Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, & VPNs
GCFW Practical Assignmnet
Version 1.5b

By: Matthew Keogler

A Security Architecture has been designed for GIAC Enterprises. GIAC Enterprises will be conducting their business over the Internet. With this in mind, this architecture is tailored for multiple business relationships.

There will be a department called the NOC (Network Operation Center). Their sole duty is to monitor the enterprise servers and network 24/7. They will act as first level support for security issues as they arise outside of normal business hours.

The thought process behind the architecture is that each location (Corporate Headquarters and Data Center) is self-sufficient. Each location will have all necessary servers/services to run the business with little need for connections to each other. Usually the only connections would be for data replication and management purposes. The master database would be located at corporate with data replication being done at the slave databases at the data center.

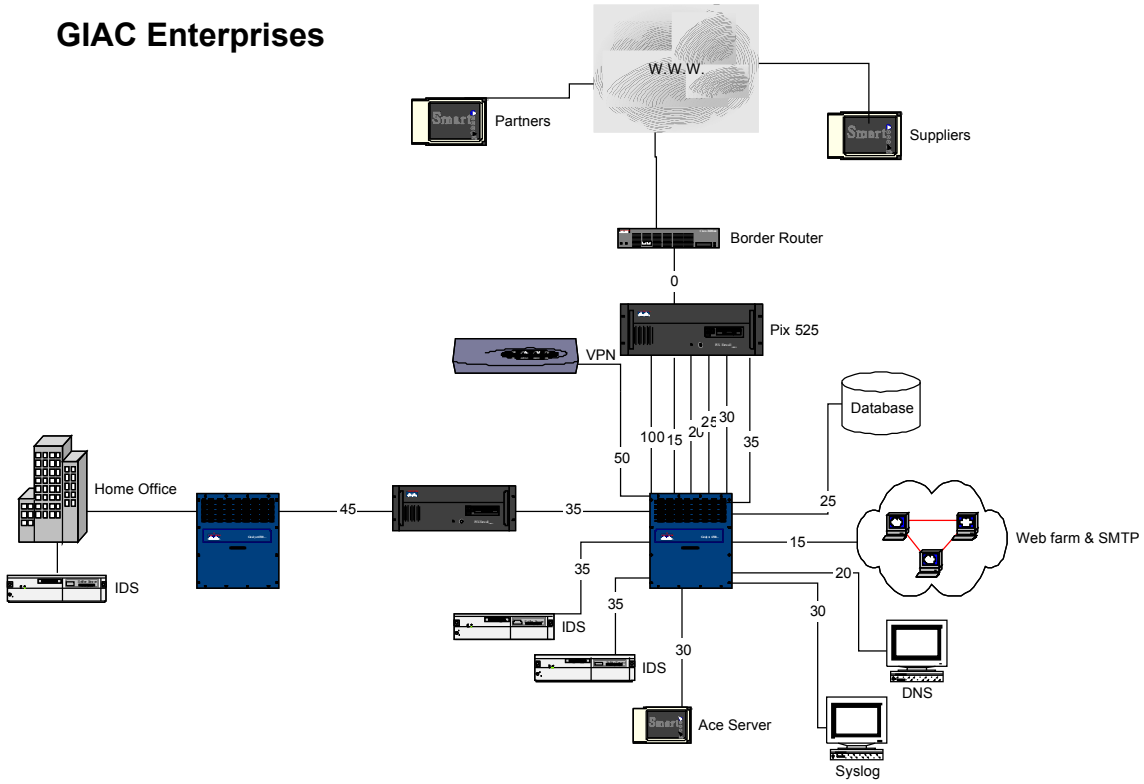
Basics of layout:

- All connections connecting network equipment are redundant.
- Web farm is behind a load balancer.
- All servers are multi-homed.

The vendors used were decided on by three factors:

- A proven track record for delivering on functionality.
- Had to be at least number two in there industry.
- A solid Support Department.

Security Architecture



Firewall:
The firewalls used is the Cisco Pix 525. The version is 5.2.3, this version is found to be the most stable with most applications (previous versions had some issues with SMTP). The Internet firewall is being utilized as a stateful router. It will deny all except for what is specifically allowed. The Corporate firewall is being utilized as a gateway that also denies everything besides what is allowed in.

Router:
The router used is a Cisco 3640. The version of code is 12.0(5). This perimeter router allows for scalability and growth. The function of this router is to be the first layer of defense that is tasked with filtering out traffic that is not benign.

Switches:
The switch of choice is the Cisco Catalyst 6509. The version of code is 5.5.(5). There will be a MSFC card in slot 0. This switch has a 9 module capacity. This will allow the company to grow within reason without worrying about out growing existing equipment.

VPN:
The VPN server utilized is the Cisco VPN Concentrator 3030. The 3030 can handle

bandwidth requirements of up to 50Mbps and handle up to 1500 simultaneous users. This model can also be bought with redundant hardware (power, and SEP- Security Encryption Processor module) built into it.

Secure Remote Access:
Secure remote access will be handled by RSA Ace Server. We will be deploying the SecurID tokens to our suppliers and partners. The version for the Ace Server will be 4.1 running on Solaris 8 with all up to date patches.

IDS:
I will be deploying three Intrusion Detection System. The first one is ISS RealSecure Network Sensor. The version of ISS is 5.0 for Solaris 2.7 on a U5 with a 333Mhz processor and 512MB RAM. The second one is snort. The version will be 1.7 running on Solaris 8 on a U5 with 333Mhz processor and 512MB RAM. Both of these IDSs will be located at the DataCenter.

GIAC Enterprises customers, suppliers and partners will be clearly defined independently of each other. The customers will flow into the web farm utilizing SSL 128 bit encryption when transactions are being placed. The suppliers and partners will use VPN with the SecurID token. The VPN will define their access capabilities and encryption type. The SecurID token will be the authentication engine for the VPN Concentrator.

Security Policy

The policy will cover the firewalls, the router, the VPN and the IDS systems. I will explain how traffic will flow and how each piece works with the others to complete the business requirement.

Here is how the technologies are used to build this architecture:

The FW-Internet has eight physical interfaces. Here is the breakdown:

- Ethernet0 – outside and also security0 (connection to the router)
- Ethernet1 – inside and also security100 (internet VLAN)
- Ethernet2 – dmz1 and also security20 (web farm and SMTP VLAN)
- Ethernet3 – dmz2 and also security20 (DNS VLAN)
- Ethernet4 – dmz3 and also security25 (database VLAN)
- Ethernet5 – dmz4 and also security30 (syslog and ace server VLAN)
- Ethernet6 – dmz5 and also security35 (Management and IDS VLAN)

The significance of the numbers is the ability to control how traffic flows. " For interfaces with a higher security level such as the inside interface, or a perimeter interface relative to the outside interface, use the nat and global commands to let users on the higher security interface access a lower security interface. For the opposite direction, from lower to higher, you use the access-list command…" (taken from Cisco pix configuration web page). One main reason for this is to keep a web server from being compromised and then used as a jump point to the databases. Here is how the configuration would look:

```
nat (inside) 1 0 0
nat (dmz5) 1 0 0
nat (dmz4) 1 0 0
nat (dmz3) 1 0 0
nat (dmz2) 1 0 0
nat (dmz1) 1 0 0
```

This allows each interface to talk to lower security interfaces. The first NAT allows inside users to make connections to any lower security interface. The 1 is the NAT ID. The 0 0 is the host ip and subnet mask. This is in case you want to be specific on a host or a range of hosts that can access this DMZ.

```
global (outside) 1 2.2.2.6
global (outside) 1 2.2.2.5 netmask 255.255.255.224
global (dmz1) 1 192.168.15.10-192.168.15.100 netmask 255.255.255.0
```

The first global command is setting the IP address of all outbound traffic. When ever a packet from the inside network is destined for the outside interface. The source IP address will be x.x.2.6. The second global command is utilizing PAT. This allows 65,535 hosts to start a connection to the outside using this registered IP of x.x.2.200 address. The last global command statement for dmz1 lets users on the inside, dmz2, dmz3, and dmz4 start connections on the dmz1 interface.

```
!maps 2.2.2.31 to GIACs web server.
static (inside,outside) 2.2.2.31 192.168.15.31 netmask 255.255.255.255 0 0
!maps 2.2.2.32 to GIACs SMTP server.
static (inside,outside) 2.2.2.32 192.168.15.32 netmask 255.255.255.255 0 0
!maps 2.2.2.31 to GIACs DNS server.
static (inside,outside) 2.2.2.33 192.168.20.31 netmask 255.255.255.255 0 0
```

The static statement above configures a static translation between our outside address to a private address. The mapping is a one to one with a 32 bit netmask because we are being specific to a host.

access-list dmz1_dmz3 permit tcp 192.168.20.x 255.255.255.0 192.168.25.x 255.255.255.0 eq 1521
access-group dmz1_dmz3 interface dmz3 in

This will allow for the web servers to talk to the databases on port 1521 (Oracle). The access-group applies the access-list to an interface.

access-list outin permit tcp any host 2.2.2.31 eq www
access-list outin permit tcp any host 2.2.2.31 eq 443
access-list outin permit udp any host 2.2.2.32 eq smtp
access-list outin permit udp any host 2.2.2.33 eq domain
access-group outin in interface outside

IP Access List

access-list *1-99* permit|deny *address mask* ip access-group *1-99* access-class 1-99 out|in *(for terminal line assignment)*

Extended IP Access List

access-list *100-199* permit|deny ip|tcp|udp|icmp *source source-mask dest dest-mask /*lt|gt|eq|neq *dest-port]* ip access-group *100-199*

Bold is from the Cisco web site.

Break down of the first access-list.

- outin = is the name of the access-list.
  - I use outin to show that traffic is coming from the outside to the inside.
- permit = which tells the firewall to allow this traffic.
- protocol = I am being specific to tcp.
  - (note: I could have used ip but that would have allowed UDP on that same port to come into my network.)
- any = I'm allowing any network (source; source-mask)to access this defined server.
- host = host is used in conjunction with the destination ip address. I'm telling the pix that the source is mapped to a specific host at 2.2.2.x.
- eq = is an operand. I'm telling the Pix firewall that the source can talk to this destination only if the service equals port 80.

telnet 192.168.45.0 255.255.255.0 inside
telnet timeout 5

This tells the firewall to only allow nodes coming from the .45 subnet to connect to it from the inside interface. This network is from the corporate office. The reason you don't see ssh is because you cannot run Pixs in failover mode with ssh. You get one or the

other with the present versions of code Cisco has released for the Pix Firewall.

The router is my true connection to the Internet. It physically connects my network with my ISP (Internet Service Provider). It has two interfaces, both are Fast Ethernet allowing for 100Mbps. Interface e0 will be used to connect to my Internet Service Provider. Interface e1 will be used to connect to the outside interface of the FW-Internet.

Here is the configuration for the border router:

```
! a very secure, encrypted password according to Cisco
service password-encryption
enable secret 5 !@##$%%654321hIU$#
!
no ip source-route
no service tcp-small servers
no service udp-small-servers
no service finger
no ip http server
no ip bootp server
no ip broadcast
!
! Interface Ethernet 0 (e0 - outside)
interface Ethernet0
    ip address 2.2.1.253 255.255.255.252
    ip access-group 110 in
    no ip directed-broadcast
    no ip unreachables
    no ntp enable
!
! Filtering packets coming into our network
access-list 110 deny tcp any any eq telnet log
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 208.1.1.100 0.0.0.255 any log
access-list 110 deny ip any 192.168.0.0 0.0.255.255 eq 1999 log
access-list 110 deny ip 224.0.0.0 31.255.255.255. any log
!
! Allowing packets destined for services GIAC offers
access-list 110 permit tcp any 2.2.2.0 0.0.0.255 eq 80
access-list 110 permit tcp any 2.2.2.0 0.0.0.255 eq 443
access-list 110 permit tcp any 2.2.2.0 0.0.0.255 eq 25
```

```
access-list 110 permit udp any 2.2.2.0 0.0.0.255 eq 53
access-list 110 deny ip any any log
!
```

******Explanation of Interface Ethernet 0 configuration*******

The *no ip source route* is to help prevent an attacker from controlling the route the IP datagram takes to the destination and in some cases the route the reply will take.

The *no service tcp-small servers* and *no service udp-small servers* is to deny access:

- echo (7/tcp, 7/udp)
- discard (9/tcp, 9/udp)
- daytime (13/tcp, 13/udp)
- chargen (19/tcp, 19/udp)
- time (37/tcp, 37/udp)

These are diagnostic services that could be exploited by an attacker to deny service to a target or map out a network. (taken from, Intrusion Detection & Packet Filtering, by Hal Pomeranz and Vicki Irwin.)

Blocking port 1999 is done because this is a Cisco router. Port 1999 is the "Cisco indentification port", and remote attackers can distinguish Cisco devices from other OSs by sending a SYN packet at this port. (taken from, Intrusion Detection & Packet Filtering, by Hal Pomeranz and Vicki Irwin.)

The *no ip unreachables* is a way to configure Cisco routers to silently drop packets that would normally generate an ICMP error message.

The *service password-encryption* tells the IOS to encrypte the password. This is a weak encryption method and should be used just to keep someone from looking over your shoulders from seeing the password. The line below it, *enable secret* command uses MD5 hash for encryption. Considered secure by most but is still prone to a dictionary attack if the hash got in the wrong hands. For those that need to see the difference between the two, please visit www.boson.com at this url.

******Explanation of Interface Ethernet 1 configuration*******

Interface Ethernet 1 (e1 – inside)

```
! Internal Interface
interface Ethernet1
    ip address 2.2.2.6 255.255.255.0
```

```
    ip access-group 111 out
    no ip directed-broadcast
    no ip unreachables
!
! Filtering packets leaving our network destined for the Internet.
! Deny all other packets. This is to deter our network from using spoofed IPs.
access-list 111 permit ip 2.2.2.0 0.0.255.255 any
access-list 111 deny ip any any log
!
! syslog server
logging 192.168.30.31

! banner
banner / Warning! Authorized Users Only! /
! The end of the configuration
```

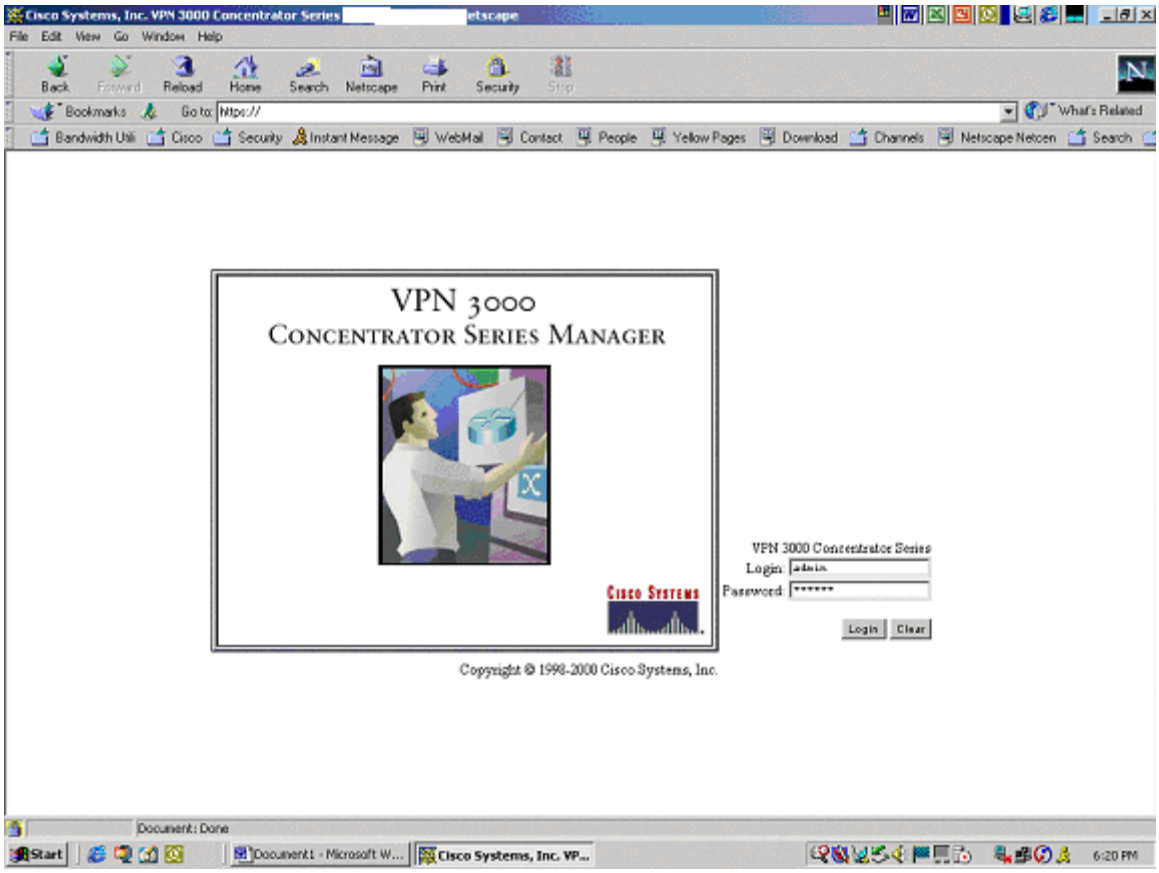
VPN Security Policy:

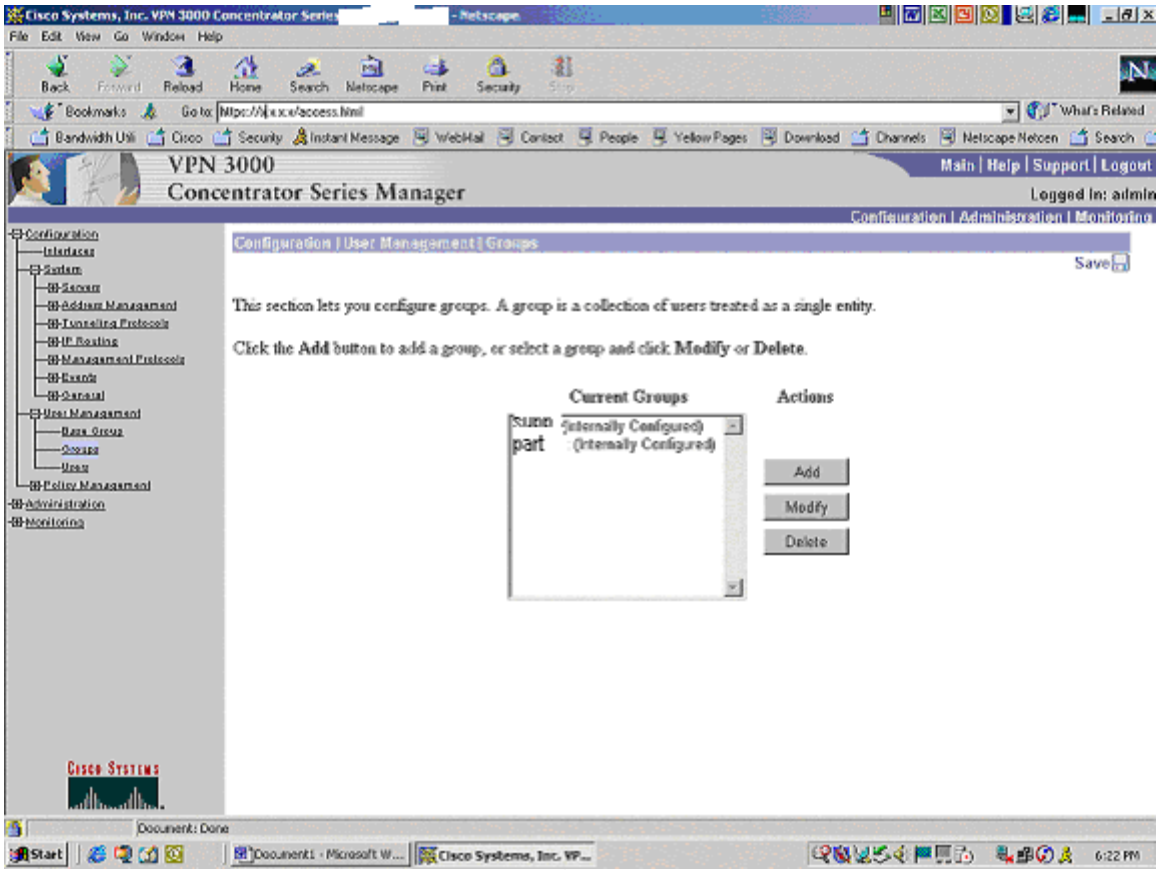
VPN is being utilized as the remote access method. We will be using VPN as the secure tunnel with the RSA SecurID authentication engine for token-based authentication. The combination of the two solutions makes a solid remote access solution.
VPN will be configured:

- to only allow IPSec traffic utilizing 168 bit encryption.
- group userid/passwd will be between 8-12 alphanumeric in length.
    - There will be one group per partner and supplier. Each group will have their own DHCP pool so their routing can be controlled at the VPN Concentrator or at the routers.
    - Their routing access will be defined by their business requirements.
- The authentication method for all groups will be SID (SecurID).
    - Each partner and supplier will receive a specified number of tokens that will make every receipt in each group accountable for their actions within this network.

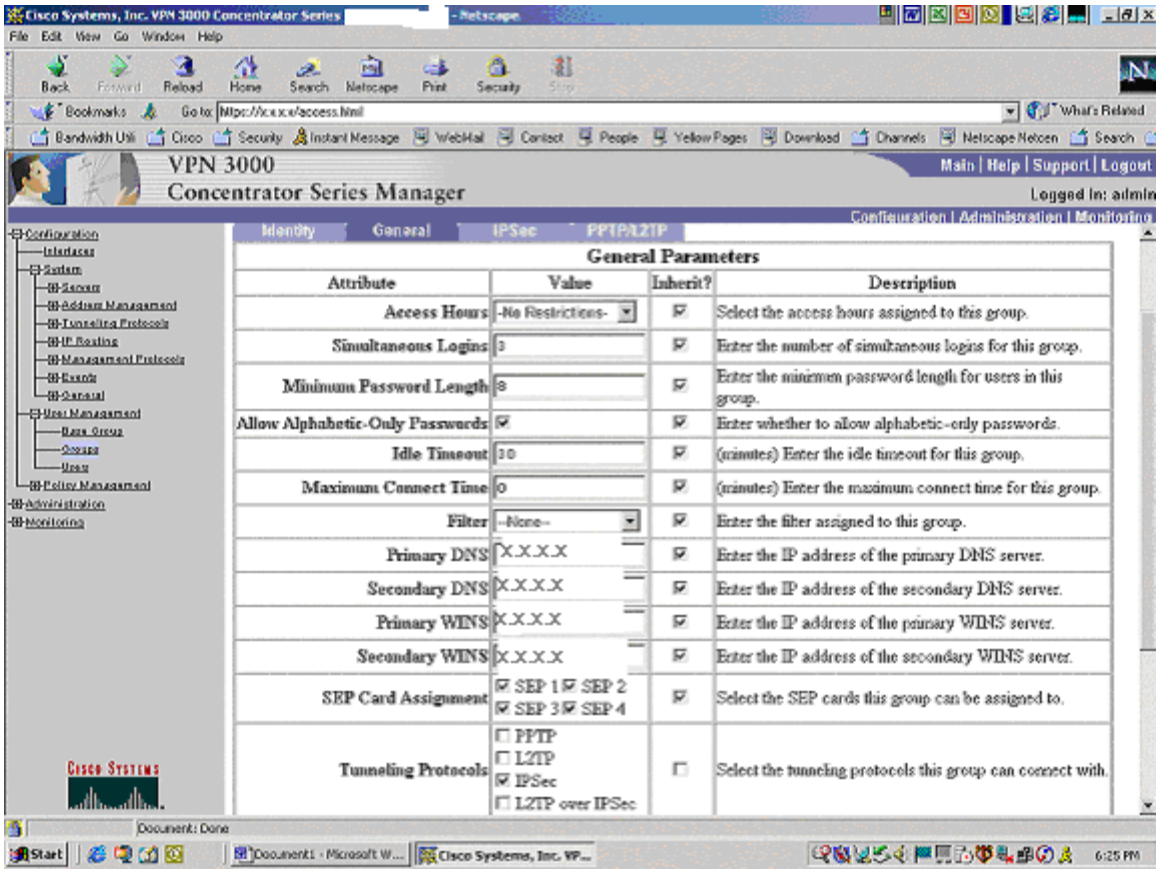
Here are some screenshots of what the VPN Concentrator will look like:

The login screen for Administrative purposes:





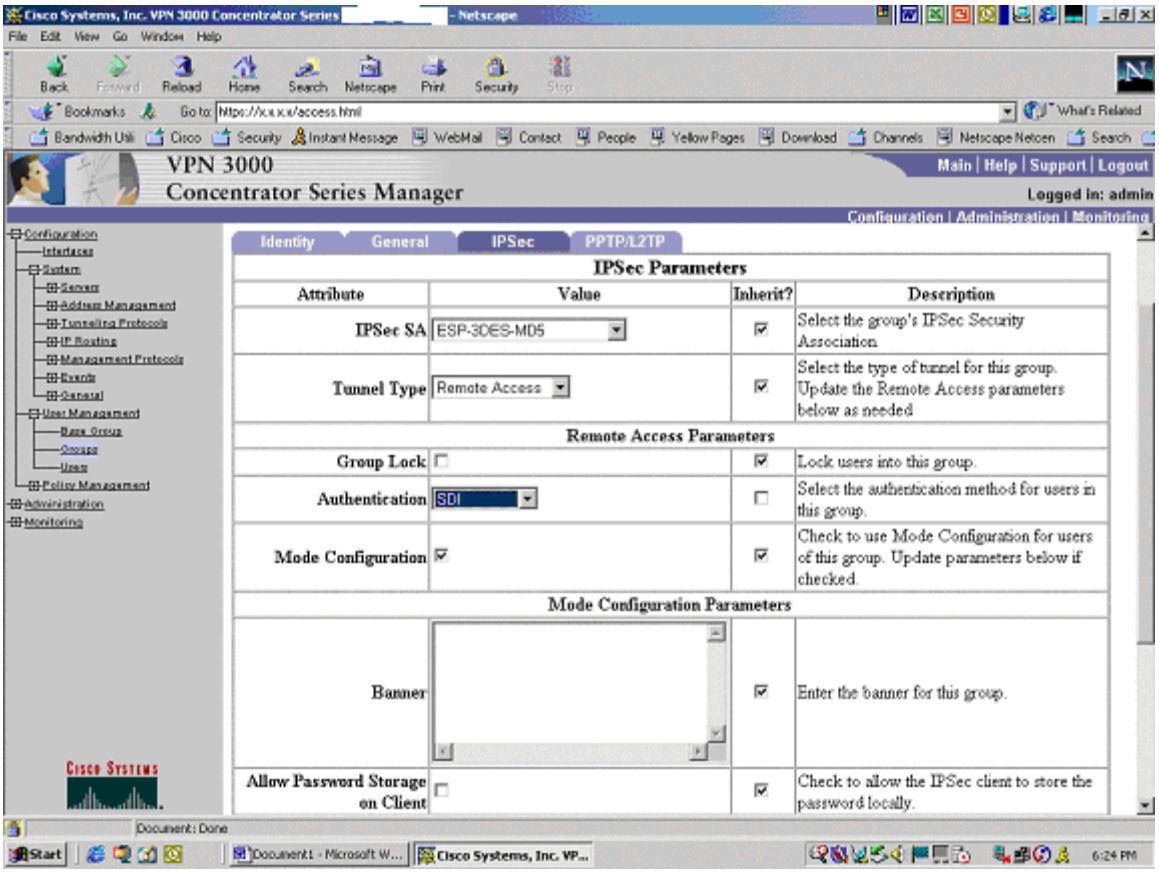
This is where the supp (suppliers) and the part (partner) groups are defined. Once they are defined, we will configure them.



Here are the General settings:

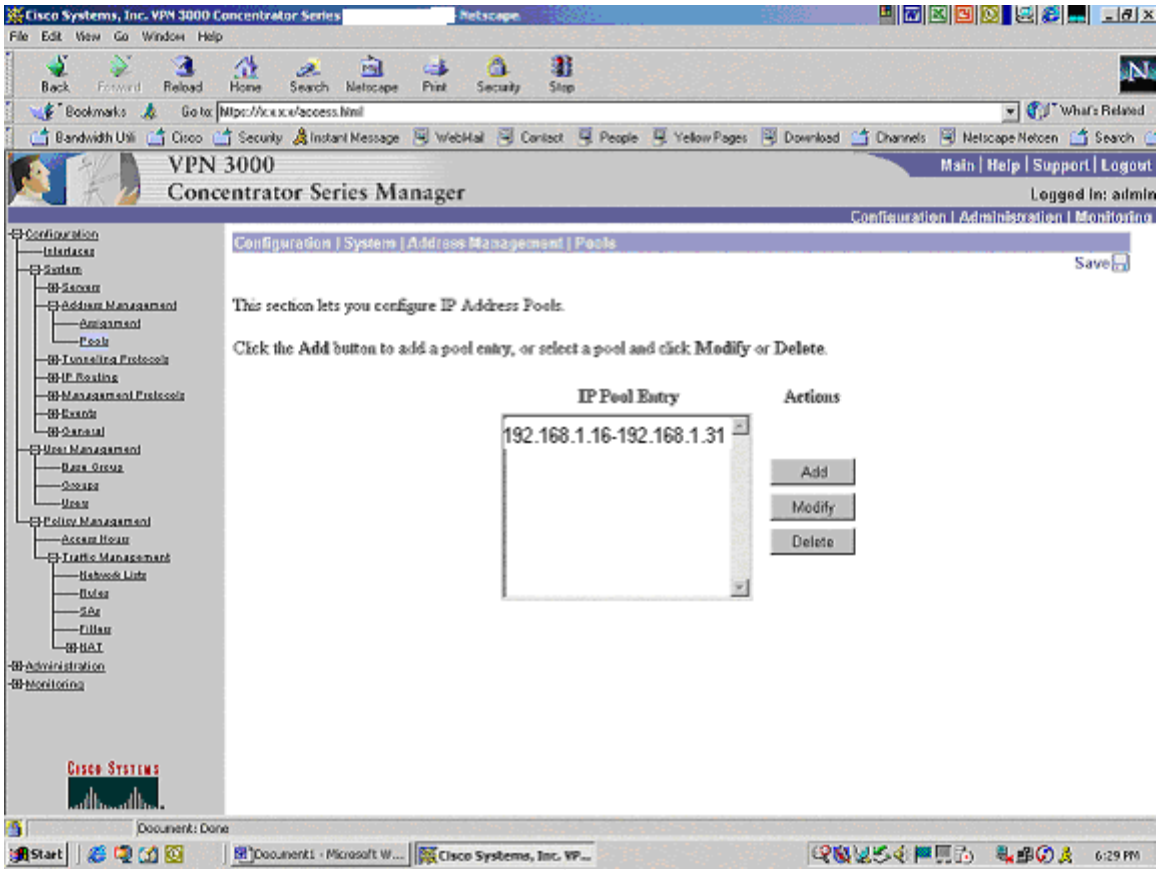
- The *Simultaneous Logins*, *Minimum Password Length* and *Allow Alphabetic-Only Passwords* box are irrelevant settings because the Ace Server will control these settings.
- The DNS and WINS servers will most likely not be configured. This will be decided on GIAC's requirements.
- The SEP card assignment is referring to the Security Encryption Processors. We will be utilizing only one as the other is in stateful fail-over mode.
- The only tunneling protocol that will be allowed is IPSec.
    - IPSec in my opinion is the most secure way to transfer traffic.

You will notice the check boxes under the Inherit heading. If the check boxes are checked then this group is using the base groups configurations. (I happen to know the base group is configured exactly like this.) If the boxes are unchecked then it means that this configure has been tailored towards this group.



We are now in the IPSec tab which controls the IPSec parameters and the Authentication for this group. The IPSec SA we have chosen is the ESP-3DES-MD5. This means that the Security Association is using:

- Encapsulation Payload (ESP) protocal
- 168 bit encryption (3.7x10(50th power)) will be the encryption algorithm (3DES)
- Message-Digest Algorithm (MD5) will ensure that the message actually came from the right person.

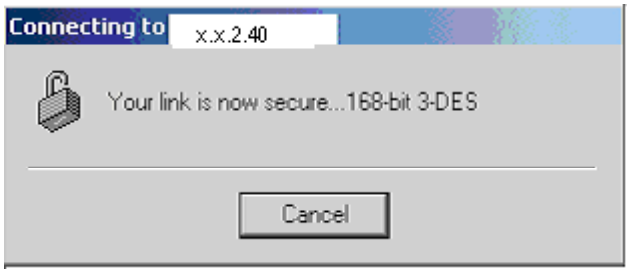


Here is where I configure the DHCP pool for each group. In this version that I am showing the DHCP pool is a global configuration for all groups. In the version that will be used (it has been released by Cisco and I tested it as part of there beta team) for GIAC Enterprises it will allow each pool to be assigned to the individual groups.

Here is how the groups would look:

- Suppliers
  - Tunneling protocol will be IPSec with 3DES only.
  - Authentication will be SecurID.
  - Dedicated IP range for trouble-shooting, monitoring and security purposes.
- Partners
  - Tunneling protocol will be decided upon the concensus of the location of our International partners. We will consult the International laws concerning encryption levels and the level of encryption will be decided upon the lowest allowed by a partners country.
  - Authentication will be SecurID.
  - Dedicated IP range for trouble-shooting, monitoring and security purposes.

If all settings are correct, when the user double clicks on the VPN icon on his/her desktop and they are authenticated in. They will see this message:



I.D.S. (Intrusion Detection System) Features:

We will be deploying two systems. This is a preferred configuration, which allows each system to be a check and balance for the other. Plus it offers the company flexibility to create filters as needed and also to have support. (Snort is very flexible and filters can be created when the need arises. ISS offers a dedicated support staff.)

They both will have two interfaces on the inside network. One will be on the management vlan (35) and the other will be running in promiscuous mode. Which means it has no IP address.

This is what it would like like:

> hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2 inet 192.168.30.31 netmask ffffff00 broadcast 192168.30.255
> hme1:flags=10008c3<UP,BROADCAST,RUNNING,NOARP,MULTICAST,IPv4 > mtu 1500 index 3 inet 0.0.0.0 netmask ff000000

The port that hme1 is plugged into will be spanned. The catalyst 6509 will send both source port traffic ports which consist of the inside interface of the primary and secondary Pix firewalls. These source ports will be mirrored to the destination port of the IDS hme1. This configuration is used for both IDS's.

In an effort to manage both of these systems from a control center, I will install the ISS console on a server in the center. The Snort system creates a directory per IP address that triggers an alert (rule). This can however be very difficult to quickly see what rules that get triggered and when. I will utilize SnortSnarf to build hourly reports of rules that have been triggered by src ip. (Tip: Snort and SnortSnarf create directories per source ip address that triggers a rule. If you have a busy site that triggers a rule quite often, you WILL hit a directory limit of the OS. On Solaris it's about 34000+ directories. You will have to customize your implementation to deal with this issue.)

Tying it together from a technical perspective:

- The Internet router will be utilized as the connection from the ISP to our systems. The router will also act as our first layer of security, filtering out IPs that should not be coming in. Plus filtering out ports like the small services. A benefit that might not be obvious yet is the border router can also play a key role in thwarting a DOS attack (more on this later).
- The FW-Internet is acting as my firewall and router. All servers behind the firewall will use the firewall interface for that vlan as its default route. This allows the firewall to utilize the security interface numbers. The firewall by default will deny everything coming in. The ACLs previously discussed allows port 80, 443 and 53 inside from the Internet.
- The VPN Concentrator is on vlan 50, which is outside of the range of the Pix. It has only been recently that VPN traffic works with a Pix firewall and I'm not one that likes to be the first to implement a new feature when it comes to security and Internet borders. The VPN client access is controlled by the group specifications. The traffic destined for the inside network will go through the MSFC in the Cisco Catalyst 6509.(Tip: If the traffic access becomes a burden on the Concentrator or it's decided to break up this functionality. The MSFC in the 6509 can easily take on this role by placing ACLs on the virtual interface on the MSFC.
- The FW-Corporate will be our connection between corporate headquaters and servers on the DMZ. This firewall will only allow port 22 (ssh), only specific hosts on port 23 (telnet), and only specific hosts on port 1521 (Oracle) through. The plan is to have each location self-relient for all services needed. The configuration will call for a pull concept from headquaters to the remote data center. The data center will not be able to establish a connection to headquarters. This is to keep headquarters isolated as best as possible from a security breach that could occur at the data center.
- Servers/Services
    - The web servers and SMTP servers will be on the same vlan but on dedicated servers. The web servers will be allowed to establish a connection with the Internet. Plus have the ability to establish a connection with the database vlan on port 1521. The SMTP servers can only establish a connection with the Internet.
    - The DNS server and Ace Server are placed one level higher than the web and mail servers. My thought is that DNS is more secure and less susceptible to attacks than the web and mail servers. (However, Linux and bind are starting to prove me wrong.) The DNS server has an ACL in the FW-Internet that allows outside connections to it for UDP port 53 queries only.

- The databases are above the DNS server, the web server and the SMTP server. This is to keep from any of these services from being compromised and then using that vlan to connect to the database. The database is allowed to talk to the web server only on port 1521.
- The IDS and syslog servers are on the second highest security level. This is because these services are less prone to attack as they have limited interaction with the lower security interfaces. The IDS will have two interfaces, one on this security interface for management and console updates, the other interface will be in promiscuous mode capturing data from the FW-Internet. The physical CAT 5 will have the transmit pair clipped in order to ensure the IDS system does not transmit anything while running on security interface100. The syslog server captures the logging from the FW-Internet and the border router. The FW-Internet is on a higher security interface, so there is nothing to do here.
- The security interface35 is the management vlan. This is how corporate manages the data center servers. This vlan is always higher than all services out at the datacenter. This is to keep from any server at the datacenter from establishing a connection to corporate headquaters. This is one more layer of security to assist in protecting corporate from any security breach at the datacenter.

Tying it together from a Business perspective:

- Customers will utilize port 80 and port 443. Port 80 is for normal web browsing of the site and port 443 (SSL) will be utilized for transactions or viewing of there account. The customer simply types in www.gaiccorp.com and away they go.

- Partners will double click on the VPN icon on there desktop. This icon has their specific group userid/passwd in it. This group authentication will then ask for the SecurID token userid/passwd. If the passwords match, then they are authenticated on the network. The group authentication is what handles the resources (hosts/services) they are allowed access to. This is still to be determined.

The suppliers have the same setup as the partners. The only difference will be their group userid/passwd and DHCP IP range. This is to distinguish the two from each other and for greater flexibility on resources they are allowed to access.

Audit of Security Architecture

GIAC Enterprises has commissioned us to conduct a security audit on there systems. During this time we will be working with GIAC's network department to ensure they are well informed of our actions. It has been decided the audit will take place each morning at 4AM for a week starting on Monday. This is to minimize exposure if a piece of equipment acts negatively to our security audit. Half of the GIAC network team will be at the office during this time. The other half of the team is left to daily tasks and job duties. The project is projected to take 5 days at 8 hours a day. The statement of work at an hourly rate of 200.00 will cost $8,000.00.

The audits considered risky will be conducted early in the morning with the less intrusive audits running into business hours. GIAC has advised us the site cannot be down for any length of time during this audit. We consider any audit directed specifically at the firewall or router as being risky considering the circumstances. (note: I have seen audits done on firewalls and routers. You might not want to be the one that finds out that a certain crafted packet throws the OS into the bit bucket. It happens, so take precautions.)

Here are some considerations that need to be taken. This audit is to ensure that all perimeter configurations are functioning as configured. Plus we will ensure that basic security practices are being taken. Some examples of these practices would be your own registered IP block is not being used as the source for inbound traffic. In addition, your DNS server will not issue a listing of the zone or zones.

We will first start with information gathering. I will use Sam Spade 1.14, NeoTracePro, and nslookup to ensure data integrity.

```
C:\>nslookup
Default Server:  ns1.someisp.com
Address:  x.1.2.3

> set type=any
> giac.com
Server:  ns1.someisp.com
Address:  x.1.2.3

giac.com
      primary name server = ns1.giac.com
      responsible mail addr = tech.giac.com
      serial  = 2001345678
```

refresh = 28800 (8 hours)
retry = 7200 (2 hours)
expire = 604800 (7 days)
default TTL = 86400 (1 day)
giac.com nameserver = ns1.giac.com
giac.com internet address = 2.2.2.31
giac.com MX preference = 9, mail exchanger = postoffice.giac.com
giac.com nameserver = ns1.giac.com
ns1.giac.com internet address = 2.2.2.33

Know lets find out the IP range they are registered for:

Sam Spade IP block output:

03/28/01 19:12:10 IP block www.giac.com@whois.geektools.com
Trying 2.2.2.31 at ARIN
Trying 2.2.2 at ARIN
Somedatacenter, Inc. (NETBLK-GIAC) NETBLK-GIAC
2.2.2.0 - 2.2.2.255

From the information above, we know the IP(s) for their web servers, mail server and where their DNS server is. Plus we also know the IP block that GIAC would use to allow external access to an internal service. This information will be used extensively during the security audit.

By using the information above gathered we now know these bits of information:

- There registered IP range is 2.2.2.0/24
  - There outside services are somewhere in this IP address range.
- We know the IP address for their web server(s), DNS server(s) and mail server(s).
  - However, these are the IP that resolve. They could offer other services in their IP range that are not in DNS. Maybe VPN or testing servers…????

The firewall assessment:

Here is the output from the firewall syslog from a TCP and a UDP scan.

Using nmap with this command: [root-331]:./.nmap -vv -sT 2.2.2.0/24
TCP Scan starts now:

Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied from x.x.34.35/63213 to 2.2.2.31/214 flags SYN on interface outside
Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied

from x.x.34.35/63214 to 2.2.2.31/957 flags SYN on interface outside
Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied from x.x.34.35/63215 to 2.2.2.31/907 flags SYN on interface outside
Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied from x.x.34.35/63216 to 2.2.2.31/4672 flags SYN on interface outside
Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied from x.x.34.35/63217 to 2.2.2.31/455 flags SYN on interface outside
Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied from x.x.34.35/63218 to 2.2.2.31/763 flags SYN on interface outside
Mar 29 20:32:58 [x.x.x.x.2.2] %PIX-2-106001: Inbound TCP connection denied from x.x.34.35/63219 to 2.2.2.31/535 flags SYN on interface outside

Using nmap with this command: [root-331]:./.nmap -vv -sU 2.2.2.0/24
(this command has to be done as root)
UDP Scans starts now:

Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/151 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/989 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/14 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/438 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/263 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/2106 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/739 on interface outside
Mar 29 20:35:30 [x.x.x.x.2.2] %PIX-2-106006: Deny inbound UDP from x.x.34.35/4619 to 2.2.2.31/687 on interface outside

Though the entire log is not displayed, it is appearant from the logs that the primary firewall is denying ports and/or protocols that are not allowed. Now lets verify that allowed ports like 80 are accepting traffic. Again a browser to 2.2.2.31 can be used or nmap with this command:

[root-336]:./nmap -vv -p '80' 2.2.2.31

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect() scan. Use -sP if you really don't want to portscan (and just want to see what hosts are up). Host

www.autotrader.com (2.2.2.31) appears to be up ... good.
Initiating TCP connect() scan against www.giac.com (2.2.2.31)
Adding TCP port 80 (state open).
The TCP connect scan took 0 seconds to scan 1 ports.
Interesting ports on www.giac.com (2.2.2.31):
Port State Service
80/tcp open http

Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds

Here is port 25 being verified on the mail server:

[root-329]:./nmap -vv -p '25' 2.2.2.32

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect() scan. Use -sP if you really don't want to portscan (and just want to see what hosts are up).
Host (2.2.2.32) appears to be up ... good.
Initiating TCP connect() scan against (2.2.2.32)
Adding TCP port 25 (state open).
The TCP connect scan took 0 seconds to scan 1 ports.
Interesting ports on (2.2.2.32):
Port State Service
25/tcp open smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds

The –p option allows me to scan a specific port. The –vv means very verbose. '25' is specifying port 25 and the IP is the IP address of the mail server. So we can see that SMTP is available on this IP address.

The information above proves that our Firewall is denying and permitting based on our configuration. Now lets try a packet that is abnormal. During the writing of this paper this teardrop attack came across from the wild. This is the real thing (IPs have been altered to protect…who??):

Mar 16 10:08:57 [x.x.x.x.2.2] %PIX-2-106020: Deny IP teardrop fragment (size = 20, offset = 8) from x.x.x.x to y.y.y.y

A great resource for understanding this type of attack is "Network-Based Intrusion Detection Analysis and Intrusion Detection Workshop," by Stephen Northcutt. (Note: if your going to play around with this type of attack, it's highly recommended you do this in a controlled environment. Some people might take this type of attack seriously considering someone has gone out of there way to send a potential D.O.S. attack there way ;-))

Before we end the audit we will verify that the DNS server is configured with basic security practices.

Can anyone list the DNS domain or conduct zone transfers.

```
C:\>nslookup
Default Server:  giac_corporate
Address:  x.x.x.x

> server x.x.x.x
Default Server:  ns1.giac.com
Address:  x.x.x.x

> ls -d giac.com
[ns1.giac.com]
*** Can't list domain giac.com: Query refused
```

This proves that the allow-transfer is set to none. Which also means that zone transfers are not allowed on TCP port 53. Here is what it would look like in /etc/named.conf

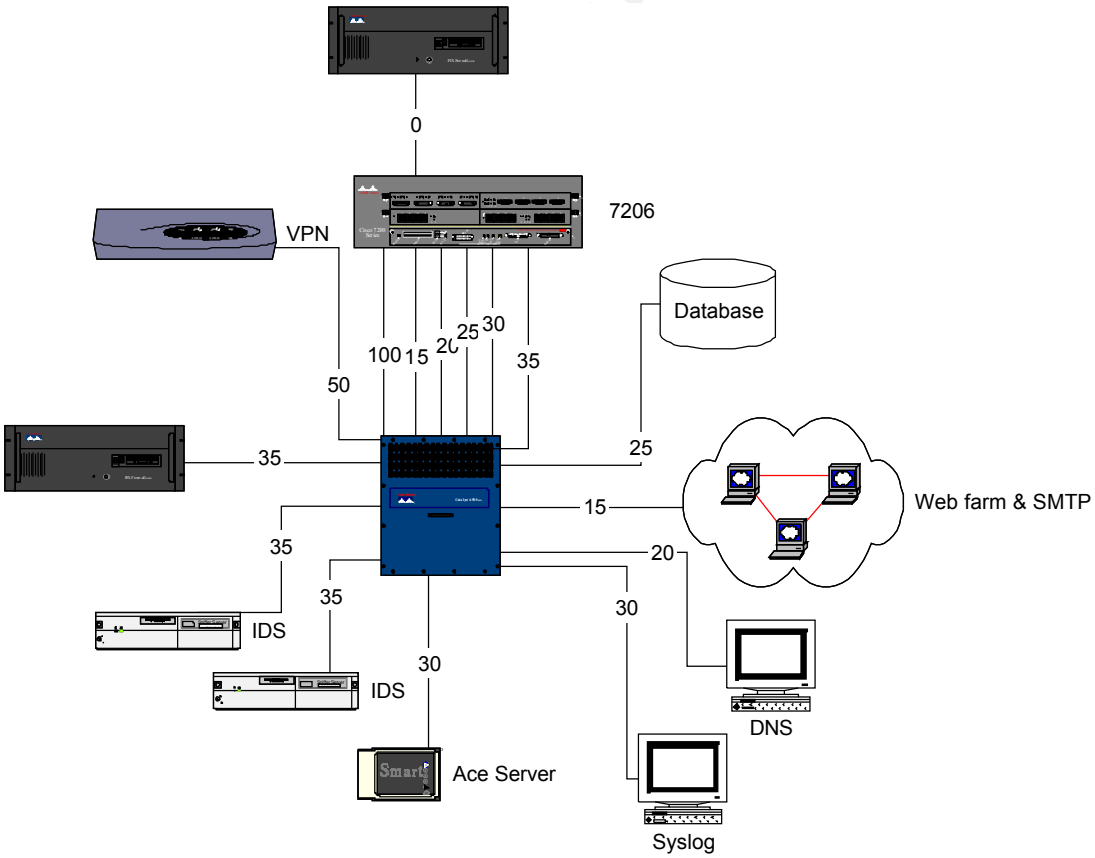
```
zone "giac.com" IN {
      file "giac.com.bk";
      allow-update { localhost; };
      allow-transfer { none; };
};
```

Perimeter Analysis

From the information I have gathered from my assessment and also from looking at the architecture. I have come up with some recommendations.

Architecture:

I like the design though I'm concerned about scalability. The architecture is designed around a fixed number of physical interfaces. If GIAC was to acquire enough new companies or decide to offer services that might best sense on a separate network, this architecture would most likely run into scalability issues. My recommendation would be to replace the Cisco Router 3640 with the Pix firewall and let the pix act as a stateful perimeter router. A Cisco 7206 with the IOS Firewall Feature Set, version 12.0(T) would take the place of the Pix Firewall. This IOS has the same capability for the security levels per interface except that these interfaces are virtual instead of physical. Previously, the design had the Pix acting as the router and firewall. Here I have changed the roles for the router to act as the firewall.

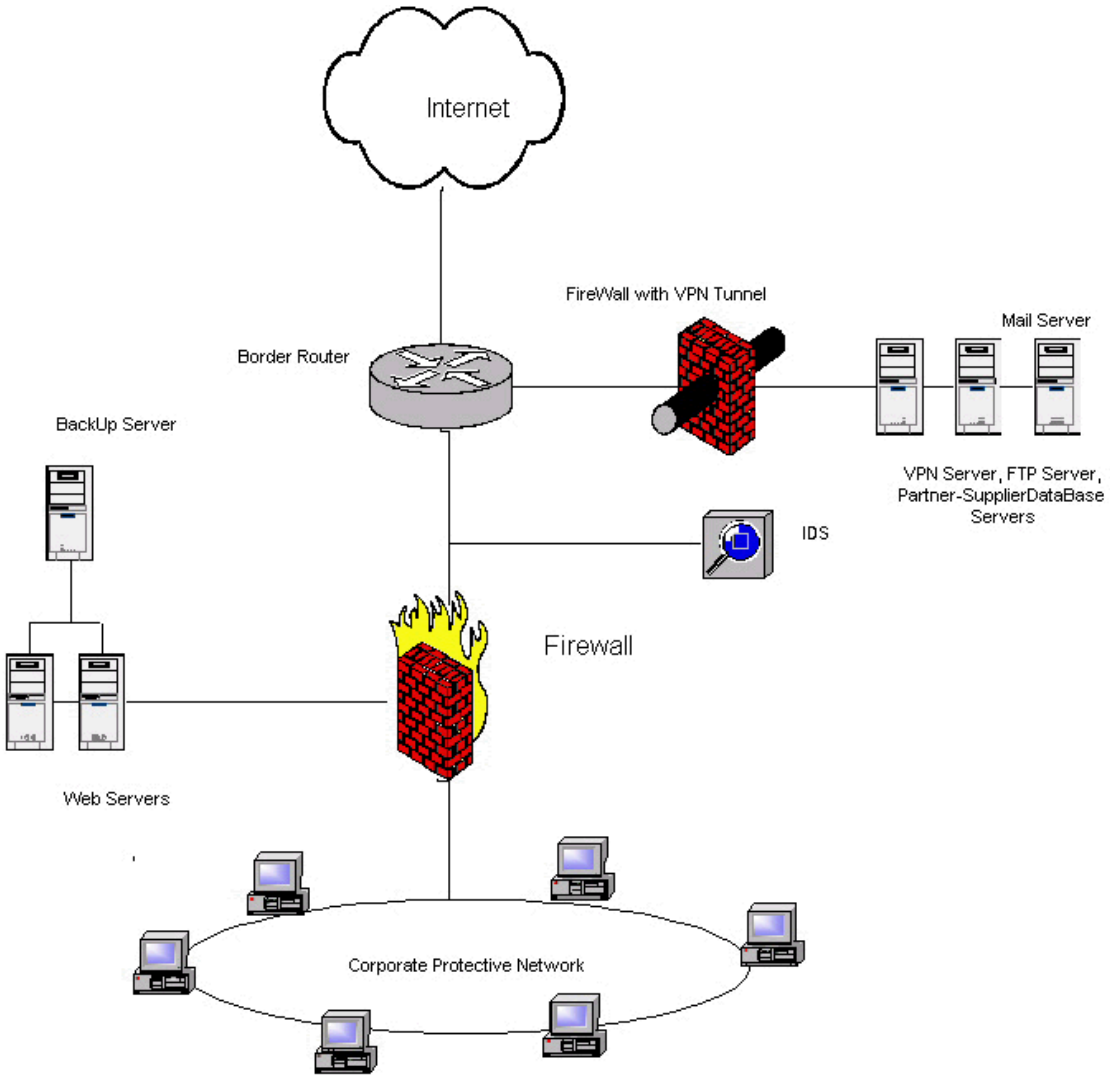


Another recommendation would be to verify if the firewalls are configured with the correct static statement. Here is what a static statement is defined as:

> The static command creates a permanent mapping (called a static translation slot or "xlate") between a local IP address and a global IP address. Use the static and access-list commands when you are accessing an interface of a higher security level from an interface of a lower security level; for example, when accessing the inside from a perimeter or the outside interface.
> Reference: Cisco Web Site: url.
>
> Here is what the command looks like:
>
> static [(internal_if_name, external_if_name)] global_ip local_ip [netmask network_mask] [max_conns [em_limit]] [norandomseq]
> Reference: Cisco Web Site: url.

The recommendation pertains to the max_cons and em_limit. If either one of these are not defined they will default to zero which means unlimited. The max_cons is the number of connections for this IP translation. The em_limit is the number of half open connections to allow for this IP translation. Again if the number is not specified then it defaults to zero which means unlimited. This is a bad thing because we have now left ourselves open to a flood attack.

Design Under Fire



The network design shown above was done by a certified GIAC student named, Deepak Midha. The purpose of the design under fire is to show that firewalls are not perfect network defense appliances or software. The following paragraphs do not represent Deepaks inability to design a good secure network architecture but to show that no vendor has come up with a flawless software/appliance.

The above design utilizes Pix 515s. This firewall with most versions of Cisco IOS is prone to a DOS attack exploited by a fragment attack.

Explanation:

Most Cisco Pixs are configured by using static translations for services like DNS, SMTP

and HTTP. When a fragmented packet, split into 2 with the FIN-flag set, it was noticed that the packet with the TCP-header was correctly dropped but the second part of the fragment was let through to the host. The DOS attack is easily exploited by sending a lot of fragmented packets to a port that is allowed access through the Pix.

This firewall under a denial of service attack by 50 compromised cable modem/DSL systems using TCP SYN, UDP or ICMP floods does have countermeasures to mitigate the attack but only if configured to do so. Here is how to configure a Pix firewall to deal with a DOS attack with the three attacks listed above.

To thwart a TCP SYN flood, use a non-zero embryonic limit in the static command. This was discussed earlier in the paper but can also be viewed here in more detail:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/commands.htm#xtocid223367

By using a non-zero number you have configured the Pix to limit the amount of half open connections that it will retain. Without this limit, the Pix can use all resources to retain the half open connection until it times out. Which would most likely be after the attack is done.

By looking at the design on the previous page, I would try to compromise meaning gain unauthorized access to IIS Server(s) through ODBC Data Access with RD5. The heart of any company is usually its data. The best way to a database is through its weakest link/connection…i.e. the web server. The firewall is configured to allow outside TCP port 80 traffic to access the web server. I will be going after an expoit in IIS servers that was found in 1998 but lately proven to be still very exploitable. The exploit is going after an IIS web server that has not been properly patched that has the component MDAC (Microsoft Data Access Components) installed be default.

ISSUE
=====
The RDS DataFactory object, a component of Microsoft Data Access Components (MDAC), exposes unsafe methods. When installed on a system running Internet Information Server 3.0 or 4.0, the DataFactory object may permit an otherwise unauthorized web user to perform privileged actions, including:
- Allowing unauthorized users to execute shell commands on the IIS system as a privileged user.
- On a multi-homed Internet-connected IIS system, using MDAC to tunnel SQL and other ODBC data requests through the public connection to a private back-end network.
- Allowing unauthorized accessing to secured, non-published files on the IIS system.

(taken from Stanford's SUNSeT Security Advisory.

What happens is that an external user can use the web servers ability to read crafted url strings that are passing connection strings to the backend database. Unfortunately there a still many databases that have the default passwords or easily guessed passwords in production.

For more information and for instructions to patch this problem, please visit Microsoft's web site here.