Global Information Assurance Certification Paper

SECURITY PROPOSAL FOR GIAC ENTERPRISES

GCFW Practical Submission v1.5a

Gareth Thomas

Security Proposal for GIAC Enterprises

Dear Mr Northcutt and Associates,

Thank you for this opportuni ty to provide GIAC Enterprises with a comprehensive security solution proposal.

In the defined scope of work provided to me, based on your expected revenue, as a guide I would suggest a budget of 2 -3% of annual earnings for the initial security infrastru cture. Actual costs would not be discussed unless you were prepared to proceed with this implementation, at which time we can itemise the costs involved. Ongoing yearly cost of IT security staff and maintenance would also be covered at that time.

Due to the fact that your businesses entire logistics will rely on electronic transfer of information and money, it is important to set a solid security policy to complement and enable your business growth.

The most important factor to remember in implementing an y security policy is that it is in fact a constant work in progress. Vigilance and constant reviews and research are required to stay ahead of any vulnerabilities that would lead to a security breach.

By connecting yourself to a public network carries wi th it an implied risk, you have to mitigate this for your companies well being, the aim of this document is to provide you with a risk analysis so you can make that decision in an informed way. There are no guarantees that any system is 100% secure, but th at does not mean that I will provide anything less than what I know to be secure at this point in time.

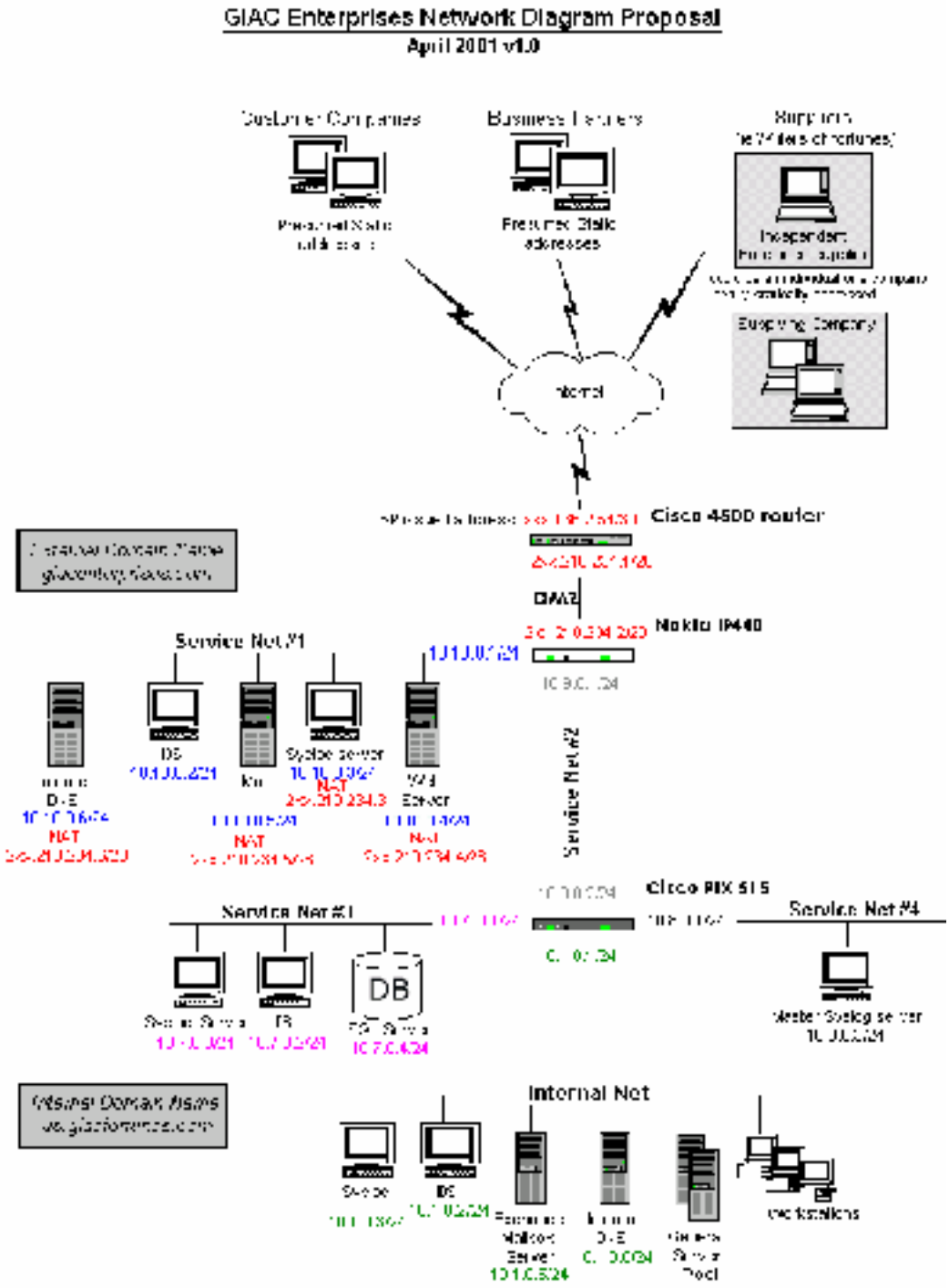
I highly recommend having this policy independently assessed before implementation and audited every 6 months to ensure your security expectations are being achieved and are accountable.

As you have just competed a merger and as such been operating as a business in some form, you will likely have some form of databases, web server and mail system already in place. Judging from the amount of submissions you have already received for this tender, I suspect you may be looking for a Windows -based infrastructure rather than Unix -based to use this infrastructure you currently own. For that reason I am proposing an infrastructure to secure an existing Microsof t Windows -based network.

1. SECURITY ARCHITECTURE

Below is a diagram of the proposed network. (see Fig 1.)
Please print to see more clearly if necessary.

Fig 1.



The security equipment shown in Fig 1, specifically: -

Cisco 4500 Router	ios v 12.1
Nokia IP440	FW-1/VPN-1 v4.1 SP3 (used for VPN also)
Cisco Secure PIX 515	v 5.3

have been chosen for: -

- Their proven reliability
- Secure platforms, that are updated regularly for any vulnerabilities that become apparent.
- Performance (throu ghput/speed)
- Scalability (the ability to expand) should the need arise

I recommend the purchase of these devices to replace the specific devices you may have in place currently.

Below is a table listing the host devices and their respective addresses, colour coded to assist use with the diagram.

Host Address Table

DMZ	Device	External IP	Internal IP	Internal IP2	Internal IP3
	Border Router	xxx.136.2.54/30	2xx.210.234.1/28		
	NOKIA	2xx.210.234.2/28	10.10.0.1/24	10.9.0.1/24	
Service Net #1	IDS		10.10.0.2/24		
	Syslog	2xx.210.234.3/24	10.10.0.3/24		
	Web Server	2xx.210.234.4/28	10.10.0.4/24		
	Mail Server	2xx.210.234.5/28	10.10.0.5/24		
	DNS Ext	2xx.210.234.6/28	10.10.0.6/24		
Service Net #2	PIX	10.9.0.2/24	10.8.0.1/24	10.7.0.1/24	10.1.0.1/24
Service Net #3	IDS		10.7.0.2/24		
	Syslog		10.7.0.3/24		
	SQL Database		10.7.0.4/24		
Service Net #4	Master Syslog		10.8.0.3/24		
Internal Network	IDS		10.1.0.2/24		
	Syslog		10.1.0.3/24		
	Exchange		10.1.0.5/24		
	Internal DNS		10.1.0.6/24		
	WINS		10.1.0.7/24		

Generic Password Policy

Passwords control your network access, you can secure your network but if a password is compromised, so is your company information.

Passwords across the board will be minimum 7 characters, combining alpha -numeric characters preferably a extended character or non visible ascii characters, enforced by NT policy and Passfilt.dll

NT domain servers will have the SYSKEY 128bit password hardener, PASSFILT.DLL on all workstations and PASSPROP /ad minlockout installed.

All passwords will change every 30 days, automated to change where possible, otherwise security staff will be entrusted to continue this annoying but necessary procedure on all equipment.

See the Microsoft Knowledgebase or Hacking E xposed for details on obtaining and implementing the NT specific hardeners above.

Your Suppliers

Your suppliers, I would suggest, will change from time to time, and differ in size from independent freelance writers to publishing companies. This causes s ome issues to address. These companies will always try to do the easiest solutions for themselves, probably emailing fortune cookie scripts. This means re -keying into your database and as well as absolutely no security.

We must enforce the use of the web server interface to submit their work, instantly they will receive acknowledgement of their submissions, no wondering whether the mail got there.

In the case of an Independent freelancer, this will run over the Checkpoint VPN SecuRemote client in the ca se of independent freelancers and BlackIce will be pushed down to their machines. This will be discussed in detail in section 2

In the case where the company has solid infrastructure of there own and static IP addressing an IPSec VPN will be created from their as yet unspecified IPSec compliant VPN device to the Nokia IP440.

Staff changeover and lost laptops or stolen equipment must be reported to GIAC Enterprises within 4 hours of the incident, in order to maintain good security for your supplier to cont inue being trusted.

They will be required to provide usernames and contact information for all staff connecting to your site. Individual usernames and passwords will be supplied to all staff requiring access with regular password changes and password poli cy as above.

Your Customer Companies & Business Partners

You are reliant on your Customer Companies and Business Partners for security from their end. It will be assumed they will install a similar security policy and where possible

Your business partne rs & customer companies are assumed to have some solid infrastructure and as such static IP addresses linked to their perimeter.

They will be required to provide usernames and contact information for all staff connecting to your site. An IPSec VPN will b e created from their as yet unspecified IPSec compliant VPN device to the perimeter Nokia IP440.

NB. Your tender did not indicate you would do "e -business" with customer individuals, only customer companies, this scenario has not been accounted for in thi s policy.

2. SECURITY POLICY DEFINED

In supplying this policy document to your company, I would suggest that the implementation be done by your staff rather than me. Any issues can be addressed then, such as syntax errors, or extra business requirement s they believe need to be addressed.
Your staff get to know the security environment more thoroughly and hopefully learn from the experience. When complete, I would come in to do an evaluation and audit of the system.

As such I am providing this docume nt as a means for your security team to complete this implementation.

Changes to the Policy

During the security implementation, the policy defined can be "thrown out the window" in order for testing purposes to be completed.

For example some connectivi ty problems may arise during the PIX firewall installation. Is it one of the routers? An access list? The firewall itself? In this case ICMP (specifically for Ping testing) may be turned on to isolate the problem and clarify connectivity. The issue of removing unrestricted ICMP then becomes one of "we'll do it later when we know everything is talking correctly" This is fine as along as it *is* readdressed *before* the system goes live.

This issue can have hundreds of variations, such as, allowing Telnet to th e border router "to save time" or leaving a default password in place until all staff are notified of the new passwords. In isolation they seem low risk, and provided the system is not live, they do not harm anyone, but the potential for one of these items to go unchecked before connecting to the world is a grave risk. I suggest creating a 'register of changes' to the policy, where the policy cannot be carried out fully, due to needing clarification or testing, an entry is made to the register noting the ch ange, the reason and the administrator, making the change. Before the go live date, the register is given to the security team to address all changes and 'make right' according to the policy.

No Policy is perfect and business plans, and risks change on y our corporate direction. If changes to the policy are found to be needed, then signing off by the CIO, Head of Security Team and myself should be required to put a change into effect.

Cisco 4500 router (Border Router)

After establishing a suitable pass word combination and ensuring the enable password is MD5 hashed (enable secret 5 *xxxxx*), it is time to configure the border router. Parts of the config are not present if not entirely relevant, telnet access should not be permitted. Configuring from the co nsole is preferred and trusted.

The rule base of the border router is order dependent, it is vital to implement the policy in the order listed.

```
! Negate built in services
no service udp -small-servers
no service tcp -small-servers
no service finger
no ip http server
no snmp
! Prevent bordering Cisco enumerating yours
no cdp run
! Prevent source routing
no ip source -route
!
interface Ethernet0
 ip address 2xx.210.234.1 255.255.255.240
 ip access-group 102 in
!
interface Serial0
 ip address xxx.136.2.54 255.  255.255.252
 ip access-group 101 in
! Don't accept router ICMP redirections
no ip redirects

! log
logging trap debugging
logging 2xx.210.234.3
!
! Block telneting to router see line vty 0 4
access-list 10 deny   0.0.0.0 255.255.255.255
!- - Deny spoofin g (101 inbound serial0)
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny   ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny   ip 0.0.0.0 255.255.255.255 any log
!
!- - Deny connections to denied services or enumeration info (101 inbound seria      l0)
access-list 101 deny   tcp any any eq 1999 log
access-list 101 deny   tcp any any eq 9001 log
access-list 101 deny   tcp any any range ftp telnet log
access-list 101 deny   tcp any any range 135 139 log
access-list 101 deny   udp any any eq 135 log
access-list 101 deny   udp any any range netbios   -ns 139 log
access-list 101 deny   udp any any eq 139 log
access-list 101 deny   tcp any any eq 445 log
access-list 101 deny   udp any any eq 445 log
!
! -  - Permit access to web, mail, dns, VPN (101 inbound s     erial0)
access-list 101 permit tcp any host 2xx.210.234.4 eq www log
access-list 101 permit tcp any host 2xx.210.234.5 eq smtp log
access-list 101 permit tcp any host 2xx.210.234.6 eq domain log
access-list 101 permit udp any host 2xx.210.234.6 eq domain l     og
access-list 101 permit tcp any host 2xx.210.234.1 eq 256 log   !  SecuRemote & VPN access
access-list 101 permit tcp any host 2xx.210.234.1 eq 264 log   !  SecuRemote & VPN access
access-list 101 permit udp any host 2xx.210.234.1 eq 500 log   !  IKE VPN       access  Udp259 not needed no FWZ
!
! - - Trash what's left and log (101 inbound serial0)
```

```
access-list 101 deny   ip any any log
!
! - - Permit our net to go out, if its not our 2xx.210.234. net going out, deny (102 inbound eth0)
access-list 102 permit ip 2  xx.210.234.0 0.0.0.39 any
access-list 102 deny   ip any any log
!
liny vty 0 4
login
! prevent telnet from anywhere   – see access list 10
access-class 10 in

! Set console to be password protected and close after 30 seconds of no use
line console 0
 login
 password xxxxx
 exec-timeout 1  30
```

This should provide us with sufficient anti spoofing, and reduce your risk of being used in an ICMP amplifying attack such as Smurf. Still allow in and out what needs to get to your DMZ. And stop remote configuration .

Nokia IP440 Checkpoint Firewall -1/VPN-1

For your perimeter firewall I have decided to implement the Nokia IP440 Firewall Appliance with three active interfaces. Checkpoint Firewall -1 is a Stateful inspection firewall software, in other words unlike a packet filter, it maintains a table (state table) which lists the current set of valid requests passing through it.
A timer is set to this list to work out when a connection should be torn down, typically 3600sec for TCP. The table then allows the firewal l to work out whether an incoming packet is part of a pre existing session and should be allowed to pass, or instead a packet to drop.
For instance a new unrequested response packet with the SYN ACK flags set (a supposed response) is sent by a malicious h ost, to try to bypass a non -stateful filter. The table would be looked at, noted that no session had been initiated previously to that host and sequence and then denied entry and discarded.

The Nokia appliance firewalls are a pre -hardened hardware platfor m, with Checkpoint Firewall-1 running on Nokia's IPSO (modified FreeBSD) operating system. Use the manual to get it up and running, set the addresses for the device as per the diagram and table.

The Nokia will also facilitate your VPN connections to the Customer Companies, Business Partners and Suppliers around the globe. See the VPN section below.

Once up and running we will want to create the security policy to allow authorised communications.
Firewall-1 is object based to make it a little more user fr iendly and visually easier to see the flow of the rulebase. As such objects and networks must be clearly defined. An object will need to be defined for every object in the diagram. Try to maintain the colours of objects as per the diagram to make it easier to see what goes where.
See the manual for creating network objects.

In setting up your Firewall object set the *Exportable* tick **ON** in the VPN tab, to allow SecuRemote clients to pick up the required keys and site info.

Again the rulebase of Firewall -1 is order dependent. It is extremely important to follow the rulebase defined below. Also the higher in the order a rule is the quicker it is processed, as not all rules must be attempted to match. You may find you can better "load balance" the rule base by putting a heavily used rule (except 16) closer to the top where functionality is not affected.

Network names will be defined as *Networkname* eg. Internal, Net4

Object names will be defined as *Networkname_Host* eg. Net1_web, Net3_sql

Properties Setu p
Firewall-1 has default psuedo rules on after installation. These relate to Firewall -1 control connections, DNS, RIP, ICMP. Turn off, Accept Firewall -1 Control Connections, RIP, Domain Name queries, ICMP. Accept Outgoing packets. These can all be configur ed as specific rules and not hidden away.
You may choose to change the timeouts at a later time.
Rules should be applied Eitherbound to ensure the rules are enforced incoming and outgoing of the Firewall, this will impact on your throughput of your firewal l as the rules must be run through twice and will double your logging on an event.

Logging and Alerting
Logging is essential to the whole security process. If you don't know it happened/is happening, who defend you? As such logging will be set to log to t he syslog server on Service Net 1, this inturn passes on logs to the master syslog server on Service Net 4.

SYNDefender
SYNDefender should be turned on in Passive mode. It will intercept SYN requests from remote hosts to yours and wait for a specified tim e before dropping them. Thereby reducing chances of a denial of service attack against one of your visible hosts eg Web server. If a remote host were to generate thousands of SYN requests that did not exist, the Web server would be unable to communicate wi th legitimate hosts.

Network Address Translation (NAT)
NAT will be defined on a per object basis for the following Service Network #1 objects: - Web server, SMTP server, syslog and DNS. Their Firewall -1 objects will have NAT entries as per the HOST table in Section 1. These public address must be added to the $FWDIR/conf/local.arp file in the format below, as FW -1 does not keep an ARP table in memory.

IP address of host	Mac Address of Firewall external if
eg. 2xx.210.234.4	03 03 93 a4 bf 84 *(invented Mac address)*

The internal network object should be NATed to produce the IP address of the firewall external interface. So when users surf the Net ony the public address of the Nokia box is published.

Checkpoint Point's Malicious activity Detecti on (CPMAD)
CPMAD is a new feature that looks for suspicious activity in the log files and can be set up to notify administrators. It looks for SYN Attacks, Anti -Spoofing port scanning etc. This feature is well worth enabling, but has in my experience been known to slow the performance of the Firewall somewhat, so some testing in your environment may be necessary.
By editing the $FWDIR/conf/cpmad_conf.con, you can turn CPMAD on and adjust the settings to cause a trigger event/alert for suspected spoofing, su ccessive multiple connections, how much memory it can use.
See the Checkpoint knowledgebase for more detailed usage. (www.checkpoint.com/kb)

VPN
The VPN connections stipulated in the tender, will operate in the following fashion.

The VPNs with: -
"GIAC and Business Partners" & "GIAC and Customer Companies" will operate identically.
In order to do business with your company, your Customer/Business Partner must supply

1. A secure infrastructure (within reason)
2. An IPSec compliant VPN device, preferably Firew all-1
3. An acceptance of our practices on their staff, ie usernames & passwords, contact information and notification of breaches or staff changeover.

VPN Crypto Specfications

We setup the encryption on the workstation object defined for the Nokia firewall .
Edit the object, on the VPN tab
You must also create an object for the destination Customer Company/Business Partner IPSec compliant device.
One the VPN tab of both objects, setup Manual IPSec as the Encryption scheme.
Define your encryption domain "Ser viceNet1" for your firewall and their "Partner23_Net" for their encryption domain on their firewall object.
We make up an SPI unique to our Bus Partners for instance. Manage/Keys/New SPI
Encryption for Encapsulating Security Payload (ESP) we choose 3DES for maximum key strength.
Authentication Header we choose SHA -1
We then define a seed and generate a key.
We then define a rule specifically for that Bus Partner. Detailing the SPI for that partner and specify them in the Allowed peer gateway of IPSec

And each and every supplier and customer and partner. To allow for instance, one VPN tunnel to be separated to disconnect one Customer on credit hold, or who has failed in their security requiements. Exchange the seed with the destimation and a VPN tunnel sho uld be able to be established.

Again ensure the Exportable for SecuRemote tick is ON, to allow key exchange and session negotiation for SecuRemote hosts and the Firewall.

The "GIAC and Suppliers VPN" will operate as above (with Business Partners etc) w here possible.

However where your supplier is not a company but a freelance writer etc, another VPN solution is necessary. A rollout of SecuRemote client for Windows based clients on a host by host basis will be necessary. The SecuRemote client can be pr econfigured with configs and keys preinstalled. Simply copy the usersc.c file from a configured client and copy to all other installs. http://www.phoneboy.com/faq/0303.html

Network Ice's (www.networkice.com) product Black Ice will be setup to be pushed t o SecuRemote users from having their VPN channel hijacked. Logging will occur if the user attempts to turn off the facility, thereby leaving themselves open for an attack.

Firewall-1 Rulebase

Note. For space constraints and longer explanation the not es explaining the rules will appear above the rule.

No.	Src	Dest	Service	Action	Track	Time	Install on
Allow SecuRemote negotiations							
1	any	Nokia_dmz	Tcp 256 (FW1) Tcp 264 (FW1) Udp 500 (IKE)	accept	long	Any	Gateways
Allow your supplier individuals to create a secure tunnel and connect to Net1. They CAN connect to all servers on NET1							
2	Suppliers@any	Net1_encdomain	http, https	Client Encrypt	Long	Any	Gateways
Stop broadcasts directed at internal networks. Create a net for all NETs representing 'x' ie 10.1.FF.FF 10.2.FF.FF etc							
3	**NEGATE** GIAC_intnetworks	255.255.255.255 10.x.255.255	All but Bootp	DROP	**Alert**	Any	Gateways
Stop the internal nets from broadcasting outside their subnets							
4	GIAC_intnetworks	255.255.255.255 10.x.255.255	Any	DROP	long	Any	Gateways
Allow your Exchange server to get mail to the SMTP outbound queue							
5	Int_exchange	Net1_mail	smtp	accept	long	Any	Gateways
Allow SMTP access to the world & log							
6	Any Net1_mail	Net1_mail Any	smtp	accept	long	Any	Gateways
Allow inbound web access to the world & log							
7	any	Net1_web	http, https	accept	long	Any	Gateways
Allow DNS lookups to the world & log							
8	Any Net1_dns	Net1_dns any	Udp53 Tcp53	accept	long	Any	Gateways
Allow internal DNS to lookup the world							
9	Internal_DNS	any	Udp53 Tcp53	accept	long	Any	Gateways
Allow your business partners to create a secure tunnel and connect to your network							
10	Bus_partners Cust_Companies Giac_Net	Bus_partners Cust_Companies Giac_Net	IPSEC	accept	long	Any	Gateways
Individual rule for each customer/partner detailing their SPI							
11*	**Bus_partners Cust_Companies**	**Net1_web**	**http, https**	**encrypt**	**long**	**Any**	**Gateways**
Allow internal network to surf, ftp, & acess stream content							
12	Internal_Net	Net1_web	http, https, RealAudio	accept	long	Any	Gateways
Allow Net1 Syslog to log to Net4 master							
13	Net1_syslog	Net4_syslog	Udp 514	accept	long	Any	Gateways
Allow Border Router to log to Net1 syslog							
14	DMZ_Router	Net1_syslog_nat	Udp 514	accept	long	Any	Gateways
Allow Webserver to query database							
15	Net1_web	Net3_SQL	Tcp 1433	accept	long	Any	Gateways
Allow internals to web server							
16	Internal_Net	any	http, https	accept	long	Any	Gateways
Deny what's left and log it							
17	any	any	any	drop	long	Any	Gateways

** NB. Rule 11 specifies one rule for all VPN to VPN connections with all p artners and customers, this was done for simplicity. In actual fact this would be one rule for each supplier, customer and partner who had a different Security Parameter Index (SPI) under IPSec encryption ie different tunnels for different locations. Ther efore a new rule for each.*

Cisco Secure PIX

To add another layer of defence for your Internal network and your SQL server, I have chosen to implement a Cisco Secure PIX 515 v5.3 with four interfaces. The slightly unusual configuration in weighting of networks, where the Internal network sdoes not have the highest security integer, reflects our need to keep the Net3 and Net4 secure from internal hacking. But still allow the Internal net to get outside.

PIX configuration

```
nameif ethernet0 net2 security0
nameif ethernet1 internal security50
nameif ethernet2 net3 security70
nameif ethernet3 net4 security100

interface net2 100full
interface internal 100full
interface net3 100full
interface net4 100full

ip address net2 10.9.0.2 255.255.255.0
ip address internal 10.1.0.1 255.255.255.0
ip address net3 10.7.0.1 255.255.255.0
ip address net4 10.8.0.1 255.255.255.0

hostname pixie

arp timeout 14400
! If we implement another PIX set to come online in event of a failure, we would change.
no failover

logging buffered debugging
logging on
logging facility 20
logging history 7
logging host inside 10.8.0.3

route outside 0.0.0.0 0.0.0.0 10.9.0.1 1

mtu net3 1500
mtu internal 1500
mtu net4 1500
mtu net5 1500

! Permits internal network outside to lower value nets ie only Net#2 therefore outside.
nat (internal) 1 0 0
global (internal) 1 10.1.0.20-10.1.0.250 netmask 255.255.255.0
!
!
! Permit Web server to access SQL
conduit permit tcp host 10.10.0.4 255.255.255.0 10.7.0.4 eq 1433
!
! Permit Syslog to master
conduit permit udp host 10.10.0.3 255.255.255.0 10.8.0.3 eq 514
conduit permit udp host 10.7.0.3 255.255.255.0 10.8.0.3 eq 514
conduit permit udp host 10.1.0.3 255.255.255.0 10.8.0.3 eq 514
!
!
! Permit DNS queries outside
conduit permit udp host 10.1.0.6 255.255.255.0 0.0.0.0 eq 53
conduit permit tcp host 10.1.0.6 255.255.255.0 0.0.0.0 eq 53
!
!
! Permit SMTP in and out of internal net
conduit permit tcp host 10.10.0.5 255.255.255.0 10.1.0.5 eq 25
conduit permit tcp host 10.1.0.5 255.255.255.0 10.10.0.5 eq 25
fixup protocol smtp 25
!
```

Windows NT 4.0 Standards

All servers shall have Service Pack 6a installed plus current hot fixes for security and availability, and other where appropriate.

As mentioned above, NT domain servers will have the SYS KEY 128bit password hardener, PASSFILT.DLL on all workstations and PASSPROP /adminlockout installed.

All NT passwords will change every 30 days through User Manager

Auditing will be turned on to all NT Servers for Failure events of
"logon and logoff", "use of user rights" and failure and successful "security policy change".

Regularly review all servers for Admin and Domain Admin members, ensuring they are legitimate.

Ensure NTFS volumes with adequate permissions are set. Often root directories are lef t with Everyone FULL CONTROL, a definite mistake especially when administration shares are setup automatically by the system eg \\servername \C$ if someone were to circumvent the sharing permission, problems may well result.

Restricting anonymous access to a server is another essential requirement of all NT servers. With a registry editor, at HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet \Control\LSA Add the Reg_DWORD **RestrictAnonymous** equal to **1**
And restart the server. This will stop null session connec tions to your servers, that even unauthorised staff may try to take advantage of.

Internet Mail - SMTP & Integrating with your current Exchange 5.5 server/server cluster

Securing your web server and perimeter is usually considered the extent of keeping unwanted people out of your business. What if your staff were to click a trojan horse email that collects the contents of their desktop and emails out of the company to an account in Zimbabwe? With the advent of Electronic Mail (email), you can't assume t hat your staff aren't forwarding your secrets voluntarily out the door without your knowledge with greater speed and mobility than ever before.

Email like all the information we have covered can be filtered. In fact its probably the best way to find what staff are working against you. And stopping the viruses and productivity killing executables from polluting your network and bloating staff mailboxes. Bandwidth you are paying for.

In my particular legal jurisdiction it *IS* legal to read staff email. I wil l assume this is true for your company also, though you may want to seek legal advice on this issue.

Mailsweeper 4.2 for SMTP from Baltimore Technologies (www.mailsweeper.com) is a great product for locking down the emailed data in and out of your network .

Incoming mail is scanned by the Mailsweeper engine and its content is evaluated against the scenarios. The scenarios are typically GUI based but can be entered in text form (see below)

In this example we have a set of scenarios (rulebase) for incoming mail. We have chosen to Block executable files, scan for Viruses, check for profanity as well as other content. In the case of executables, attachments are scanned, not by an extension (.exe .com etc) but by their content (eg Executable/Win32Dll) This is a short example of the content it can scan for.

[Scenarios \Incoming]
k:Block EXE=MIMEsweeper Data Type Manager Scenario
k:Macfee Virus Scan=MIMEsweeper Virus Manager Scenario
k:Large Email Block=MAILsweeper for SMTP Size Manager Scenario
k:Profanity Check =MIMEsweeper Text Analyzer Scenario

k:Love Letter=MIMEsweeper Text Analyzer Scenario
k:Att: No Code=MAILsweeper for SMTP Attachment Manager Scenario
k:HTML Scan=MIMEsweeper Html Manager Scenario
k:Att: Has Code=MIMEsweeper Text Analyzer Scenario
k:VBS Scri pt Stop=MIMEsweeper Virus Manager Scenario

[Scenarios \Incoming \Block EXE \Content \BLOCK]
v:Description=$SBlocked
v:RootOnly=$Bfalse
v:FormatTypeL ist=$S,Executable/Win32Exe,Executable/Win32Dll,Executable/Win32Unknown,Executable/Win3
1Exe,Executable/DosExe,Ex ecutable/JavaByte

Using Mailsweeper allows us to block mail travelling to the recipient (in or outbound) deemed inappropriate, be it graphic images, movies, racial language, or key words you define. An example of that might be, you believe staff are apply ing for other jobs while being employed by you. Looking for key words in staff email such as “Resume” “CV” “Curriculum Vitae” may turn up surprising results, what if the key word was “Project CookieMonster” and was a classified project in -house only. Imple menting Mailsweeper may save money in lost company secrets, law suits for sexual or racial harassment, or just keeping your staff’s work hours focused on the your company.

Other products such as Mail Marshal are also available and work along the same line s.

Mailsweeper would be configured on an NT 4.0 server running SP6a. The manual contains information about preventing use as a mail relay.
Mailsweeper will then make a SMTP connection to your Exchange Server’s Internet Mail Service (IMS) on your Internal Net. To configure forwarding to host 10.1.0.5, use the Mailsweeper install manual. The Exchange Server is setup to only accept mail from 10.10.0.5. your Exchange server will not require any major configuration, changing its Forward Internal mail to field t o 10.10.0.5 to ensure mail goes out via Mailsweeper.
I suggest changing the SMTP greeting on Mailsweeper to make it more difficult to know what SMTP server is being targeted. It is changeable in the Properties of the Mail Relay tab.

Mailsweeper is not im mune to attack either, being open to the world on Port 25, check the support website regularly, looking for updates, security bulletins and add ons to filter new exploitative content. Apply these updates whenever necessary.

Implementing Pretty Good Privac y 6.5 (www.pgp.com) and above would enable seamless integration with your Outlook client. Encrypting outgoing mail may make it difficult for a hacker to steal outgoing email with any reliable result, if they don’t have the intended recipient’s private key . This ofcourse would depend on the ability and frequency to use encryption with recipients. Incoming mail will depend on the sender’s preference or paranoia as to whether encryption has been implemented.

Integrating with your current IIS 4.0 server/serv er cluster

Your web interface through to your database back end is probably already configured as such it may require some minor reprogramming to account for the change in network location and firewall.

IIS 4.0 is a great flexible platform for web hosti ng, unfortunately it suffers from constant security failings. Your web server is highly exposed due to the need to keep Port 80 open to the world, once this policy is implemented and time passes, you are only as safe as your staff can keep you. As such the re are specific things they should proactively do to reduce its exposure. Running updated versions STAT, Nessus, Saint and ISS will enable to see your web server the way the hackers do, as vulnerable!
So you can at least be one step ahead in preventing yo ur system from getting caught out.

As an example, the recent well publicised “Soviet E -business Hacks” that resulted in reputedly around 1 million stolen credit card numbers stolen and affected many well known e - businesses, was due to IT staff not heeding the security warnings, some vulnerabilities were

known up to 12 months prior to the attack. Doing some pretty simple and quick, updates could have stopped those companies becoming a statistic.

Patchwork was commissioned by the Center for Internet Securi ty to test the vulnerabilities used in this exploit (after the fact ofcourse). It suggests the recommended course of action. Usually getting a patch or updating the registry. It also checks for known hacking utilities installed.

Sample Result from Patchwo rk.exe from www.cisecurity.org & grc.com

- Detected MDAC version: 2.50.4403.8
  MDAC NOT operating in SafeMode ...
  Found DANGEROUS ADCLaunchKey:
  RDSServer.DataFactory
  Found DANGEROUS ADCLaunchKey:
  AdvancedDataFactory
  Found DANGEROUS ADCLaunchKey:
  VbBusObj.VbBusObjCls
  MDAC is NOT CONFIGURED for safe operation. See the following URL for complete info:
  http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

Search regularly for the files be low, they are well known hacking utility files, that could be installed on your compromised computer, delete or quarantine if found : -

ntalert.exe ; sysloged.exe ; tapi.exe ; 20.exe ; 21.exe ; 25.exe ; 80.exe ; 139.exe 1433.exe ; 1520.exe ; 26405.exe ; i. exe ; lomscan.exe ; mslom.exe ;lsaprivs.exe ; pwdump.exe ; serv.exe ; smmsniff.exe

Turn off unnecessary services, Microsoft have a list of what you need to run and what you don't. Query the Microsoft Knowledgebase for "List of Services needed to run a S ecure IIS Computer" This list mirrors almost exactly "The SANS Institute Securing Windows NT Step by Step" This SANS booklet should also be used to secure not just your web server but all your Windows NT servers.

If you find the server is compromised, a n inconvenient but useful step would be to prevent all communications to the web server over ports 135 -139. Filtered in the Network settings of the NIC. So ports 80 and 443 are all you can talk to it with.
Give your web developers a test server, when they are ready to make a change to the server, put the site files on a removable media (CD or Zip) and physically install the update locally in the presence of a security team member. No file sharing….less headaches. This scenario would require a great deal of patience at times. And would be a separate non -domain server. Requiring more administration of usernames at that server also. This would inhibit Event Log Monitor from being able to access logs.

Integrating with your current Microsoft SQL 7.0 server/ server cluster

Your SQL server is ofcourse a main target for any network attack, it contains the product you sell. Stealing it, compromising it or crashing it, has a direct effect on your businesses health. As such we again must keep the server patched (d aily to weekly) to avoid new exploits found. As with your web server running updated versions STAT, Nessus, Saint and ISS will enable to see your web server the way the hackers do, as vulnerable! But fix the holes before attackers exploit them.
Again the Patchwork utility should be run on the SQL server as there is a vulnerability targeted at it also.

Again the SANS, Securing Windows NT Step by Step booklet should be used here also.

Additional Windows NT 4.0 utilities

I highly recommend installing thes e utilities into your network to allow better central management of logs to your master Syslog server, consistent updating of NT/2000 patches, security and others, and an NT 4.0 specific vulnerability scanner. All three utilities are available through Sunb elt-Software or their producer separately.

Event log Monitor (ELM) (www.tntsoftware.com)
ELM is a program to centralise all NT/2000 event logs into one or more management stations. Instead of having to monitor 20 servers and 3 logs on each (System, App, S ecurity) you can have ELM transmits whatever information you request through use of a filter. You tell it what servers, and types of events you want it to monitor and ELM will send those back to your administrator in real time. Increasing Security, Availab ility and saving precious time.
It can act as a syslog client to send those events to your master syslog server. Alternatively although not recommended in this instance, it can act as Syslogd server itself and have the Cisco's and Linux/Unix hosts post eve nts to it. The software is very straightforward to install and configure, see the online manual for filtering events and setup as a syslog client.

SPQuery (www.stbernard.com)
Service Packs and Hotfixes are released daily for the NT/2000 platforms, its di fficult for your security and admin staff to keep track. SPQuery provides a database of all patches, will download on request, will give you detailed info about the patch for your staff to determine when a patch should and shouldn't be installed. It will q uery machines to log what service packs and hotfixes are already applied and le you know what is available for it.

Having fixes in a centralised place makes it easier for you staff to see, when how and why patch was installed rather than it being a esote ric change one person decided to try. It doesn't fix everything for your staff but instead keeps them informed quickly and easily leaving the decisions up to them. See the online manual for installations and configuration.

STAT (www.statonline.com)
There are several good intrusion vulnerability scanners on the market, I particularly like STAT for its focus on the NT/2000 platform. STAT is updated continually with new vulnerabilities specific to NT. Very few other scanners do 900+ NT specific checks. It ca n view a single machine or an entire domain. It should be used in conjunction with Nessus, Saint, ISS Internet Scanner to get a better overall idea of where you need to tighten security.

DNS

Domain Name System (DNS) tells the world who you are, as such we simply can't block it, it also has to be available to update by your staff as new systems come into place or old systems are decommissioned.

We will implement a split DNS scenario. Specifically, one DNS server will serve as Master (Primary) for the external internet name requests and a slave (secondary) name server.

A separate Master DNS will serve the internal networks except Service Net1.

In order to allow the two systems to be separate and not fail requests, two different domain names (FQDN) will be used to not "confuse" name resolution.
The domain us.giacfortunes.com will be used internally, to differentiate it from external requests for giacenterprises.com, and internal requests going to your SMTP and web servers.

Service Net 1 DNS
The master (primary) DNS will run on a Linux server running BIND 8.2.2p5
This server will have all services removed that are not necessary for networking and BIND.
We will allow zone transfers via the /etc/named.conf to the ISPs secondary server (see below)
We will setup the log file to log to /var/adm/bind_xferlog to show all attempts to zone transfer.

The Slave (secondary) DNS can be hosted by your ISP to provide some redundancy provided your ISP can prove zone transfers are not permitted from its DNS. If we find zone transfers are open, we will host the secondary internally and amend the network diagram and policies, at that time.

Use nslookup on both your and the ISP (or your 2nd) DNS servers to test zone transfer.
ls –d giacenterprises.com
It should return a system error of some sort, if however, it returns you're A records and SOA information, then the server has not been secured correctly.

Internal DNS
We will run Microsoft DNS service on a NT 4.0 file server, probably running WINS and DHCP for convenience, and run MS DNS on a low usage file server for Slave (secondary) services. As this server (Master) is protected from the outside world we will allow it only to connect out and make name server queries to external sources. We cannot configure MS DNS to be a forwarder only, but in this scenario there is no great risk to the server.

Syslog server

The Syslog Daemon allows a syslog aware client to send it logging messages over the network. This provides us with two useful outcomes: -

1. Our logs can be centralised
2. If one log is compromised and deleted, hopefully we have the master log.

By its nature Syslog requires a great deal of disk space to cover all logged messages. Our Master Syslog server on Service Net 4 will require many gigabytes of HDD space and memory to ensure we can receive all the logs, aswell as an excellent SCSI controller buffer, when requests outpace disk write speeds.

A Linux host will act as our master syslog server in Net4 and Event log monitor (NT4)hosts will be in place in our networks. This allows us to log NT Event Log Messages with the logs of the routers and firewall devices also.

Syslog servers receive logs via UDP port 514. This must be enabled from all necessary devices to all syslog servers. The security policy rulebase specifies this.

Simple Watch (Swatch ftp.stanford.edu/general/security -tools/swatch) will be setup to perform alerts or notifications when particular log text sequences are found, or in the case of a DoS, when no logs have occurred in a set time.
Swatch will requiring some tweaking to do what your Security staff see fit. Ie Email, execute a program to SMS and Alert pagers etc.

Intrusion Detection systems SNORT

A decision has been made not to install intrusion detection beyond the perimeter firewall, this has been made due to the high rate of positives that will hit your DMZ. An administrator could probably be posted permanently on this machine analysing data. If you see fit, you could setup another IDS station here, and simply analyse it when needed.

IDS stations will be made up of Linux workstations running SNORT (www.snort.org) and TCPDUMP (tcpdump.org). Snort will be configured to detect certain known suspicious packet scenarios and sequences, such as SYN ACK RST FIN flags all set, or frames that overlap size for the corresponding sequence number.

TCP Dump will be used to analyse this data in depth.

Use of an off the shelf product such as ISS Realsecure (www.iss.org) would also be beneficial with predetermined functions that it looks for to trigger aler ts and actions.

Installation of Cisco Catalyst 2900XL switches (or similar) will enable us to mirror ports to one port giving us our IDS entry point per Service Network (& DMZ if required).

We're being attacked! Now what do we do?

Have a plan, know you r ISP intimately. Don't act rashly.
When the guns go off, people tend loose their focus, so when the phones start ringing hot and you're the centre of a DoS attack, the tendency to "pull the plug" and hope it goes away after a while is tantamount to stick ing your head in the sand. Its time to think.

Your plan should involve, contacting your ISP letting them know what is happening fast.
Giving them any info your intrusion detection systems or firewall logs are producing as to source IPs and ports. Some of it will be fraudulent that's part of the attack.
Your ISP should work with you to resolve the process. They're paying for the bandwidth too!

Ensure something is capturing the attack, if nothing else it will provide good case studies for your staff to lea rn from and try to prevent in the future.

Have the security team seen anything strange in the logs recently they thought was a little off but nothing serious? This may be related. Is this new exploit, or are we behind in our patching?

Can we disable one service rather than all of them, for a period to discourage the DoS.
Is there an expert your team can call on, perhaps they submit the attack to someone for some help. The "other" GIAC (www.sans.org/giac) is a good example.

Antivirus

Viruses, Troja n Horse and Worms have got their fare amount of attention over the last 2 years and for good reason. They have brought what were considered secure blue chip companies (as well as smaller ones) to an information stand still and in many case resulted in sign ificant data loss, resulting in large costs to a company like yours.

I consider Virus writing at this point in time to be the hacking tool of email (granted virus can come from anywhere not just email), particularly Windows based email. As such I recommen d a detailed anti virus strategy to combat this.

Using two Anti Virus products on your email servers, Mailsweeper SMTP and Exchange server. In particular I have had good success with Norton Anti -Virus (www.sarc.com) and McAfee (www.nai.com) without wanti ng to show preference of products these two have stable software that is updated regularly (although always after the fact)

Running AV software on the desktop of all clients is essential, as well as on your server pool particularly your web server and fi le servers. Again two layer is better than one. As with your firewall we hope one vendor will produce a fix faster than another.

Restrict or remove floppy drives from machines, USB floppies can be provided to authorised staff or on a per use basis where n ecessary to prevent threats coming in from staff's homes.

Physical Security

Physical security of your infrastructure is always a primary concern. Why would anyone develop an elaborate and complicated attack when they can easily sabotage, or gain acce ss to your systems physically. As such the computer room would be sufficiently secured, with the alarm system logging the entry and exit times of each authorised staff member. This can also be a valuable tool when trying to decipher who made the last adjus tment to a system that is now malfunctioning, for instance.
In keeping with general building practise, raised floors and gas discharge fire detectors should also be installed to reduce risk should a fire or similar disastrous event occur.

Disaster Reco very

Although not necessarily detailed in your brief, I feel it is important to mention Disaster Recovery. As computer security is about mitigating risk it is only sensible to plan out scenarios of risk and the resulting steps to bring your infrastructure back to working order.

This can mean a second or third “hot site” ready to go live in case of an emergency. It could mean having spare equipment off site ready to replace you failed equipment, or simply a detailed plan of action, that would include step s to rebuilding all infrastructure to the security levels before the disaster. This would include patch lists, software and security configurations files such as router and firewall backups to put the devices back into active service.

I would suggest con sulting a specialist disaster recovery company for assistance in this area.

Dialup security and PABX/PBX security

Modem lines that do not pass through your firewall or some stringent security device are like giving a stranger the key to your office to come in at any hour. In implementing the VPN portion of this document I would suggest the abolition of all modems in your company.
At the very least reconfigure them not to auto answer (change register to S0=0) so banking transfer software for instanc e can dial out but external calls cannot be auto -answered on that modem device, or block incoming calls on the line.

Your PABX/PBX may be susceptible to some sort of misuse, such as someone using your phone system to ring overseas and not appear on your c all accounting records. There are many different exploits for the many types of proprietary systems. I highly recommend you contact your PABX/PBX vendor to ensure this is being addressed and maintained periodically.

Some systems contain modems so support staff can configure your PABX/PBX remotely, but if this is an IP telephony setup you may well be letting that technician or whoever into your internal IP network.

The Threat from Within

To assume that securing your perimeter will keep your systems an d data intact and secure places a great deal of trust on your existing staff. Probably too much trust. From using your company resources to access offensive materials, running their own business from yours, to trading your company's secrets to your compet itors. It is impossible to watch all your staff all the time.

As such I recommend:
Logging your staff's access to your key systems such as your database with as much detail as your customer's access.
I also recommend implementing
Mailsweeper for SMTP fr om Baltimore Technologies (mentioned previously)
Websweeper from Baltimore Technologies

Websweeper acts as a proxy server checking content for possible malicious webpage code such as ActiveX & Java, it can strip this content for you based on GUI policy, i t can block the download of executables which helps you maintain your SOE at the desktop. Instead of having staff download new and untested plugins and utilities, aside from the chances of downloading viruses. Address blocking is also a feature, restrictin g your staff from inappropriate sites, you can add to these, for instance, if you find your staff trade shares online during business hours, a common problem, you may choose to limit their broker access.

All policies for Mailsweeper and Websweeper can be configured across the board or for a specific user. So your Admin staff can download plugins to your intranet and then staff can download them from there, reducing wasted download bandwidth as an example.

You can run reporting features on both products to get an idea of email and web usage.

These technologies allow you to see what your staff are sending out of the company and bringing into the company. Being NT based they will be somewhat familiar to your system administration staff.

Even if your staff a re 100% honest they make mistakes, such as running a virus in their email system or giving away too much information to a "not so genuine" customer inquiry.

Staff should also be advised never to give away internal system and procedural information to any unauthorised person. It may be genuine market research, it may not. Network security isn't about helping others! And everyone has to play their part.

Security Staff

Staff to man the security team will be employed primarily on experience. Relevant industry certification would be taken into consideration and highly regarded dependent on its merits to the infrastructure.

Staff would be expected to be available 24hrs a day based on rotational shifts, with pagers and mobile phones to enable automated messaging from equipment in the case of an attack or device failure.

A focus on teamwork, particularly trying to work in pairs so that no one staff member, becomes the "guru" Trying to eliminate a point of failure in your staff is vital, should that "guru" member decide to depart.

Staff would be provided with resources and time to access these resources. Particularly newsgroup access, email lists, industry publications and industry texts. In order to have a relevant and up to date library with which to draw solutions close at hand. Staff would be allocated atleast 2 hours per day primarily for looking for new exploits, participating in Newsgroups and lists such as Bugtraq, Ntbugtraq and the like.

Security Staff will be advised not to complete surveys/market research unless anonymously, and absolutely not to divulge systems info to any unknown person at any time. Every little bit helps an attacker, and your team should know better.

Independent Security Audits

Independent audits are a good security practise for two main reasons. It keeps your staff honest and accountable as to their implementing good security policy. It also allows you to call in this auditing company should something go wrong that your staff can't solve or otherwise, without an external company having to do hours of general information gathering to get to a point where they can be of assistance to negate a threat to you. Every six months would be advisable.

Good Security, but cheap hardware?

Having a secure network on poor performing equipment is a waste of everybody's time, especially yours. If your systems fall over constantly then your security is probably *too* good ie. Nobody can access anything!
The installation of quality brand name server, implementing fast redundant disk arrays, fast and reliable backup equipment, redundant/spare power supplies for servers/router/firewalls, clustering servers to reduce single point of failure, having spare parts and maintenance agreements in place. All these things contribute to good business sense, maximum uptime and trust in your security equipment.

3. AUDITING THE SECURITY ARCHITECTURE

How to audit when to audit, what we need?

The Audit will take place late at night, (10pm – 5am) probably on a weekend if possible, because that's when a compa ny doesn't notice an attack (except DoS which would be best planned for in the business day to cause as much damage as possible), less general staff, less bandwidth usage. A good time to try to exploit.
If a serious vulnerability is found and may impact bu siness' day to day running (we crash the perimeter firewall), the effect is minimised by the late hour.

Is the Primary firewall working? How do we know?

A few basic tests as a baseline: -

Can the internal staff access the Internet……yes
Can the internal staff send & receive email……yes
Can the internal staff access the web server and amend the fortune cookie database……yes
Can an external host access the website…..yes
Can the external host access the website database…… *Will depend on database security*
Do our internal and external DNS systems talk…..no, (except resolving giacenterprises.com hosts) good
Can SecuRemote clients access the Web server….yes
Can our Corporate/Bus Partners access via their IPSEC vpn…..yes, noted over ports 50,51

From a business stand point, we seem able to "do business"

But is it secure business?

Conduct a perimeter analysis, how can we improve, diagram it

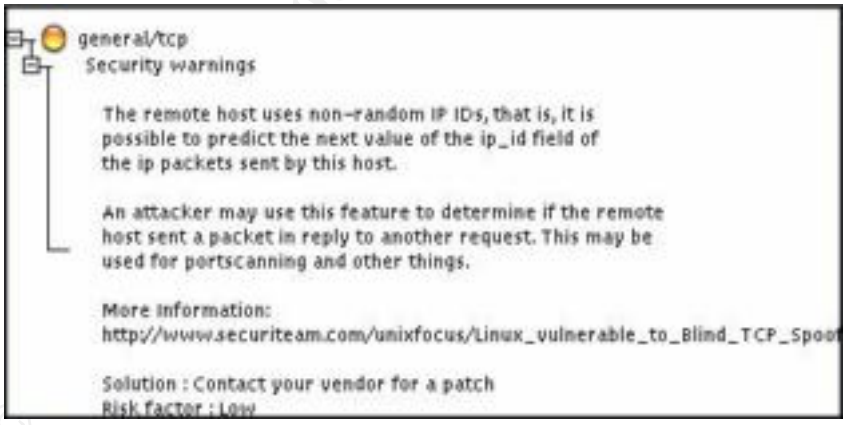
Our perimeter analysis will incorporate the use of several scanning tools.
Nessus 1.07 with plug ins.
STAT
ISS Internet Scan ner
Nmap 2.53 (www.insecure.org/nmap)

We will run the tools on/at all internal hosts and from external point run the tools at internet connected systems. Using the best tool/s for the job.

Nessus (www.nessus.org)

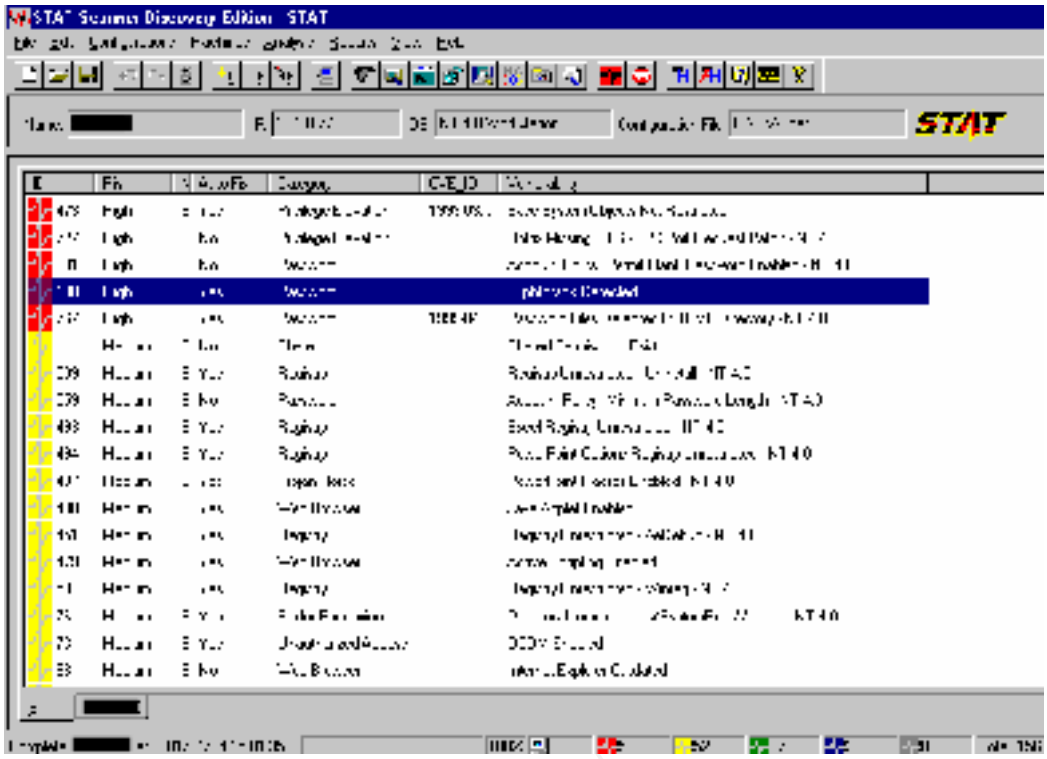
Running Nessus on your web server we find a vulnerability that may have a large risk associated. If the current dvwssr.dll remains an attacker may be able to alter your website.

Nessus (via the help of nmap) points out here on the scan of your router that its sequence numbers are not quite as random as we might like. Using Nmap with the –O option will estimate the suspected OS in this case it guesses Cisco IOS 12.0 - 12.1, but then most border routers are Cisco's and it is relatively up to date.



STAT (www.statonline.com)

On this a dministrator's workstation we find some very interesting results. It appears this administrator has been running L0phtcrack, a password cracking tool for NT and Lanmanager passwords. Among a host of other potential problems. We must decide whether L0phtcra ck is "responsibly installed" on this workstation. Has the Syskey hardener been installed yet? STAT is very thorough in is analysis, and will prompt you to fix the majority of problems on the spot. (Nb the AutoFix field)



ISS Internet Scanner (www.iss.net)
The result below signifies we may have a trojan listening on port 31337, in this instance, a programmer has installed a utility called Genius (www.indiesoft.com) with Port Guardian enabled which waits for port scans on a common backdoor port/s to en trap “hackers” Although not a risk we will disable the software regardless as it is unnecessary.

Host IP Address	DNS Name	Status	Operating System
2xx.210.234.4	localhost	Reachable	Windows NT 4.0

Vulnerability Name	Severity
Portd running	High

Additional Info

N/A

More Info

Description

A port daemon or a potential backdoor program has been detected on port 31337 of the target machine. This usually means that an attacker has backdoored the system.

Fix

If the process is unauthorized, consider the computer and possibly your network compromised. Follow your company's policy for recovering from a system compromise.

Database Security
Access to your database is possible via the general public, this is heavily dependent on the inherent security of the database itself to keep hackers out. This should be reviewed

I would highly recommend if possible, splitting your Public access web server and your database access web server to two separate entities.

Or locking off access to you Public Access server and hosting that site at a hosting company or similar.

SecuRemote
SecuRemote clients can access ports 80 and 443 for all hosts on the Service Net1. This is a problem also. Although we presume these suppliers have your web site being up in their best interest so they can make money. If a laptop was stolen or disgruntled former supplier could take advantage of this through some unknown exploit, there could be grave consequences.

DNS
DNS appears secure nslookup –d giacenterprises.com results in an error. Unspecified Error on a sample NT workstation.

Querying the name servers results in

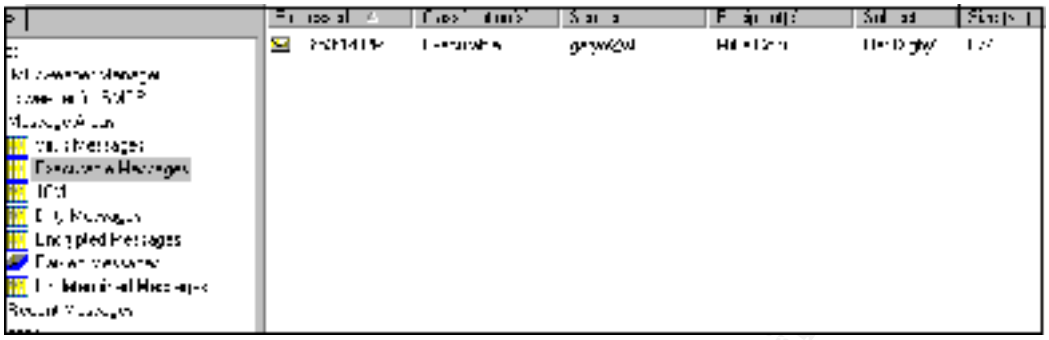
```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47205
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 0
;;        giacenterprises.com, type = NS, class = IN
giacenterprises.com.      0S IN NS        ns.giacenterprises.com.
giacenterprises.com.      0S IN NS        ns.isp.net.
```

So resolution is taking place as required.

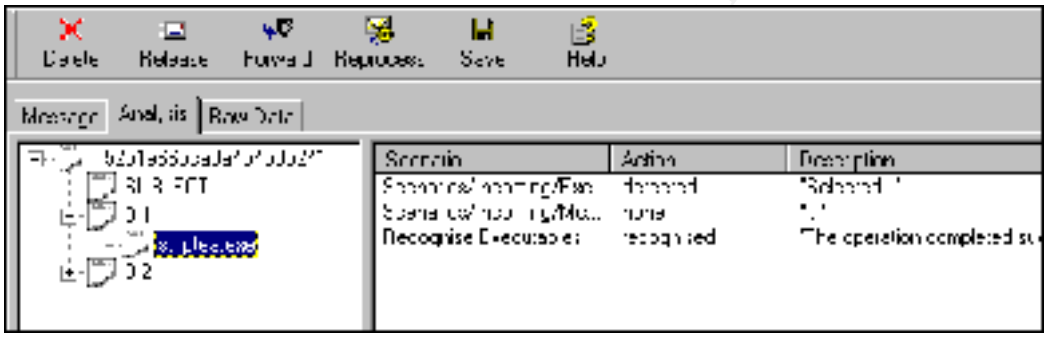
Web Server
If the web server is plagued by IIS vulnerabilities, consider upgrading to Windows2000 and IIS 5.0 or porting website to a more proven web platform, running on Apache over Linux or similar.

Email

Mailsweeper seems to be doing an adequate job of filtering mail and mail attachments. Here we see an inbound executable quarantined into a holding message area. The content can then be determined and deleted.



Breakdown of Mime components and what triggered the quarantine



Retried procedure for vbs, screensavers, macro viruses in documents.
Restriction on outbound mail for the same objects adds to your good neighbour policy of not being a conduit of viruses, executable files and pornography etc.

Email Viruses are checked at both the SMTP server via one up to date AV product, and again internally at the Exchange server vi another product also up to date for virus definitions.

Final Conclusions of the Audit

The perimeter security is sound in terms of firewall and router configuration. Risks to DoS and reconfiguration of objects has been minimised.

Reliance on your ISP for DNS support may or may not pose a risk, the tendency for your ISP to misconfigure the devices ability to zone transfer although small, is out of your control. You may want to consider bring the Slave server in -house and host it yourselves.

Database security and inherent programmed security with SQL and IIS is the greatest concern as mentioned above. Consider having the database independently assessed from a programming point of view with regard to security.

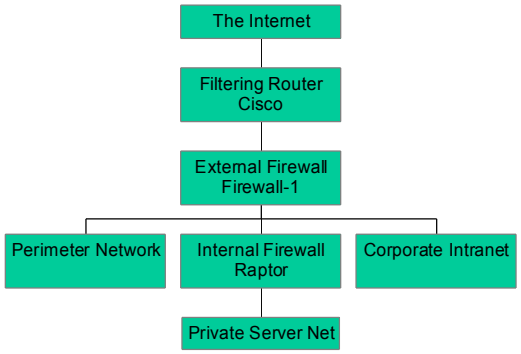
Ensure your servers particularly web servers are patched on daily basis, and ensure that known vulner abilities are understood by security staff, as to how they work and why.

The logging and intrusion detection of this policy should be detailed in greater depth.

4. DESIGN UNDER FIRE

GIAC Submission chosen from Jeffrey Roth http://www.sans.org/y2k/practical/Jeffrey_Roth_GCFW.zip

GIAC Enterprises Security Architecture



Attack their firewall, choose the attack and explain the outcome for that firewall.

My attack to the firewall and DoS have been combined into the one attack.

Checkpoint Firewall -1 4.1 prior to SP2 (4.0 SP7) was susceptible to a fragmented packet denial of service attack (although many believe it to be a resource exhaustion exploit).

In a word JOLT2.

As the security policy chosen did not specify a service pack level to implement. We must assume at the time of installation and a short period after (depending on the Security Administrator's vigilance) they were running Firewall -1 v4.1 **no service packs** . Sorry to be pedantic.

Will our router rules help? Not really for this. On a standard Cisco ios fragmented packets will be passed on. If the Cisco does try to drop them, it will become the point of the DoS as the Cisco would have less resources (than the firewall) to be consumed, resulting in DoS even faster.

Our 50 compromised cable modems courtesy of some up and coming ne w ISP that focused on performance and forgot about security, should be also be thanked at this stage.

The Jolt2.c utility has been specifically designed to craft and stream large IP fragments, and in this case we direct them at Firewall -1. The CPU usage w ill jump to 100% and a continuing stream of these packets will result in the firewall becoming a wall which stops legitimate business use and causes admin staff to panic. The log file will also rapidly fill, possibly overflowing your logs making them usele ss for anything but this attack.

The attacks can be referenced at these links. The SANS link also contains the JOLT2.c code to compile and use in the attack.
www.checkpoint.com/techsupport/alerts/ipfrag_dos.html
www.sans.org/infosecFAQ/malicious/jolt2.htm

Could we have avoided this? Yes!
Either by installing the latest service pack (then Sp2) now up to SP3 (4.1) and SP8 (4.0) or as the system is a solaris box, entering $FWDIR/bin/fw ctl debug –buf at the command line to stop fragmentation logging. If on N T, get the service pack!

Compromise an internal System, why that system? Describe the process?

Although briefly mentioning it as a risk, we find according to the policy nothing has actually been instigated to prevent even a simple executable or vbs att achment entering the network. Anti virus programs unfortunately can't block "intent"

Compromising an internal system will require some hit and miss "Telesales".

1. A bit of phone work outlining vital "market research" (read *Hacker research*)should allow us to determine. The victims Mail server and client, their platform 9x/NT/2000/Mac/Unix. Potential usernames, maybe even an email list. Domain registry for the site can give us admin contact names for usernames to privileged accounts. Can they connect out to my "sales website" @ "www.bogus_sales.com" and see what I'm selling? They can get out to Port 80…interesting.

What we are looking for is a "dumb user" on 9x/NT/2000. When we find someone, preferably the PA to a General Manager or Managing Director privy to company secrets but no concept as to the worth of that information. I must convince the user (or probably don't have to) to run an executable file from their email that, then acts as a trojan horse.

For 9x/Outlook
It runs a malicious vbs script to run and forwards the contents of their in and out mailbox to my temporary mail account.

For NT/2000 (regardless of email)
It installs a keystroke logger running invisibly (something like Invisible Keystroke Logger Stealth www.amecisco.com/iksnt.htm) and a vb s script to run and forward the log of the keyboard logger after some specified time period repeated interval to our Netcat service listening on port 80 at out temporary website. Collecting what they have been typing.

I apologise the trojan "didn't work" when she ran it and send her a second dummy working attachment to alleviate suspicion.

No I can hopefully see the correspondence (in one form or another) of our victims superior, and maybe even some passwords.

Thanks for your assistance, "Ms Rogers" I'l I be watching your typing and checking for errors.

We could probably repeat this process two or three times in a day, without creating any great suspicion. And hopefully tripling our results our pay off!

Not exactly rocket science, but something that any one with the ability to alter an existing VBS mass emailer virus and some good phone manner could accomplish. And who knows what that information is worth?

Hardcopy References:

Cisco Product literature
Configuration guide for Cisco Secure PIX Firew all Version 5.3
Installation guide for Cisco Secure PIX Firewall Version 5.3

Baltimore -Technologies – Mailsweeper Product Documentation and Support website

Checkpoint Product literature
Checkpoint Firewall -1 Security Courseware

SANS Firewalls and Intr usion Detection Courseware
SANS - Securing Windows NT Step by Step pdf

CCNA Study Guide – Lammle Porter Chellis - Sybex

Hacking Exposed 1 st Ed– Stuart McClure & Joel Scambray – Osbourne
Linux System Administration Black Book – Dee-Ann Leblanc - Coriolis

Sunbelt -Software Products Literature
Sans.org – Weekly digests - email list

Website References:

www.phoneboy.com – Independent Checkpoint FW1 product support and FAQs, all OSes

search.support.microsoft.com/kb/ Microsoft Online Knowledgebase

www.cisco.com Cisco Systems Website

www.microsoft.com/technet/security/ Microsoft Security Bulletins

www.sans.org/y2k/practical/Mike_Ciavarella_GCFW.zip Mike Ciavarella GCFW I wish I wrote that!

www.sans.org - SANS Institute Website

www.mailsweepe r.com Mailsweeper and Websweeper Home

www.win2000mag.com - WindowsNT/2000 Magazine website

www.sunbelt -software.com Sunbelt -Software supply & support (ELM, STAT, SPQuery)

www.statonline.com STAT homepage

www.tntsoftware.com ELM homepage

www.stbernard .com SPQuery homepage

www.iss.net Internet Security Systems website

www.insecure.org Nmap port scanner website

www.ntbugtraq.com NT Bugtraq

www.ntsecurity.net NT security website

www.hackingexposed.com Website accompanying the book above.

www.sans .org/y2k/practical/Jeffrey_Roth_GCFW.zip Jeffrey Roth GCFW Assignment