Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst Certification Practical Assignment

Version 1.5e

SANS Rocky Mountain 2001 – Denver, Colorado

By: John Palumbo

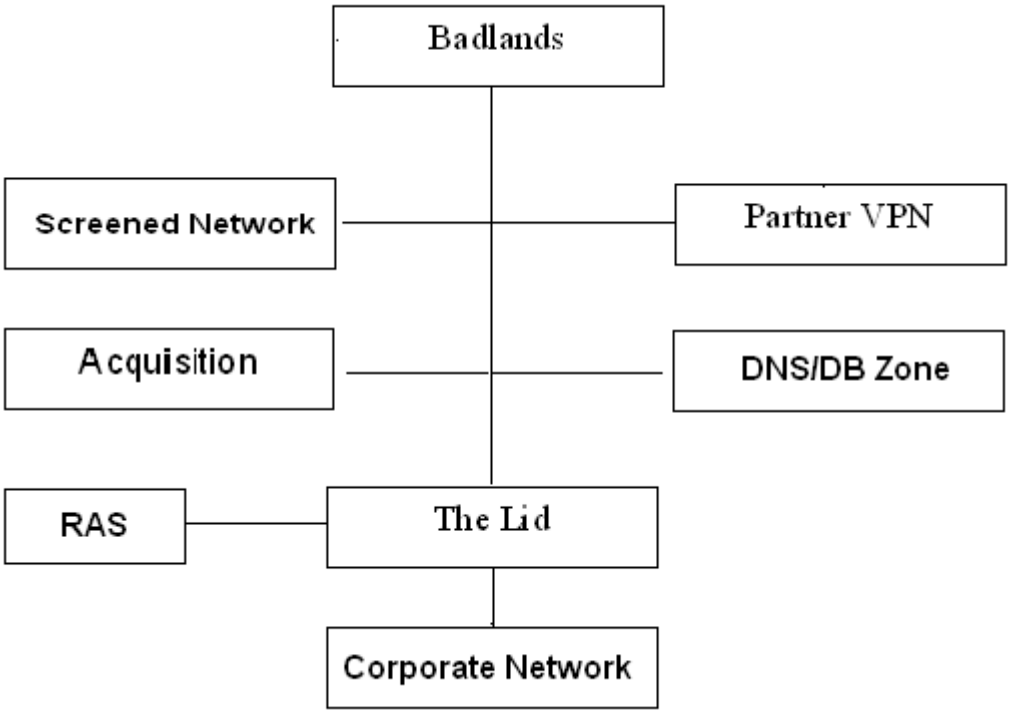
Assignment 1 – Security Architecture

"Guarding the Fortune Cookie Jar"

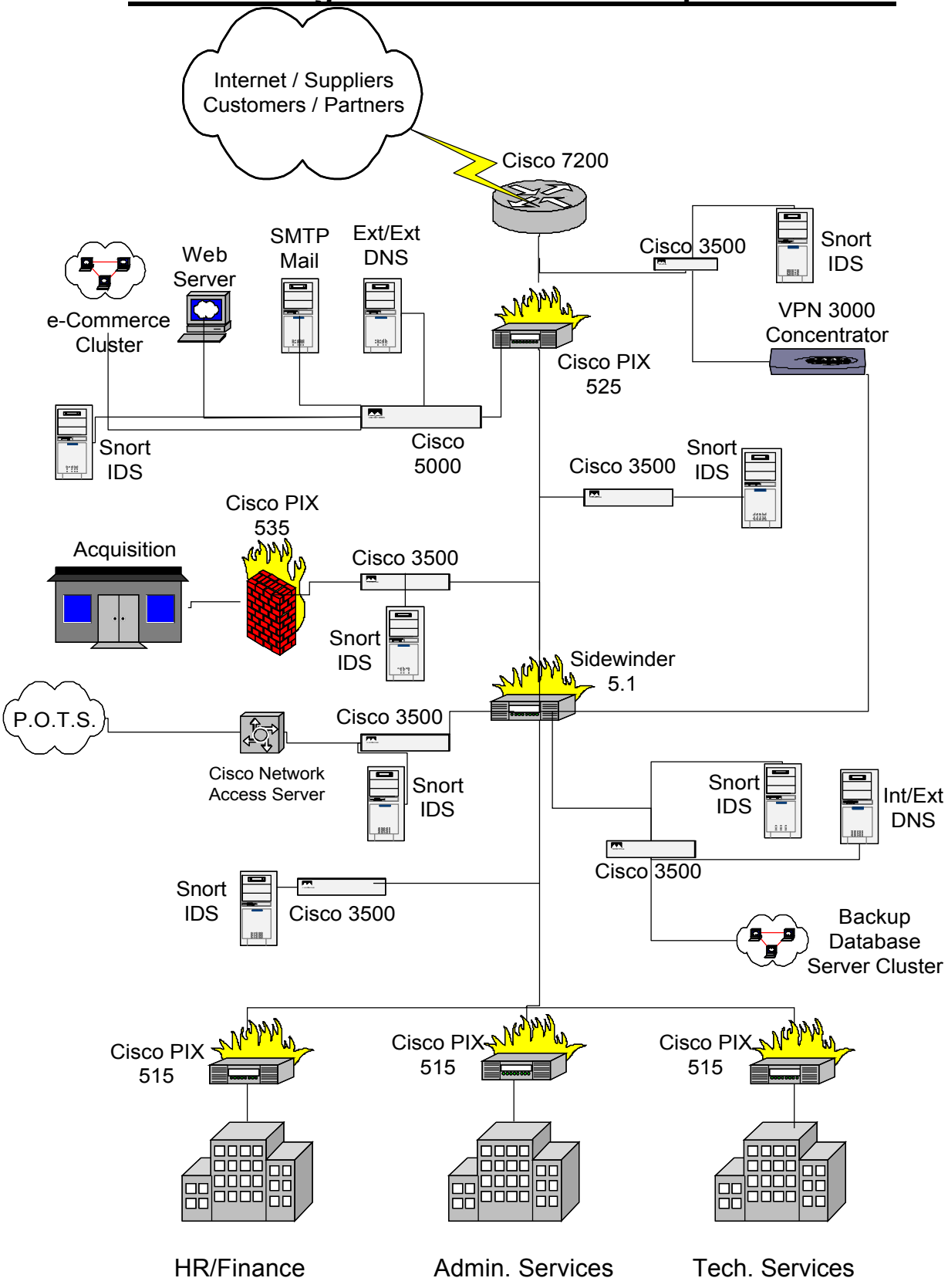
GIAC Enterprises Security Architecture

The modular overview of the GIAC Enterprises Security Architecture is shown below. This modular design assists in providing smaller network segments in order to simplify the installation and administration of the security architecture.

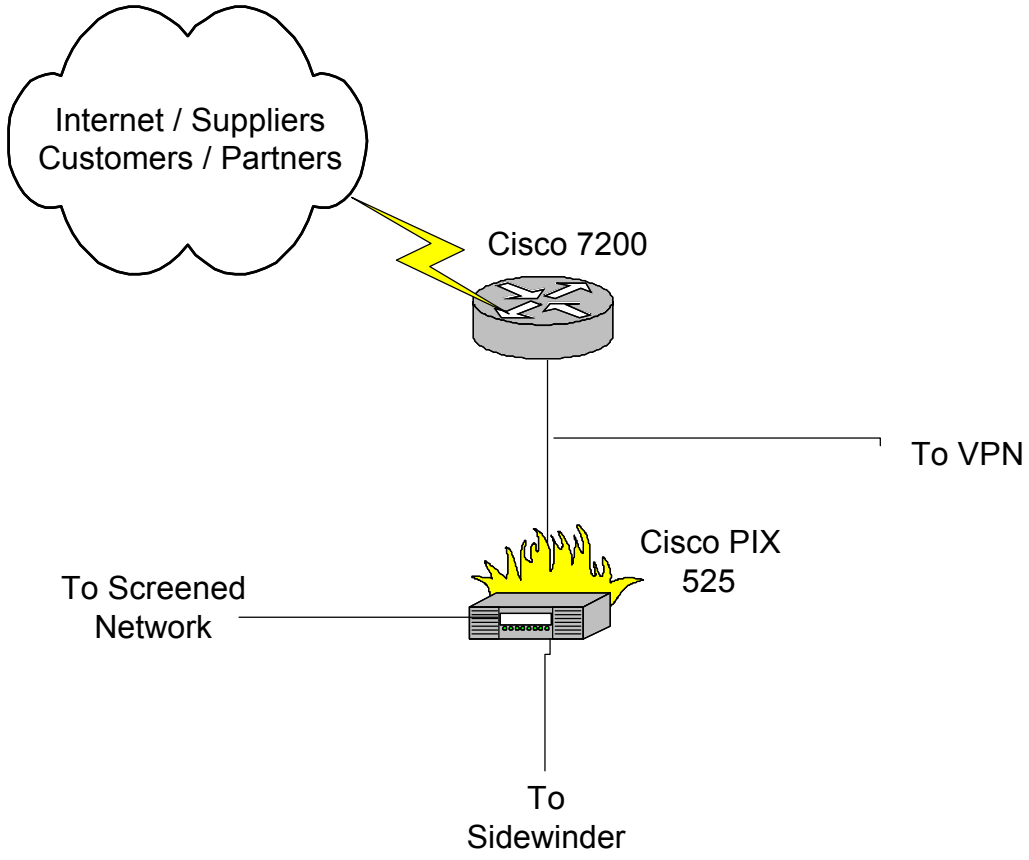
From this point forward, the GIAC Enterprises Security Architecture will be referred to as SAGE (**S**ecurity **A**rchitecture for **G**IAC **E**nterprises) for ease of reference.



Network Diagram for the GIAC Enterprise Network



“Badlands”

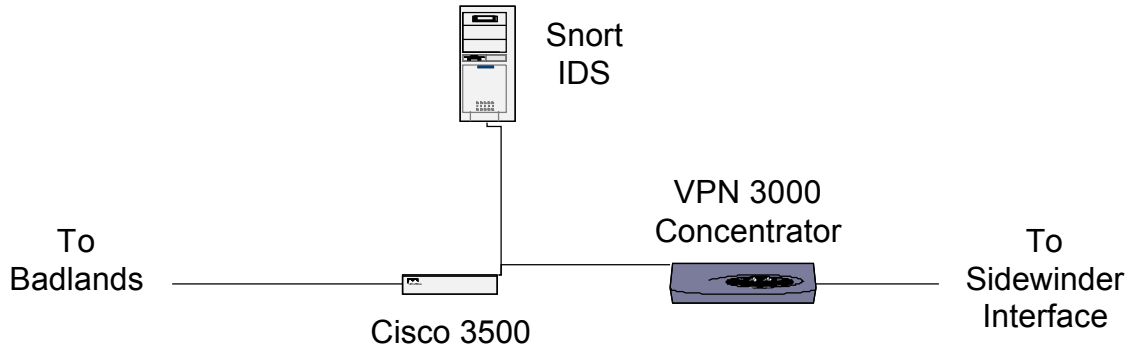


The first module in SAGE is the “Badlands” module. This is the outermost section of the GIAC Network and through this border router is the primary point of connection for all data entering the GIAC Network from untrusted sources, namely the Internet.

With a singular T-3 connection, the Cisco 7204 router will be the device utilized for the border router. This device was chosen due to its capacity, redundancy and expandability. With the 7204, GIAC Enterprises, Inc. will be able to enhance its bandwidth and increase redundancy as needed with minimal additional cost. The router configuration, as well as all other device configurations within SAGE, will be implemented according to the GIAC Enterprises security policy.

Also establishing a position inside the “Badlands” is the Cisco Secure PIX 525 Firewall device. The PIX 525 was chosen because of its speed, redundancy, scalability and failover capabilities. The Cisco PIX 525 was also chosen because it utilizes a form of stateful inspection enabling the firewall to track source and destination addresses, TCP sequence numbers, TCP packet flags, and port numbers.

“The VPN”



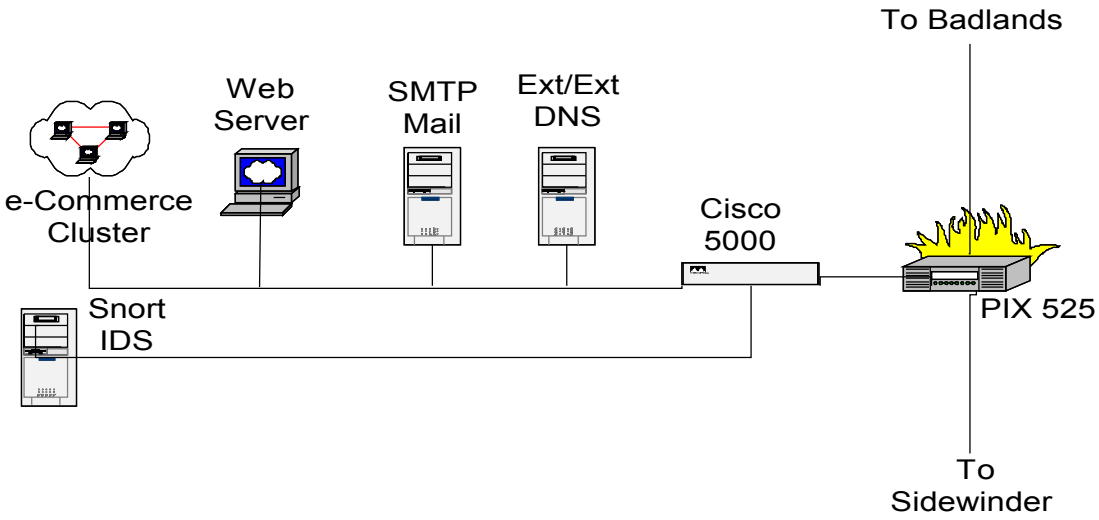
The VPN segment of SAGE contains a Cisco Catalyst 3512XL Switch, a computer running SNORT as its Intrusion Detection System software, and the Cisco VPN 3030 Concentrator providing the VPN services to the GIAC Enterprises, Inc. partners.

The Cisco VPN 3030 Concentrator VPN solution was chosen for this application for several reasons, primarily speed (50 Mbps encryption throughput) and the fact that there is an available hardware encryption module with a redundant module option. The Cisco 3030 also has a complete upgrade path and redundancy options to enable upgrading the unit to meet demands with minimal cost involved.

SNORT will be used as the Intrusion Detection System solution throughout SAGE because it is a multi platform open source IDS that can be quickly deployed and configured on any segment within the GIAC Enterprise network, not to mention it undoubtedly provides the best bang for the buck.

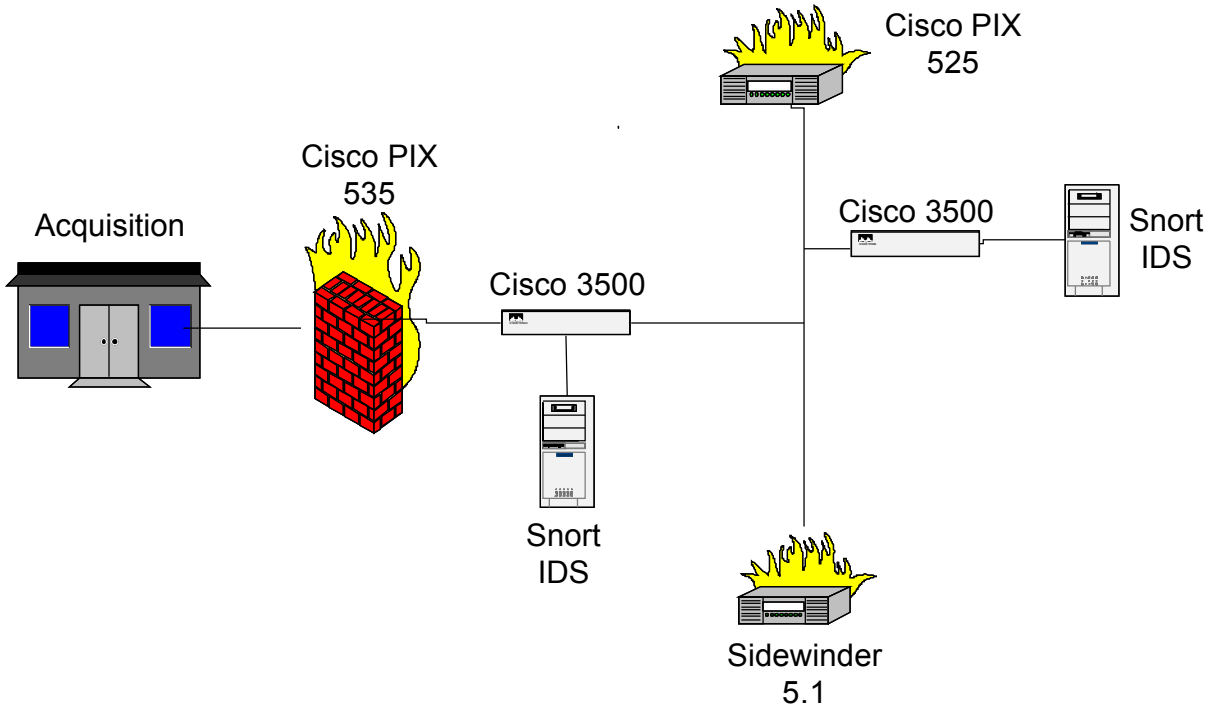
The Cisco 3512XL switches provide expandability in that they are Gigabit ready and stackable up to 16 units to provide increased port density when needed. Switches also make it more difficult to sniff the network segments they serve.

“The Screened Network”



Located in the screened network segment of SAGE is the GIAC Enterprises Web Server, an SMTP Forwarding Server that provides content scanning/filtering for e-mail messages as well as virus scanning, an External/External DNS Server (GIAC is implementing Split/Split DNS[1]) for name resolution of servers external to GIAC Enterprises, an e-Commerce cluster which houses the database servers which are updated ONLY from the backup database server located in the DNS/DB zone, a SNORT IDS, and a Cisco Catalyst 5509 Switch. The Catalyst 5509 provides redundancy, expandability and Gigabit speeds for optimum backend data processing between all servers in the e-Commerce cluster.

“The Acquisition”



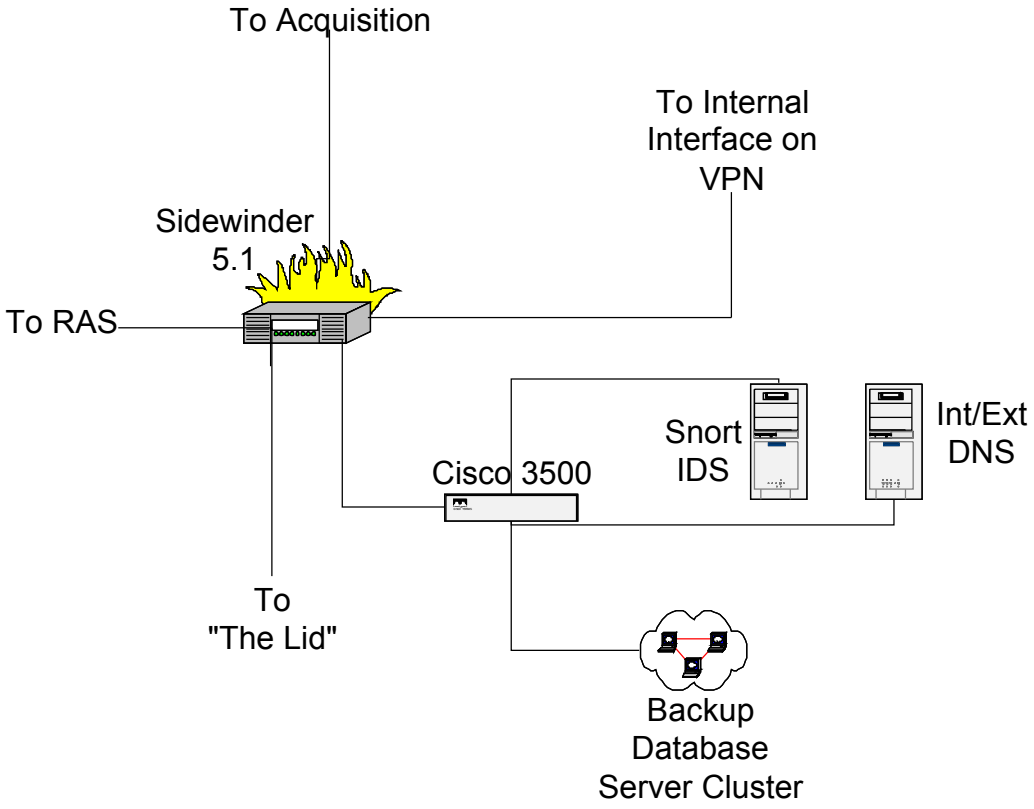
The Acquisition module of SAGE consists of two Cisco PIX 535 Firewall devices, one at the Acquisition location and on site at GIAC Enterprises. The two Firewalls are connected across a T-3 line as a Site-to-Site VPN using IPSec. GIAC Enterprises will provide all of the Internet connectivity needs of the acquired company, i.e. e-mail, Internet browsing, etc., through this VPN connection.

Also placed in the Acquisition segment of SAGE are a SNORT IDS and a Cisco 3512XL switch.

Between the Cisco PIX 525 in the “Badlands” segments of SAGE and the Sidewinder 5.1 Firewall, a Cisco 3512XL Switch and a SNORT IDS are placed to detect for any penetration attempts coming from the “Badlands” segment. From this point, the PIX 525 terminates into a Sidewinder 5.1 Firewall.

The Sidewinder Firewall product was chosen as a compliment to the PIX 525 Firewall located in the “Badlands” segment of SAGE. The Sidewinder is an application gateway firewall, enabling the ability to filter the application layer traffic that will flow from the screened network segment. For example, the Sidewinder Firewall provides the ability to filter HTTP based traffic on ports, headers, version, and maximum length or FTP traffic for Put, Rename, Del, and Get commands.

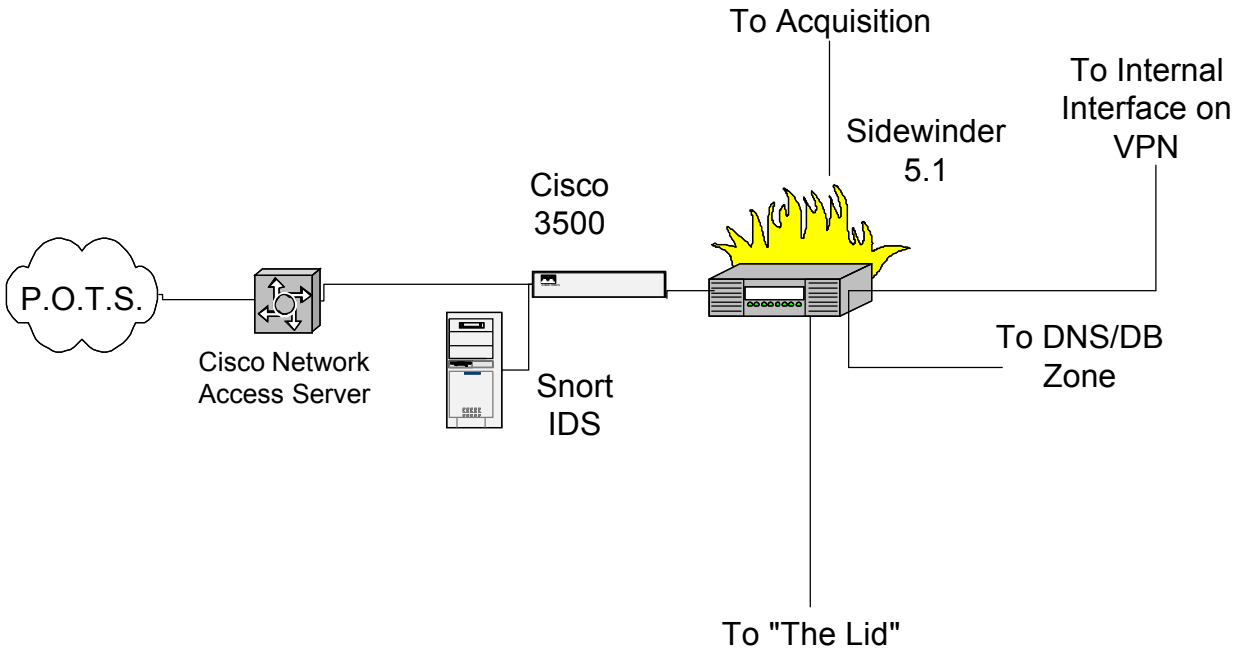
“The DNS/DB Zone”



The DNS/DB Zone consists of the usual Cisco 3512XL and the Snort IDS Server, but in addition is an Internal/External DNS server which is the second of three DNS servers used to implement a split/split DNS architecture. The split/split DNS Architecture increases your protection from an attacker who attempts to poison the DNS cache of your DNS servers by shielding the Internal DNS from the External DNS.

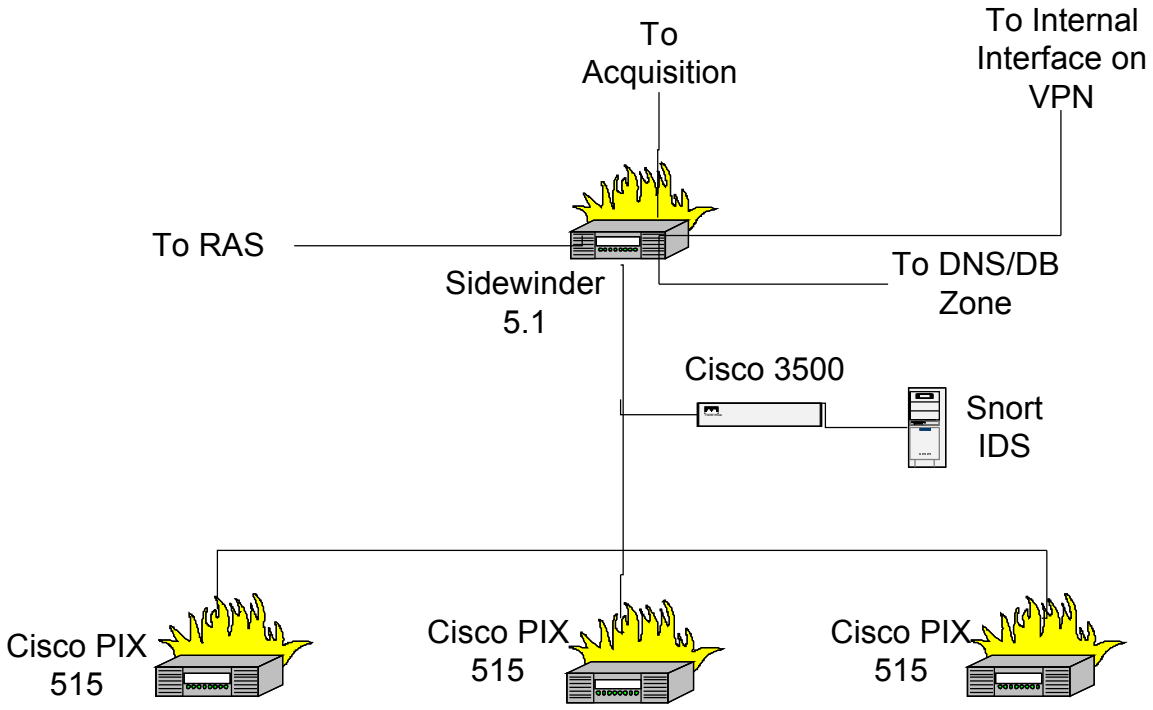
Also located in this zone is a backup e-commerce database cluster. This cluster receives updates from the Master database located on the internal network of GIAC Enterprises. The Master database updates the backup e-commerce database cluster via a one way connection, which in turn updates the e-commerce cluster located in the screened network segment. This is done to limit the ability of compromising the Master database.

RAS
(Remote Access Service)



The RAS module of SAGE was set up to establish a method of connecting corporate users to the GIAC Network without them having to dial an Internet Service Provider and enter via the VPN. A Cisco Network Access Server is utilized as the authentication mechanism for users that dial in. Also located in this segment are the usual Cisco 3512XL and the SNORT IDS Server.

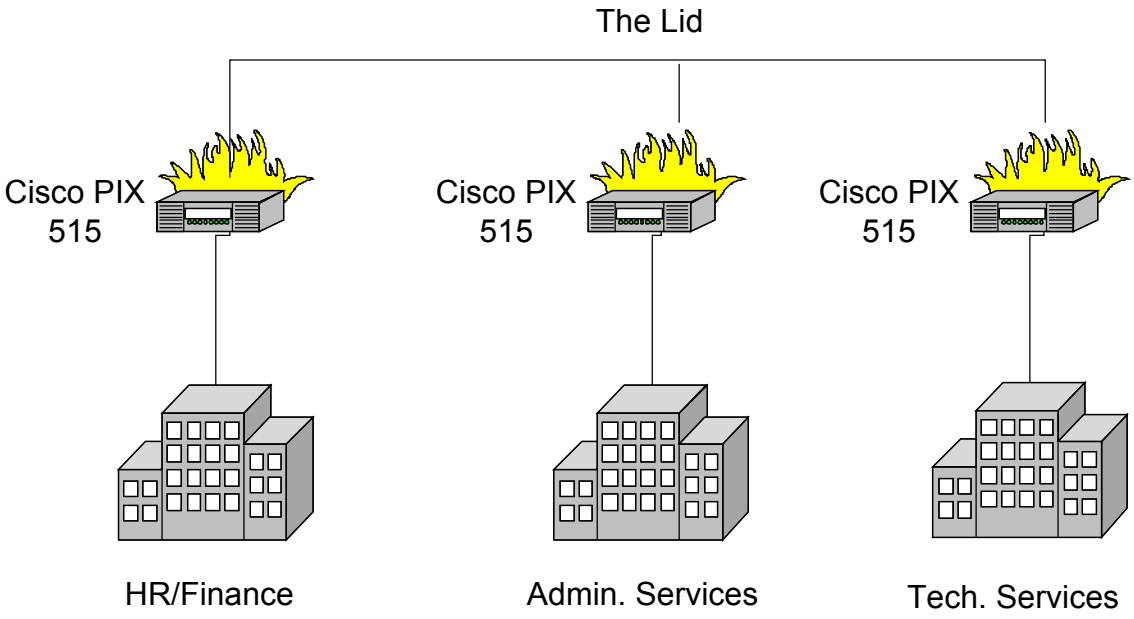
"The Lid"



The Lid, as its name implies, is the last SAGE segment to protect the “Fortune Cookie Jar” or the internal network of GIAC Enterprises.

The segment entering from the PIX 525 contains a Cisco 3512XL switch and a SNORT IDS to monitor for any attack signatures or abnormalities that make their way into this most sensitive segment. From this point, each of the GIAC Departments sits behind a Cisco PIX 515 to lock any remaining doors that may be opened.

Corporate Network



The final segment of SAGE is the Corporate Network segment. Each department within the Corporate Network has been segmented in accordance with that department's business function. The HR/Finance Department does exactly what its name implies. All payroll, AR and AP functions as well as Human Resources functions are carried out in this department. The HR/Finance department is then segmented from the remaining two departments by the Cisco PIX 515 Firewall device located in the Lid segment. This is done to prevent any of the other departments from accessing sensitive information to which they are not privy.

Admin. Services are the support group for the HR/Finances and the Tech. Services Departments. Admin. Services concentrates primarily on Secretarial and office support functions such as ensuring the availability of all office supplies and the shipping and receiving functions of GIAC Enterprises, Inc.

Finally there is the Tech. Services Department. This is the segment where all of the Syslog servers, primary database servers, corporate back-up servers, file servers, print servers, etc., and all technical administrative personnel are located.

Assignment 2 – Security Policy

The need for a security policy may well be the most important tool in protecting information stored on computer systems. Before security can truly be enforced, an unambiguous policy governing information access must be developed. There must be specifics outlined in the policy dealing with issues such as who has access to what, how the company will react to violations of the policy, how information is to be transmitted to others, and how client information is to be handled. There are of course many other items that could be added to this list, but that is beyond the scope of this assignment.

The policies in this document have been drawn from many resources, namely "Site Security Handbook" (RFC 2196) [2] and "GIAC Basic Security Policy" version 1.34.[3] I have chosen to implement Issue Specific Policies because to develop more comprehensive policies is beyond the scope of this assignment.

Issue Specific Policy # 1.2: Hours of Operation

GIAC Enterprises Inc. will have a complete Information Systems staff on the premises twenty-four hours a day and an on call emergency staff will be available during the holidays.

Issue Specific Policy #1.3: Password Policy

All passwords will be between 7 and 9 characters in length and shall consist of at least one letter, one number, and one punctuation symbol.

Issue Specific Policy #2.2: IP Addressing

The purpose of this policy is to document the IP Addressing of the GIAC Enterprises network.

All IP addressing within the GIAC Enterprises, Inc. network will conform with RFC 1918, "Address Allocation for Private Internets" at http://www.ietf.org/frc/rfc1918.txt?number=1918.

Registered Public IP Address Assignments:

GIAC E-mail (mail.fortune-cookies.com) –	X.15.0.5 subnet 255.255.255.0
GIAC External DNS (auth.fortune-cookies.com) –	X.15.0.6 subnet 255.255.255.0
GIAC Web Site (www.fortune-cookies.com) -	X.15.0.7 subnet 255.255.255.0

Unregistered Public IP Address Assignments:

GIAC VPN 3030 External Interface – X.15.0.4 subnet 255.255.255.0
Acquisition Cisco PIX 535 External Interface – X.65.0.1 subnet 255.255.255.0
GIAC Cisco PIX 535 External Interface – X.15.1.1 subnet 255.255.255.0

Issue Specific Policy #3.1: Cisco 7204 Border Router Configuration

The purpose of this policy is to document the running configuration of the Cisco 7204 border router located in the Badlands segment of SAGE.
Note: Since it is beyond the scope of this assignment, this document will contain only the access-control list associated with this router instead of the entire router configuration.

```
version 12.2

!       Turns off small services (chargen, echo, discard) to eliminate associated exploits.
no service tcp-small-servers
no service udp-small-servers

!       Block Source Routing to aid in preventing IP Spoofing.
no ip source-route

!       Block against Smurf attacks.
no ip directed-broadcast

!       Turns off Finger server to eliminate associated exploits.
no service finger

!       Turns off HTTP for router configuration.  Router should be configured from the
!       console.  This is normally done by default but it is better to error on the side of
!       caution.
no http server

!       Turns off bootp (DHCP).  The IP address for the router should be static.
no ip bootp server

!       Turns off snmp to eliminate associated exploits.
no snmp-server

!       Filter all ICMP traffic to make information gathering more difficult.
Access-list 108 deny  icmp any any

!       Blocks loopback and reserved ip addresses to aid in preventing IP Spoofing.
access-list 108 deny   ip 192.168.0.0 0.0.255.255 log
access-list 108 deny   ip 127.0.0.0 0.255.255.255 log
access-list 108 deny   ip 172.16.0.0 0.15.255.255 log
access-list 108 deny   ip 10.0.0.0 0.255.255.255 log
access-list 108 deny   ip 224.0.0.0 0.255.255.255 log
access-list 108 deny   ip 240.0.0.0 7.255.255.255 log
access-list 108 deny   host 0.0.0.0 log
```

```
!       Blocks Net BIOS Services to eliminate associated exploits.
access-list 108 deny tcp any any eq 135 log
access-list 108 deny udp any any eq 135 log
access-list 108 deny udp any any eq 137 log
access-list 108 deny udp any any eq 138 log
access-list 108 deny tcp any any eq 139 log
access-list 108 deny tcp any any eq 445 log
access-list 108 deny udp any any eq 445 log

!       Block Remote Procedure Call (RPC), NFS and lockd services.  RPC allows for
!       devices to execute programs on other devices and NFS and lockd are services
!       that are vulnerable to RPC exploits.
access-list 108 deny tcp any any eq 111 log
access-list 108 deny udp any any eq 111 log
access-list 108 deny tcp any any eq 2049 log
access-list 108 deny udp any any eq 2049 log
access-list 108 deny tcp any any eq 4045 log
access-list 108 deny udp any any eq 4045 log

!       Block X-Windows ports to eliminate associated exploits.
access-list 108 deny tcp any any range 6000 6255  log

!       Apply access-list 108 to the routers external interface
int eth0
 ip access-group 108 in

!       Add a warning banner to strengthen you position if you are ever in a criminal or
!       civil lawsuit with an attacker that has gained access to your system.
banner motd ^C
        Authorized personnel only!  Unauthorized use of system is unlawful
and may be subject to civil or criminal penalties.
Use of the system is monitored and logged.  The logs may
be used as evidence in the court of law.
^C

!       Limit the local access to the router so that someone can not just obtain access
by !    sitting at the console
line con 0
 password XXXXXXXX      !  XXXXXXXX is a difficult password to guess.
 login local
 exec-timeout 2 0
line aux 0
 password XXXXXXXX      !  XXXXXXXX is a difficult password to guess.
 login local
```

```
!       Deny remote access to the router.  Since there is twenty-four hour coverage in
!       the building, to add the risk of allowing remote router access is unwarranted.
access-list 15 deny any
line vty 0 4
 access-class 15 in
 exec-timeout 0 1
 login local
 transport input none

end
```

Issue Specific Policy #3.2: <u>Cisco PIX 525 Border Firewall Configuration</u>

The purpose of this policy is to document the running configuration of the Cisco PIX 525 border firewall located in the Badlands segment of SAGE.

This, and all Firewalls located in the GIAC Enterprises, network will be configured utilizing the "Deny all" model.
Note: Since it is beyond the scope of this assignment, this document will contain only the access-control list associated with this firewall instead of the entire firewall configuration.

```
PIX Version 6.0

!       This allows systems to establish a connection to the SMTP e-mail server.
access-list dmz1_acl permit tcp any host X.15.0.5 eq 25

!       This allows systems to establish a connection with the Ext/Ext DNS server.
access-list dmz1_acl permit tcp any host X.15.0.6 eq 53

!       This allows systems to establish a connection to the GIAC Web server.
access-list dmz1_acl permit tcp any host X.15.0.7 eq 80

!       This allows systems to establish an SSL session with the GIAC Web server.
access-list dmz1_acl permit tcp any host X.15.0.7 eq 443

!       This allows internal systems to establish outbound sessions.
nat (inside) 1 10.0.0.0 255.0.0.0

!       This defines the address scope that internal systems will draw an IP address
!       from while connected to the Internet
global (outside) 1 X.0.15.15-X.0.15.254
```

```
!       This defines a Port Address Translation (PAT) in the event that the address pool
!       allocated in the above entry becomes exhausted.
global (outside) 1 X.0.15.14

static (dmz1,outside) X.15.0.5 10.5.1.5 netmask 255.255.255.255
static (dmz1,outside) X.15.0.6 10.5.1.6 netmask 255.255.255.255
static (dmz1,outside) X.15.0.7 10.5.1.4 netmask 255.255.255.255
```

Issue Specific Policy #3.3: Cisco VPN 3030 Concentrator Configuration

The purpose of this policy is to document the configuration of the Cisco 3030 VPN Concentrator located in the Badlands segment of SAGE.

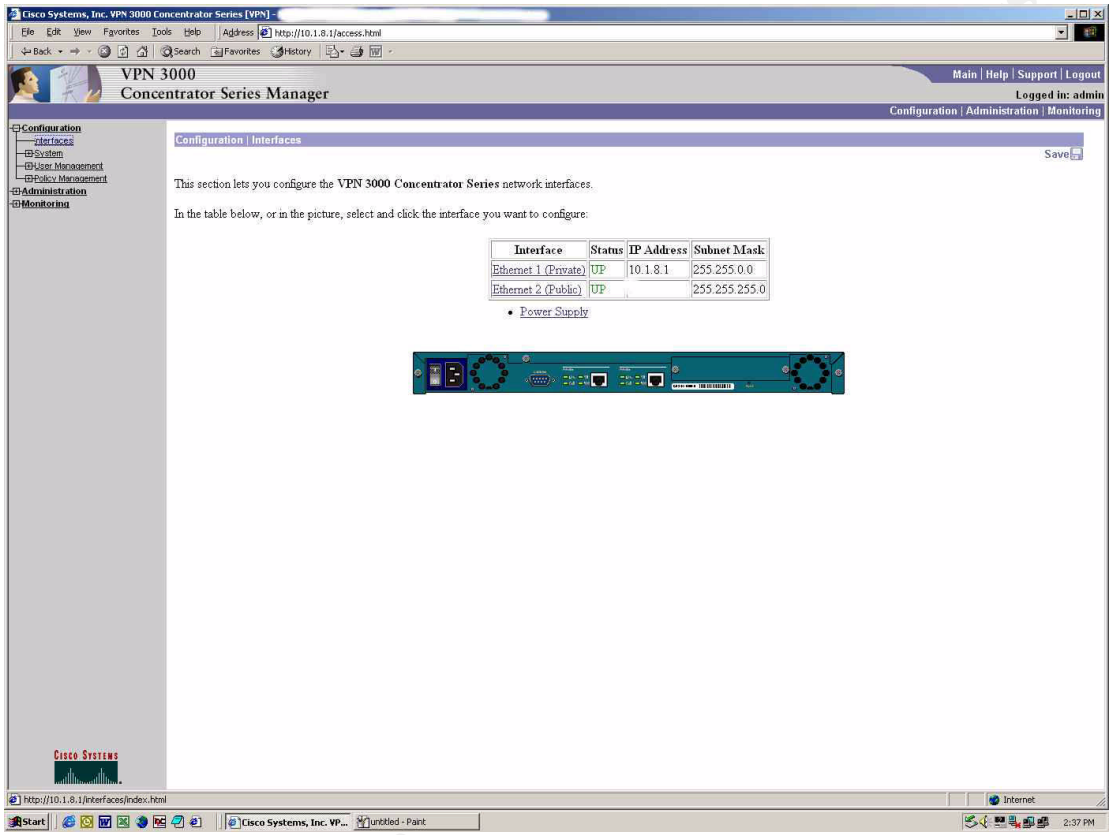
Note: Since it is beyond the scope of this assignment, this document will contain only the access-control list associated with this VPN device instead of the entire device configuration.

Split tunneling is disabled by default on the Cisco 3030 VPN Concentrator, per the vendor, and under no circumstances shall be turned on for this device.

```
!       Configuration for the [  IP Ethernet 1  ] interface will be the only interface
!       configured via command line for this device.
[  IP Ethernet 1  ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 10.1.8.1
```

The remainder of the device configuration will be done using HTTP to the device. The screen below shows the initial logon. The default username and password is admin.

The external interface of the Concentrator can be configured by clicking on "Configuration" and then "Interfaces" in the left pane. Click on the "Ethernet 2 (Public)" link and enter X.15.0.4 subnet 255.255.255.0.



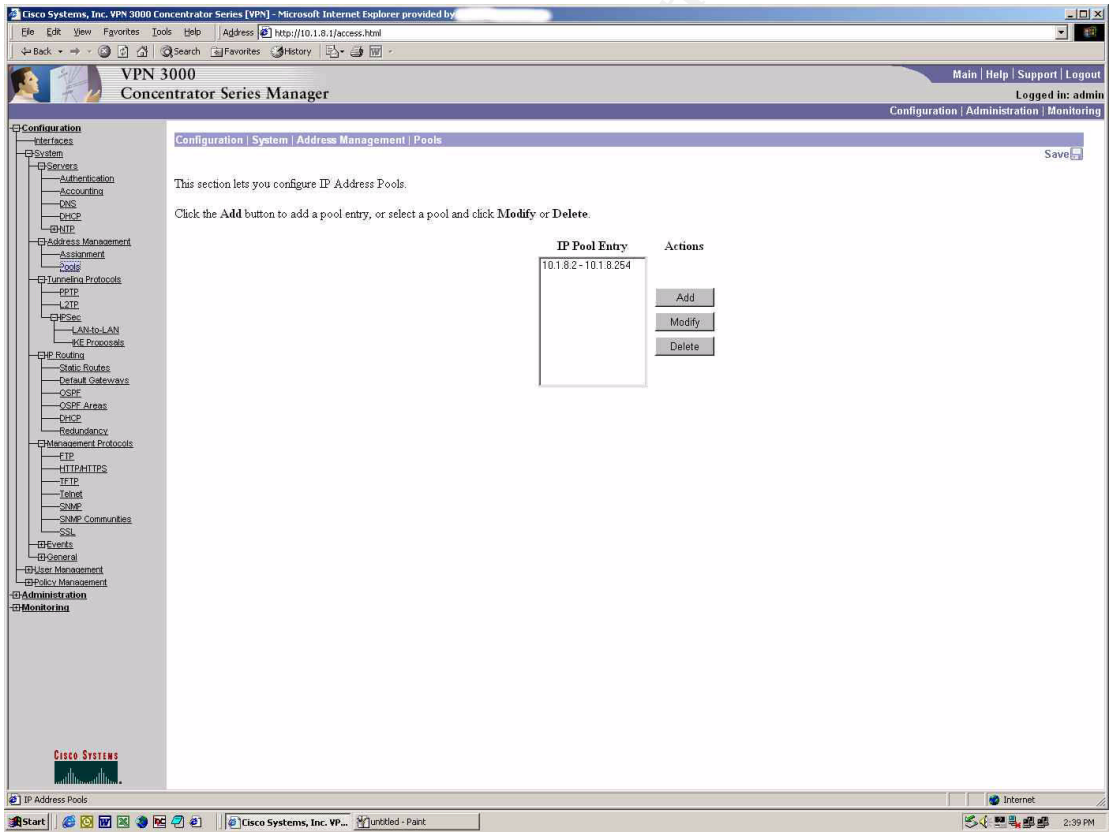
Next the address pools that the clients will use can be established. By selecting

"Address Pools" and then "Management" IP addresses can be configured for connecting users. There will be four blocks of addresses created, they are as follows:

- 10.1.8.2 – 10.1.8.254, 10.1.9.1 – 10.1.9.254. These IP addresses will be used for partners and staff members that reside in the United States.
- 10.1.10.1 – 10.1.10.254, 10.1.11.1 – 10.1.11.254. These IP addresses will be used for our International partners.

As shown in the diagram below just click on the "Add" button and add the address listed above.

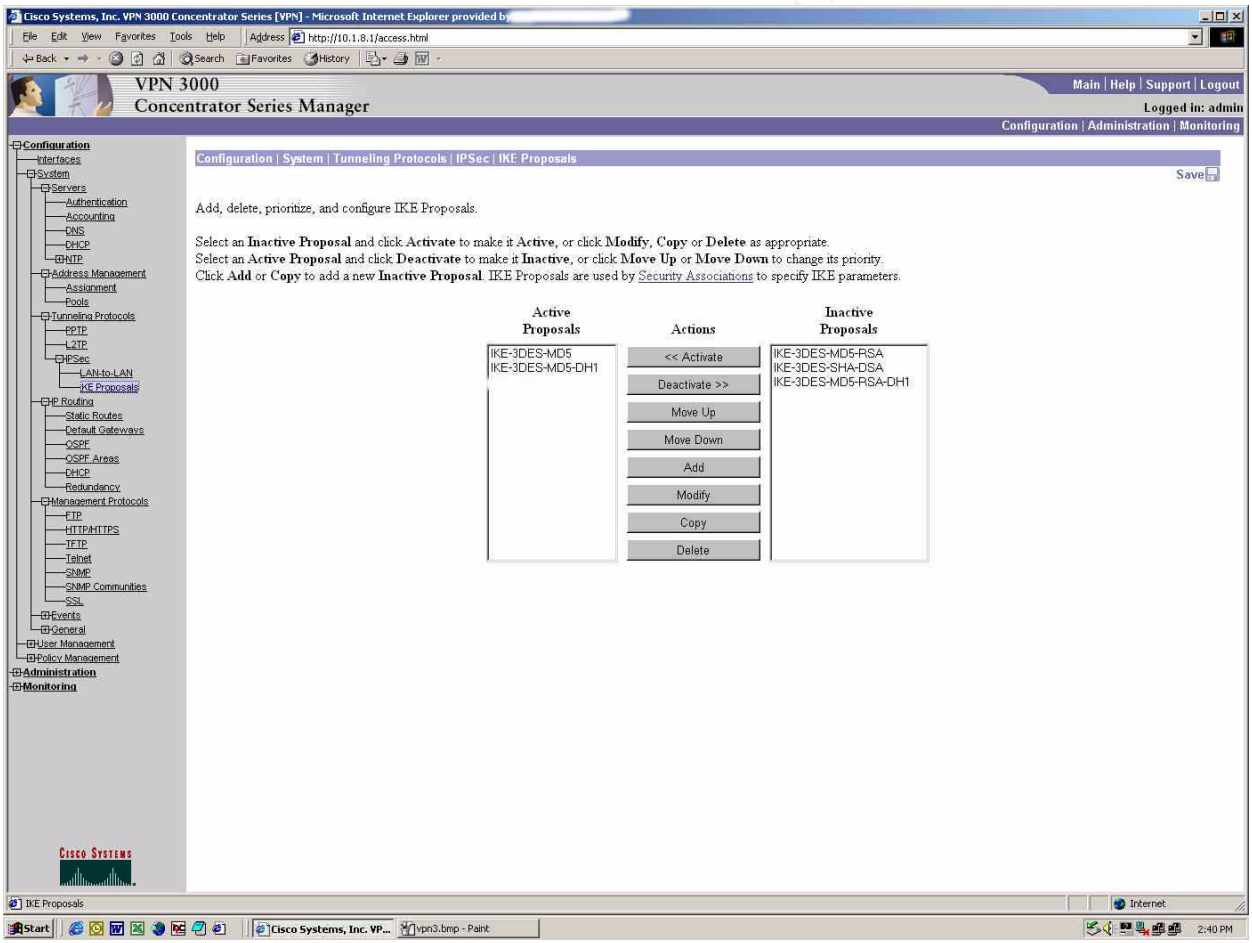
Note: The separation of IP addresses is done so that when Groups are created, the International partners can be placed in groups where the encryption settings can be configured to abide by the cryptography laws of the nation in which they reside.



IKE (Internet Key Exchange) parameters are next to be configured. Under “Tunneling Protocols” – “IPSec” – “IKE Proposals” from the menu on the left is where the parameters will be set from. During the establishment of the VPN “Tunnel” under IPSec, the first phase is to establish the tunnel (IKE Security Association or IKE SA) and then to govern the traffic within the tunnel (IPSec SA covered later).

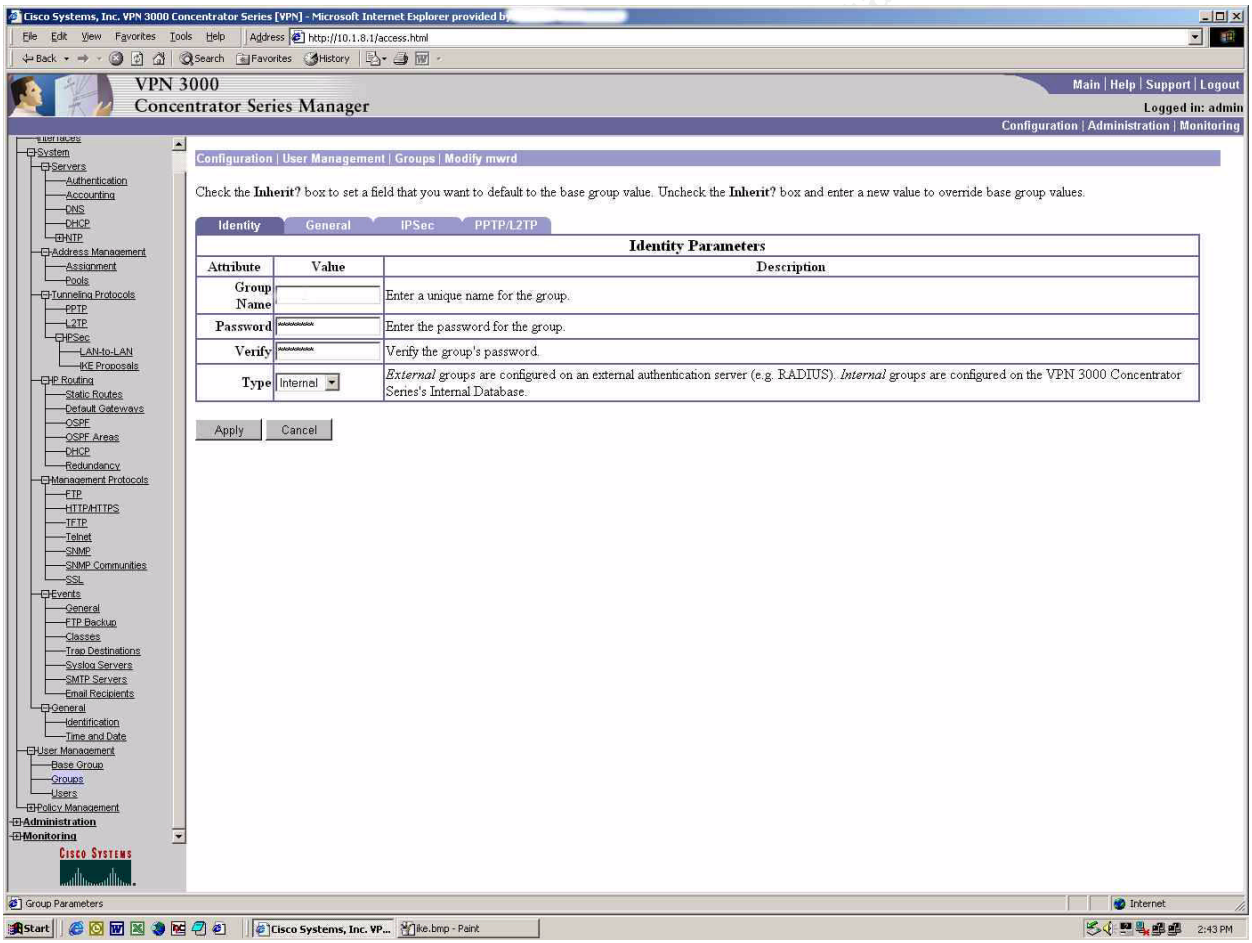
By default the activated IKE Proposals are IKE-3DES-MD5, IKE-3DES-MD5-DH1, and IKE-DES-MD5. Click on IKE-DES-MD5 and select the “Deactivate” button, as we do not want to use IKE-DES-MD5 because it only supplies us with a 56-Bit encryption algorithm. This leaves us with **IKE** (key exchange)-**3DES**(encryption)-**MD5** (128-bit key hash function) and IKE-3DES-MD5-**DH1** (Diffie-Hellman Group 1 at 768-Bits).

Note: IKE-3DES-MD5 also uses Diffie-Hellman but it uses Diffie-Hellman 2 at 1024-Bits

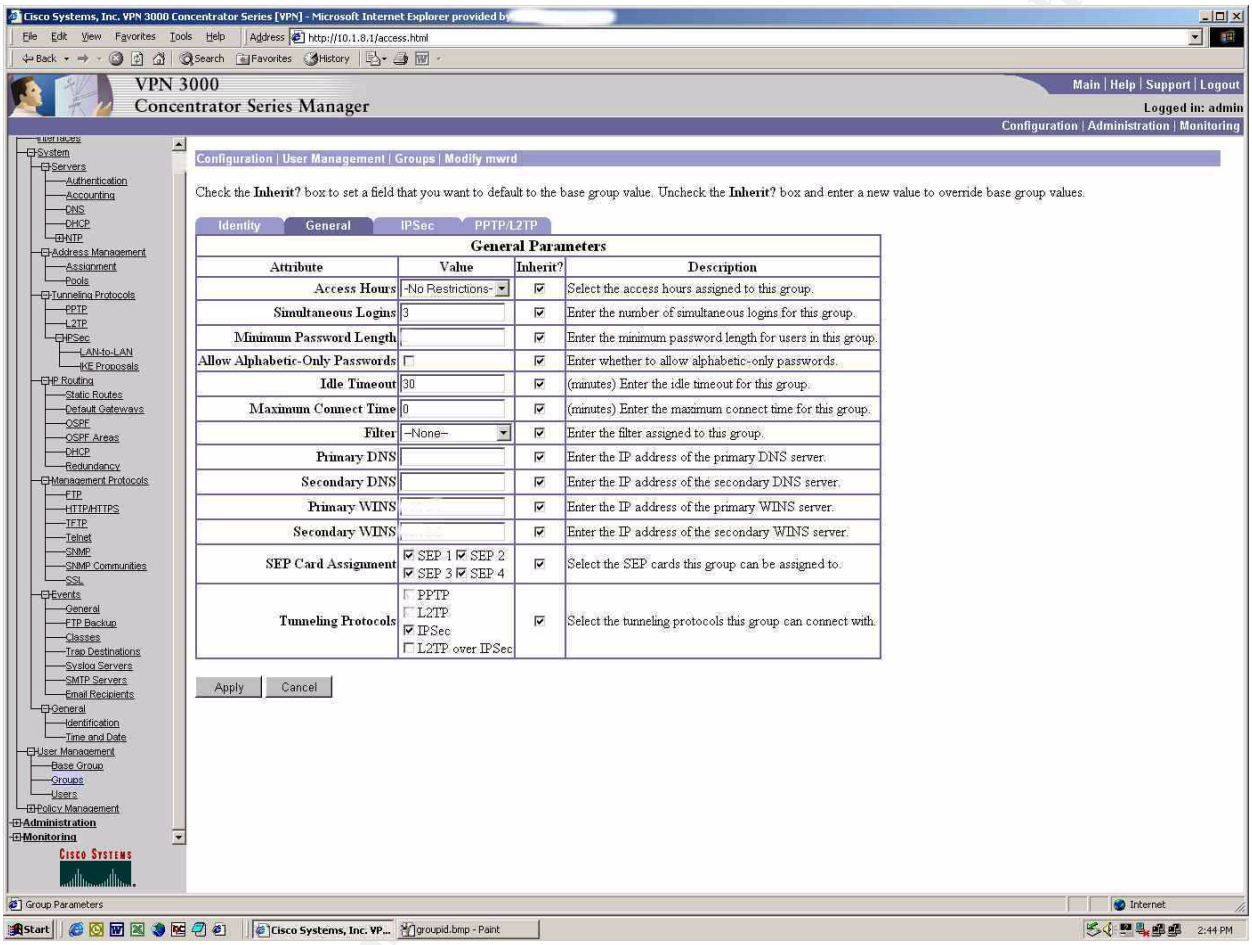


Now the groups will be configured by selecting “User Management” and then the “Groups” option from the left side menu. The screen below will then be displayed. The creation of two different groups will need to be accomplished. The first group is GIAC and will encompass all of the United States partners the second group will be GIACINT and will encompass all of the International partners. Each group must be assigned a password that will be established within the guidelines of the GIAC Enterprises, Inc. Issue Specific Policy #1.3: Password Policy.

Note: This document will only cover the set-up parameters used for the GIAC group as cryptography export law is beyond the scope of this document and was mentioned only to make readers aware that it is an issue that would need to be addressed.



Under the “General” tab of the group configuration windows is where the password length is to be assigned, again in accordance with the GIAC Enterprises, Inc. Issue Specific Policy #1.3: Password Policy. And also in this section is where the tunneling protocols that will be used are determined. The option of “IPSec” will be selected and all other options will remain unchecked (PPTP, L2TP, and L2TP over IPSec).

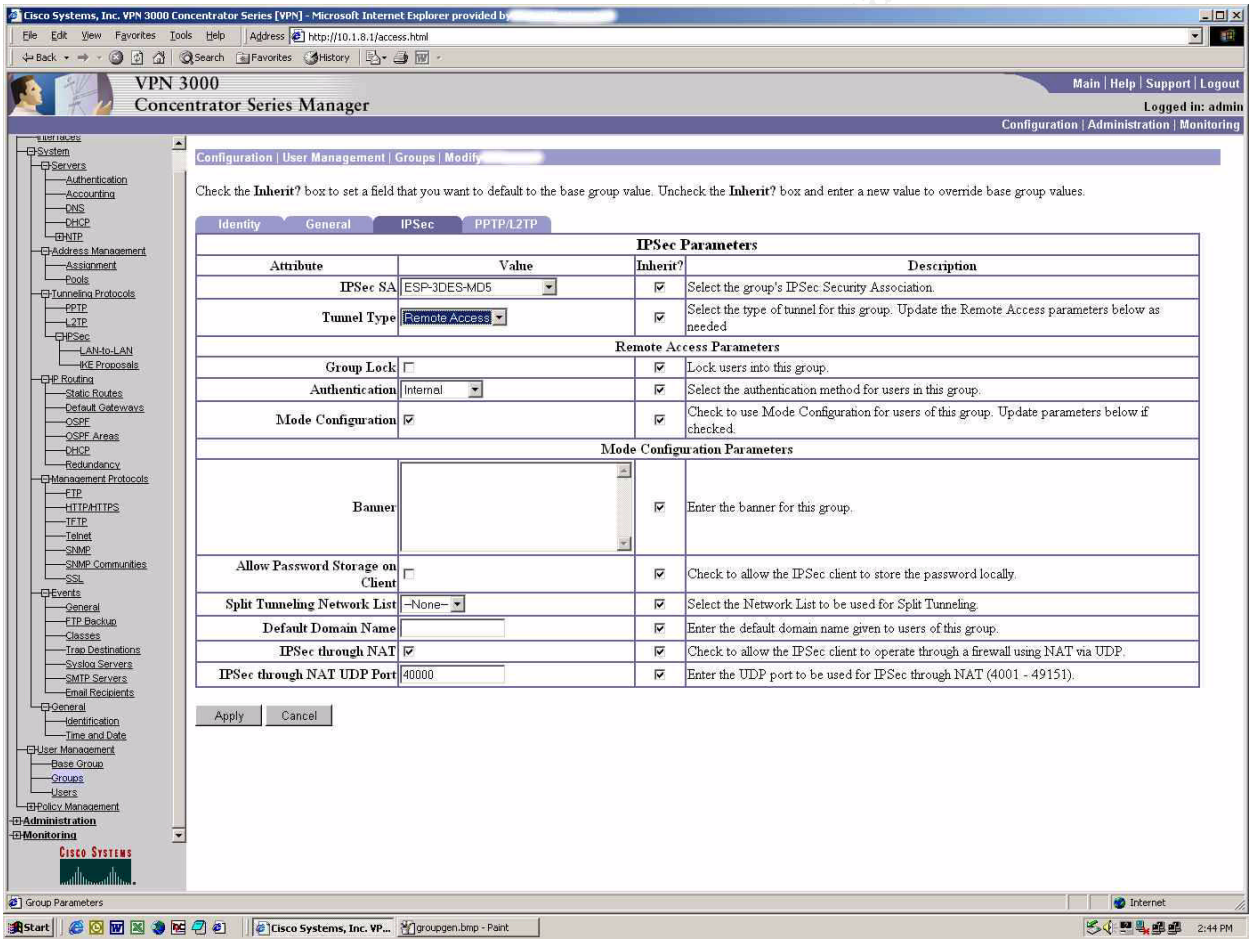


The next tab, “IPSec”, is where the parameters for IPSec will be configured. For the

IPSec Security Association (SA), **ESP**(protocol)-**3DES**(encryption)-**MD5**(128-bit key hash function) is the option to select. This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC (Hash Message Authentication Coding) –128 for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel. This selection is chosen because it is the most secure connection available on the Concentrator product.

A banner for the group must also be entered on this screen. The syntax is given below.

> Authorized personnel only! Unauthorized use of system is unlawful and may be subject to civil or criminal penalties.
> Use of the system is monitored and logged. The logs may be used as evidence in the court of law.



Now simply click on the “Save Needed” icon in the upper right hand side of the screen and save the settings.

Assignment 3 – Audit Your Security Architecture

There will be three phases of the security audit for the GIAC Enterprises network. Phase one will be the planning phase. In this phase, all of the coordination between the local and remote teams will be outlined and the software/hardware tools for use during the audit will be acquired and installed.

Phase two will consist of performing the audit against the internal segment of the network and will overlap into Phase three of the audit which will concentrate primarily on the external segments of the GIAC Enterprises network.

Phase One

For internal network auditing, two members form the first and last shifts will be performing the audit. Wave one of the audits will start at 7:45 A.M and continue until 9:45 A.M. This is done to monitor network traffic when most of the users are logging onto their workstations. Wave two of the audit will begin at 12:00 P.M. and will continue until 3:00 A.M. This is done to primarily monitor users for leaving machines on, suspicious ports being open on computer systems, and close monitoring of syslog output.

External auditing will take place over the same times, but the locations will vary extensively. We will be coupling with partners in our International operations so that we can test for vulnerabilities of foreign releases of software as well as what affect lower levels of encryption have on the overall security of the network. The same four members of the internal auditing team will be utilized for the external audit to keep the results and testing methods consistent.

The tools that will be utilized will be much the same as those that hackers would use. The reason for this is that it is best to see what your network will look like through similar eyes. Also, freeware tools are easily accessible via the Internet and they may even be in the arsenal of some GIAC Employees.

The following is a list of tools that will be used for the exercises.

- SuperScan Version 2.03 Copyright Lazypig (date unknown)
- Sam Spade Version 1.14 Copyright Steve Atkins 1997-1999
- Cerberus Internet Scanner Version 5.0.02 Copyright 2000 Cerberus Information Security Ltd.
- Legion Version 2.11 Copyright 1999 by Rhino9
- Nmap Version 2.53 Author Fyodor
- Analyzer version 2.2 Copyright 1997 – 1999 Politencio di Torino

Each of the tools listed above are freeware tools so the cost is only the time that it will take for the users to download them.

All of the members of the auditing team will be fitted with two laptop computers

because some of the tools are operating system specific and will be necessary to run simultaneously. The estimated cost of the laptops is $3100.00 per person and with four personnel conducting the audit the estimated cost is $12,400.00. A total of $3500.00 has also been attached to the audit to cover the traveling expenses of those performing the audits.

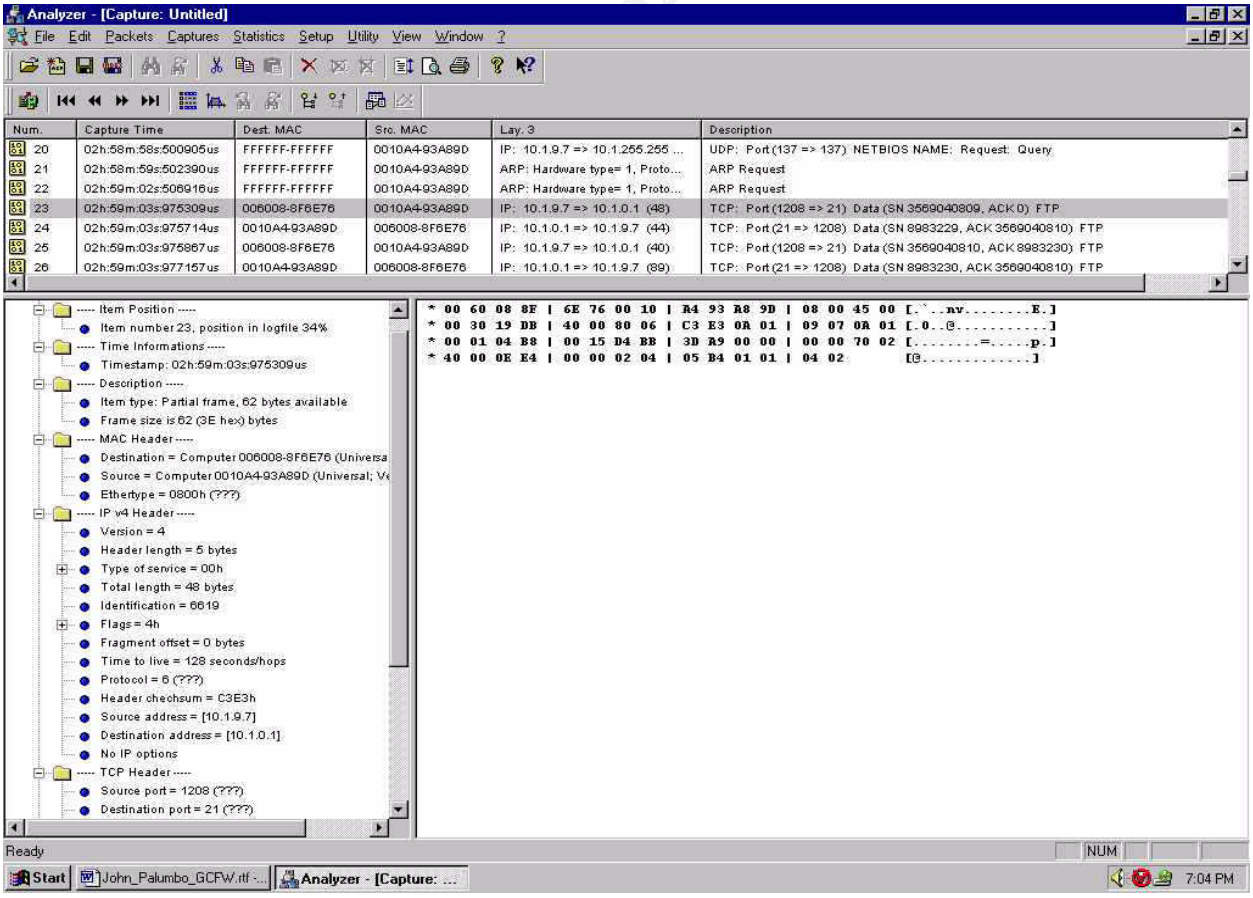
The total estimated expense to complete the audit is as follows:

Computer Hardware	$12,400.00
Travel Costs	$ 3,500.00

Total	$15,900.00

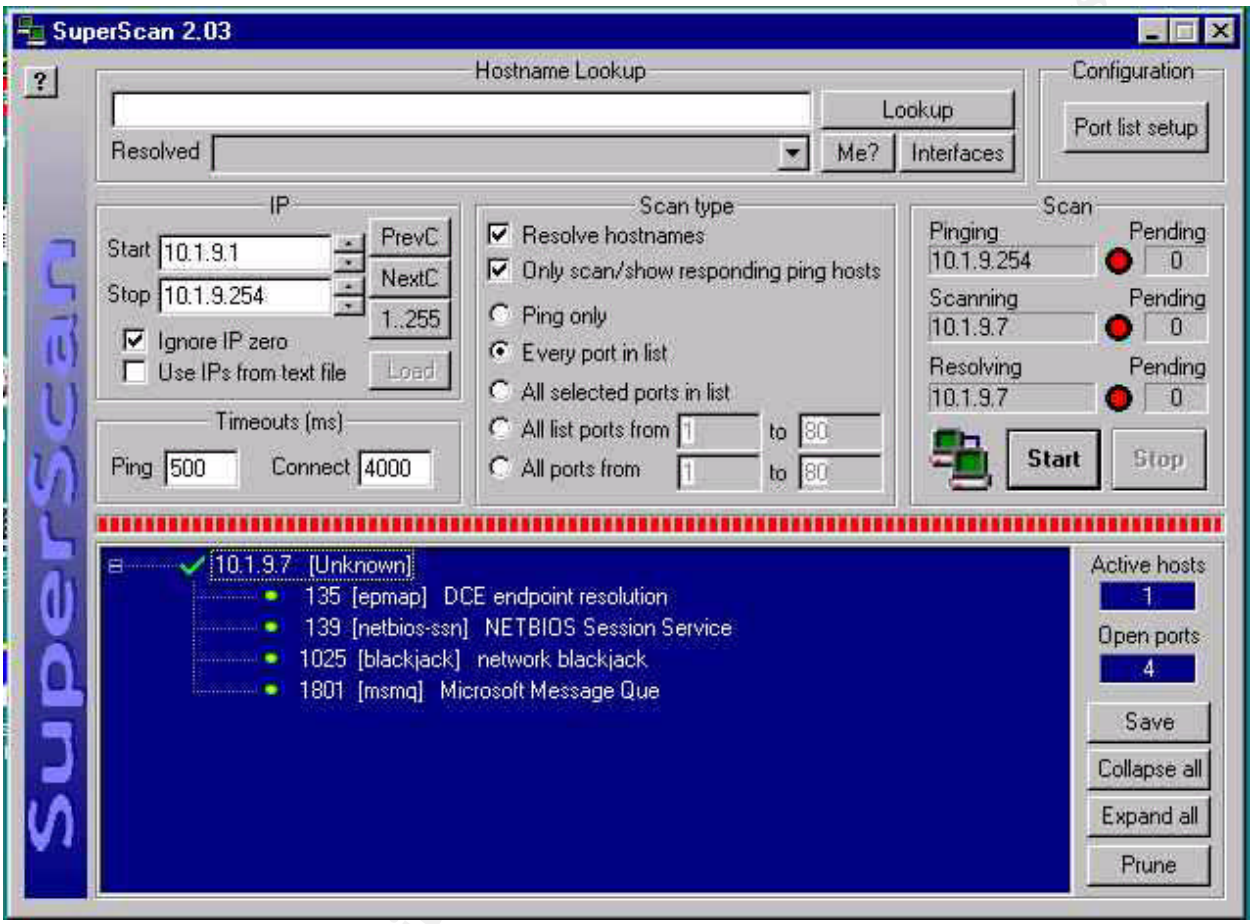
Phase Two

Analyzer was the first program placed on the network for the internal audit. Analyzer is a packet capturing software that sniffs a network segment capturing all of the data on the wire. It then outputs the data via a graphical interface in TCPdump format. As shown in the screen shot below, someone was running FTP on the local network.



Next a port scan was run using a product called SuperScan. There were some

interesting results as shown below. This particular workstation is obviously a Windows machine due to the Net Bios port being open, but it also looks like they may be trying to kick up a game of network blackjack, bet the CIO will love this.



Next the team used the Cerberus scanner against all of the Web servers located in the network. The report did uncover one server that is in dire need of some attention. The report is shown below.

Web Service
Web Server Software is Microsoft-IIS/4.0
Security Issues
The web service on Microsoft's Internet Information Server 4.0 has a buffer overrun vulnerability when a 3000+ character long request is made for a .htr file. This vulnerability could allow a remote attacker to execute arbitary code and gain control of the computer. Ensure that the patch has been installed. If it hasn't - until the patch is installed remove .htr as a registered IIS file extention.

http://10.1.0.1/scripts/samples/search/qfullhit.htw

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager.

http://10.1.0.1/scripts/samples/search/qsumrhit.htw

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager.

.htw files are still mapped to webhits.dll

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager. If you use the webhits functionality ensure the patch has been installed. See Microsoft's advisory for more details.

msg=The user 'IUSR_SERVER' is not authorized to execute the 'open service' method. It is possible by making a vermeer RPC request to /_vti_bin/shtml.dll to get the name of the anonymous Internet account. If you don't use FrontPage delete this dll.

http://10.1.0.1/_vti_bin/fpcount.exe?Page=default.htm|Image=3|Digits=15

Fpcount.exe has been found in the /_vti_bin/ directory. If, when the link above is followed , fifteen digits are displayed this version of fpcount.exe is from the FrontPage Server Extentions 97 package and it contains a buffer overrun that allows remote execution of arbitary code.

This should be deleted until a copy of the 98 version of FrontPage can be obtained.

http://10.1.0.1/iisadmpwd/aexp2.htr

From here an attacker can launch password attacks against the local machine or or proxied attacks against other machines on the network. More information can be found here

http://10.1.0.1/cgi-bin/htimage.exe?2,2
htimage.exe, on error will reveal physical paths. Consider removing it.

http://10.1.0.1/scripts/samples/search/qfullhit.htw

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager.

http://10.1.0.1/scripts/samples/search/qsumrhit.htw

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager.

http://10.1.0.1//_vti_bin/shtml.dll Shtml.dll can be abused to gain the source of server side scripts such as ASP pages. Ensure the most up to date version of Front page is being used.

The Analyzer program was placed on each network segment and traffic w3as tested on the inside and outside interfaces of each firewall located in SAGE. As expected all of the traffic that was traversing the network was being properly filtered. All that needed attention were the few instances found on some internal hardware.

Phase Three

The final phase went off without a hitch, and the border router filters prevented any ICMP traffic and NAT seemed to work very well at hiding our internal address space. The use of International software and the lower encryption standards posed no threat as policy has been implemented to decrease the amount of time that user accounts can go without logging in and passwords must be changed more frequently.

Security Assessment Review

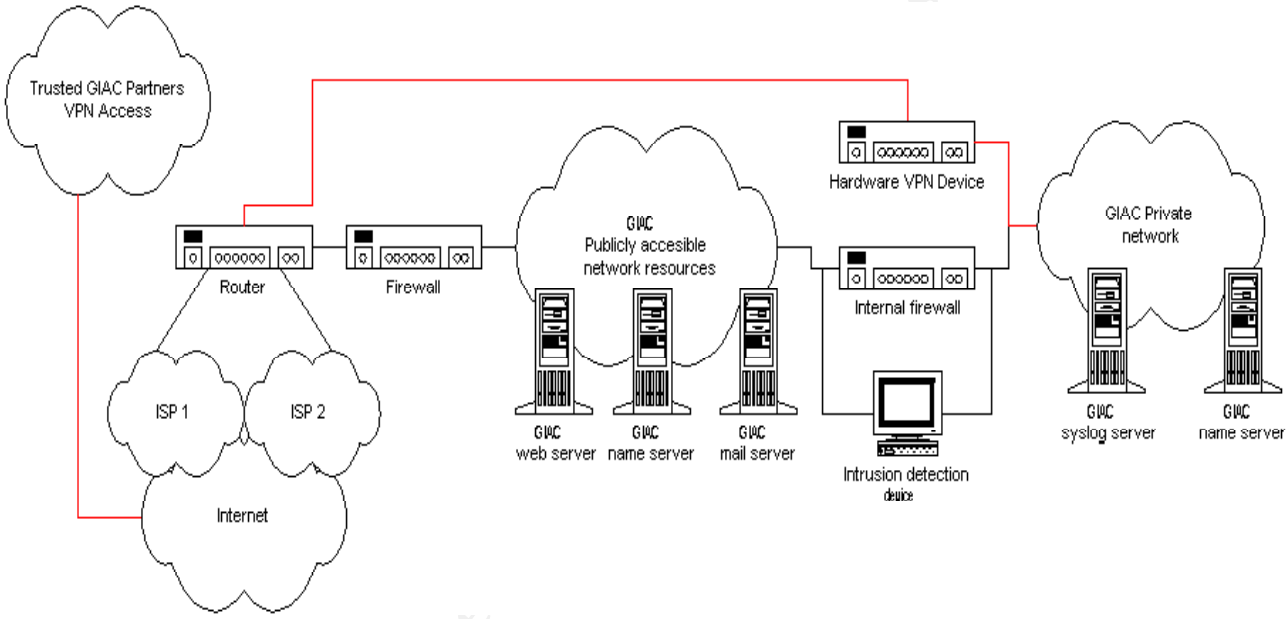
The overall assessment of the GIAC Enterprises network showed few flaws in its design. The recommendations made are as follows:

Windows NT and IIS for external Web servers. Given the recent and unbelievable number of security flaws directly attributed to Microsoft products, there may be a need to shift away from the use of these systems outside the GAIC Network. Further analysis must be done on this matter.

VPN Placement. The most difficult decision in the design of the GIAC Network was where to place the VPN. The location of the external interface being outside a firewall could cause some potential problems. But, the only available ports are those used for encryption and there are limited exploits available for such services. I think, however, that the VPN must be moved entirely behind the Firewall to truly be secured.

Assignment 4 – Design Under Fire

For this assignment I will be evaluating the design that was submitted at http://www.sans.org/y2k/practical/ken_colson_gcfw.doc.



Firewall Attack

The firewall that was used in this submission was a Linux Server with the latest kernel release and all software patches being up to date. Though not clarified, I will assume that the distribution is Red Hat.

Since this Firewall was implemented using Linux, I will attempt to use the Linuxconf Buffer Overflow vulnerability sin I am not sure which version of Linux the machine is running.

Armed with Netcat and the linuxconf exploit code located at http://newdata.box.sk/neworder/lconf.txt the exploit can be run as follows:

```
./linuxconf.exe ; cat | nc host-ip-address 80
```

Since port 80 is open for web traffic, the exploit should work and cause a buffer overflow on the target.

DoS Attack

The method of DoS attack that I have chosen for the network is the SYN Flood. By using the code synful.c which can be found at the following address http://anticode.antionline.com/download.php?op=geninfo&did=224180. The border router is not configured to limit the number of half-opened connections enabling a successful SYN Flood DoS.

The counter this attack the number of half-open connections allowed on the router should be configured.

Perimeter System Attack

The target for a perimeter attack would undoubtedly be via e-mail. I would send a Trojan Horse and/or a worm virus to ever user that I could on the inside of the network. Through a little social engineering and some possible dumpster diving, I'm sure I could find out just about every e-mail address on the network. Someone is bound to open one e-mail from someone who "Loves Them".

References

1) Rocky Mountain SANS Conference Denver, Colorado. June 29 - July 3, 2001Cole, Eric Instructor.
2) RFC 2196, Network Working Group. Fraser, B. September 1997.
3) GIAC Basic Security Policy, Version 1.34. Various Authors. July 6, 2000.
4) Web Commerce Technology Handbook. Minoli, Daniel, Minoli, E. 1998. McGraw Hill
5) Internet Security, Professional Reference Second Edition. Atkins, Derek, Buis, P., Hare, C., Kelley, R., Nachenberg, C., Nelson, A., Phillips, P., Ritchey, T., Sheldon, T., Snyder, J. 1997. New Riders Publishing
6) Complete Hackers Handbook. Dr. K. 2000. Carlton Books Limited
7) Practical Firewalls. Ogletree, William June 2000. QUE Publishing
8) www.microsoft.com/technet
9) www.cisco.com
10) www.sidewinder.com
11) www.astalavista.box.sk
12) www.anticodeonline.com