a larger digest for better security but is slightly slower
- encrypted traffic will be between the specified subnets only
- esp will be used since data confidentiality is critical

Primary Firewall / VPN configuration:

```
PIX Version 6.0(1)
nameif ethernet0 outside security0
nameif ethernet1 service security10
nameif ethernet2 supplier security40
nameif ethernet3 partner security50
nameif ethernet4 corporate security100
enable password uFuWClnBygRBYNWM encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname GIAC_Ent
domain-name giac.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list acl_out permit tcp any host x.x.7.34 eq www
```

```
access-list acl_out permit tcp any host x.x.7.34 eq 443
access-list acl_out permit tcp any host x.x.7.35 eq smtp
access-list acl_out permit udp any host x.x.7.36 eq 53
access-list acl_out permit tcp host x.x.1.100 host x.x.7.36 eq 53
access-list acl_corporate permit tcp 192.168.20.0 255.255.255.0 any eq 21
access-list acl_corporate permit tcp 192.168.20.0 255.255.255.0 host x.x.10.17 eq 23
access-list acl_corporate permit tcp 192.168.20.0 255.255.255.0 any eq 80
access-list acl_corporate permit tcp 192.168.20.0 255.255.255.0 any eq 119
access-list acl_corporate permit tcp 192.168.20.0 255.255.255.0 any eq 443
access-list acl_corporate permit udp host 192.168.20.10 any eq 53
access-list acl_corporate permit udp host 192.168.20.11 any eq 53
access-list acl_corporate permit ip 192.168.20.0 255.255.255.0 192.168.50.0
255.255.255.0
access-list acl_corporate permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
access-list acl_corporate permit ip 192.168.20.0 255.255.255.0 192.168.11.0
255.255.255.0
access-list acl_corporate permit ip 192.168.20.0 255.255.255.0 x.x.7.32
255.255.255.224
access-list acl_service permit tcp x.x.7.32 255.255.255.224 any gt 1023 established
access-list acl_service permit tcp x.x.7.32 255.255.255.224 host x.x.10.21
access-list acl_service permit tcp x.x.7.32 255.255.255.224 any eq 21
access-list acl_service permit tcp x.x.7.32 255.255.255.224 host x.x.10.17 eq 23
access-list acl_service permit tcp x.x.7.32 255.255.255.224 any eq 80
access-list acl_service permit tcp x.x.7.32 255.255.255.224 any eq 443
access-list acl_service permit tcp host x.x.7.35 any eq 25
access-list acl_service permit tcp host x.x.7.36 host x.x.1.100 eq 53
access-list acl_service permit udp x.x.7.32 255.255.255.224 host x.x.1.50 eq 53
access-list acl_service permit udp x.x.7.32 255.255.255.224 host x.x.1.51 eq 53
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 eq 4004 192.168.60.0
255.255.255.0 gt 1023
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 eq 4004 192.168.61.0
255.255.255.0 gt 1023
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 eq 4004 192.168.62.0
255.255.255.0 gy 1023
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 any eq 21
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 host x.x.10.17 eq 23
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 any eq 80
access-list acl_supplier permit tcp 192.168.10.0 255.255.255.0 any eq 443
access-list acl_supplier permit udp 192.168.10.0 255.255.255.0 host x.x.1.50 eq 53
access-list acl_supplier permit udp 192.168.10.0 255.255.255.0 host x.x.1.51 eq 53
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 192.168.70.0
255.255.255.0
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 192.168.71.0
255.255.255.0
```

```
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 192.168.72.0
255.255.255.0
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 192.168.73.0
255.255.255.0
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 any eq 21
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 host x.x.10.17 eq 23
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 any eq 80
access-list acl_partner permit tcp 192.168.11.0 255.255.255.0 any eq 443
access-list acl_partner permit udp 192.168.11.0 255.255.255.0 host x.x.1.50 eq 53
access-list acl_partner permit udp 192.168.11.0 255.255.255.0 host x.x.1.51 eq 53
access-list supplier1 permit ip 192.168.10.0 255.255.255.0 192.168.60.0 255.255.255.0
access-list supplier2 permit ip 192.168.10.0 255.255.255.0 192.168.61.0 255.255.255.0
access-list supplier3 permit ip 192.168.10.0 255.255.255.0 192.168.62.0 255.255.255.0
access-list partner1 permit ip 192.168.11.0 255.255.255.0 192.168.70.0 255.255.255.0
access-list partner2 permit ip 192.168.11.0 255.255.255.0 192.168.71.0 255.255.255.0
access-list partner3 permit ip 192.168.11.0 255.255.255.0 192.168.72.0 255.255.255.0
access-list partner4 permit ip 192.168.11.0 255.255.255.0 192.168.73.0 255.255.255.0
access-list r_user1 permit ip 192.168.20.0 255.255.255.0 192.168.50.0 255.255.255.240
access-list r_user2 permit ip 192.168.20.0 255.255.255.0 192.168.50.8 255.255.255.240
access-list r_user3 permit ip 192.168.20.0 255.255.255.0 192.168.50.16
255.255.255.240
access-list r_user4 permit ip 192.168.20.0 255.255.255.0 192.168.50.24
255.255.255.240
access-list r_user5 permit ip 192.168.20.0 255.255.255.0 192.168.50.32
255.255.255.240
access-list r_user6 permit ip 192.168.20.0 255.255.255.0 192.168.50.40
255.255.255.240
access-list r_user7 permit ip 192.168.20.0 255.255.255.0 192.168.50.48
255.255.255.240
access-list r_user8 permit ip 192.168.20.0 255.255.255.0 192.168.50.56
255.255.255.240
access-list r_user9 permit ip 192.168.20.0 255.255.255.0 192.168.50.64
255.255.255.240
access-list r_user10 permit ip 192.168.20.0 255.255.255.0 192.168.50.72
255.255.255.240
access-list r_user11 permit ip 192.168.20.0 255.255.255.0 192.168.50.80
255.255.255.240
access-list r_user12 permit ip 192.168.20.0 255.255.255.0 192.168.50.88
255.255.255.240
access-list r_user13 permit ip 192.168.20.0 255.255.255.0 192.168.50.96
255.255.255.240
access-list r_user14 permit ip 192.168.20.0 255.255.255.0 192.168.50.104
255.255.255.240
access-list r_user15 permit ip 192.168.20.0 255.255.255.0 192.168.50.112
255.255.255.240
```

```
access-list r_user16 permit ip 192.168.20.0 255.255.255.0 192.168.50.120
255.255.255.240
access-list r_user17 permit ip 192.168.20.0 255.255.255.0 192.168.50.128
255.255.255.240
access-list r_user18 permit ip 192.168.20.0 255.255.255.0 192.168.50.136
255.255.255.240
access-list r_user19 permit ip 192.168.20.0 255.255.255.0 192.168.50.144
255.255.255.240
access-list r_user20 permit ip 192.168.20.0 255.255.255.0 192.168.50.152
255.255.255.240
access-list nonat permit ip 192.168.20.0 255.255.255.0 192.168.50.0 255.255.255.0
access-list nonat permit ip 192.168.20.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat permit ip 192.168.20.0 255.255.255.0 192.168.11.0 255.255.255.0
access-list nonat permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
access-list nonat permit ip 192.168.10.0 255.255.255.0 192.168.60.0 255.255.255.0
access-list nonat permit ip 192.168.10.0 255.255.255.0 192.168.61.0 255.255.255.0
access-list nonat permit ip 192.168.10.0 255.255.255.0 192.168.62.0 255.255.255.0
access-list nonat permit ip 192.168.11.0 255.255.255.0 192.168.20.0 255.255.255.0
access-list nonat permit ip 192.168.11.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat permit ip 192.168.11.0 255.255.255.0 192.168.70.0 255.255.255.0
access-list nonat permit ip 192.168.11.0 255.255.255.0 192.168.71.0 255.255.255.0
access-list nonat permit ip 192.168.11.0 255.255.255.0 192.168.72.0 255.255.255.0
access-list nonat permit ip 192.168.11.0 255.255.255.0 192.168.73.0 255.255.255.0
pager lines 24
logging on
logging monitor errors
logging buffered debugging
logging trap debugging
logging host inside 192.168.20.10
interface ethernet0 10baset
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
mtu outside 1500
mtu service 1500
mtu supplier 1500
mtu partner 1500
mtu corporate 1500
ip address outside x.x.10.18 255.255.255.240
ip address service x.x.7.33 255.255.255.224
ip address supplier 192.168.10.1 255.255.255.0
ip address partner 192.168.11.1 255.255.255.0
ip address corporate 192.168.20.1 255.255.255.0
ip audit info action alarm
```

```
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 x.x.10.19
global (outside) 2 x.x.10.20
global (outside) 3 x.x.10.21
nat (service) 0 x.x.7.32 255.255.255.224 0 0
nat (supplier) 0 access-list nonat
nat (supplier) 1 192.168.10.0 255.255.255.0
nat (partner) 0 access-list nonat
nat (partner) 2 192.168.11.0 255.255.255.0
nat (corporate) 0 access-list nonat
nat (corporate) 3 192.168.20.0 255.255.255.0
static (service,outside) x.x.7.32 x.x.7.32 255.255.255.224
access-group acl_out in interface outside
access-group acl_corporate in interface corporate
access-group acl_service in interface service
access-group acl_supplier in interface supplier
access-group acl_partner in interface partner
route outside 0.0.0.0 0.0.0.0 x.x.10.17 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community 67yhr57
no snmp-server enable traps
floodguard enable
sysopt security fragguard
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set supplier esp-3des esp-sha-hmac
crypto ipsec transform-set partner esp-des esp-sha-hmac
crypto ipsec transform-set r_user esp-3des esp-sha-hmac
crypto map gfalls 10 ipsec-isakmp
crypto map gfalls 10 match address supplier1
crypto map gfalls 10 set peer x.x.10.1
```

```
crypto map gfalls 10 set transform-set supplier
crypto map gfalls 11 ipsec-isakmp
crypto map gfalls 11 match address supplier2
crypto map gfalls 11 set peer x.x.202.2
crypto map gfalls 11 set transform-set supplier
crypto map gfalls 12 ipsec-isakmp
crypto map gfalls 12 match address supplier3
crypto map gfalls 12 set peer x.x.20.3
crypto map gfalls 12 set transform-set supplier
crypto map gfalls 20 ipsec-isakmp
crypto map gfalls 20 match address partner1
crypto map gfalls 20 set peer x.x.45.4
crypto map gfalls 20 set transform-set partner
crypto map gfalls 21 ipsec-isakmp
crypto map gfalls 21 match address partner2
crypto map gfalls 21 set peer x.x.29.5
crypto map gfalls 21 set transform-set partner
crypto map gfalls 22 ipsec-isakmp
crypto map gfalls 22 match address partner3
crypto map gfalls 22 set peer x.x.38.6
crypto map gfalls 22 set transform-set partner
crypto map gfalls 23 ipsec-isakmp
crypto map gfalls 23 match address partner4
crypto map gfalls 23 set peer x.x.209.7
crypto map gfalls 23 set transform-set partner
crypto map gfalls 30 ipsec-isakmp
crypto map gfalls 30 match address r_user1
crypto map gfalls 30 set peer x.x.104.8
crypto map gfalls 30 set transform-set r_user
crypto map gfalls 31 ipsec-isakmp
crypto map gfalls 31 match address r_user2
crypto map gfalls 31 set peer x.x.104.9
crypto map gfalls 31 set transform-set r_user
crypto map gfalls 32 ipsec-isakmp
crypto map gfalls 32 match address r_user3
crypto map gfalls 32 set peer x.x.104.10
crypto map gfalls 32 set transform-set r_user
crypto map gfalls 33 ipsec-isakmp
crypto map gfalls 33 match address r_user4
crypto map gfalls 33 set peer x.x.104.11
crypto map gfalls 33 set transform-set r_user
crypto map gfalls 34 ipsec-isakmp
crypto map gfalls 34 match address r_user5
crypto map gfalls 34 set peer x.x.104.12
crypto map gfalls 34 set transform-set r_user
```

```
crypto map gfalls 35 ipsec-isakmp
crypto map gfalls 35 match address r_user6
crypto map gfalls 35 set peer x.x.104.13
crypto map gfalls 35 set transform-set r_user
crypto map gfalls 36 ipsec-isakmp
crypto map gfalls 36 match address r_user7
crypto map gfalls 36 set peer x.x.104.14
crypto map gfalls 36 set transform-set r_user
crypto map gfalls 37 ipsec-isakmp
crypto map gfalls 37 match address r_user8
crypto map gfalls 37 set peer x.x.104.15
crypto map gfalls 37 set transform-set r_user
crypto map gfalls 38 ipsec-isakmp
crypto map gfalls 38 match address r_user9
crypto map gfalls 38 set peer x.x.104.16
crypto map gfalls 38 set transform-set r_user
crypto map gfalls 39 ipsec-isakmp
crypto map gfalls 39 match address r_user10
crypto map gfalls 39 set peer x.x.25.17
crypto map gfalls 39 set transform-set r_user
crypto map gfalls 40 ipsec-isakmp
crypto map gfalls 40 match address r_user11
crypto map gfalls 40 set peer x.x.25.18
crypto map gfalls 40 set transform-set r_user
crypto map gfalls 41 ipsec-isakmp
crypto map gfalls 41 match address r_user12
crypto map gfalls 41 set peer x.x.25.19
crypto map gfalls 41 set transform-set r_user
crypto map gfalls 42 ipsec-isakmp
crypto map gfalls 42 match address r_user13
crypto map gfalls 42 set peer x.x.25.20
crypto map gfalls 42 set transform-set r_user
crypto map gfalls 43 ipsec-isakmp
crypto map gfalls 43 match address r_user14
crypto map gfalls 43 set peer x.x.25.21
crypto map gfalls 43 set transform-set r_user
crypto map gfalls 44 ipsec-isakmp
crypto map gfalls 44 match address r_user15
crypto map gfalls 44 set peer x.x.25.22
crypto map gfalls 44 set transform-set r_user
crypto map gfalls 45 ipsec-isakmp
crypto map gfalls 45 match address r_user16
crypto map gfalls 45 set peer x.x.25.23
crypto map gfalls 45 set transform-set r_user
crypto map gfalls 46 ipsec-isakmp
```

```
crypto map gfalls 46 match address r_user17
crypto map gfalls 46 set peer x.x.25.24
crypto map gfalls 46 set transform-set r_user
crypto map gfalls 47 ipsec-isakmp
crypto map gfalls 47 match address r_user18
crypto map gfalls 47 set peer x.x.25.25
crypto map gfalls 47 set transform-set r_user
crypto map gfalls 48 ipsec-isakmp
crypto map gfalls 48 match address r_user19
crypto map gfalls 48 set peer x.x.25.26
crypto map gfalls 48 set transform-set r_user
crypto map gfalls 49 ipsec-isakmp
crypto map gfalls 49 match address r_user20
crypto map gfalls 49 set peer x.x.25.27
crypto map gfalls 49 set transform-set r_user
crypto map gfalls interface outside
isakmp enable outside
isakmp key ******** address x.x.10.1 netmask 255.255.255.255
isakmp key ******** address x.x.202.2 netmask 255.255.255.255
isakmp key ******** address x.x.20.3 netmask 255.255.255.255
isakmp key ******** address x.x.45.4 netmask 255.255.255.255
isakmp key ******** address x.x.29.5 netmask 255.255.255.255
isakmp key ******** address x.x.38.6 netmask 255.255.255.255
isakmp key ******** address x.x.209.7 netmask 255.255.255.255
isakmp key ******** address x.x.104.8 netmask 255.255.255.255
isakmp key ******** address x.x.104.9 netmask 255.255.255.255
isakmp key ******** address x.x.104.10 netmask 255.255.255.255
isakmp key ******** address x.x.104.11 netmask 255.255.255.255
isakmp key ******** address x.x.104.12 netmask 255.255.255.255
isakmp key ******** address x.x.104.13 netmask 255.255.255.255
isakmp key ******** address x.x.104.14 netmask 255.255.255.255
isakmp key ******** address x.x.104.15 netmask 255.255.255.255
isakmp key ******** address x.x.104.16 netmask 255.255.255.255
isakmp key ******** address x.x.25.17 netmask 255.255.255.255
isakmp key ******** address x.x.25.18 netmask 255.255.255.255
isakmp key ******** address x.x.25.19 netmask 255.255.255.255
isakmp key ******** address x.x.25.20 netmask 255.255.255.255
isakmp key ******** address x.x.25.21 netmask 255.255.255.255
isakmp key ******** address x.x.25.22 netmask 255.255.255.255
isakmp key ******** address x.x.25.23 netmask 255.255.255.255
isakmp key ******** address x.x.25.24 netmask 255.255.255.255
isakmp key ******** address x.x.25.25 netmask 255.255.255.255
isakmp key ******** address x.x.25.26 netmask 255.255.255.255
isakmp key ******** address x.x.25.27 netmask 255.255.255.255
isakmp identity address
```

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 3600
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 3600
telnet 192.168.20.0 255.255.255.0
telnet timeout 5
ssh 192.168.20.0 255.255.255.0
ssh timeout 5
terminal width 80
```

Assignment 3 – Audit Your Security Architecture

You have been asked to conduct a technical audit of the primary firewall (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

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

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

Planning the Audit

In my design the border router and the firewall share the task of securing the network and therefore my audit will test the policy's implemented on both devices. Since it is

pointless to duplicate rules on both devices they have a layered affect to provide a total security policy.

The audit will be conducted from outside probing GIAC's network to insure that it allows all the required access as well as prevents all non authorized access. Various tools will be used to scan for open ports and vulnerabilities as well as to confirm that required access is allowed. The audit will also be conducted from our various network segments to insure that outbound access is restricted/allowed as per our policy as well.

By having a 16 block assigned for their outside segment gives them the possibility to place other devices outside their border router to capture packets for analysis as well as to perform testing for our audit. Test devices placed outside the border router on this subnet have to bypass both the border router and firewall for access to other subnets to allow true end to end testing.

The audit should be performed during the busy day of the month. In GIAC's case this has been determined to be the last Friday of the month. While the firewall is at its busiest is the most likely time for it to fail. The risk is it may fail, causing problems during your busiest time. Also it should be noted that tools like nmap may cause systems to lock up, reboot, or cause other issues that may result in downtime or performance issues.

It is also recommended that GIAC provide a complete audit of all their IT systems and procedures many of which are not covered in this paper. For example, a vulnerability scanner could be used to probe servers for unpatched vulnerabilities. In addition things like the backup procedure should be audited to insure that it is working properly and that data can be restored as planned.

The audit plan, procedure and analysis to follow strictly deals with testing the firewall, VPN, and border router policies to insure they are implemented properly and working as intended and to insure nothing has been over looked.

In order to conduct the audit several tools will be used to verify the security policy is working as intended and nothing has been over looked. These tools will include netcat, nmapnt, ethereal, and a laptop running Windows NT.

The first step in the audit should be to check that DNS is working properly and is secured to prevent divulging to much detail to attackers. It is worth while to note at this point that there is a real existing domain giac.com. However, for the point of this paper, it is assumed that we were able to register giac.com and the following screen shots throughout the audit have been modified to show typical results that we would expect to see if this network really existed and was under our control.

The second step would be to scan the network from the outside to determine what ports are open, closed or filtered. In addition the border router should be scanned to insure that no unnecessary services are still enabled.

The third step would be to confirm that spoofed addresses are blocked.

The fourth is to determine that IPSEC is functioning.

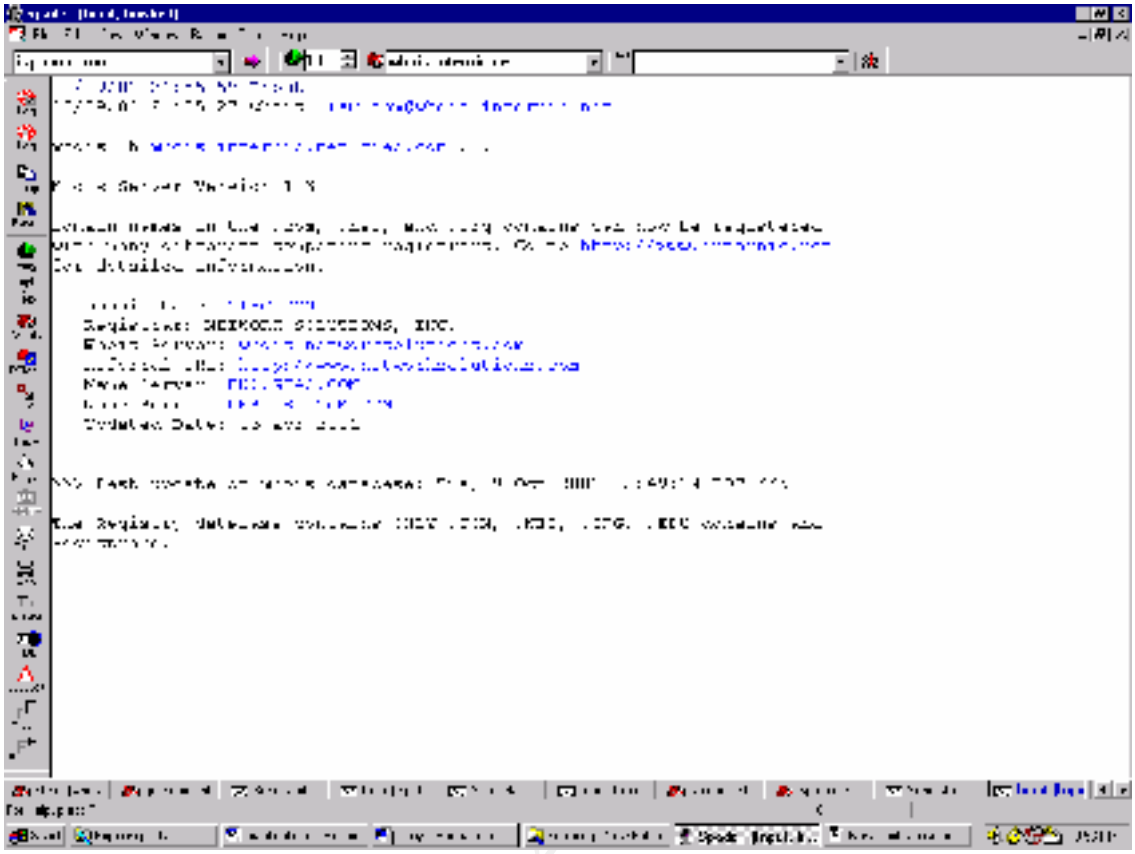
Finally a scan should be ran from inside each subnet of the firewall to insure that outbound restrictions are working as planned.

The estimated time to complete the planning, perform the audit, and present the results is three days effort for a total cost of $2400.

Performing the Audit

Since I did not have the hardware to build a replica of the GIAC architecture the following screen shots and results are modified examples of what the results should look like. In addition the IP addresses have been masked out with x.x for the first two octets.

The first step would be to use a tool such as Sam Spade to make sure that giac.com exists where it is registered and what are the authoritative DNS servers. The following screen shot shows a typical response of a whois on giac.com. From it we can see that it is registered with Network Solutions and the authoritative DNS servers are Primary dns.giac.com with a secondary of dns.isp.com.com.



The next step would be to do a nslookup to determine the IP address of both of these DNS servers. The following would be typical output from these lookups.

C:\>nslookup
Default Server: dns1.roadrunner.nf.net
Address: 192.75.13.69

> dns.giac.com
Server: dns1.roadrunner.nf.net
Address: 192.75.13.69

Non-authoritative answer:
Name: dns.giac.com
Address: x.x.7.36

C:\>nslookup
Default Server: dns1.roadrunner.nf.net
Address: 192.75.13.69

> dns.isp.com.com

Server: dns1.roadrunner.nf.net
Address: 192.75.13.69

Non-authoritative answer:
Name: dns.isp.com.com
Address: x.x.1.100

The next test would be to insure that both of these servers contain the required records for public access but will not allow zone transfers or provide information that should not be publicly available. In order to test this again you would use the nslookup utility. This time you would set your server to be the correct DNS server for giac.com. You would check to insure that it contains records for your mail and web server as well as checking to insure it blocks zone transfers.

The primary DNS server appears to hang when attempting to do a zone transfer this is because TCP 53 is blocked by the firewall. As a result when the DNS server switches from UDP to TCP to do a large transfer the packet is blocked and therefore no results are displayed.

C:\>nslookup
Default Server: notitia.roadrunner.nf.net
Address: 192.75.13.67

> server dns.giac.com
Default Server: dns.giac.com
Address: x.x.1.100

> ls -d giac.com

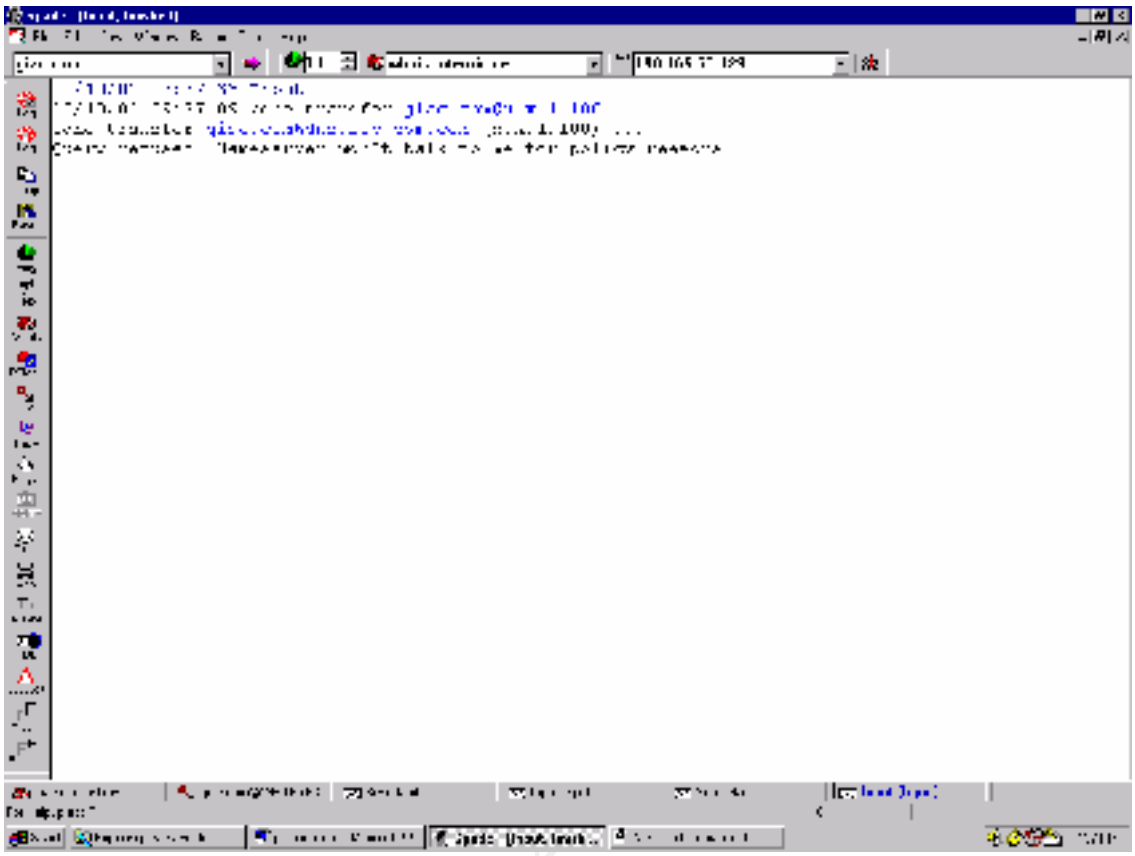
As shown below the secondary DNS does not permit zone transfers.

C:\>nslookup
Default Server: dns1.roadrunner.nf.net
Address: 192.75.13.69

> server dns.isp.com.com
Default Server: dns.isp.com.com
Address: x.x.1.100

> ls -d giac.com
[dns.isp.com.com]
*** Can't list domain giac.com: Query refused

As an alternative you can use Sam Spade to attempt to do a zone transfer to confirm it is blocked as well as demonstrated below:



Checks of both confirm they do return the required records for public access.

C:\>nslookup
Default Server: dns1.roadrunner.nf.net
Address: 192.75.13.69

> server dns.giac.com
Default Server: dns.giac.com
Address: x.x.7.36

> set type=ANY
> giac.com
Server: dns.giac.com
Address: x.x.7.36

giac.com
	primary name server = dns.giac.com
	responsible mail addr = hostmaster.mail.giac.com
	serial = 2001100301
	refresh = 10800 (3 hours)
	retry = 3600 (1 hour)

```
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
giac.com        MX preference = 0, mail exchanger = mail.giac.com
giac.com        nameserver = dns.giac.com
giac.com        nameserver = dns.isp.com.com
mail.giac.com internet address = x.x.7.35
dns.giac.com      internet address = x.x.7.36
dns.isp.com.com      internet address = x.x.1.100
> www.giac.com
Server:  dns.giac.com
Address:  x.x.7.36

www.giac.com    internet address = x.x.7.34
giac.com        nameserver = dns.giac.com
giac.com        nameserver = dns.isp.com.com
dns.giac.com      internet address = x.x.7.36
dns.isp.com.com      internet address = x.x.1.100
```

The next step of the analysis is to scan the network from the outside to insure there are no open ports that we are unaware of. This can be accomplished by placing the laptop outside of the router and running nmap with the following parameters.

-v for verbose mode which gives more information about what is going on
-g53 sets the souce port to be 53 which may be allowed through some firewalls
-sS performs a half open scan which is not logged by many sites
-sR attempts to determine if ports are RPC port
-P0 do not ping before scanning since many firewalls block icmp which will result in the scan not being performed
-O attempt to identify the OS on founf hosts
-p1-65535 scan all ports from 1 to 65535
-oN test.txt logs results to human readable file named test.txt
x.x.7.33-36 scans IP's from x.x.7.33 to x.x.7.62
.

```
nmapnt -v -g53 -sS -sR -P0 -O -p1-65535 -oN test.txt x.x.7.33-62

D:\nmap\Nmapnt>nmapnt -v -g53 -sS –sR -P0 -O -p1-65535 -oN test.txt x.x.7.33-62


Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Initiating SYN half-open stealth scan against  (x.x.7.34)
The SYN scan took 4089 seconds to scan 65535 ports.
Initiating RPC scan against  (x.x.7.34)
```

```
The RPC scan took 0 seconds to scan 65535 ports.
Warning:  No TCP ports found open on this machine, OS detection will be MUCH les
s reliable
Interesting ports on  (x.x.7.34):
(The 65532 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
80/tcp     open        http
443/tcp    open        https

Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Initiating SYN half-open stealth scan against  (x.x.7.35)
The SYN scan took 4089 seconds to scan 65535 ports.
Initiating RPC scan against  (x.x.7.35)
The RPC scan took 0 seconds to scan 65535 ports.
Warning:  No TCP ports found open on this machine, OS detection will be MUCH les
s reliable
Interesting ports on  (x.x.7.35):
(The 65532 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
25/tcp     open        smtp

Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Nmap run completed -- 2 IP address (2 host up) scanned in 4110 seconds

D:\nmap\Nmapnt>
```

Repeat the scan changing the IP address range to be x.x.10.17-30. The results from this scan should show that all traffic is being filtered.

Finally repeat the scan against the outside interface of the router x.x.18.2. Once again the results should be that all ports are filtered with the exception of port 20 which should display as being closed. If any ports were open they would be displayed as in this example below of a router that had finger, http, and telnet access allowed.

D:\nmap\Nmapnt>nmapnt -v -g53 -sS -sR -P0-O -p1-65535 -oN firewall.txt x.x.2
8.2

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security (http://www.eEye.com)
based on nmap by fyodor@insecure.org (www.insecure.org/nmap/)

Initiating SYN half-open stealth scan against (x.x.28.2)
Adding TCP port 80 (state open).
Adding TCP port 23 (state open).
Adding TCP port 79 (state open).
The SYN scan took 589 seconds to scan 65535 ports.
Initiating RPC scan against (x.x.28.2)
The RPC scan took 0 seconds to scan 65535 ports.
Interesting ports on (x.x.28.2):
(The 65532 ports scanned but not shown below are in state: closed)

Port	State	Service (RPC)
23/tcp	open	telnet
79/tcp	open	finger
80/tcp	open	http

Nmap run completed -- 1 IP address (1 host up) scanned in 594 seconds

We can also use nmapnt to generate packets with spoofed IP's to insure they are being blocked as well. In order to confirm this we should place a machine running a packet sniffer such as Ethereal inside the router plugged into a mirrored switch port of the router internal interface. By using the –S <IP_ADDRESS> with the nmapnt scan you can set your IP address to be a spoofed address. By capturing the data inside the router you can confirm these packets are being filtered. You can also from the router show the appropriate ACL and see that there are matches for the rule that blocks the spoofed address tested.

While you have your packet sniffer set up you can confirm as well that partner, supplier, and remote user traffic is encrypted as well. You can generate traffic from your network to theirs' and confirm that the data is encrypted from your captured packets.

Finally, the scan would be performed again from inside each subnet to confirm that the expected ports are filtered as intended and the required access is permitted.

Another useful tool is netcat. It can be used to attempt connections to any tcp or udp port, insuring that you can initiate traffic destined for the respective ports. In order to

use netcat, for instance, to test a connection to a mail server using pop3 you would simply type the following at a command prompt:

nc x.x.x.x 110

Replace x.x.x.x with an IP that you know is running a pop3 server. You should see this server respond and wait for pop3 commands.

You can also use netcat to listen on any udp or tcp port. By doing so can place it on the outside network and set it listening on the required ports to insure you can get to them through the firewall. In order to set netcat up listening on a particular port you simply type the following at a command prompt:

nc -l -p 23 -t -e cmd.exe

This example would start netcat listening on port 23, and spawn a command shell when someone connects to it. You could then attempt to connect to the box running netcat to confirm that telnet is functioning from inside the firewall.

By using these tools you will be able to confirm each individual required service is functioning and that there are no unexpected holes in the network.

Evaluate the Audit

Seeing as it is assumed that the network analysis confirms proper configuration and operation the results would be prepared and presented to GIAC.

In addition, I would point out when their budget permits they should invest in some redundant hardware. Currently they have some single points of failure. I would recommend that they consider a second PIX and run them in failover mode. They also should consider a second router and implement HSRP Hot Standby Routing Protocol.

I would also recommend they look into a AAA server to perform authorization and accounting. This would allow them to force people to be authorized before being allowed to initiate ftp, http, and telnet access which would reduce the chance of a hacker using these services to connect to other devices or from downloading a tool kit if they gain access to any network segment. Finally I would suggest they investigate Websense. Websense would allow them to control web site access. Additional information on Websense can be found at http://www.cisco.com/warp/public/cc/so/neso/sqso/csap/wbsn_rg.htm.

Assignment 4 – Design Under Fire

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

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

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

In designing your attacks, keep the following in mind:

- The attack should be realistic. The purpose of this exercise is for the subject to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

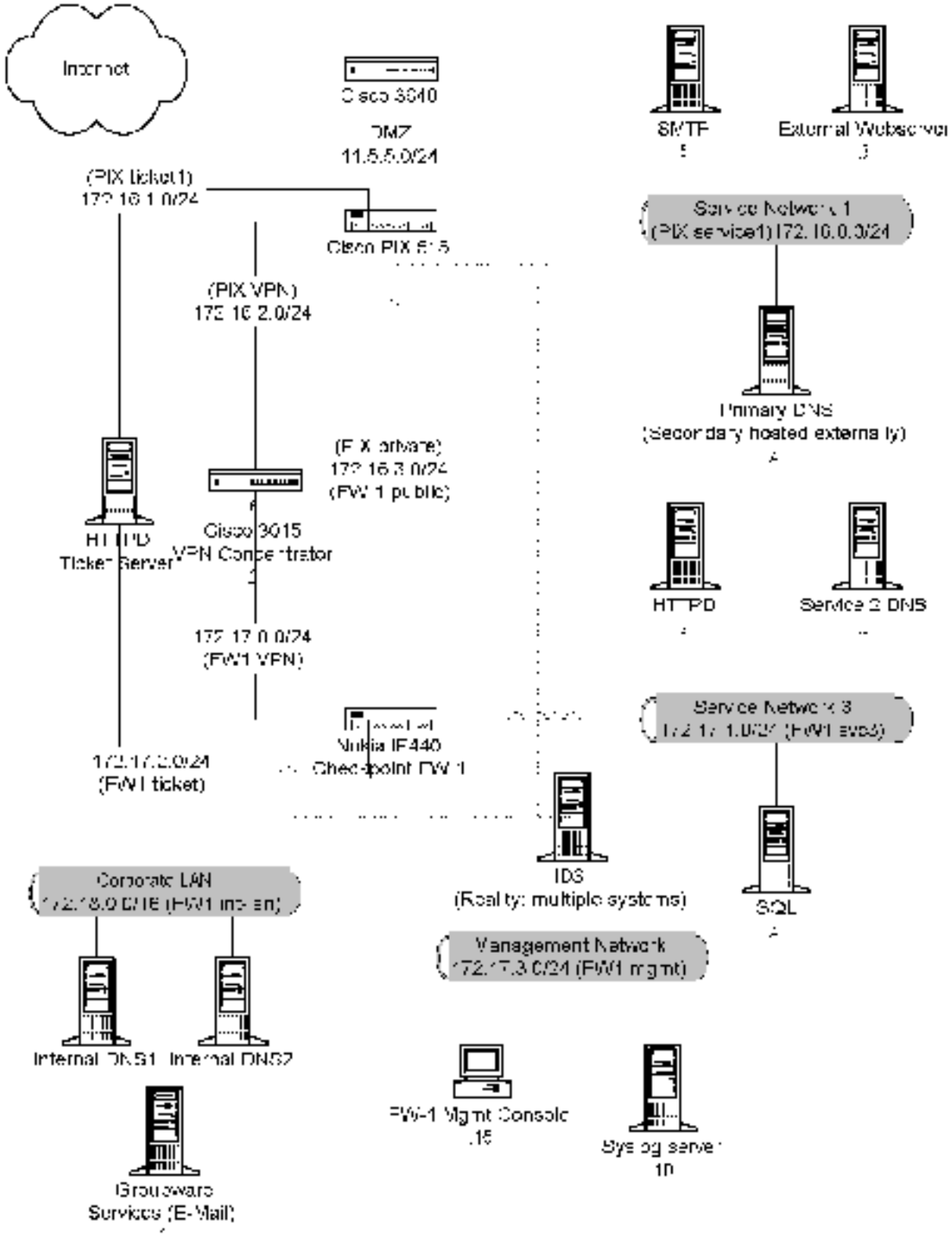
- The attack should be reasonable. The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should not assume that it is an unpatched, out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)

- You must supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

- The attack does not necessarily have to succeed (though a successful attack is often the more interesting approach). If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

Christopher M. Kellogg's Practical

I have chosen to attack Mr. Kellogg's practical, simply because he has used a PIX firewall which I have used as well. By doing the research for vulnerabilities against the PIX I have learned information that can be used in the future to help protect networks I am responsible for, from similar attacks. Mr. Kellogg's practical can be found at: http://www.sans.org/giactc/gcfw.htm



Three Vulnerabilities Against a PIX Firewall

All three vulnerabilities can be found at http://packetstormsecurity.org/advisories/cisco/

Cisco Secure Pix Firewall TCP Reset Vulnerability[5]

```
Cisco Secure PIX Firewall TCP Reset Vulnerability

Revision 1.0

For Public Release 2000 July 11 06:00 US/Eastern (UTC+0400)

  ---------------------------------------------------------------------
----

Summary
=======

The Cisco Secure PIX Firewall cannot distinguish between a forged TCP
Reset
(RST) packet and a genuine TCP RST packet. Any TCP/IP connection
established
through the Cisco Secure PIX Firewall can be terminated by a third
party from
the untrusted network if the connection can be uniquely determined.
This
vulnerability is independent of configuration. There is no workaround.

This vulnerability exists in all Cisco Secure PIX Firewall software
releases
up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1). The defect has
been
assigned Cisco bug ID CSCdr11711.

This notice is posted on Cisco's Worldwide Web site at
http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml.


Affected Products
=================

Cisco Secure PIX Firewalls with software versions up to and including
4.2(5),
4.4(4), 5.0(3) and 5.1(1) are affected.

No other products are vulnerable to this defect.


Details
=======
```

[5] Complete advisory and explanation as posted at http://packetstormsecurity.org/advisories/cisco/cisco.00-07-11.tcpreset

When the Cisco Secure PIX Firewall receives a TCP Reset (RST) packet, it
evaluates that packet based on data contained in the TCP packet header: source
IP address, source port, destination IP address, and destination port. If
these four values match an entry in the stateful inspection table, the
associated connection will be reset. This affects only TCP sessions. Data
exchange based on any other protocol is not affected.

To exploit this vulnerability, an attacker would need to have or infer:

* Detailed knowledge of the connection table in the Cisco Secure PIX
  Firewall prior to launching the attack

Or

* Detailed knowledge of the source and destination IP Address and ports
  associated with a particular connection to be attacked

This particular vulnerability only affects the connection table (which keeps
state regarding the connections being made through the device). It does not
affect the translation table (in which address mappings are stored).

Cisco Secure PIX Firewall software has been fixed so that it now checks for
a valid sequence number before removing a connection from the connection
state table.

Impact
======

Any Cisco Secure PIX Firewall that provides external access to the Internet
and for which all of the preceding conditions are met is vulnerable to the
disruption of individual sessions.

Software Versions and Fixes
===========================

For the version listed in the left-most column below, customers should upgrade
to at least the version shown in the center column. Please note the hardware
requirements following the table.

Affected Version	Projected first fixed regular release (fix will carry forward into all later versions)	Date Available
All versions of Cisco Secure PIX up to version 4.2(5) (including 2.7, 3.0, 3.1, 4.0, 4.1)	4.4(5)	2000-06-09
All 4.3.x and 4.4.x versions up to and including version 4.4(4)	4.4(5)	2000-06-09
Version 5.0.x up to and including version 5.0(3)	5.1(2)	2000-06-09
Version 5.1.1	5.1(2)	2000-06-09

A 128MB upgrade for the PIX Firewall is necessary if:

* Version 4.3 or 4.4 is used on a PIX 'Classic'
  (excluding PIX10000, PIX-510, PIX-520, and PIX-515)

Or

* Version 5.0 is used on a PIX 'Classic', PIX10000, or PIX-510
  (excluding PIX-520 and PIX-515)

As with any new software installation, customers planning to upgrade should

carefully read the release notes and other relevant documentation before
beginning any upgrade. Also, it is important to be certain that the new
version of Cisco Secure PIX Firewall software is supported by your hardware
and especially that enough memory is available.

Obtaining Fixed Software
========================

Cisco is offering free software upgrades to remedy this vulnerability for all
affected customers.

Customers with contracts should obtain upgraded software through their regular
update channels. For most customers, this means that upgrades should be
obtained via the Software Center on Cisco's Worldwide Web site at
http://www.cisco.com/.

Customers without contracts should get their upgrades by contacting the Cisco
Technical Assistance Center (TAC). TAC contacts are as follows:

* +1 800 553 2447 (toll-free from within North America)
* +1 408 526 7209 (toll call from anywhere in the world)
* E-mail: tac@cisco.com

Additional contact information for the Cisco TAC for non-English speakers is
available at
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Give the URL of this notice as evidence of your entitlement to a free
upgrade. Free upgrades for non-contract customers must be requested through
the TAC. Please do not contact psirt@cisco.com or security-alert@cisco.com for
software upgrades.

Workarounds
===========

There are no workarounds for this defect. Customers are urged to upgrade to
the versions of code containing the fix for CSCdr11711.

Exploitation and Public Announcements
=====================================

Cisco has received no reports of malicious exploitation of this vulnerability. The vulnerability was reported to Cisco by a customer and has
been discussed on BUGTRAQ, a public full-disclosure security mailing list.

Status of This Notice: FINAL
==========

This is a final notice. Although Cisco cannot guarantee the accuracy of all
statements in this notice, all of the facts have been checked to the best of
our ability. Cisco does not anticipate issuing updated versions of this notice
unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this notice.

Distribution
==========

This notice is posted at http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml on Cisco's Worldwide Web site. A text version of this notice will be clear-signed with
the latest Cisco PSIRT RSA PGP key and posted to the following e-mail recipients and Usenet newsgroups:

* cust-security-announce@cisco.com
* bugtraq@securityfocus.com
* firewalls@lists.gnac.net
* first-teams@first.org (includes CERT/CC)
* cisco@spot.colorado.edu
* cisco-nsp@puck.nether.net
* comp.dcom.sys.cisco
* Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web
server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL
given above for any updates.

Revision History
==========

Revision 1.0	2000-07-11	Initial public release

```
Cisco Product Security Incident Assistance Process
==================================================

The web page at
http://www.cisco.com/warp/public/707/sec_incident_response.shtml
describes how
to report security vulnerabilities in Cisco products, obtain
assistance with
security incidents, and register to receive product security
information from
Cisco Systems, Inc., including instructions for press inquiries
regarding
Cisco Security Advisories and notices. This advisory is Cisco's
official
public statement regarding this vulnerability.

  ------------------------------------------------------------------
----

This notice is Copyright 2000 by Cisco Systems, Inc. This notice may
be
redistributed freely after the release date given at the top of the
text,
provided that redistributed copies are complete and unmodified,
including
all date and version information.

  ------------------------------------------------------------------
----
```

Summary of TCP Reset Vulnerability

As shown by the above advisory there is a vulnerability in release 5.1(1) and earlier versions of the PIX IOS which may be exploitable to disconnect active sessions that are in progress through the PIX.

In earlier releases of the software it only used source port / source IP and destination port / destination IP to track sessions in the state table. Using only this information it was possible to send the PIX a forged reset packet if you could determine these four parameters for an active session.

Using only these four parameters it was impossible for the PIX to distinguish forged resets from real resets. As a result it was possible for any third party to terminate an active session if they could some how determine these four parameters.

In order to fix this problem Cisco in later versions of the software added sequence numbers to the parameters in the state table. By doing so it makes it much more difficult to have a forged reset packet match the entry in the state table because it would be very difficult to guess the corresponding sequence number in addition to the other four parameters.

It is advised that anybody using a PIX firewall insure that they are running the latest version of the IOS to protect themselves from this and other exploits.

Cisco PIX and CBAC Fragmentation Attack[6]

```
Field Notice:
Cisco PIX and CBAC Fragmentation Attack

Revision 1.1
For release 08:00 AM US/Pacific, Friday, September 11, 1998
Cisco internal use only until release date
============================================================

Summary
=======
Neither Cisco's PIX Firewall, nor the Context-Based Access Control
(CBAC)
feature of Cisco's IOS Firewall Feature Set, protects hosts against
certain
denial of service attacks involving fragmented IP packets. This
vulnerability does not permit network "breakins". The vulnerability is
most
severe in configurations involving static NAT entries, or in
configurations
not involving any use of NAT.

The vulnerability is present in Cisco PIX firewall software up to and
including version 4.2(1), and in CBAC versions of Cisco IOS software
through
11.2P and 11.3T, and will be present in initial 12.0 revisions of CBAC
software.

The Cisco Centri firewall does not share this vulnerability.

Stateless packet filtering products,  such as the extended access
lists
available in non-CBAC versions of Cisco IOS software, share the
vulnerability because of the inherent limitations of stateless
operation.
This it is not considered a defect in stateless filtering. More
information
is in the section on "Stateless Packet Filters" in this document.

This vulnerability will be fixed in Cisco PIX Firewall software
version
4.2(2), which is tentatively scheduled for release on September 14,
1998. The vulnerability is scheduled to be fixed for CBAC in Cisco IOS
software release 12.0(2) and 12.0(3)T, which are tentatively scheduled
for release in late November, 1998, and in late January, 1999,
respectively. All schedules are subject to change.
```

[6] Complete Advisory and explanation as posted at http://packetstormsecurity.org/advisories/cisco/cisco.98-09-11.pix_cbac_frag

The possibility of IP fragmentation attacks against packet filters, from Cisco and other vendors, has been widely known for a very long time. However, exploitation does not seem to be increasing. Therefore, Cisco does not believe that the majority of its customers are critically exposed by this vulnerability. Cisco is, however, prepared to support any customers who suffer actual attacks, or who have specific reason to think that they are likely to be attacked in this way.

Who Is Affected
==========
All users of Cisco PIX Firewalls with software versions up to and including 4.2(1) are affected. Users of the CBAC feature on Cisco IOS software versions up to and including 11.2P and 11.3T (all edit levels), as well as 12.0 versions and 12.0T versions up to and including 12.0(1) and 12.0(2)T, are also affected.

A similar vulnerability affects all users who rely on stateless packet filtering products, from Cisco or any other vendor. The packet filters affected are those which are capable of filtering based on information, such as TCP or UDP port numbers, that may not be present in every fragment of a datagram. This vulnerability is not considered a defect for a stateless packet filtering product.

Packet filtering using non-CBAC Cisco IOS software extended access lists falls into this category of stateless filtering, and such access lists are vulnerable in all versions of Cisco IOS software. The affected extended access lists are numbered lists from 100-199, or named access lists created with the "extended" keyword. Non-extended Cisco IOS access lists, numbered from 1-99, are not capable of filtering on port numbers, and are not affected.

Impact
======
Even though the firewall keeps an attacker from making actual connections to a given host, he or she may still be able to disrupt services provided by

that host. This is done by sending many unmatched non-initial IP fragments,
which use reassembly resources on the target host. Hosts vary widely in the
quality of their resource management and in their response to this attack.
Some hosts can be made nearly useless by traffic levels that might realistically be available to attackers.

The attack can be launched only against hosts to which the attackers can
address packets. If dynamic NAT is being used, attack packets can be sent
only to hosts which are actively communicating with the Internet, since NAT
translation table entries will not exist for other hosts.

Because the firewall drops only the initial fragments of blocked datagrams,
attackers can exploit this vulnerability by sending streams of complete
fragmented packets. The attacker in this case deliberately intends the initial fragments to be blocked by the firewall. Since only the non-initial
fragments will be forwarded, the effect on the target host will be similar
to the effect of sending only the non-initial fragments to begin with. This
method involves some waste of the attacker's resources, and is therefore
slightly less effective than simply sending the non-initial fragments alone.
This method is of interest because it allows attacks to be launched using
relatively standard networking tools, without any special exploit program.

PIX Firewall Details
====================
This vulnerability on the PIX Firewall has been assigned Cisco bug ID CSCdk36273.

Problem description for the PIX Firewall
- -----------------------------------
PIX firewall software up through version 4.2(1) will pass any non-initial
fragment destined for any host for which either a static or a dynamic NAT
table entry exists. Static NAT table entries are created with the PIX Firewall static command, and dynamic entries are created by inside hosts
initiating IP traffic exchanges with outside hosts. No checks are made as to
whether or not non-initial fragments belong to actual existing connections,

```
so it is possible for any outside host to send fragments to any inside
host
that has a NAT entry, regardless of whether or not there is a
connection
between the two hosts, and regardless of whether a conduit is
configured.

Immediate Response for the PIX Firewall
- -----------------------------------
The following changes have been made to the behavior of the PIX
Firewall for
version 4.2(2):

   * Interfragment state is now being kept. Any non-initial fragment
will be
     discarded unless the corresponding initial fragment was permitted
to
     pass through the firewall. Non-initial fragments received before
the
     corresponding initial fragments will be discarded.

     This eliminates the possibility of overloading host resources
with
     unmatched non-initial fragments, and requires attackers to use
     relatively elaborate address spoofing for attacks using unmatched
     initial fragments.

     This change may have undesirable effects in certain cases, since
it
     will result in the firewall's discarding any datagram whose
fragments
     arrive out of order. There are a number of circumstances that may
cause
     out-of-order delivery of legitimate fragments. Cisco therefore
advises
     caution in installing the new software, although Cisco does not
believe
     that legitimate out-of-order fragmented traffic (or indeed
fragmented
     traffic of any kind) is common at Internet firewalls.

   * Fragments received for hosts without conduits are discarded
unless
     those fragments can be matched with active connections. Matching
is
     performed using IP source and destination address and protocol
type.

   * The amount of memory dedicated to fragmentation state is limited
in
     order to reduce the chance of denial of service attacks against
the PIX
     Firewall itself. Fragmentation state is created only in response
to
     initial fragments, and is kept until either all fragments of the
```

```
     datagram in question have been processed, or a timeout expires.
Initial
     fragments received when fragmentation state resources are
exhausted are
     discarded.

     Unfragmented traffic will never be discarded because of lack of
     fragment state memory. Even when the system is under heavy attack
with
     fragmented packets, legitimate fragmented traffic, if any, will
still
     get some fraction of the firewall's fragment state resources, and
     legitimate unfragmented traffic will flow unimpeded.

These or equivalent changes will be carried forward into all PIX
Firewall
software versions after version 4.2(2).

Getting Fixed Software for the PIX Firewall
- -----
Cisco is offering free upgrades to 4.2(2) software for all PIX
Firewall
customers, regardless of service contract status. The upgrades will be
available as soon as the 4.2(2) software has been released.

Once the software has been released, customers with service contracts
may
download it from Cisco's Worldwide Web site.

Customers without service contracts should get their upgrades by
contacting
the Cisco TAC. TAC contacts are as follows:

   * +1 800 553 2447 (toll-free from within North America)
   * +1 408 526 7209 (toll call from anywhere in the world)
     e-mail: tac@cisco.com

Give the URL of this notice as evidence of your entitlement to a free
upgrade. Free upgrades for non-contract customers must be requested
through
the TAC. Please do not contact either "psirt@cisco.com" or
"security-alert@cisco.com" for software upgrades.

As with any new software installation, PIX Firewall customers planning
to
upgrade to version 4.2(2) should carefully read the release notes and
other
relevant documentation before beginning any upgrade.

Long-term Plans for the PIX Firewall
- ----------------------------------
Cisco is evaluating the  possibility of making additional changes in
PIX
Firewall fragment handling, with the intention of closing additional
```

```
fragmentation-related vulnerabilities. If further changes are made,
they are
likely to be of a relatively major nature, and therefore will probably
appear in a PIX Firewall release after release 4.2.

Workarounds for the PIX Firewall
- ------------------------------
Although there are no direct workarounds for this vulnerability,
customers
can reduce their exposure by avoiding reliance on static NAT entries.
Hosts
actively using dynamic NAT will remain vulnerable to some degree until
fixed
software is installed. However, exploiting the vulnerability against
dynamically allocated addresses is more difficult than exploiting it
against
statically allocated addresses. To exploit the vulnerability via
dynamic
NAT, an attacker must do extra work to determine which dynamic
addresses are
active at any given time, and to which hosts those active addresses
correspond.

CBAC (IOS Firewall Feature Set) Details
=======================================
This vulnerability in the CBAC feature has been assigned Cisco bug ID
CSCdk41516.

Problem Description for CBAC
- ---------------------------
The Cisco IOS CBAC feature, up through all 11.2- and 11.3-based
versions
including 11.2P and 11.3T, and up through 12.0-based versions through
12.0(1) and 12.0(2)T, does no filtering of non-initial IP fragments.
The
CBAC feature performs much of its filtering by dynamically modifying
extended IP access lists,  and, as with all Cisco IOS extended access
lists,
the access lists modified by CBAC  always pass non-initial fragments.

Immediate Response for CBAC
- --------------------------
The following changes will be made to the behavior of the CBAC
feature, and
are presently targeted for versions 12.0(2) and 12.0(3)T:

   * Interfragment state will be kept. Any non-initial fragment will
be
     discarded unless the corresponding initial fragment was permitted
to
     pass through the firewall. Non-initial fragments received before
the
     corresponding initial fragments will be discarded.
```


```
     This applies only to packets being processed by CBAC as
configured with
     the ip inspect configuration commands; fragmentation state checks
will
     not be applied to router traffic not being inspected by CBAC,
even if
     that traffic is filtered with access lists.

     This change eliminates the possibility of overloading host
resources
     with unmatched non-initial fragments, and requires attackers to
use
     relatively elaborate address spoofing for attacks using unmatched
     initial fragments.

     This change may have undesirable effects in certain cases, since
it
     will result in the firewall's discarding any packet whose
fragments
     arrive out of order. There are a number of circumstances that may
cause
     out-of-order delivery of legitimate fragments. Because routers
running
     Cisco IOS software are used in a very large variety of networks,
and
     because the CBAC feature is often used to isolate parts of
internal
     networks from one another, the new behavior will not be enabled
by
     default.  Fragment checking must be explicitly enabled using the
ip
     inspect name inspect-name fragment configuration command. Cisco
     recommends that this command be used whenever CBAC is being used
as an
     Internet firewall, unless there are special circumstances that
dictate
     otherwise. Cisco believes that legitimate out-of-order fragments
are
     rare at Internet firewalls.

   * The amount of memory dedicated to fragmentation state is limited
in
     order to reduce the chance of denial of service attacks against
the
     firewall router itself. Fragmentation state is created only in
response
     to initial fragments, and is kept until either all fragments of
the
     datagram in question have been processed, or a timeout expires.
Initial
     fragments received when fragmentation state resources are
exhausted are
     discarded.

     Unfragmented traffic will never be discarded because of lack of
```

```
     fragment state memory. Even when the system is under heavy attack
with
     fragmented packets, legitimate fragmented traffic, if any, will
still
     get some fraction of the firewall's fragment state resources, and
     legitimate unfragmented traffic will flow unimpeded.

   * Fragment lengths will be checked for legality, and fragment
offsets
     will be checked to avoid port-number overwrite attacks. This
offset
     check duplicates the check already applied by extended access
lists,
     for those unusual configurations where CBAC is being used without
     access lists.

These or equivalent changes will be carried forward into all future
versions
of the IOS Firewall Feature Set.

Getting Fixed Software for CBAC
- -----
Cisco is offering free upgrades to all customers who have purchased
the
IOS Firewall Feature set, regardless of service contract status. Since
there
is no defect in stateless packet filtering, this free upgrade program
does
not apply to customers who have purchased only non-firewall IOS.

When the updated software has been released, customers with service
contracts should obtain Cisco IOS software updates through their usual
channels. Customers with service contracts purchased from Cisco or
from most
resellers may download updates from Cisco's Worldwide Web site.

Customers without service contracts should get their upgrades by
contacting
the Cisco TAC. TAC contacts are as follows:

   * +1 800 553 2447 (toll-free from within North America)
   * +1 408 526 7209 (toll call from anywhere in the world)
     e-mail: tac@cisco.com

Give the URL of this notice as evidence of your entitlement to a free
upgrade. Free upgrades for non-contract customers must be requested
through
the TAC. Please do not contact either "psirt@cisco.com" or
"security-alert@cisco.com" for software upgrades.

As with any new software installation, customers planning to upgrade
should
carefully read the release notes and other relevant documentation
before
```

```
beginning any upgrade. Also, it is important to be certain that the
new
version of Cisco IOS software is supported by your hardware, and
especially
that enough DRAM is available.

Long-term Plans for CBAC
- ----------------------
Cisco is evaluating the  possibility of making additional changes in
Cisco
IOS Firewall Feature Set fragment handling, with the intention of
closing
additional fragmentation-related vulnerabilities. If further changes
are
made, they are likely to be of a relatively major nature, and
therefore will
probably appear in a Cisco IOS software release after release 12.0.

Workarounds for CBAC
- ------------------
There are no CBAC workarounds specific to this vulnerability. However,
customers may be able to reduce their exposure by using dynamic NAT.
Also,
non-extended IP access lists can filter IP fragments, and may be
useful in
controlling potential attacks in some configurations.

Stateless Packet Filters
========================
A stateless IP packet filter, such as a traditional access list in
Cisco
IOS software, must make all of its forwarding decisions for any
specific
packet based only on information in that packet. If the filtering is
based
on criteria such as TCP or UDP port numbers, the necessary information
is
typically present only in the initial fragment of a fragmented
datagram. It
is therefore impossible to tell if a non-initial fragment is part of a
forbidden datagram or of a permitted one. Therefore, stateless packet
filters that use such criteria must pass all, or substantially all,
non-initial fragments. Such filters rely on blocking of initial
fragments to
prevent completed delivery of any forbidden datagrams. This makes them
vulnerable to the fragmentation denial of service attacks discussed in
this
notice.

Extended access lists in Cisco IOS software can filter based on TCP
and
UDP port numbers, as well as based on ICMP packet types, and therefore
fall
into the vulnerable category. A Cisco IOS software extended access
list will
```

pass any non-initial fragment of a fragmented IP datagram.

Stateless packet filters that do not use information such as port numbers do
not suffer from this vulnerability, since all the information used by such
filters is present in every fragment of a datagram. Cisco IOS software's
non-extended access lists do not match on port numbers. They therefore can
(and do) filter non-initial fragments as well as initial fragments.

Vulnerability to fragmentation attacks is a well-known and largely inherent
limitation of stateless IP packet filtering. Cisco does not consider this a
defect in its stateless packet filtering products, and plans no immediate
response for those products. Although Cisco may in the future choose to
improve the fragment handling in its stateless filtering products, there is
no way to completely prevent an attacker from constructing fragments that
will pass any given stateless packet filter if the filtering criteria
include port numbers. There is therefore no way to entirely avoid
fragmentation-based denial of service attacks using such a filter.

Exploitation and Public Announcements
=====================================
This vulnerability is common to numerous packet filtering devices, both
stateful and stateless, from Cisco and other vendors. This vulnerability is
a well-known one in the area of router-based stateless packet filtering, and
is occasionally exploited by attackers when stateless filters are in use.
Exploitation against stateful filters such as the PIX firewall and CBAC may
reasonably be expected to occur from time to time.

Because it is possible to exploit this vulnerability "by accident" with
packet floods of various sorts, this vulnerability probably causes some
number of problems in cases where even the attackers themselves do not fully
understand the mechanism by which they are damaging their targets, as well
as in cases where the attackers have deliberately decided to target this
specific problem.

Cisco knows of no organized, systematic exploitation specific to this

vulnerability, but flooding attacks that could exercise it are reasonably
common events on the Internet. Such flooding attacks cause a wide range of
negative responses in targeted networks, and this vulnerability represents
one of those negative responses.

Flooding tools capable of exploiting this vulnerability are widely
available. Special-purpose tools designed to selectively exploit this
vulnerability seem relatively uncommon, but Cisco has not conducted a
thorough search for such tools. Such a tool would be easy for a moderately
sophisticated network programmer to produce.

This vulnerability has been publicly discussed with specific reference to
the Cisco PIX Firewall on the BUGTRAQ mailing list, beginning in late August
of 1998. There have been many other discussions in other public forums
regarding this vulnerability as it applies to packet filters in general, and
it is reasonable to suppose that there may have been public discussions of
this vulnerability as applied specifically to Cisco products. This
vulnerability should be considered to be widely known in both the computer
security community and the "cracker" community.

Status of This Notice
=====================
This is a final field notice. Although Cisco cannot guarantee the accuracy
of all statements in this notice, all the facts have been checked to the
best of our ability. Cisco does not anticipate issuing updated versions of
this notice unless there is some material change in the facts. Should there
be a significant change in the facts, Cisco may update this notice.

Distribution
- ----------
This notice will be posted on Cisco's Worldwide Web site at
http://www.cisco.com/warp/public/770/nifrag.shtml. In addition to Worldwide
Web posting, the initial version of this notice is being sent to the
following e-mail and Usenet news recipients:

* cust-security-announce@cisco.com
* bugtraq@netspace.org
* first-teams@first.org (includes CERT/CC)
* cisco@spot.colorado.edu
* comp.dcom.sys.cisco

```
   * first-info@first.org
   * Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's
Worldwide
Web server, but may or may not be actively announced on mailing lists
or
newsgroups. Users concerned about this problem are encouraged to check
the
URL given above for any updates.

Revision History
- --------------
Revision 1.0,        Initial released version
15:30 US/Pacific,
10-SEP-1998

Revision 1.1,        REAL initial released version; corrected PIX
07:00 AM US/Pacific, release date
11-SEP-1998

Cisco Security Procedures
=========================
Please report security issues with Cisco products, and/or sensitive
security
intrusion emergencies involving Cisco products, to security-
alert@cisco.com.
Reports may be encrypted using PGP; public RSA and DSS keys for
"security-alert@cisco.com" are on the public PGP keyservers.

The alias "security-alert@cisco.com" is used only for reports incoming
to
Cisco. Mail sent to the list goes only to a very small group of users
within
Cisco. Neither outside users nor unauthorized Cisco employees may
subscribe
to "security-alert@cisco.com".

Please do not use "security-alert@cisco.com" for configuration
questions,
for security intrusions that you do not consider to be sensitive
emergencies, or for general, non-security-related support requests. We
do
not have the capacity to handle such requests through this channel,
and will
refer them to the TAC, delaying response to your questions. We advise
contacting the TAC directly with these requests. TAC contact numbers
are as
follows:

   * +1 800 553 2447 (toll-free from within North America)
   * +1 408 526 7209 (toll call from anywhere in the world)
   * e-mail: tac@cisco.com
```

```
All formal public security notices generated by Cisco are sent to the
public
mailing list "cust-security-announce@cisco.com". For information on
subscribing to this mailing list, send a message containing the single
line
"info cust-security-announce" to "majordomo@cisco.com". An analogous
list,
"cust-security-discuss@cisco.com" is available for public discussion
of the
notices and of other Cisco security issues.

=============================================================
This notice is copyright 1998 by Cisco Systems, Inc. This notice may
be
redistributed freely after the release date given at the top of the
notice,
provided that redistributed copies are complete and unmodified,
including
all date and version information.
=============================================================
```

Summary of Fragmentation Attack

As shown by the above advisory there is a vulnerability in release 4.2(1) and earlier versions of the PIX IOS which may be exploitable to cause Denial of Service attacks.

Early versions of the PIX IOS only dropped the initial fragment of blocked datagrams. As a result if a user sent data that should be blocked as a stream of fragments only the initial packet was blocked and all other fragments were passed on through the PIX. This behaviour left hosts that could be reached through the firewall, such as ones not using NAT or with Static NAT entries, susceptible to Denial of Service attacks using fragmentation attacks such as Teardrop and Ping of Death.

Since the PIX does not check to see if non initial fragments belong to an existing connection that was blocked it is possible for any outside hosts to send fragments to any inside host. Obviously hosts using dynamic NAT would be harder to exploit because first you would have to determine which hosts are active currently on what addresses. However no host would be protected from a fragmentation attack.

Later versions of the IOS software have corrected this problem and interfragment state is now being kept. As a result fragments are checked against entries in the state table and if the initial fragment was not permitted the non initial fragments will be discarded.

There is one problem with this in that if a non initial fragment arrives before the initial fragment it will be discarded even though it may be valid. However the risk of not doing so far out weighs the possibility of valid fragments being discarded and therefore everybody should insure they are running the latest release of the IOS. Running the latest version of IOS will protect from possible fragmentation attacks as well as other vulnerabilities.

Cisco Secure PIX Firewall FTP Vulnerabilities[7]

```
Cisco Secure PIX Firewall FTP Vulnerabilities

Revision 1.3

For public release 2000 March 16 05:00 PM US/Pacific (UTC+0800)
================================================================
=

Summary
=======

The Cisco Secure PIX Firewall interprets FTP (File Transfer Protocol)
commands out of context and inappropriately opens temporary access
through
the firewall.  This is an interim notice describing two related
vulnerabilities.

The first vulnerability is exercised when the firewall receives an
error
message from an internal FTP server containing an encapsulated command
such
that the firewall interprets it as a distinct command.  This
vulnerability
can be exploited to open a separate connection through the firewall.
This
vulnerability is documented as Cisco Bug ID CSCdp86352.

The second vulnerability is exercised when a client inside the
firewall
browses to an external server and selects a link that the firewall
interprets as two or more FTP commands.  The client begins an FTP
connection
as expected and at the same time unexpectedly executes another command
opening a separate connection through the firewall.  This
vulnerability is
documented as Cisco Bug ID CSCdr09226.

Either vulnerability can be exploited to transmit information through
the
firewall without authorization.

Fixed software and workarounds are available to address the first
vulnerability.  Fixed software is not yet available for the second
vulnerability but a workaround is provided.


Who Is Affected
===============
```

[7] Complete advisory and explanation as posted at http://packetstormsecurity.org/advisories/cisco/cisco.pix-ftp.txt

All users of Cisco Secure PIX Firewalls with software versions up to and
including 4.2(5), 4.4(4), and 5.0(3) that provide access to FTP services are
at risk from both vulnerabilities.

Cisco Secure PIX Firewall with software version 5.1(1) is affected by the
second vulnerability only.

Cisco Secure Integrated Software (formerly Cisco IOS® Software Firewall
Feature Set) is not affected by either vulnerability.

Impact
======

Any Cisco Secure PIX Firewall that has enabled the fixup protocol ftp
command is at risk of unauthorized transmission of data through the
firewall.

Details
=======

The first vulnerability has been assigned Cisco bug ID CSCdp86352. The
second vulnerability has been assigned Cisco bug ID CSCdr09226.

The behavior is due to the command fixup protocol ftp [portnum], which is
enabled by default on the Cisco Secure PIX Firewall.

If you do not have protected FTP hosts with the accompanying configuration
(configuration example below) you are not vulnerable to the attack which
causes a server to send a valid command, encapsulated within an error
message, and causes the firewall to read the encapsulated partial command as
a valid command (CSCdp86352).

To exploit this vulnerability, attackers must be able to make connections to
an FTP server protected by the PIX Firewall. If your Cisco Secure PIX
Firewall has configuration lines similar to the following:

```
        fixup protocol ftp 21
```

and either

```
        conduit permit tcp host 192.168.0.1 eq 21 any
```

```
or

          conduit permit tcp 192.168.0.1 255.255.255.0 eq 21 any


It is possible to fool the PIX stateful inspection into opening up
arbitrary
TCP ports, which could allow attackers to circumvent defined security
policies.

If you permit internal clients to make arbitrary FTP connections
outbound,
you may be vulnerable to the second vulnerability (CSCdr09226).  This
is an
attack based on CERT advisory "CA-2000-02: Malicious HTML Tags
Embedded in
Client Web Requests" and
detailed in the BUGTRAQ post: "Extending the FTP 'ALG' vulnerability
to any
FTP client".

The recommendation in the workarounds section of this document will
provide
protection against this vulnerability.


Response for the first vulnerability (CSCdp86352)
================================================

The following changes have been made to the "fixup protocol FTP"
behavior of
the PIX Firewall:

   * Enforce that only the server can generate a  reply indicating the
PASV
     command was accepted.
   * Enforce that only the client can generate a PORT command.
   * Enforce that data channel is initiated from the expected side in
an FTP
     transaction.
   * Verify that the "227" reply code and the PORT command are
complete
     commands and not part of a "500" error code string broken into
     fragments.
   * Enforce that the port is not 0 or in the range between [1,1024]

These or equivalent changes will be carried forward into all PIX
Firewall
software versions after version 5.1(1).


Response for the second vulnerability (CSCdr09226)
==================================================
```

Cisco is working on a fix for this issue. This notice will be updated when
we have produced a fix.

Software Versions and Fixes
==========

Getting Fixed Software
==========

Cisco is offering free software upgrades to remedy this vulnerability for
all affected customers. Customers with service contracts may upgrade to any
software version. Customers without contracts may upgrade only within a
single row of the table below, except that any available fixed software will
be provided to any customer who can use it and for whom the standard fixed
software is not yet available. As always, customers may install only the
feature sets they have purchased.

Version Affected	Interim Release**(fix will carry forward into all later versions) Available Now through the TAC	Projected first fixed regular release (fix will carry forward into all later versions)
All versions of Cisco Secure PIX up to version 4.2(5) (including 2.7, 3.0, 3.1, 4.0, 4.1)	4.2(5)205**	4.2(6) Currently not scheduled.*
All 4.3.x and 4.4.x up to and including version 4.4(4)	4.4(4)202**	4.4(5) Estimated date available: 2000 April 15*
All 5.0.x up to and including version 5.0(1)	5.0(3)202**	5.0(4) Estimated date available: 2000 April 30*
Version 5.1(1) - not affected-	unaffected	Currently available

* All dates are tentative and subject to change

** Interim releases are subjected to less internal testing and verification
than are regular releases, may have serious bugs, and should be installed
with great care.

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should
be obtained via the Software Center on Cisco's Worldwide Web site at http://www.cisco.com/.

Customers without contracts should get their upgrades by contacting the
Cisco Technical Assistance Center (TAC). TAC contacts are as follows:

* +1 800 553 2447 (toll-free from within North America)
* +1 408 526 7209 (toll call from anywhere in the world)
* e-mail: tac@cisco.com

Give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through
the TAC. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Hardware requirements
=====================

If version 4.3 or 4.4 is utilized on a PIX 'Classic' (excludes PIX10000,
PIX-510, PIX-520, and PIX-515)

or

If version 5.0 is utilized on a PIX 'Classic', PIX10000, or PIX-510 (excludes PIX-520 and PIX-515)

A 128MB upgrade for the PIX Firewall is necessary. As with any new software
installation, customers planning to upgrade should carefully read the release notes and other relevant documentation before beginning any upgrade.
Also, it is important to be certain that the new version of Cisco Secure PIX
Firewall software is supported by your hardware, and especially that enough
memory is available.

Workarounds
===========

The behaviors described in this document are a result of the default command
"fixup protocol ftp [portnum]". To disable this functionality, enter the
command "no fixup protocol ftp". This will disable support of the fixup of

the FTP protocol in the PIX, and will eliminate the vulnerabilities. The
command "fixup protocol ftp 21" is the default setting of this feature, and
is enabled by default on the Cisco Secure PIX Firewall.

This workaround will force your clients to use FTP in passive mode, and
inbound FTP service will not be supported. Outbound standard FTP will not
work without fixup protocol ftp 21, however, passive FTP will function
correctly with no fixup protocol ftp configured.

Exploitation and Public Announcements
=====================================

This vulnerability was proposed on the BUGTRAQ list, and in follow-ups to
the article, the Cisco Secure PIX Firewall was also identified as
susceptible. As the vulnerabilities have been widely discussed, Cisco is
posting this advisory prior to having a full fix. We will update this
notice again, when we have a full fix available.

Cisco has had no reports of malicious exploitation of this vulnerability.
However, versions of exploit scripts have been posted to various security
related lists.

This vulnerability was reported to Cisco via several sources, shortly after
the time of the original supposition.

Status of This Notice
=====================

This is an interim field notice. Although Cisco cannot guarantee the
accuracy of all statements in this notice, all the facts have been checked
to the best of our ability. Cisco anticipates issuing updated versions of
this notice within two weeks.

Distribution
============

This notice will be posted on Cisco's Worldwide Web site at
http://www.cisco.com/warp/public/707/pixftp-pub.shtml. In addition to
Worldwide Web posting, the initial version of this notice is being sent to
the following e-mail and Usenet news recipients:

```
   * cust-security-announce@cisco.com
   * bugtraq@securityfocus.com
   * first-teams@first.org (includes CERT/CC)
   * cisco@spot.colorado.edu
   * comp.dcom.sys.cisco
   * firewalls@lists.gnac.com
   * Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's
Worldwide
Web server, but may or may not be actively announced on mailing lists
or
newsgroups. Users concerned about this problem are encouraged to check
the
URL given above for any updates.


Revision History
================

 Revision 1.02000 March 16 08:00 AM US/Pacific (UTC+0800)- Initial
public
             release

 Revision 1.12000 March 16 08:00 AM US/Pacific (UTC+0800) - Link
             corrections, table head clarification.

 Revision 1.32000 March 16 14:00 PM US/Pacific (UTC+0800) - Addition
of 2nd
             vulnerability issues.


Cisco Security Procedures
=========================

Complete information on reporting security vulnerabilities in Cisco
products, obtaining assistance with security incidents, and
registering to
receive security information from Cisco, is available on Cisco's
Worldwide
Web site at
http://www.cisco.com/warp/public/707/sec_incident_response.shtml. This
includes instructions for press inquiries regarding Cisco security
notices.
  -----------------------------------------------------------------
-------
This notice is copyright 2000 by Cisco Systems, Inc. This notice may
be
redistributed freely after the release date given at the top of the
text,
provided that redistributed copies are complete and unmodified,
including
all date and version information.
```

Summary of FTP Vulnerabilities

As shown by the above advisory there are two vulnerabilities in release 5.0(3) and earlier versions of the PIX IOS which may be exploitable to cause unauthorized data to pass through the firewall. In addition IOS release 5.1(1) is vulnerable to the second exploit only.

For the first vulnerability to be exploited you must allow access to an ftp server protected by a PIX firewall that is running the fixup protocol ftp command. If these conditions exist it is possible to trick the PIX firewall into opening up arbitrary TCP ports in it's state table.

You can open a separate connection through the firewall by having an internal ftp server send an error message that contains an encapsulated command to the firewall. The firewall misinterprets this as a separate distinct command and temporarily opens a new tcp connection allowing attackers to bypass your security rules.

For the second vulnerability to be exploited you must allow internal clients to make outbound ftp connections. If you do it is possible for clients browsing an ftp external server to access a link that the firewall mistakenly sees as two or more ftp commands. When this happens the client begins an ftp connection as expected but at the same time completes another command that opens a new connection through the firewall.

Once this new connection is opened through the firewall it is possible to pass data through this connection which would normally be blocked by your security rules.

In order to protect your PIX from this and other vulnerabilities is recommended to insure that you are running the latest release of the PIX software as well as watching for any new known vulnerabilities in the software.

Possible Attack using TCP Reset Attack

Since Mr. Kellogg does not specify the version of his PIX software I have assumed that he is running version 5.1(1) or earlier. This being the case his firewall would be susceptible to the TCP reset vulnerability.

Mr. Kellogg's PIX is only using source port, source IP, destination port, and destination IP to track connections in the firewall's state table. If we can determine these four parameters for any active sessions taking place through the PIX it may be possible to disrupt these services.

Therefore I plan to attempt to disrupt GIAC's larger customers from accessing GIAC Enterprises' web site. We can easily determine the IP address of the web server by simply doing a DNS lookup for GIAC's web site. We also know which port it will be using since it is a web site and therefore port 80. Already with very minimal effort we have two of the four parameters needed to allow a remote third party to disrupt the connection.

The last two parameters will be considerably harder to determine. We know the client port will be greater than 1023 and less than 65535. As a result we can write a script that starts at port 1024 and increments by one until it reaches 65535. If we use this as the source port we know we will cover all the possibilities valid for this parameter.

Finally the last parameter or IP address of the clients could be anything since anyone anywhere on the Internet may be browsing the web server. It would be very hard to accurately guess a valid IP address, however there are a couple of ways that we can significantly reduce the number of likely IP addresses to be accessing the web server.

One method of greatly reducing the likely candidates is if you are able to sniff traffic entering and leaving GIAC's firewall. By analyzing this data you will be able to determine frequent users of the web server and use their IP addresses in your attack. However in order to monitor this traffic you would have to somehow get a device at their perimeter to sniff data and capture it for later analysis. This may not be possible although if it is this would provide very accurate IP information for use in the attack.

Instead I will resort to the second method which may provide less accurate information but is generally much easier to obtain. I will use social engineering to try and determine as much information as possible about GIAC's customer base. Social Engineering is a method where by you get employees of GIAC or other organization to provide you with information which they may not consider sensitive or see as dangerous which you can then use in your attack attempts.

Companies are usually very proud of some of their large accounts and typically freely boast of who some of their clients are. By compiling a list of GIAC's top 5 clients and some doing reconnaissance of those clients we should be able to get a list of likely IP's that frequent the web site.

Many people and companies today use PAT (Port Address Translation) for their clients when browsing the web. If we determine that 4 of GIAC's top 5 customers use PAT and we can use further reconnaissance and social engineering to determine what single IP address these customers use for PAT of outbound connections it will give us 4 likely IP addresses to use for the client address in our attack.

One way to possibly determine what IP address they PAT to is again to use social engineering. Simply calling up an IT person at one of these companies and pretending that you are trying to trouble shoot a connection issue, one of their users is having when

trying to connect to your web site. By telling this individual you are checking the logs for issues and were wondering what IP address range their users would be coming from he may come right out and tell you the IP they use for PAT. Another possibility is to call up a user at one of these sites and using some pretense have him connect to a box you are using just for this purpose. You can then monitor the box and see what IP address the connection came from.

Once we have gathered this information we can use four machines to implement our attack. Now that we have compiled a list of values to use for each parameter in our attack we can launch our attack against the firewall.

We simply send forged packet resets to the firewall using the IP address of the web server, and port 80 for the destination parameters, and on each client we use one of our four likely client IP addresses for the source IP and the script increments from 1024 – 65535 for the port as the destination parameters.

Since the PIX can not distinguish these forged resets from real ones every time they match an active session in the state table the PIX will tear the session down. As a result active sessions from these clients to the web site will be disconnected.

The results of this attack will be clients sporadically being disconnected from the web server every time a forged reset matches an active session . This type of problem is very hard to diagnose and may cause GIAC problems for some time with their customers calling and saying that they keep getting disconnected from the web server.

To prevent this type of attack an OS upgrade on the PIX is required.

Denial of Service Attack

I have chosen an ICMP flood attack which is extremely easy to implement. I simply went to www.powertech.no/smurf/ to get a list of possible amplification sites that are available to use. The following were posted as the top ten amplification sites.

Current top ten smurf amplifiers (updated every 5 minutes)
(last update: 2001-10-09 13:31:56 CET)[8]

Network Registered at	#Dups Home AS	#Incidents	
212.1.130.0/24	38	0	1999-02-20 09:41 AS9105
129.78.64.0/24	37	0	1998-08-13 08:54 AS7570
209.241.162.0/24	27	0	1999-02-20 08:51 AS701
204.158.83.0/24	27	0	1999-02-20 10:09 AS3354

[8] Top Ten List of Smurf Amplifiers from www.powertech.no/smurf/

159.14.24.0/24	20	0	1999-02-20 09:39 AS2914
204.193.121.0/24	19	0	1999-02-20 08:54 AS701
192.220.134.0/24	19	0	1999-02-20 09:38 AS685
198.253.187.0/24	16	0	1999-02-20 09:34 AS22
164.106.163.0/24	14	0	1999-02-20 10:11 AS7066
199.98.24.0/24	13	0	1999-02-18 11:09 AS6199

2412156 networks have been probed with the SAR
601 of them are currently broken
192217 have been fixed after being listed here

(clicking on any of the above will only show the verbose registry object for the network, it will not be re-probed)

In order to attack the chosen site all that is required is to send a spoofed ping packet to the broadcast address of one of the above registered sites using the source IP of the victim's external IP address. This will result in all PC's on the network sending an echo-reply to the victim. Even if the victim discards or filters echo-replies they will still not be protected. Since the packets have to get to the firewall in order to be filtered there will be too much traffic and congestion on the pipe that no valid traffic can get in or out.

This simple attack is not easily defended against and requires no special tools. The counter measures that can be put in place to help defend against this attack are to have two redundant Internet paths. However if the attacker is aware of this they can just as easily attack both paths by sending a spoofed ping packet using both external IP's as source addresses. It is also possible to block the attack once started, as long as you can identify it, by having your ISP discard the ICMP packets on their end where the pipe is considerably larger before they flood your pipe. The other possibility is if you do not require ICMP packets and your ISP is willing to block all ICMP traffic at the ISP's interface preventing them from ever entering your pipe.

An Attack Against the Mail Server Through the PIX

Cisco Secure PIX Firewall Mailguard Vulnerability[9]

```
Cisco Security Advisory: Cisco Secure PIX Firewall Mailguard
Vulnerability

Revision 1.1

Updated, for public release 2000 October 5 04:00 PM US/Pacific
(UTC+0700)
```

```
Summary

   The Cisco Secure PIX firewall feature "mailguard," which limits
SMTP
   commands to a specified minimum set of commands, can be bypassed.

   This vulnerability can be exploited to bypass SMTP command
filtering.

   This vulnerability has been assigned Cisco bug ID CSCdr91002 and
   CSCds30699.

   A new aspect of this vulnerability has been assigned Cisco bug ID
   CSCds38708.

   The complete advisory is available at
   http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-
pub.shtml.

Affected Products

   All users of Cisco Secure PIX Firewalls with software versions up
to
   and including 4.4(6), 5.0(3), 5.1(3) and 5.2(2) that provide access
to
   SMTP Mail services are at risk.

   The IOS Firewall featureset is not affected by either of the above
   defects.

Details

   The behavior is a failure of the command "fixup protocol smtp
   [portnum]", which is enabled by default on the Cisco Secure PIX
   Firewall.

   If you do not have protected Mail hosts with the accompanying
   configuration (configuration example below) you are not affected by
   this vulnerability.

   To exploit this vulnerability, attackers must be able to make
```

[9] Complete advisory and explanation as posted at http://packetstormsecurity.org/advisories/cisco/cisco.00-09-27.ciscosecure_pix

```
   connections to an SMTP mail server protected by the PIX Firewall.
If
   your Cisco Secure PIX Firewall has configuration lines similar to
the
   following:

             fixup protocol smtp 25

   and either

             conduit permit tcp host 192.168.0.1 eq 25 any

   or

             conduit permit tcp 192.168.0.1 255.255.255.0 eq 25 any

   or

             access-list 100 permit tcp any host 192.168.0.1 eq 25
             access-group 100 in interface outside

   The expected filtering of the Mailguard feature can be circumvented
by
   an attacker.

  Impact

   The Mailguard feature is intended to help protect weakly secured
mail
   servers.  The workaround for this issue is to secure the mail
servers
   themselves, or upgrade to fixed PIX firewall code.

   In order to exploit this vulnerability, an attacker would need to
also
   exploit the mailserver that is currently protected by the PIX.  If
   that server is already well configured, and has the latest security
   patches and fixes from the SMTP vendor, that will minimize the
   potential for exploitation of this vulnerability.

Software Versions and Fixes

  Getting Fixed Software

   Cisco is offering free software upgrades to remedy this
vulnerability
   for all affected customers. Customers with service contracts may
   upgrade to any software version. Customers without contracts may
   upgrade only within a single row of the table below, except that
any
   available fixed software will be provided to any customer who can
use
   it and for whom the standard fixed software is not yet available.
As
   always, customers may install only the feature sets they have
```

purchased.

	Fixed Regular Release available now; fix will carry forward into all later releases
All versions of Cisco Secure PIX up to version 4.4(6) (including 2.7, 3.0, 3.1, 4.0, 4.1)	4.4(7)
Version 5.0.x up to and including version 5.0(3)	5.1(4)
All 5.1.x up to and including version 5.1(3)*	5.1(4)
Version 5.2(2)	5.2(3)

*For customers who may have engineering releases addressing specific unrelated defects, designated as 5.1(2)2xx, version 5.1(4) only includes the SMTP security fixes and does not include any other bugfixes. Customers requiring engineering releases to address specific unrelated defects will need to use 5.1.4(200) or 4.4.7(200), which include all SMTP vulnerability fixes.

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained via the Software Center on Cisco's Worldwide Web site at http://www.cisco.com.

Customers without contracts should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as

```
   follows:
     * +1 800 553 2447 (toll-free from within North America)
     * +1 408 526 7209 (toll call from anywhere in the world)
     * e-mail: tac@cisco.com

   Give the URL of this notice as evidence of your entitlement to a
free
   upgrade. Free upgrades for non-contract customers must be requested
   through the TAC. Please do not contact either "psirt@cisco.com" or
   "security-alert@cisco.com" for software upgrades.

Workarounds

   There is not a direct work around for this vulnerability.  The
   potential for exploitation can be lessened by ensuring that mail
   servers are secured without relying on the PIX functionality.

Exploitation and Public Announcements

   This vulnerability was first reported to Cisco by a customer.  This
   vulnerability has been discussed on public forums.

Status of This Notice: Revised FINAL

   This is a final field notice. Although Cisco cannot guarantee the
   accuracy of all statements in this notice, all of the facts have
been
   checked to the best of our ability.   Cisco does not anticipate
   issuing updated versions of this notice unless there is some
material
   change in the facts. Should there be a significant change in the
   facts, Cisco may update this notice.

Distribution

   This notice will be posted on Cisco's Worldwide Web site at
   http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-
pub.shtml.
   In addition to Worldwide Web posting, a text version of this notice
is
   clear-signed with the Cisco PSIRT PGP key and is posted to the
   following e-mail and Usenet news recipients:
     * cust-security-announce@cisco.com
     * bugtraq@securityfocus.com
     * first-teams@first.org (includes CERT/CC)
     * cisco@spot.colorado.edu
     * comp.dcom.sys.cisco
     * firewalls@lists.gnac.com
     * Various internal Cisco mailing lists

   Future updates of this notice, if any, will be placed on Cisco's
   Worldwide Web server, but may or may not be actively announced on
   mailing lists or newsgroups. Users concerned about this problem are
   encouraged to check the URL given above for any updates.
```

```
Revision History

   Revision 1.1  05-OCT-2000  New defect ID reference, and revised the
Fixed
in versions to
                              reflect recent fixes.
   Revision 1.0  27-SEP-2000  Initial Public Release

Cisco Security Procedures

   Complete information on reporting security vulnerabilities in Cisco
   products, obtaining assistance with security incidents, and
   registering to receive security information from Cisco, is
available
   on Cisco's Worldwide Web site at
   http://www.cisco.com/warp/public/707/sec_incident_response.shtml.
This
   includes instructions for press inquiries regarding Cisco security
   notices.
     ___________________________________________________________________

   This notice is copyright 2000 by Cisco Systems, Inc. This notice
may
   be redistributed freely after the release date given at the top of
the
   text, provided that redistributed copies are complete and
unmodified,
   including all date and version information.
     ___________________________________________________________________
```

Summary of Mailguard Vulnerability

As shown by the above advisory there is a vulnerability in release 5.2(2) and earlier versions of the PIX IOS that allows users to bypass the SMTP command filtering.

Mailguard is a feature of the PIX firewall that is suppose to protect poorly secured mail servers by limiting the commands that can be sent to them. Mailguard is suppose to limit the data allowed to the mail server to be valid SMTP commands of HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. All other commands are rejected.

However a failure of the Mailguard feature in earlier releases of the IOS software allowed this filtering to be bypassed and left mail servers behind the PIX vulnerable to attack.

Since the fixup protocol was not working as expected users would be able to circumvent the SMTP filtering and have access to the mail server to attempt to exploit it.

In order to protect against this and other vulnerabilities you should insure your PIX is running the latest IOS release and monitor for new vulnerabilities to be discovered.

Cert Advisory for Sendmail Vulnerability[10]

CERT® Advisory CA-1997-05 MIME Conversion Buffer Overflow in Sendmail Versions 8.8.3 and 8.8.4

Original issue date: January 28, 1997
Last revised: September 26, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received reports of a vulnerability in sendmail versions 8.8.3 and 8.8.4. By sending a carefully crafted email message to a system running a vulnerable version of sendmail, intruders may be able to force sendmail to execute arbitrary commands with root privileges.

The CERT/CC team recommends that you install a vendor patch (Section III.A) or upgrade to sendmail 8.8.5 (Section III.B). We have provided a workaround that you can use on vulnerable versions of 8.8.3 and 8.8.4 until you are able to implement one of these solutions (Section III.C).

Regardless of the solution you apply, we urge you to take the additional precautions described inSection III.D. Note that this advisory contains additional material to that previously published by other response teams.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

Sendmail version 8 contains support for MIME (Multipurpose Internet Mail Extensions) as defined initially by RFC 1341 and modified by RFC 1521. The central idea behind MIME is the following, taken from the introduction to RFC 1341:

"... designed to provide facilities to include multiple objects in a single message, to represent body text in character sets other than US-ASCII, to represent formatted multi-font text messages, to represent non-textual material such as images and audio fragments, and generally to facilitate later extensions defining new types of Internet mail for use by cooperating mail agents."

The support in sendmail version 8 includes data translations in which a message's body is either stripped to 7-bit ASCII, achieved by forcing the 8th bit to be off, or 8-bit MIME, achieved by leaving the 8th bit as is.

Sendmail can be configured for either of these translations on a mailer-by-mailer basis depending on the flags defined for that mailer. The flags in question here are `7', `8', and `9'

[10] Complete advisory and explanation as posted at http://www.cert.org/advisories/CA-1997-05.html

(the default). Refer to the "Sendmail Installation and Operations Guide," Section 5.4, for a more complete discussion. A PostScript version of this guide is included in the sendmail distribution in the /doc/op directory.

With the release of sendmail version 8.8.3, a serious security vulnerability was introduced that allows remote users to execute arbitrary commands on the local system with root privileges. By sending a carefully crafted email message to a system running a vulnerable version of sendmail, intruders may be able to force sendmail to execute arbitrary commands with root privileges. Those commands are run on the same system where the vulnerable sendmail is running.

In most cases, the MIME conversion of email is done on final delivery; that is, to the local mailbox or a program. Therefore, this vulnerability may be exploited on systems despite firewalls and other network boundary protective measures.

Versions before 8.8.3 do not contain this vulnerability, but they do contain other vulnerabilities. We strongly recommended that you follow the steps given in Section III below to eliminate those vulnerabilities from your systems.

Determining if you are vulnerable

Systems are vulnerable to this attack if both of the following conditions are true:

1. **The version of sendmail is 8.8.3 or 8.8.4.**

   To determine the version of sendmail, use the following command:

   % /usr/lib/sendmail -d0 -bt < /dev/null | grep -i Version

   If the string returned is "Version 8.8.3" or "Version 8.8.4", then this version of sendmail contains the vulnerability. Typically, sendmail is located in the /usr/lib directory, but it may be elsewhere on your system.

2. **When you examine the sendmail configuration file (usually, /etc/sendmail.cf), the `9' flag is set in the "F=" (Flags) section for any Mailer specifications (Sections starting with `M' in the first column, such as "Mprog" or "Mlocal").**

   Use of the `9' flag can usually be determined using the following command (depending on your sendmail configuration):

   % grep '^M.*F=[^,]*9' /etc/sendmail.cf

   If any lines are output from this command, then the sendmail configuration may be vulnerable.

   The `9' flag is set by default for the local and program mailers when the sendmail.cf file is generated using the m4 files distributed with sendmail version 8.8.x. Versions of sendmail before 8.8.0 did not set this flag by default when generating sendmail.cf. The `9' flag is also set by default in the precompiled example configuration files found in the cf/cf/obj/ subdirectory of the sendmail version 8.8.x distribution.

II. Impact

Remote users can gain root privileges on a machine running sendmail versions 8.8.3 or 8.8.4 that does 7-to-8 bit conversion. They do not need access to an account on the system to exploit the vulnerability.

III. Solution

Install a patch from your vendor if one is available (Section A) or upgrade to the current version of sendmail (Section B). Until you can take one of those actions, we recommend applying the workaround described in Section C. In all cases, you should take the precautions described in Section D.

A. Install a vendor patch.

Below is a list of vendors who have provided information about sendmail. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Caldera OpenLinux
Cray Research - A Silicon Graphics Company
Data General Corporation
Digital Equipment Corporation
Hewlett-Packard Corporation
IBM Corporation
NEC Corporation
NeXT Software, Inc.
Silicon Graphics, Inc.
Sun Microsystems, Inc.

B. Upgrade to sendmail version 8.8.5.

Eric Allman has released a new version of sendmail which fixes this vulnerability. This can be obtained from the following locations:

ftp://ftp.sendmail.org/pub/sendmail/
ftp://ftp.cs.berkeley.edu/ucb/src/sendmail/
ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/
ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/
ftp://ftp.cert.org/pub/tools/sendmail/

The MD5 checksum for this distribution is:

MD5 (sendmail.8.8.5.patch) = 775c47d16d40ebd2b917dfcc65d92e90

MD5(sendmail.8.8.5.tar.gz) = 7c32c42a91325dd00b8518e90c26cffa

MD5 (sendmail.8.8.5.tar.sig) = b62ba16c7e863853b3efeb955eec4214

MD5 (sendmail.8.8.5.tar.Z) = 7b847383899c0eb65987213a5caf89c8

Also in that directory are .Z and .sig files. The .Z file contains the same bits as the .gz file, but it is compressed using UNIX compress instead of gzip. The .sig is Eric Allman's PGP signature for the uncompressed tar file. The key fingerprint is

```
 Type bits/keyID    Date       User ID
 pub  1024/BF7BA421 1995/02/23 Eric P. Allman eric@CS.Berkeley.EDU
        Key fingerprint =  C0 28 E6 7B 13 5B 29 02  6F 7E 43 3A 48 4F
45 29
                                Eric P. Allman  eric@Reference.COM
                                Eric P. Allman  eric@Usenix.ORG
                                Eric P. Allman  eric@Sendmail.ORG
                                Eric P. Allman  eric@CS.Berkeley.EDU
```

When you change to a new version of sendmail, we strongly recommend also changing to the configuration files that are provided with that version. (In fact, it is highly likely that older configuration files will not work correctly with sendmail version 8.) It is now possible to build a sendmail configuration file (sendmail.cf) using the configuration files provided with the sendmail release. Consult the cf/README file for a more complete explanation. Creating your configuration files using this method makes it easier to incorporate future changes to sendmail into your configuration files.

C. Workaround for existing sendmail version 8.8.3 and 8.8.4 installations

Eric Allman, the author of sendmail, has provided the following workaround, which you can use until you can take the steps recommended in Sec. A or B.

The /etc/sendmail.cf file should be modified to remove the use of the `9' flag for all Mailer specifications (lines starting with `M').

As an example, the sendmail.cf file should look similar to the following which is for a Solaris 2.5.1 system running sendmail version 8.8.4:

```
                P=/usr/lib/ml.local, F=lsDFMAw5:/|@qSnE, S=10/30, R=20/40,
Mlocal,         T=DNS/RFC822/X-Unix,
                A=mail -d $u
                P=/usr/local/bin/smrsh, F=lsDFMoqeu, S=10/30, R=20/40,
Mprog,          D=$z:/,
                T= X-UNix,
!               A=smrsh -c $u
```

This can be achieved for the "Mlocal" and "Mprog" Mailers by modifying the ".mc" file to include the following lines:

```
                OSTYPE(solaris2)
                FEATURE(smrsh, /usr/local/bin/smrsh)
+               define(`LOCAL_SHELL_ARGS', `smrsh -c $u')
                define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)
                define(`LOCAL_MAILER_FLAGS',
                        ifdef(`LOCAL_MAILER_FLAGS',
```

```
                        `translit(LOCAL_MAILER_FLAGS, `9')',
                        `rmn'))
define(`LOCAL_SHELL_FLAGS',
        ifdef(`LOCAL_SHELL_FLAGS',
                        `translit(LOCAL_SHELL_FLAGS, `9')',
                        `eu'))
```

Next, rebuild the sendmail.cf file using m4(1). See also Section III.D for additional precautions that you should take. These precautions have been taken in the example above.

The defines of LOCAL_MAILER_FLAGS and LOCAL_SHELL_FLAGS should be placed in your m4(1) input file *after* the operating system is identified using the OSTYPE directive, and after any other defines of either the LOCAL_MAILER_FLAGS or LOCAL_SHELL_FLAGS.

It is possible to directly edit the sendmail.cf file to resolve this vulnerability. However, take caution to ensure that the sendmail.cf file is not replaced in the future with a new version rebuilt from configuration files that include the `9' flag.

Once the configuration file has been modified, all running versions of sendmail should be killed and the sendmail daemon restarted with the following (done as root):

```
# kill -1 `head -1 /var/run/sendmail.pid`
```

The pathname may be different on your system. Verify that a new daemon was started using "(echo quit; sleep 1) | telnet localhost 25". Alternatively, reboot your system.

D. Take additional precautions

Regardless of which solution you apply, you should take these extra precautions to protect your systems. These precautions do not address the vulnerabilities described herein, but are recommended as good practices to follow for the safer operation of sendmail.

- Use the sendmail restricted shell program (smrsh)

  With *all* versions of sendmail, use the sendmail restricted shell program (smrsh). You should do this whether you use vendor-supplied sendmail or install sendmail yourself. Using smrsh gives you improved administrative control over the programs sendmail executes on behalf of users.

  Many sites have reported some confusion about the need to continue using the sendmail restricted shell program (smrsh) when they install a vendor patch or upgrade to a new version of sendmail. You should always use the smrsh program.

  smrsh is included in the sendmail Version 8 distribution in the subdirectory smrsh. See the RELEASE_NOTES file for a description of how to integrate smrsh into your sendmail configuration file.

  smrsh is also distributed with some operating systems.

If you are using the m4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file, where /usr/local/bin is replaced by the name of the directory where you have installed smrsh on your system:

FEATURE(smrsh, /usr/local/bin/smrsh)

- Use mail.local

  If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included with the standard distribution. It is also included with some other operating systems distributions, such as FreeBSD.
  Although the current version of mail.local is not a perfect solution, it is important to use it because it addresses vulnerabilities that are being exploited. For more details, see CERT advisory CA-95.02:

  http://www.cert.org/advisories/CA-95.02.binmail.vulnerabilities.

  To use mail.local, replace all references to /bin/mail with /usr/lib/mail.local. If you are using the M4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file:

  define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)

- WARNING: Check for setuid executable copies of old versions of mail programs

  If you leave setuid executable copies of older versions of sendmail installed in /usr/lib (on some systems it may be installed elsewhere), the vulnerabilities in those versions could be exploited if an intruder gains access to your system. This applies to sendmail.mx as well as other sendmail programs. Either delete these versions or change the protections on them to be non-executable.

  Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

Summary of MIME Conversion Buffer Overflow in Sendmail

As shown by the above advisory there is a vulnerability in Sendmail that allows for a buffer overflow attack in Versions 8.8.3 and 8.8.4.

When these versions of Sendmail translate data from 7 bit ASCII to 8 bit MIME they are susceptible to a buffer overflow. As with all buffer over flows they occur when input data goes beyond the expected range and the program does not handle this gracefully. Once the range is exceeded and spills over onto the stack it is possible to execute arbitrary code or commands.

The arbitrary commands are executed as the UserID of the original program which is often root for Sendmail. Obviously once you have root access to execute arbitrary commands the box is yours to do as you please.

As a result a Sendmail box can be exploited by sending a carefully crafted packet which takes advantage of the buffer overflow to execute arbitrary commands as root.

The Attack

Once again since Mr. Kellogg has not specified what mail server and version he is using I have taken the liberty of assuming that is is Sendmail 8.8.4. Also as I have stated previously it is assumed that the PIX is running IOS 5.1(1). Therefore I have chosen to attack his mail server through his firewall as there are existing vulnerabilities that would allow this.

In order to receive mail from external organizations Mr. Kellogg would be required to allow connections to his mail server on port 25. Based on the fact that he is running a version of PIX software that suffers from the Mailguard vulnerability traffic to his mail server is not being limited as expected.

It is possible that since the mail server is believed to be protected by the PIX that the IT staff at GIAC have not been diligent in keeping the Sendmail server patched and up to date. After all they feel that the PIX is limiting traffic to the mail server to a very limited set of SMTP commands. The PIX may have given them a false sense of security and since all IT staff are extremely busy and prioritize their work based on need and risk they may have not gotten to those updates for the mail server yet since it is low risk (already protected by the PIX) and therefore low on their ever increasing to do list.

Now that I can access the mail server through the firewall and the commands are not being filtered by Mailguard and they are running an older unsecured version of Sendmail I can attack the mail server through the firewall.

By carefully crafting a mail packet I can take advantage of both vulnerabilities to overflow the buffer of the Sendmail server and execute arbitrary commands and / or code. Once I have the ability to execute commands or code on the Sendmail server as root I own the box and the choices are unlimited.

If Mr. Kellogg's mail server was patched and kept up to date this type of attack would not be possible because the buffer over flow would be removed. In addition if the PIX firewall was running a newer version of the PIX IOS with the Mailguard vulnerability corrected it would not be possible to send arbitrary commands to the mail server which would also foil the attack.

I took the liberty of choosing his software versions since they were not listed and believe that the events as described are possible. However if an organization

understands that firewalls are not magic silver bullets that protect all, it is unlikely that they would be running an unpatched version of Sendmail. It is also unlikely that an organization that takes security seriously would be running a firewall with a published vulnerability. So it is also quite likely if Mr. Kellogg's network really existed that the attack as described would have failed.

References

IPSEC User Guide for the Cisco Secure PIX Firewall Version 5.2. Cisco Systems Inc., 2000

Configuration Guide for the Cisco Secure PIX Firewall Version 5.2. Cisco Systems Inc., 2000

SANS Couseware Track 2 – Firewalls, Perimeter Protection & VPN's. SANS Institute, 2001

Paquet, Catherine and Teare, Diane. Building Scalable Cisco Networks. Cisco Systmes Inc, 2000

Giles, Roosevelt. All-In-One CCIE Study Guide., McGraw-Hill, 2000

Lusignan, Russell, Steudler, Oliver, Allison, Jacques. Managing Cisco Network Management., Syngress, 2000

Rudenko, Innokenty and Computing, Tsunami. Cisco Routers for IP Networking., The Coriolis Group, 2000

Paquet, Catherine. Building Cisco Remote Access Networks., Cisco Systems Inc., 2000

"Improving Security on Cisco Routers". URL: http://www.cisco.com/warp/public/707/21.html

"Cisco IOS Command Reference 12.2". URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122mindx/crfindx.htm

"Cert Coordination Center", URL: http://www.cert.org

"Cisco Systems", URL: http://www.cisco.com

"American registry for Internet Numbers ", URL:http://www.arin.net

"SANS Institute", URL: http://www.sans.org

"Packet Storm", URL : http://packetstormsecurity.org/

"Top Ten Smurf Amplification Sites", URL:
www.powertech.no/smurf/