SANS GCFW Practical Assignment

(v1.9)

"Protecting the Reputation and Fortunes of GIAC Enterprises"

June 18, 2003

By: Brent Whitmore

Table of Contents

Table of Diagrams

Assignment 1 Security Requirements

A little history of fortune- GE founder Chen Fu Chao, immigrated to San Francisco, USA in 1940 and started his own business manufacturing fortune cookies integrated with their own unique sayings. The business is a typical "bricks and mortar" enterprise and had done quite well in recent years by providing fortune sayings to 80% of the American Chinese restaurant market. They have 60 employees, including international sales representatives.

A Father's painful lessons- Chen Fu and his sons last year provisioned an internet link to their facility and asked the Internet Service Provider (ISP) to provide a "firewall thing", which was a 1706 Cisco router, to allow access to the internet. They also set up a static content website using Microsoft technology as a first step, run straight from the setup wizards. Everyone was in high spirits with the ability to do "way cool" things like browse the internet for new Chic Chinese restaurant prospects and pipe Chinese music from Beijing via streaming, UNTIL, Chen Fu noticed his mouse moving on his computer screen, WITHOUT his control!!!! The website had some strange content that day; and after several of his customers called to see why GE was now so "unpatriotic" by bashing certain things on their website, Chen Fu knew something was amiss.

Suffice to say, there was much consternation in the house of Chen FU, and after much dishonoring of his sons, Chen Fu with one hand ripped the internet T1 cable out of ISP router in the broom closet. Chen Fu's trust was broken, and his sons needed badly to gain back his respect and their honor.

That's where we come in….."We" are a small security "boutique."

1.1 Discovery of GIAC Enterprises

1.1.1 Introduction-First things first

A changed mind- Last year Chen Fu was not as trusting of the role of technology or security in expanding his business as his sons; however after this recent security breach, they have persuaded him to test their wisdom by using some new security measures to meet their challenging business goals.

Business goals- Chen Fu and his sons who make up of the board of directors want to grow GE sales by 200% in the next 2 years. They plan to meet this business objective with two initiatives:

1. *Expanding to serving new US restaurant markets as well as to Latin and European markets (Thai, Vietnamese, Korean restaurants)*

2. *Developing a savvy global restaurant marketing strategy and name branding*

The Need for a New Plan- We will build a new Security infrastructure that will support Chen Fu's business goals of increasing revenues of 200% by "Expanding Markets and Promoting their Brand Name."

However, we shared with them that business objectives should always drive technology objectives; not the other way around. Wise old Chen Fu is not impressed with technology, and he has told us that he requires strong persuasion that his sons' new Web application solutions, his proprietary data, and his name brand will be "dragon-protected", in his words.

So our major stakeholder is committed! That is the first step for ensuring success and in bulding our security policy.

Our bottom line Security Objectives are:

- **To Protect GE's electronic assets within reasonable costs**
- **To Protect GE's name brand and reputation within reasonable costs**

Business goals should drive the technical solution. This paper will propose a Security design that provides both a solution once we are able to collect the business goals. Technology should always meet the business goal.

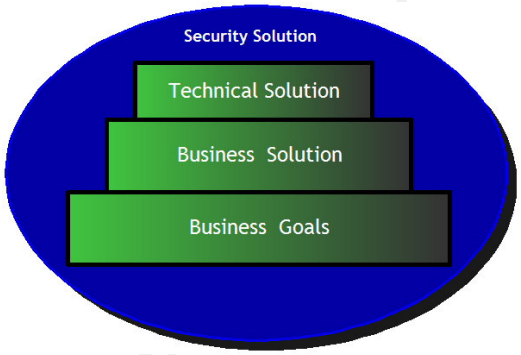


Diagram 1.1—1 Business goals drive Security Solutions

With the business goals defined, Chen Fu's sons have begun work on creating an internal web application/database and basic networking infrastructure that meets their needs. They want us to deliver a reasonable Perimeter security plan that will help to get them back into their father's good graces.

Our Methodology:

Discover the business and security Goals

Design a workable security plan that will protect critical business functionality

Deploy and **Test** the Security Solution

Up and Down the OSI Model:

Many security solutions aim at securing OSI (Open Systems Interconnect) Layers 1-4, but many of the exploits post-year 2000 are focusing on vulnerabilities above Layer 4, which comprises the Session, Presentation, and Application layers. We will attempt to protect ALL layers within reasonable cost.

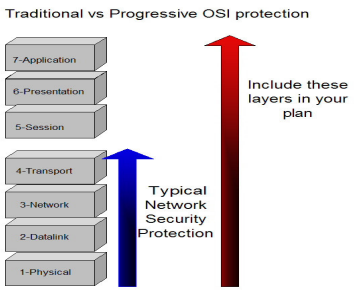


Diagram 1.1—2 Traditional OSI Protection

1.1.2 Kick-off with Project Sponsor(s)

Before we can begin to create a security solution for GE we must sit down and talk with the Business sponsor **to get an idea of his expectations**. Even though the board has brought us in, we must talk with owner and chairman to facilitate communication and education, which are paramount to security solutions.

Best Practice- Basic security policy must be supported by the top of the command chain.

1.1.2.1 Commit them with their requirements

First, we will engage our client by having them complete a short informal questionnaire with us. This does three things for us:

- **It actively INVOLVES the decision makers**
- **It provides a way to find out any hidden agendas and true motives of performing a security "overhaul'.**
- **It allows for the education of security to begin!**

We will address the following issues with Chen Fu and sons and ask them to rate each of the major areas of security. These are to be rated from one to 10, with 10 being most critical. This provides the basis for Assignment 1.

Here are the statistics from the 4 board members and co-owners of the company:

Client's Rating of Business factors:	Priority
Increase sales via electronic retail and wholesale means via web sales	**3.35**
Maintaining company reputation via electronic means through protection	**2.13**

Control costs as much as possible	**1.23**
Enable easy development of business applications and business channels	**1.02**
Fault tolerance or business continuity of systems	**0.89**
Allowing the most speed of online transactions by web customers	**0.76**
Allow the most protection in electronic layers	**0.63**

Response: We validate with GE that they want the design to provide a simple and easy security solution that protects online web sales and their electronic "image" by controlling costs whenever possible.

Client's Rating of Security factors:	Priority
Allow easy access to business systems for external sales force and partner	**3.43**
Keeping unwanted persons out of company electronic perimeter	**3.12**
Protect application integrity	**1.13**
Protect database integrity Control employee access to untrusted areas such as internet	**0.87**
Provide easy to manage security solutions	**0.68**
Provide more ability to monitor business and security systems	**0.45**
Protect network integrity	**0.38**

1.1.3 Current architecture Budget

As was mentioned above, GE has a single Cisco router, and 5 daisy chained hubs, connecting some older Compaq tower servers and desktop machines. They have budgeted extra money from a special account to purchase 1U servers and new racks to mount the infrastructure gear. They also want to place the servers in a new windowless room that they are building on a new floor in their existing 4 story building.

1.1.4 Budget for Phase One - OVERHAUL

Chen Fu and his sons have not given us a budget. They want us to perform a complete redesign and to implement a basic Phase 1 Security plan. They are interested in possibly investing more after 1 year where we can come in to add more redundancy, layers, and countermeasures as Phase 2.

Luckily most of the cost for the project like routers, switches and servers will fall under the new application, GEfortunes.com, being developed by one of Chen Fu's sons. He has given us an "unspoken" security budget of about $100-150K. All of the servers will be 1U rackable Dell PowerEdge servers, unless noted.

1.1.5 Current Support Staff and Policies

Although some of the system administration has been done by Chen Fu's sons, they have recently hired competent and experienced infrastructure administrators. They also are responsible for maintaining the company database and web applications, so their time is spread over several projects. They seem glad that we are here to assist in the security design, especially after we have involved them in the decision process!

GE's current techical policy is to stay Industry standard! Most of their skill sets are in Microsoft .NET and Windows, where one admin claims to know Linux by running it at home. They have adequate comfort with Cisco and SQL skills. There is no current 24 hour on site support at the facility, but that is an option in the future.

1.1.6 Major GE User Groups and their Access requirements

These are groups that will help define GE's business process. We must keep each of these groups in mind in our security design:

1. **Customers**-who must be allowed at all times to buy online from www.GEfortunes.com
2. **Suppliers**-must be able to submit fortune sayings to GE and track acceptance and payments using secure online submittal forms
3. **Partners-**
   a. **Translation service partners-**must be able to access, download and upload untranslated sayings to translate them in 4 different languages
   b. **Resellers-**must be able to purchase e-wholesale sayings to resell
4. **Internal GIAC employees-** will need to access the following areas:
   a. *Internal resources*- to perform private business operations
   b. *External resources*-to perform research
5. **GIAC mobile sales force and teleworkers-**must be able to place sales orders access sales automation tools on the Corporate Zone securely from the internet

Each of these groups is important for reaching GE's business goals by allowing them easy but secure access to and from the internet.

1.1.7 Access Matrix for Groups

GE wants us to design a strategy that allows each of the above groups to access ONLY what they need to access according to the basic details listed below. Note that as business changes, we need to have the flexibility to allow and deny access with different protocols and services.

Who?	***What Application?***	***From/To Where?***	***Why?***
Web Customers-Untrusted	WEB application, www.GEfortunes.com-HTTP/HTTPS	Internet->DMZ	To allow sales revenues
Suppliers-Untrusted	Webified Supply Chain software and billing,	Internet->DMZ	To streamline saying procurement by easing

	supp.GEfortunes.com. unique login-HTTPS		submittal by web
Partners-untrusted	Partners.gefortunes.com Mini-store front hosting from main page, different login HTTP/HTTPS	Internet->DMZ	To allow anytime access to submit and/or receive product, or sell wholesale
Internet employees-trusted	Corporate-IPSEC VPN HTTP/HTTPS	Internet->Corporate Internet->DMZ	Sales automation, webmail, network resources
Internal GIAC employees	Outgoing/incoming email/web-SMTP/HTTP/streaming	Corporate ->Internet	To allow market research, business operations

1.2 Architecture of New Design

Our new security design will help meet the company's business goals by protecting/restricting access for each of the 5 groups. First, we will present some guidelines.

1.2.1 Design Guidelines

Successful security design requires a multitude of layers, which provide defense in depth. But because more layers increase complexity for GE, we will simplify the design with 3 layers. Most successful designs follow rules similar to the following:

Guideline 1: **Prioritize your assets in measurable terms**

Guideline 2: **Security is a Process by all, not a Product by "one"**

Guideline 3: **Layer your defenses, Limit your liabilities**

Guideline 4: **Simplicity is your friend, both in protection and in troubleshooting!!! Costly solutions don't always save lives.**

Guideline 5: **Ongoing Safety is the reward of the diligent man, or woman**

We have indentified and learned that the Valuable Assets of GE are:

- **The Data sitting in a dynamic database on the Corporate network**
- **The Reputation of GE on the e-business front is paramount(behind protecting the "Valuable Assets"), and protection must be in place by preventing defacing of public documents and web image.**

We must endeavor to protect these assets.

1.2.2 Our Security Policy

We begin to caputre these design goals and guidelines above to create a written security policy. Here is a simple Overview of our Security policy:

Direction	FROM		TO	Access
OUT	INSIDE	,----------\>| NO!	OUTSIDE	NONE
IN	OUTSIDE	,----------\>| NO!	INSIDE	NONE
ACROSS	VPN	,<--------- NO! --------->	DMZ	NONE
OUT	DMZ	,----------> Filter	OUTSIDE	FILTERED
IN	DMZ	,----------> Filter	INSIDE	FILTERED
OUT	INSIDE	,---------->	VPN	ALLOWED
IN	VPN	,---------->	INSIDE	ALLOWED

Major Rule- NO traffic will traverse from INSIDE to OUTSIDE without Packet inspection, breakdown, or reconstruction

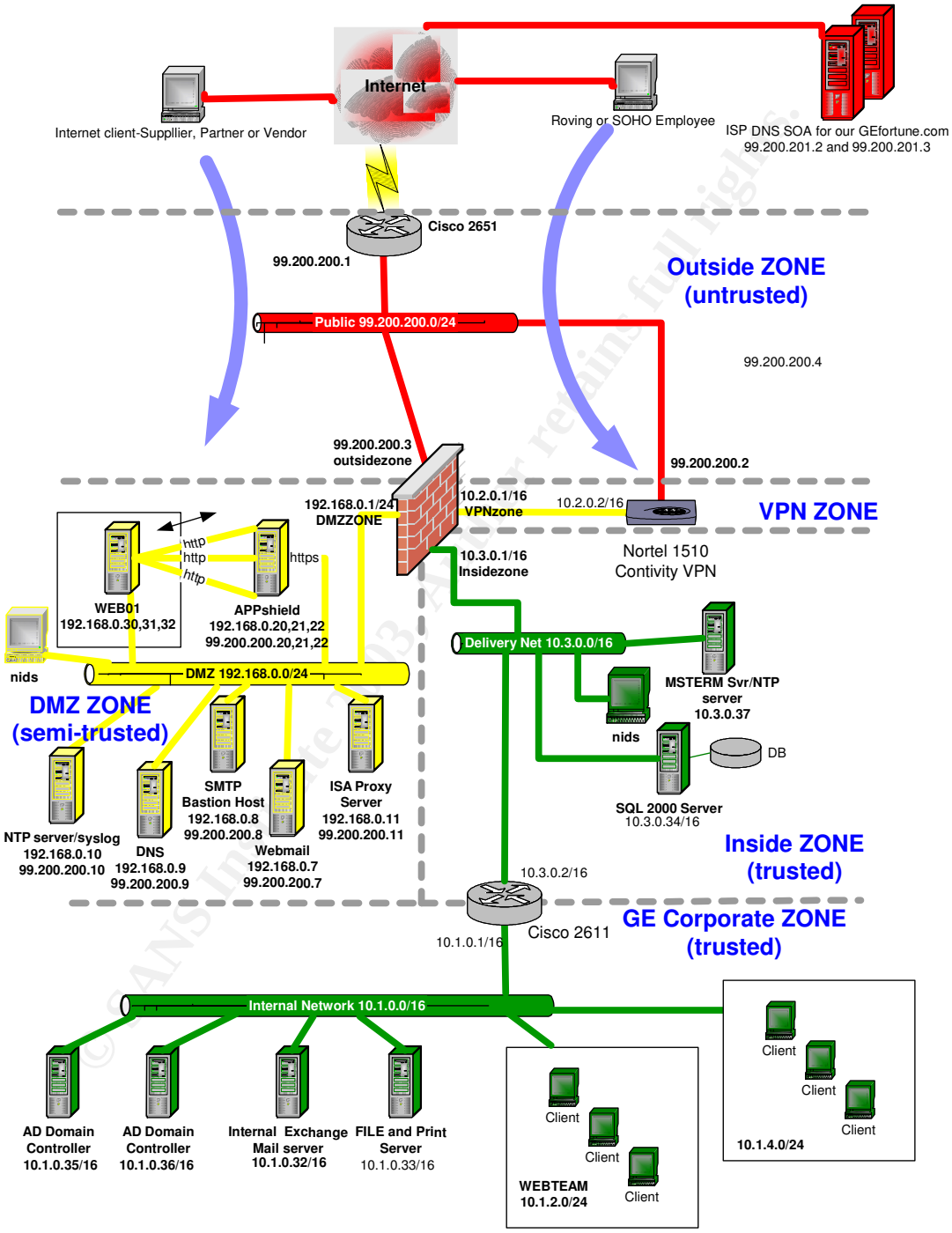
Minor Rule- Any Many to One or One to Many access will ALWAYS be located in the DMZ

We can now write out the security policy for defining the access, direction, technology, and Zones with the firewall must control. The security policy should abide to these parameters:

Who (Users)	Who (Host)	Direction	FROM	TO	WHAT access	WHY	HOW	WHEN	LOG ON FW?	Relation-ship
INSIDE										
Inside Users	ALL INSIDE HOSTS	OUT	INSIDE-ALL	DMZ-PROXY ONLY	HTTP/FTP/HTTPS/ configurable	Business research	VIA PROXY	24/7	on Proxy	many:1
	PROXY SVR	OUT	DMZ-PROXY ONLY	OUTSIDE ANY	HTTP/FTP/HTTPS/ configurable	DIRECT CONNECT FOR INTERNAL CLIENT	NAT	24/7	ON PROXY	1:1
Developers	WEB TEAM	Across	INSIDE	DMZ web SVRS	HTTP/FTP/HTTPS/ configurable	web dev and support	DIRECT	24/7	Yes	few:few
Sysadmins	MSTermSVR	across	MSTERMsvr	all DMZ, VPN, CORPORATE	TCP port 3389	support	DIRECT	24/7	Yes	1:many
NETWORK SVCS										
	NTP server	OUT	DMZ	OUTSIDE -2 NTP SVRS ONLY	UDP 123	INET TIME UPDATE	NAT	24/7	YES	1:2
	NTP SVR	LOCAL	DMZ ALL SERVERS	DMZ-NTP ONLY	UDP 123	DMZ SYNC	DIRECT	24/7	YES	many:1
	NTP SVR	ACROSS	INSIDE-NTP SVR ONLY	DMZ-NTP SVR ONLY	UDP 123	INSIDE SVR SYNC	DIRECT	24/7	YES	1:1
	NTP CLIENT	ACROSS	INSIDE	INSIDE-NTP ONLY	UDP 123	INSIDE USERS SYNC	DIRECT	24/7	NO	many:1
	SYSLOG SVR	IN	DMZ, FW, and border router	SYSLOG	UDP 514	collect logging	NAT	24/7	NO	many:1
Webmail users	WEBMAIL SVR	IN	OUTSIDE-ANY	DMZ-WEBMAIL ONLY	TCP 80/443	ACCESS web-based mail	NAT	24/7	YES	many:1
Webmail users	WEBMAIL SVR	IN	DMZ-WEBMAIL ONLY	INSIDE EXCHANGE ONLY	TCP 110	Connection for corporate email	DIRECT	24/7	NO	1:1
	DNS SVR	OUT	DMZ-DNS ONLY	OUTSIDE ANY	TCP 53	for Proxy recursive lookups, outgoing mail hosts	NAT	24/7	YES	1:many
Outside hosts	DNS SVR	IN	OUTSIDE ANY	DMZ-DNS ONLY	TCP 53	to allow 3rd backup for DNS, to allow for zone transfers from ONLY ISP dns SOA	NAT	24/7	YES	many:1
	DNS SVR	LOCAL	DMZ PROXY SVR DMZ SMTP SVR	DMZ-DNS ONLY	TCP 53	TO ALLOW OUR DMZ SVRS NAME LOCAL NAME RESOLUTION	NAT	24/7	N/A	1:1
Mailusers	EXCHANGE	OUT	INSIDE EXCHANGE ONLY	DMZ-SMTP ONLY	TCP 25	to send INSIDE smtp mail out to internet to SMTP gateway	DIrect	24/7	NO	1:1
Mailusers	SMTP Gateway	IN	DMZ-SMTP ONLY	INSIDE-EXCHANGE ONLY	TCP 25	send outside SMTP mail IN	DIrect	24/7	NO	1:1
Mailusers	SMTP Gateway	OUT	DMZ-SMTP ONLY	OUTSIDE-ANY	TCP 25	send filtered mail OUT to ANY	NAT	24/7	NO	1:many
Mailusers	SMTP Gateway	IN	OUTSIDE-ANY	DMZ-SMTP ONLY	TCP 25	send filtered mail IN		24/7	YES	many:1
OUTSIDE USERS										
Customers	www.gefortunes.com 99.200.200.20	IN	OUTSIDE-ANY	DMZ-APPSHIELD WEB	HTTP/HTTPS	Sales Order/buy	NAT	24/7	NO	many:1
Suppliers	supp.gefortunes.com 99.200.200.21	IN	OUTSIDE-ANY	DMZ-APPSHIELD WEB	HTTP/HTTPS	Supplychain and billing	NAT	24/7	YES	many:2
Partner & Translators	partners.gefortunes.com 99.200.200.22	IN	OUTSIDE-ANY	DMZ-APPSHIELD WEB	HTTP/HTTPS	uploading sayings, selling wholesale and retail	NAT	24/7	YES	many:3
DMZ SQL ACCESS										
USER AUTH AND TRANSACTIONS	WEB01	ACROSS	DMZ-WEB01 ONLY	INSIDE SQL ONLY	TCP 1433	FILTERED AUTH AND UPDATING OF ACCESS TO DATABASE	DIRECT	24/7	YES	1:1
VPN USERS FROM OUTSIDE										
Mobile Workers	VPN clients	IN	OUTSIDE-ANY	INSIDE CORPORATE	all protocols if encrypted with ESP	Business Sales automation Collaboration Administration	VPN	24/7	Yes, on vpn	many:1

1.2.3 Network Design

Based on the written requirements, the following graphic is representative of what we propose for GE:



1.2.4 IP Address assignments

The following chart outlines the private IP address ranges for each network segment or Zone. The DMZ could have been used in the 10.0.0.0/16 address space, but we decided to change the numbering to another RFC1918 address space for easy identification. Note that the 99.0.0.0 is currently unregistered according to IANA, so we will be using that as our GE network.

IP address/Range	Zone	Information
99.200.200.1/24	OUTSIDEZONE(Untrusted)	Internet accessible(public)
192.168.0.0/24	DMZZONE(semi-trusted)	Filtered Private RFC 1918
10.3.0.0/16	INSIDEZONE (trusted)	Private RFC 1918
10.2.0.0/16	VPNZONE (semi-trusted)	Private RFC 1918
10.1.0.0/16	GE Corporate (trusted)	Private RFC 1918
10.4.0.0/16	Future subnets	expandability
……		For growth
10.255.0.0/16	Future subnets	For growth
99.200.200.21	www.gefortunes.com	Main WWW site
99.200.200.22	Supp.gefortunes.com	Supplier authenticated site
99.200.200.23	Partner.Gefortunes.com	Partner site, up/download
99.200.200.7	Webmail.gefortunes.com	Web-based mail
99.200.200.8	SMTP.gefortunes.com	SMTP Bastion HOST
99.200.200.9	NS3.gefortunes.com	DNS secondary server
99.200.200.10	Unnamed	NTP/SYSLOG sever
99.200.200.11	Corp.gefortunes.com	PROXY server for internal

1.2.5 Traffic flow, per access group

Charting the data flow by access groups in your security framework will reveal the types of measures you will need to put in place to protect the Most Valuable assets. There are two main groupings for this: Trusted and Untrusted groups.

Untrusted- The external groups Customers, Suppliers, and Partners are NOT to be totally trusted. However, they DO need to be authenticated to authorize the actions listed above. We do not have ANY management control over the Untrusted groups' source devices or security policies.

Trusted- We will trust the Internet Users and the Internal users via authentication since we have more control over their accessing systems via antivirus, personal firewalls, and personal privacy software controls.

1.2.5.1 Untrusted Groups-Web customers', Suppliers', and Partners' traffic flow-

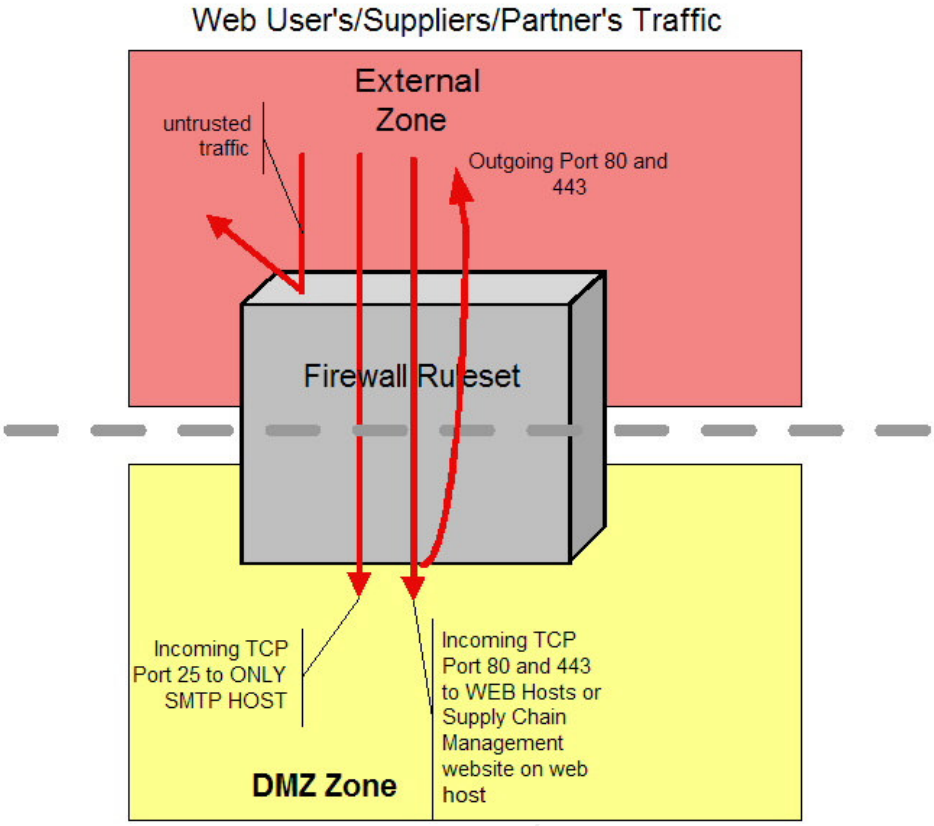


Diagram 1.2—1 Untrusted Groups data flow

Requirements-

Traffic for web customers and suppliers will be filtered at OSI layers 2-5 at the firewall. Layers 4-7 can be filtered using a positive Policy using a tool called Appshield. Traffic will be allowed for valid TCP sessions and authenticated by user name for shopping cart orders. Once authenticated all traffic will be encrypted using server certificates. Web customers can peruse the site for Saying of the Day and to purchase Fortunes for immediate downloading, or orders to be shipped via Parcel service. Suppliers and Partners can check a separate website for status on current Purchase Orders and Sales Orders for ingredients, paper, etc.

Web customers need to access website www.GEfortunes.com, in DMZ via TCP ports 80 and 443 (HTTP/HTTPS), as well as UDP port 53 (DNS), same as below

Suppliers need to access Supplier website Supp.GEfortunes.com in DMZ via TCP ports 80 and 443 (HTTP/HTTPS)

Partners need to access website Partners.GEfortunes.com in DMZ via TCP ports 80 and 443 (HTTP/HTTPS) and secure FTP via TCP port 21/22/

Group Restrictions:

- **None of these groups should be able to DIRECTLY access GE's corporate network segment.**
- **None of these groups should be able to access any databases directly**
- **Each group will access a different logical website on the single webserver. One group will not be able to access another group's website so authentication must be set in place.**

1.2.5.2 Trusted GIAC employees' Internet Access Traffic Flow

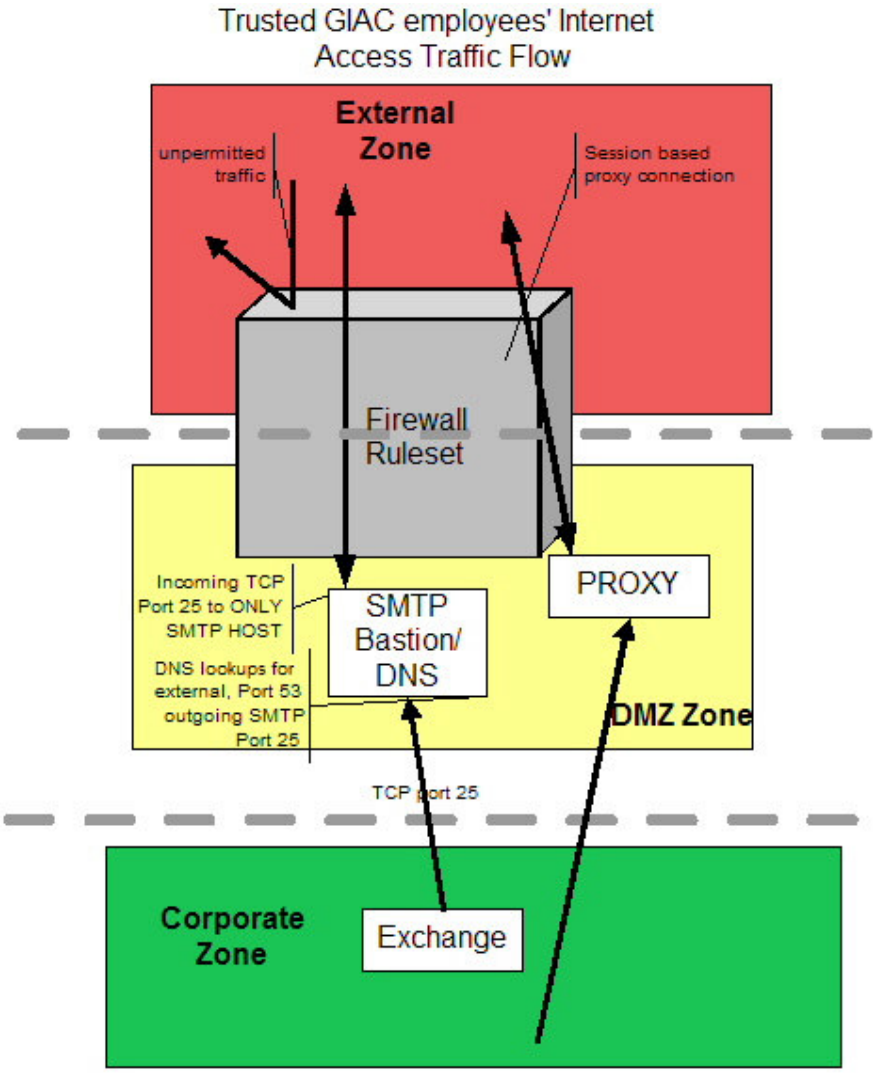


Diagram 1.2—2 Trusted Groups Data flow

Requirements: Current business practices require that internal GE Employee access the internet. This access should be available for all employees.

Restrictions: Chen Fu wants to have the flexibility to restrict and log access to certain internet sources if deemed necessary. We want to provide him with antivirus protection for this outbound browsing.

Microsoft Windows 2000 ISA Server-Having a Web and Winsock Proxy allows for outbound user internet traffic. A Proxy will "act on behalf of" a web client seeking access to the outside. This provides some protection in that only ONE host is actually making TCP connections out of the GE network. Proxies can usually filter on OSI layer 3-7, as well as cache information for the internet user, which allows for better performance. The Proxy will have antivirus real time mechanisms.

1.2.5.3 Trusted GIAC mobile sales force and teleworkers Traffic Flow

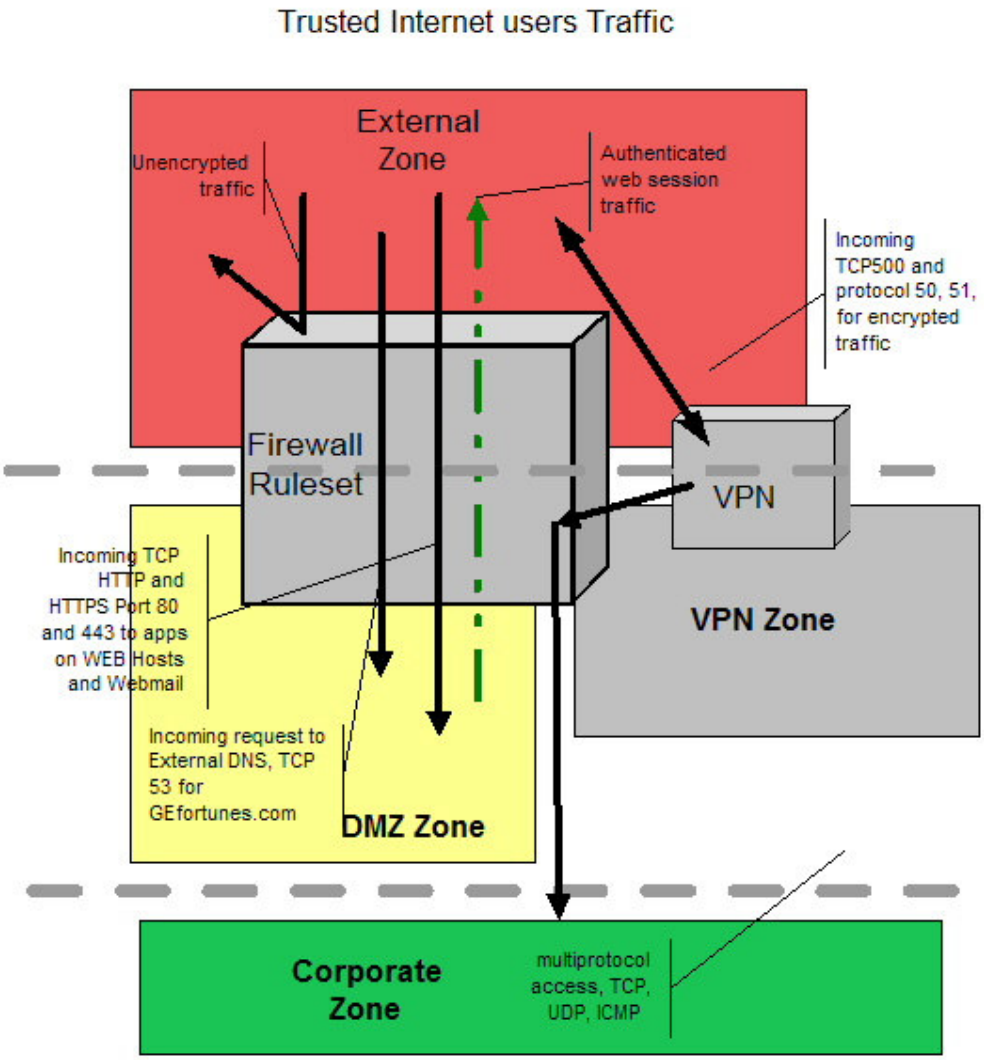


Diagram 1.2—3 Mobile Users' Data flow

All Outsiders are not all bad. We need to allow ONLY those people we want for business reasons. That is why we must perform some checking on their identity and encrypt all traffic since they will be coming inside from untrusted networks. This is done quite easily by using Virtual Private Networking host to provide access to these folks. All traffic in VPNs can be safely tunneled inside normal IP packets and the data payload encrypted to prying external eyes. We can trust these teleworkers

because we have administrative control over their laptops, and have installed personal firewalls upon their systems. Other SOHO broadband home employees we have imposed a voluntary security policy by mandating they install a company provided personal firewall. We can determine this by scanning their public IP address when they are connected.

Requirements:

Access all internal network resources such as Intranets, certain network file shares and printers, and email

Easy access to email services

Domain pass through authentication

Restrictions:

Internet Employees users cannot access databases, POP3, nor MSTerminal server hosts

Personal firewalls are a must on all VPN access source locations

1.2.6 Major Components of OUTSIDE ZONE

1.2.6.1 Border Router – Cisco 2651XM

```
Cisco IOS Release 12.2(15) T, Firewall Feature Pack
```

Two Cisco 3620 routers were originally proposed to provide Internet link redundancy, but we could not obtain an Autonomous System Number (ASN) needed for BGP in time for deployment. Also since we are keeping costs down, Chen Fu liked the idea of using one router until the next phase.

1.2.6.1.1 Security Function-First layer of Filtering Protection

This is our first layer of defense. By enabling access control lists on the Internet interface (Internet-facing), we can filter out unwanted packets by IP address and Port number before they hit our inward layers. This router will allow only explicit traffic into our inward zones. This layer keeps traffic to the main firewall "clean" in that it drops all traffic that does not fit its Access Control list. Enabling the Context Based Access control will allow for stateful inspection, which is a stronger method of filtering than just stateful filtering or static filtering. Stateful filtering looks at just the IP header and tracks items like TCP Sequence number, SYN-SYN/ACK-ACK connections, etc. While this is good, it is not as foolproof. Context Based Access Control (CBAC) actually knows the protocol behavior and therefore looks deeper than just the IP header. This allows us to dynamically allow certain response traffic back into the router that it is expecting.

1.2.6.1.2 Protocol specifics for access

Console VTY-Access to this router is only by the local Console port for protection. SSH will be considered in Phase 2.

Syslog (UDP 514) – This router will push its logging into the Syslog server in the DMZ Zone. We will not be setting any NTP access for this router as well. We will keep the local clock synched within 20 seconds with the NTP DMZZone server.

1.2.6.2 Cisco PIX 515UR

```
Cisco IOS SF-PIX-6.3-EAL4 PIX v6.3 Software, EAL4 evaluated, for PIX
Chassis, 433MHz, 64MB, 2 stock + 3 interfaces for 5 total interfaces
```

Best Practice-Use hardened security appliances whenever possible, as this allows for simplicity of administration and minimal patching maintenance

This hardware-based firewall appliance has an internal hardened operating system that can provide for future stateful failover High Availability (HA) functionality. This interests GE for providing resiliency and excellent security to the company's accessible resources. Stateful inspection allows for a packet stream to be compared to a dynamic state table. The PIX series also allows for statefully inspecting packets up to Layer 7 by using configurable fixups. This PIX array also protects the unencrypted buffer zone for VPN traffic coming in from the OUTSIDE ZONE and protects traffic coming from the INSIDEZONE before it is encrypted on its way out of the VPN device.

1.2.6.2.1 Security Function-Second layer of Filtering Protection

This is our second layer of defense behind the filtering perimeter router. This is the workhorse of our security policy. Its role is to function as a traffic cop to only allow PERMITTED traffic, and to block and log all other traffic that may have found its way through the first layer of protection.

1.2.6.2.2 Protocol specifics for access

Web access - HTTPS (TCP 443), HTTP (TCP 80) -allows traffic to and from the web architecture in the DMZ

Email access- SMTP (TCP 25) - Provides for incoming and outgoing mail traffic

Domain name services access- DNS (TCP 53) - DNS will need to be allowed to/from the secondary name server (SOA-Start of Authority) in the DMZ. Our SOA server must be able to connect with the other PRIMARY DNS servers at our ISP.

SYSLOG and alerting– UDP 514 - Syslog messages will be sent only to one server in the DMZ

Telnet (TCP 23) - Telnet from the inside is used to administer, troubleshoot, and check on the Firewall array for proper configuration and new updates.

Network Time Protocol-UDP 123- our PIX requires access to several the NTP in the DMZ for time synchronization.

1.2.6.3 OUTSIDE Zone Hub, with hot spare hub

```
3Com® OfficeConnect® Dual-Speed Hub 8
```

1.2.6.3.1 Security Function-Platform for testing traffic

This hub will function as a connection between the filtering Border router and the PIX firewall array. Why a Hub, you ask? A hub is used here because of its low cost and simplicity[1], as well as it is NIDS-friendly.

[1] A Note about Hubs and Switches- A hub propagates all of the packets it receives to ALL of its ports, regardless if the packet was intended for that port. This is collision domain in Ethernet networks. A switch, on the other hand, is more intelligent in that

A second hub is ready to be rolled in case the first hub becomes inoperable.

1.2.6.3.2 Protocol specifics for access

This hub will allow all traffic, since it operates totally on Layer 2, the MAC layer. Hubs will propagate all traffic to all ports as one collision and broadcast domain, allowing easy traffic capture. We can have the flexibility of plugging in a network based Intrusion detection device as an ad-hoc method of handling incidents or investigating abnormal traffic behavior. We can also easily insert a network packet sniffing device for future auditing and troubleshooting.

1.2.7 Major Components of DEMILITARIZED ZONE (DMZ)

This zone provides the buffer between the untrusted Public zone and the trusted Corporate zone. We call this area semi-trusted, in that actual public traffic reaches most of the hosts in this zone. This zone allows for all flowing traffic to be "converted" via application means. It provides us the ability to more closely investigate those packets that will be "ushered" to only designated resources. Our goal here is to NOT allow any public packets into the corporate zone. One exception is SMTP packets, but they themselves are deconstructed and constructed using CVP (content vectoring protocol) mechanismson the SMTP Gateway.

1.2.7.1 IIS web server /Application server

Microsoft Windows 2003, IIS 6.0, hardened, IISLOCKDOWN,

A single WEB server is proposed for Phase 1 currently. Another web server will join it with identical content to be implemented for Phase 2, which will provide for redundancy.

1.2.7.1.1 Function-Presentation of the company

This server provides the front end content for 3 distinct sites; web customers, suppliers, and partners. They have no personal or private data and any database functionality is accessed in the INSIDE zone. The server is hardened using Microsoft's recommended security configurations for operating system security settings.[2]

The server cannot be accessed by any hosts except the APPSHIELD host, which validates all traffic. The WEB01 host will not initiate traffic to the internet..

1.2.7.1.2 Protocol specifics for access

HTTP (TCP 80) – provides for basic content viewing and web navigation for all sites

HTTPS (443) – for special authentication, HTTPS is used to encrypt all authentication from the internal database as well as uploading and downloading content.

---

it maintains a port to MAC address mapping so that one packet destined for HOST B never sees any packets that HOST A is sending HOST B. A HUB is unmanaged, meaning that you cannot remotely connect to it for configuration, but it does provide easy access for performing network analysis.

[2]http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2003/W2003HG/SGCH08.asp

Database (TCP 1433) – The Web server components access a SQL server database on the Inside zone. No web users are allowed to make direct SQL calls to the database.

Best Practice-Try not to let any other webuser or host to access your Database by locating your database on the other side of a filtering device.

1.2.7.2 Sanctum Appshield Server 4.0 (Web Proxy)

Running on Hardened Windows 2000 server, Service Pack 3

1.2.7.2.1 Function-Web traffic filtering

Hackers have learned that breaching a perimeter is much easier by attacking an application than a firewall, proxy or router. Most web developers are not as well versed on hardening their code as much as their network counterparts.

Best Practice-add some Layer 6/7 filtering in front of your Application web servers in order to complete your security shield on your network. These filters will validate legitimate requests and drop others.

Therefore, we will use Sanctum's Appshield Server to be used to provide strong filtering at the web layer 5-7 by validating all incoming HTTP and HTTPS based SSL traffic to GE's website array. This solution uniquely offers "positive policy" in that it ONLY allows valid requests such as certain parameters in either static websites' forms or dynamic web services, instead of checking requests against an exploit database. Appshield, detects subtle protocol variations, and denies yet-to-be defined exploits often passed by traditional firewalls.

Appshield offers Application layer protection against the following exploits:

Threat	AppShield Protection
Buffer Overflows	Yes
Cookie Poisoning	Yes
Cross-Site Scripting	Yes
Hidden Field Manipulation	Yes
Stealth Commanding	Yes
Parameter Tampering	Yes
Forceful Browsing	Yes
Published Vulnerabilities	Yes
Unpublished Vulnerabilities	Yes
3rd Party Misconfiguration	Yes
SQL Injection	Yes

Cookies, sessions, and buffers are controlled by Appshield. The fact that SSL can be proxied or terminated, along with the scalability of adding SSL hardware based acceleration in the future makes Appshield a near perfect complement to our total OSI protection scheme.

1.2.7.2.2 Protocol specifics for access

HTTP (TCP 80) HTTPS (443) - We will be proxying SSL from the Appshield server itself. This will balance performance with security in that the Web server will not have to process Secure Sockets Layer encryption.

128 bit Encryption is provided via Verisign certificates. Backups for these certificates are located offsite.

MSTERM (TCP3389) We will be administering the DMZ hosts with controlled internal MSTRM.

If an unpermitted request finds it way to our Appshield, this screen will be returned to the user:

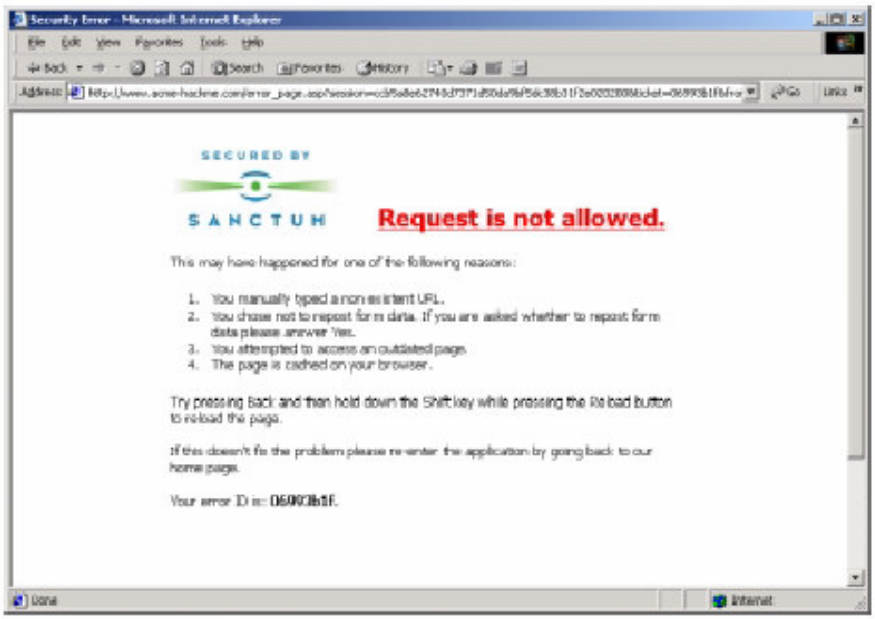


Diagram 1.2—4 Appshield Deny screen for malformed HTTP request

1.2.7.3 Antivirus/SMTP Bastion HOST

McAfee e250 appliance, McAfee WebShield Version 2.5 with HotFix 4

Best Practice- Since most security breaches are a result of email-borne viruses and Trojans using incoming SMTP, you should prioritize your protection by dedicating these functions at one point of the network

1.2.7.3.1 Function-SMTP, SPAM, and content filtering

As most network exploits arrive via email, we agree that we HAVE to protect GE's internal mail resources. A bastion was a wall in medieval days that protected a structure or army. Having a SMTP relay/content filter act as a bastion is almost a necessity in today's world, so we will provide both inbound and outbound SMTP traffic filtering. We also will provide content protection in ensuring that certain content inside SMTP traffic will be filtered out in both directions. UCE (Unsolicited Commercial Email), or SPAM will be checked here as well using DNS-based blackhole list support and user-defined content rules.

SMTP backup-we have asked GE's ISP to provide secondary email queuing, in case this host dies for some reason. This is done by adding a second MX record in the main zone file on the primary and secondary DNS servers. We can dequeue email from this box once it is operational again.

1.2.7.3.2 Protocol specifics for access

SMTP (25) – We will allow all incoming SMTP traffic to this server, provided they are not bounced in the border router's and PIX firewall's ruleset. Once the traffic is examined for viruses and content, it will be forwarded to the corporate firewall. Outgoing traffic is also filtered, but less so, in order to "protect" the Internet from our users.

Best Practice-Always double-check that you are not allowing open relaying on your SMTP hosts out to the internet. Spammers will find you and use your poor server for their shenanigans!!!!

NOTE: OPEN SMTP relaying- we will NOT allow incoming email traffic to be automatically relayed back OUT to the internet via the WebShield appliance. Many administrators forget about locking this relay feature down on their mail servers only to find their sites blacklisted on several public service antispamming sites. We do NOT want to jeopardize GE's reputation by having them publicly blacklisted!

We also have the opportunity to filter out FTP and HTTP with the e250 but we will use other means to protect those.

MSTERM (TCP3389) We will be administering the DMZ hosts with controlled internal MSTRM

1.2.7.4 DNS server

```
Microsoft Windows 2003, hardened, NON-Active Directory
```

A single DNS server will provide two functions, caching for our ISA proxy and domain zone transfer from our ISP for redundancy. This DNS server will not share pluck internal DNS from the AD servers; they will only use this server as a internet lookup source.

DNS (TCP and UDP53) Incoming and outgoing traffic will be allowed, but we restrict zone transfers to only our two SOA servers.

MSTERM (TCP3389) We will be administering the DMZ hosts with controlled internal MSTRM

1.2.7.5 WEBMail server

```
Microsoft Windows 2003, running SENDMAIL 1.1 CGI extensions on IIS6
hardened,
```

This server will receive incoming HTTP and HTTPS requests and proxy mail functions via SMTP and POP3 protocols back to the Exchange server. This allows us to segment our process and allows for domain authentication.

proposed for Phase 1 currently. Another web server will join it with identical content to be implemented for Phase 2, which will provide for redundancy.

HTTP/HTTPS (TCP 80/443) Incoming traffic will be allowed

MSTERM (TCP3389) We will be administering the DMZ hosts with controlled internal MSTRM

1.2.7.6 Microsoft ISA Proxy server

```
Microsoft Windows 2003, hardened, Microsoft ISA Server with Feature
Pack 1, running Trendmicro Webprotect 3.0 and Surfcontrol
```

A single DNS server will provide two functions, caching for our ISA proxy and domain zone transfer from our ISP for redundancy. Outbound Internal users will

interact with the Internet through this filtering and caching server. ISA will provide logging, reporting, and content and antivirus scanning. Trendmicro's Webprotect product will add an extra measure of security in that it will scan on the proxy protocols that you have enabled for your users.

Multiple protocols-outgoing traffic will be allowed, but we restrict incoming nonstate traffic

MSTERM (TCP3389) We will be administering the DMZ hosts with controlled internal MSTRM

1.2.7.7 NTP/SYSLOG server

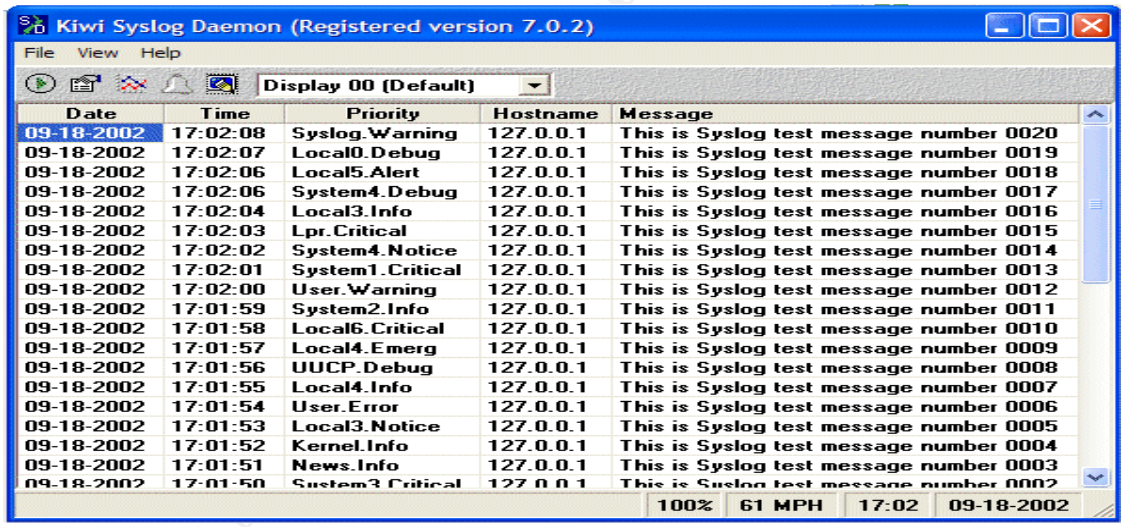
Microsoft Windows 2003, hardened, with NETTIME NTP and KIWI Syslog service

All internal hosts will update and sync their timeclocks with this NETWORK TIME PROTOCOL server. This keeps the enterprise on the same page in the event of an incident. Also Syslog will be used on this server to collect various hosts and devices error and security logs.

UDP 123 –NTP-outgoing traffic will be allowed, but we restrict incoming nonstate traffic

UDP 514-Syslog

MSTERM (TCP3389) We will be administering the DMZ hosts with controlled internal MSTRM



Date	Time	Priority	Hostname	Message
09-18-2002	17:02:08	Syslog.Warning	127.0.0.1	This is Syslog test message number 0020
09-18-2002	17:02:07	Local0.Debug	127.0.0.1	This is Syslog test message number 0019
09-18-2002	17:02:06	Local5.Alert	127.0.0.1	This is Syslog test message number 0018
09-18-2002	17:02:06	System4.Debug	127.0.0.1	This is Syslog test message number 0017
09-18-2002	17:02:04	Local3.Info	127.0.0.1	This is Syslog test message number 0016
09-18-2002	17:02:03	Lpr.Critical	127.0.0.1	This is Syslog test message number 0015
09-18-2002	17:02:02	System4.Notice	127.0.0.1	This is Syslog test message number 0014
09-18-2002	17:02:01	System1.Critical	127.0.0.1	This is Syslog test message number 0013
09-18-2002	17:02:00	User.Warning	127.0.0.1	This is Syslog test message number 0012
09-18-2002	17:01:59	System2.Info	127.0.0.1	This is Syslog test message number 0011
09-18-2002	17:01:58	Local6.Critical	127.0.0.1	This is Syslog test message number 0010
09-18-2002	17:01:57	Local4.Emerg	127.0.0.1	This is Syslog test message number 0009
09-18-2002	17:01:56	UUCP.Debug	127.0.0.1	This is Syslog test message number 0008
09-18-2002	17:01:55	Local4.Info	127.0.0.1	This is Syslog test message number 0007
09-18-2002	17:01:54	User.Error	127.0.0.1	This is Syslog test message number 0006
09-18-2002	17:01:53	Local3.Notice	127.0.0.1	This is Syslog test message number 0005
09-18-2002	17:01:52	Kernel.Info	127.0.0.1	This is Syslog test message number 0004
09-18-2002	17:01:51	News.Info	127.0.0.1	This is Syslog test message number 0003
09-18-2002	17:01:50	System3.Critical	127.0.0.1	This is Syslog test message number 0002

Diagram 1.2—5 Kiwi Syslog Console

1.2.7.8 Network based Intrusion Detection (NIDS) Server

Snort for Windows, Microsoft Windows XP, SP1, Trend Micro OfficeScan 5.5

1.2.7.8.1 Function

Although GE doesn't seem to be all that interested in logging and alerting, we have started educating them on the numerous benefits of keeping and perusing logs. Since Snort is free via Open Source channels, we have included a basic Network based Intrusion detection system that will serve to "ease" the GE staff in learning about their vulnerabilities and hence, dedicate more thought and manpower into creating a more robust logging/alerting scheme for the future.

1.2.8 Components of the VPN Neutral Zone

1.2.8.1 Nortel Contivity 1510 VPN switch

```
Server Software, V02_61.05
```

1.2.8.1.1 Function-Virtual Private Networking

This host will setup up remote client security associations (SAs) which will provide the foundation for encrypting private data and encapsulating it inside a pubic packet. This host will also verify a remote user's identity by pass worded authentication.

1.2.8.1.2 Traffic Flow

Encapsulation Security Payload- Protocol 50-This protocol provides the encryption and the encapsulation features of VPNs. Protocol 51 is also opened for AH, which is Authentication Header, which provides a different function than ESP

ISAKMP- UDP port 500-This protocol provides the key exchange and management functionality of VPNs

1.2.9 Major Components of Inside/CORPORATE ZONE

1.2.9.1 Cisco 2611 router with Firewall feature set

1.2.9.1.1 Function-Internal filtering with CBAC capability

This router will provide the boundary between the INSIDE and CORPORATE zones. Segmenting the network provides some traffic and security benefits. Typically routers will provide a broadcast and collision domain boundary, so this keeps extraneous traffic from accidentally finding its way into the DMZ or internet. This router also is configured with Cisco's CBAC that allows stateful TCP and UDP traffic, as well as provides inward traffic via extended Access Control Lists.

1.2.9.1.2 Traffic Flow

DNS (53) (proxy) – Internal requests for public DNS records will be handled by allowing recursive lookups from our Internal DNS server, housed on one of the Active Directory domain controllers.

HTTP (80)/HTTPS (443) proxy – All HTTP will be focused at the caching PROXY server, which allows us to only allow this device to access the internet

SMTP (25) proxy – This allows e-mail to/from Exchange server and the SMTP bastion host

Database (TCP 1433) – The Web server components access a user database inside the corporate zone. No web users are allowed to make direct SQL calls to the database.

1.2.9.2 Internal Mail Server (Exchange)

```
Microsoft Exchange 2000 with Service Pack(SP) 3, Windows 2000 Server,
SP3, Trend Micro ScanMail for Microsoft Exchange, v6.1
```

This GE domain member server will be the main mail server for the company. It is also protected by ScanMail which will address any viruses that the McAfee e250 appliance misses.

Best Practice-Whenever possible and affordable, use two different vendor's virus signature to maximize your "defense in depth" strategy.

1.2.9.3 Database Servers

Microsoft SQL 2000 database, Microsoft Windows 2000, SP3, Trend Micro ServerProtect 5.5, GE Domain member

This server will sit safely in the INSIDE Zone. Since this is where the data for GE resides, it is considered the "Crown jewels" of the firm. This server should be especially hardened at the OS level and the Database server level.

1.2.9.3.1 Function-Database for the Web applications and Internal data use

We will be performing HTML form authentication for our supplier, user, and partner web sites. These Web servers forward the request information using Database connectity parameters through the internal firewall to the SQL database. SA password is NOT blank or password, but will use a strong password. We are quick to perform both SQL and OS level hardening according to best practices.

Make sure to not forget about hardening your SQL host by using some of the Hardening SQL practices found at:

[3]http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=4&tabid=12

[4]http://www.microsoft.com/downloads/details.aspx?familyid=9552D43B-04EB-4AF9-9E24-6CDE4D933600&displaylang=en

We will make sure to patch the database server for the SQL slammer worm exploit that listens for services running on UDP port 1434!!!

1.2.9.3.2 Traffic Flow

Database connection (1433) – Only the DMZ webserver and select internal hosts can access this server.

1.2.9.4 Internal Network Servers (Active Directory, DNS, DHCP, File and Print, etc)

Microsoft Windows 2000, SP3, GE Domain member, Trend Micro ServerProtect 5.5

We will have two Windows 2000 Domain controllers that will provide our normal network services. The DNS will host a private domain zone, which will NOT be published to outsiders. We will configure both servers to act as forwarders to the DNS server in the DMZ Zone. They will cache these entries for 6 hours. Most internet browsers will rely on the Proxy server to resolve Domain names.

1.2.9.5 Backup Server

Microsoft Windows 2000, SP3, GE Domain member, Trend Micro ServerProtect 5.5, Backup Exec 9.0

3

4

This server will provide the Backup console for the other servers.

NOTE: all servers in the DMZ will be backed up using a static port to this server.

1.2.10 Miscellaneous software

1.2.10.1 Client security software (OfficeScan, Trend Micro)

Each workstation and laptop is protected by antivirus and stateful inspection personal firewall provided by Trend Micro. The personal firewall component protects against Trojan horses, Outlook email client exploits, and backdoor viruses.

1.2.10.2 Network Monitoring software (What's Up Gold)

Having a good baseline for normal traffic patterns and utilization is a good way to be proactive in managing GE's network. We have suggested the affordable WUG software to help them become more familiar with their current network performance. This software can also be used to troubleshoot further issues.

1.2.10.3 GE Computer desktop profile.

GE Client are using Windows 2000 Professional or XP Professional in order to maximize local desktop and laptop security. The client machines have antivirus and personal firewalls in stalled.

1.2.11 Server Management strategies

Management for the hosts in the DMZ will be provided via the administrative console using Microsoft Terminal Services. This is a free service as long as it is used for managing the servers. The Port used for communication will be allowed in the inside 2611 router. No external MS Terminal Services will be allowed from the Internet. If an administrator wants to remotely access the servers in the DMZ, then they will use the VPN to establish that connection.

In hammering to GE the importance of host OS patching we sense some level of frustration with GE's IT staff in the number of patches that are release during each quarter. Therefore we have shared with them the idea to utilize Microsoft's Server Update Services (SUS), which will allow them to perform HOTFIX/Patch management more easily. This may be included in the project's Phase 2.

1.2.12 Planning for Phase 2 check

In Phase 2 we will move to provide further host based Intrusion Detection and redundancy of routers between the DMZ ZONE and the CORPORATE ZONE. We will provide another Cisco 2611 router in a HSRP (Hot Standby Router Protocol) array. We will provide a Security Roadmap to Cheng Fu and his team once we complete Phase 1. This will allow them to plan and budget for the next phase.

Assignment 2 -Implementing Security Policy

2.1 Introduction

We will look at the security policies of each of the GE's defense layers, from the outside in. We will share some configuration tips along the way for:

- **Perimeter router**
- **PIX Firewall Gateway**
- **VPN**

We will also provide a tutorial on the Cisco PIX.

2.2 Border Router-Filtering the NOISE

This device is our first line of defense against the wild environment of the internet. Its role is to provide an armored entry point into our GE landscape and to simply evaluate incoming traffic and drop specific unwanted traffic and filter out undesirable specific sources.

Hardening this router against would-be attackers is an important first step. The second step is to FILTER out and block certain addresses and protocol exploits. This eliminates "noise" and keeps the inner layers free from having to process this useless and possibly dangerous traffic. Another benefit of filtering here is that it will proportionately improve the performance of our main firewall waiting just inside the next layer.

The only drawback for explicit filtering is that it could prove more challenging to troubleshoot access issues for legitimate traffic, so we must be careful about being too "gung ho" on applying the security policy at this layer.

Filtering is accomplished in routers using Access Control Lists, or ACLs.

2.2.1 ACLs Primer

ACLs add powerful control to a router. While there are many types of ACLs that can be used, we will cover only the fundamentals of standard and extended ACLs. Cisco provides some excellent primers on ACLs[5].

Standard ACLs are simplest and therefore less taxing on a router, as they will check more basic components of an IP header, such as source address and basic inverse masking. Extended ACLs provide more IP header coverage in that they can validate an IP packet's source and destination address, along with protocols, flags, and port numbers. The benefits that Extended ACLs offer in flexibility is a tradeoff, in that will

5 http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml#info

they require more router resources. Reflexive and Context-based Access Control Lists provide even more session state validation of a packet, but they also carry the cost of chomping more router resources than standard or extended ACLs. There is a tradeoff of ACL usage and Router performance.

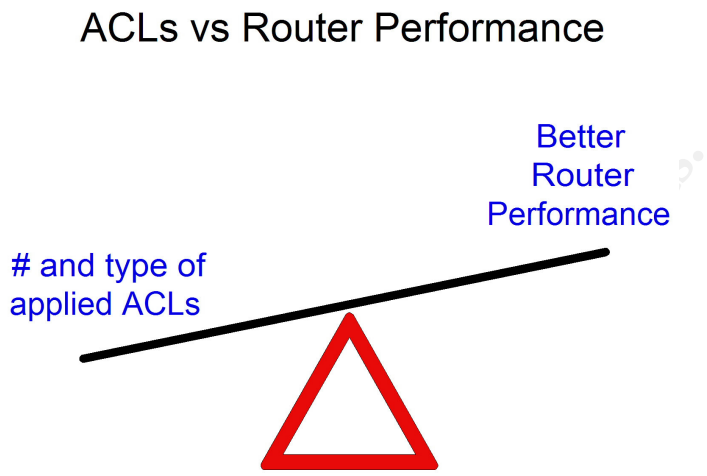


Diagram 2.2—1 Balancing ACLs with Router performance

There are two steps to utilizing ACLs:

- **1. Craft your ACL**
- **2. Apply your ACL to the router's specific interface, with a direction, IN or OUT**

2.2.1.1 Golden rules of ACLs:

- **Only one ACL per Interface, per direction**
- **A packet always is processed from top to bottom, one line at a time**
- **Once a match occurs, processing stops, and the packet is Denied or Permitted.**
- **Anything that is not explicitly permitted is denied (implicit deny)**
- **You must have a least 1 PERMIT statement in your ACL or all traffic will be blocked**
- **ACLs are created in Global configuration mode but remember to use the same number for your `access-list` and `access-group` commands**
- **Remember that the last implied rule for an ACL is "DENY any any", so use a "PERMIT any any" as the last line for your incoming traffic on your Border router!**

2.2.2 Border Router Configuration

We will document the general hardening of the router as well as the filtering access control lists (ACLs) in the following pages.

There are two ways to implement better security at the Cisco router at this internet barrier:

1. **Global configuration-**provides the hardening of the router applied to the ROUTER itself

2. **ACLs-**provide the ruleset FOR INTERFACES that will apply to the TRAFFIC that will filter out the unwanted packets from undesirable sources

Global configuration settings are simple to apply, but you must carefully consider your ACLs, such as which interface, which traffic direction, and the order of the rules.

1. Line entries while in Global Configuration of Router	
`Hostname GEborder`	This names the router
`Logging 99.200.200.10`	This sets up logging to our Syslog server which NATs to 192.168.0.10
`Logging trap debug`	Limits the number of messages logged to the terminal lines
`logging console critical`	This logs level2 LOG_CRIT To the console
`enable secret 5 <removed>`	This defines the password as encrypted for privileged Exec mode, using level 5
`No enable password`	This removes any unencrypted password
`service password-encryption`	Turns on the service enabling PW encryption
`clock time central -7 0`	Set time zone of clock , Pacific time
`clock set 14:16:00 28 may 2003`	Set clock and date
`ip tcp selective-ack`	Increases performance by sending TCP sender ACKs for selective packets

`banner motd ^CC`
`WARNING!!!!!!!!!!!`
`This is a private system operated for`
`and by GE Enterprises Network Personnel ONLY.`
 	
`Use by unauthorized persons is prohibited!!!!`
`Contact Networkteam@yourcompany.com for further questions.`
`^C`
	Provides a legal warning signs to unauthorized users trying to break into the router. While this sounds trivial, I have heard that this was used in a court of law to show the burden of proof for trespassing.

`no ip source-route`	Turn off all the ability to control which router a packet may traverse
`no ip finger`	We will politely turn off finger service RFC 742, as that opens reconnaissance opportunities

no ip bootp server	Turn off bootp service, don't need
No ip http server	Turn off Web service daemon, as this has been known to have some denial of service vulnerabilities
no ip domain-lookup	Tells router not to try to lookup domain names
no cdp run	While CDP is great for troubleshooting, it offers hackers the ability to recon your topology. We will turn off Cisco Discovery protocol
no service udp-small-servers no service tcp-small-servers	These are UNNEEDED, so let's disable them!
no ntp master	This tells the router to NOT act as a NTP master clock server
no snmp-server	This turns off SNMP messaging until we want to implement this at GE, Syslog should be sufficient for now
2. Line Entries for Configuring External and Internal Interfaces (Config Interface-Mode)	
No ip directed-broadcast	This turns off broadcasts directed to a host
no ip proxy-arp	We should turn off proxying of arps for hosts, it is not needed
no ip unreachables	Turns off response traffic for unreachable IPs, as this will give hackers more info than we want them to have about our topology
No cdp enable	This is turned off in global configuration, but lets be extra careful and apply it on each interface (see above)
No ip redirects	This prevents resending ICMP redirects back out the same interface
3. DEFINE THE ACLs for the External interface IN, using Global Configuration mode- ORDER is Important!	**<LOG> WILL SEND TO OUR SYSLOG SERVER>** **<log-input> also adds the MAC ADDRESS**
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log access-list 101 deny ip 172.16.0.0 0.15.255.255 any log access-list 101 deny ip 10.0.0.0 0.255.255.255 any log	Block all incoming Private RFC1918 addresses. These would be ANTIspoofing measures.
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log access-list 101 deny ip 255.0.0.0 0.255.255.255 any log	Block all incoming localhost & broadcast traffic
access-list 101 deny ip host 0.0.0.0 any log	Block any incoming IP unnumbered
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log	Block any APIPA addresses, which is the

	Automatic Private IP Addressing implemented in many Microsoft operating systems
`access-list 101 deny ip 224.0.0.0 15.255.255.255 any log`	Blocks multicast traffic, the 15 in the inverse mask means "skip" 4 right most bits in the first octet, so summing the remaining 4 bits on the left is 224d, or 11110000b. Remember, 0=match, 1=any
`access-list 101 deny ip host 99.200.300.1 any log`	Block external interface of our border router, which should NOT be sending to itself!!!
`access-list 101 permit ip any 99.200.200.0 0.0.0.255`	This last rule allows all other traffic to the public GE net. Logging is optional, but we can do that at the Firewall
4. DEFINE the ACLs for Internal interface IN (Internet bound traffic) using Global Configuration mode - - ORDER is Important!	**<LOG WILL SEND TO OUR SYSLOG SERVER> <log-input> adds the MAC ADDRESS OF**

`access-list 102 deny ip 192.168.0.0 0.0.255.255 any log`
`access-list 102 deny ip 172.16.0.0 0.15.255.255 any log`
`access-list 102 deny ip 10.0.0.0 0.255.255.255 any log`
	Block any RFC1918 addresses, as these should have been NAT-ed at the Firewall

`access-list 102 deny ip any any 137 log`
`access-list 102 deny ip any any 138 log`
`access-list 102 deny ip any any 139 log`
`access-list 102 deny ip any any 445 log`
	Block MS ports, as we don't want any traffic sharing our domain or computernames to outsiders

`access-list 102 deny icmp any any log`	Do not let ANY ICMP out of our network-Be careful with this one!
`access-list 102 permit ip 99.200.200.0 0.0.0.255 any`	We will allow packets from our public netblock range and NATted traffic
`access-list 102 deny ip any any log`	Block all other traffic

Rob Thomas has put together an excellent template for locking down border routers, as referenced below.[6]

[6] http://www.cymru.com/Documents/secure-ios-template.html

Here are a couple of good references in relation to configuring ACLs:
Global config and ACLs
From:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tip1r/p1ftip2.htm#1019682

http://www.cisco.com/cgi-bin/Support/Cmdlookup/ios-command-lookup.pl?type=reference&query=&paging=25&counter=0&sa=Submit

http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-07/0039.html

http://www.pasadena.net/cisco/secure.html

Cisco golden rules about ACLs
From: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/scacls.htm#12853

2.2.3 APPLYING THE Access Control List (ACL)

After defining the ACLs for the filtering router we need to APPLY those ACLS to the proper Interfaces. Typically we want to **apply the ACLs on the interface that is closest to the source of the traffic**. Look at the diagram below.

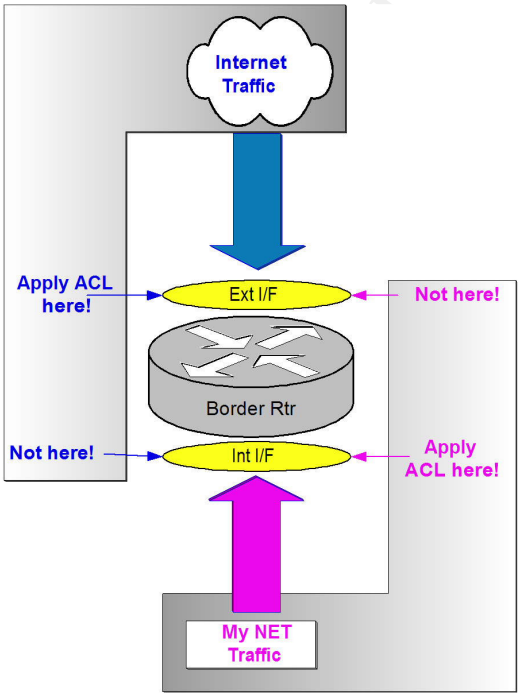


Diagram 2.2—2 Applying ACLS

Best Practice- on Router Interfaces and direction-apply ACLs on the interface receiving your watched traffic. Think FILTER IN. This will conserve your router's processor and memory utilization. The same is true with filtering outbound traffic from private IP addresses at the internal interface. (i.e. -We don't want to send out packets with RFC 1918 addresses as their source or destination)

5. APPLYING THE ACLS	
Now we want to apply the Access lists to the interfaces, for Traffic flowing IN	Using Interface Config mode

`interface ethernet0/1`
`ip address 99.200.200.1 255.255.255.0`
`ip access-group 102 in`
	Applying ACL to Internal interface

`interface serial0/1`
`ip address 99.200.300.1 255.255.255.0`
`ip access-group 101 in`
	Applying ACL to External interface

2.2.4 A quick check of our Ruleset

Before applying our ACLS we should use a tool such as Router audit tool to determine if there are any glaring issues with our ruleset. This tool will download a config or load a config, evaluate it, and create a HTML report on whether that Entry in the ACL is good or unacceptable.

Another test we can perform is to open up a browser and see if we can connect out through the border router.

2.2.5 Configuring existing ACLs

There are a couple of things to note about ACLs on a Cisco router:

NOTE: If you should need to add another criteria statement (a rule), it will be APPENDED to the end of the access list statements. However sad this has been in Cisco's rule of rulesets, some newer IOS's are allowing line by line deletes, adds, and modifications, without having to reload the whole ACL.

Otherwise, you will need to use a text editor like NOTEPAD to copy, edit, and paste your current ACL so you can re-apply it to your Interface.

Here is a good formula when editing your ACL rules:

1. Copy/Create the properly ordered ACL in NOTEPAD.
2. Enter your router's configuration mode for your interface
3. DELETE that existing ACL (this ensures accuracy)

```
router#configure terminal

      Enter configuration commands, one per line.  End with CNTL/Z.

      router(config)#no access-list 101 deny icmp any any
```

4. Paste your newly edited access list to the console
5. Test your ACL!
6. Save your changes to be persistent once you are confident!

```
router#copy run start
```

2.3 CISCO PIX Firewall Configuration

The border router is our first layer defense. Our second layer is the PIX firewall and provides most of the perimeter security as it examines each and every packet that traverses its interfaces.

2.3.1 Hardware or Software based Firewalls?

There have been many newsgroups "discussions" about using an appliance-based or software-based firewall for the BEST perimeter protection. There is some confusion as to what "software" actually entails. Usually it means that the software code is run on a hardened operating system on a server or a chassis platform.

Remember that the firewall code has to run from a software image somewhere.

Appliance-based will load firewall code from a diskette, disk drive, or EPROM (erasable Programmable Read Only Memory). This is the software for appliances.

Software-based firewalls usually run on a hardened UNIX kernel set, hardened NT/Windows 200x, or a proprietary embedded version of either. Embedded operating systems are those that are "componentized" to run only the software modules and drivers that are needed. It is important to keep the underlying Operating System patched on Software firewalls, which can be a drawback.

Examples of Appliance-based firewalls are NETSCREEN and Cisco PIX-sometimes these platforms use ASICs, which offload processing load from the processor and allow for better performance.

Examples of Software-based firewalls are Symantec Raptor, Checkpoint Firewall-1, and Microsoft ISA Server.

2.3.2 Types of Firewalls

There are several types of firewalls, described briefly with benefits and disadvantages below:

1. **Packet Filtering firewall- This** router-based firewall simply and quickly filters out the first 4 layers (envelopes) of the Packet, that is, layers of the Open Systems Interconnect Model (OSI). This method has proven very high performance, uses ACLs to filter certain traffic that does not fit a policy, and offers very primitive session state adherence. The disadvantage of this firewall is that it, according to Cisco, "is not foolproof, and that companies must consider additional options and should augment router security with a standalone firewall" (Cisco PIX – Stateful Inspection Whitepaper[7])

2. **Proxy based Firewall-**To provide for better security, Proxy firewalls act as a client's network ambassador will check every single layer of the packet, and its goal in life is to parse the highest Application layer, to ensure compliance with its rule set. The proxy firewall will then pass the accepted packet in a stream. Proxy firewalls will break down a packet and reconstruct it for a client's request. Thus, this Firewall is very secure, but demands that more configuration effort take place both at the firewall service and the client.

[7] Pix Firewall and stateful Firewall security, Cisco Systems, http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

Another drawback of this firewall is that it requires heavy CPU utilization in order to deconstruct, inspect, and construct each packet.

3. Stateful Filtering Firewall-The stateful filter firewall will go a step further than packet filtering. This firewall will look above the Layer 4, say TCP port 80, and will utilize a special session flow table to verify the destination, source IP address, TCP sequence number, TCP flags, IP header, etc. This type of security filtering provides much better performance than proxy firewalls. NOTE: that this type of firewall does NOT inspect the packet's payload

4. Stateful Inspection Firewalls- This type of firewall is a hybrid of the above, in that it protected more of the packet flow. These firewalls are not panaceas[8], however, because they only protect a few of the most common protocols like HTTP, FTP, etc. For any protocol they do NOT provide a stateful application proxy, they revert to stateful filtering. .Still, these firewalls provide common hacking countermeasures, such as IP spoofing, SYN Flood attacks, Denial of Service, SMTP, and ActiveX and Javascript filtering.

What is stateful inspection? Stateful inspection is the process by which packets are tracked in a stream session, where the firewall looks deeper into the IP packet than just the 20 byte header. This allows more protection for data streams. Even the connectionless UDP can be tracked for certain types of protocols. Stateful Inspection is PER Protocol, not Per Firewall; hence a firewall may provide stateful inspection with a TCP protocol SMTP, but not with HTTP.

The following is a chart the outlines what each type of firewall provides:

Examines:	Static	Stateful	Stateful Inspection	
	Filtering			
Packets:	Individually	In a session	In a session	
IP address	Yes	Yes	Yes	**IP Header**
Protocol	Yes	Yes, basic	Yes, session	
Port	Yes	Yes	Yes	
Sequence #	No	Yes	Yes	
Flags (i.e. syn)	No	Yes	Yes	
Uses State table	No	Yes	Yes	
Payload of packet/content	No	No	Yes	
Mechanism	ACLs	Reflexive lists	As Proxy or Inspect, protocol specific	
Examples	Cisco routers w/o firewall feature set	broadband SOHO routers	PIX, CkPt FW1, and Cisco FW Routers	

[8] Track 2-Firewalls 101: Perimeter Protection with Firewalls, SANS Institute, Module 3, page 94, 2002.

2.3.3 Tutorial of PIX setup for GIAC Enterprises

We have chosen the PIX because of its simplicity, Stateful inspection, and scalability. We will also be able to add another PIX in a Failover (FO) configuration in Phase 2 if we should need.

Cisco first introduced the PIX in 1994 and it is considered one of the top firewalls available on the enterprise market. Cisco includes it in its SAFE architecture. It offers true NAT via Request for Comment (RFC) 1631.

PIX is a Stateful inspection firewall, as it offers Stateful Inspection of traversing packets, which is a step up in security from Stateful filtering(see chart). The PIX has no moving parts such as hard drives, is appliance-based, and sports an embedded Operating System, which means that its kernel is loaded from firmware and runs in flash memory.

The PIX uses Adaptive Security Algorithm (ASA) to inspect each packet for common protocols. This is what is implemented as "FIXUPs" in the PIX's config. Each FIXUP inspects the contents of the packet and matches it with a state table. If it is a malformed packet, or it does not match in sequence number, payload or header with the contents in the state table, the packet is dropped.

NOTE-PIX reverts to Stateful filtering if the allowed protocol does not match an available FIXUP.

Those familiar with Cisco IOS commands are happy to know that PIX contains similar IOS-like command similar to that of routers. In recent versions, Cisco has replaced the CONDUIT functionality with Access Control Lists (ACLs), which are easier to follow the rule base logic.

2.3.3.1 Step 1 – Diagram your Perimeter and Security Policy

Looking at our security policy and diagram outlined in Assignment 2, we can create a foundation for setting up our firewall. With the diagram in hand, we begin to configure the 4 port PIX 515E, Unrestricted (allowing for future FO, more scalability).

2.3.3.2 Step 2 – Go to Global Configuration mode and NAME the Firewall

This tutorial expects the reader to have some familiarity with Cisco commands. To go to Global config mode, we must connect a laptop to the console port with COM1, 9600 baud, 8 data bits, No parity, stop bits to 1. Wit this we get a prompt similar to:

```
Firewall>
```

This is unprivileged mode for the PIX. Now we type in the command:

```
Firewall> enable

Firewall#
```

Now we are in privileged mode, which allows us to look the firewall. You can use the

```
Firewall#write term
```

to reveal the Default configuration that the PIX ships with. The default config runs all of the FIXUPs, sets translation table parameters, allows telnet and timeout, but offers NO ACLs, NAT, or other unique configurations.

To start our configuration, we should move into configuration mode by typing in the following:

```
Firewall#Config terminal
```

which allows us to begin our configuring. We name our firewall PIX1 by using the following syntax:

```
Firewall(config)#hostname PIX1
PIX1(config)#
```

Now our PIX is creatively named!

2.3.3.3 Step 3 – Set the user and enable passwords for the Firewall

```
PIX1(config)#passwd user password
PIX1(config)#enable password privileged_password_here
```

The first command sets the PIX user login that can be used with telnet. The second command above sets the privileged mode for global configuration.

2.3.3.4 Step 4 – Name the Interfaces and set Security levels for the Firewall

The PIX starts out with default Ethernet names such as ethernet0, ethernet2, ethernetx, and so on. Naming the interfaces requires 2 things:

Set the name of the security zone

Set the numeric value of "trustiness", where 0 is low security, 99 is high security

```
PIX1(config)#nameif ethernet0 outsidezone sec0
PIX1(config)#nameif ethernet1 dmzzone sec20
PIX1(config)#nameif ethernet2 vpnzone sec50
PIX1(config)#nameif ethernet3 insidezone sec100
```

We want to set the security settings with distinct numbers from 1-99 since the PIX will not pass traffic across similar value security settings. Best practices tell us to use even based security zone numbers.

PIX Golden Rule: By default, PIX will always pass from a higher security level to a lower level, but not the opposite. ACLs are required for passing traffic to more secure zones.

2.3.3.5 Step 5 – Configure each Interface's speed, duplex, and MTU

Configuring the interfaces requires setting the speed, duplex and maximum transmission unit (MTU) for each interface. We use the `interface` command to set the interfaces to 100 mbps and full duplex, as leaving these to `auto` has been known to cause some issues with switch mismatching:

```
PIX1(config)#interface ethernet0 100full
```

```
PIX1(config)#interface ethernet2 100full
PIX1(config)#interface ethernet3 100full
PIX1(config)#interface ethernet4 100full
```

Now we will ensure we have 1500 bytes MTU for each interface, which sets the largest size window with which to send and receive Ethernet frames.

```
PIX1(config)#mtu outsidezone 1500
PIX1(config)#mtu dmzzone 1500
PIX1(config)#mtu vpnzone 1500
PIX1(config)#mtu insidezone 1500
```

2.3.3.6 Step 6 – Configure each Interface with IP address

Here is where we will set up the actual IP address and subnet on each interface. The syntax is:

IP address interface_name ip_address subnet_mask

We will configure each named interface.

```
PIX1(config)#ip address outsidezone 99.200.200.3 255.255.255.0
PIX1(config)#ip address dmzzone 192.168.0.1 255.255.255.0
PIX1(config)#ip address vpnzone 10.2.0.1 255.255.0.0
PIX1(config)#ip address insidezone 10.3.0.1 255.255.0.0
```

Now is would be wise to write this to memory permanently using the following:

```
PIX1(config)#write mem
```

This concludes the basic configuration of our PIX. Next we move to the more advanced features of the firewall with how it handles Network address translation, packet flow, and processes the rulebase.

2.3.3.7

2.3.3.8 Step 7 – Configure the Global IP Pools and NAT IDs tags for the OUTSIDEZONE

In order for our PIX to keep our internal addresses "secret" we must tell it to translate our Private IP RFC1918 addressing into publicly available addresses. The PIX must translate the source and destination addresses in each packet's IP header to communicate with only publicly available addresses. This translation is called NAT-ting (or Network Address Translation).

In order for NAT to work on a PIX, we must first map inside networks to Public IP pool(s). These pools are ranges of addresses that are useable for inside hosts. A pool of two or more `addresses` requires a NAT ID tag, starting at 1 and up. A NAT ID tag of 0 designates that NAT should NOT be used, for example using public addresses in the DMZzone as well as the public. We will be using NAT for all internal private IP addresses.

Before we assign any NAT pools, let us review the types of NAT:

2.3.3.8.1 3 Types of NAT

Static NAT-is one for one address translation, such as an internal SMTP server with an internal 192.168.0.3 IP address gets translated to outside 99.200.200.3 address. This requires one address for each internal protected host. Uses a "pool" of one external address.

Global NAT-Where multiple internal hosts dynamically use a pool of one or more external addresses in a many to many translation. This requires enough external addresses for internal host mappings. The disadvantage of this NAT method is consumption of external addresses which can be costly

HIDE NAT or PAT-Where multiple hosts all "gang up" and use ONE external IP address in a many to one translation. The firewall keeps track of each session by means of different TCP and UDP port numbers and connections. Also known as PAT (Port Address translation) this is commonly used as it allows for much better utilization of public addresses, i.e., you can have nearly unlimited number of hosts (up to 65535) access the outside via one external IP address.

NO NAT-Although this is not really NAT, it should be considered for meeting some networks' needs. There is NO translations for this type of topology, and this can be used in situations that require public addresses to be used in the DMZ, for example. Cisco uses a NAT ID tag of 0 for this very method.

2.3.3.8.2 NAT strategy

Static NAT is necessary if GE wants to host any publicly available services, so we need to define the one for one static NAT. We will also need to address how to NAT all of the internal employees accessing the internet via the ISA proxy. We could use Global NAT, but we choose HIDE NAT since it will conserve the amount of external addresses we will have to lease from our ISP, which is currently a whole class C address space of 254 addresses.

Using NAT gives us some semblance of security by obscurity in that it hides the internal addressing schemes used by clients sending packets out through the firewall.

2.3.3.8.3 Defining GE's Global Address Pools and Static "Pools"

We will use several static NAT entries and one PAT Global definition to allow outgoing access from inside. Static NATs provide for incoming requests from the internet, whereas Global NATs usually provide for the outgoing requests.

Static NAT-Since we are not allowing any dynamic connections directly from the inside or other zones, we have chosen to define multiple static NATs for the firewall from the DMZzone. NOTE: Static Pool translations are persistent!

NO NAT-We will not be utilizing network translation between the VPNZONE, DMZZONE, and the INSIDEZONE.

Global Pool with PAT-since we currently are not allowing any internal hosts internet access except for explicit servers, we will NOT use these kinds of NAT (except for

the Proxy server, which will use a one to one Hide NAT). All internet traffic from the employees will proceed to and from the ISA Proxy server and we will allow this proxy access to all external access. The future, though, may demand that a VIP user will demand total access, and in that case, we will need to allow that host out. This presents some issues, in that we must place a static IP address on that client's host in order for the rule to continue to allow her through, and also remember that each individual Hide NAT will require an additional rule or ACL. We want to keep the rulebase as simple as possible. NOTE: Global Pool translations are configurable by timeout period.

2.3.3.8.4 Cisco PIX Global IP Pools and NAT: Two peas in a Pod

Global pools and NAT statements are always used together where we need to allow traffic from HIGH security to LOW security zones. **CAN ACLS be used?** The PIX allows this by default because it assumes that the HIGH security zone is trusted. Whenever a TCP SYN request goes out to the internet, the PIX checks the packet's contents against the state table. Since there will not be an entry for the packet (or session) the PIX checks the ACL for outgoing traffic, if there is one. After the PIX finds the match in the ruleset for outgoing traffic, it will place this information in its session state table so when the corresponding SYN/ACK comes back in, the PIX will allow the returning packet provided the sequence numbers and IP addresses are matching in the state table. NO ACLS are checked for this session's traffic stream, because the State Table is checked before the ACL ruleset.

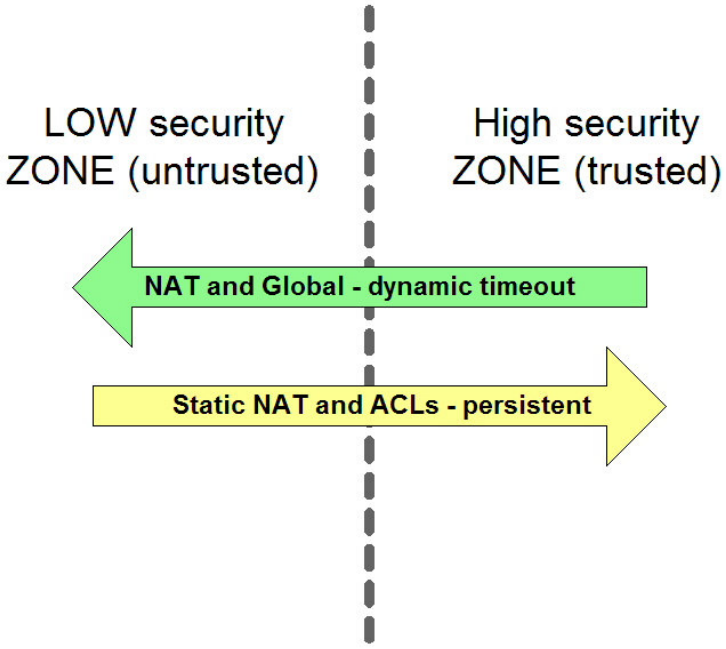


Diagram 2.3—1 NAT and Security Zones

Golden Rules:

Global pools and NAT statements are always used together from Trusted to Untrusted zones and are dynamic

Static NAT pools are usually used with ACLs from Untrusted to Trusted zones and are persistent.

2.3.3.8.5 Configuring GE's Global NAT and the "pool" for ISA server

First we will define the external Global IP address "pool" to use for our ISA server. This "pool" is an address of ONE, 99.200.200.11, because we are proxying internal internet requests out to the internet on behalf of the GE employees using that single address. We should also understand that Cisco states that when using PAT, we must provide a reverse lookup DNS entry for those IP addresses. The syntax for a global pool is:

Global (interface_name) NAT_ID PUBLIC_IP_range netmask mask

where the public ip range is a contiguous range of public addresses.

The corresponding NAT statement syntax is:

Nat (interface_name) NAT_ID inside_network_to_be_natted mask

Now we will begin configuring the PIX for GE. We will use the NAT ID of 1.

```
PIX1(config)#global (outsidezone) 1 99.200.200.11 netmask 255.255.255.0
```

The statement above says, "Reserve an outside Public IP address of 99.200.200.11 and assign it a NAT ID tag of 1." Remembering that global NATs always are used with NAT statements, we need to assign an inside network to that NAT ID.

The next line assigns the inside DMZ address of 192.168.0.11 for the ISA Server to the NAT ID of 1:

```
PIX1(config)#nat (dmzzone) 1 192.168.0.11 255.255.255.255
```

Notice that the netmask above is for 255.255.255.255. This designates that only the ISA server can be translated for communicating outside. The global pool and its linked "nat" statements are used to connect the external IP address(es) with the internal IP address(es). This is what we want because we don't want users directly accessing the internet!

At this point you might wonder why we set up a PAT Global Pool NAT instead of a Static NAT. This is mainly for two reasons. One, we want to allow only initiating traffic OUT to the outsidezone from ISA and our internal internet clients, and the second reason is that static NAT translation tables are persistent, whereas Global translation tables are timed out as defined by the following line in the PIX config:

```
Timeout xlate 1:00:00  <for 1 hour>
```

Golden rule: You can assign multiple interfaces and subnets to a NAT ID tag.

NOTE: The statements immediately below are theoretical and are not part of the PIX config for GE.

In the future if we wanted to set up more than one external address in our Global pool, like 50 public IPs, we could use the following:

```
PIX1(config)#global (outsidezone) 2 99.200.200.50-99.200.200.100 netmask
255.255.255.0
```

And we would use the corresponding NAT statement using a NAT ID tag of 2:

```
PIX1(config)#nat (insidezone) 2 10.0.0.0 255.0.0.0
```

The statement above would cover address translation for all of the inside addresses, or if we wanted to be more selective by subnet we could use the following statement instead:

```
PIX1(config)#nat (insidezone) 2 10.1.0.0 255.255.0.0
```

This statement would assign the NAT ID tag of 2 to only the hosts from the 10.1.0.0 subnet.

2.3.3.9 Step 8- Configure the STATIC NAT

Now we move to allowing outside access to our protected DMZ servers by setting up the static NAT for the DMZzone. Just as Global Pools are linked with NAT statements, static "pools" are linked to ACLs. We will discuss ACLS last, as they are the foundation of our rulebase.

We will use the external addresses to create our static NAT. In the PIX global configuration mode we enter the static entries for the DMZ servers to be allowed access outside. The syntax for static NAT is following:

Static `(int_if_name,ext_if_name) public_IP private_IP netmask` **mask** 0 0

Where:

`int_if_name` is the more trusted interface name where traffic headed

`ext_if_name` is the less trusted interface name from where traffic is coming.

`public_IP` is your registered public IP address

`private_IP is` your private RFC 1918 IP address

`mask` is the subnet mask, usually 255.255.255.255 to designate the host

`0` designates maximum incoming connections which can connect

`0` designates NUMBER of "half open" connections (EMBRYONIC LIMIT), 0 is unlimited

NOTE: Static NAT does not use the Global NAT ID tags

Golden rule: as a memorial to an ancient Egyptian king, Static Pool NAT statements can be remembered with this syntax:

```
Static (trusted, untrusted) untrusted trusted9
```

Or

```
Static (T, U) U T  <TUT, get it?>
```

1. First we set up our **WEBMAIL server** that uses the SENDMAIL CGI product. It uses Port 80 and Port 443 for outside access and POP3 and SMTP to Exchange for internal access(to be discussed later)

```
PIX1(config)#static (dmzzone,outsidezone) 99.200.200.7 192.168.0.7 netmask
255.255.255.255 0 0
```

The command above says, "whenever an inbound packet hits the PIX for the address `99.200.200.7` convert it to `192.168.0.7` on the other side." The 255.255.255.255 designates that ONLY that host is translated.

Next we will set up Static NAT for our SMTP bastion host from the DMZzone:

```
PIX1(config)#static (dmzzone,outsidezone) 99.200.200.8 192.168.0.8 netmask
255.255.255.255 0 0
```

3. Now we set up Static NAT for our DNS host from the DMZzone:

```
PIX1(config)#static (dmzzone,outsidezone) 99.200.200.9 192.168.0.9 netmask
255.255.255.255 0 0
```

4. Next we will set up Static NAT for our **Syslog**/**NTP server** from the DMZzone:

```
PIX1(config)#static   (dmzzone,outsidezone)   99.200.200.10   192.168.0.10
netmask 255.255.255.255 2 2
```

We only need 2 incoming and half open connections so we use 2 2 as the syntax above.

5. Finally we will set up Static NAT for the **Appshield host** from the DMZzone. Remember that this host will reverse proxy HTTP/HTTPS requests to the Webhost using a positive policy for only the criteria that it expects. All other web traffic is dropped by Appshield. Each website has a distinct IP address, and there is a corresponding IP address for the AppShield server that proxies requests for each GE web site:

```
PIX1(config)#static   (dmzzone,outsidezone)   99.200.200.20   192.168.0.20
netmask 255.255.255.255 0 0
PIX1(config)#static   (dmzzone,outsidezone)   99.200.200.21   192.168.0.21
netmask 255.255.255.255 0 0
PIX1(config)#static   (dmzzone,outsidezone)   99.200.200.22   192.168.0.22
netmask 255.255.255.255 0 0
```

[9] Steve Textor, April 29, 2002, The Installation and configuration of a Cisco PIX Firewall with 3 Interfaces and a Stateful Failover Link, http://www.sans.org/rr/firewall/cisco_pix.php

Note that we only define the IP addresses that correspond to the Appshield server. It handles the proxying of request to the IIS web host on unpublished IPs on the WEB Host which are not permitted to send packets out to the outsidezone. Here is the logical flow for the Appshield/Web Host pair.

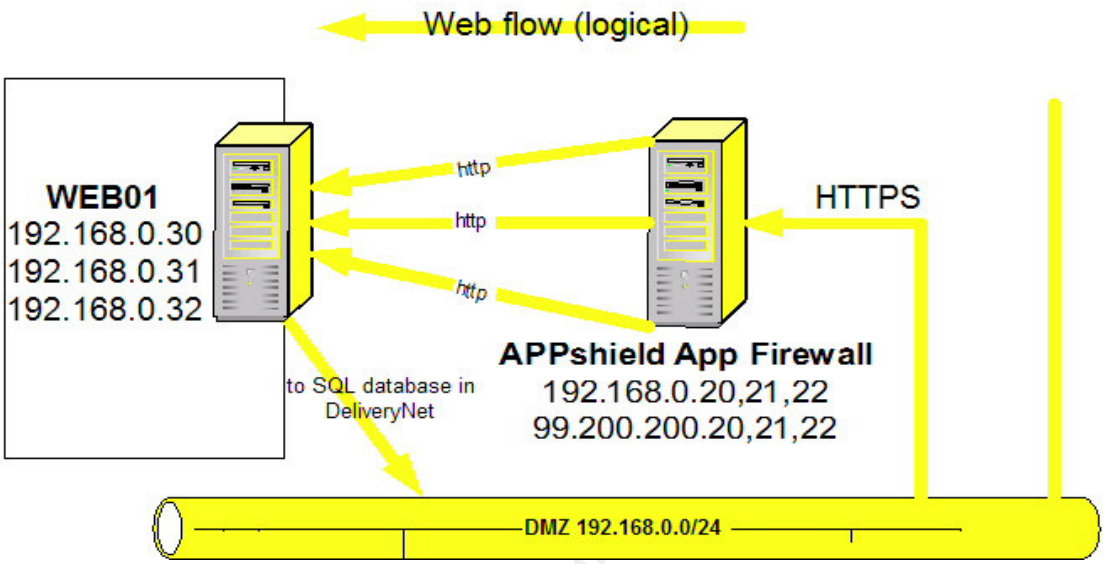


Diagram 2.3—2 Application flow of GEFORTUNES.COM

This should be all of the static NAT entries for the (Insidezone, DMZzone). Now we must consider interzone traffic flow.

2.3.3.10 Step 9- Configure Traffic flow with NO-NAT statements

Although we do NOT need to provide address translation between our insidezone, DMZzone, and VPNzone, we do need to define these "NO-NAT translations so that two way traffic can flow in the first place. We will apply ACLs to restrict access later.

2.3.3.10.1 Insidezone to DMZzone, Insidezone to VPNzone

Firstly we will define the translation between the DMZZONE and INSIDEZONE by using persistent static NATs with the following:

```
PIX1(config)#static (insidezone,dmzzone) 10.3.0.0 10.3.0.0 netmask
255.255.0.0 0 0
PIX1(config)#static (insidezone,dmzzone) 10.1.0.0 10.1.0.0 netmask
255.255.0.0 0 0
```

Note that we need to incorporate all of the 10.x.x.x subnets in the No-NAT statements. This statement allows for inside hosts to access the DMZ.

Now we need to define the translation between the VPNzone and Insidezone by using persistent static NATs because we want to allow all traffic out to the VPN "cloud".

```
PIX1(config)#static (insidezone,vpnzone) 10.3.0.0 10.3.0.0 netmask
255.255.0.0 0 0
```

```
PIX1(config)#static (insidezone,vpnzone) 10.1.0.0 10.1.0.0 netmask
255.255.0.0 0 0
```

This diagram depicts outgoing traffic patterns for which the NO-NAT provides:

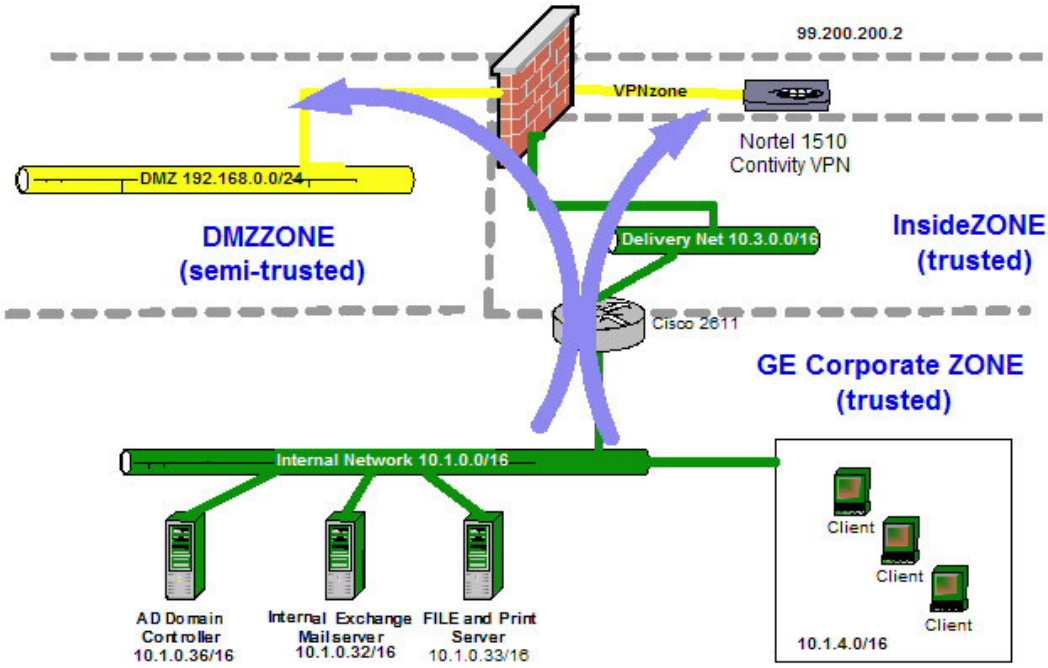


Diagram 2.3—3 NO NAT into DMZ and VPN ZONES

Now would be a good time to save our work to the startup configuration. Perform a write memory with the following:

```
PIX1(config)#write mem
```

2.3.3.11 Step 10- Set up Fixups and ACLs for all traffic flow

Now that we have all of the NAT/host/subnet translations defined, it is time to lock down our traffic flows. We do this by using Fixups and ACLs together.

2.3.3.11.1 Fixups- Application proxies that scan a packet's payload

We first need to enable the particular FIXUP protocols (or applications) for which the PIX will perform stateful inspection. These fixups are similar to application proxies in that they actually look into the payload of a packet to check for embedded IP addressing that particular protocols like FTP passive mode uses. This requires a much deeper level of inspection, thus providing a greater level of protection.

The ASA component of the PIX performs this application inspection. Cisco has an excellent explanation of how ASA works, and has described in the following paragraph[10]. Cisco states:

"ASA uses three databases for its basic operation:

[10] Cisco, http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb727.html#1064072

- Access control lists (ACLs)—Used for authentication and authorization of connections based on specific networks, hosts, and services (TCP/UDP port numbers).
- Inspections—Contains a static, pre-defined set of application-level inspection functions.
- Connections (XLATE and CONN tables)—Maintains state and other information about each established connection. This information is used by ASA and cut-through proxy to efficiently forward traffic within established sessions."

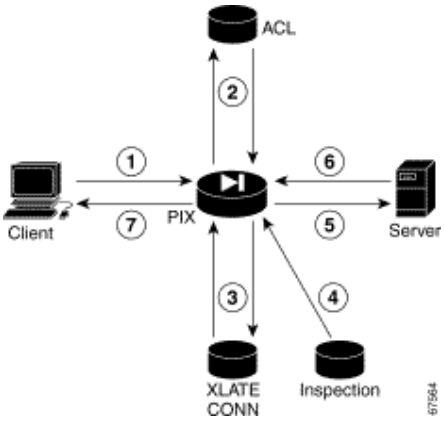


Diagram 2.3—4 PIX Packet flow Internal Databases, from Cisco.com

Cisco also states (from the same previous reference) the traffic flow that is used with ASA:

"1. A TCP SYN packet arrives at the PIX Firewall to establish a new connection.

2. The PIX Firewall checks the access control list (ACL) database to determine if the connection is permitted.

3. The PIX Firewall creates a new entry in the connection database (XLATE and CONN tables).

4. The PIX Firewall checks the Inspections database to determine if the connection requires application-level inspection.

5. After the application inspection function completes any required operations for the packet, the PIX Firewall forwards the packet to the destination system.

6. The destination system responds to the initial request.

7. T he PIX Firewall receives the reply packet, looks up the connection in the connection database, and forwards the packet because it belongs to an established session."

Since the PIX comes with several default fixups, I suggest that you use a NO FIXUP PROTOCOL to disable all of the unneeded applications that you know you won't be using. For GE's network, here are the fixups we will include in the configuration:

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol ftp 443
fixup protocol dns  53

fixup protocol ils 389
fixup protocol icmp error

! PIX's Mail guard
fixup protocol smtp 25
```

A note about some of the Fixups:

The Mail guard feature will restrict mail servers from receiving the seven minimal commands defined in RFC 821, section 4.5.1 (HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT). All other commands are rejected.

The HTTP fixup can be used in conjunction to filter out java and activeX components with the commands, **filter activex** *port local_ip mask foreign_ip mask* and **filter java** port[-port] *local_ip mask foreign_ip mask,* respectively.

2.3.3.11.2 ACLs-the traffic cop for the PIX interfaces

We can control traffic by implementing ACLs in a ruleset. PIX ACLs work very much the same way as Cisco router ACLs. One important point to remember if Access from a more trusted network is translated properly to a lesser trusted network, the PIX will allow the traffic IF THERE IS NO ACCESS LISTS applied for that traffic.

It is considered a Best Practice that all outgoing traffic (from More trusted to less trusted) should be explicitly restricted. This helps to protect against unintentional broadcasting private network information and inadvertent Trojan horses that may pop through to our private subnets.

Golden Rule-by Default, higher secure trusted zones can access lower secure zones.

Golden rule-Each interface supports ONE inbound (IN) ACL, so for 4 interfaces we should have 4 ACLs

Golden Rule- like Cisco routers, PIXes have a implicit deny at the end of their ACLs.

Like Cisco routers, ACLs are implemented in two steps(mentioned earlier):

1. Configure the ACLs

2. Apply the ACLs IN to the interface nearest the traffic source(PIX can only have ACLs applied to the inward direction relative to the PIX.

2.3.3.11.3 ACL entries for INSIDEZONE named "from_inside"

Looking at the diagram above we see the traffic flow that is needed for internal users. There should be no direct traffic from the Insidezone to the Outsidezone according to our policy. We define our ACL from INSIDEZONE as from_inside:

Allow only Exchange to SMTP bastion host in DMZ:

```
PIX1(config)#access-list from_inside permit tcp host 10.1.0.32 host 192.168.0.8 eq 25
```

Here we allow Inside web clients to ISA proxy, as we will deny access by IP address on the ISA server when we observe some internet abusers inside. Also we can lock down each protocol on the ISA server.

```
PIX1(config)#access-list from_inside permit ip 10.0.0.0 255.0.0.0 host 192.168.0.11 any
```

Allow MSTERM Svr to access the DMZ for management:

```
PIX1(config)#access-list from_inside permit tcp host 10.3.0.37 192.168.0.0 255.255.255.0 eq 3389
```

Allow only Active Directory Primary DNS server in INSIDEzone to perform recursive lookups to DMZ DNS HOST. All other internal users will use the AD DNS for resolution.

```
PIX1(config)#access-list from_inside permit tcp host 10.3.0.35 host 192.168.0.9 eq 53
PIX1(config)#access-list from_inside permit udp host 10.3.0.35 host 192.168.0.9 eq 53
```

Allow INSIDEzone management of VPN clients in VPNZone

```
PIX1(config)#access-list from_inside permit ip 10.0.0.0 255.0.0.0 10.2.0.0 255.255.0.0 any
```

PIX Object-lists allow admins to summarize multiple entities under one name. Here we create object-lists to include the group IPs for the Webteam and the IPs for the WEBservers (WEBSVCS), so it will be easy to configure a single ACL for each.

```
PIX1(config)# object-group network webservers
      PIX1(config-network)#network-object host 192.168.0.20
      PIX1(config-network)#network-object host 192.168.0.21
      PIX1(config-network)#network-object host 192.168.0.22
      PIX1(config-network)#network-object host 192.168.0.30
      PIX1(config-network)#network-object host 192.168.0.31
      PIX1(config-network)#network-object host 192.168.0.32
      PIX1(config-network)#exit
PIX1(config)#
PIX1(config)# object-group network webteam
      PIX1(config-network)#network-object 10.1.2.0 255.255.255.0
      PIX1(config-network)#exit
```

Now we create object-list for the service websvcs group allowing TCP80 and 443

```
PIX1(config)# object-group service websvcs tcp
      PIX1(config-service)#port-object eq www
      PIX1(config-service)#port-object eq ftp
      PIX1(config-service)#port-object eq 443
      PIX1(config-service)#exit
```

Now we can allow the Webteam on insidezone to access the web services DMZ for management.

```
PIX1(config)#access-list from_inside permit TCP object-group webteam object-group webservers
       object-group websvcs
```

We will allow NTP requests to our NTP server in the DMZzone.

```
PIX1(config)#access-list from_inside permit UDP 10.0.0.0 255.0.0.0 host 192.168.0.10 eq 123
```

To be extra cautious, we will now restrict all other access to the DMZzone. Since the ACLs are processed top to bottom, most of our allowed traffic to the DMZ has already been forwarded. This rule confirms no other access to the DMZzone:

```
PIX1(config)#access-list from_inside deny ip 10.0.0.0 255.0.0.0 192.168.0.0 255.255.0.0 any
log-input
```

Now we place a final explicit deny for all other traffic from the insidezone, even if spoofing is attempted:

```
PIX1(config)#access-list from_inside deny ip any any log-input
```

2.3.3.11.4 ACL entries for DMZzone named "from_dmz"

Now we are ready to configure the PIX with a NEW from_dmz ACL to allow initiating traffic to access the Outsidezone.

The servers needing to initiate traffic are:

- **the Webserver**
- **the NTP server**
- **the SMTP bastion host**
- **the ISA server proxy**
- **the DNS server**
- **the Webmail server**

These servers have been set up with static NAT and each will have an entry. Here we allow access for each by placing the most used entries first, which would the traffic of our WEB server, SMTP host, and ISA server:

WEBserver-Allow only the WEB01 server to access the MS SQL server from the DMZzone. Note that the webserver itself is allowed to access the SQL database, and no other host, including the AppShield application firewall. If the Appshield host was compromised, there is no way for outsiders to access the WEB servers.

```
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.30  host 10.3.0.34 eq 1433
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.31  host 10.3.0.34 eq 1433
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.32  host 10.3.0.34 eq 1433
PIX1(config)#access-list from_dmz deny ip any  host 10.3.0.34 eq 1433
```

This Last line protects our SQL server from the DMZZone.

SMTP Bastion-This allows for the SMTP host to communicate outside to other SMTP servers, to Exchange and allow MX record lookups for performance reasons, and lastly to McAfee for AV signature auto updates

```
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.8  host 10.1.0.32  any eq 25
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.8  any eq 25

PIX1(config)#access-list from_dmz permit tcp host 192.168.0.8  any eq 53
PIX1(config)#access-list from_dmz permit udp host 192.168.0.8  any eq 53
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.8  host ftp.nai.com eq 21
```

ISA PROXY-We allow all outbound access for our AV protected PROXY server, denying smtp and other protected services on the proxy as we see fit.

```
PIX1(config)#access-list from_dmz permit ip host 192.168.0.11 any any
```

DNS-Allow our SOA DNS host to access first using TCP 53 and then UDP 53 if unsuccessful. Since our Start of Authority is at our ISP, we will only allow traffic to the two SOA hosts there. Zone transfers to our DNS secondary server will be allowed only from those servers from the outside

```
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.9  host 99.200.201.2 eq 53
PIX1(config)#access-list from_dmz permit udp host 192.168.0.9  host 99.200.201.2 eq 53
```

WEBMAIL-Allow the SENDMAIL Web-based mail host to initiate connection to our Exchange server using POP3 for outside users

```
PIX1(config)#access-list from_dmz permit tcp host 192.168.0.7  host 10.1.0.32 eq 110
```

NTP-After following netiquette by emailing permission to use a timemaster's NTP servers, we set up one NTP server will allow all of our critical systems to have the same timestamp in the case of an incident. Open access NTP servers can be found at http://www.eecis.udel.edu/~mills/ntp/clock1a.html. We find a NTP server close to GE's point of presence in the San Francisco Bay area.

```
PIX1(config)#access-list from_dmz permit udp host 192.168.0.10  host 192.6.38.127 eq 123
PIX1(config)#access-list from_dmz permit udp host 192.168.0.10  host 128.9.176.30 eq 123
```

Next we explicitly deny all other access from the DMZzone, remembering that there is an implicit deny all with each ACL applied

```
PIX1(config)#access-list from_dmz deny ip 192.168.0.0 255.255.0.0 10.0.0.0 255.0.0.0 any log-input
PIX1(config)#access-list from_dmz deny ip any any log-input
```

2.3.3.11.5 ACL entries for VPNzone named "from_vpn"

All users using ISAKMP and IPSEC will have their Security Associations (SAs) established at the Nortel Contivity VPN gateway. All traffic currently is from remote access VPN clients, and they use a dynamic pool of 10.2.0.0/16. This allows the clients to appear as though they are directly on the VPNZone. Currently we are

allowing all access for these VPN clients, but GE may decide to open up satellite offices and/or partners using site to site VPNs. At that time we can create more restricted ACL entries. First we begin by allowing access from this less trusted security zone to the Insidezone. We are NOT allowing the VPN users to access the DMZzone from the VPN. If they would like to do that, they will need to terminate the VPN, since we do not allow split tunnelling.

```
PIX1(config)#access-list from_vpn permit ip 10.2.0.0 255.255.0.0 10.0.0.0 255.0.0.0 any
PIX1(config)#access-list from_vpn deny ip 10.2.0.0 255.255.0.0 192.168.0.0 255.255.0.0 any log-input
PIX1(config)#access-list from_vpn deny ip any any log-input
```

2.3.3.11.6 ACL entries for Outsidezone named "from_outside"

Lastly we define the entries for external access to our DMZ hosts, using the static NAT public addresses. Again we place the order for the most used entries at the top to maximize performance, but first we will block any spoofing RFC 1918 packets that the border router might have allowed.

```
PIX1(config)#access-list from_outside deny ip 192.168.0.0 255.255.0.0 any
PIX1(config)#access-list from_outside deny ip 172.16.0.0 255.240.0.0 any
PIX1(config)#access-list from_outside deny ip 10.0.0.0 255.0.0.0 any
```

AppShield- Allowing everywhere access to the GE web service, we notice that there is no access directly to the webserver, which is a good thing

```
PIX1(config)#access-list from_outside permit tcp any  99.200.200.20 255.255.255.0 80
PIX1(config)#access-list from_outside permit tcp any  99.200.200.21 255.255.255.0 80
PIX1(config)#access-list from_outside permit tcp any  99.200.200.22 255.255.255.0 80
PIX1(config)#access-list from_outside permit tcp any  99.200.200.20 255.255.255.0 443
PIX1(config)#access-list from_outside permit tcp any  99.200.200.21 255.255.255.0 443
PIX1(config)#access-list from_outside permit tcp any  99.200.200.22 255.255.255.0 443
```

SMTP-We must allow all SMTP servers to send mail to our Mail Bastion host and on to our Exchange. This allows no direct connection to the insidezone from the outside.

```
PIX1(config)#access-list from_outside permit tcp any 99.200.200.8 255.255.255.0 25
```

DNS-We are using the DMZ DNS server as a third SOA in case the first two Internet servers go down, so we must allow all to access our DNS server

```
PIX1(config)#access-list from_outside permit tcp any  99.200.200.9 255.255.255.0 53
PIX1(config)#access-list from_outside permit udp any  99.200.200.9 255.255.255.0 53
```

Webmail-This entry allows us to allow any access to the Sendmail web mail host using HTTPS. All traffic from the internet is sent via TCP port 80 and 443.

```
PIX1(config)#access-list from_outside permit tcp any  99.200.200.7 255.255.255.0 www
```

```
PIX1(config)#access-list from_outside permit tcp any  99.200.200.7 255.255.255.0 443
```

Syslog- This allows for Syslog messages from the border router, and only the outside router, using a non-standard UDP port for Syslog (normally UDP 514). We ensure that we have configured the Syslog host in the DMZ with the non-standard port of 1050.

```
PIX1(config)#access-list from_outside permit udp host 99.200.200.1 host
99.200.200.10 1050
```

Deny all other traffic and log it. The first entry will alert us to a possible physical breach of our network, since only authorized personnel can access our switch, router, and PIX. The other is the final deny all entry.

```
PIX1(config)#access-list from_outside deny ip any 99.200.200.0 255.255.255.0 any log-input
PIX1(config)#access-list from_outside deny ip any any log-input
```

2.3.3.12 Step 11- Apply the ACLs to the Interfaces

Now comes the final part, as we apply the ACL IN to each interface. Our naming convention allows us to easily perform this task.

```
PIX1(config)#access-group from_inside IN insidezone
PIX1(config)#access-group from_vpn IN vpnzone
PIX1(config)#access-group from_dmz IN dmzzone
PIX1(config)#access-group from_outside IN outsidezone
```

Finally, let us save our work, and reboot the firewall:

```
PIX1(config)#write mem
PIX1(config)#reload
```

2.3.3.13 Step 12- Set up static routes on the PIX

The PIX will need static routes for all networks that are not directly connected to it, as well as the all important default static route. First we will set up the default route, which should point out to the Border router's Ethernet interface

```
PIX1(config)#route outsidezone 0 0 99.200.200.1 1
```

This tells the PIX that "for any packet that you don't know where to route, if it gets this far, then send it to 99.200.200.1 which is one hop away"

The other route we need is for the Corporate zone behind the enterprise router.

```
PIX1(config)#route insidezone 10.1.0.0 255.255.0.0 10.3.0.2 1
```

This tells the PIX that any traffic bound for any host on the 10.1.0.0 network send it over to the Enterprise router

2.3.3.14 Step 13- Final PIX settings for Production and RELOAD

Here are the final miscellaneous settings that can are to be performed.

We will need to configure the PIX to allow incoming telnet sessions from our MSTERMsvr for this operation. The statement below says, "only allow telnet sessions to the PIX from the MSTermsvr." This allows an admin to remote VPN and look at the PIX.

```
PIX1(config)#telnet host 10.3.0.37 255.255.255.255 inside
```

Even though protection against flooding with uauths is enabled, we expressly enable this feature to reclaim TCP user resources.

```
PIX1(config)#floodguard enable
```

Enable and configure NTP

```
PIX1(config)#ntp authentication-key 1234 md5 ********
PIX1(config)#ntp authenticate
PIX1(config)#ntp trusted-key 1234
PIX1(config)#ntp server 192.168.0.10 key 1234 source dmzzone prefer
```

These lines tell the PIX to use a NTP server to adjust its clock using a message digest 5 authentication password. Our PIX will accept connections from the NTP server in the dmzzone.

Logging

```
PIX1(config)#Logging on
PIX1(config)#Logging host 192.168.0.10 udp 1050
PIX1(config)#Logging buffered
PIX1(config)#Logging timestamp
PIX1(config)#No logging console
PIX1(config)#No snmp
```

The lines above set up syslogging to the Syslog host using nonstandard port UDP 1050, as well as turns off snmp.

Final step:

```
PIX1(config)#write mem
PIX1(config)#reload
```

2.3.4 Testing the configuration

Now we will perform some perfunctory testing of our PIX to see if we can be proud of our work and show our client. We can use several tests to and from each zone.

Test 1-Testing Internet access from Insidezone

We fire up our Internet Explorer, configure the web proxy setting to point to our ISA proxy at 192.168.0.11, and hit google.com in the address bar. The friendly font letters greet us after a few seconds. We close out, and create a session to the MSTermsvr with the Terminal Services client, log in, and open its IE browser and hit the same URL, and it instantly brings up the Google page, but more quickly this time.

This verifies that the ISA server is caching content, and our rules from the inside segments, to the DMZ, and out to the internet are working correctly.

Test 2- Testing Web access from outside and VPN access-

To test this, we dial up using a laptop to hit our MSN ISP from the our laptop modem using PPP. After the long delay of connecting a 36600, we now are connected to the internet. We first ping our Web servers at 99.200.200.20 and get no response. Scratching our heads, we forgot that we denied any ICMP from the external interface of our border router. Now we enter the IP in the IE browser and get our GE home page. This is good.

After shutting down the IE browser, we fire up the Contivity VPN Extranet client, log in with our username and password. After the successful connection we open up Outlook to read mail. After 30 seconds, we see mail in our inbox. We send a mail to ours Yahoo account and close outlook out. The mail was sent apparently. Now we pull up the IE browser to check Yahoo email but find that our browser is timing out. What is it? OK, we remember that we have NOT allowed split tunneling on the VPN device and that we are blocking all access from the VPNzone to the outside.

Test 3- Test scan of our DMZ using Superscan 3.0

Since we know our public class C address, we run Superscan and find that only ports 80, 443, 53, and 25 are open to just a few of the hosts. We are pleased with the results and look forward to start looking at the Syslog logs on the Syslog host for other interesting traffic.

2.4 VPN Configuration

Now that we have configured the PIX and border router, it is time to visit the VPN device, which will be a Nortel Contivity Model 1510. The Contivity line is a very robust product line and my experience has shown them to be easy to configure and administer.

2.4.1 Types of VPNs

Typically there are two major types of VPNs:

- **Site to site VPNs**
- **Remote VPNs**

A VPN device can satisfy both types of VPNs above. Cisco, for example allows VPNs to and from their Access routers, PIX firewalls, and VPN concentrators. Typically a VPN device acts like a VPN Gateway device for both ephemeral remote users and persistent site to site connections. Almost all firewall vendors, including Microsoft's ISA server, offer VPN capabilities with their firewalls. Some of these vendors include Netscreen, Checkpoint, Watchguard, and Cisco. Nortel excels in the VPN dedicated appliance platform. An article I wrote on the different types of Cisco VPN access methods can be found at

http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci854037,00.html

VPNs work by "tunneling" one IP packet inside of another packet, and running an integrity algorithm, encrypting the contents, and providing authentication. The tunneling aspect is depicted below, where a VPN user is attached to the public internet with a public IP address. The VPN software will then use this network configuration to send a IKE (Internet Key Exchange) packet of UDP 500 to the PUBLIC IP address of the VPN device. Once the client provides the correct authentication, keys are set up and managed via ISAKMP/Oakley/IKE that will provide the foundation for the encapsulation(ESP-Encapsulating Security Payload), encryption(ESP), and validating integrity in that VPN session(ESP or AH – Authentication Header). Notice the blue Public IP packet which carries the encrypted contents of the red packet. When that packet exits out the other side of the VPN device, all we will see is the red packet!

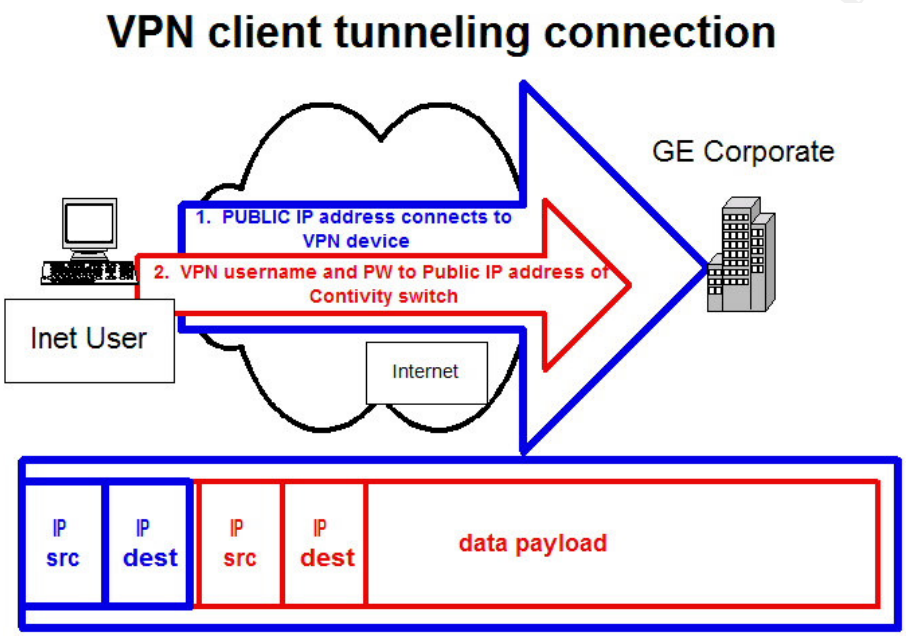


Diagram 2.4—1 VPN tunneling

The following example, from Oration's website[11], is a the sequence of UDP packets that initiate a VPN connection with a Nortel Contivity (CES). The first 6 packets show how the client and VPN device negotiate using a common key management method using UDP 500, then initiate the actual VPN encrypted IP-based protocol 50 ESP connection using a MD5 with 56-bit encryption.

Frame	Direction	Protocol(src,dest)	Length
1	CLIENT->CES	UDP(500,500)	264
2	CES->CLIENT	UDP(500,500)	240
3	CLIENT->CES	UDP(500,500)	60
4	CES->CLIENT	UDP(500,500)	340
5	CLIENT->CES	UDP(500,500)	292
6	CES->CLIENT	UDP(500,500)	60
7	CLIENT->CES	IP(Protocol 50/No Port)	144
8	CES->CLIENT	IP(Protocol 50/No Port)	152

2.4.2 VPN Definitions

2.4.2.1 What is IPSEC?

The IP Security (IPsec) is actually a suite of protocols the does several things. The IETF has a working group just for IPSEC protocols and technologies, found at http://www.ietf.org/html.charters/ipsec-charter.html

The (IPsec) standard defines a set of security protocols that:

- Authenticate incoming IP connections.
- Add data secrecy and integrity to IP packets.
- Are transparent to applications and the underlying network infrastructure.

2.4.2.2 Key Management-

This allows for 2 peers to quickly and dynamically agree on compatible security and connection parameters (shared keys, encryption, and authentication). Renamed IKE (Internet Key Exchange) from ISAKMP/Oakley (Internet Security Association Key

[11] http://www.oration.com/nortel-bay/ces-faq.shtml#Q5,

Management Protocol) because, according to security group chair Robert Moskowitz, "ISAKMP/Oakley resolution is a mouthful." [12]

IKE uses the Diffie-Hellman algorithm to exchange the keys.

2.4.2.3 ESP-Encapsulating Security Payload

This provides integrity, authentication, replay protection, and data confidentiality (in that it encrypts everything in the packet that follows the header).

2.4.2.4 AH- Authentication Header

This provides authentication, integrity, and replay protection (but not confidentiality). Its key difference with ESP is that AH also authenticates the entire packet, including parts of the IP header of the packet. AH does NOT perform encryption.

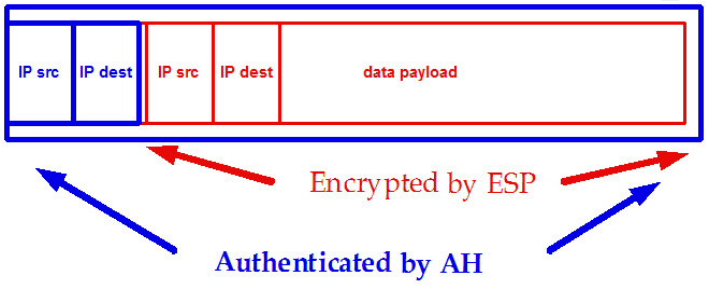


Diagram 2.4—2 AH and EXP Packet details

2.4.2.5 IPSEC Tunnel Mode vs. Transport Mode-

Transport mode is used by a host that is generating the packets that can attach directly to the other host, without a gateway in between them.

Tunnel mode is used when one of the ends of the VPN connection is connected to a VPN gateway of some sort. This applies to most remote client or site to site VPNs.[13]

Security Associations (SA)-a security association for a VPN client is a one way data pipe to a Gateway that is matched with another SA from the Gateway back to it. This pair is given a Security Parameter Index (SPI) upon initiation that uniquely identifies that pair with certain security settings like key and policy information.

2.4.3 IPSEC policy requirements

In order to create IPSEC tunnels, two modes are used during the IKE process.

The first mode is for Key Exchange, where the following can be used to negotiate an SA pair.

The following are what is required for 1st Phase[14]: The encryption algorithm: DES, 3DES, 40bitDES, or none.

1. The integrity algorithm: MD5 or SHA.
2. The authentication method: Public Key Certificate, preshared key, or Kerberos V5 (the Windows 2000 default).

12 Robert Moskowitz, from http://sunsite.uakom.sk/sunworldonline/swol-06-1998/swol-06-ipsec.html
[13] SANS Day 4, Track2, VPNs, Book 2.4, p.88
[14] Taken loosely from Windows 2000 Server online help, Microsoft Corporation.

3. The Diffie-Hellman group. ISAKMP uses the DH algorithm to share keys…

The second mode is for refreshing the keys for the SAs before they expire. This needs to be automatic.

The following are what is required for 2nd Phase:[15]

1. The IPSec protocol: AH, ESP.
2. The integrity algorithm: MD5, SHA.
3. The encryption algorithm: DES, 3DES, 40bitDES, or none.

2.4.4 Defined IPSEC policy for GE

We will choose the following IPSEC components that will make up the Security Policy for the VPN device at GE.

GE IPSEC POLICY

1st Phase:

1. The encryption algorithm: 3DES
2. The integrity algorithm: SHA-1.
3. The authentication method: preshared key
4. The Diffie-Hellman group. ISAKMP uses the DH algorithm to share keys…

2nd Phase

4. The IPSec protocol: AH, ESP.
5. The integrity algorithm: SHA-1
6. The encryption algorithm: 3DES

2.4.5 Nortel Contivity Components

We won't go into the details on what it takes to configure the Contivity, but we should address some key components of VPN devices.

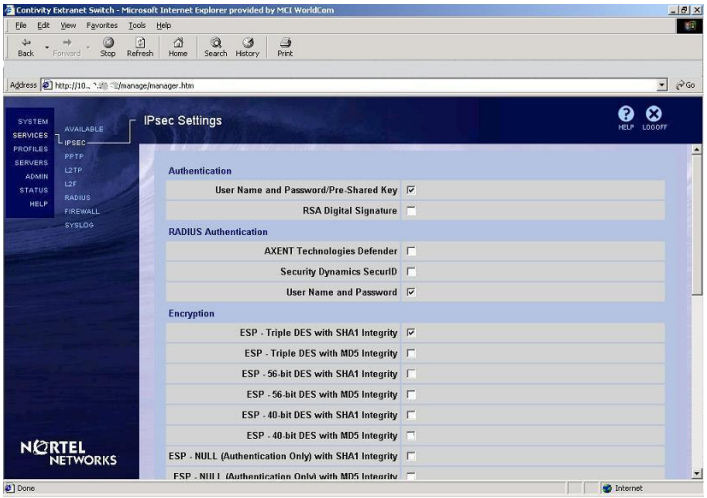
2.4.5.1 Settings for the Contivity

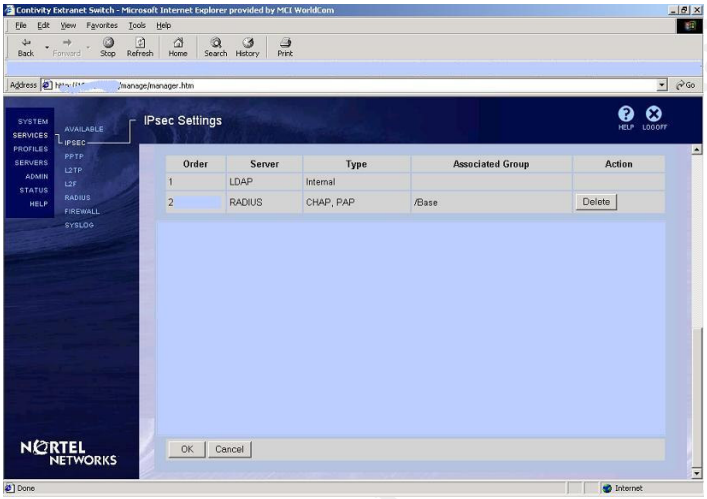
Here are some of the more important VPN settings for the Contivity. There is Contivity capability to filter each Individual user or group profile by source and destination IP address; port, service, and protocol type, however we have chosen to give all remote users full access to our network just like they are directly attached. Note that we are currently NOT using a firewall, as this model was coupled with the choice to have Checkpoint's Firewall-1 product, but our buyer did not purchase it. We will be restricting VPN users from the PIX firewall anyway.

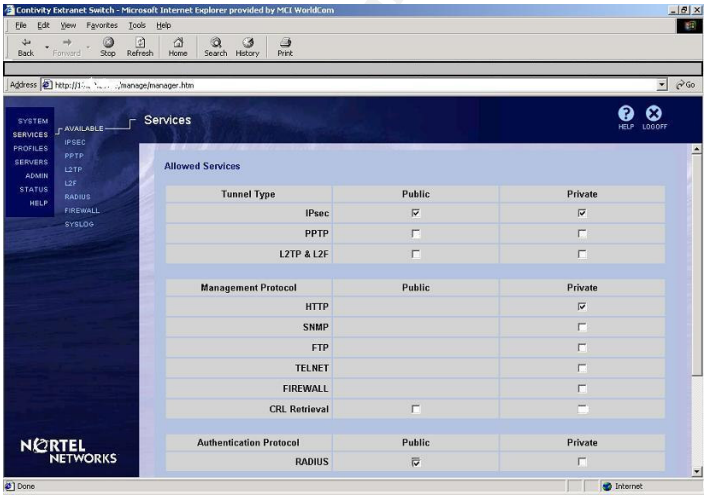
2.4.5.2 IPSEC settings

We have set up the IPSEC settings as the following screenshots display, with using a Pre-shared key and username/PW, and have matched our IPSEC policy above.

[15] Taken loosely from Windows 2000 Server online help, Microsoft Corporation.

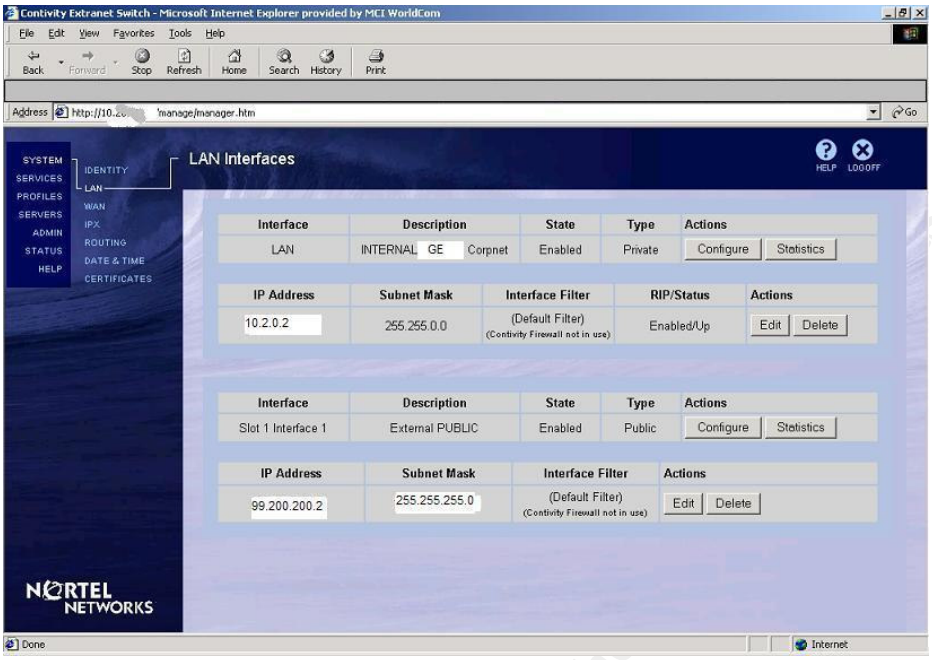






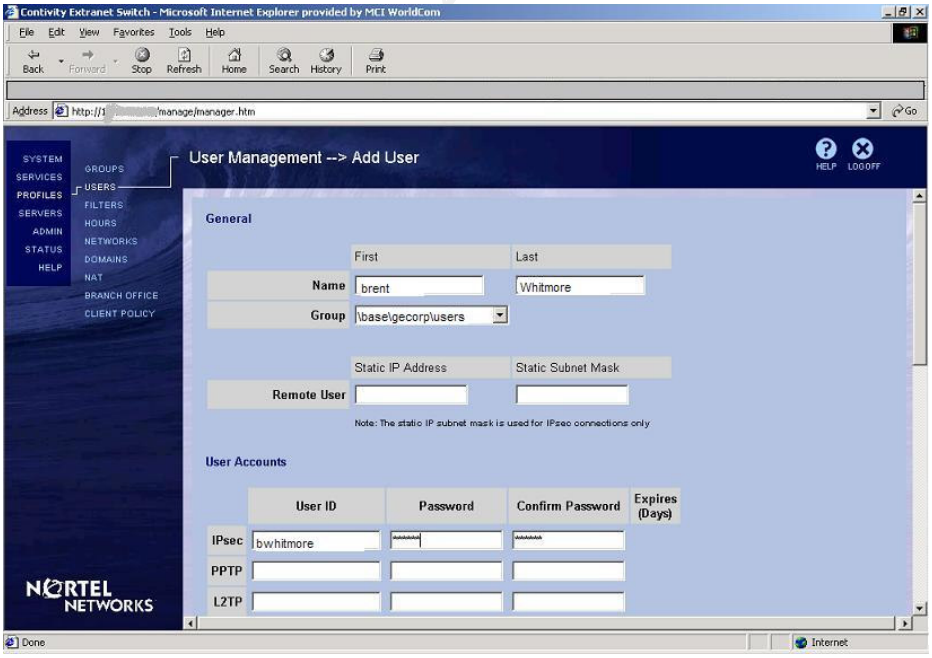
2.4.5.3 Setting the Interfaces of the Contivity

The other important element to configure on the Contivity is the Interfaces.

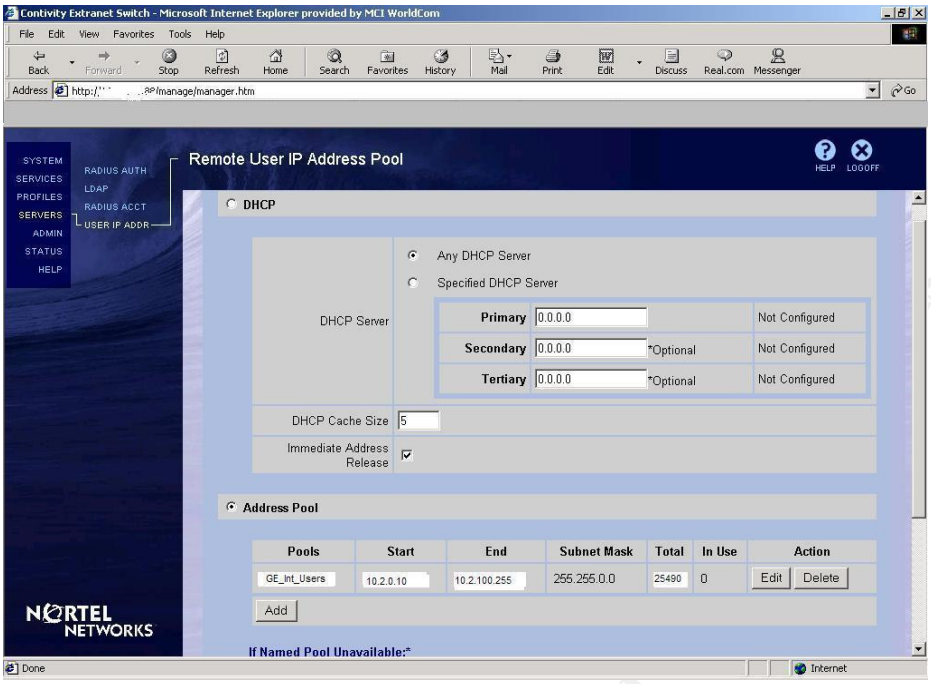


2.4.5.4 Creating Tunnelling Groups and users

Finally, we will set up the users and match them with a group and tunneling option, which will be IPSEC using ESP.



The user groups are then associated with the IP address pools that have those IPSEC policies set.

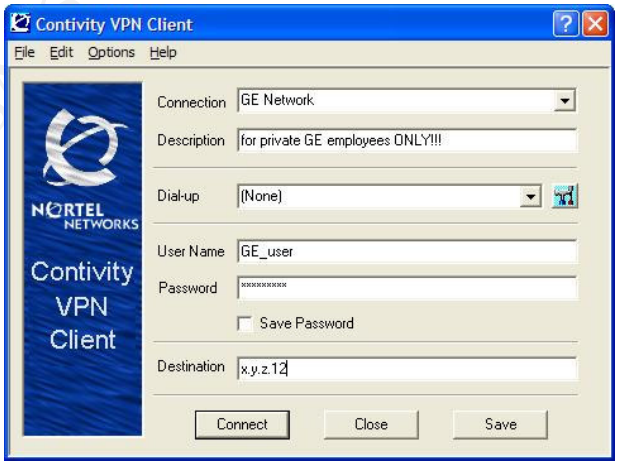


2.4.5.5 To Split Tunnel or NOT to Split Tunnel

Split tunneling is the concept that connected VPN clients can directly access the internet from their public IP addresses. The client will not remove the route to the internet in lieu of the route to the VPN tunnel(private IP address)

This creates a drastic security hole by which a hacker can attack an unsuspecting and unpatched travel laptop with no personal firewalls. Regardless, our GE Security Policy will require personal firewalls for all remotely connected VPN users and their computers. Soon VPN devices will be able to detect if there is a certain antivirus signature version and personal firewall in place so that this "written" policy will be enforced. Zonealarm's Integrity product might fit in nicely here in Phase 2.

Here is a screenshot of the Remote User's configuration of the VPN client:



Assignment 3 - Audit of the Primary Firewall

3.1 Introduction - The Process and Goal

Now that we have implemented our firewall and its policy for maximizing our layered defense system, we will proceed to testing whether the firewall configuration and the firewall ruleset is performing exactly what we have defined in GE's security policy.

3.1.1 Scope of the Audit - The Firewall

Dr. Eugene Schultz states that creating Firewall testing goals and the resulting scope is important[16]. Since we will be focusing on the targeted Audit, our scope will be focusing on auditing only this PIX device, so we will NOT be testing VPN, external border router, internal hosts, etc.

This audit is NOT to be construed to be a penetration test or exhaustive security audit of GE Enterprises.

3.1.2 Project Goal of the Audit

Our GOAL is to provide evidence that the firewall configuration and implemented ruleset is indeed protecting, filtering, and logging the correct traffic from and to the intended Zones in our network.

3.1.3 Components of the Firewall Audit:

Before we start kicking off multiple tools to satisfy this scope, we need to define what components we will be auditing. As Lance Spitzner writes in his excellent Firewall Audit tutorial, it is wise to verify 3 main components: your Firewall itself, its rulebase, and its secure authentication.[17]

We will look at each of these components below.

3.1.3.1 Firewall itself

3.1.3.1.1 Verify Firewall is physically and logically secure (enough said)

3.1.3.1.2 Verify that Firewall's underlying OS is hardened

Since we are using a hardware based firewall appliance, we have an advantage over hardening a 3rd party Operating System that other Software-based firewalls utilize.

3.1.3.1.3 Verify that the Firewall is hardened

We can verify this with PORT scanning it using ICMP, UDP, and TCP. It should not respond to pings, nor become unstable after malformed packets are fired at it. One

[16] E. Eugene Schultz, Ph.D., How to Perform Effective Firewall Testing, http://www.remainsecure.com/whitepapers/firewalls/fwtesting.htm

[17] Lance Spitzner, http://www.spitzner.net/audit.html

good source to cross check is NSA's reference guide that outlines hardening IOS devices, as described in http://nsa2.www.conxion.com/cisco/guides/cis-1.pdf.

3.1.3.2 Firewall rulebase

We will also use some auditing methods to verify our PIX firewall's ruleset, or Access Control Lists. These are the crucial elements that comprise our Security Policy that separates the different Security Zones. We need to verify that the PIX will only pass ALLOWED traffic FROM and TO certain hosts, and DENY all other traffic.

It is too easy to trust that the ACLs in the PIX config will perform as we expect. It is necessary for us to validate that in fact these ACLs will provide the Security Policy that we have created for GE.

3.1.3.3 Firewall secure authentication

As Lance states in his Firewall whitepaper[18], it is also helpful to validate that any remote authentication by VPN users and administrators is encrypted into and out of the proper interface of the PIX, as well as over the wire from the originating zone. We quickly test this by using a packet capture tool like Ethereal and find that our passwords are indeed encrypted.

3.2 Planning the Audit

3.2.1 Communication plan for the Audit-

We also have communicated to all business stakeholders and technical administrator about the schedule in which we will be performing the audit, and obtained written permission to perform Firewall testing with its associated risks.

3.2.2 Timeframe and duration of the Audit

Since service disruption needs to be kept to a minimum, the timeframe with which we will perform this Firewall audit will be during evening off hours. The estimated time to perform this firewall audit is 16 hours which will require the full time schedules of 2 consultants and 1 to 2 GE Subject Matter experts.

3.2.3 Resources performing the Audit

In order to begin educating GE's IT staff on the importance of security auditing, we are involving several of their personnel. We have picked their system administrator and a web site developer/dba. This allows for better collaboration and trust within the teams, as well as GE's self sufficiency in managing their systems once we leave the engagement. Also, we have included the owner Chen Fu in observing our testing to demonstrate to him how proactive a company should be in managing their security infrastructure.

[18] Lance Spitzner, http://www.spitzner.net/audit.html

Role	Rate/Hr	Effort (Hours)	Estimated Cost
Audit Lead	$150	32	$ 4800
Audit engineer	$100	32	$ 3200
GE provided resource, preferably Web developer/Dba	$internal	32	$ 0
GE provided resource, pref. a network admin	$internal	32	$ 0
Total			$8000

3.2.4 Audit Risks and Considerations

We will define some basic risks and mitigations. We must communicate to GE that testing and auditing networks and firewalls are an ongoing process and not totally foolproof. We can never "be totally safe." We also share that full involvement from the GE IT team members is important to develop a health mindset towards keeping the perimeter secure.

Risk Item	Probability	Impact	Mitigation Plan
Possibility of increase in project scope due to additional reqs	Medium	High	Consulting company has made every effort to define requirements for auditing the firewall only.
Availability of GE's SME.	Medium	High	Schedule meetings and work ahead of time and on a regular basis.
Possible server or network outage due to firewall audit scanning.	Low	Medium	All backups of servers and configs of routers and firewalls are current and tested. A rebuild or reload can be used.
Some hidden exploit not found by firewall audit	High	High	This audit is a snapshot in time. Future auditing must be continued to provide ongoing assurances.

3.2.5 Methodology for the Audit

Let us take another look at the Security Policy to ensure the correct methodology for the Audit.

3.2.5.1 Hitting Each Zone, Each Direction

We will focus on each of GE Security Zone's ability or inability to access other Zones. This will be executed unidirectionally, from a Launch Zone to a Target Zone.

We will be using two laptops to perform the central part of our Firewall auditing. The first SENDING LAPTOP acting as our exploiter agent will attempt to send test network traffic to the other Zones. From this laptop we will engage our arsenal of common hacking attack methods (CHAM) using software tools listed below.

We will also be utilizing a Reconnaissance (RECON) LAPTOP that we will use to determine what type of traffic is actually traversing into and out of the target Zone. This laptop will be running a packet capture software tool that requires that its network interface be running in "Promiscuous Mode." Promiscuous Mode is simply an operation by which the host's NIC will not only receive all packets that reach its buffers, but it will also record all detailed Ethernet traffic that is being sent within the collision domain of that ZONE.[19] The RECON Laptop will be running Ethereal's Network Analyzer.

Here is a diagram of the Audit test topology of the laptop pair:

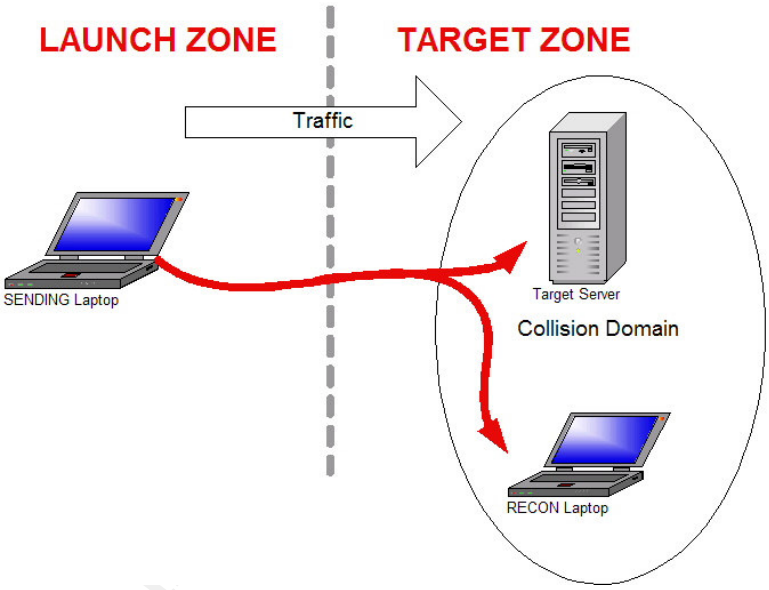


Diagram 3.2—1 Using 2 Laptop to validate Firewall's ruleset

Why perform this test from both Zones of the Firewall? Even though the SENDING laptop's scanning logs will tell us what Hosts and services are available, we cannot always determine if some of those SENDING packets actually do "leak" through the Firewall to the other side unless we capture packets independently using the RECON laptop.

[19] A *collision domain* is where all packets are sent within a certain area. A hub forwards all traffic to all of its ports, whereby a switch will forward only packets intended for a particular "learned" port, also called a microsegment. Our DMZ and PUBLIC zone are hubs that will allow for easy reconnaissance for Network IDs or RECON Laptops. The Corporate Zone uses a series of switches.

This double testing of exploit traffic will provide the most comprehensive test for validating our firewall ruleset. After this Audit, though, we may choose to just use the SENDING laptop to perform ruleset validation.

3.2.6 Hardware Audit Tools we will use

We will be using 2 1GHz Laptops to perform our audit testing. One laptop will attempt to send certain packets through the Firewall and the other laptop will capture all traffic on the other side.

Laptop 1- will be the SENDING Laptop, which will use the scanning tools below

Laptop 2- will be the RECONNAISANCE Laptop that will receive all packets bound for that zone using a collision domain-based media access device like a hub.

3.2.7 Software Audit Tools we will use

3.2.7.1 Footprinting tools-

The following tools will be used to glean the first fruits of the target. Using these tools can help us gather GE's general information such as public DNS servers, administrative contacts, possible geographical locations, and IP address ranges, or netblocks. All of the tools need to be compatible with Windows platform, as that is what is most comfortable with the GE IT staff, which will be working with us. Some screen shots of the Windows based tools below can be seen in the appendix.

Necrosoft Whois-by Necrosoft, found at http://www.nscan.org/?index=whois

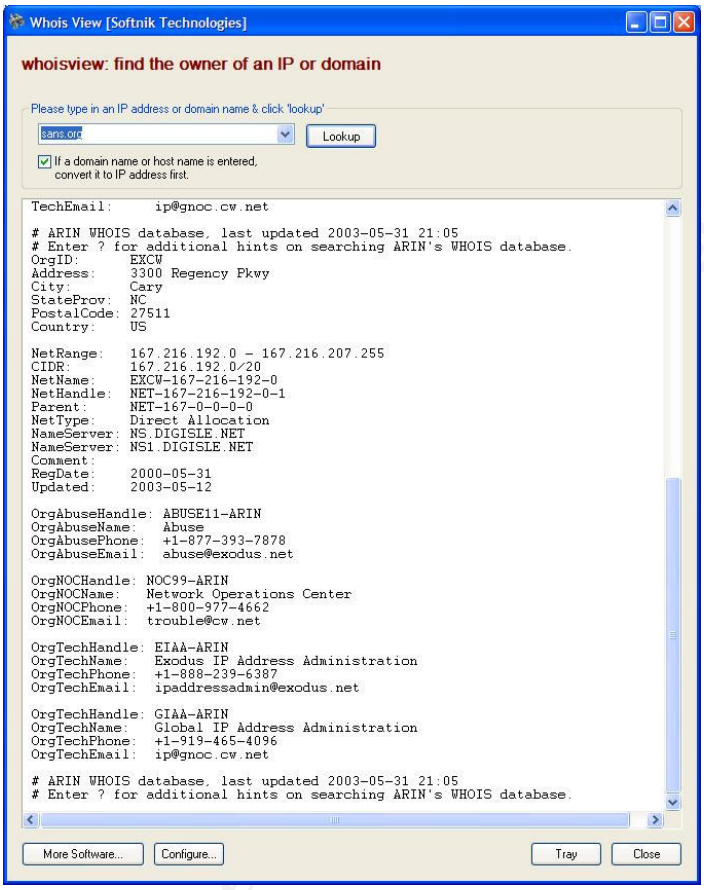
These tools query various WHOIS servers for our domain information and will provide DNS, netblock, administrative, and Internet Service Provider information

SAM SPADE Network Suite, found at http://samspade.org/ssw/download.html, is a Swiss Army knife of footprinting tools that also provides some scanning capabilities.

Whois View, by Sofnik Technologies,

found at http://www.whoisview.com/products/whoisview/

This tool is useful to discover basic public internet information about the target, as in the finding SANS.org's hosted NETBLOCK below:



From the information above, we can find the DNS SOA name server authoritative in giving out hostname to IP address mappings for GE's public hosts.

Nslookup, from Windows NT, Windows 2000/2003, and Windows XP, provides a means to gather relevant public hosts such as the SMTP, WEB, FTP servers.

Once we determine the DNS servers for GE, we can use NSLOOKUP to perform a quick attempt to initiate a ZONE TRANSFER from that server, giving us every single public host name and IP address. DNS should refuse this query if configured properly.

Here is the syntax for the query for GE whose response should be refused.

```
C:\path\nslookup
Server ns1.GE<s>ISP.co<m>

ls -d gefortunes.com
[ns1.eyz-dns.co<m>]
 gefortunes.com.                SOA    ns1.GE<s>ISP.co<m> root.ns1.
GE<s>ISP.co<m>. (20
01030610 10800 3600 604800 86400)
 gefortunes.com.                NS     ns1. GE<s>ISP.co<m>
 gefortunes.com.                A      99.200.200.20
 gefortunes.com.                MX     30   smtp.gefortunes.com
 ns3                            NS     ns3.gefortunes.com
 us                             MX     30   smtp.gefortunes.com
 smtp                           A      99.200.200.8
 webmail                        A      99.200.200.7
 corpvpn                        A      99.200.200.2
```

PING, from Windows NT, Windows 2000/2003, and Windows XP, allows us to gather information by sending various echo requests stimuli.

TRACERT, from Windows NT, Windows 2000/2003, and Windows XP, allows us to quickly determine some network topology constructs. Oftentimes the firewall will answer these requests for the traced hosts, divulging the nature of its armor and of the servers it might be protecting. We can also use this tool to possibly learn the IP of the Border router.

3.2.7.2 Scanning/Enumeration tools-

NMapWIN for Windows[20], NMapWin is a Open Source Windows GUI-based and command line network "exploration" tool. It performs many different audit tasks such as determining what types of filters are placed on firewalls, protected hosts on a subnet, what services they are offering, and what Operating System the hosts are running. It is based on the most excellent UNIX-based nmap v2.54beta36 that is used by hackers and firewall auditors alike. Although *nix users might disparage the Windows port from UNIX, it is a very useful and free tool for Windows users. This tool requires WINPCAP, a network interface packet capture driver.

The documentation for Nmap summarizes it capabilities:

> "nmap supports a large number of scanning techniques such as: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, IP Protocol, and Null scan."21

[20] http://www.nmapwin.org

[21] http://www.insecure.org/nmap/data/nmap_manpage.html,

We will use NMAP for performing scanning and fingerprinting operations to validate that are Firewall is doing what we want it to for protection. An example of a typical command line for NMAP.EXE might be:

Nmap [scan type(s)] [Discovery options] <scan options> [host options] [Time throttle] TARGETHOST_or_SUBNET

NMAP -sS -PT -p 80,443,U:53 -O –vv -T 3 99.200.200.1/24

Where:

-sS is Stealth TCP SYN Scan

-PT designates to send TCP ACKs instead of ICMP echo request packets

-p 80,443 designates scanning TCP port 80 and 443, UDP port 53

-O allows for nmap to try fingerprinting the target host's OS using various techniques

-vv VERY verbose mode output

-T 3 tells nmap to allow for NORMAL timing between scans of hosts and ports

99.200.200.1/24 designates the subnet or host you want to audit or scan

Some of the more important switches we will be using are as follows:

Nmap Scan Switch	What it does	Open port on target if:	Firewall is filtering if:
-sS	Scans using TCP SYN packets, which allows for "half open" connections	SYN ACK response	RST or nothing, usually not logged by FW
-sA	Excellent firewall scan, sends a TCP ACK to test for stateful filtering	RST response, not logged by nmap	ICMP unreachable or nothing
-sP	Normal ICMP echo req scan	Echo reply response	Possibly with no response
-sU	sends 0 byte UDP packet	No response	No response or ICMP destination unreach., this is usually an unreliable test
-sT	Std TCP scan	SYN ACK	It allows only open ports
-sP	ICMP Ping scan	Echo response	ICMP destination unreachable or none

Nmap Pre-Scan Discvry options	What it does	Open port on target if:	Firewall is filtering if:
-PO	Do NOT try to Ping, very stealthy		

-PT <port>	Send a TCP ACK	RST response	No response
-PI <port>	Send a ICMP echo request	Echo reply	Port unreachable

Nmap will yield several types of responses:

OPEN-this port is accepting connections, firewall is generous

CLOSED-a RST flag is sent back in response by the firewall or host

Filtered-where the firewall or host simply drops your packets, NO RST is sent

Other Nmap options	(case sensitive)
-O	Allows for Host OS Identification and fingerprinting using various processes
-f	FRAGMENTS SYN, FIN, XMAS, or NULL scans to use a 38 byte fragment (from Win XP), which tests whether a static filter will pass it because it cannot see any ports in the fragment-Good stateful firewalls will buffer these fragments and reconstruct them before allowing them to pass
-F	FAST-Allows NMAP to only scan ports acc to nmap svcs file
-r	Do NOT RANDOMIZE ports number to scan; this makes it easier for me to find the ports I'm auditing

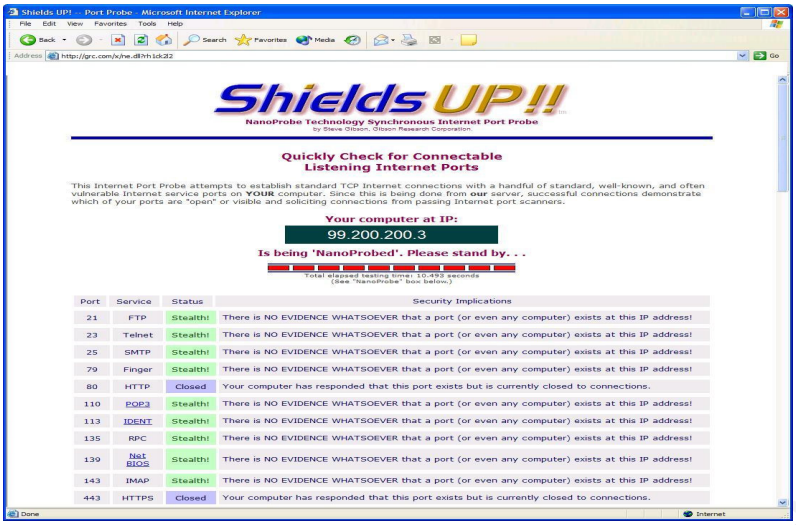
We will be using this tool as the SENDING application for testing the firewall.

Ethereal Network Analyzer 0.9.9, by Gerald Combs, found at www.ethereal.com, is also a Windows port, will provide exhaustive packet capturing using the above WINPcap, which is necessary for the tool to run in promiscuous mode. This tool will be the RECEIVER application for testing the firewall. Ethereal will record all traffic that is entering the TARGET Zone to validate if that traffic supposed to be allowed into that Zone.

Superscan 3.0, a Windows TCP scanner for networks and hosts, is a wonderful tool to quickly determine what ports are open on what IP addresses. This tool also allows some primitive reconnaissance on banners.

ShieldsUP[22], is an online port scanning site from Gibson Research Corporation, or GRC.com. Steve created a PORT scanner he calls NANOPROBE that will scan your host (or firewall). This online utility will determine if the Firewall is determining if a port is OPEN, CLOSED, or "stealthed" port by not allowing outside access to that port. For an initial firewall check, we use Shields UP!! from clients inside the DMZ and the INSIDE Zone. We should see only the external IP of the associated NATted IP address, which reveals what ports the firewall is allowing.

[22] http://www.grc.com , Steve Gibson has created a compendium of easy to read infosec materials on his site.



3.3 Performing the Audit

3.3.1 Introduction

We will start our ruleset audit from the least trusted Outside zone and launch our tools against the Firewall protecting the DMZ, VPN, and INSIDE Zones. The Sending laptop will be the initiator of the traffic, and the RECON laptop will be the listening node to capture all traffic using Ethereal.

All capture decodes will be saved by name, date, targets up on the network server in a secured file share so that we can use them for future audits. We trust that the firewall log will show our exploit attempts as well, both locally and on the Syslog server.

The graphic below shows the different zones we will target to start our audit. Immediately after auditing each zone barrier, we will include a section of the results and a brief commentary. At the end of this section we will provide recommendations for changes.

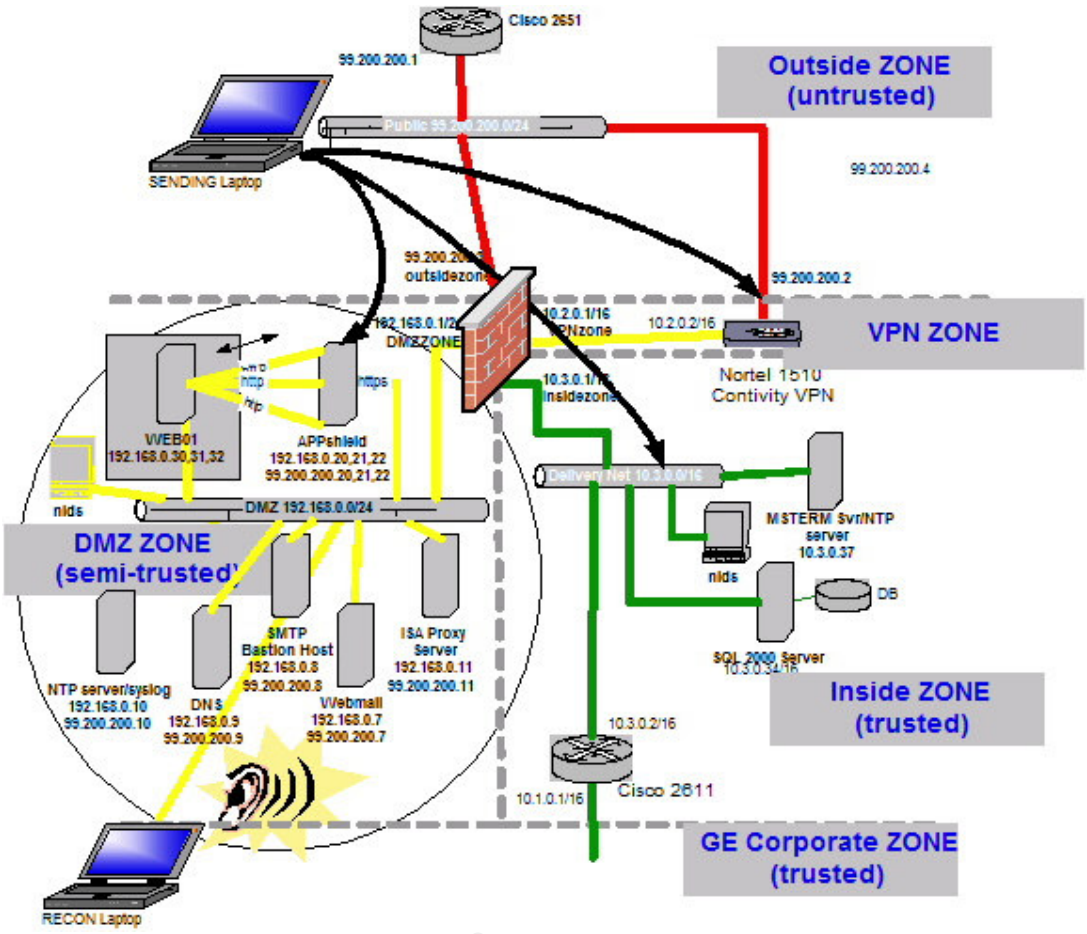


Diagram 3.3—1 Scanning from the OUTSIDE ZONE

3.3.2 Starting From the OUTSIDE Zone

We place our SENDING laptop out on the HUB between the Border router and the Firewall. We have procured the public IP address netblock from our WHOAMI DNA tools above. After scanning the external subnet with Superscan and Nmap ping sweep, we can see that we have several external IP addresses, which are actually Hosts inside our network. This matches perfectly with our STATIC NAT and ACL pairing of our firewall.

Note that we must give the sending laptop a static IP address in this zone, or we could configure it with a different IP address to simulate spoofing.

Here is a diagram of how we will test from the Sending Laptop, noting the direction of the intended access for each host and service protocol.

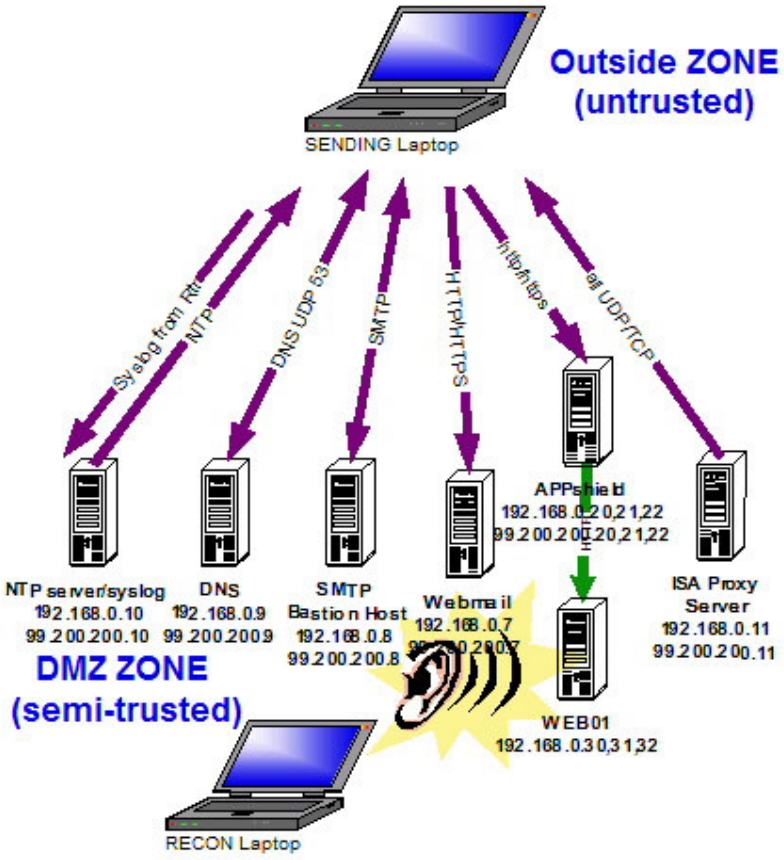


Diagram 3.3—2 Scanning into the DMZ Zone from OUTSIDE

3.3.2.1 Scanning the DMZ Zone and the Firewall itself

Our major tests for verifying our Firewall are:

- **The firewall should not be vulnerable to direct attacks against it**
- **The firewall will allow ONLY explicit traffic to pass by host, protocol, and direction.**
- **The firewall will NOT allow traffic to traverse directly from OUTSIDE to INSIDE Zones.**

This is probably the most critical audit test, in that the DMZ Zone is the only Zone that the PIX will allow access to from the Outside. We want to prove that the PIX is acting as a true buffer zone, so that no packet directly traverses from OUTSIDE Zone to the INSIDE Zone. Because of the NAT that we have set, the FIREWALL will allow only certain IP addresses to be accessed from outside. While we trust in our skills and the PIX's reputation, we still must prove our accuracy by providing actual evidence that our rulebase is "rock solid".

Before we fire up NMapWIN on the SENDING Laptop (SENDING from here on), we need to set up the RECON laptop (RECON from here on) with Ethereal recording any traffic. Once we begin capturing packets, we tell our colleague to fire off NMAP stealthily using the following to hit our website gefortunes.com. We plan on using nmap's ACK, SYN, and WINDOWS scans, along with both ICMP and TCP discovery.

Note that in this version of NMAP for Windows the command lines are listed at the bottom. We can also use the nmap command line.

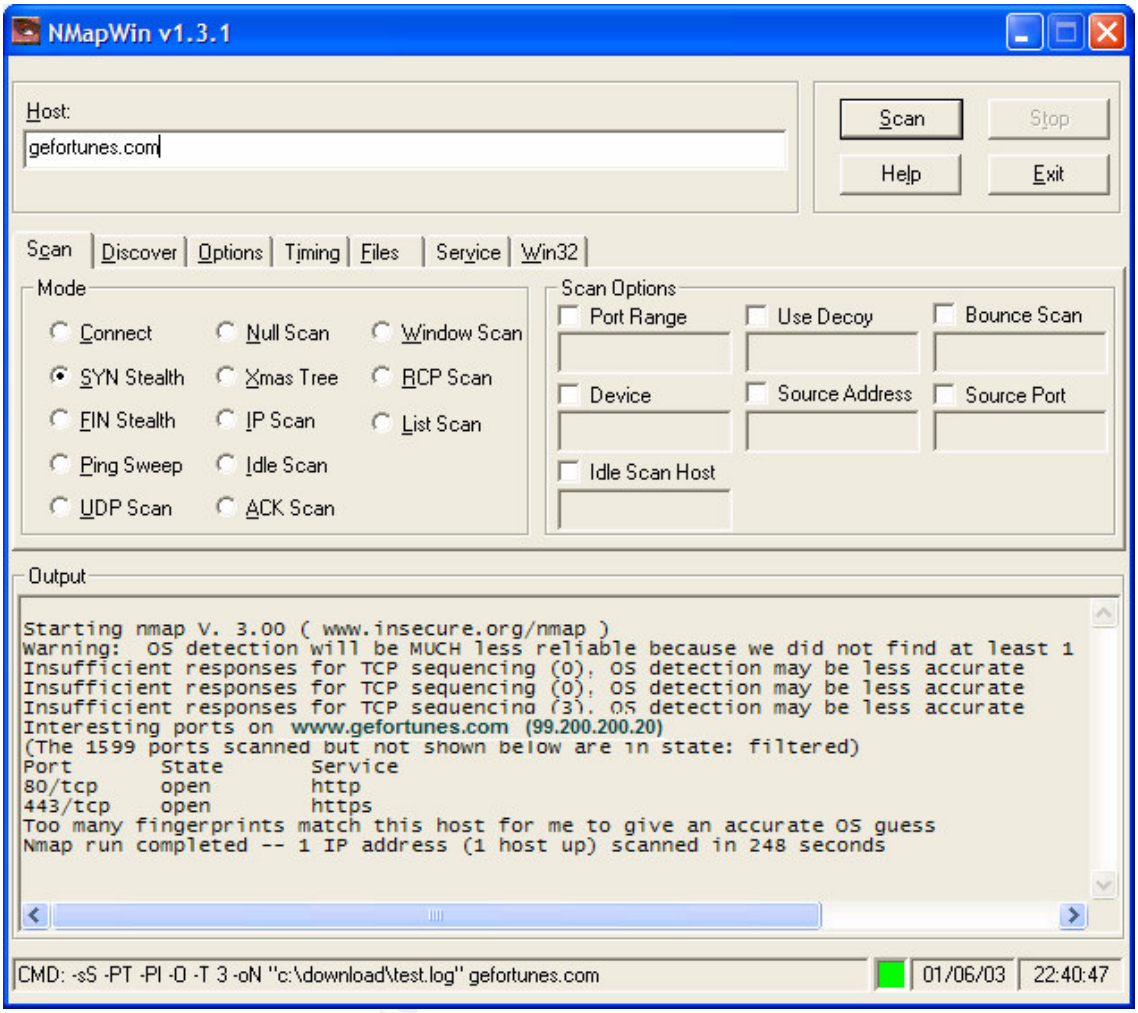
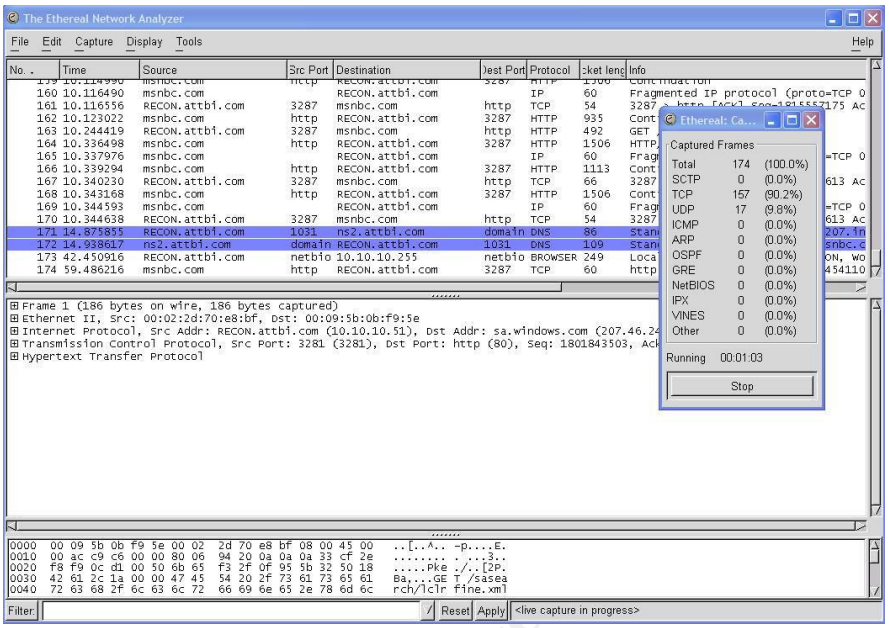


Diagram 3.3—3 NMAP scanning the Web server for GEFORTUNES.COM

The SYN ACK responses above are for the web host, which is really the Sanctum Appshield Application Firewall. The 1599 ports are filtered, proving that our firewall is enforcing access in between us and the web server. On the other side we can look at the Ethereal packet decode to see that only Incoming TCP SYN, SYN ACK, and ACK packets and initiation of HTTP and HTTPS to the correct Appshield box was occurring. Since we have the RECON host on the DMZ hub running in promiscuous mode, we can "catch" all of what is coming through from the outside. No other packets are seen in the decode from any the outside host, or any spoofed hosts, which is a good thing.

While we may be quick to filter capture decodes, we decide it is better to save all of the packets coming into that zone, and use display filters to look for key IP addresses. We save the results of the Ethereal capture in a properly recognizable file with the Audit Launch Zone, Target Zone, and date, along with the output from nmap(above).

Here is a shot of the Ethereal Network Analyzer in the process of capturing traffic on the wire:



Now that we see that the DMZ tests are working properly, it is time to run the SENDING host to scan the full gamut of the outside subnet using the various tools like Superscan, etc.. We collect this data to be analyzed after all of our testing is complete.

Now we need to focus our audit by attempting to probe each host that may respond to us behind the firewall. If we receive a SYN ACK in response to a Stealth SYN nmap probe, we record this as positive internal resource validation and note the service (port) that was allowed into the DMZ. The list of servers and ports we see from nmap that can connect to from the Outsidezone is:

APPSHIELD Web firewall	www.GEfortune.com	TCP80/443	99.200.200.20
APPSHIELD Web firewall	supp.GEfortune.com	TCP80/443	99.200.200.21
APPSHIELD Web firewall	partners.GEfortune.com	TCP80/443	99.200.200.22
Syslog		UDP 514	99.200.200.10
SMTP Bastion host		TCP25	99.200.200.8
DNS		UDP/TCP53	99.200.200.9
WEBMAIL		HTTP80/443	99.200.200.7

We should run several types of nmap exploits here, such as –sA , -sW, and –sP (ACK Scan, Windows Scan, and Ping Sweep, respectively). We see from Diagram 3.3-3 the example of discovering what services our Firewall (and HOST) is allowing to be accessed from the outside. The Host may have other ports open, though, so we should use various options such as the Fragmenting of packets using nmap's –f switch. The scanning shows our firewall does NOT pass fragmented, ACKs, or Ping ICMP echo requests. Performing a UDP scan reveals that all ports seem open for the host, but that is because our PIX is not responding to those UDP scans, which is why these types of scans are not as valuable as the others. The –sA and the –sW scans were probably the most useful here in validating our firewall rulebase. We can use spoofing here as well trying to connect to a 10.0.0.0 address, in order to validate

that the firewall is allowing only intended hosts and preventing INSIDE access. **This NMAP testing procedure will be used throughout the following tests. We will not be displaying the nmap results for brevity.**

NOTE: To test the firewall itself, we should use the same NMAP testing procedure to attacking the external IP address of the PIX. We see that there are no open ports in any of the nmap's results on the firewall, except for the Firewall's logs screaming to the Syslog server that a local external host is attempting unpermitted access.

3.3.2.2 To the VPN Zone

Next we will run the same SENDING host scan test against the firewall, but this time we will situate the listening RECON host in the VPN Zone to collect any packets originating from the OUTSIDE Zone.

We are not surprised to learn that NMAP picked up on the VPN components (ISAKMP UDP500 and ESP Protocol 50)that are being exposed on the external interface of the VPN gateway, for incoming VPN clients. Our RECON machine shows no public packet leak coming in from the outside.

3.3.2.3 To INSIDE Zone

After the VPN zone we move the RECON host to the INSIDEZONE to capture any traffic coming from the outside while scanning through the firewall. Notice that any traffic bound for the Enterprise in the CORPORATE Zone will also be mapped here, as this zone also hosts a broadcast/collision domain. The packet capture on the INSIDE ZONE show NO traffic from the Nmap machine.

3.3.2.4 Results from the OUTSIDE Zone

After analyzing our NMAP logs, Ethereal decodes, and comparing their times with the firewall logs, we are happy to see that the PIX is performing well under the expected attacks that we released on it. It's ASA based FIXUPs were able to deal nicely with the unpermitted and stateless ACKs. We see from the logs that ICMP echo requests were dropped, which shows why we never saw them from the RECON host.

WEB and WEBMAIL servers- our data shows that although we attempted to connect to each public IP address using Port 80, Nmap's default, we see that the firewall did not allow any SYN ACK responses from any server except for the Application Firewall Appshield, running on 99.200.200.20,21,22. Even though we did not see any traffic from the outside going to the protected WEB01, we make a note that we should verify and check an ACL on the DMZzone interface to deny any internet bound traffic leaving the DMZ from WEB01.

Our PIX demonstrates its strength in that it doesn't permit any non-Web traffic from the outside. Hence, the only traffic the Web/Webmail servers will respond is only from port 80 and 443 SYN requests from outside, with a little help from our ASA WEB Fixup on the PIX.

DNS server-we see that UDP and TCP ports 53 were allowed in as intended in our security policy. Not only are we not allowing anything but port 53, but our PIX's DNS FIXUP will ensure that only DNS commands are able pass, such as for Zone transfers from out Primary DNS at our ISP and from Internet recursive lookups.

NTP Server/SYSLOG-When we tried to connect to the NTP server using nmap's SYN for port 123, we never saw the traffic or a response from the RECON host's

point of view. This too is acceptable but we must remember to test outgoing NTP requests from this box in our next tests.

The Ethereal capture decodes show that the SYSLOG service on this DMZ host did receive packets from the outside, but only from the router, not the rogue SENDING host. When we spoof the router's address 99.200.200.1 on nmap, then we can craft a SYN packet to that host on port 123. We note this aberration.

SMTP Gateway-Looking at our nmap and ethereal logs, we see that port 25 traffic easily traverses the firewall as expected. Another dump of using Telnet to connect to smtp.gefortunes.com on port 25 allows us to see that we are running the WebShield SMTP service. While this is ok, perhaps we should research this to neutralize the banner being published for our mail gateway. We want to keep the hackers a little honest by working for their reward.

Proxy-although we did not see any traffic coming in from the SENDING host on the OUTSIDEzone, our RECON host did capture traffic that was coming in from public hosts such as server121aa.akamai.com, realmedia-a800.d4p.net, and m2.doubleclick.net, destined for the ISA Proxy in the DMZ. Hmm, this probably is from one of our colleagues on the CorporateZone getting bored and surfing the web. Traffic coming in from the internet to the Proxy is acceptable, as long as traffic originating from the outside is not allowed to pass into the INSIDEzone by the firewall, which we will test soon.

3.3.3 Scanning From the DMZ Zone…

Now we move our Launching host SENDING to the DMZ and change its IP address to match. Here we want to test the firewall rules to determine if the PIX will only allow certain traffic in to certain hosts, and to verify that it will ALLOW only certain hosts' traffic OUT, such as the NTP, DNS, SMTP and PROXY servers.

Here is a diagram of allowed DMZ traffic that should mirror our Firewall Ruleset.

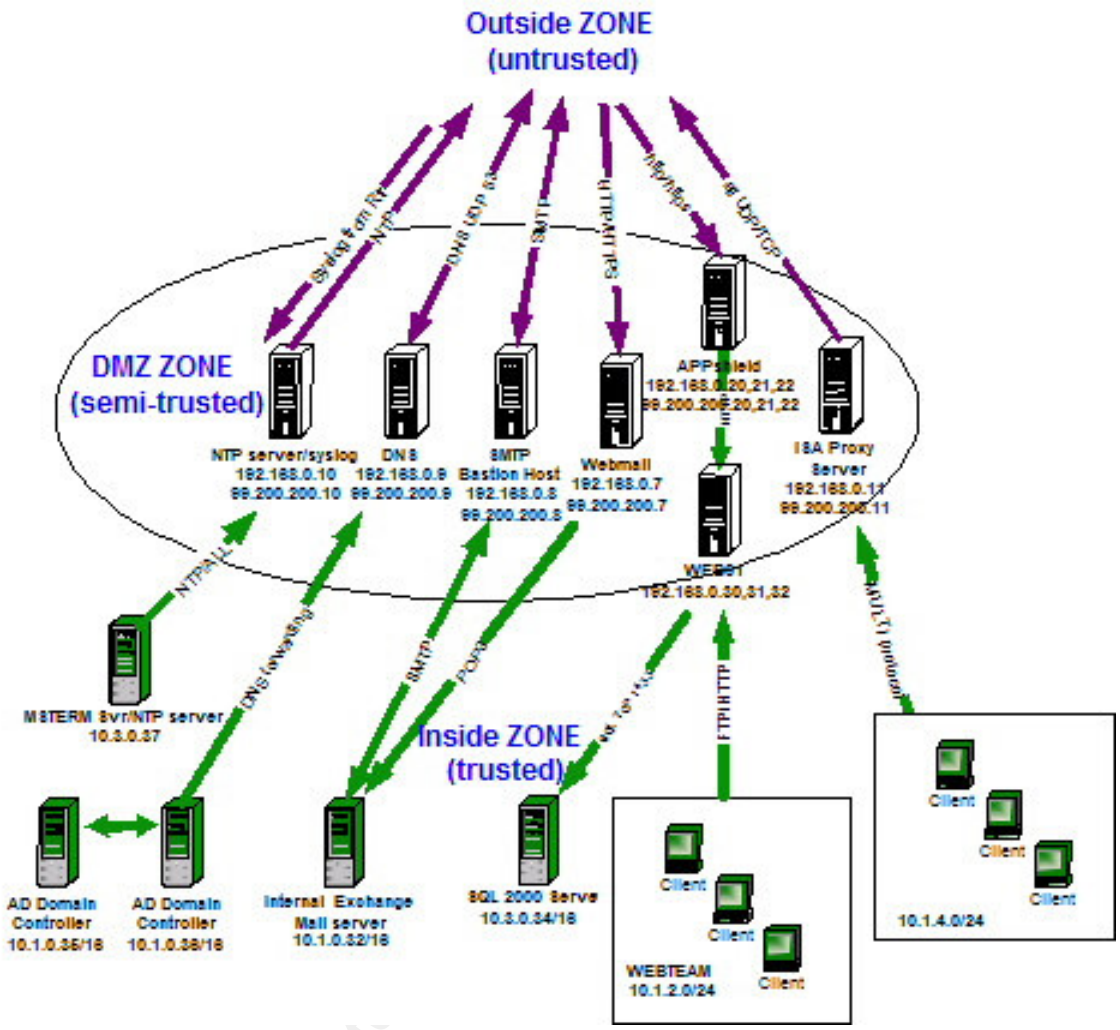


Diagram 3.3—4 Flow of traffic through DMZZone

Our Audit should support our Policy exactly, which stipulates that no direct packets will ever traverse from the OUTSIDE or INSIDE without packet inspection and/or encapsulation or encryption. The hosts in the circled zone will allow communications from the Inside and Outside. The VPN host is not pictured, but functions the same way.

NOTE: Yes, it is a whip to keep moving the two LAPTOPs from zone to zone, but that is required for our first Audit and since we have no proven NIDS in place. After there are any firewall changes or upgrades, a preliminary test might involve using only the SENDING machine running NMAP and telnet for auditing.

3.3.3.1 To the OUTSIDE Zone

Here we wish to place the SENDING host on the DMZ to test for possible Firewall holes in allowing unexpected traffic out to the internet or INSIDEZONE. Our RECON box on the other side will stealthily catch any traffic that may be passing through the firewall that we do NOT want passed.

A Note on Spoofing-Using spoofing in auditing firewalls is difficult. It is more difficult to spoof addresses for discovering targets hosts because the target needs a way to send the SYN ACK or RST response back to you. If you are spoofing another address, make sure that you are directly connected to the intermediary routing/firewall so that you can broadcast an ARP entry for that IP address. Be careful though, because SYN flooding can occur where packets get sent to the real IP address and not to you. To perform spoofed source addresses, we can use NMAP to do this for us, using either DECOY or SPOOF switches. Here is the command line with which to send spoofed packets through a firewall.

> **Nmap [scan type(s)] [Discovery options] <scan options> [host options] [Time throttle] TARGETHOST–D 555.555.555.555 OR –e eth01 –S 444.444.444.444**

Where:

> **555.555.555.555** is a decoy that will be used IN ADDITION to your real IP
>
> **eth01** is your physical interface
>
> **444.444.444.444** is your spoofed IP

DECOY will send out packets with the DECOY IP source address, whereas spoof will ONLY send out that spoofed IP address to the target.

A word of CAUTION!!!-unintended Denials of service can result from your spoofing audit testing. Many ARP entries will remain in a host's or device's ARP cache for up to 4 hours. Microsoft hosts usually will cache this arp entry for 10 minutes, whereas Cisco devices usually cache them for 4 hours. You will have to flush these values or take those spoofed Hosts offline.

It is probably better to "Impersonate" the real hosts by first disconnecting them from the DMZ during testing. We need to ensure that once we are done, we reconnect the real host, and ensure that all ARP caches are flushed in the zone.

3.3.3.2 To the VPN Zone

We move the RECON box to the VPN Zone and begin testing, remembering that each time we move the RECON host requires us to change its IP address. Thankfully we are using Windows XP and therefore we do not have to reboot often.

Our SENDING host is unsuccessful in sending packets through the firewall to the 10.2.0.0 VPNZone, because we pick up NO packet during the test activity.

3.3.3.3 To INSIDE Zone

Finally we wish to trace all packets that may be trickling through the firewall into our trusted zone, or Inside Zone. Placing the RECON host on the INSIDE Zone will be easier to do because we have a simple hub on that subnet.

NOTE: if we want to provide packet capturing on a switched network, we must first configure the switch to "echo" all traffic from one Server's port to our RECON port.

3.3.3.4 Results from the DMZ Zone

We have tested sending packets from the DMZ segment in general using nmap to all three other Zones. Ethereal decodes tell us only explicit DMZ hosts can initiate packets. For each of these hosts IP we will impersonate using the SENDING host:

NTP server, DNS Server, SMTP Bastion Host, ISA PROXY

NTP/SYSLOG Server-NTP requires only a couple of packets, so it might be wise to filter Ethereal capturing. Doing this, we send NTP packets using source and destination UDP ports 123 to various IP addresses. We only get responses from our 3 public NTP servers that the Firewall ruleset allows: `192.6.38.127, 128.9.176.30,` and our firewall itself, since it is time synced with the NTP DMZ host. We are also pleased that the NTP server accept NTP update request from the INSIDEZONE and CORPORATE Zones.

Syslog traffic is blocked from propagating outside, but incoming traffic is allowed as expected from the other 2 more Secure zones, VPNZONE and INSIDEZONE.

DNS Server-Our secondary DNS host's outbound traffic is global, except for our zone transfers that need to be restricted to our ISP. We ask our ISP to allow only pushed Zone transfers to our 99.200.200.9 DNS using TCP 53. All other traffic is successful only if it is designating a destination port of UDP 53, both from the Ethereal decode on the other side, and our nmap SYN attempts to various internet addresses. No traffic is coming from the 10.0.0.0 range either, as only the SMTP and PROXY hosts should be using it locally.

SMTP Server-any packets sent out toward the internet from this host is shown to be with the destination port of Port 53 and Port 25. We reconstruct a SMTP session using the Ethereal FOLLOW TCP STREAM feature to view the contents of the mail interchange and find the banner for the MAIL Bastion Host is listed as WEBSHIELD. This should be changed by configuring the mail host's banner.

We validate also that SMTP packets are able to be sent to the internal EXCHANGE server at 10.1.0.32.

ISA Proxy-this is probably our most "open" host, as in our decodes and nmap logs we find that it can indeed communicate with ANY internet HOST using ANY protocol. While this is a risk, we have taken safeguards by allowing only outbound access and preventing any initiating packets from outside, as well as limiting the protocols that the proxy can use to service our GE employees. A content vectoring solution as well as on-host antivirus protection should be added soon, maybe in Phase 2.

3.3.4 Scanning from the VPN Zone…

Now we turn our attention to the VPN Zone by setting our SENDING host to launch NMAPWIN from that subnet.

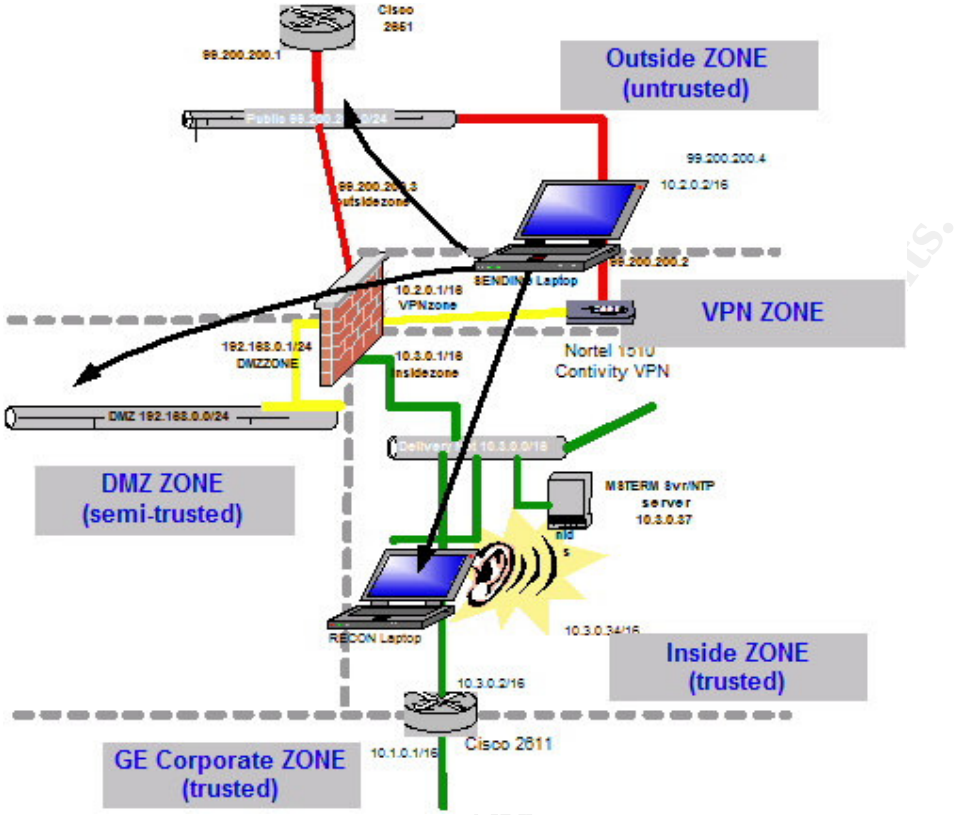


Diagram 3.3—5 Scanning from the VPN ZONE

3.3.4.1 To INSIDE Zone

The PIX is configured to only allow traffic from this subnet to the INSIDE Zone and Corporate Zone unrestricted. We place the listening RECON box in the INSIDEZONE running Ethereal to capture all of the packets. We should see almost ALL of the packets come through on the RECON host.

3.3.4.2 To the OUTSIDE Zone and To the DMZ Zone

Both of these zones should be OFFLIMITs to any traffic originating from the VPN zone, so we place the RECON host in the OUTSIDE ZONE and the DMZ ZONE to test our firewall ACLs.

NOTE: When we were LISTENING with RECON from the OUTSIDE we were also able to validate the VPN routing and IPSEC policy of the VPN gateway. NO unencrypted traffic was found be propagating from the VPN device, and we saw only ESP IP protocol 50 IP traffic and a couple of UDP 500 ISAKMP packets trickle in to that VPN Contivity, which would be any VPN clients' traffic. Our VPN logs show it was indeed a legitimate VPN user. Verifying the encryption we use Ethereal to determine we can see no data past the first IP Header in the IP packet.

We didn't expect to see any traffic with the source address of 10.20.0.0/16 in the outside, which was proven when we saw NO unencrypted or misrouted traffic traversing the FIREWALL or the VPN to the outside.

3.3.4.3 Results from the VPN Zone

Our testing showed that no PUBLIC IP traffic is leaking out of the VPN from the OUTSIDEZONE. Our test while LISTENING with Ethereal outside demonstrated that all external VPN traffic entering GE was encrypted.

All is well in the VPN world.

3.3.5 Scanning From the INSIDE Zone…

Finally from the Inside Zone, we want to document the traffic that is only being allowed out to which host in the DMZ and VPN Zones. Remember, all packets exiting unencrypted to the internet should not pass directly without being filtered at least once by the PIX firewall's ASA stateful inspection, the VPN Contivity, or the DMZ hosts like SMTP and PROXY.

Just any Corporate host will not have unfettered access to the internet, including any consultants or supplier working inside. They will either have to install a proxy/firewall client, or configure their browser to use ISAPROXY for internet access.

3.3.5.1 To the DMZ Zone

Placing the RECON host on the DMZ Zone allows us to take a packet recording of all traffic emanating from the 10.0.0.0 zones. As expected, we learn that many clients are using the NTP server, as well as some Syslog traffic from both the VPN and INSIDE zones. We also test access to the Webmail, DNS, and SMTP hosts to validate that NO traffic is allowed due to our PIX ACLs.

TESTED Internal Access to the DMZ:

AD Domain controller, dc01.ge.local, is the only host allowed to NTP and DNS server. All other attempted ports and addresses are blocked by the PIX ruleset

Exchange.ge.local is shown that it is the ONLY host that can connect and receive TCP 25 SMTP traffic from the SMTP Bastion host using Nmap, PIX, and Ethereal logs. All other attempted ports are blocked by the PIX ruleset, except for the POP3 connection coming from WEBMAIL in the DMZ to Exchange.ge.local.

3.3.5.2 To the OUTSIDE Zone

We place the SENDING host on the INSIDE Zone and leave the capturing RECON box at the outside, and run our testing once again. This seems like it is getting repetitive, but it is necessary to be this detailed when performing a firewall audit FROM ALL SIDES AND FROM ALL DIRECTIONS after setting it up. It makes for good insurance besides making us proud to say we installed that Firewall.

After our tests, we see that there is NO traffic coming from the INSIDE. Checking our firewall logs shows several ACLs that are iterating due to non-proxy directed web traffic. Our RECON listener shows no traffic leaking from the Inside.

3.3.5.3 To VPN Zone

Again the test that all traffic should be passing from the Inside Zone to the VPN Zone needs to be tested as before, but we are reversing the direction. This ensures that any FIREWALL ACL for the Inside Zone is configured correctly.

We test this "should be" by having a client dial into the internet, connect successfully to the VPN, get issued a 10.2.0.0 address, and then attempting to scan that client with SYNs, ACKs, and ICMP requests. We have shown in the section above that no

entering or exiting VPN traffic is leaking unencrypted. We do note that perhaps we should add a DENY all on the BORDER router for the VPN at 99.200.200.2, except for ISAKMP and ESP traffic, of course.

3.3.5.4 Results from the INSIDE Zone

All testing from inside the company is completed, and a couple of minor issues were noted which will be placed in the recommendations.

3.3.6 Scanning From the GE Corporate Zone… (Optional)

If we desire, we can perform an audit on traffic passing from the two trusted zones, Inside and Corporate. Currently we are not employing ACLs on the inside router, but we plan to do this in Phase 2. Notice we have set the TERMINAL Server and the SQL Server on this "delivery" Zone because we want to isolate the administration components and the Crown Jewels of GE by limiting access to the SQL server database by the corporate employees. If this router was IOS v 12.2 or later, we could upgrade to the FW feature pack to allow for stateful inspection and even user based Authentication Proxied dynamic ACLs for excellent segment lockdown.

Benefits of placing ACLs on Internal Router:

1. Prevents inside "curious Georges" from eavesdropping or eyeing the SQL server.
2. Double wall defense in depth capability for internal network
3. One defense barrier for incoming VPN traffic.

3.4 Analyzing the Audit results

As we have commented on the results of the testing, we will summarize the issues we see, and make recommendations.

3.4.1 Recommendations

1. Add a deny rule for WEB01 to outside from DMZZone for extra precaution.
2. Verify or Add a rule to deny direct access to pix.
3. Update the PIX's passwd encryption vulnerability to CAN-2002-0954 [23](under review) The encryption algorithms for enable and passwd commands on Cisco PIX Firewall can be executed quickly due to a limited number of rounds, which make it easier for an attacker to decrypt the passwords using brute force techniques.
4. LOCK down incoming Syslog traffic to Syslog from certain hosts only
5. Use a router to act as a NTP server on the inside to simplify ACLs, instead of having all internal clients have to traverse the DMZ to update. This was in our original design, but it was forgotten.

[23] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0954

6. Reconfigure the SMTP Bastion Host- FOLLOW TCP STREAM feature of Ethereal to view the contents of the mail interchange and find the banner for the MAIL Bastion Host is listed as WEBSHIELD. This should be changed by configuring the mail host's banner to obscure our OS and internal IP addressing scheme(see Diagram 3.4—1).
7. Log and monitor the SMTP gateway This is probably our most "open" host besides our Web server, as in our decodes and nmap logs we find that it can indeed communicate with ANY internet HOST using ANY protocol. While this is a risk, we should take safeguards by allowing only outbound access and preventing any initiating packets from outside.
8. Lock down ICMP packets from your firewall and border router, using Rob Thomas' mini whitepaper on ICMP Packet Filtering[24]

It is important to perform network traces of different types of allowed protocols that egress out of the internal network toward the internet, such as SMTP. Microsoft Exchange not only banners out its build number, but also its internal IP addresses(see below)!!! Now a bad guy knows our internal IP scheme where the mailserver resides!

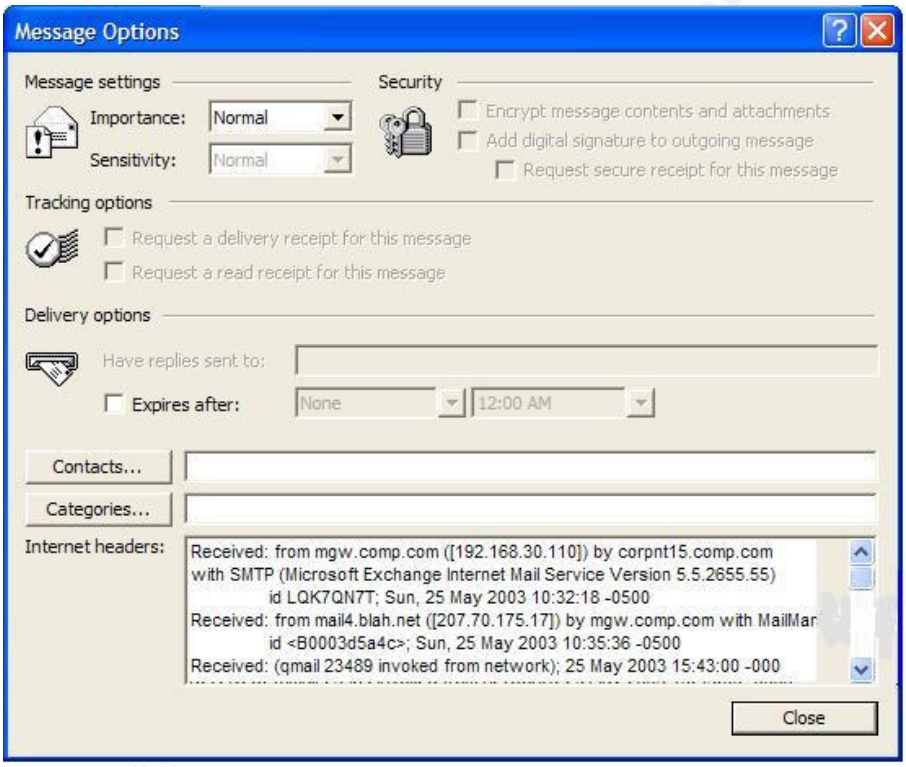


Diagram 3.4—1 SMTP header leakage

There are several ways to prevent mailserver's from stamping its banner on its SMTP traffic. One way is to use a separate SMTP bastion host, which GE will be deploying. Other ways are to obfuscate the banner by placing a Sendmail banner onn exchange server, such as described by Paul Robichaux25.

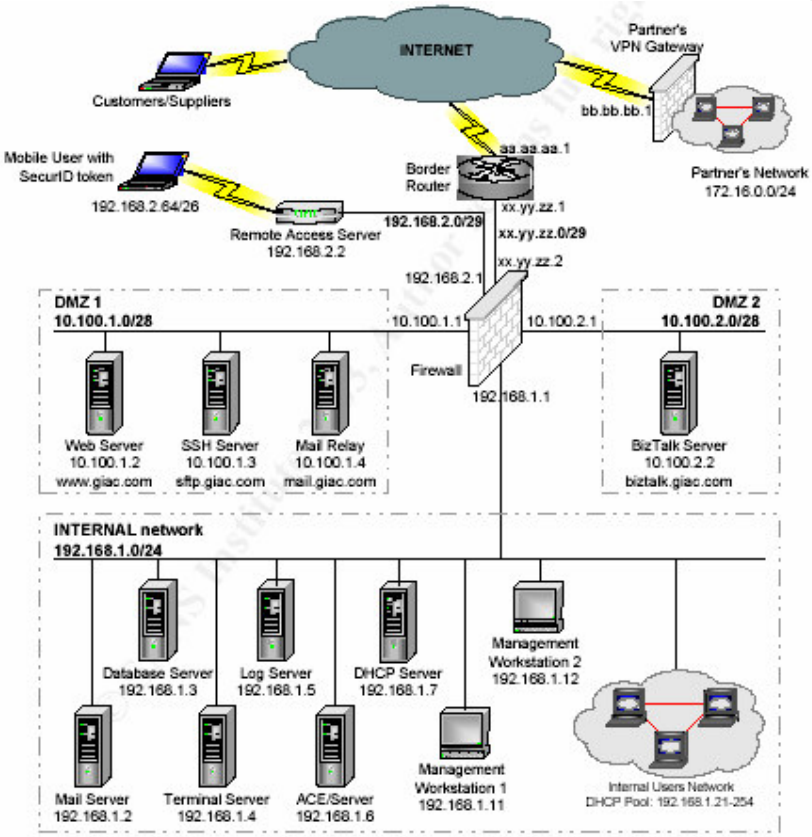
[24] Rob Thomas, March 12, 2003, http://www.cymru.com/Documents/icmp-messages.html
[25] Paul Robichaux, January 2002
http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=23155&pg=1&show=812

Assignment 4 - Hack Another's Design

4.1 Attack!

Ok, Auditing is tedious work. Now it is time to have a little harmless fun, as we now get to think like a hacker who wants to plunder GE. If we imagine we know nothing about the internal network for them…we must start from scratch.

We have chosen to attack Aloysius Johannes' design, who is listed as Analyst # 0366, in January 2003. His practical can be found at: http://www.giac.org/practical/GCFW/Aloysius_Johannes_Kolibonso_GCFW.pdf



4.1.1 Footprinting and Scanning-

We will approach the audit by first "pretending" that we know nothing about the GE web presence and domain zone information. We will use common tools to "footprint" GE's resources and public records, in order to focus our scanning on any networks and systems that we find publicly available.

This best simulates the actions that will be taken by a prospective hacker that desires to infiltrate GE's defenses. As in the Auditing of the Firewall section above,

we pull out our DIG, WhoIS View, WHOIS, and NSLOOKUP to determine the netblock and host names to focus our scanning attack.

4.1.2 Scanning-

This will allow us to check the responding hosts with our security policy.

4.1.3 Enumeration-

Intensive probing of exposed systems-After verifying what IP address and port assignments are permitted through the firewall, we will attempt to execute more profiling with trying to gain unauthorized access.

This will involve various tests that will attempt to identify what type of operating system that runs on a particular accessible host by sending stimuli that reveals banner checking and profiling by IP and TCP behavior.

4.2 Attack on the Firewall Vulnerabilities

4.2.1 Attack on the Firewall

Aloysius has chosen the Cyberguard firewall to protect his perimeter. We begin by searching for any vulnerabilities at:

4.2.1.1 Cyberguard Firewall Vulnerabilities research

We begin looking at the more obvious places for possible Cyberguard weaknesses.
http://www.kb.cert.org/vuls/html/search

http://www.securityfocus.com/search

http://cve.mitre.org

http://www.google.com

After searching the above and other "reputable" security sites, we are surprised that there are NO reported exploits or weaknesses with the Cyberguard firewall. This does not give us much to work with! But being tenacious, we search more to find the following link below, which was released by ICSA in mid 2002.

http://www.icsalabs.com/html/communities/firewalls/newsite/certification/vendors_4/CyberGuard/cyberguard.pdf

It seems there are several possible compromises were found by the ICSA's Network Security Lab team during its firewall testing with CyberGuard Firewall for UnixWare release 5.0P1 on a base OS of UnixWare release 2.1.3. Since Aloysius states his version is 5.0, we will assume that it has not been patched with PSU3 yet.

ISCA found in their testing that:

- IP Protocols 50 and 51 were not logged.
- The product did not log raw IP Protocols 1, 6, and 17 if the packets did not contain valid ICMP, TCP, or UDP header information respectively.
- The product did not complete a proper TCP handshake before passing TCP traffic through the product.[26]
- The product was found to be unable to block fragmented IP datagrams on <common> ports.

The test report goes on to say that Cyberguard provided a hotfix (0071) to resolve these issues. They also require tuneable kernel parameters to make the changes to correct the issues. We will attempt to attack with these finds as our ammunition.

4.2.1.2 Plan and mount attack based on the vulnerability

First we will attempt to perform more stealthy attacks on the firewall by using some non "quiet" commands of NMAP to the external IP address of the firewall. We don't want to raise Aloysius' eyebrows!

We begin by scanning for IP protocol leakage using:

nmap -sO -P0 -O -iR -T 3 xx.yy.zz.2

but this does not reveal anything interesting because it says all ports are open. Next we try to perform a Stealth SYN and ACK fragmented scans in order fragment the traffic we are sending to and through the firewall, to see if it indeed will plunge through the firewall.

Nmap -sS -P0 -f -O -vv -T 3 –p 1-1024 xx.yy.zz.2

Nmap -sA -P0 -f -O -vv -T 3 –p 1-1024 xx.yy.zz.2

And the result is:

```
Host  (xx.yy.zz.2) appears to be up ... good.
Initiating ACK Scan against  (xx.yy.zz.2)
Skipping host   (xx.yy.zz.2) due to host timeout
Warning: Packet fragmentation selected on a host other than Linux,
OpenBSD, FreeBSD, or NetBSD.  This may or may not work.
Nmap run completed -- 1 IP address (1 host up) scanned in 301 seconds
```

Hmmm, no luck in trying to pilfer through this firewall. We cannot tell if our attempts are getting logged. The paper says that Protocol 1, 6, and 17, ICMP, TCP, and UDP might not be logged if they have a valid header. This sounds like a lot of work to just get by without being logged, but we do note this feature. Maybe there is a reason that there are little to no exploits published on the internet about Cyberguard. Going all out, we forget about being clandestine and forget about detection.

We run another scan using a UDP scan, scanning it with TCP and ICMP:

nmap -sU -PT -PI -R -F -O -vv -T 5 cyberguard.com

and the result is even worse. We don't even see the host respond to us.

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

[26] ICSA Labs, reference given.

```
Host  (xx.yy.zz.2) appears to be down, skipping it.

Note: Host seems down. If it is really up, but blocking our ping
probes, try -P0

Nmap run completed -- 1 IP address (0 hosts up) scanned in 7 seconds
```

We try to open a telnet session directly to the firewall next, but that fails as well.

```
C:\WINDOWS\system32>telnet xx.yy.zz.2

Connecting To xx.yy.zz.2...Could not open connection to the
host, on port 23: Connect failed
```

Ok, so if we cannot get to it directly, lets try to resort to crude methods, so we will spoof our address. First we will look at the tracert to the site, and look at the next to last entry, which should be the border router.

```
C:\WINDOWS\system32>tracert xx.yy.zz.2

Tracing route to comcast.net [24.153.64.7]
over a maximum of 30 hops:

  1   14 ms 15 ms  15 ms  10.1.1.1
  2   16 ms 14 ms  23 ms  10.2.2.2
  3   17 ms 15 ms  15 ms  10.3.3.3
  4   15 ms 20 ms  20 ms  gbr6dkdkfk.dkdk.ddd [10.4.4.4]
  5   28 ms 18 ms  16 ms  tbr2-p013701.dlstx.2l32 [10.5.5.5]
  6   33 ms 30 ms  30 ms  10.6.6.6
  7   32 ms 33 ms  31 ms  xx.yy.zz.2
Trace complete.
```

We can see that the last hop before the firewall is 10.6.6.6, so we fashion one last NMAP test by spoofing that address to see if the firewall will think we are its border router.

nmap -sS -PT -PI -S 10.6.6.6-R -F -O -vv -T 3 xx.yy.zz.2

Note that this attack is not really designed to give us any response, as there is no way for the return packets to get back to us. Well, we are mad, so now we will try to do further damage.

4.2.2 Denial of Service Attack

Assumptions- Our assumptions is that we have 50 DSL/Cable Modem users' compromised machines at our disposal.

Tools- We will assume that the package that has been installed surreptitiously on each of the 50 machines is the Tribal Flood Network 2000 (TFN2K). This is a classic distributed master-zombie slave tool[27] that allows an attacker to configure those zombies to mount up to 4 different types of flood methods. TFN2K will randomly alternate attack patterns between ICMP, UDP, SYN and Smurf methods to one or more hosts.

[27] January 15, 2001, http://www.cert.org/incident_notes/IN-99-07.html

We can even alter the packets to further cause havoc with this resistant firewall we have been toying with.

The ATTACK - We mount the attack from our master by sending out a blowfish encrypted IP target package to our zombies, who are waiting for us, and the immediately start to bombard the xx.yy.zz.2 address from 50 different distributed IP addresses.

Judging from typical cablemodem users in North America, Broadband reports a typical upstream dataflow of about 200-250 kbps for most broadband users[28]. So dividing up 1544 kbps up by 200 means that it will only take about only 8 to 9 clients that are running to mount this attack.

The Results- We try to ping the target IP address through a open proxy that we found yesterday on the internet, and there is no response from the firewall. GOOD! We guess that it is the border router that hanging, or even an upstream ISP router that is choking due to the mass of traffic trying to flow downstream to the firewall. (remember that the connect is 10 or 100 mbps between the border router and the firewall)

Possible Countermeasures This is good, but how long will this last? It is difficult to recover from a directed attack, but here are a couple of ways to mitigate the denial:

1. Develop a VERY good relationship with your ISP to assist you in configuring your/there routers when a DDOS is coming down their pipe to you. It is far better to stop it at their end before it gets to your network. They can use rate limiting and/or Quality of Service, or simply block that netblock if it is not distributed. This is a good RFC- ftp://ftp.isi.edu/in-notes/rfc2827.txt
2. Patch your hosts and gateway boxes
3. Disallow ICMP to broadcast and multicast addresses from the outside

[28] http://www.dslreports.com/stest/0 this requires a free signup and login, but is well worth the time.

How to tell if your Windows machine is being attacked with a denial of service

Microsoft publishes a good article on SYN Flooding and how it occurs on their site[29] and shares a simple way to discern if you are being attacked:

The idea is to look for multiple unexplainable "SYN_RECEIVED" state entries in the NETSTAT response.

```
netstat -n -p tcp
```

Active Connections

```
  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1030         127.0.0.1:1032         ESTABLISHED
  TCP    127.0.0.1:1032         127.0.0.1:1030         ESTABLISHED
  TCP    10.57.8.190:21         10.57.14.154:1256      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1257      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1258      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1259      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1260      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1261      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1262      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1263      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1264      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1265      SYN_RECEIVED
  TCP    10.57.8.190:21         10.57.14.154:1266      SYN_RECEIVED
  TCP    10.57.8.190:4801       10.57.14.221:139       TIME_WAIT
```

4.2.3 Internal System attack

4.2.3.1 Select the host

In looking at our quarry, we see the low hanging fruit of the Aloysius' web server, but we want more than just IIS. We would like to use some IIS exploits with which to get at the real assets of Giac Enterprise: their database. It appears that their Business to business Biztalk solution also is directly connected to this MS SQL server as well, so as an attacker we might be able to find out more about GIAC Enterprises' business partners to gather politically dangerous information to use for a little "coercion." .

Target: SQL Server DATABASE

First to OWN their database, I must go through the Web Server. And looking at Aloysius' service pack history, SP2 is installed on the database server. All I need to do first is to login as a valid user…using an anonymous proxy of course, as to not reveal my tracks.

Aloysius mentions that he has applied URLSCAN and IISLockdown to his webserver, as well as OS patches. It is to be noted that URLSCAN needs to be updated periodically like antivirus signature files, and it acts as an ISAPI filter on IIS. URLSCAN will not prevent the following:

Cookie poisoning

Hidden field manipulation

Parameter tampering

SQL Injection

[29] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q142641&sd=tech

4.2.3.2 The attack

Since this attack is above layer 4 beyond our network comfort zone, we look to some internet resources for help, which are in ample supply. We look at several types of SQL exploits:

SQL Slammer worm, looking on UDP port 1433
SQL Injection into an ASP web form

Since the SQL Slammer worm was more of a self propagating worm, we will focus on using SQL Injection methods to try to control, own, and steal any data that seems valuable to us.

A SQL Injection attack is a good example of the ways hackers today are bypassing the rock solid walls of the network firewall and dancing over the web services in OSI layers 5-7.

A SQL injection is an attack that can change the way an unprotected web based application will interacts with the database it is designed to update and read. It is simple to add extra parameters into a web based form, and have it "manipulate" the data in the database. This includes adding information into even a "read only" database. Pete Finnigan, for example, in his article SQL Injection and Oracle, Part One, states:

> "… that by adding a single quote (') to the parameters, it is possible to cause a second query to be executed with the first.
>
> An attack against a database using SQL Injection could be motivated by two primary objectives:
>
> 1. To steal data from a database from which the data should not normally be available, or to obtain system configuration data that would allow an attack profile to be built. One example of the latter would be obtaining all of the database password hashes so that passwords can be brute-forced.
> 2. To gain access to an organisation's host computers via the machine hosting the database. This can be done using package procedures and 3GL language extensions that allow O/S access.[30] "

Here is a short example of how easy it is to inject information at will into the SQL database.

An excellent brief tutorial, and is explained here in part, by Mitchell Harper, http://www.devarticles.com/art/1/138/3

SQL Injection tutorial by Mitchell,

http://localhost/products.asp?productId=0%20or%201=1

Each %20 in the URL represents a URL-encoded space character, so the URL really looks like this:

[30] Pete Finnigan, http://www.securityfocus.com/infocus/1644

http://localhost/products.asp?productId=0 or 1=1

When used in conjunction with products.asp, the query now looks like this:

```
select prodName from products where id = 0 or 1=1
```

Using a bit of know-how and some URL-encoding, we can just as easily pull the name of the products field from the products table:

http://localhost/products.asp?productId=0%20having%201=1

This would produce the following error in the browser:

Microsoft OLE DB Provider for SQL Server (0x80040E14)
Column 'products.prodName' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
/products.asp, line 13

Now, we can take the name of the products field (products.prodName) and call up the following URL in the browser:

http://localhost/products.asp?productId=0;insert%20into%20products(prodName)%20values(left(@@version,50))

Here's the query without the URL-encoded spaces:

http://localhost/products.asp?productId=0;insert into products(prodName) values(left(@@version,50))

Basically it returns "No product found", however it also runs an INSERT query on the products table, adding the first 50 characters of SQL server's @@version variable (which contains the details of SQL Server's version, build, etc) as a new record in the products table.

In a real-life situation, you would obviously have to exploit the products table more than this as it would contain dozens of other fields, however the methods would still remain the same.

To get to the version, it's now a simple matter of calling up the products.asp page with the value of the latest entry in the products table, like so:

http://localhost/products.asp?productId=(select%20max(id)%20from%20products)

What this query does is grab the ID of the latest row added to the products table using SQL server's MAX function. The result outputs the new row that contains the SQL server version details:

Got product Microsoft SQL Server 2000 - 8.00.534 (Intel X86)

This method of injection can be used to perform a numerous amount of tasks, however the point of this article was to give tips on how to prevent SQL injection attacks, which is what we will look at on the next page.[31]

With this type of exploit, after we are able to pass information such as an anonymous email address to the SQL server, we can have it send all or some of the email addresses of fortune saying customers to a SMTP server in Biloxi, Mississippi by

31

instructing the SQL server to send mail directly to the Exchange server using the domain administrator's account. Maybe tomorrow we will go for his business Partner's email addresses that are in the next table in the db.

NOTE: With this type of exploit, it is relatively easy to bypass the security of a traditional network firewall. While their role is still critical, it is just as critical to have application and database layered defenses as well.

4.2.3.3 Avoiding detection

It is most likely that Aloysius is too busy watching his network syslogs and IDS log than to worry about the database, yet that is where his greatest risk lies. I am sure that he can see my source IP appear into the log into the web services host, but my IP address is masked by that anonymous proxy that I found last night.

If I wanted to, I could create a couple of database tables that could include executable code with which to invoke cmd.exe and download a certain file called nc.exe. Netcat will allow me to load it and listen for any launching point attack that I want. Since I have local access, and this is a domain member machine, tomorrow I shall try to download a remote sniffer with which to promiscuously pick up user names and passwords from the wire.

4.2.3.4 Countermeasures

4. To prevent SQL injection, it is good to be the wise administrator and apply all patches, but here are some steps to lock down the web services as well as the database.
5. Create a reverse proxy to protect the WEB server from the internet, and to do filtering on form lengths, etc on a separate host in the architecture, not locally
6. Apply good programming security best practices with your application and script design-Microsoft sent all of their developers to a mandatory 2 week security programming workshop!
7. Never use sa and default password; instead create unique user accounts.
8. Remove all unneeded scripts, triggers, and stored procedures, as some of the crafted SQL injection scripts will attempt to use the vanilla out of the box procedures such as xp_cmdshell and xp_grantlogin
9. Replace dangerous injectable single quotes into more benign double quotes
10. Perform validation on your fields by numeric/alpha and length.
11. Use stored procedures to write to the database for the users, instead of allowing them to directly write to it by allowing them access tables or views.

All of this is hacking effort istestament to the importance that now the network, database, and developer engineers all work together to put together a solid and secure architecture. From looking at recent security strategies, it appears that our IT future will require us to get along with one another. Security will require skills and knowledge from Programming, Infrastructure, and Databases.

References

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2003/W2003HG/SGCH08.asp

http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=4&tabid=12

http://www.microsoft.com/downloads/details.aspx?familyid=9552D43B-04EB-4AF9-9E24-6CDE4D933600&displaylang=en

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml#info

http://www.cymru.com/Documents/secure-ios-template.html

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tip1r/p1ftip2.htm#1019682

http://www.cisco.com/cgi-bin/Support/Cmdlookup/ios-command-lookup.pl?type=reference&query=&paging=25&counter=0&sa=Submit

http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-07/0039.html

http://www.pasadena.net/cisco/secure.html

http://nsa2.www.conxion.com/cisco/guides/cis-1.pdf

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/scacls.htm#12853

Pix Firewall and stateful Firewall security, Cisco Systems, http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

Track 2-Firewalls 101: Perimeter Protection with Firewalls, SANS Institute, Module 3, page 94, 2002.

Steve Textor, April 29, 2002, The Installation and configuration of a Cisco PIX Firewall with 3 Interfaces and a Stateful Failover Link, http://www.sans.org/rr/firewall/cisco_pix.php

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml#info

from Cisco.com, Cisco PIX Firewall Series, Features and Benefits, http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

Track 2-Firewalls 101: Perimeter Protection with Firewalls, SANS Institute, Module 3, page 94, 2002.

Aloysius Johannes, GCFW analyst 0366, http://www.giac.org/practical/GCFW/Aloysius_Johannes_Kolibonso_GCFW.pdf

http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb727.html#1064072
time clocks http://www.eecis.udel.edu/~mills/ntp/clock1a.html

My article on cisco vpns, brent Whitmore

http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci854037,00.html

SANS Day 4, Track2, VPNs, Book 2.4, p.88

Taken loosely from Windows 2000 Server online help, Microsoft Corporation.

Taken loosely from Windows 2000 Server online help, Microsoft Corporation.

http://www.oration.com/nortel-bay/ces-faq.shtml#Q5,

Robert Moskowitz, from http://sunsite.uakom.sk/sunworldonline/swol-06-1998/swol-06-ipsec.html

http://www.grc.com , Steve Gibson has created a compendium of easy to read infosec materials on his site.

Rob Thomas, March 12, 2003, http://www.cymru.com/Documents/icmp-messages.html

Paul Robichaux, January 2002 http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=23155&pg=1&show=812

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q142641&sd=tech

http://www.kb.cert.org/vuls/html/search

http://www.securityfocus.com/search

http://cve.mitre.org

http://www.google.com

http://www.icsalabs.com/html/communities/firewalls/newsite/certification/vendors_4/CyberGuard/cyberguard.pdf

[1] January 15, 2001, http://www.cert.org/incident_notes/IN-99-07.html
[1] http://www.dslreports.com/stest/0 this requires a free signup and login, but is well worth the time.
Mitchell Harper, http://www.devarticles.com/art/1/138/3
1 Pete Finnigan, http://www.securityfocus.com/infocus/1644
a good article on network rate limiting ftp://ftp.isi.edu/in-notes/rfc2827.txt

Appendix A

PIX processing order Golden rule-The State table for traffic is checked before the ACL ruleset. IF an ACL match occurs with subsequent packets, the PIX will route the packet using its static route table. Order of processing when a responding packet enters a PIX interface can be thought of like this:

Check the State table for a match

If allowed, check the ACL

If allowed, route to directly connected networks, or use Route table to switch packet to adjacent interface for next hop

Apply the proper NAT to the packet