Global Information Assurance Certification Paper

SANS San Diego Network Security 2001

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.6a (revised October 26, 2001)
Resubmission/Retake II

GIAC Certification
Alex Icasiano
Resubmitted March 8th, 2002

TABLE OF CONTENTS

INTRODUCTION

As a customer security coordinator, my normal day job in customer support is to provide vulnerability assessment on computer systems the company sells and incident handling/forensics on customer compromised systems. I do not normally receive the opportunity to work on perimeter security at work, so this was exciting paper to write.

Regrettably, the company Corporate I/S department does not allow customer support people to "play" with the company firewalls/routers or in the "DMZ." So the following network design was developed and tested on my home DSL environment.

The challenge was to architect a decent secure network environment with whatever equipment I could beg and borrow from friends or colleagues. Unfortunately, the spare equipment they had available for loan was not current generation or at the latest software revisions, as can be seen in the equipment inventory in the below table. Just what was available and lying around collecting dust at the moment.

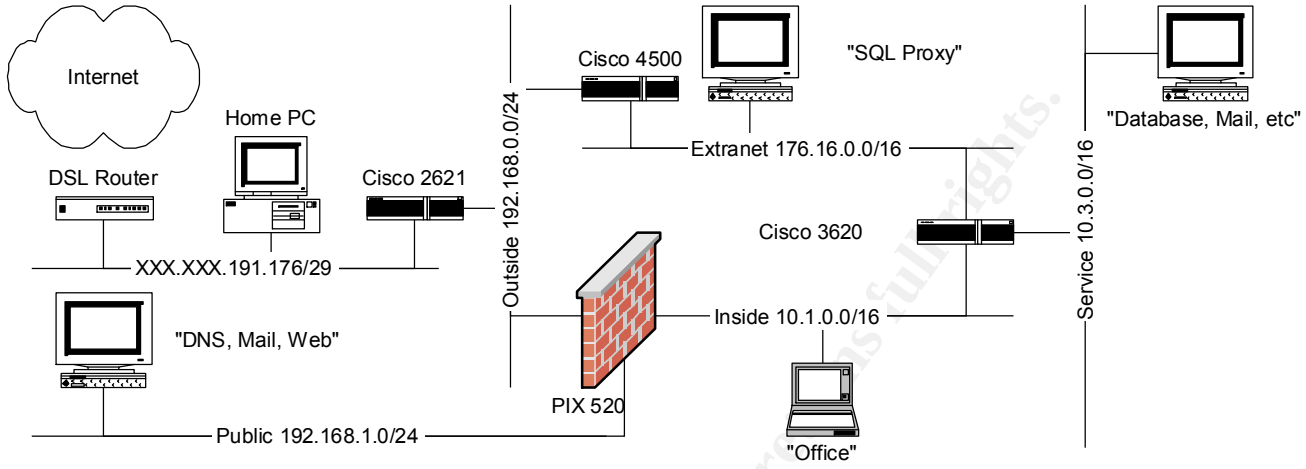
Among the equipment that was available, I chose all Cisco devices as I do not have an opportunity to play with them at my work and was hoping their simplicity (does not use a general purpose operating system like Windows or Linux) would lend themselves to making it easier to secure and configure them. Boy, was I wrong. There is a large learning curve in order to program Cisco devices. To learn Cisco IOS and PIX OS, I read online manuals, analyzed sample configuration files found on Cisco website and relied on Cisco ConfigMaker to setup the initial configuration on the routers.

Equipment Inventory

- Cisco 2621 Router with 2 Fast Ethernet ports running Cisco IPS 12.1.3(T)
- Cisco 3620 Router with 3 Ethernet ports running Cisco IOS 12.0(4)T
- Cisco 4500 Router with 2 Ethernet ports running Cisco IOS 11.(3)1
- PIX 520 Firewall with 3 Ethernet cards running PIX OS 5.1
- Cabletron SmartSwitch 2200 with 24 ports
- Laptop with 1 Ethernet port and Cisco Console Port Cable running Windows ME
- PC with 1 Ethernet port running RedHat 7.2 Linux
- My Home PC running Windows ME

Because I only had one switch available, this is not a real world network, but an experimental environment and lab to test out concepts for a final network design. In a real security perimeter, do not rely on a single switch or VLANs as a protection mechanism, as they can be bypassed. The single Linux system was used to simulate services like single system DNS, mail and web servers. The laptop was used both as a Cisco console and TFTP server, and a client on the network.

The proposed network architecture was designed to take full advantage of the limited equipment that was available at the time. The home test network below tried to simulate the proposed GIAC Enterprise network architecture.



For testing purposes, all the networks were connected to the same switch. The servers listed on the Public, Extranet and Services network were actually just the one PC running Linux which was moved around during testing. The laptop used as a console server and client on the inside networks. My home PC was the intruder lurking on the outside.

The IP addresses 66.33.61.127 and network 64.29.19.0/24 were chosen, because they some of the true addresses for the real www.giac.com.

The Lab

ASSIGNMENTS

Assignment 1 - Security Architecture (15 points)

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.

GIAC Enterprises is a startup with about 150 employees. Their current corporate network is on a Class C subnet 64.29.19.0/24 and their systems are on the open Internet. They currently rely on host based security to protect their systems. The company is open to IP address renumbering and network restructuring using Network Address Translation (NAT RFC1918).

In order to define a new security architecture for GIAC Enterprises, some assumptions need to be stated to limit the scope of the final network design.

Assumptions

- Limited Equipment Available
- Business Systems
- Business Connectivity
- Security Policy

Limited Equipment Available

GIAC wants to use any available unused network hardware in their current inventory for their network security perimeter and currently cannot afford to purchase additional equipment.

Network Devices Inventory

- Cisco 2621 Router with 2 Ethernet ports
- Cisco 3620 Router with 3 Ethernet ports
- Cisco 4500 Router with 2 Ethernet ports
- PIX 520 Firewall with 3 Ethernet cards
- Lots of network switches and patch cables

GIAC has various systems as servers, as well as Windows PC desktops/laptops for office employee use. They have a few extra systems that can be reconfigured to be servers.

The security perimeter is designed for possible future expansion of more services like authentication servers or adding more interfaces to the firewall when funding is made available.

Business Systems

- Internet Systems
- Office Systems
- Remote Systems
- Public Servers
- Internal Servers
- Shared Servers

The focus of this architecture is on network based security to enforce a company security policy that defines a new network security perimeter designed to protect corporate systems from attacks/intrusion. This paper does not cover host based system security. The SANS Step-by-Step Consensus Guides[1] are a good place to start on how to do this. There is also the SANS Securing Windows and Unix courses. It is assumed all systems are patched to current revisions to close known security issues. Also assume that not-known-to-the-general-public-yet security issues can be used to compromise any of the systems in GIAC Enterprise network, so services are hardened/restricted to only what is needed to minimize exposure and access is restricted between networks to compartmentalize the possible intrusion.

The systems and servers listed below are typical machines found in most corporate office environments. No special attention is placed on them, as the focus of this paper is using network based security devices to protect operating systems and restrict access between networks.

Internet Systems

These are systems on the Internet, which my include employees not doing a VPN back to the office, the IDS systems, customers or even intruders.

Traffic Flow

Internet Systems to Office Systems
Not allowed. Only Remote Systems running VPN can contact Office Systems.

Internet Systems to Remote Systems
Not allowed. No split tunneling is allowed on VPN clients.

Internet Systems to Public Servers
Stateful Inspection: Restricted access to DNS, Mail and Web Servers.

Internet Systems to Internal Servers
Not allowed. Blocked by the firewall, only Remote Systems with VPN have access.

[1] http://www.sansstore.org/Templates/frmTemplateK.asp?SubFolderID=22&SearchYN=N

Internet Systems to Shared Servers
Not allowed. Blocked by firewall and VPN router, only Partners using IPSEC VPN.

Office Systems

Employees have Windows based PC desktops with standard Microsoft collaboration applications like Microsoft Office and have access to standard Microsoft Servers like Active Directory and Exchange servers to support their habits.

Office systems are relatively open for collaboration work among groups, but all systems at least have both anti-virus software installed and Microsoft Server Management Software (SMS)[2] deployed or a similar technology to push software updates to systems.

It is assumed that no amount of patching and virus updating will protect the Windows based PC desktops from a compromise, so nightly backups of the systems are done by a centralized server to protect the corporate data.

Traffic Flow

Office Systems to Internet
Stateful Inspection, no restriction of services.

Office Systems to Remote Systems
Stateful Inspection, no restriction of services.

Office Systems to Public Servers
Stateful Inspection, no restriction of services.

Office Systems to Internal Servers
Filtered to Mail, DNS, Web, Database, Active Directory and Backup Servers.

Office Systems to Shared Servers
Disallowed by the 3620 router. Only Partners have access to Shared Servers.

Remote Systems

Remote employees have Windows based laptops or home office desktops with standard Microsoft Office applications, Microsoft SMS push technology and anti-virus software.

In addition to the above software, laptops and other remote access home office systems also have personal firewalls[3] to protect them in the event they are not currently plugged in to the corporate network.

[2] http://www.microsoft.com/smsmgmt/default.asp
[3] http://www.cert.org/tech_tips/home_networks.html

It is assumed that the personal firewall or antivirus will fail to protect a remote system from a compromise, so remote employees are encouraged to back up their data to removeable media or the centralized backup server.

Traffic Flow

Remote Systems to Internet Systems
Disallowed. No split tunneling when VPN is active. Must proxy thru firewall.

Remote Systems to Office Systems
Stateful Inspection. No restriction of services.

Remote Systems to Public Servers
Stateful Inspection. No restriction of services.

Remote Systems to Internal Servers
Filtered to Mail, DNS, Web, Database, Active Directory and Backup Servers.

Remote Systems to Shared Servers
Disallowed by the 3620 router. Only Partners have access to Shared Servers.

Public Server

There are several servers the public has access to from the Internet. The primary servers are DNS, Mail, and Web servers. Assume all public servers are running some flavor of the Unix or Linux operating system that can be broken into given enough trained monkeys and time. To minimize the weakness of the server operating systems, the public servers have been patched, hardened and extraneous services removed[4], so only necessary services and minimal daemons are running on the servers. To lock the configuration down, a tool like tripwire[5] or equivalent is used to checksum the drives and detect any unauthorized changes on the systems.

These servers service domain, smtp, http and https requests to the public. All other services are filtered from Internet access. To hide internal IP addresses and support NAT, split-horizon DNS is implemented on the public DNS server. The public mail server is running an SMTP service. The web server is running an HTTP and HTTPS service. For remote administration access, SSH is installed on all the public servers.

Assume all services of the public server can be exploited given enough time. To minimize the potential weakness of the services, domain, smtp, http and https daemons can be further hardened by running them in a jail environment using the chroot command, so even if they compromised, the intruder is trapped in an isolated environment.

[4] http://www.cert.org/tech_tips/unix_security_checklist2.0.html
[5] http://www.tripwire.com/

The public log server is used to centralize log files from the public servers. No public or employee access is allowed to it. Its access is restricted to the internal log server.
Traffic Flow

Public Servers to Internet Systems
Stateful Inspection. Only responses to domain, smtp, http and https requests allowed.

Public Servers to Office Systems
Stateful Inspection. Only responses allowed back, no restrictions.

Public Servers to Remote Systems
Stateful Inspection. Only responses allowed back, no restrictions.

Public Servers to Internal Servers
Stateful Inspection. Only responses from Log Server requests.

Public Servers to Shared Servers
Not allowed by 3620 Router.

Internal Servers

There are several servers GIAC employees have access to. The key ones include DNS, Mail, Microsoft Servers, Internal Corporate Web Page, centralized backup and a data base server. The internal servers are configured not to directly access the Internet. They use relay servers to relay information from the Internet. In fact, they pull information from the relay servers, instead of the relay servers pushing the content to them.

The employees do not have access to the log server, which is used to record events and centralize log files from the public log server and internal servers. The internal log server pulls information from the public log server.

All internal servers run Microsoft Server operating system Windows 2000, except the log server which runs a Unix operating systems. It can also be assumed that all systems have been hardened and currently patched to close all known security issues. To lock the configuration down, a tool like tripwire or equivalent is used to checksum the drives and detect any unauthorized changes on the systems.

Traffic Flow

Internal Servers to Internet Systems
Not allowed by both 3620 Router and Firewall.

Internal Servers to Office Systems

Filtered responses from Mail, DNS, Web, Database, Active Directory and Backup Servers.

Internal Servers to Remote Systems
Filtered responses from Mail, DNS, Web, Database, Active Directory and Backup Servers.

Internal Servers to Public Servers
Only requests to pull down log files from Public Log Server and Admin Access via SSH.

Internal Servers to Shared Servers
Stateful Inspections. Only responses from database sent to the SQL proxy server.

Shared Servers

There is currently one server which is shared among GIAC employees, Suppliers and Partners which is the database server. In future expansion projects, there may be more shared servers.

Shared Servers to Internet Systems
Disallowed by 3620 and 4500 routers.

Shared Servers to Office Systems
Disallowed by 3620 router.

Shared Servers to Remote Systems
Disallowed by 3620 router.

Shared Servers to Internal Servers
Stateful Inspection. Restricted by 3620 CBAC ACL from SQL Proxy to Database.

Business Connectivity

- Employees
- Remote Employees
- Customers
- Suppliers/Partners

Each business function has connectivity requirements. Only those access requirements are allowed and all other connectivity is restricted by the security policy.

Employee Connectivity

As per the GIAC's network usage policy, employees can access Internet during the course of normal business. Some personal use is tolerated, but excessive personal use of corporate Internet access may be disciplined per the company security policy.

When funding is available, future expansion hardware may include proxy servers and content filters to monitor and control employee network usage.

Employees can also access all of the internal servers such as the mail, database and file servers except the internal log server.

Remote Employee Connectivity

In the new security architecture, remote employees will use Cisco Secure VPN client[6] to access the corporate network from the employee's local ISP. The client is free to Cisco customers under a support contract making it an attractive solution to GIAC Enterprises.

When remote employees are connected to the corporate network, split tunneling is disabled to prevent a relayed attack through the split tunnel.

In this phase of the security perimeter implementation, remote access authentication will be done thru pre-shared secrets. When more funding is made available, one time password authentication servers like SafeWord[7] or similar technology are planned.

Customer Connectivity

Customers purchase bulk fortunes from GIAC Enterprise's public commerce web server. The customers use a standard web browser using SSL encryption to secure their connection.

Business Suppliers/Partners

Both suppliers and partners have access to a shared fortune database. Suppliers populate the database and Partners download the database to translate and resell.

In the new security perimeter, Suppliers and Partners will access this shared database thru Business To Business (B2B) IPSEC VPN links. Cisco routers will be used on both endpoints of the VPN. Pre-shared secrets will be used to authenticate between the routers and ESP encryption protocol will be used to keep the links private.

Security Policy

- Compartmentalize
- Minimize Exposure
- Default Deny Stance

[6] http://www.cisco.com/warp/public/cc/pd/sqsw/vpncl/index.shtml
[7] http://www.safeword.com/

GIAC has a well defined and documented company security policy. The security policy is composed of standard widely accepted business practices[8]. The policy includes physical security, offsite backups, network usage policy, host and server security, remote access policy, what to do in the event of an intrusion[9] or a natural disaster, recovery[10] and business continuity procedures, and other such common sense standard practices. The policy will be augmented to define the new security perimeter architecture.

Compartmentalize

Divide up the network into separate business functions. Group together similar business functions on the same network. Assign each network a security policy based on their connectivity needs.

For this architecture, business functions will be defined by what type of business system is being used and connectivity needed. The network was partitioned in the following way:

- Public Servers - 192.168.0.0/24 mapped to 66.33.61.0/24 on Outside
- Shared Servers - 176.16.0.0/16
- Office Systems - 10.1.0.0/16
- Remote Office Systems - VPN clients mapped to 10.2.0.0/16
- Internal Servers - 10.3.0.0/16

The hope is that an intrusion in one compartmentalized network can be contained within that partitioned network. For example, an intruder in the public servers network will be trapped in that network environment.

Compartmentalization is popular on host based security, for example when Unix chroot is used to create a virtual cage for BIND DNS named. If named was exploited, the intruder is trapped in the virtual cage and theoretically cannot access the real underlying operating system. See the web document "How to break out of a chroot jail"[11] for more details.

The hope is to extend this concept to a network based security perimeter.

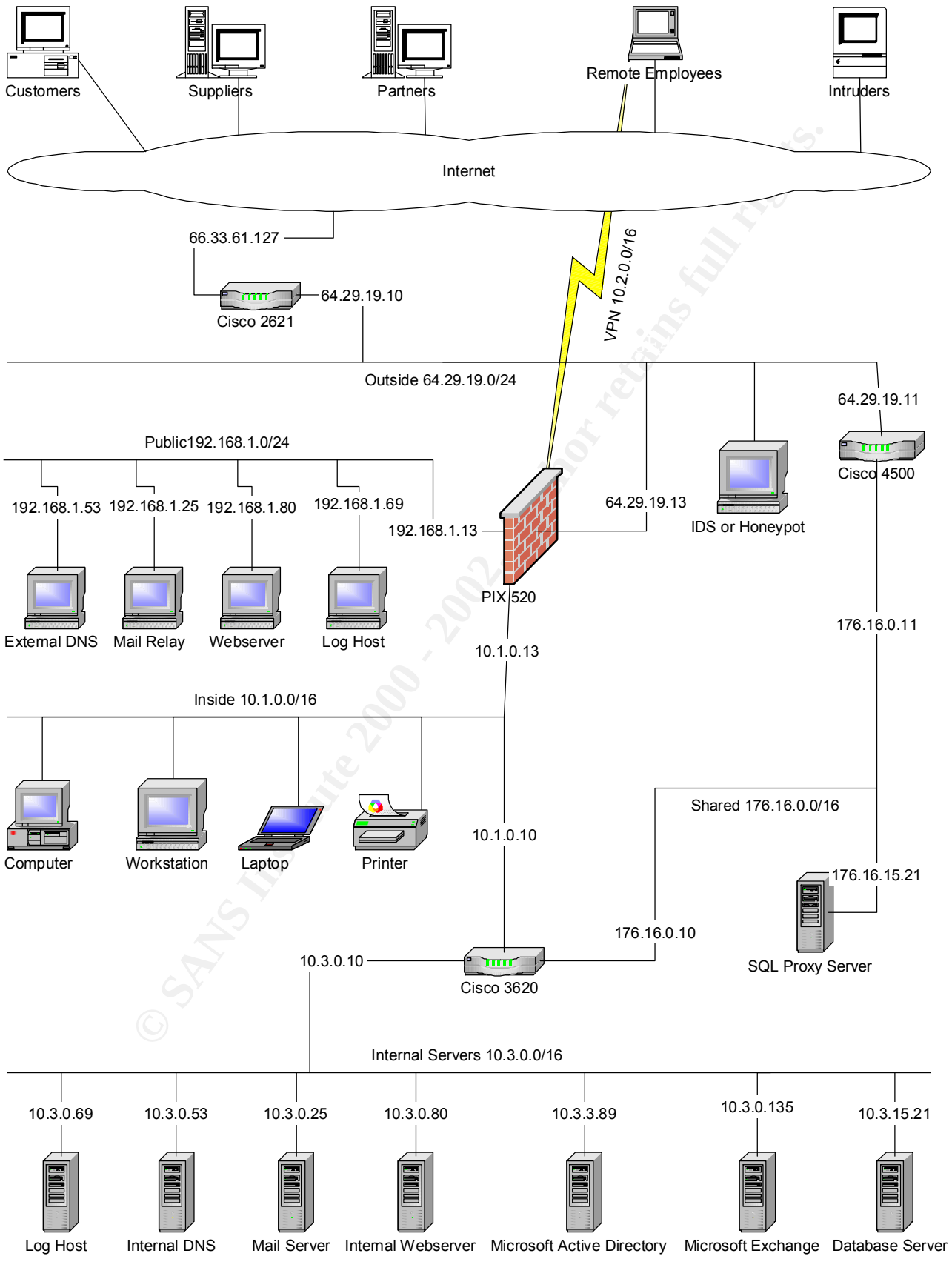
[8] http://www.cisecurity.org/
[9] http://www.cert.org/tech_tips/intruder_detection_checklist.html
[10] http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
[11] http://www.bpfh.net/simes/computing/chroot-break.html

Minimize Exposure

Limit access to only needed services and servers based on business function connectivity and service needs. Remove or filter extraneous services from servers. Minimize access to only what is necessary between business functions. Restrict all other access.

Default Deny Stance

A default deny stance will be applied to routers, firewalls and servers. Allow only what is express permitted, deny everything else.



Description of the network security devices:

- Cisco 2621 Router with 2 Fast Ethernet ports running Cisco IOS 12.1.3
- Cisco PIX 520 running PIX Firewall OS 5.1.2
- Cisco 4500 Router with 2 Ethernet ports running Cisco IOS 11.3.1
- Cisco 3620 Router with 3 Ethernet ports running Cisco IOS 12.0.4

Each security perimeter network device was placed in order to provide optimum access control between networks thereby enforcing GIAC Enterprises' company security policy.

Cisco 2621 Router with 2 Fast Ethernet ports running Cisco IOS 12.1.3

The Cisco 2621 router was chosen as the border route for performance reasons. Since it will be doing mostly static filtering, it seems to the best fit for the task. This makes the other routers available to be placed in more router CPU intensive areas of the network.

This router was placed to compartmentalize or separate the business from the Internet. Its placement is a choke point for which all traffic destined or sourced for the Internet must pass.

The 2621's main tasks are to offload ingress/egress filtering from the firewall and minimize exposure of the Outside network from the Internet. With ingress filtering, only "valid" IP addresses should be going into the business, and with egress, internally created spoofed IP addresses should not be leaving the business to the Internet.

Access Controls are programmed into the router to limit the exposure of systems in the Outside network.

Except for ingress/egress and minimize exposure filters, most other network traffic is allowed through, which breaks the default deny company security policy. This allows an IDS system placed in the Outside network to observe any unusual Internet traffic. Otherwise, the router would filter this traffic and it would be difficult to determine any network scans or sweeps.

Future upgrades to this router may include Cisco IDS feature set installed, or even Cisco Content Based Access Control (CBAC) feature installed or denial of service (DoS) protection, CPU performance permitting. For this initial phase and implementation of the security architecture, the goal was to start with a simple foundation and in the future build from it.

To lock the configuration down, a tool like tripwire or equivalent is used to checksum the router and detect any unauthorized changes on the IOS configuration file.

Cisco PIX 520 running PIX Firewall OS 5.1.2

The Cisco PIX 520 was an obvious choice for a firewall with it firewall rich feature set. It is placed to separate Internet and Outside networks to enforce company security policy. On the 3rd network interface, the PIX separates the public servers from the Outside Internet. Only specific services on the public servers are made available to Internet users, which protects the server by limiting their exposure.

The firewall also provides VPN access to remote employees who connect using Cisco Secure VPN client.

Cisco 4500 Router with 2 Ethernet ports running Cisco IOS 11.3.1

The Cisco 4500 router was chosen as the IPSEC VPN router, as the 3 Ethernet ports on the 3620 were needed elsewhere on the network and the R4600 MHz processor would help in VPN encryption performance.

The shared network is designed for services in the between Suppplier and Partners

In the network architecture, the 4500 was placed to isolate the shared network from the rest of business. Shared services are placed in this network, limiting exposure to the internal business systems. Pre-shared secrets will be used to authenticate between the routers and ESP encryption protocol will be used to keep the links private.

To further minimize exposure of business systems, a database SQL proxy server[12] can be placed on the shared network which can be used for user authentication and validation of SQL command relayed to the internal database server.

The router was upgraded to Cisco IOS 12.1(12) with IPSEC 56 feature set to support VPN. The older software did have the IPSEC feature set.

To lock the configuration down, a tool like tripwire or equivalent is used to checksum the router and detect any unauthorized changes made on the IOS configuration file.

Cisco 3620 Router with 3 Ethernet ports running Cisco IOS 12.0.4

The Cisco 3620 router was the only router with 3 network interfaces and was placed to partition the office systems, internal and shared server networks from each other as an internal "firewall" between inside networks.

[12] http://www.firstworks.com/sqlrelay.html

The router has an access control lists to limit access from the inside office network to the internal servers. Limited ports are open to inside network to minimize the exposure of the internal severs.

The 3620 also has a Cisco CBAC filter in place to limit access from the SQL proxy server on the shared network to the database server on the internal network. The CBAC filter validates the packets to make certain they contain valid SQL protocol in them. The inside office network cannot contact the shared network. On the internal server network, only the database sever can contact the SQL proxy server.

To lock the configuration down, a tool like tripwire or equivalent is used to checksum the router and detect any unauthorized changes made on the IOS configuration file.

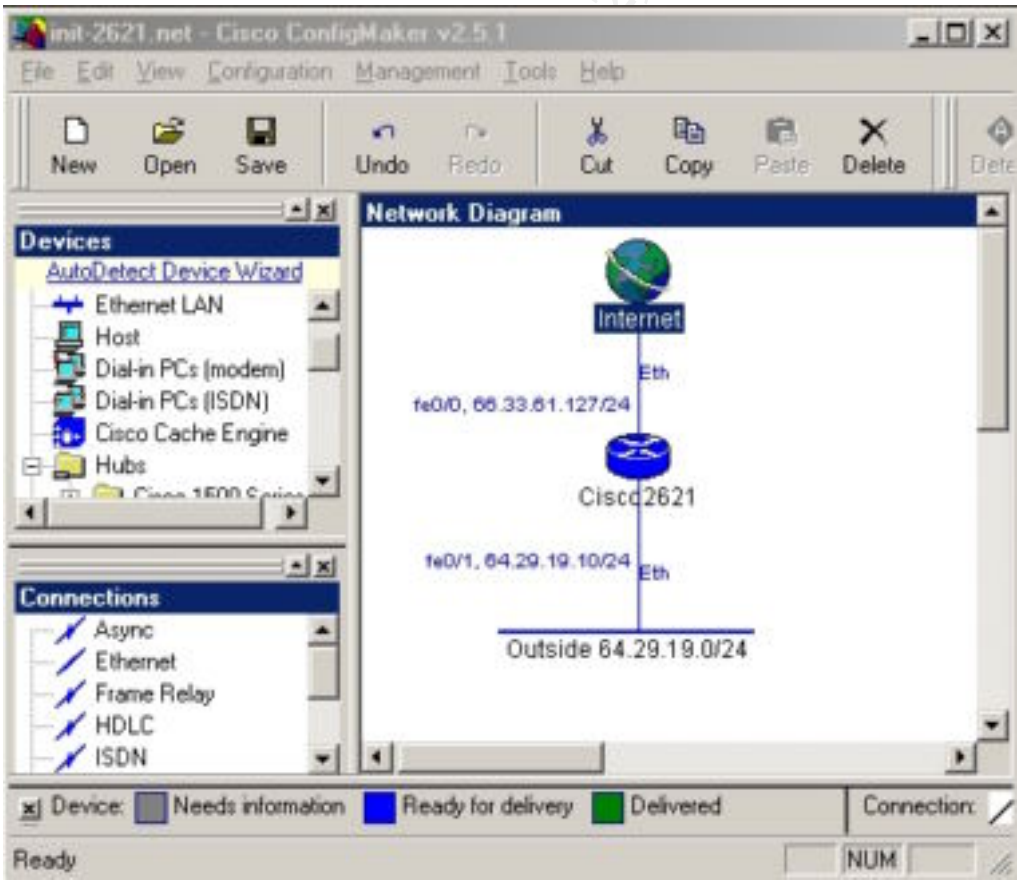
Assignment 2 – Security Policy (35 points)

Provide a security policy for the following components:

- Border Router
- Primary Firewall
- B2B VPN

Border Router

The initial configuration for the Cisco 2621 was done in Cisco ConfigMaker[13], a Windows application suggested by the instructor and demonstrated in class. It is very useful for those new to Cisco IOS, like me, in setting up router initial configurations and then expand the configuration file from that base using sample configuration files found on the Cisco website.



[13] http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml

The default ConfigMaker's configuration file for 2621 was expanded using information from Rob Thomas's Secure IOS Template Version 2.3[14]. Rob's template was developed with Cisco IOS commands for ISP class Cisco Routers, which this 2621 router did not support, but the template had some great ingress and egress filtering ACLs which are detailed in the expanded configuration file.

Information on how to configure Cisco router access control lists[15] were covered in the class lecture so it is not covered by a tutorial.

Future updates to this configuration file requires a better understanding of what Cisco IOS features can offer to make a better implementation of Rob Thomas Secure IOS template and make full use of the Cisco 2621 router's security capabilities.

It is much easier to use Cisco ConfigMaker to push its default 2621 router configuration via serial console to get basic network connectivity to the router, and then install the Cisco TFTP Server[16] Windows application and use notepad to edit the configuration file.

With TFTP, configuration files can be copied to and from the Cisco router using the following commands:

To copy the start up configuration file to a TFTP server
- copy startup-config tftp://<TFTP Server IP Address>/<filename>.txt

To copy from the TFTP server to the router's running configuration
- copy tftp://<TFTP Server IP Address>/<filename>.txt running-config

To save the routers running configuration as the startup configuration
- copy running-config startup-config

See Appendix A for the final 2621 Cisco IOS configuration file.

[14] http://www.enteract.com/~robt/Docs/Articles/secure-ios-template.html
[15] http://www.cisco.com/warp/public/732/abc/technologies/access_control.shtml
[16] http://www.cisco.com/cgi-bin/tablebuild.pl/tftp

Primary Firewall

Frist time configuration for the PIX 520 with Firewall OS 5.1.2 proved to be difficult, as unlike a router, the default deny policy make it a bit difficult to configure remotely. Almost all the initial configuration had to be done via serial console cable and a Windows PC using Cisco IOS terminal to input commands.

There was once a Windows application called Pix Firewall Manager (PFM)[17] available on the Cisco website, which was similar to Cisco ConfigMaker, a GUI to make it easier to setup the PIX Firewall's inistall configuration easily. Unfortunately, the PFM application can no longer be found on the Cisco website. PFM was replaced with Pix Device Manager (PDM)[18] for PIX OS 6.0 which is a Java based application which runs on any Java capable browser. Regrettably, this PIX 520 has only a 2MB ISA flash card and therefore cannot run any PIX OS higher than 5.1.(2). To run PIX OS 6.0, a Cisco 16MB ISA flash card would need to be purchased as an upgrade, which has an MSRP of $1,000

PIX Firewall OS is similar to Cisco IOS and IOS configuration was covered in class by the instructor, but the PIX command set is both similar and different in many ways to the Cisco router command set. After reading the PIX Firewall 5.1 Configuration Guide[19] and studying several configuration examples[20] , the Cisco web document "Using nat, global, static, conduit and access-list Commands and Port Redirection on PIX"[21] made it easier to understand how to program the device.

Security Policy Tutorial on PIX Access Control Lists

Since PIX OS was not covered in class, here is a quick tutorial on how to implement a security policy on a PIX Firewall by comparing differences between IOS which was covered in class. There are three main differences between Cisco IOS access control lists and the PIX and three sample access control lists (ACLs) policies will be used to show the differences.

1) Just like Cisco IOS, PIX OS allows the uses of access-lists, but difference is in the way the network mask is specified.

Cisco IOS snippet taken from above Cisco 2621 router configuration

```
! Allow IP access to the intranet (firewall filters specific ports)
access-list 2010 permit ip any 64.29.19.0 0.255.255.255
```

PIX OS snippet taken from below PIX 520 configuration

[17] http://www.cisco.com/warp/public/110/41.shtml
[18] http://www.cisco.com/warp/public/110/41.shtml - Q8a
[19] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/index.htm
[20] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/examples.htm
[21] http://www.cisco.com/warp/public/707/28.html

```
! Allow Office and Severs Networks to contact Remote Employees
access-list 111 permit ip 10.1.0.0 255.255.0.0 10.3.0.0 255.255.0.0
```

Notice the netmask is specified differently. The PIX OS network mask is the traditional method to specify a netmask, but the Cisco IOS specifies the inverse netmask.

On the PIX, it is very easy to test this ACL, without it in place no remote employee cannot contact system on the inside internal network. This ACL does allow any remote employee via VPN to contact any inside system, so if a remote employee's system is compromised, this ACL allows the intruder to connect to office systems. The hope is that either we can prevent an intrusion from occurring on the remote systems by using personnel firewalls, antivirus, and not allowing split tunnels when connected via VPN, or we can contain the intrusion to the office network by limiting access to other inside networks.

2) Unlike routers, by default network traffic is not allowed across PIX interfaces until specifically permitted. The PIX requires each network interface has a security level specified. Also, the PIX ACL's to allow traffic to flow from a higher security level interface to the lower security level interface is different than allowing traffic from lower security level interface back to the higher security level interface. Examples are given below.

Assign a security level and label each network interface:

```
! Label the network interfaces and assign a security level
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 public security50
```

To allow the internal network (inside - higher level security) to contact internet (outside – lower security level) network:

```
! Create a Dynamic pool of IP addresses so public and inside networks
! can get to the outside (internet) network
global (outside) 1 64.29.19.100-64.29.19.250

! If we run out of Dynamic IP addresses, switch to PAT
global (outside) 1 64.29.19.251

! Allow inside and servers nets to access outside network (internet)
nat (inside) 1 10.1.0.0 255.255.0.0
```

To test these access control lists, a system on the inside network should be able to access a system on the Internet. Without these ACLs, no office system could access the Internet. The problem with these ACLs, is a compromised office system has unrestricted access to the Internet, which is detailed in the audit section of this practical. It is hope this PIX firewall, antivirus software installed on the office systems, and pushing software updates to office systems using SMS can prevent an intrusion from occurring.

3) To allow the internet (lower security level) to contact the public network (higher level) the following commands are used:

```
! Put Webserver on the Internet, but allow access to port 80 & 443 only
```

```
static (public,outside) 64.29.19.80 192.168.1.80
access-list ouside_acl permit tcp any host 64.29.19.80 eq 80

! Apply the outside_acl rules to the outside interface
access-group outside_acl in interface outside
```

It is very easy to test these access control lists, as without in place no one from the Internet could access the web server on the screened public network on port 80. To make sure only port 80 was being allowed, a port scan can be done which is detailed in the audit section of this practical. The danger with any public web server is that there is always the possibility of a compromise. The hope is to minimize this danger by limiting access to only port 80 of the web server, creating a chroot jail for the http daemon, keeping the software updated and containing the intruders to the public network when the http daemon does get compromised.. Another possibility is to use an http proxy to validate and relay the http traffic to a real web server, like was implemented on the shared database.

The Three Interface with NAT Configuration Example[22] from PIX 5.1 manual was used as a template and modified for the GIAC network perimeter. Then this template was augmented and expanded to include VPN client example configuration[23] to allow remote access for GIAC employees.

Once a basic setup was installed for the Inside network interface, the following commands could be used the copy to and from a TFTP server on the Inside network interface:

To copy from the TFTP Server
- configure net <TFTP IP Address>:<Filename>

To copy to the TFTP Server
- write net <TFTP IP Address>:<Filename>

This made easier to configure the rest of the PIX firewall configuration within Windows Notepad on the TFTP server.

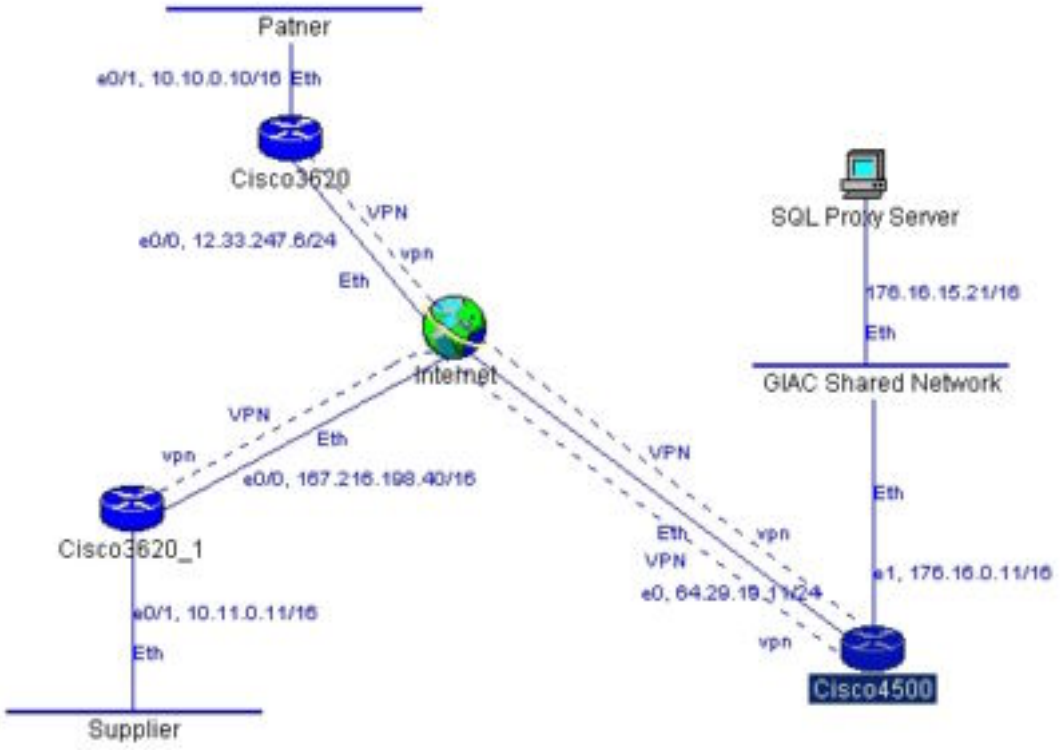
See Appendix B for the final PIX 520 Firewall Confiuration.

[22] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/examples.htm-xtocid248585
[23] http://www.cisco.com/warp/public/707/29.html

B2B VPN

The IPSEC VPN for GIAC Partners and Suppliers was implemented using a Cisco 4500 Router. Both business partners and suppliers will be using the same IPSEC policy on the router, and have Cisco 3620 routers for their VPN link.

Cisco ConfigMaker, once again proved to be invaluable in setting up the basic router configurations which were then expanded to cover the GIAC security policy.



Instead of public key certificates, pre-shared secrets will be used to authenticate between the routers. When GIAC Enterprises has more funding available, a future project in place is to purchase a certificate authority (CA) server and use RSA certificates. This same CA server can also be used to authenticate remote access employees using Cisco Secure VPN client.

IPSEC ESP encryption protocol will be used to keep the links private. The IPSEC policy will enforce DES encryption, MD5 checksums and 768bit Diffi-Hellmen (DH) session key exchange between routers.

The Cisco 4500 router will also limit access of the suppliers and partners to only the SQL proxy server. The hope is that an intrusion at a partner or supplier network would limit exposure of GIAC Enterprise to only the proxy server to the intruders.

See Appendix C for final 4500 Cisco IOS configuration file.

Assignment 3 – Audit Your Security Architecture (25 points)

You have been asked to conduct a technical audit of the primary firewall for GIAC Enterprises.

Audit

- Plan
- Security Policy
- Reconnaissance
- Drill Down
- Document
- Repeat

Plan

The first step to any audit requires in-depth planning and coordination. This requires documenting the audit plan and meeting with system and network administrators to go over the details of the audit.

First determine what the requirements are for the audit. Certain audits are done to fulfill a certification, others are done to benchmark the current security level of a company, and some are done to verify the policy is being adhered to. This audit is focused on adherence to the firewall security policy.

Second, determine who should perform the audit. It is usually best to hire a security consulting firm with good references to perform the audit, but it also the most expensive route. One quote for a full security scan of 1 IP address can cost $5-8K from one of the top-rated security firms. GIAC's firewall has 3 IP addresses and networks to contend with. Since GIAC does not have adequate funding, the audit would be performed in-house using GIAC employees to perform the audit. Ideally, it would one person for network/IP address to be audited. This way the audit can be performed simultaneously and the auditors can relay information to each other during the audit. Otherwise for a single auditor, a network sniffer would be needed on the "other side" to verify packets did or did not go thru the firewall. It is wise not to depend on the firewall logs to see if a packet was blocked or dropped, as they can be incorrect.

Third, decide on a time when to perform the audit. The actual audit may disrupt daily business. To minimize disruption of the business, it may be best to conduct the audit after business hours or weekends. There is a possibility that innocent probing and prodding of a server or service can halt the service or crash a system. Discuss a recovery procedure if necessary and make sure backups are done of key systems before the audit. This audit will be performed after business hours, but not before a weekend or holiday. This assures there will be extra help the next day to take over if something goes wrong. Monday night

seems like a good day. When can you start? Expect to take it all night and probably the following evenings depending on what is found. A full complete protocol port scan of a single IP address can take 30 minutes, and a scan of a network takes longer. For GIAC's firewall, estimate at least 150 hours worth of work for one person.

Security Policy

The goal of this audit is to validate conformance to the company's network security policy. Before an audit is performed, the security policy itself should be audited to make sure it is in line with industry standard security practices and common sense. The security policy should be visited yearly, updated after any security incidents and any network, service, or policy changes.

At minimum, the security policy should dictate preparation for disaster such as backups or off-line servers; what needs to be done and who will do it during an incident be it natural disaster, physical theft, or network intrusion; and business recovery procedures from the incident like turn on the gas electric generators or collect from the company insurance policy and try again.

Reconnaissance

To start this technical audit, a network scan or an inventory needs to be performed on all networks the firewall is attached to see what services are being offered by each server or network device like routers. This information should be compiled and compared with the firewall security policy to make certain they match what the firewall thinks it is protecting.

Then the firewall itself should be port scanned from each network interface to validate access control policy to the firewall itself. Any workstations, servers or routers that the firewall trusts needs to be included in the audit. If the firewall trusts it, why considering breaking into the firewall at all? Maybe the firewall remote console workstation at the administrator's home has weaker security and can be used to relay an attack onto the firewall itself.

Lastly, the scans need to be done thru the firewall interfaces in all directions to verify the access controls between networks are in place and working correctly. Make certain that these scans are detected by the firewall, IDS and log host systems.

Drill Down

After networks, servers, ports and services have been scanned and compiled into large list, each service needs to be drilled down into and inspected. Make sure that the service needs to be enabled, verify it has been hardened and patched for security issues. Possibly this means running the service in a Unix chrooted environment or without administrator or root privileges. Favorites are to chroot DNS named service and run sendmail without root privileges.

A banner grab of the service can help determine what exploits and vulnerabilities are available in the public. Consider changing the service banner to list a false version or disabling banners altogether. Have the web server report and simulate it is Microsoft IIS even though in reality it is Apache.

To automate the process of inspecting the actually application/daemon behind the service or open port, use a security scanner to determine if there are vulnerabilities or exploits available. There are many commercial ones, but since GIAC Enterprises is on a budget, Nessus[24] is a good free vulnerability scanner.

Document

The data for the audit needs to be collected, sorted and evaluated for an overall assessment for adherence to the firewall security policy.

Repeat

The audit should be repeated after some time and performed routinely as matter of course and preventative maintenance to maintain the health of the security perimeter.

GIAC Firewall Audit

The Cisco Secure PIX Firewall is an unusual beast, as it is a combination of a standard firewall and Cisco router, so it was rather difficult to audit its security policy for adherence. The PIX uses pseudo IP addresses to advertise services and wait for responses for requests made behind the firewall. This means a scan of a PIX pseudo IP address is not really scan of the server protected by the firewall. It is akin to a proxy server, where there is really no "direct" IP access to the servers and systems behind the firewall.

For example, using nmap[25] utility to do a default port scan the web server on public network 192.168.1.0/24 with –v verbose flag reveals the following open ports:

```
bash-2.04# nmap -v 192.168.1.80

Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect()
scan. Use -sP if you really don't want to portscan (and just want to
see what hosts are up).
Machine 192.168.1.80 MIGHT actually be listening on probe port 80
Host (192.168.1.80) appears to be up ... good.
Initiating Connect() Scan against (192.168.1.8063.198)
Adding open port 5000/tcp
Adding open port 139/tcp
```

[24] http://www.nessus.org/
[25] http://www.insecure.org/nmap/index.html

```
Adding open port 113/tcp
Adding open port 80/tcp
The Connect() Scan took 12 seconds to scan 1548 ports.
Interesting ports on (192.168.1.80):
(The 1544 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
113/tcp    open        auth
139/tcp    open        netbios-ssn
5000/tcp   open        fics
```

The open ports and services are inline for a laptop running Windows ME with Apache Win32 running on port 80 which simulates GIAC's public web server. In a real production environment, those extra ports would be disabled or filtered on the host as defense in depth, just in case the firewall fails in its duty to limit access to port 80.

When another nmap port scan is done, this time with –O option to guess the operating system, on the PIX's outside interface which advertises the pseudo IP address 64.29.19.80 for the public webserver, the following output was generated.

```
bash-2.04# nmap -v -O 64.29.19.80

Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect()
scan. Use -sP if you really don't want to portscan (and just want to
see what hosts are up).
Host  (64.29.19.80) appears to be up ... good.
Initiating Connect() Scan against  (64.29.19.80)
Adding open port 80/tcp
The Connect() Scan took 829 seconds to scan 1548 ports.
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
For OSScan assuming that port 80 is open and port 43995 is closed and
neither are firewalled
Interesting ports on  (64.29.19.80):
(The 1547 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http

Remote OS guesses: AIX 4.02.0001.0000, AIX v4.2, AIX 4.2, AIX 4.2.X,
AIX 4.3.2.0-4.3.3.0 on an IBM RS/*, AIX 4.3, IBM AIX v3.2.5 - 4, Cayman
2E <http://www.cayman.com/>
OS Fingerprint:
TSeq(Class=TR%IPID=I%TS=0)
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
```

```
TCP ISN Seq. Numbers: BAF25A0A F2BB0611 1FF90F14 1AC05B42 BE5027D2
FAFDD8F1
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 834 seconds
```

This matches the PIX rule:

```
! PIX 520 ACL
static (public,outside) 64.29.19.80 192.168.1.80
access-list ouside_acl permit tcp any host 64.29.19.80 eq 80
```

Two things of note in the above nmap output are:

1) The ACL rule correctly minimized exposure of the web server and limited access to only port 80.

2) nmap could not correctly determine that the web server behind the firewall was a Windows system. Like a proxy server, the PIX is not directly routing the packets between network interfaces, but rather receiving and delivering packets on behalf of the web server.

Unfortunately, a nmap port scan of the PIX firewall on the outside Internet interface reveals too much information:

```
bash-2.04# nmap -v -O 64.29.19.13

Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect()
scan. Use -sP if you really don't want to portscan (and just want to
see what hosts are up).
Host  (64.29.19.13) appears to be up ... good.
Initiating Connect() Scan against  (64.29.19.13)
The Connect() Scan took 14 seconds to scan 1548 ports.
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (64.29.19.13):
(The 1546 ports scanned but not shown below are in state: closed)
Port       State      Service
23/tcp     filtered    telnet
1467/tcp   filtered    csdmbase

Remote operating system guess: Cisco Secure PIX Firewall Version 5.0(2)
OS Fingerprint:
T5(Resp=Y%DF=N%W=400%ACK=S++%Flags=AR%Ops=WNMETL)
T6(Resp=Y%DF=N%W=400%ACK=S%Flags=AR%Ops=WNMETL)
T7(Resp=Y%DF=N%W=400%ACK=S++%Flags=UAPR%Ops=WNMETL)
PU(Resp=N)


Nmap run completed -- 1 IP address (1 host up) scanned in 18 seconds
```

This report suggests that we need to tighten up the access control list on the telnet port of the firewall and investigate what service port 1467 is used for. As a precaution, ACLs on the Cisco 2621 border router needs to be added to filter these ports from the Internet. These Cisco 2621 IOS ACLs should accomplish this task and is placed before the permit ip any 64.29.19.0 ACL:

```
! Filter tcp port 23 and 1467 until we find out why they are open
access-list 2010 deny tcp any host 64.29.19.13 eq 23 log-input
access-list 2010 deny tcp any host 64.29.19.13 eq 1467 log-input

! Allow IP access to the intranet (firewall filters specific ports)
access-list 2010 permit ip any 64.29.19.0 0.255.255.255
```

Note that the order of this ACL is important and must be placed before the permit ip any rule for these ACLs to filter these PIX firewall ports. Otherwise, if placed after permit ip any rule, the filtering rule would never trigger and these firewall ports would still be open to the outside.

Evaluation of Audit

I did not have all the equipment needed to simulate all the services, systems and servers that composed the simulated GIAC Enterprises, but never the less several weak points were discovered with the over all network architecture and the firewall itself.

When investigating the open port 1467 on the PIX firewall by searching the Cisco web site, I came across a mailguard vulnerability.[26] Mailguard is designed to limit the SMTP command set used during mail transfers to limit exposure of the internal mail server.

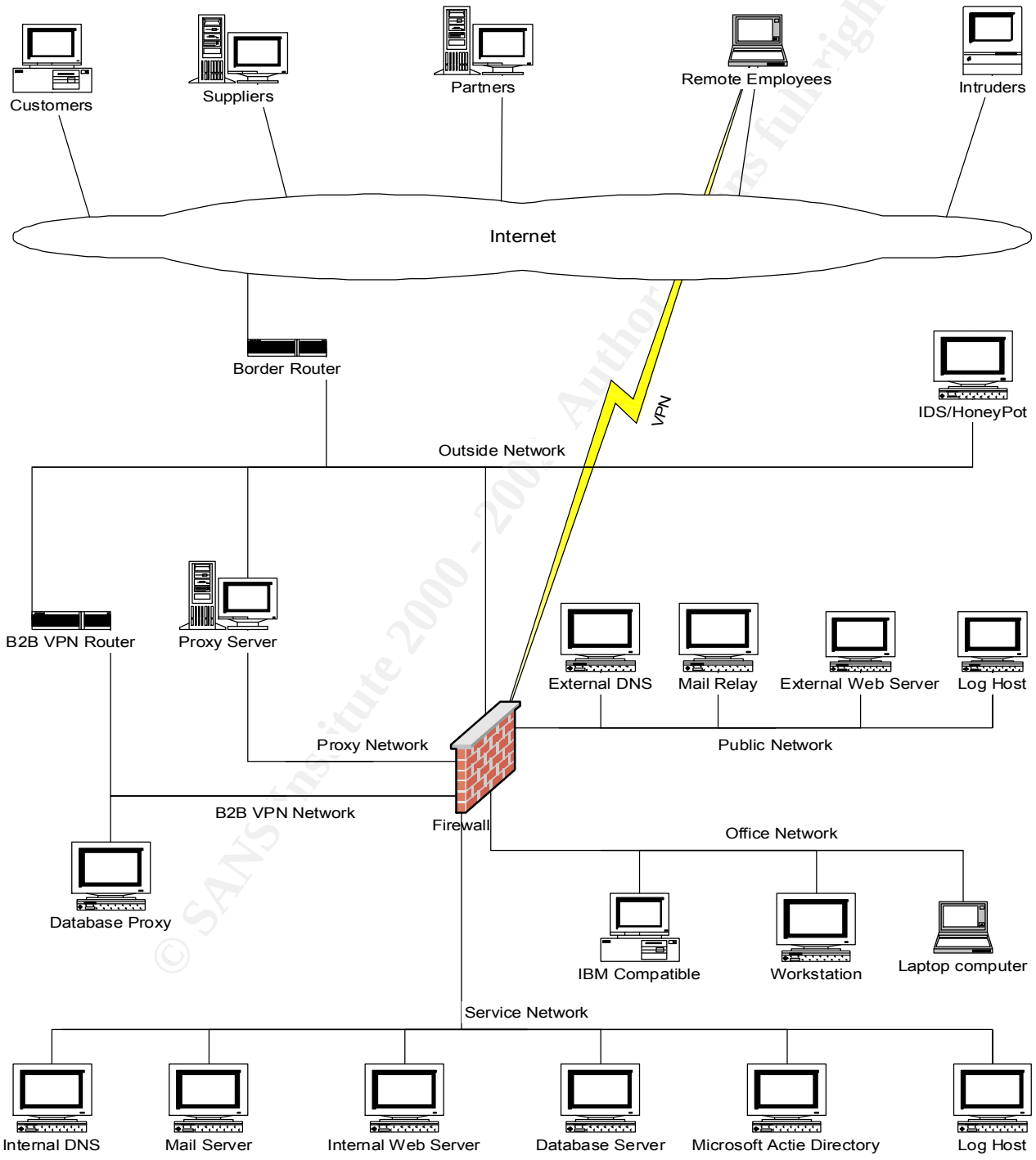
Unfortunately, the fix is to upgrade the PIX to 5.2, which this firewall cannot support unless the flash card is upgraded. In fact, digging deeper, PIX 5.1 OS has been end of life[27] per Cisco. No wonder this firewall was available to be loaned out. ☺

Given that I could not find exact information on what port 1467 on the PIX does, I was toying with the idea of using the Cisco 2621 border to filter all ports on the PIX firewall except ESP port 500 so remote employees can still establish VPN links. I was hesitant this may break the client VPN connectivity, so I opted for a filtering ACL rule, but something to try in the future. The nice thing about the PIX, filtering the single IP address of the firewall does not limit access to inside and the public networks, since the PIX is using different pseudo IP addresses to give them access.

While testing traffic thru the various firewall interfaces, there seems to be too much trust placed on the inside office network. There does not seem much to limit the outbound Internet activities of employees. Suggestions to remedy this situation would be to place a proxy server between the inside network that only the firewall trusts, purchasing more

[26] http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml
[27] http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/1303_pp.htm

interfaces for the firewall and placing the employees on a lower PIX security level. The ultimately trusted security level 100 should be reserved for an administration network like the internal servers network.The proxy server can be used to inspect, validate and limit access to outgoing traffic from the office network to the Internet.The ideal situation is to put each network (business function) on separate interface cards on the PIX. So instead of three network interfaces on the PIX, there would be six.

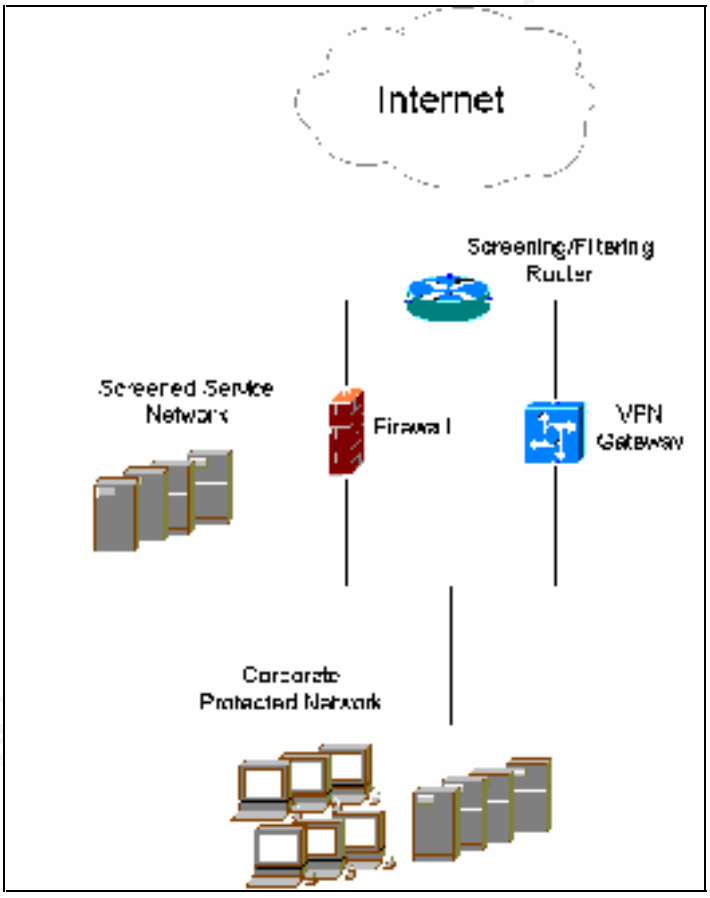


Assignment 4- Design Under Fire (25 points)

Select a network design from any previously posted GCFW practical.[28] Research and design two attacks against this architecture from the following three types:

1. An attack against the firewall itself.
2. A denial of service attack from 50 compromised cablemodems/DSL systems.
3. An attack plan to compromise an internal system through the perimeter system.

The network design chosen was developed by Colin Stuckless.[29]



[28] http://www.giac.org/GCFW.php
[29] http://www.giac.org/practical/Colin_Stuckless.doc

By mere coincidence, Mr. Stuckless is using a Cisco PIX Firewall with 3 network interfaces and a screened network. Unfortunately, no PIX OS release was listed in the practical, so assume PIX Firewall OS 5.3 which is their current general release. In all fairness, I liked the simplicity of Colin's network design and was one of the few I was considering implementing for GIAC Enterprise's PIX from the many example network architectures. But rummaging through class lecture notes, I came across a warning from the instructor to start partitioning and monitoring those pesky VPN gateways. Treat the home office VPNs as a partner or supplier, semi-trusted. Don't trust them as you would a local office system. I have heard stories of corporate intrusions[30] from home office DSL and cablemodems that connect via VPN.

An attack against the firewall itself

From Assignment 3, I already know the PIX firewall is one tough nut to crack and attack directly. There are relatively few Cisco security advisories[31] or exploits to work with, as compared with other firewall products. I think the best attack against the PIX firewall itself is the SSH CRC-32 attack[32] which is being widely used[33] against most devices that incorporate SSH1 for secure access. Worst case, the attack may be used against unpatched Cisco routers that the firewall may trust. Patch those devices!

Another way to bypass the firewall is to attack one of the servers it is trying to protect or screen. Let's say there is a telnet sever in the PIX screened network, then the recent login vulnerability[34] for some of the major Unix vendors might do the trick.

My favorite type of attack is to discover what the firewall trusts and see if the trusted source has weaker security. It's akin to skipping picking the lock in the front door and try for the good old sliding door or most windows locks. This can include unauthorized modems in the office or my favorite, wireless access points[35] and cracking the WEP encryption protocol[36].

Otherwise, I could not find three realistic and reasonable vulnerabilities for the PIX firewall itself, but found several attacks against the servers in the screened subnet the PIX is trying to protect.

[30] MS blocks staff dial-in access after 'minor' hack
[31] http://www.cisco.com/warp/public/770/52.html
[32] http://www.cisco.com/warp/public/707/SSH-multiple-pub.html
[33] http://www.cert.org/advisories/CA-2001-35.html
[34] http://www.cert.org/advisories/CA-2001-34.html
[35] http://www.sans.org/infosecFAQ/wireless/equiv.htm
[36] http://airsnort.sourceforge.net/

A denial of service attack from 50 compromised cablemodems/DSL systems

Unfortunately, the PIX does not defend well against denial of service attacks.[37] There is a USENIX paper[38] on how poorly the PIX behaved in a SYN flood attack. To demonstrate, using Colin Stuckless design and the PIX I have on loan, I used NINUNet's synflood tool[39] to send ten forged TCP SYN packets against the web server which the PIX is screening on port 80.

```
bash-2.04# ./synflood-NIUNet 192.168.1.1 64.29.19.80 80 10
synflooding  64.29.19.80 from 192.168.1.1 port 80 10 times
spoofing 129.62.13.81
spoofing 129.62.13.191
spoofing 129.62.13.26
spoofing 129.62.13.93
spoofing 129.62.13.246
spoofing 129.62.13.193
spoofing 129.62.13.8
spoofing 129.62.13.4
spoofing 129.62.13.221
spoofing 129.62.13.148
```

If you try to access the web server thru the firewall during this attack, you will receive a timeout. The timeout will clear itself in about 2 minutes and the web server can then be accessed again. Throwing more TCP SYN packets just makes the period to clear the timeouts longer and the firewall becomes "hung" for 10 minutes until the packet memory and state tables are cleared.

This was an attack using only one system and only 10 forged TCP SYN packets. 50 systems were not needed keep this firewall down, just one system using about 28kps link. Luckily the PIX firewall does not crash or hang indefinitely. When the attack stops, the PIX will eventually timeout and clear its state table and become functional again.

Two countermeasures are available to protect the PIX firewall. One is to implement TCP Intercept[40] on the Cisco border router to intercept SYN packets and let the Cisco router validate the SYN request. This will off load the SYN attack to the router, but the router has to have enough performance and memory to deal with these packets. The second is to upgrade the PIX OS to support TCP Intercept[41] which is available in PIX OS 5.2 and above.

[37] http://www.tech-mavens.com/synflood.htm
[38] http://www.usenix.org/events/sec01/invitedtalks/oliver.pdf
[39] http://cs.baylor.edu/~donahoo/NIUNet/SYNFlood.html
[40] http://cio.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm
[41] http://lists.gnac.net/pipermail/firewalls/2001-May/082737.html

An attack plan to compromise an internal system through the perimeter system
So how to get into the protected corporate network and compromise an office system thru a firewall? Simple, start a company called GotoMyPC[42] that offers remote access using almost any web browser from any where in the world back to your Windows office system thru almost any firewall. Prices start as low as $9.95 a month and just requires a windows application installed on your inside corporate network which polls an outside server checking for any request for connections. That's right, it's an outbound connection/tunnel, on port 80 or 443 or , so conveniently no changes are required on the firewall to let the traffic out thru.[43] Once a connection is requested via web browser and authenticated on the polling server, you have a tunnel back to your office system so you can remote control it. I loved the idea so much, I tried no credit card required free trial. It's great! It actually works thru my company firewall. Seriously, I did warn my Corp I/S I was going to trial test it. I can't wait until they have free open source versions of this idea. Wait. They do. ProxyTunnel,[44] Loophole,[45] and HTTPTunel[46] I just got to figure out to how to configure VNC[47] to work thru the tunnel. Honestly, I am working on the poor mans version…

As for a more reasonable and realistic compromise of an internal system through the firewall, let's target an office system on the protected corporate network behind the firewall. This means, the "attacker" is actually the employee trying to circumvent a security policy.

Assume the security policy for Colin Stuckless architecture does not allow office systems to become public servers accessible to the outside Internet. Remote employees must use encrypted VPN links to access their office systems.

An employee decides to disregard this security policy because the VPN software is not available for their home Macintosh or Linux box, or even more far fetched, somehow someone installed an application on employees desktop with out their knowledge. The application is called LapLink Gold 11.0.[48] This release of LapLink contains a feature called SurfsUp which has the same polling service as http://www.gotomypc.com/ described above, but instead uses LapLink's polling servers to establish outbound connections. Then the employee uses a unique system name, user name and password to access their office system from any system that supports a web browser. LapLink uses encryption also, making it difficult to analyze the traffic. A unique feature to LapLink's Surfs Up[49] is that it allows up to ten users to simultaneously connect to the office PC behind the firewall as a sharing server of sorts.

---

[42] https://www.gotomypc.com/
[43] https://www.gotomypc.com/help2.tmpl?#securitykeep
[44] http://freshmeat.net/projects/proxytunnel/
[45] http://freshmeat.net/projects/loophole/
[46] http://freshmeat.net/projects/httptunnel/
[47] http://freshmeat.net/projects/virtualnetworkcomputing/
[48] http://www.laplink.com/products/llgold/overview.asp
[49] http://www.pcmag.com/article/0,2997,s%253D1470%2526a%253D20629,00.asp

I believe this functionality will available in future Trojans, so intruders can get access behind firewalls back to office PCs they infected. The moral of the story is start watching and monitoring those outbound connections. The client constantly polling the outside poll server leaves a signature which can be detected, but the best countermeasure so far is to run a proxy server which validates outbound packets, requires employees to authenticate themselves for outbound connections and limit access to the outside polling servers of GotoMyPC, LapLink and any other IP addresses that offer this service commercially or for free.

APPENDICES

Appendix A – Cisco 2621 Border Router Configuration

```
! ************************************************************
! Cisco2621.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5.1 Build 10
! Appended with Rob Thomas Secure IOS Template
! Comments added by Alex Icasiano
!
! Hostname: Cisco2621
! Model: 2621
! ************************************************************
!
! Show timestamps in the log
service timestamps debug uptime
service timestamps log uptime

! "ROT13" passwords to hide them from shoulder surfers when viewing
! this configuration file on the router or TFTP server
service password-encryption

hostname Cisco2621

! The root or administrator password to this router
enable secret insert-password-here


! For the following commands I searched Cisco website[50] to find comments

! Disable services like echo, chargen, etc.
no service tcp-small-servers
no service udp-small-servers

! Do not enable host-name-to-address translation
no ip name-server
no ip domain-lookup

! Disable built-in webserver[51]
no ip http server

! Disable SNMP info
no snmp-server location
no snmp-server contact

! Allow us to go classless and use a netmask which ends in zero
ip subnet-zero
ip classless

! IP Static Routes
!ip route 0.0.0.0 0.0.0.0 FastEthernet 0/0
```

[50] http://www.cisco.com/univercd/cc/td/doc/product/software/ssr83/tsc_r/54008.htm
[51] http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml

```
! Changed ConfigMaker's default route to point to GIAC's ISP Router
ip route 0.0.0.0 0.0.0.0 66.33.61.1

! Something to scare away innocent people
banner motd ^C
CISCO 2621 Border Router.

No unauthorized access. Go away. You are not welcome here.
Violators will be violated and prosecuted. No trespassing.
^C

! Console Login
line console 0
 exec-timeout 0 0
 password insert-password-here
 login

! Telnet Login
line vty 0 4
 password insert-password-here
 login

! End of default Cisco ConfigMaker 2621 configuration file

! Additions from Class lecture[52] and Rob Thomas Secure IOS template

! Disable more services, I wish there was a document which
! details which Cisco IOS services are enabled by default
no snmp
no service finger
no ip source-route
no ip finger
no ip bootp server
ntp disable

! Enable Logging
logging 64.29.19.69
logging trap debug
logging console emergencies

! End additions from class lecture

! The following was added from the Secure IOS Template
!
! The below comments are from Rob in his Secure IOS Template
! My comments are marked with -Alex

! Do not share CDP information, which contains key bits about our
! configuration, etc. This command disabled CDP globally. If you
! require CDP on an interface, use cdp run and disable cdp
! (no cdp enable) on the Internet-facing interface.
no cdp run

interface FastEthernet 0/0
```

[52] Class lecture, Book 2.3, Page 56 & 57

```
 no shutdown
 description connected to Internet
 ip address 66.33.61.127 255.255.255.0
 keepalive 10
! Apply ingress filtering -Alex
 ip access-group 2010 in
! Don't send redirects.
 no ip redirects
! Don't send unreachables.
 no ip unreachables
! Don't propogate smurf attacks.
 no ip directed-broadcast
! Don't pretend to be something you're not. :-)
 no ip proxy-arp
! Do not reveal our netmask
 no ip mask-reply
!
! Deny any packets from the RFC 1918, IANA reserved, test,
! multicast as a source, and loopback netblocks to block
! attacks from commonly spoofed IP addresses.
access-list 2010 remark Anti-bogon ACL
! Claims it came from the inside network, yet arrives on the
! outside (read: Internet) interface. Do not use this if CEF
! has been configured to take care of spoofing.
access-list 2010 deny ip 64.29.19.0 0.0.0.255 any log-input
! Bogons
access-list 2010 deny ip 1.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 2.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 5.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 7.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 23.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 27.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 31.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 36.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 37.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 39.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 41.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 42.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 49.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 50.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 58.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 59.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 60.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 69.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 70.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 71.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 72.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 73.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 74.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 75.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 76.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 77.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 78.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 79.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 82.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 83.0.0.0 0.255.255.255 any log-input
```

```
access-list 2010 deny ip 84.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 85.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 86.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 87.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 88.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 89.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 90.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 91.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 92.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 93.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 94.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 95.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 96.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 97.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 98.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 99.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 100.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 101.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 102.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 103.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 104.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 105.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 106.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 107.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 108.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 109.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 110.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 111.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 112.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 113.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 114.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 115.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 116.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 117.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 118.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 119.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 120.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 121.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 122.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 123.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 124.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 125.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 126.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 127.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 169.254.0.0 0.0.255.255 any log-input
access-list 2010 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 2010 deny ip 192.0.2.0 0.0.0.255 any log-input
access-list 2010 deny ip 192.168.0.0 0.0.255.255 any log-input
access-list 2010 deny ip 197.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 201.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 221.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 222.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 223.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 224.0.0.0 31.255.255.255 any log-input
! Drop all ICMP fragments
access-list 2010 deny icmp any any fragments log-input
! Allow IP access to the intranet (firewall filters specific ports)
```

```
access-list 2010 permit ip any 64.29.19.0 0.255.255.255
! Our explicit (read: logged) drop all rule
access-list 2010 deny ip any any log-input
!
!
interface FastEthernet 0/1
 no shutdown
 description connected to Outside 64.29.19.0/24
 ip address 64.29.19.10 255.255.255.0
 keepalive 10
! Add an egress filter -Alex
 ip access-group 115 in
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip mask-reply
!
! Configure an ACL that prevents spoofing from within our network.
access-list 115 remark Anti-spoofing ACL
! Allow Outside Net to get out on the Internet -Alex
access-list 115 permit ip 64.29.19.0 0.0.0.255 any
! Now log all other such attempts.
access-list 115 deny ip any any log-input
!
! Configure null0 as a place to send naughty packets. This
! becomes the "roach motel" for packets -- they can route in,
! but they can't route out.
interface null0
 no ip unreachables
!
! Black hole routes. Be VERY careful about enabling these
! when running TCP Intercept.
ip route 1.0.0.0 255.0.0.0 null0
ip route 2.0.0.0 255.0.0.0 null0
ip route 5.0.0.0 255.0.0.0 null0
ip route 7.0.0.0 255.0.0.0 null0
ip route 10.0.0.0 255.0.0.0 null0
ip route 23.0.0.0 255.0.0.0 null0
ip route 27.0.0.0 255.0.0.0 null0
ip route 31.0.0.0 255.0.0.0 null0
ip route 36.0.0.0 255.0.0.0 null0
ip route 37.0.0.0 255.0.0.0 null0
ip route 39.0.0.0 255.0.0.0 null0
ip route 41.0.0.0 255.0.0.0 null0
ip route 42.0.0.0 255.0.0.0 null0
ip route 49.0.0.0 255.0.0.0 null0
ip route 50.0.0.0 255.0.0.0 null0
ip route 58.0.0.0 255.0.0.0 null0
ip route 59.0.0.0 255.0.0.0 null0
ip route 60.0.0.0 255.0.0.0 null0
ip route 69.0.0.0 255.0.0.0 null0
ip route 70.0.0.0 255.0.0.0 null0
ip route 71.0.0.0 255.0.0.0 null0
ip route 72.0.0.0 255.0.0.0 null0
ip route 73.0.0.0 255.0.0.0 null0
ip route 74.0.0.0 255.0.0.0 null0
```

```
ip route 75.0.0.0 255.0.0.0 null0
ip route 76.0.0.0 255.0.0.0 null0
ip route 77.0.0.0 255.0.0.0 null0
ip route 78.0.0.0 255.0.0.0 null0
ip route 79.0.0.0 255.0.0.0 null0
ip route 82.0.0.0 255.0.0.0 null0
ip route 83.0.0.0 255.0.0.0 null0
ip route 84.0.0.0 255.0.0.0 null0
ip route 85.0.0.0 255.0.0.0 null0
ip route 86.0.0.0 255.0.0.0 null0
ip route 87.0.0.0 255.0.0.0 null0
ip route 88.0.0.0 255.0.0.0 null0
ip route 89.0.0.0 255.0.0.0 null0
ip route 90.0.0.0 255.0.0.0 null0
ip route 91.0.0.0 255.0.0.0 null0
ip route 92.0.0.0 255.0.0.0 null0
ip route 93.0.0.0 255.0.0.0 null0
ip route 94.0.0.0 255.0.0.0 null0
ip route 95.0.0.0 255.0.0.0 null0
ip route 96.0.0.0 255.0.0.0 null0
ip route 97.0.0.0 255.0.0.0 null0
ip route 98.0.0.0 255.0.0.0 null0
ip route 99.0.0.0 255.0.0.0 null0
ip route 100.0.0.0 255.0.0.0 null0
ip route 101.0.0.0 255.0.0.0 null0
ip route 102.0.0.0 255.0.0.0 null0
ip route 103.0.0.0 255.0.0.0 null0
ip route 104.0.0.0 255.0.0.0 null0
ip route 105.0.0.0 255.0.0.0 null0
ip route 106.0.0.0 255.0.0.0 null0
ip route 107.0.0.0 255.0.0.0 null0
ip route 108.0.0.0 255.0.0.0 null0
ip route 109.0.0.0 255.0.0.0 null0
ip route 110.0.0.0 255.0.0.0 null0
ip route 111.0.0.0 255.0.0.0 null0
ip route 112.0.0.0 255.0.0.0 null0
ip route 113.0.0.0 255.0.0.0 null0
ip route 114.0.0.0 255.0.0.0 null0
ip route 115.0.0.0 255.0.0.0 null0
ip route 116.0.0.0 255.0.0.0 null0
ip route 117.0.0.0 255.0.0.0 null0
ip route 118.0.0.0 255.0.0.0 null0
ip route 119.0.0.0 255.0.0.0 null0
ip route 120.0.0.0 255.0.0.0 null0
ip route 121.0.0.0 255.0.0.0 null0
ip route 122.0.0.0 255.0.0.0 null0
ip route 123.0.0.0 255.0.0.0 null0
ip route 124.0.0.0 255.0.0.0 null0
ip route 125.0.0.0 255.0.0.0 null0
ip route 126.0.0.0 255.0.0.0 null0
ip route 127.0.0.0 255.0.0.0 null0
ip route 169.254.0.0 255.255.0.0 null0
ip route 172.16.0.0 255.240.0.0 null0
ip route 192.0.2.0 255.255.255.0 null0
ip route 192.168.0.0 255.255.0.0 null0
ip route 197.0.0.0 255.0.0.0 null0
ip route 201.0.0.0 255.0.0.0 null0
```

```
ip route 221.0.0.0 255.0.0.0 null0
ip route 222.0.0.0 255.0.0.0 null0
ip route 223.0.0.0 255.0.0.0 null0
!
end
```

Appendix B – PIX 520 Firewall Configuration

```
PIX Version 5.1(2)
! Setup login and administrator passwords, then hostname
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname giac-pix

! Pause every 24 lines when viewing this config file
pager lines 24

! Only Server Network can telnet directly to the PIX
telnet 10.3.0.0 255.255.0.0 inside
telnet timeout 5
terminal width 80

! Diable SNMP
no snmp-server location
no snmp-server contact
no snmp-server community
no snmp-server enable traps

! Enable floodguard to protect from attacks
floodguard enable

! IP Address for Log Host
logging host public 196.168.1.69
! Enable Logging
logging on
! We want timestamps in the log
logging timestamp
! Send warnings and above messages to the log server
logging trap warnings
! Specify SYSLOG Facility
logging facility 20

! GIAC does not have a 2nd PIX for failover
no failover

! Label the network interfaces and assign a security level
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 public security50
! Set the speed of the network interfaces
interface ethernet0 auto
interface ethernet1 auto


interface ethernet2 auto
! Set the MTU for each network interface
mtu outside 1500
mtu inside 1500
mtu public 1500
! Set the IP address for each network interface
ip address outside 64.29.19.13 255.255.255.0
```

```
ip address inside 10.1.0.13 255.255.0.0
ip address public 192.168.1.13 255.255.255.0
arp timeout 14400

! Set a default route to the border router
route outside 0.0.0.0 0.0.0.0 64.29.19.10 1

! Set a static route to get to the Server Network
route inside 10.3.0.0 255.255.0.0 10.1.0.10 1

! Activate PIX's Adaptive Security Algorithm to Inspect Traffic
fixup protocol ftp 21
fixup protocol smtp 25
fixup protocol http 80
fixup protocol h323 1720
! Removed due to graders comments that it allows rsh back in?
!fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521

! Create a Dynamic pool of IP addresses so public and inside networks
! can get to the outside (internet) network
global (outside) 1 64.29.19.100-64.29.19.250

! If we run out of Dynamic IP addresses, switch to PAT
global (outside) 1 64.29.19.251

! Create a pool of IP addresses so inside network can access
! the public network
global (public) 1 192.168.1.100-192.168.1.250

! Allow inside and servers nets to access outside network (internet)
nat (inside) 1 10.1.0.0 255.255.0.0
nat (inside) 1 10.3.0.0 255.255.0.0

! Allow inside users to access public network
nat (public) 1 192.168.1.0 255.255.255.0

! Map the hosts in public networks, so they are available
! to the outside (internet) network

! Put Webserver on the Internet, but allow access to port 80 & 443 only
static (public,outside) 64.29.19.80 192.168.1.80
access-list ouside_acl permit tcp any host 64.29.19.80 eq 80
access-list ouside_acl permit tcp any host 64.29.19.80 eq 443

! Add Internet access to DNS server to only UDP port 53
! No zone transfers here
static (public,outside) 64.29.19.53 192.168.1.53
access-list ouside_acl permit udp any host 64.29.19.80 eq 53

! Allow access to Mail server on port 25
static (public,outside) 64.29.19.25 192.168.1.25
access-list ouside_acl permit tcp any host 64.29.19.80 eq  25

! Allow access to Log host from Router
static (public,outside) 64.29.19.69 192.168.1.69
```

```
access-list ouside_acl permit tcp host 64.29.19.10 host 64.29.19.69 eq

! Apply the outside_acl rules to the outside interface
access-group outside_acl in interface outside

! Start of Employee Remote Access VPN Policy

! Create a pool of IP Addresses for Remote Employees
ip local pool vpnaddresspool 10.2.0.50-10.2.250.250

! Allow Office and Severs Networks to contact Remote Employees
access-list 111 permit ip 10.1.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list 111 permit ip 10.3.0.0 255.255.0.0 10.3.0.0 255.255.0.0

! Disable NAT for translation for inside networks
nat (inside) 0 access-list 111

! Allow Remote Employees to Access Outside (Internet) Network
nat (inside) 1 10.2.0.0 255.255.0.0

! Allow IPSEC clients through the firewall
sysopt connection permit-ipsec

! VPN Policy is ESP with DES encrpyption and MD5 checksums
crypto ipsec transform-set vpntransformset esp-des esp-md5-hmac

! Assign an access-list to this VPN Policy
crypto dynamic-map vpnmap 10 set transform set vpntransformset

! Assign a policy stating we want to use ISAKMP to share keys.
crypto map vpnmap 11 ipsec-isakmp dynamic vpndynamicmap

! PIX will assign an IP address to each remote client
crypto map vpnmap client configuration address initiate

! PIX will accept requests for an IP address from any VPN client
crypto map vpnmap client configuration address respond

! Assign this VPN Policy to the outside interface
crypto map vpnmap interface outside

! Enable isakmp connection to outside interface
isakmp enable outside

! Create a single shared password for all VPN clients
! When GIAC has more funding changa to Radius or TACACS+ servers
isakmp key put-password-here address 0.0.0.0 netmask 0.0.0.0

! When PIX identifies itself, use an IP address for ISAKMP identitity
! If using RSA certificates, use hostnames as certificates contain hostnames
isakmp identity address

! Assign the VPN IP Address pool to the outside interface
isakmp client configuration address-pool local vpnaddresspool outside
```

```
! ISAKMP Policy: pre-shared password, DES encryption and MD5 checksum
isakmp policy 12 authentication pre-share
isakmp policy 12 encryption des
isakmp policy 12 hash md5

! Group 1 is 768-bit Diffie-Hellman key exchange, Group 2 is 1024 bit
isakmp policy 12 group 1

! This ISAKMP policy lasts one day (86400 seconds)
isakmp policy 12 lifetime 86400
```

Appendix C – Cisco 4500 IPSEC VPN Router Configuration

```
! ****************************************************************
! Cisco4500.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5.1 Build 10
! Comments added by Alex Icasiano
!
! Hostname: Cisco4500
! Model: 4500
! ****************************************************************
!

! These are same default commands as 2620 router, see comments there
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Cisco4500
!
enable secret insert-password-here
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing

!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 64.29.19.10

no ip http server
no snmp-server
no snmp-server location
no snmp-server contact

! Enable Logging
logging 64.29.19.69
logging trap debug
logging console emergencies

line console 0
 exec-timeout 0 0
 password insert-password-here
 login
!
line vty 0 4
 password insert-password-here
 login
```

```
! This section begins differences between Cisco 2621 router config
!
! VPN Security Policy
!
! Internet Key Exchange (IKE)

! Enable IKE negotiation on the router globally
crypto isakmp enable

! Identify in negotiations by IP address, if using RSA certificates
! change to hostname, as they use hostname instead of IP address to ID
crypto isakmp identity address

! Partner IKE Policy, use shared password, DES, MD5 and 768bit DH
crypto isakmp policy 1
 encryption des
 hash md5
 authentication pre-share
 group 1
 lifetime 86400
crypto isakmp key insertpartnerpasswordhere address 12.33.247.6

! Supplier IKE Policy, use shared password, DES, MD5 and 1024bit DH
crypto isakmp policy 2
 encryption des
 hash md5
 authentication pre-share
 group 2
 lifetime 86400
crypto isakmp key insertsupplierpasswordhere address 167.216.198.40

!
! IPSec
!

! Apply the crypto map to the outside interface Ethernet 0
crypto map cm-cryptomap local-address Ethernet 0
!

! Partner IPSEC Policy, ESP, DES encryption and MD5 checksums
crypto ipsec transform-set cm-transformset-1 esp-des esp-md5-hmac
crypto map cm-cryptomap 1 ipsec-isakmp
 match address 100
 ! The Partners Cisco router
 set peer 12.33.247.6
 set transform-set cm-transformset-1
 ! Change the session key ever 3600 seconds or 4608000 kilobytes
 set security-association lifetime seconds 3600
 set security-association lifetime kilobytes 4608000

! Suppliers IPSEC Policy, same as above
crypto ipsec transform-set cm-transformset-2 esp-des esp-md5-hmac
crypto map cm-cryptomap 2 ipsec-isakmp
 match address 101
 set peer 167.216.198.40
 set transform-set cm-transformset-2
```

```
 set security-association lifetime seconds 3600
 set security-association lifetime kilobytes 4608000
!
interface Ethernet 1
 no shutdown
 description connected to GIAC Shared Network
 media-type 10BaseT
 ip address 176.16.0.11 255.255.0.0
 ip access-group 1 in
 keepalive 10
!
interface Ethernet 0
 no shutdown
 description connected to Internet
 media-type 10BaseT
 crypto map cm-cryptomap
 ip address 64.29.19.11 255.255.255.0
 no ip route-cache
 keepalive 10


! Don't allow outside (Internet) access from the shared network
! Access Control List 1
!
access-list 1 deny any

! Access Control List 100 for Partner

! Allow the routers to access each other
access-list 100 permit ip host 64.29.19.11 host 12.33.247.6

! Allow Partner only to access SQL Proxy Server Port via IPSEC
access-list 100 permit tcp 10.10.0.0 0.0.255.255 host 176.16.15.21 eq
1521

! Deny everything else
access-list 100 deny ip any any log

!
! Access Control List 101 for Supplier
!
access-list 101 permit ip host 64.29.19.11 host 167.216.198.40
access-list 101 permit tcp 10.11.0.0 0.0.255.255 host 176.16.15.21 eq
1521
access-list 101 deny ip any any log

end
```

ACKNOWLEDEMENTS

I would like to thank the company I work for and my manager John Becker for providing the resources and time off to attend the SANS certification courses. I especially want to thank my co-worker Michael O'Connor for covering for me when I am out at SANS conference or writing the practical. Without their support, I would never have the time to learn what SANS has to offer.

I want to thank Chanda and Chris of Atebion, Inc., Dean of PacketSense, and Krishna from SGI, Inc. for lending me their unused Cisco equipment necessary to research this paper.

I want to thank Miguel Sanchez of Para-Protect for providing me insight from consulting side of the world.

To my family and friends, I apologize for disappearing and not attending get togethers when I was busy with this paper. Forgive me.

REFERENCES

Frequently Visited Cisco Website

Technical Tips
http://www.cisco.com/public/technotes/serv_tips.shtml

NAT Technical Tips
http://www.cisco.com/warp/public/556/index.shtml

Cisco Technical Assistance Center (TAC) Top Issues
http://www.cisco.com/public/support/tac/top_issues.shtml

Cisco Secure Pix Firewall
http://www.cisco.com/warp/public/110/top_issues/pix/pix_index.shtml

Virtual Private Networks (VPN)
http://www.cisco.com/warp/public/471/top_issues/vpn/vpn_index.shtml

IOS Software Installation and Upgrade Procedure
http://www.cisco.com/warp/public/130/sw_upgrade_proc_ram.shtml

Password Recovery Procedures
http://www.cisco.com/warp/public/474/pswdrec_2600.shtml

Cisco Manuals Consulted

Configuration Guide for Cisco Secure PIX Firewalls 5.1
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/index.htm
Cisco IOS Security Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/

Example Cisco Configurations

Configuring Cisco PIX-to-VPN Client Wild-card, Pre-shared, Mode Config
http://www.cisco.com/warp/public/110/A.html

Configuring IPSec Router-to Router with NAT Overload
http://www.cisco.com/warp/public/707/ios_D.html

Configuring the Cisco Secure PIX Firewall with Three Internal Networks
http://www.cisco.com/warp/public/110/19c.html

Configuring the PIX Firewall with Mail Sever Access on the DMZ Network
http://www.cisco.com/warp/public/110/mailserver_dmz.html

Practicals Reviewed

http://www.giac.org/GCFW.php
Alan Moe
Stephen Carroll
Colin Stuckless
Jeff Stelzner
Jim Hendrick
Dwan Denter
Todd Williams
Asad Alsader
Mark Fennig
Mario Serrano
Thomas McDermott
David Stanislawski