Global Information Assurance Certification Paper

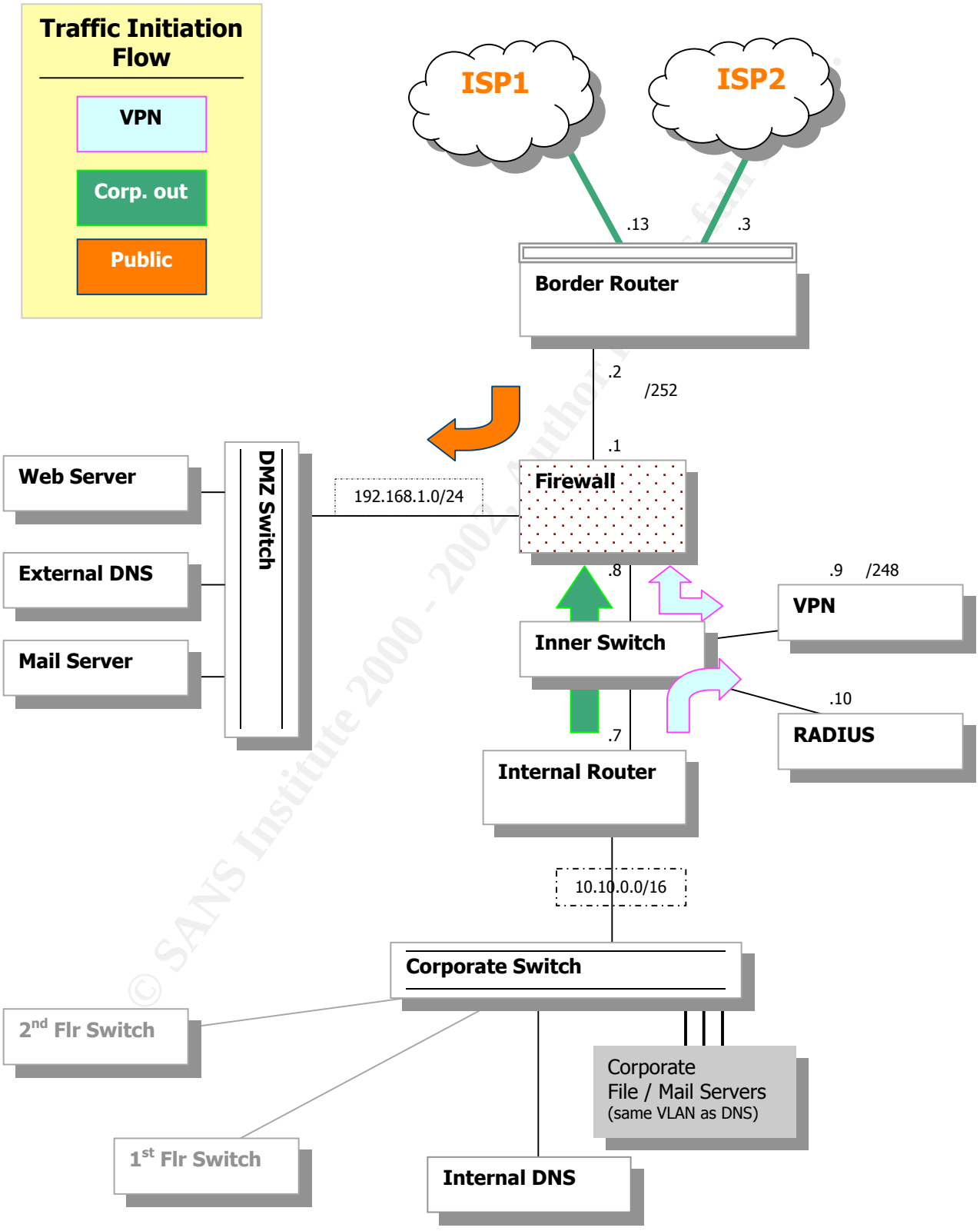
Tracy M. Thurston
GCFW v1.6

SANS GIAC Firewalls, Perimeter Protection, and VPNs
GCFW Certification Practical

GIAC E-Fortune Cookies Company
Security Architecture, Design, and Audit

---

1 - Security Architecture



I. Device Specifics

Device	Hardware	Software
Border Router	Cisco 3620	12.2.3
Firewall	Cisco PIX 515	6.0.1
VPN	Cisco VPN 5002	6.0.19
External DNS	Netra X1	Solaris 2.9 patched, tripwire, tcpwrappers installed
Internal DNS	Netra X1	Solaris 2.9 patched, tripwire, tcpwrappers installed
Internal Router	Cisco 3620	12.2.3 fw/ipsec plus
RADIUS	Cisco Secure ACS	v2.6 (Win2000 Server)
DMZ Switch	Cisco 2924	12.1.9
Web / SSL Server	X86	Win2000 Server - Hardened non-default install – all updates to date.
Corporate Switch	Cisco 2948	12.1.9

II. Physical and administrative access security

All equipment listed is located at corporate headquarters in a physically secured room. The routers, switches, primary firewall and VPN use RADIUS for access and access is only allowed from network engineering staff members. The primary firewall is only accessible from console or terminal server on the private lan.

III. Device purposes, security roles and placement functionality

The *Border Router* provides redundant Internet connectivity via two separate ISPs and initial packet filtering for traffic entering the network.

The *Firewall* provides the access control to protect our publicly accessible servers while shielding our corporate network space. This version of software provides for port mapping of services, which will obfuscate network information such as addressing, relationship, and layout. A separate interface will provide connectivity to the VPN server, separating it from the other public traffic area. It can then pass unencrypted to the internal router which can inspect the traffic provide access via ACLs.

The *DMZ Switch* provides connectivity to our public servers and an access point for an IDS.

The *External DNS, Web Server* and *RADIUS* server are provided on their own interface off the firewall because they are public servers. We can filter on the services needed while protecting our corporate LAN from any of this public traffic.

The *Web Server* will host the company web site and provide SSL shopping. This box also hosts an ftp server for non-confidential data. All confidential data exchange will be done via VPN.

The *VPN concentrator* needs to be publicly accessible for remote access connections. These clients will all be RADIUS authenticated users. Once authenticated, the username associates the user with a group within the VPN concentrator, with will determine the network ip address that is assigned. They then get access to the corporate via the Internal Router. The unencrypted traffic passes through here we can use the source network to determine via ACL, what servers are accessible.

The *Internal Router* will provide routing of VLANs off the corporate switch. An additional firewall is provided with an IOS firewall feature set. Unencrypted VPN traffic will also pass through here, so will define access rules here. This firewall feature set will help us in restricting and auditing of corporate internet use as well.

The *Corporate Switch* will minimize broadcasting and provide security between departments as needed via VLAN separation. Will also run Snort here as IDS alerting system.

The *External DNS* will answer queries from outside about our external services.

The *Internal DNS* will service the internal network including host machines, and internal mail and file servers.

2 – Security Policy

Network Acceptable Use Policy

Employees
Employees of company will have access to internet for research and other work related purposes. This excludes external mail services via pop or web mail service, any instant messaging service, remote control services and applications including but not limited to pcAnywhere, RemoteDesktop, etc. Remote access will be provided via VPN services for access to corporate file servers and mail.

Customers
Customers will have access to the company web server which provide for secure shopping via 128 bit SSL

Suppliers, Partners
Suppliers and partners shall have access through the a VPN consisting of GIAC's Cisco 5008 VPN Concentrator and a router residing on the partner / supplier Internet access point. Encryption shall be 3DES and MD5 for authentication.

Part 1 - Defined

Border Router

Password encryption will help keep our router password a bit more secret. It shows up encrypted in the configuration listings, so if an engineer were to get pulled away from her desk with the configuration displayed (and didn't lock her workstation) someone could not get the passwords for later access. The timeout feature will also aid us in protecting from this type of security breach.

```
service password-encryption
enable secret 5 $1u8#$%hjufr$@&Y4H#56K!M2&%$KO72J4K3
enable password 7 089097345PIW891B
```

Warning banner
Cases against hackers have actually proven to be easier to prosecute if warning banners stating that unauthorized access was, in fact, illegal.

```
banner login ^C ****************************
Should you BE here?
Access for authorized users only.
Unauthorized access is prohibited and punishable by law.
****************************^C
```

We will block any attempted access from obvious spoofed addresses. Traffic received from the internet should not be private addresses, loopback, or from anything inside the border router. Since these all can be filtered on the source address, we can use a standard access list, which is less overhead on the router, but since we also need to define services to block by port on the same interface, we will use extended.

```
access-list 120 deny ip host 127.0.0.1 any log
access-list 120 deny ip 10.0.0.0 0.255.255.255 any log
access-list 120 deny ip 172.16.0.0 0.240.255.255 any log
access-list 120 deny ip 192.168.0.0 0.0.255.255 any log
access-list 120 deny ip xxx.xxx.xxx.0 0.0.0.240 any log
access-list 120 permit ip any any log
```

We also want to block any service ports that should never be entering or exiting this router, such as NetBios traffic - ports 135-139, 445 (Windows 2000) (pg 129 in 2.2) Also we are using ssh, so we will block telnet. Unix services that are not offered such as portmapper, rlogin, rsh, and rexec will also be blocked here. We normally want to log everything but NetBios scans happen so much, there would not be enough disk space on the planet.

```
access-list 120 deny ip any any range 135 139
access-list 120 deny ip any any eq 445
access-list 120 deny tcp any any eq 23 log
access-list 120 deny ip any any eq 111 log
access-list 120 deny ip tcp any any range 512 514 log
```

We want to set timestamps on our log messages for aid in troubleshooting. This will also allow us to see the correct time of any security breaches and, with the use of ntp, synchronize traffic logs between devices. Set the internal log buffer size, set the logging level, and the source interface, which will make logging by device easier to understand in the syslog server. Using ntp across all of our network devices will ensure that all of the logs are in sync and accurate.

```
service timestamps log datetime localtime show-timezone
logging buffered 4096 debugging
logging trap debugging
logging source-interface Serial0/0
logging xxx.xxx.2.7
ntp update-calendar
ntp server 172.22.66.18 prefer
```

Block unnecessary service

Drop packet with source route option set

```
no ip source-route
```

Turn off finger service

```
no ip finger
```

Don not accept boot configuration from lan

```
no ip bootp server
```

Disable access to the Echo, Discard, Chargen, and Daytime ports

```
no service  tcp-small-servers
no service  udp-small-servers
```

Disable Cisco Discovery Protocol (no need to give away information about hw/sw)

```
no cdp run
```

RADIUS authentication

Configuration explanations can be found at
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt1/scathen.htm#30132

```
aaa new-model
aaa authentication login default group radius enable
aaa authentication login linmethod group radius enable
aaa authentication login vtymethod group radius enable
aaa authentication login conmethod group radius enable
aaa accounting update newinfo
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting system default start-stop group radius
radius-server host xxx.xxx.xxx.9 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key $0m3th1ngGr3@t
```

Restrict telnet access to inside address space only

```
access-list 50 permit xxx.xxx.nat.space
access-list 50 permit sys.log.add.res
access-list 50 deny   any log

line vty 0 4
 access-class 50 in
```

On our interfaces facing the internet, we will restrict ICMP unreachable message responses. ICMP unreachables can help potential hackers in mapping your network.

```
interface Serial0/0
 description Schmerio link to Internet
 ip address xxx.xxx.xxx.13 255.255.255.252
 no ip unreachables

interface Serial0/1
 description SchmobalX link to Internet
 ip address xxx.xxx.xxx.3 255.255.255.252
 no ip unreachables
```

Since we will have public IP addresses coming off the inner switch for VPN and RADIUS, we will put a static route to them on the border router.

Primary Firewall
See Appendix A for specific commands referenced below.

- Fixup protocol

This command enables the use of a service or protocol through the PIX Firewall. The ports you specify are those that the firewall listens to for each respective service. This can prevent embedded commands within a protocol and traffic invalid for the service specified on that port.

- Access-lists

The access lists on the firewall will specify what protocols and port are allowed per source and destination specified.

- NAT

NAT through the firewall is actually PAT in this case as it is a many-to-one mapping. This allows out internal users with private addresses to get mapped to the public address for access to the internet. NAT is a good security implementation as it "hides" you internal network addresses and does not allow direct access.

- Deny ICMP to firewall

Since there is no reason we would want to have the firewall respond to pings, we will deny ICMP echoes to the outside interface. This helps obscure the network further to potential hacks and also alleviates any vulnerability to the PIX itself from a DoS attack.

- Port redirection

We will use port redirection to further obscure out network and public servers. This version of PIX software allows an address and port to specifically map to another address and port. The same address and *different* port may map to a different address altogether. With this feature it would be possible for all of your network services to seem as though they were on the same box.

- URPF (Unicast reverse path forwarding)

"ip verify reverse-path interface <int>" causes the firewall to perform a reverse route lookup for source IP addresses (per session) These two commands protect the outside interface from network ingress attacks from the Internet, and the inside from egress attacks from users on the inside network.

- IP audit

"IP audit info action alarm" and "ip audit attack action alarm" will look for signatures considered informational or attacks and report them to the syslog server.

- Timeouts

Timeout settings are a security setting as well as a resource management setting. These values specify when each particular type or state of connection will be reset.

- Floodguard

This command allows the firewall to protect itself in case of an attack in that if the resources become depleted, it will actively reclaim them in order of timewait, finWait embryonic and idle connections.

VPN Concentrator

Our VPN concentrator will allow us multiple partner tunnels as needed for business partners, suppliers, and future needs. This will also provide secure remote access for employees.

The Cisco VPN 5002 Concentrator allows up to 255 Customer Virtual Contexts (CVC) and up to 5,000 concurrent tunnels per card. Each CVC is completely shielded from others for security between separate entities. The Main CVC holds routing and default configurations for the appliance itself, as well as knowledge of all CVCs.

```
[ General ]
Context         = partners

[ Tunnel Partner VPN 1 ]
SharedKey               ="G1@Crul3$"
Peer                    = "10.10.10.0/24"
Partner                 = xxx.xxx.xxx.xxx
BindTo                  = "ethernet 1:0"
KeepaliveInterval       = 120
InactivityTimeout       = 900
KeyLifeSecs             = 10000
Transform               = esp(md5,3des)
```

```
LocalAccess          = "10.10.0.0/16"
KeyManage            = Reliable
Mode                 = Main

[ IP Ethernet 0:0.1 ]
IPAddress            = 10.10.253.253
SubnetMask           = 255.255.255.255
Mode                 = Routed
VLANID               = 101
Encapsulation        = dot1q

[ IP Static ]
10.10.0.0 255.255.0.0 xxx.xxx.xxx.7 1

[ VPN Users ]
myuser@partnergroup config="partnergroup" sharedkey="cisco"

[ VPN Group "partnergroup" ]
StartIPAddress       = 10.10.30.1
MaxConnections       = 40
AssignIPRADIUS       = Off
IPNet                = 10.10.0.0/16
Transform            = esp(md5,3des)

[ Radius "partnergroup" ]
PrimUseSecret        = On
AuthPort             = 1645
ChallengeType        = CHAP
Authentication       = On
BindTo               = "ethernet 0:0"
PrimAddress          = "xxx.xxx.xxx.9"
Secret               = "ucantsee"
```

Our VPN concentrator will have a public address on the interface off the firewall, statically mapped through the firewall. The other interface will also be public off the internal router. This will allow direct access to the VPN through the firewall and access from internal user to communicate with VPN partners. The inside firewall interface and outside internal router interface will also have private IP addresses so that internal users can get out to the firewall to be NAT-ed. We will still be able to inspect the VPN traffic on the internal router.
Here is a snapshot of the router configuration on VPN partners' side.

```
crypto isakmp policy 1
 hash md5
```

```
 authentication pre-share
 lifetime 10000
crypto isakmp key G1@Crul3$ address xxx.xxx.xxx.10
!
crypto ipsec transform-set giacset esp-3des esp-md5-hmac
!
crypto map giacmap 1 ipsec-isakmp
 set peer xxx.xxx.xxx.10
 set security-association lifetime seconds 10000
 set transform-set giacset
 match address 101

interface Serial0/0
 description connected to internet
 ip address xxx.xxx.xxx.xxx 255.255.255.252
 crypto map giacmap

interface FastEthernet1/0
 description connected to corp
ip address 10.10.11.1 255.255.255.0


access-list 101 permit ip 10.10.11.0 0.0.0.255 10.10.0.0 0.0.255.255
```

Internal Router –
Our internal router has an interface to the firewall (fa1/0), an interface to the VPN (fa1/1), and an interface to the inside (fa1/2).

Here we can:

- enforce some aspects of our security policy with Context Based Access Control (CBAC)
- route internal users to VPN gateway
- inspect incoming traffic from the VPN
- route between VLANs on the corporate switch

Here are our options for CBAC:

R2# ip inspect ?

```
  alert-off          Disable alert
  audit-trail        Enable the logging of session information (addresses and bytes)
```

```
  dns-timeout          Specify timeout for DNS
  max-incomplete       Specify maximum number of incomplete connections before
                         clamping
  name                 Specify an inspection rule
  one-minute           Specify one-minute-sample watermarks for clamping
  tcp                  Config timeout values for tcp connections
  udp                  Config timeout values for udp flows
```

```
R2(config)#ip inspect name allwork ?
  cuseeme    CUSeeMe Protocol
  fragment   IP fragment inspection
  ftp        File Transfer Protocol
  h323       H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
  http       HTTP Protocol
  netshow    Microsoft NetShow Protocol
  rcmd       R commands (r-exec, r-login, r-sh)
  realaudio  Real Audio Protocol
  rpc        Remote Prodedure Call Protocol
  rtsp       Real Time Streaming Protocol
  smtp       Simple Mail Transfer Protocol
  sqlnet     SQL Net Protocol
  streamworks  StreamWorks Protocol
  tcp        Transmission Control Protocol
  tftp       TFTP Protocol
  udp        User Datagram Protocol
  vdolive    VDOLive Protocol
```

Here we could choose h323, realaudio, rtsp, cuseeme and do audit-trail on them. We could also check fragment and alert and audit-trail on that.

```
R2(config)#ip inspect name allwork tcp ?
  alert        Turn on/off alert
  audit-trail  Turn on/off audit trail
  timeout      Specify the inactivity timeout time
  <cr>
```

```
ip inspect name allwork realaudio audit-trail on
```

We may also want to turn on max-incomplete in case a DOS attempt did get through the firewall or VPN.

```
R2(config)#ip inspect tcp ?
  finwait-time        Specify timeout for TCP connections after a FIN
  idle-time           Specify idle timeout for tcp connections
```

max-incomplete Specify max half-open connection per host
synwait-time Specify timeout for TCP connections after a SYN and no further data

```
ip inspect tcp max-incomplete host 75
```

Route internal users to VPN

```
Ip route 10.0.0.0 255.0.0.0 xxx.xxx.xxx.10 255.255.255.248
```

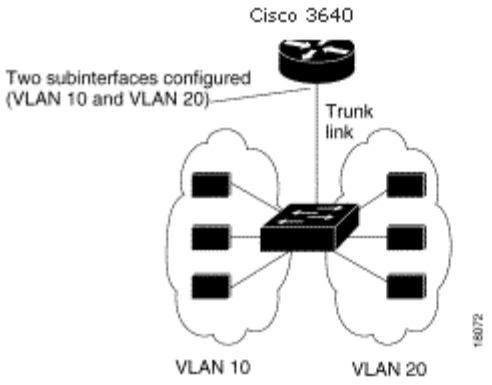
Everything else goes to the firewall to be NAT-ed

```
0.0.0.0 0.0.0.0 <private address inside interface>
```

Route between VLANS

An important aspect to remember **behind** the firewall is interdepartmental security. We need to segment departments such as Human Resources, Finance, and Engineering (the security people). VLANs also offer a performance value since they break up broadcast domains, and broadcasts are bandwidth hogs.

Figure 3-2: InterVLAN Routing Over a Single Trunk Link



On the switch we configure VTP (Virtual trunking protocol), assign the domain, create our VLANs, assign ports to the VLANs and set the trunk port, which carries inter-VLAN traffic to the router:

```
set vtp mode server
set vtp domain Corp_Net
set vlan 100
set vlan 200
set vlan 100 3/1-12
set vlan 200 3/13-24
set trunk 1/1 on
```

On the router, create three subinterfaces, one for each VLAN configured on the switch. Configure ISL encapsulation for each VLAN on the appropriate subinterface, and assign IP addresses to the VLAN interfaces:

```
configure terminal
R2(config)#interface fastethernet2/0.10
R2(config-subif)#encapsulation isl 10
R2(config-subif)#ip address 10.10.1.1 255.255.0.0
R2(config-subif)#interface fastethernet2/0.20
R2(config-subif)#encapsulation isl 20
R2(config-subif)#ip address 10.20.1.1 255.255.0.0
R2(config-subif)#interface fastethernet2/0.30
R2(config-subif)#encapsulation isl 30
R2(config-subif)#ip address 10.30.1.1 255.255.0.0
```

Part 2 – Tutorial on GIAC Enterprises' Security Policy concerning VPN partners.

Overview of standards:

IPSec – Set of protocols (IKE, AH, ESP) that add security services to the network layer

Authentication

- AH – (Authentication Header) integrity and authenticity ; packet cannot be tampered with
- ESP – (Encapsulating Security Payload) confidentiality, integrity, and authenticity of the data (not the ip header).

Algorithms used:

- Message-digest 5 (MD5) digital signature – any message -> 128 bit string ; used to verify integrity
- Secure Hash Algorithm (SHA)

Encryption

- DES – Data Encryption Standard ; 56 bit key to encrypt the data
- 3DES (triple DES) – used three different keys and 3 applications of the DES algorithm

Key management

- IKE (ISAKMP) - Internet Key Exchange; IKE is a derivative of ISAKMP

GIAC Security policy states that we will use:

- 3DES
- MD5
- pre-shared keys
- reeks no less than 10,000 seconds

How to create a crypto isakmp policy and crypto map with an access-list and apply it to an interface.

In global configuration mode, enter:

crypto isakmp policy # ; '#' is the priority of this particular policy

This puts you into isakmp configuration mode. Here you can enter the specifics of the policy:

Hash md5 ; algorithm used in integrity check
Authentication pre-share ; specifies that pre-shared keys will be used
Lifetime 10000 ; lifetime of key in seconds (lower number=higher security)

Then create a transform set, which groups together the encryption type and authentication and gives it a name:

Crypto insect transform-set graces esp-3des esp-md5-hmac

Then the crypto map, which gets a name for later applying to an interface, a sequence number, and states to use ipsec with the isakmp policy.

Crypto map giacmap 1 ipsec-isakmp

This put you into map configuration mode. Here we specify the peer address (tunnel endpoint), sa lifetime in seconds, and we apply the transform set that we created earlier. These are all straightforward commands:

set peer xxx.xxx.xxx.10
set security-association lifetime seconds 10000
set transform-set giacset

We then need to tell it what traffic we want to encrypt exiting the router. This is done with a regular access-list and then applied to the crypto map in map configuration mode:

Match address 101

The access list is done beforehand in global configuration mode. This access-list states a match for traffic from our local lan (on the 10.10.11.0/24) that is destined to 10.10.0.0/16

access-list 101 permit ip 10.10.11.0 0.0.0.255 10.10.0.0 0.0.255.255

The router will now inspect all traffic against it's new crypto map with this access list, and if the addresses match, the data will be encrypted according to the transform set.

A few things to note

1. Applying a crypto map to an interface is similar to applying (and removing) an access-list. Before making any changes to the crypto map, be sure to remove it from the interface –especially if you are connected via that interface.
2. Crypto map names are actually cases sensitive.
3. All rules apply as normal on the access-lists – order matters. Put more specific rules (addresses) on top so that they may fall through as warranted.

Troubleshooting tips

Figure 5 shows the information you get with the command
show crypto engine conn active

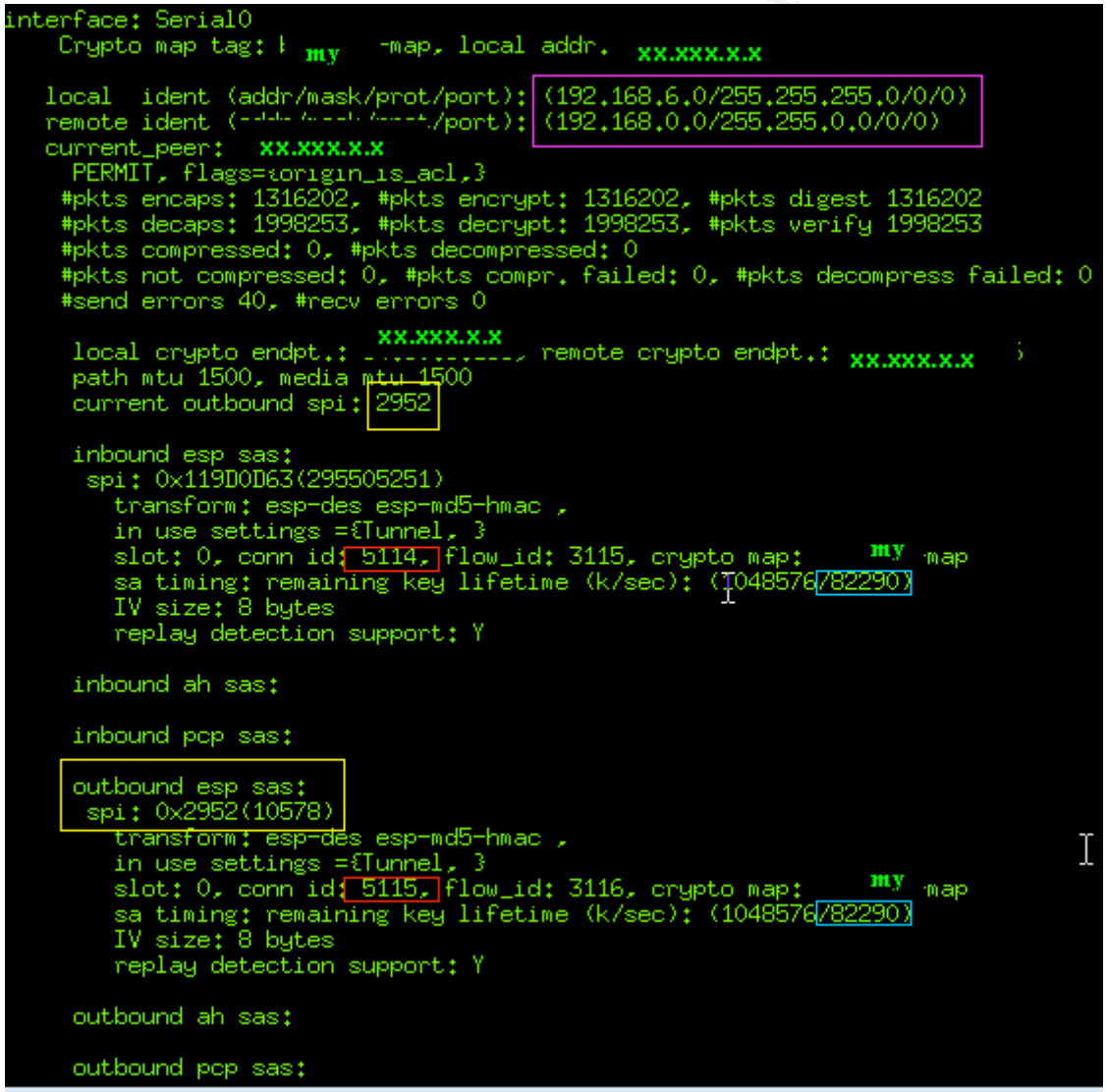
As you can see the count on encrypted packets and decrypted packets is 0 for both.

```
MyNewRouter# sh crypto eng conn act

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
1564 <none>          <none>          set    HMAC_MD5+DES_56_CB        0        0
5114 Serial0         [illegible]     set    HMAC_MD5+DES_56_CB        0        0
5115 Serial0         [illegible]     set    HMAC_MD5+DES_56_CB        0        0
MyNewRouter# ping ip
Target IP address: 192.168.7.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.6.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/41/44 ms
robson-buffalo#sh crypto eng conn act

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
1564 <none>          <none>          set    HMAC_MD5+DES_56_CB        0        0
5114 Serial0         [illegible]     set    HMAC_MD5+DES_56_CB        0        6
5115 Serial0         [illegible]     set    HMAC_MD5+DES_56_CB        6        0
```

Then we do an extended ping across the VPN network, which we see is successful.

Now if we **show crypto engine conn active** again, we see that the traffic got encrypted and the replies got decrypted. This test is useful if there is a misconfiguration on one side of the tunnel, then you may see either encryption or decryption, but not both.

Another command that shows interesting information is **show crypto ipsec sa.** In Figure 6 we can see the output of this command. This shows the security associations (uniquely identified by a randomly chosen unique number called the security parameter index (SPI) and the destination IP address), the local and remote network assignments, the time (or kilobytes, depending on what your policy defines) left before re-key, and your connection IDs, which you can see match up with the connections we saw in Figure 5.



3 – Audit

Planning

Technical approach - We will work with engineers and senior level security staff to run tests with selected traffic to determine that the firewall is implementing the security policy of GIAC Enterprises

Shift/day – We have a holiday weekend approaching and management has agreed to conduct the audit during this time. These tests shall be run at two distinct times: Friday at 8:30 pm and Monday morning at 9:15 am. These times reflect different bandwidth utilization and other variables that may not be apparent to security staff. These variables include things such as batch scripting that may change access rules, etc. Running the audit twice at different times will also give us more solid evidence with the consistency of the data we discover.

Costs - This will be a small to medium level effort due to the architecture and central location of the company. The three employees of GIAC are all salaried employees and will love to come in on the holiday weekend. The costs of the auditors are as follows:

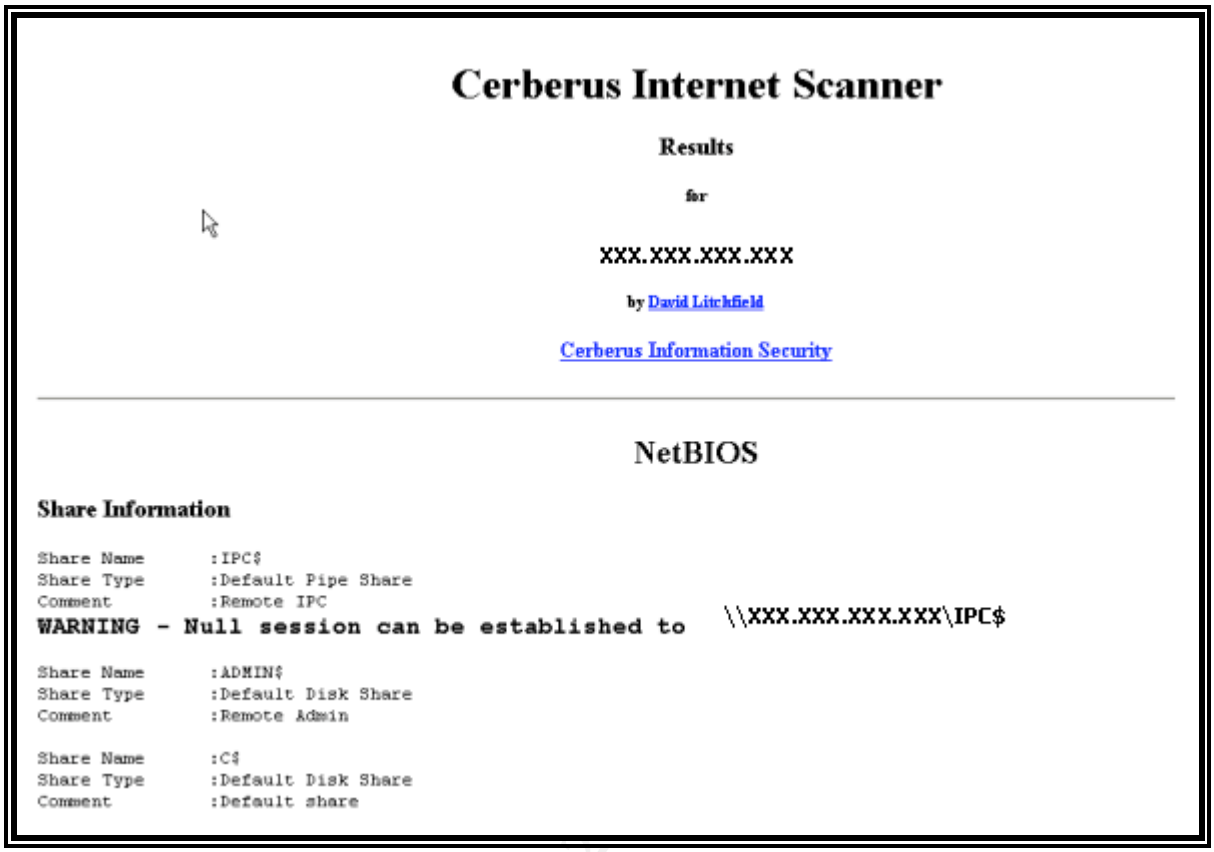
Planning/coordination - flat fee (determined by company size)
$3000
Audit hours – estimated at 8 hours
$150/hour
Evaluation, Assessment, Recommendation Session – estimated at 8 hours
$150/hour
_____
Totaling: $5400

Risks/considerations – Since we are in control of all tests and non are destructive or obtrusive in any way, there is very little risk involved. In case of any problems there will be the engineers on hand to reset or 'fix' anything that may go awry.

Auditing

The following chart specifies the parameters of the security policy that will be tested and the tools and location used in each case.

Tool	Placement	Test
trash.c http://packetstormsecurity.org/DoS/trash.c	Outside firewall	blockage of spoofed addresses
nbtdump http://www.atstake.com/research/tools/index.html **See Figure 1**	Outside firewall	Ability to get user accounts, establish null session, Windows
nmap http://www.insecure.org/ **See Figure 2 (results similar to example)**	Outside firewall	Open ports
SamSpade http://www.samspade.org/ **See Figure 3**	Outside firewall	Blocked zone transfers
Applications denied in Security Policy	Inside firewall	Blocked ports outbound
Firewall statistics **See Figure 4**	On firewall	Check ACL usage and VPN traffic



Cerberus Internet Scanner

Results

for

XXX.XXX.XXX.XXX

by David Litchfield

Cerberus Information Security

NetBIOS

Share Information

```
Share Name      :IPC$
Share Type      :Default Pipe Share
Comment         :Remote IPC
WARNING - Null session can be established to   \\XXX.XXX.XXX.XXX\IPC$

Share Name      :ADMIN$
Share Type      :Default Disk Share
Comment         :Remote Admin

Share Name      :C$
Share Type      :Default Disk Share
Comment         :Default share
```

Figure 1

nbtdump showing default shares and null session open on the RADIUS server.

Figure 1 shows an issue with our RADIUS server running on Windows 2000. Null sessions can be connected to by issuing the command:

c:>net use computeripc$ "" /user:""

Things that can be accessed through a null session:

- The list of user accounts on that server
- RAS callback numbers
- Status of the account lockout for all users
- Last logged on date and time for user accounts
- Remote access to the Registry
- Status of all NTFS file permissions on the system
- Account policy on machine
- User rights on the machine
- List of services on the machine and their status

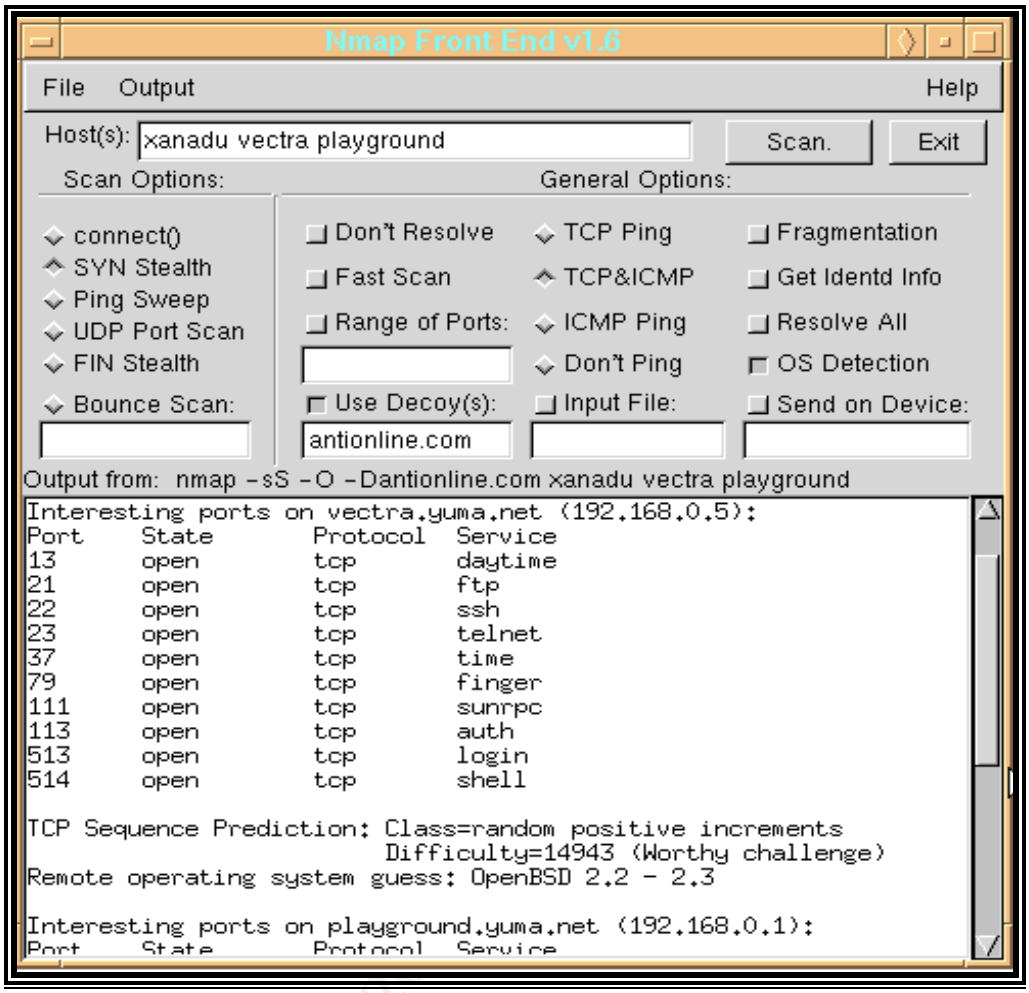


Figure 2

This shows nmap in action. It shows open ports it found doing a "stealth" scan with just syn packets, and also how it can detect the OS of the scanned machine. You can see some other fun options as well.

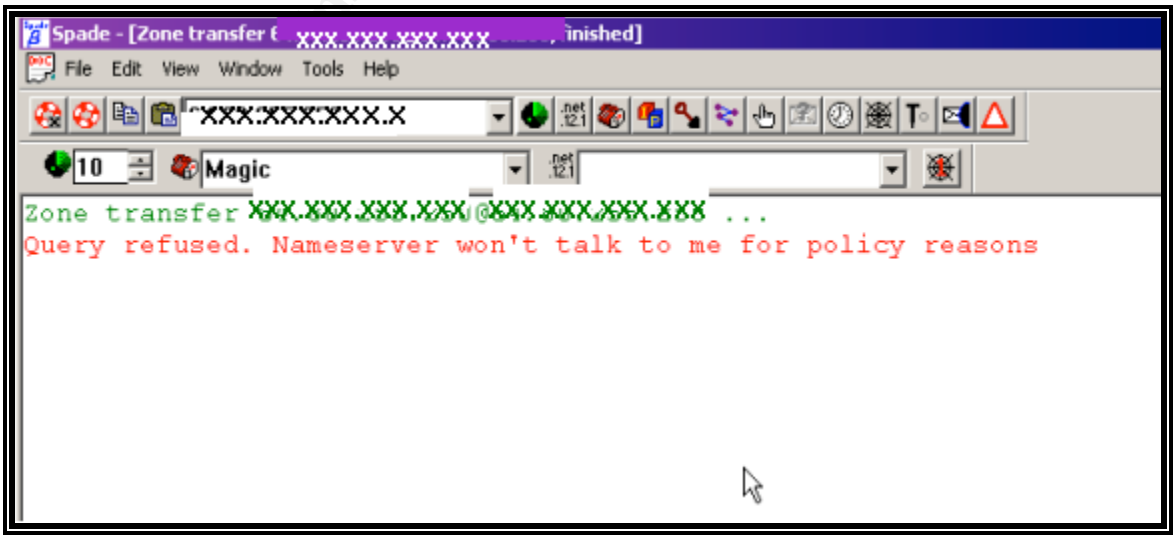


Figure 3
SamSpade used to test DNS zone transfers blocked

```
access-list dns deny icmp any any unreachable (hitcnt=5346815) ← deny "unreachable"
access-list dns permit icmp any any (hitcnt=1540816)

access-list dns permit udp any host xxx.xxx.8.174 eq isakmp (hitcnt=1)  ← VPN client connection
access-list dns permit esp any host xxx.xxx.8.174 (hitcnt=10)  ← VPN traffic
```

Figure 4
Firewall access lists at work
Here we tested that our access-lists picked up the VPN traffic, and that icmp type 3 is indeed being blocked.

We can also check the current connection status of any host with the command

```
show conn local xxx.xxx.xxx.xxx
```

```
pix# sh conn local xxx.xxx.8.174
5850 in use, 35674 most used
UDP out 1x4.8.11.1x4:500 in xxx.xxx.8.174:500 idle 0:01:15 flags -
UDP out 1x4.8.1x.xx2:500 in xxx.xxx.8.174:500 idle 0:00:04 flags -
UDP out 1x4.8.1x.138:500 in xxx.xxx.8.174:500 idle 0:00:39 flags -
UDP out 1x4.8.x10.51:500 in xxx.xxx.8.174:500 idle 0:00:06 flags
UDP out 1x4.8.1x2.2xx:1813 in xxx.xxx.8.174:2051 idle 0:00:04 flags –
```

Evaluation

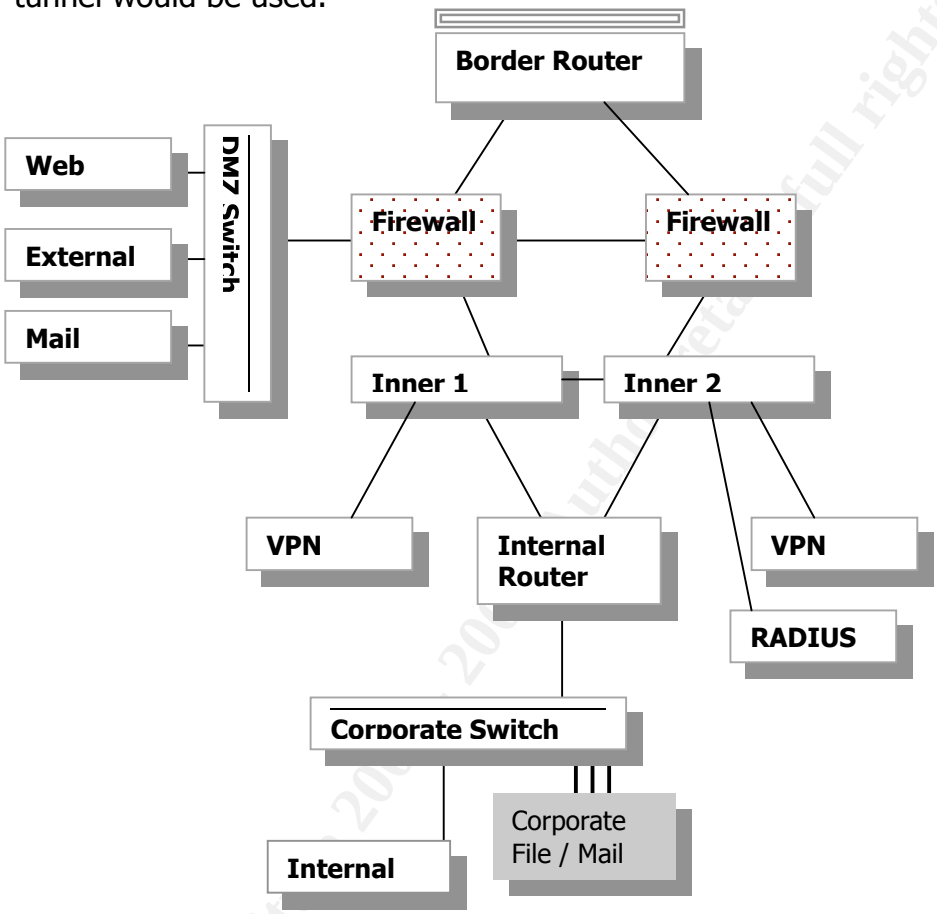
The results of our test turned out pretty well except for the RADIUS server issue. Fixes for this vulnerability are listed on http://www.aztechbiz.com/forums/41/109/ as well as many others.

Recommendations

1. Change enable passwords at least every 90 days
2. Implement IDS on DMZ segment with configured alerts. Recommend Snort with current rules set. Although it was in place before we need to step it up and get it configured with alerting, not just a sniffer for troubleshooting.
3. Implement ntp for syslog synchronization on all network devices

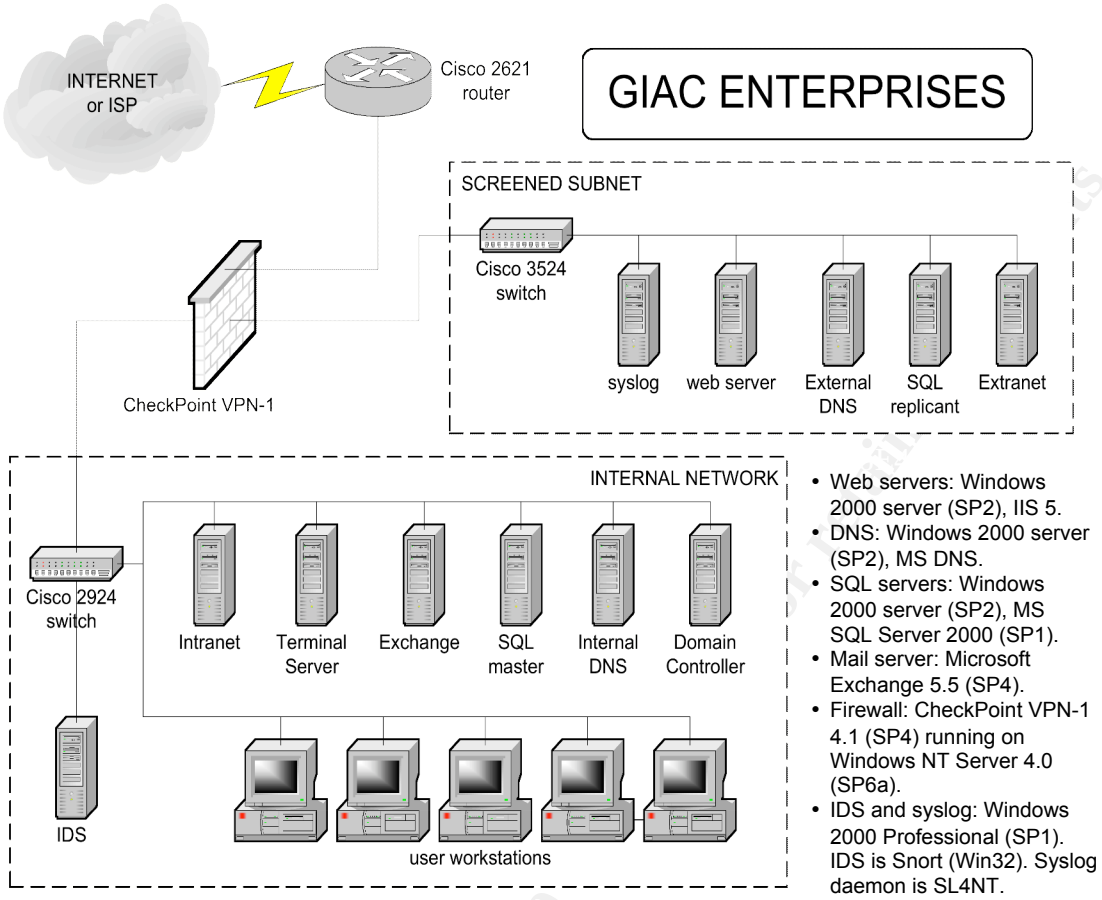
Alternate architecture

My recommendation for an alternate architecture would be redundant firewalls, since this poses a single point of failure problem, another switch for fuller redundancy and a secondary VPN concentrator. It may be possible to do GRE-in-IPSec Tunnels and configure multiple tunnels to each business partner, so that in case of a failure, the secondary tunnel would be used.



4 – Design Under Fire

Design from:
http://www.sans.org/y2k/practical/Loring_Rose_GCFW.zip



Vulnerabilities Found:

From: http://msgs.securepoint.com/fw1/ :

Check Point FireWall-1
GUI Buffer Overflow
September 19, 2001

Summary:
An issue exists in VPN-1/FireWall-1 Management Server running on Windows NT or Windows 2000. A malicious administrator can exploit a buffer overflow condition in the GUI authentication code to potentially impair management station functionality or to execute code. Any attack must come from an IP address explicitly defined as an authorized GUI client. Only management stations running Windows NT or Windows 2000 are affected. This includes any standalone VPN-1/FireWall-1 Gateways (with Management Server and enforcement points installed on the same machine), but does not include module-only (enforcement point) installations.

From: http://www.checkpoint.com/techsupport/alerts/format_strings.html

Format Strings Vulnerability

Updated September 13, 2001

Summary:
A security issue exists in VPN-1/FireWall-1 version 4.1 whereby a valid firewall administrator connecting from an authorized management client may send malicious data to a management station inside a control connection, possibly preventing proper operation of the management station. This issue exists because some instances of improper string formatting occur in VPN-1/FireWall-1 version 4.1. By sending specially constructed commands through authorized communication channels, arbitrary code may be inserted onto the operating system stack of a VPN-1/FireWall-1 management station. This vulnerability may only be exploited by an authorized and authenticated VPN-1/FireWall-1 administrator connecting from a workstation explicitly trusted by the management station, although read/write permission is not required in order to perform this attack. Since full access (read/write) administrators and those at the local system console already have direct access to the firewall system, this is an escalation of privilege only for read-only administrators.

Check Point FireWall-1 RDP Bypass Vulnerability
From http://www.inside-security.de/advisories/fw1_rdp.html :

> As FireWall-1 rule sets are created they are translated into the INSPECT language (similar to C) and by default include the file $FWDIR/lib/base.def which itself includes $FWDIR/lib/crypt.def in line 259. Together they define protocol names and the so-called implied rules (for FireWall-1 management). In line 62 the macro accept_fw1_rdp is defined to accept any eitherbound connection that matches the following characteristics:
> - Protocol UDP
> - Destination port 259 (RDP)
> - RDP Command RDPCRYPTCMD (100), RDPCRYPT_RESTARTCMD (101), RDPUSERCMD (150) or RDPSTATUSCMD (128).
>
> The RDP command types RDPCRYPT = {RDPCRYPTCMD,RDPUSERCMD,RDPSTATUSCMD} and RDPCRYPT_RESTART = {RDPCRYPT_RESTARTCMD} will permit traversal of faked RDP packets (regardless of the value of NO_ENCRYPTION_FEATURES, undefined by default).

Proof Code for RDP Bypass is here:
http://www.inside-security.de/advisories/fw1_rdp_poc.c

A denial of service attack should be fairly easy given the size of the router – 2621 and link that it probably is handling – (T1 at most?). Also, the implied rules on the firewall state to accept ICMP. This could make an ICMP attack easy even without 50 cable modems.

Denying ICMP on the firewall would be helpful to prevent this attack.

Any of the Windows servers would be fun to attack. Probably go after Windows 2000 web server for any new IIS vulnerability – like http://www.itworld.com/AppDev/3262/itwnws010303iis/ :

"IIS 5 malformed URL DoS attack -The vulnerability is exploited using a malformed URL, which when sent repeatedly can overwhelm either IIS or Exchange and cause a failure. ……. The flaw is rooted in the handling of URLs that have a length within a narrow range of values. If such a URL is sent repeatedly to the server, it causes a memory allocation error that crashes the server."

This vulnerability is post SP2, so the web server is most likely vulnerable.

Appendix A

```
PIX Version 6.0(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 vpnz security15

enable password JNcsjout_to_inKdfhjsdf encrypted
passwd 4FBh234kKop02SzAjpz encrypted
hostname boogie
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names

access-list in_to_out permit tcp 10.0.0.0 255.0.0.0 any eq ftp
access-list in_to_out permit tcp 10.0.0.0 255.0.0.0 any eq www
access-list in_to_out permit tcp 10.0.0.0 255.0.0.0 any eq ftp-data
access-list in_to_out permit tcp 10.0.0.0 255.0.0.0 any eq telnet
access-list in_to_out permit tcp 10.0.0.0 255.0.0.0 any eq domain
access-list in_to_out deny ip any any

access-list out_to_in permit tcp any host xxx.xxx.2.14 eq ftp
access-list out_to_in permit tcp any host xxx.xxx.2.14 eq www
access-list out_to_in permit tcp any host xxx.xxx.2.14 eq 443
access-list out_to_in permit tcp any host xxx.xxx.2.9 eq domain
access-list out_to_in permit tcp any host xxx.xxx.2. eq 500
access-list out_to_in deny ICMP any unreachable
access-list out_to_in permit ICMP any
access-list out_to_in permit tcp any host xxx.xxx.8.174 eq www
access-list out_to_in permit tcp any host xxx.xxx.8.174 eq telnet
access-list out_to_in permit udp any host xxx.xxx.8.174 eq isakmp
access-list out_to_in permit esp any host xxx.xxx.8.174

access-list dmz_out permit udp host <ext-dns server> any eq domain
access-list dmz_out permit udp host <ext-mail server> any eq smtp

access-list vpnz_out permit esp host xxx.xxx.8.174 any
access-list vpnz_out permit udp any host xxx.xxx.8.174 eq isakmp

access-group out_to_in in interface outside
access-group in_to_out in interface inside
access-group dmz_to out in interface dmz
access-group vpnz_to _out in interface vpnz

nat(inside) 1 10.0.0.0 255.0.0.0
global(outside) 1 xxx.xxx.2.22
```

```
logging on
logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered informational

logging host inside 10.5.1.10
no logging message 302002
no logging message 302001
no logging message 302006
no logging message 302005
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto

icmp deny any echo outside
icmp permit any echo outside <<<<<<←-
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu vpnz 1500

ip address outside xxx.xxx.2.14 255.255.255.252
ip address inside 10.10.1.6 255.255.255.240
ip address dmz 192.168.1.1 255.255.255.0
ip address vpnz xxx.xxx.8.241 255.255.255.240

ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip audit info action alarm
ip audit attack action alarm

static (dmz,outside) tcp xxx.xxx.2.11 smtp 192.168.1.5 smtp netmask 255.255.255.255 0 0
static (dmz,outside) tcp xxx.xxx.2.11 ftp 192.168.1.7 ftp netmask 255.255.255.255 0 0
static (dmz,outside) tcp xxx.xxx.2.11 www 192.168.1.7 www netmask 255.255.255.255 0 0
static (dmz,outside) tcp xxx.xxx.2.9 53 192.168.1.6 53 netmask 255.255.255.255 0 0
static (dmz,outside) xxx.xxx.2.10 xxx.xxx.2.10 netmask 255.255.255.255 0 0
static (vpnz,outside) xxx.xxx.8.241 xxx.xxx.8.241 netmask 255.255.255.255 0 0

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute

aaa-server RADIUS protocol radius
snmp-server host inside xxx.xxx.xxx.xxx
no snmp-server location
no snmp-server contact
snmp-server community xxxxxxxx
no snmp-server enable traps
```

```
floodguard enable
no sysopt route dnat

telnet timeout 15
ssh timeout 5
```

REFERENCES

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/sysmgt.htm#xtocid14873

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/examples.htm#xtocid440810

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/layer3/routing.htm#xtocid30231

http://www.insecure.org/nmap/images/nmapfe.gif

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42cmd.htm#xtocid1201316

Brenton, Chris- The SANS Institute – Track 2 "Perimeter Protection with Firewalls"

http://www.aztechbiz.com/forums/41/109/