Global Information Assurance Certification Paper

GIAC Certification

GCFW Practical Assignment
Firewalls, Perimeter Protection, and VPNs

Version 1.5e

By Michael Semling

1 Assignment 1: Security Architecture

GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings needs a security architecture for its network.

Points which were regarded as important and which influenced the architecture:

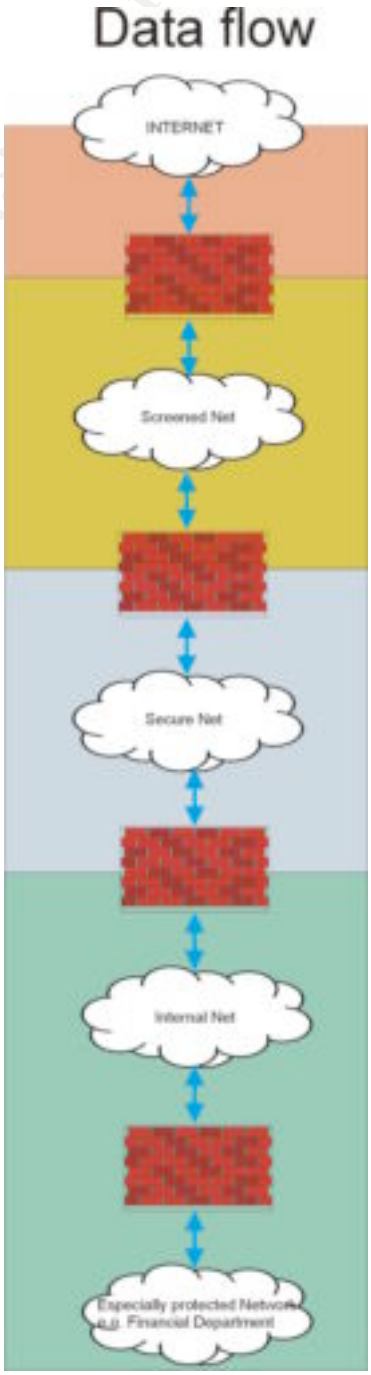
- **Several layers of security**: Based on the function and classification, the data needs more or less protection. This could be expensive but the loss of confidentiality of personal data could be even more expensive. Diversity and dept of defence are regarded as important.
- **Future possibility of adding redundancy**: At the moment, for financial reasons, the network is not redundant. But adding redundancy should be possible without changing the architecture. Of course, some parts have to be adapted.
- **Service and Management network:** A separated network for management and services is suggested to help managing the network. It is a compromise between network management wishes and security desires. Management people wish to access the machines with protocols, ports (e.g. for SNMP) and change settings e.g. routes or access options. Not too many restrictions are demanded. People responsible for security on the other side want to have closed all and everything what is not absolutely necessary to provide a service, e.g. SNMP, ICMP.
- **Administration:** For administration, not too many different products or brands should be chosen. On one side, different brands lower the risk of an exploiting a single vulnerability, on the other side rises the probability of introducing an error into one of the different configuration.
- **Reliability:** For an Internet based enterprise, reliable access with minimal downtime is expected.

This is a great chance to design a network from the scratch. The first thing is to think about the data flow and the borderlines I want to have. To design the paths, I need to know the start and endpoints of logical connections. Then I draw a logical plan with all my machines. Finally a physical plan should be available. I use colours to separate the different paths and the borders of the networks.

1.1 Data flow

“Biologically” (sometimes aka chaotically) grown networks often have several entrances or bypassing lines. It is not easy to maintain firewall-rules for several entries. I would like to avoid this and having only one single point of entry, perhaps with redundant hardware for load sharing and against hardware failure. The advantage is that the entry into the network, the logging and the protection is just one point. The disadvantage is that this is a single point of failure for (high) availability and might be a throughput bottleneck.

The Internet with our customers and suppliers is connected with an unknown router on the ISP side (which is not under our control) to our router. This acts as a packet-filter blocking several IP addresses.
This router is under the control of the security people. Other routers may be controlled by the network management but this one not.
After the first firewall the Screened Network, sometimes also called DMZ is reached. For performance reasons, the firewall could consist of several sequential firewalls, a stateful filter first to relieve the following inspection filter or application proxy.
Into this place my public accessible machines which should be bastion hosts are homed.
The secured network is the place where I have my database and internal servers. This protects against internal and external attacks. The firewall should be another brand than the one above to provide redundancy for OS or software flaws.



Data flow

The Internal Network is the official information network for all employees. For security reasons, the firewall should not be an already used brand, for maintenance reasons I prefer not using more than two brands. So I decide to use internally the same brand.
The research department might install another brand, managed from the security researchers themselves.

Especially valuable data, e.g. Financial Data, billing, human resources, etc, needs additional protection and might have their separate network.
There is another network, the service and management network (Service Net), which I will physically separate from the “normal” network. This is not shown on the picture on the right.

1.2 Access Definitions

First I define who or from where may access what:

Who	Allowed accessible services	Granted access, protocols, port number
Internet	Service incoming and outgoing from and to the Internet	In- and outgoing e-mail (TCP 25) from/to the Internet DNS (UDP 53) to Internet via Screened Network server FTP (TCP 20, 21), HTTP (TCP 80, 443) to Internet via Web Proxy
Visitor (Internet)	Non paying customer who browses the Internet and is interested in our offers	To Screened Network server: DNS (UDP 53) to external DNS Reverse Proxy (TCP 80)
Customer (Internet)	A paying customer who wants the fortune cookie service. Has access to the public part but also a special individual customer page protected with SSL and using JAVA scripts over SSL connections.	To Screened Network server: DNS (UDP 53) to external DNS Reverse Proxy (TCP 80) Reverse Proxy (TCP 443)
Partner (Internet)	An international partner who translates and resells fortune cookies.	Needs (restricted) access to the Web Proxy for ftp only. Access is granted by using VPN doing SCP to the Web Proxy. Informing the server responsible by sending an e-mail to apply the changes.
Supplier (Internet)	Suppliers are writers of the fortune cookies.	These are also accessing the Web Proxy for data exchange using SCP via VPN. The responsible person does the changes in the database.
Worker	Employees of the enterprise.	For internal networking there is an internal DNS, internal e-mail server and internal Web Proxy to access Internet HTTP and FTP server. Internal authentication is done by using an LDAP server.
Reverse Proxy	Visitors and customers.	Accepts http(s) (TCP 80, 443) connections, does the SSL work and connects the data base and web server cluster.
Screened Network	Servers accessible from Internet and Secured Network.	Machines in the Screened Network accept connections from any points in the Internet for their service.

Who	Allowed accessible services	Granted access, protocols, port number
Secured Network	Machines accept either defined connections from machines on the Screened Network or from allowed machines on the Internal Network.	Connections are made either with SSH (TCP 22) or with service ports from some machines, e.g. DNS (UDP 53), e-mail (tcp 25, tcp, udp 143, 220, 993, 995)
Finance	Special department with sales and HR. Especially protected.	The financial data is not accessible for all workers. The printers are also not freely accessible.
Internal Net	The network where the employees with their workstation, the local servers, printers etc.	Access to internal DNS, internal MAIL and Web-proxy (for http and ftp).
R&D	Very special people. With their own firewall.	The firewall is not only to protect the secrets of GIAC enterprise moreover it is to protect the normal working network from the R&D department.
Teleworker	Workers who have the permission to work from home.	They are in the network as if they were in the office. Using VPN, Secure ID and LDAP for authentication and working in the Internal Network.
Service Network	A separated network for collecting Syslog data, IDS central station, central management, configuration management, NTP, SNMP, and BACKUP.	This is a switched, non-routed network.

1.3 Logical Design

The first point is the router. The border router is the first line of defence and is connected over an E1line (2048 Mbit/s) to the provider. The router filters traffic (e.g. ICMP) and permits or denies access to service ports, depending on the IP addresses.

At the router unwanted traffic is blocked, like source-routed packets, DoS traffic, vulnerable and therefore forbidden TCP and UDP services (e.g. BOOTP). The implemented ingress-filter lets no spoofed or private addresses [RFC 1918] into our network. The egress filter avoids outgoing connections with usage of non-internal addresses. This keeps a good Internet neighbourhood. This router is connected to the service management network which uses a non-routable IP class like 192.168.0.0.

First firewall: Stateful inspection filter for incoming traffic, manages the VPN and does Network Address Translation (NAT) allowing static NAT access to the external DNS,

the external e-mail and all HTTP or HTTPS traffic to the reverse proxy on the Screened Network.

Split DNS is proposed. The visitors and customers (green) are coming from the Internet – they are allowed to access the external DNS. Our ISP (IPPLUS) demands a primary and a secondary DNS. Also the e-mail is set up redundant, it is possible having a fail-over switch just by having two MX records in the DNS entry for the enterprise.

The partner, supplier (yellow) and teleworker (orange) could use a dial-in line (e.g. CISCO 3040) but I decided that they use VPN (included in the first firewall) over the Internet, for personal authentication in the network they will use Secure-ID cards.

The reverse proxy provides a gap between user-access on the reverse proxy and the database and WWW server on the Screened Network for security and performance reasons. It does caching, SSL en- and decoding and might be used for load balancing in the future. For the HTTPS certificate a Certificate Authority (CA) like VeriSign, TC Trustcenter, Globalsign or Swisskey will be used. (Comment: While doing this work, Swisskey announced that they will do this service for the public until the end of the Year 2001, then all certificates will be revoked but for customers with an electronic means for certification requests). It gets the data from the web server and the data base on the Secured Net.

All these machines on the Screened and Secured Network are bastion hosts. They are hardened [Boran] [Spitzner_Solaris] and also have a local firewall installed.

The external e-mail server is delivering the e-mail addressed to the internal e-mail server. The External DNS receives the zone transfers from the Internal DNS. For management, SSH from the Service Network only is used. The internal DNS asks the external DNS which will search for the top-level-domains.

The IDS sensor has a silenced interface (unplumb) displayed with dotted lines.

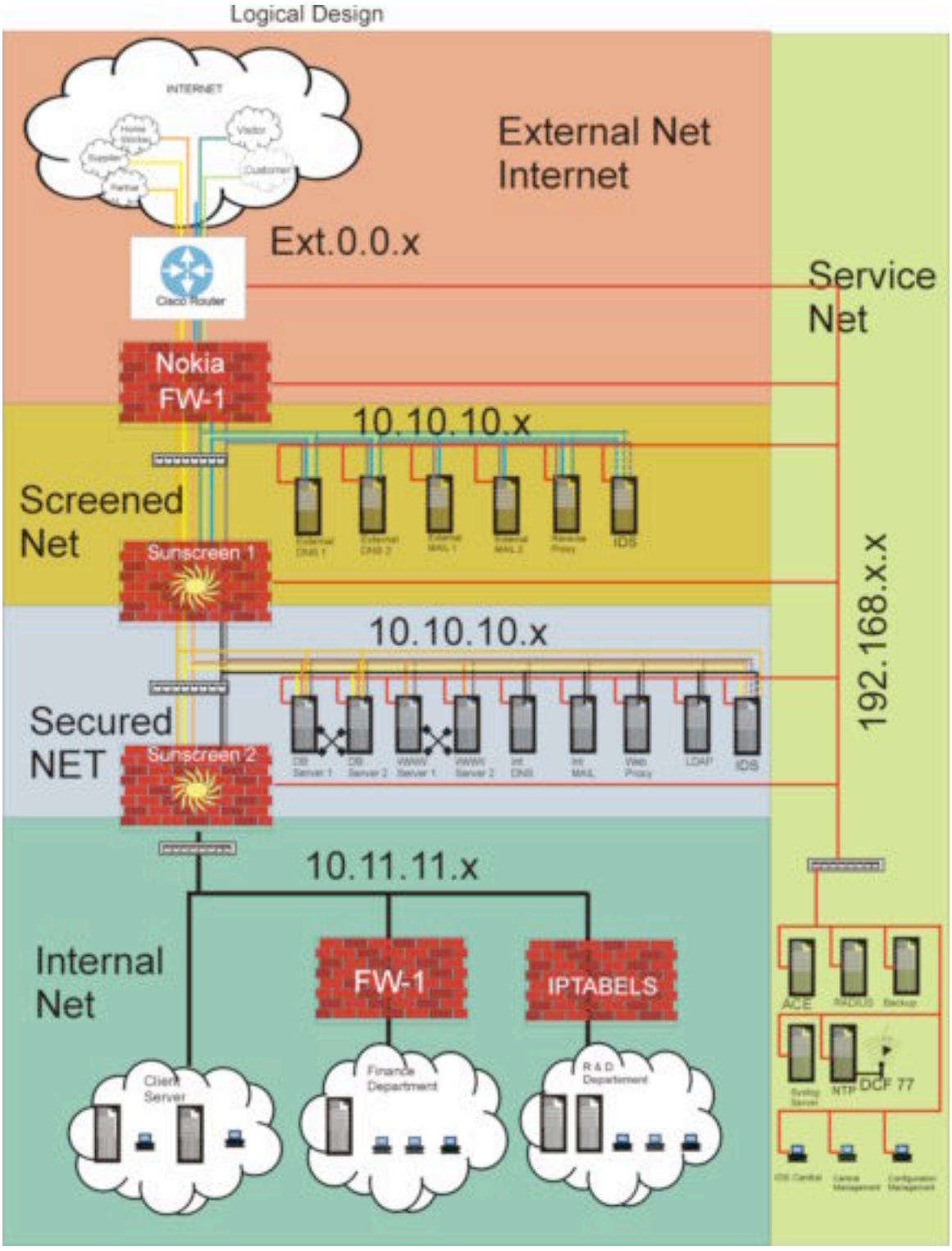
The second firewall is a stealth firewall protecting the Secured Network from the Screened Network, but the network has the same IP class. Allowed is only HTTP and HTTPS from the reverse proxy to the WWW. Traffic initiated from the External servers (DNS, E-Mail) is being blocked. It protects also the access to the database server and the web-server on the Secured Net. Traffic from the Internal Network also is blocked. Only traffic from internal DNS, internal e-mail going to the Screened Network and traffic from the web-proxy to the Internet may pass.

The database and the web server are clustered. This is for reliability. If clustering can not be afforded in the first step, a RAID (e.g. RAID 5) could avoid (decrease) possible downtime.

The third firewall between the Secured Network and the Internal Network is a hardened Solaris Sunscreen. It is responsible for passing one-way traffic from the Internal DNS, Internal e-mail and Internal web-proxy to the Secured Net.

The internal DNS, e-mail server and HTTP proxy are not redundant. This could be done but duplicating every key element and the maintenance is regarded as too expensive for the start-up. It could be realised later if the business is successfully growing. The LDAP server as authentication server is also there. It is important that

all e-mails are scanned for viruses and unwanted attachments. Internal DNS for Internal Network queries may connect the external DNS. The internal e-mail server sends and receives e-mail from and to the Internal Network. Access to the Internet is done over the Web Proxy server (HTTP, FTP, etc).



Logical Network Design

In the Internal Network are the normal workstation and servers for work. They all have local virus scanning software on their machines. The finance department, which does the billing, the salary, etc, has a special protective firewall; a Firewall F-1. The research and development group has their own firewall which they manage themselves. This is to protect the workers from experiments in the research group.

The Service Network is a physically completely separated network. The network management is done with SNMP. The IDS central database and the central syslog server are placed here. The NTP server receives the time signal from a DCF77radio receiver, connected to the serial port. The backup server is placed on the Service Network for performance reasons.

1.4 Hardware, Infrastructure and Devices

This is for the physical design and the hardware cost estimation. I assume, the GIAC fortune tellers don't trust their own sayings and prefer to have real physical security. This should include the placing of the devices, air cooling, physical security like UPS (Un-interruptable Power Supply), fire and water alarms, and physical access control.

The machines from the external, Screened and Secured Network are in one room where all the points above are realised.

For the fire and water damages appropriate alarm measures have to be taken. These measures depend also on country law and insurances.

For physical access, I propose a proper key and access code management and a simple biometric fingerprint solution. The key restricts the range of persons who can enter the room; the fingerprint solution helps to identify who entered.

UPS protects against high-voltage peaks and short-time power loss. If the power is switched off for a long time, a graceful shutdown without data loss is provided. I think it should be enough if the devices are able to hold internal machines up for 10 minutes. For Internet servers (e.g. reverse proxy, database, server, firewall, router), the time should be 2h.

In what follows, the physical devices and the interfaces are designed. I recommend using coloured cables to differentiate between the several networks, in order to avoid short circuits.

CISCO Router 3640: Rule changes can be done by connecting to the Ethernet2 interface only.

First Firewall: The first firewall is a NOKIA appliance routing firewall IP330 with a VPN plug-in which protects the Screened Network from the Internet.

External DNS 1, 2; External E-Mail 1,2: Single purpose bastion hosts SUN NETRA X1 running Solaris 8.

Reverse Proxy: There is enough power with a NETRA X1. This host could be improved with more memory (e.g. 512 MB) and also a second disk for mirroring to reduce possible downtime.

Switch: A switch, CISCO catalyst 2912 provides the connections. One is installed for the Screened Network; one is used for the Secured Network. For the Service Network a 2948 is used.

Second and third Firewall: A Sunscreen stealth firewall running on a Sun Ultra 100.

IDS: The Intrusion Detection System machines are hardened and have a silenced NIC running snort on the sniffing port. The SUN NETRA X1 has two interfaces. The second interface is connected to the Service Network.

Database and Web-server: Database and HTTP(S) (aka WEB) server are SUN Ultra 250 machines running in a cluster.

Internal DNS, E-Mail: SUN NETRA x1 with an additional hard disk for mirroring because no redundancy is planned for the first step.

Internal Proxy: SUN NETRA x1 with 512 MB memory.

Service and Management Net: This is a special network with many security critical applications. The backup server will connect all other servers securely and back up the data. This is done on a separated network for security and performance reasons. The IDS central is the central database and inspection point of the collected data from the sensor. The data is copied with SCP. [Spitzner_IDS]
The syslog server collects all the logs from all the machines on non-internal networks. On this server also the initial database of aide [aide] or tripwire [tripwire] are stored for comparison.
For synchronising the clocks, an NTP server is available which has the time-normal signal from a DCF77 atomic clock connected to its serial port.

Estimated hardware Prices:

The price is calculated without user machines, user switches, printer etc.

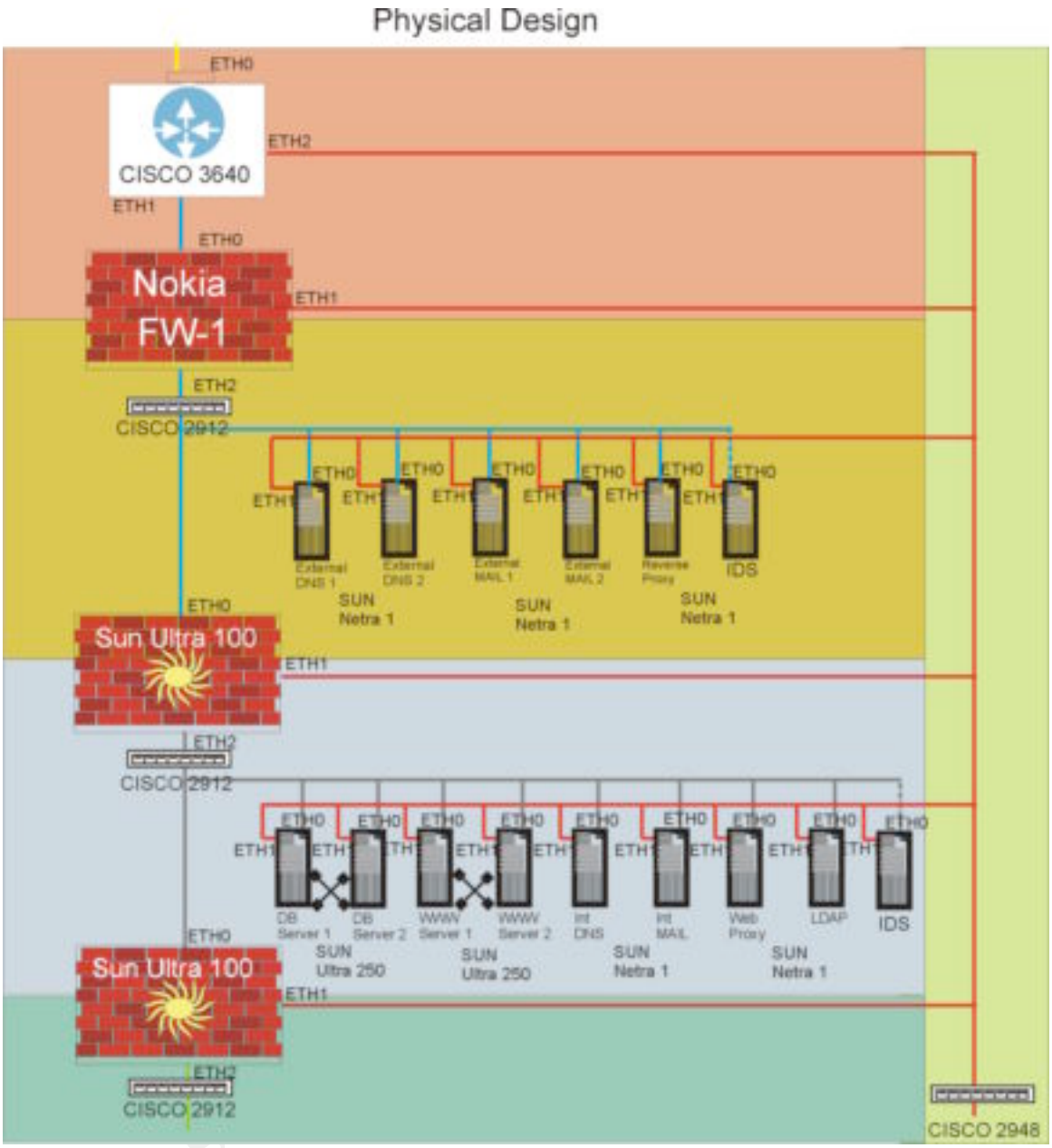
UPS: $10,000

CISCO Router 3640: 5000$
Nokia firewalls 330 with VPN plugin $30,000.
20 pieces of SUN NETRA with some improvements: $30,000.
4 pieces of SUN 250 and 2 pieces SUN 100: $80,000
Switches etc.: $20,000
ACE/RADIUS and Secure-ID: $15,000

Total: ca. 200,000$. Which is acceptable with an expected earning of $200 million per year.

Personal experience shows that 10% of the hardware costs could be calculated for repair, upgrade and maintenance per year.

In the following physical design, the Internal Network with the additional firewalls in the Internal Network is not included.



Physical Network Design

Future possibilities and enhancements:

Pitbull Solaris could enhance the security because the firewall keeps the unwanted services away but the machine providing a service must be secure! For financial aspects, (administrative education, software) this could be considered in a second step.

An additional filter firewall which protects the inspection firewall for performance reasons.

At the moment, downtime can be reduced with mirroring or RAID5 but clustering of the important systems should be realised. Redundant Internet accesses and Firewalls could avoid inaccessibility because of a hardware failure.

Hot swap for the router, switches and other devices for a secure fail over.

For special desires of the R&D department, a SOCKS proxy could be installed.

There is yet no way to allow an administrator to log in remotely. For future purpose, a second way to dial in should be considered to minimise downtime. This access point has to be protected and hardened by using at least CLID (Calling Line IDentifier), Secure-ID, and certificates! Be aware that this creates another entry into the network!

To protect the internal e-mail server, a reverse e-mail proxy might help to protect internal sensitive e-mail messages, e-mail could be fetched using an SSL line [Stunnel].

A bandwidth controller should be applied, which can help against flooding. [Packeteer]

An internal CA for internal encryption for signatures and authentication could be provided.

For the financial data network, a MAC- address policy could be implemented to avoid unknown machines in this network.

2 Assignment 2 – Security Policy

2.1 Internet Router ACL

To start with hardening the Internet access router and for the implementation procedure see [SANS_router] and [CISCO_Perimeter_Security].

In my proposed configuration, Cisco's latest IOS (12.2) is installed. The CISCO configuration guides and command reference can be found at [CISCO_12]. Minimal services and disclosed information only as much as needed is the strategy.

1. Global commands (use "conf t")

For the host name of the router, I prefer not selecting an expression which gives information about the purpose (e.g. GIAC_Internet_Router):

hostname GIAC_Machine

#

2. To protect the password and using encryption and MD5 hash:

service password-encryption
enable secret <password>

#
#To allow local console and ssh login from certain machines only from the Service Network, see [CISCO_Security_Improve]!

line con 0
exec-timeout 5 0
login local

#

line vty 0 4
access-class 11 in
access-class 11 out
exec-timeout 60 0
transport input ssh
login

#
ssh time-out and the numbers of retries

ip ssh time-out 60
ip ssh authentication-retries 3

We turn on the logging feature of the router
logging buffered
#
to send all the buffered logging-data to a syslog server

logging <IP.syslog.server>

#

#
#Blocking unwanted services: Dropping packets with the source-route flag set, which could be used for spoofing or inspection.

no ip source-route

#
Switch off the http server, there were several vulnerabilities [CERT_CISCO_HTTP]. This is default but just to be sure…..

no ip http server

#
#We do not handle DHCP or BOOTP via router.

no ip bootp server

#
#I do not want to have DNS-lookup. For disabled domain-lookup, DNS will be bypassed for rcp and rsh even if ip rcmd domain-lookup is enabled. I do not want to give away any information .

no ip domain-lookup
#

No information about unreachable addresses. This could produce more traffic because machines try several times before giving up but make it harder to find out our network (inverse mapping).
no ip unreachables
#
No packets are allowed to be redirected, which could be used to redirect the travel path to sniff, alter data
no ip redirects
#
Because we do NAT on our Firewall not on the router and we don't want to show anything.
no ip proxy arp
#
To deny the subnet zero .
no ip subnet-zero
#
#We do not need the chargen/daytime/echo service which can be used to attack others.

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

#
#Finger service giving away information what we do not want.

no service finger
#
#We do not need to synchronise time by Internet, we have DCF77 at the NTP server using NTP protocol 2 accessible on the interface Ethernet2.
NTP server <IP.NTPserver> version 2 Ethernet2
#
#CISCO Discovery Protocol can be used to get information from out router. Since we know which machines are on our network and we do not want unknown machines to cooperate, we do not use CDP
no cdp running
#
We do have SNMP on this router, and we do SNMPv1, to the Service Network side only and to two machines only and read-only and access list 11
#
snmp-server community <community-string> RO 11
snmp-server host <IP.snmp.management.machine> <community-string> snmp
snmp-server host <IP.snmp.configuration.machine> <community-string> snmp
#
Our router is connected to the NTP lets log with date and time
#
service timestamps debug datetime
service timestamps log datetime
#
Login banner for the legal message!

banner login ~
Authorised access only. Usage is monitored.
~
banner motd ~
==== You have logged onto a GIAC router. ====
~
#
3. Interface specific commands for interface eth0, eth1, and eth2, the external interface, direct broadcast are used to access many machines by one packet and are used to amplify attacks (e.g. smurf attack) or for denial of service attacks(broadcast-storms), therefore I do not want them.
Run “int e0” or the Ethernet interface you want to see (s0 is the serial 0).
#
interface Ethernet0
description “Internet”
ip address <GIAC.external.router.IP> <GIAC.external.IP-range>
ip access-group 101 in
ip access-group 102 out
no ip directed-broadcast log-input
no snmp
#
#
interface Ethernet1
description “Screened”
ip address <GIAC.internal.router.IP> <GIAC.internal.IP-range>
ip access-group 102 in
no ip directed-broadcast log-input
no snmp
#
#
interface Ethernet2
description “Service”
ip address <GIAC.management.router.IP> <GIAC.management.IP-range>
ip access-group 11 in
ip access-group 11 out
no ip directed-broadcast log-input
#
#

4. ACL : The CISCO syntax for the standard access list (number 1-99) is used for packet filtering (very fast):

access-list <number 1-99> <permit | deny> <source address> <mask> <log | log-input>
The extended access-list with number of 100-199 gives the control over IP destination, the protocol (UDP, TCP, ICMP) the ports, flags and type of service (TOS).

access-list <number 100-199> <permit | deny> <protocol> <source> <source-wildcard> [<operator port [port]] <destination> <destination-wildcard> [<operator port [port]] [established] [precedence precedence] [tos] [log]
established is for TCP connections only, to pass the ACK or RST flag has to be set. The access-lists are set globally and can be reviewed with “sh access-list 101” or the number of access-list you want to see. Do not use number 199, there were some problems with!
For the Service Network Interface
access-list 11 permit ip <IP.central.management> any
access-list 11 permit ip <IP.config.management> any
access-list 11 permit ip <IP.NTP.server> any
access-list 11 permit ip <IP.syslog.server> any
access-list 11 deny ip any any

#
Ingress Filter lets no spoofed or private address into our network log or the verbose-form log-input depending on memory and speed, (e.g. for smurf the next router can be found what I do on the interface part).
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log # invalid address
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log # private
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log # localhosts
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log # private
access-list 101 deny ip 192.0.2.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log # private
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log # multicast
access-list 101 deny ip 240.0.0.0 7.255.255.255 any log # reserved
access-list 101 deny ip 248.0.0.0 7.255.255.255 any log
access-list 101 deny ip host 255.255.255.255 any log # invalid host
access-list 101 deny ip host <external router interface> any log
access-list 101 deny ip <GIAC network> any log
access-list 101 deny ip <screened network> any log
access-list 101 deny ip <secured network> any log
access-list 101 deny ip <internal network> any log
Now what we allow explicitly:
As stated in the IPCHAINS howto: “it's definitely a BAD idea to blindly block all ICMP traffic. (In particular blocking things like "destination unreachable" and "fragmentation needed when DF option set" will cause problems for your systems when they are trying to engage in legitimate TCP/IP communications). “ So we allow incoming ICMP messages like echo-reply, time exceeded in transit, packet too big but the DF flag set and unreachable-messages. We deny all the others!
access-list 101 permit icmp any <my public network address> <mask> echo-reply
access-list 101 permit icmp any <my public network address> <mask> time-exceeded
access-list 101 permit icmp any <my public network address> <mask> packet-too-big

access-list 101 permit icmp any <my public network address> <mask> unreachable
access-list 101 deny icmp any any
#
now we allow the traffic we want to let pass, the FIREWALL will do NAT but we address the real addresses!!! Requests to our public network address range. I do NOT use the router to limit protocols, this is delegated to the firewall.
access-list 101 permit tcp any host <my public network address> <mask> log
access-list 101 permit udp any host <my public network address> <mask> log
#
we allow now traffic to the Firewalls external interface for UDP and TCP when the connection went from this interface (if the ACK or RST flag is set). This allows us to go on the Internet, the firewall does the masquerading!
access-list 101 permit udp <my public firewall address> <mask> any any log
access-list 101 permit tcp <my public firewall address> <mask> any any established log
#
finally we deny all others
access-list 101 deny ip any any log-input
#
#
#Egress filter in **EGRESS FILTER**, non-GIAC-owned addresses or private address cannot travel out
On the external interface to the Internet I place the filter to avoid public addresses from my Service Network just in case I did some misconfiguration. The same ACL does not let pass other addresses than my public addresses into the router if they come from the interface Ethernet1 (internal side of my router)
access-list 102 permit ip <my public network address> <mask> any
access-list 102 deny icmp any any
access-list 102 deny ip any any log-input
Now the implementation has to be verified. Tell the ISP when you will do the tests especially if you use private addresses. From all interfaces check the ACLs and the services available.

Tips:

1. Do not use names, use IP addresses not relying on DNS.
2. Edit the configuration file off line and keep the previous versions!.
3. I prefer the “deny-everything-but-allowed” policy though this can be very difficult to do for a “multicultural” router.
4. Do a deny specific, permit specific, then deny all the rest.
5. Copy the running configuration to the startup configuration thus if it doesn’t work the way expected, just reboot the router and the old configuration is active again.
6. Delete all old rules and start from scratch again!
7. If a new IOS is installed check for default values which weren’t in the configuration and may have changed. Better do not rely on default values – always set the values in the configuration.

2.2 How to test the ACLs:

Take a laptop with nmap [NMAP] on it. If you do not like command lines ;-) there is a graphical front-end NMAPFE [NMAPFE].

Put a HUB between router and firewall and attach a machine with a sniffer on or plug it into the sniffer port on the switch. I prefer using TCPDUMP [Tcpdump] or Ethereal [ETHEREAL].

Make a checklist what you expect to see.

Scan from the Internet side to the Intern side.	
Non-public to GIAC Public IP	ok
Non-public to GIAC Public IP ICMP	Only ICMP echo-reply, time-exceeded, packet-too-big, destination unreachable
GIAC public / private IP to GIAC Public IP	Nothing

Scan from the Service Network side to the Intern and Extern side and the other way.	
All combinations of addresses	Nothing

Scan from the Internal side to the External side.	
GIAC public IP to NON-Public/NON-private	ok
GIAC public IP to GIAC-Public/Private	Nothing
Non-GIAC to GIAC-Public/Private/NON-GIAC	Nothing
GIAC public IP to NON-Public/NON-private with ICMP	ok

Run a full UDP port scan without pinging first for your external address range. Command: “nmap –s U –p 1-65535 –P0 <my public ip range>”. This may take a lot of time.

Then run a basic, full TCP port scan without pinging first. Command “nmap –sT –p 1-65535 –P0 <my public ip range>”.

Finally, do a ping scan. “nmap –sP <my public ip range>”.

For ICMP messages use hping [Hping2].

“hping2 –H 1 –C <ICMP-TYPE> -K <ICMP code> <host to test>”

Now the result is compared against what was expected.

2.3 Firewall

Our primary firewall is a NOKIA / FW-1 solution with three interfaces. An external interface to the Internet, an interface to the Screened Network and an interface to the Service Network. It is the firewall's job to enforce the GIAC security policies with stateful communication sessions for services and VPN.

The order of the rules is very important, it starts with the lowest rule and the first matching rule fires.

No	Source	Destination	Service	Action	Track
1	FW_Admin	Firewall	FireWall1	Accept	Long
Allow the Firewall management station on the Service Network to access the Firewall. Logging long for the amount of information.					
2	Firewall	Syslog_Server	syslog	accept	Long
We have a syslog server on the Service Network.					
3	Any	Firewall	NBT Ident	Reject	
Deny Netbios and Ident traffic. This are frequent requests and I want them to be closed with a RST immediately. I don't log them, just too many.					
4	Any	Firewall	Any	Drop	Long
For Administration first rule is used. All the other things are NOT going to the firewall and are dropped. For IPSEC I use a different IP.					
5	Any	External_DNS1 External_DNS2	domain-udp	Accept	
6	External_DNS1 External_DNS2	Any	domain-udp	Accept	
DNS requests on UDP port 53 may be frequent therefore I put it early into the list. Logging for allowed traffic is going to get too many entries. For Internet access I ask other DNS for the IP.					
7	Any	Reverse_Proxy	http https	Accept	Long
Visitors and customers are allowed to access the reverse proxy using port 80 and 443.					
8	Any	External_Mail1 External_Mail2	smtp smtps	Accept	Long
E-mail is accepted on port 25 to our External_Mail1 and External_Mail2. Depending on the volume of e-mail, long logging could be replaced with short or no logging at all.					
9	External_Mail1 External_Mail2	Any	smtp smtps	Accept	Long
Sending e-mail from our External_Mail1 and External_Mail2					

No	Source	Destination	Service	Action	Track
10	WEB-Proxy	Any	HTTP HTTPS	Accept	Long
The worker can go to the Internet using the web-proxy. Port 80 and 443 is allowed. If it is necessary to open other ports (8080, 88, ….) this could be done. At the moment it is monitored. IRC, Audio, ICQ, gaming or other services are not allowed!					
11	Any	Any	Any	Drop	Long
Dropping all packets from anywhere to anywhere which services are not explicitly allowed.					

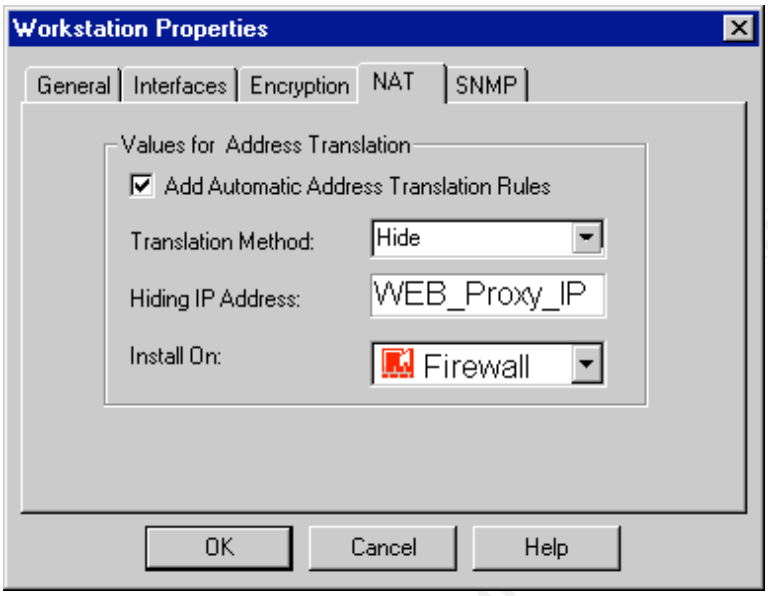
In the IDS I get alerted if any of these servers are doing services or accessing IP addresses they are not designed for and other ports are tried. Also I get a message, if DNS with TCP was required.

For the static NAT, there is a corresponding IP address for the equivalent IP on the Screened Network, we do:

No	Source	Destination	Service	Source	Destination	Service
1	Any	Reverse_Proxy	Any	Original	Screened_Net_Reverse_Proxy	Original
2	Screened_Net_Reverse_Proxy	Any	Any	Reverse_Proxy	Original	Original
After the check, any packets with any source IP which get to the external interface of the firewall with destination to the Reverse_Proxy will get into the Screened Network with the destination IP of the Reverse_Proxy in the Screened Network. And returning packets the Internal IP Address are replaced by the Internet IP address of the Reverse_Proxy.						
3	Any	External_DNS1	Any	Original	Screened_Net_DNS1	Original
4	Screened_Net_DNS1	Any	Any	External_DNS1	Original	Original
5	Any	External_DNS2	Any	Original	Screened_Net_DNS2	
6	Screened_Net_DNS2	Any	Any	External_DNS2	Original	Original
If the packet is allowed to pass the firewall, the Internet IP address of the machine is replaced by the Screened Network IP address for the DNS1 and DNS2.						
7	Any	External_Mail1	Any	Original	Screened_Net_Mail1	Original
8	Screened_Net_Mail1	Any	Any	External_Mail1	Original	Original

No	Source	Destination	Service	Source	Destination	Service
9	Any	Exter-nal_Mail2	Any	Original	Screened_Net _Mail2	Original
10	Screened_Net _Mail2	Any	Any	External_Mail2	Original	Original
Also packets to the destination e-mail server (1 and 2) are changed incoming the destination to the Screened Network address and outgoing the source to the IP address.						

We do hiding NAT on the firewall if the source is the WEB-Proxy! That allows our worker to go to the Internet.



Hiding NAT

We run the latest version (4.1) with all patches. We have disabled the implicit rules like "allow all port 53" and the rules for management connections. "Fast Mode" is switched off. [Checkpoint_FM]

2.4 Primary Firewall testing

We have to check the protection against packets from the Internet, the Screened Network and the Service Network. We can do this by disconnecting the router and all the machines on the switches on the Screened Network and the Service Network. It might be a good idea to do this as an IDS test.

Scan from the Internet side to the Screened Network.		
Public IP of the external DNS 1	Screened Net DNS1	UDP 53
Public IP of the external DNS 2	Screened Net DNS2	UDP 53

Public IP of the external MAIL 1	Screened Net MAIL1	TCP 25, 465
Public IP of the external MAIL 2	Screened Net MAIL2	TCP 25, 465
Public IP of the Reverse Proxy	Screened Net Reverse Proxy	TCP 80, 443
Scan from the Screened Network to the Internet side.		
Screened Net DNS1	Public IP of the external DNS 1	UDP 53
Screened Net DNS2	Public IP of the external DNS 2	UDP 53
Screened Net MAIL1	Public IP of the external MAIL 1	TCP 25
Screened Net MAIL2	Public IP of the external MAIL 2	TCP 25

From the Service Network from/to the Internet/ Screened Network should nothing pass!

2.5 VPN

I use 3 kind of VPN: SSL, SSH, IPSEC.

The customer does encryption using HTTPS with a strong server authentication. For transmission of the authentication password a Java program could be used instead of a CGI program but the transmission is SSL encrypted. Since our customers might be in countries with cryptography regulations we accept SSL version 2 and 3 with RC2, RC4, DES, 3DES with 40 bit up to 168 bit encryption (depending on the algorithm). You can check the supported algorithm on [SSL_SUPPORT].

SSH is used as a telnet replacement. The GIAC fortune policy does not allow telnet or ftp internally except for the Web Proxy. There is also a free SSH-Daemon for Windows NT and Windows 2000 [SSH_Cygwin] and a step-by-step installation on [SSH_Cygwin_Install]. For security SSH is configured using protocol version 2, for speed, the cipher blowfish is chosen and the compression is switched on.

IPSEC is used with VPN-1 ESP for payload encryption. The transmitted data from partners and suppliers as well as from the teleworkers should not be visible to the Internet. Partners and suppliers can deliver their data to the FTP server on the web-proxy and inform the server-responsible of the new data. This restricts the range of administrators.

User authentication is done by using IKE (ISAKMP) in conjunction with the SecureID resp. the Radius Server. For encryption, the strongest possible encryption method is negotiated in case a partner or supplier must use a weaker encryption method because of law regulations. I do not support the proprietary FWZ-1 algorithm. Supported symmetric algorithms are RC4, CAST, DES with 40 bit, DES with 56 bit, CAST 128 bit, Triple DES with 168 bit, asymmetric algorithms are RSA 512/1024 DH 512/1024 for key exchange. For data authentication, MD5 and SHA-1 is allowed.

Split tunnelling is the connection of a VPN client to other networks while connected to our network over a VPN channel. This is very hard to turn off. For legal reasons this is explicitly forbidden in the VPN contract. With Checkpoint Secure VPN client policies could be pushed to the client. [PhoneBoy_FW1] There is additional authentication needed for certain services for teleworker, they have to authenticate on the LDAP server, otherwise they can just access the Web Proxy.

Split horizon is used in distance vector protocols (e.g. RIP) to prevent the propagation of a route over the same port that supplied the route (what could lead into a dead-lock)[Tannenbaum]. In our VPN we do not use any distance-vector protocols - split horizon is not used.

3 Assignment 3 – Audit Your Security Architecture

3.1 Planing the assessment

The GIAC enterprise has a mixed environment with Solaris/Linux server and Windows/Linux workstation. The complete audit should include the physical security (keys, access control, etc) as well as the logical security for internal and external sources, for workstations and servers.

Audits should be a) regularly and announced or b) surprising.

a) regularly audits are well announced and all system responsible persons are alerted. If accidentally a machine crashes, the downtime shall be as short as possible. This audit should be done when the impact to customers is minimal. This could be a problem for GIAC enterprise when it serves customers world-wide with different time zones. Access statistics should be considered to find that time. I recommend this audit at least twice a year.

b) Surprising audits test the emergency plan, the information chain and the reaction time. This audit is not announced and should not be aggressive (not crashing if possible) but visible. This audit is not bound to a time. Such an audit should be done twice a year.

This audit is done for the primary firewall only. The firewall lets pass some traffic for specific ports. Therefore the machines behind the firewall have to be audited too. An audit can be outsourced e.g. [Securityspace],[Netwhistle]. I recommend having at least 2 people from the security group which can do the audit or analyse the audit and improve the security team. This no not an audit for the router, no DoS attacks are tested, we will not search for other points of entry (war-dialling), and no physical security (access control) is checked except for the UPS.

3.2 Implementing the assessment

The plan for the audit looks like:

Tasks	To Do	estimated Time (days)
1	Audit preparation	1
2	Verify the ACLs	1
3	Verify the FW and the filtering rules	1
4	Review the bastion hosts	2
5	Analysis of the result and the proposals	1

Starting date and deadlines for the audit and the report should be fixed.

3.2.1 Audit preparation

The following points are to be done before the audit of the firewall is carried out:

- Get the permission of the executives to do the audit. An audit might shutdown machines which could annoy a customer and lead to a loss of money. It could also lead to more work.
- Inform the ISP of your audit. We will access the firewall from the internal side of the router. Non-internal addresses should not pass – for absolute security we have to disconnect the router from the Internet.
- Check the security policy for consistency with physical and logical plans. Is there new equipment?
- Announce the security audit if it is not a surprise.
- Check for same time (working timeserver, correctly applied)
- Check for the working IDS
- Check for syslog (do all machine report?)
- Check the up-to-date status backup and restore functionality. (Restore a file!)
- Verify the up-to-date patch level (see [Boran_Patches], [University_of_Waterloo_Patch])

3.2.2 Verify the ACLs

The router acts as the front-end part of the firewall configuration, with its egress, ingress, and ICMP filter which where already tested in chapter 2. Check for changes.

3.2.3 Verify firewall and filtering rules

The firewall is a main defence for GIAC's network security. The audit and the management is so important that it should be managed from employees from the security group and a second opinion from an external independent enterprise should be asked for. E.g. [Firetower]. We check for the policy implementation as well as for the firewall functionality.

We plug a computer between firewall and router. Now with this machine and the IDS listening on all interfaces, we can start.

As stated in [Spitzner_Audit] the first step is to ensure the firewall itself is secure. For the NOKIA firewall operating system IPSO we get the patches.

The second step is to perform a scan for incoming and outgoing traffic for TCP, UDP, and ICMP to the firewall. For all non-administrative interfaces no ping nor the administrative ports (256-259) should be visible.

Next is the audit of the firewall rules. This should ensure that nothing passes the firewall which is not allowed. For this, the usage of [Firewall_Tester] might be a solu-

tion. Scans to all networks from all interfaces of the firewall but with the IP addresses related to the interface have to be done. For our network a scan is launched from external interface of the firewall to the Service Network and Screened Network. From Screened Network to Service Network and External Network and finally from Service Network to the External and Screened Network. Depending on timeout conditions (nmap) this could take several hours.

For NMAP scan I use these parameters but they change a little bit from version to version:

“nmap –s [F,S,U] –P0 –T Aggressive –n –p 1-65535 –v –O –oN External_internal_TCP_scan.log”

-sF: Fin scan, if fastmode scans only the SYN and not other packets[FW-1]

-sS: Syn-stealth scan, reduces traffic

-sU: UDP scan, the IDS or sniffer shows, what passed the firewall

-P0: Don’t ping

-T Aggressive: Be aggressive

-n: no DNS resolution, would produce too much traffic

-p 1-65535: Ports to scan

-v : Verbose

-O: Try to guess the OS

-oN: Normal output log file

With reporting open for open ports where the machine accepts connection, filtered if No Syn-Ack, no Rst-Ack or a dest unreachable or prohibited by admin was received and unfiltered or not shown are the machine’s ports if they are closed.

The test should be done for following source ports:

a port above 1023: To simulate a normal client. Use –g <source-port> for

port 0: Was a DOS possibility.[CVE-1999-0675]

port 20, 21: Some firewall have problem with ftp command / ftp data ports, active / passive ftp and the state-tables.

port 53: Some firewalls have this port open by default, good to scan the network topology.

port 80: For webserver.

port 161: SNMP.

port 256, 257, 258, 259 : RDP communication, with the latest SP and hotfix it is blocked by default. If it was not, it could be used to find out the network topology. [Checkpoint_RDP]
Port 264, 265: For SecuRemote access. They have to be blocked for the external Interface.

Use the perl-scripts [Firewall_Tester] to define the packets and see what really passes the firewall.

When all the checks are done, review the firewall logs, the syslog, the IDS to ensure that all attacks were detected and the alerts appeared. Learn to identify an attack.

Here a nmap scan, first the WEB SERVER, then the DNS.

Root @ scanmachine: nmap -sS -O -p 1-65535 -v -P0 -T Aggressive -n -oN HTTP_Server.txt <GIAC.Screened.Net>

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)

Initiate a SYN half-open stealth scan against GIAC_HTTP_SERVER
Host (192.168.0.0) appears to be up ... good.
Interesting ports on (GIAC_HTTP_SERVER)
(The 655033 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
443/tcp open https
TCP Sequence Prediction: Class=random positive increments

Difficulty=25042 (Worthy challenge)
Sequence numbers: ABEE6BC AC32CFE AC50E8E AC82426 ACB5DE4 ACE4256
Remote operating system guess: Sun Solaris 8

Host (GIAC_DNS_SERVER) appears to be up ... good.

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port

All 65535 scanned ports on (DNS) are: closed

Nmap run completed -- 2 IP address (2 host up) scanned in 126 seconds

Root @ scanmachine: nmap –sS -p 1-65535 -v -P0 -T Aggressive -n -oN DNS_Server.txt <GIAC.DNS.IP>

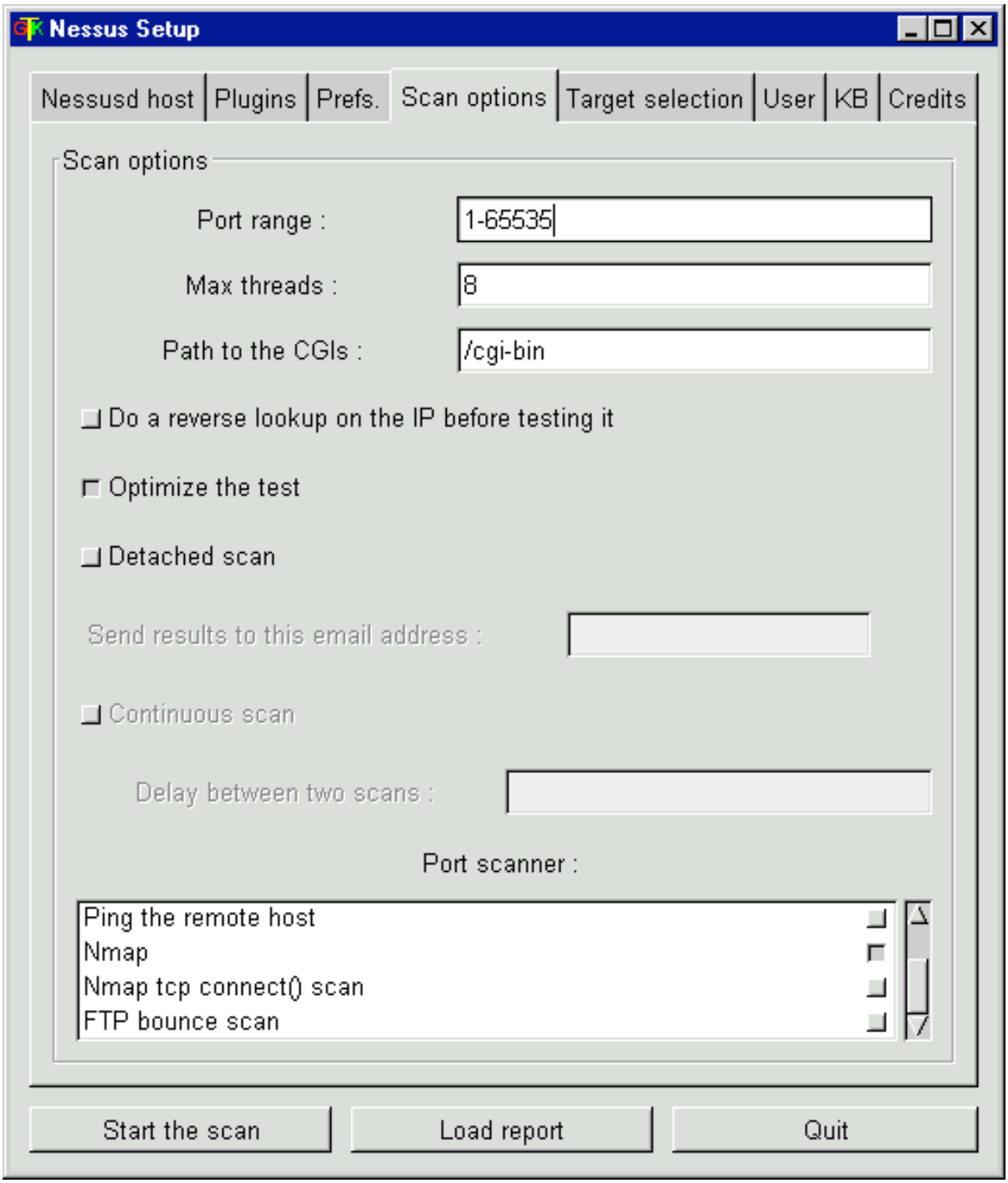
Interesting ports on (GIAC_DNS_SERVER)
(The 655034 ports scanned but not shown below are in state: closed)
Port State Service
53/udp open domain

What we expected. Use checklists as described in chapter 2 to check from all places to all machines and what you want to see compared with what you really see.

3.3 Review the bastion host

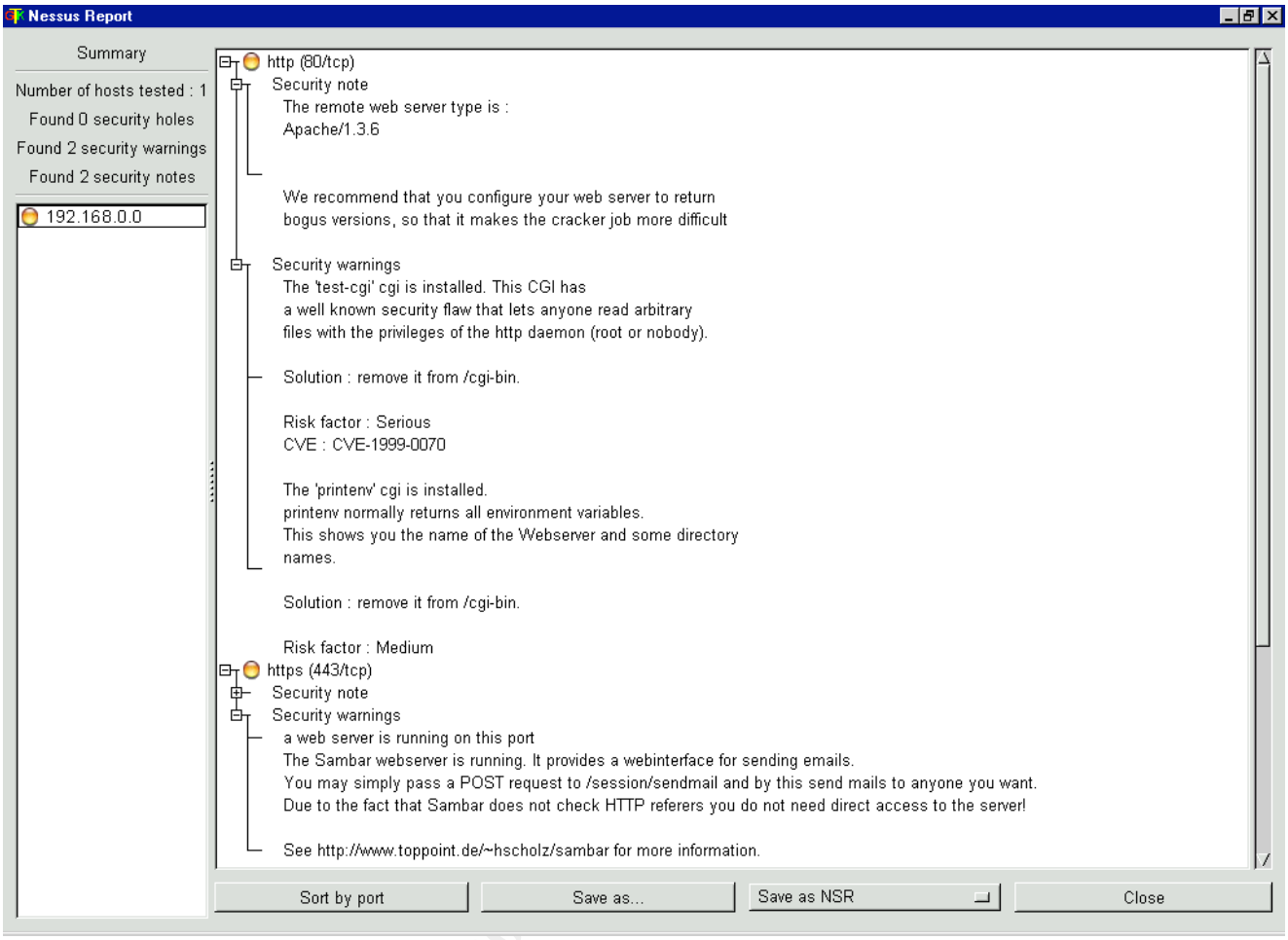
The firewall protects unneeded services and machines and with the inspection machine it adds a little bit protection to protocols the server use. But still there are possibilities to attack a server using the regular ports and protocols. Thus it is absolutely necessary to have the hosts hardened.

Vulnerability scanners help to find well known weaknesses. I prefer NESSUS [NESSUS]. I do not have to travel through the firewall; I can access the machines directly. A screenshot of Nessus' graphical interface to scan all ports looks like:



Nessus Scan Setup

The exported report for the Reverse Proxy looks like this:



Nessus Scan Report

3.4 Analysis and Report

The audit was performed on the primary firewall and against the hosts in the Screened Network. This is an extract of the results from the NMAP reports, from NESSUS output for the host scans, from the SYSLOG database and the IDS reports. The router was not included in this audit. To give a real picture of the security the audit has to be done from real outside. The test did not include DoS.

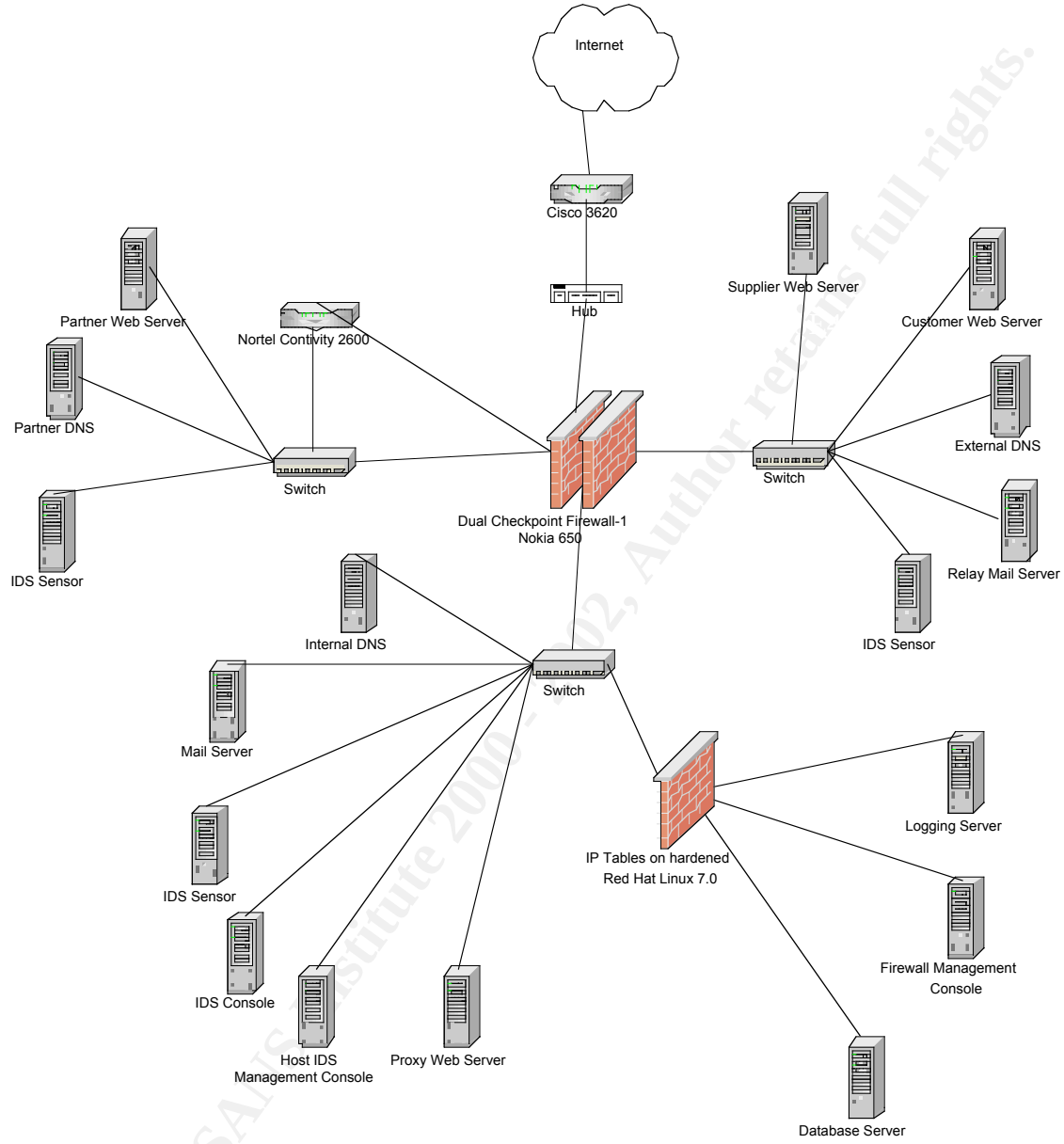
1. The UPS worked well and no data loss appeared. The batteries are all in a good state.
2. The rules on the firewall have been verified. To reduce traffic, non-open ports may already be closed at the router or an additional port filter might be installed. This adds an additional step for security but increases also the numbers of changes if a port has to be opened. The routers ACL could look like:
   # we allow the traffic we want to let pass, the FIREWALL will do NAT but we address the real addresses!!!
   access-list 101 permit tcp any host <my reverse proxy address> eq http log
   access-list 101 permit tcp any host <my reverse proxy address> eq https log
   access-list 101 permit tcp any host <my external mail1 address> eq smtp log

```
access-list 101 permit tcp any host <my external mail2 address> eq smtp log
access-list 101 permit udp any host <my external DNS1 address> eq domain log
access-list 101 permit udp any host <my external DNS2 address> eq domain log
access-list 101 permit ip any host <my external FW address>
access-list 101 deny ip any any
#
```

3. The syslog showed the scans and attacks. And it was recognised correctly.
4. The IDS showed the attacks to the different machines (HTTP, SMTP and DNS). Though it is not snort 1.8.1 it could not detect %u Unicode attacks. Upgrade even if you do not use a HTTP server supporting this kind of Unicode! You will see if an attack is made against you.
5. The host was not secured and severe security breaches were found. These vulnerabilities were found for a service which is allowed to pass the firewall. A firewall is not a magical equipment which simply protects everything – it just prevents from giving too much information and access to disallowed services. This machine is not obeying the policy and is not allowed to be accessed from Internet through the firewall as long as it is not changed. Good that the audit was done before the fortune teller service was available for the public!
6. Let an external enterprise do a regular audit.
7. Try the reactions under DoS attacks.
8. Use [Whisker] to check the CGI – disable CGI if it is not used.
9. The VPN security might be improved by not allowing the routine negotiation but a fixed routine. This depends on the laws of the partners.

4 Assignement4 – Design under Fire

I have chosen the network from Matthew P. Brown from May 2001 [Practical_Matthew_P._Brown]. The design looks like:



Design, Practical Matthew P. Brown

4.1 Reconnaissance

4.1.1 Indirect (quiet) Information collection: [Boran_Security_Cookbook].

We do not want to be detected, no attack attempt can be detected.

Use of DNS to find published information, with ‘nslookup’, ‘set type=ns’, ‘set type=mx’ for the domain.

Maybe also the info is available, with ‘set type=hinfo’.

With [Arin], [ripe] or others I find the assigned network addresses and the responsible person.

With firewalk [firewalk] I can scan the firewall. With HPING2 I can do more firewalking [Spitzner_Audit]. By using spoofed IPs I hide myself and check whether the IP stack on the spoofed machine has changed or not to find answers the victim sent out.

I search public archives for requests/answers for this domain or name.

4.1.2 Direct (noisy) Information collection:

I write an abuse message to the responsible person. Sometimes I get the message back which was forwarded several times so I get some more addresses with the feedback. If I do not get feedback, this could be a sign that the administrator is rather stressed.

For the next checks we will be visible if the firewall logs are inspected or an IDS is present. But we want to look as normal as possible.

Send a harmless looking e-mail to a probably wrong address in this enterprise. The answer could give the e-mail product and version number.

[Xprobe] is used to collect as much as possible data just by ICMP. This gently scan with slow generation of packets might not wake a IDS operator. Depending on whether ICMP is blocked or not.

Use NMAP to detect ports and OS. Probably this will appear brightly on the IDS screen. So it might be a good idea to use a free dial up connection.

If we appear in the log files lets show presence. Let’s use another machine as relay and do a Nessus/Satan/Saint/Sara scan. This gives about 80 different signatures if he uses snort.

Now we have some information. Now we wait 2 weeks just in case the are aware what is coming from my country.

4.2 Attacking the firewall

There is a Nokia 650 Checkpoint Firewall-1.

The search starts for vulnerabilities, [securityfocus][checkpoint]. The following table shows vulnerabilities which I could use.

Vulnerability	How to apply
Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability	Fixed in the latest releases. Could be worth for a try. Perl scrip on [securityfocus]
RDP Header Firewall Bypassing Vulnerability	Fixes are available. Maybe not installed?

Vulnerability	How to apply
IP Fragmentation Denial of Service	Workaround. But sysops are might be too busy to do it. The Jolt2 exploit can also be found on [securityfocus]
FireWall-1, FloodGate-1, VPN-1 Table Saturation Denial of Service Vulnerability	Dos. “nmap -sP GIAC.*.*.*“
SMTP Security Server Denial of Service	Here too, hotfix might not be installed. Try with netcat [netcat] “nc firewall 25 < /dev/zero”.

If the firewall is too hard to attack, we try to crack an internal server and attack the firewall from internal. Maybe we can sniff passwords, crack passwords which might be reused on other machines and maybe the rules are not as tight for internal machines. If the service on a machine has some vulnerabilities this might be easier than trying the firewall!

4.3 Denial of Service

Massive TCP SYN, UDP, or ICMP floods from 50 compromised cable modem /DSL systems. What could be done to reduce the effect of the flood? The theoretical bandwidth with 256kbit/s each: ~10 Mbit/s.

1. Don’t let them come into your network. Your ISP might provide a service for bandwidth regulation. Then the flood won’t come to your router. If all providers would use egress filters, this would help against spoofing.
2. Have more bandwidth than the attacker. This won’t work since we do not know what potential the attacker has. Then it is too expensive to reserve large bandwidth just for this case.
3. Do not allow the flood to reach single machines, block unused protocols and ports as soon as possible, at the border router or firewall. For SYN flood, Firewall-1, SYNDefender Gateway, IPCHAINS/IPTABLES with tcp_Syncookies. Cookies require not memory but calculation power for the CRC calculation, so the CPU must be powerful enough. If the firewall is configured as a semi-transparent gateway, letting the connection pass if a valid ack was returned, the firewall time-out has to be set carefully!
   Use ingress and egress filter. This avoids to be attacked from internal systems by an external attacker using spoofed internal IPs. This helps to keep your network working internally but the Internet is still not reachable.
   This does not help at all for attacks against an open service port e.g. TCP for e-mail or http, UDP for the DNS service.

4. Use local firewalls on machines, which can be accessed from the Internet. Send Reset back to TCP flooder and drop UDP/ICMP flooder. The machines have to process the incoming data faster than the network can deliver.
5. Exposed machines need enough memory to provide large amounts of protected kernel memory. Then the connection would just slow down. In attacks where the ACK is sent (the handshake is done,) this could be essential. [Naphta].
6. Decrease the timeout value for a connection. Resources are freed quicker; the backlog is free for new connections. [SANS_SYN_FLOOD]
   For Solaris do kernel tuning with ndd [Sean], for Solaris 8 [SUN_tune].
   Decrease the windows size for the response timeout:
   "ndd –set /dev/tcp tcp_xmit_hiwat 16384"
   "ndd –set /dev/tcp tcp_recv_hiwat 24576"
   Enlarge the socket queue against the syn attack:
   "ndd –set /dev/tcp tcp_conn_req_max_q 1024"
   And for the socket waiting with half open:
   "ndd –set /dev/tcp tcp_conn_req_max_q0 4096"
   Modify the TIME_WAIT for a busy web server:
   "ndd –set /dev/tcp tcp_time_wait_interval 60000"
   Reduce the timeout to minimise the effect of false IP table entries (1 minute).
   "ndd –set /dev/ip ip_ire_arp_interval 60000"
7. Load balancing: The throughput is divided by many machines, the Internal Network will not go down. Have several Internet access points. Use a bandwidth regulation device where you can address the maximum throughput for an IP.
8. Disable broadcast amplification.
9. Use the IDS to detect DoS attacks (e.g. Snort can detect Naphta). Carry out a reaction, e.g. block the address for a certain time. The threshold is to be chosen carefully.

It is not a good idea to react automatically, e.g. for SYN flood by sending RST to the sender. The IP was probably spoofed.

A distributed denial of service (flooding) attack is very hard, maybe impossible to block totally. And all protection methods are costly. But with the possibilities above, a successful attack is harder to do which might give the administrator more time to react.

4.4 Attacking an internal system

The reconnaissance showed the external DNS running BIND with a version for which [Bind], [Cert] and bugtraq [securityfocus] did not show any exploitable vulnerabilities. I would like to own a central system, the firewall would be great but they are not so easy to crack. Normally I have success with a DNS – but here the version is up-to-

date. So I have the possibility to attack the Customer Web Server or the Relay E-Mail Server. It looks like the Web Server is an Apache 1.3.12 on a RED HAT Linux 7.0. Possible attacks I want to try are [bugtraq id 3009], [bugtraq id 2503], and [bugtraq id 2003] were I can download the perl scripts or use the URL-attack as explained. I can use this to collect information, read directories. Maybe I get some passwords.

I am quiet sure that there is an IDS in this network. Maybe I can blind the system. If it saves the attack under a directory name or into a file named with the IP address and stores the file for an analysis once a day, I can do a DoS attack. For this I wait for Friday evening because I speculate that the logs are not scanned until Monday. I attack with more than 64.000 spoofed IP addresses a lot of fragmented small packets – I am sure these are being logged.
I use [HPING] with the command, in a script generating random spoofed addresses:
“hping2 –a <spoofed address> -f –d 70 –p 80 <IP of the WEBSERVER>”
-a <spoofed address>: Use this spoofed address as a source address
-f : fragment the packets
-d : the size of the packets is 70 Bytes plus the header(s)
-p : The destination port, 80 for the webserver
“hping2 –2 –a <spoofed address> -f –d 70 –p 53 <IP of the DNSSERVER>”
-2 : for UDP usage

If the machine is a Linux or Solaris then the maximum file number per directory is 32.000 or 64.000. If it is filled, the System can not add another file or directory.
I let run a vulnerability scanner from other machines I own, e.g. SATAN or my favourite, NESSUS for every attack on port 80. This makes the IDS analyst’s life hard. I know, the analyst will see that there was an attack but I can hide in the crowd. And this makes it hard to know anything about the success. Even if he had installed a file checking program like tripwire or aide. Will he trust them? Coming Monday there is work waiting for him.

I am sure, I was logged. And the amount of data I could get was (almost) nothing, very disappointing. So at least I made the people work there. I’ll look for an easier attack point……..

5 References and Links:

[admin_cracking_guide]: http://www.fish.com/security/admin-guide-to-cracking.html
[aide]: http://www.cs.tut.fi/~rammer/aide.html
[Arin]: http://www.arin.net/whois/index.html

[Bind]: http://www.isc.org/products/BIND/bind-security.html
[Boran]: http://www.boran.com/security/sp/
[Boran_Patches]:
http://www.boran.com/security/sp/Solaris_hardening4.html#Patches
[Boran_Security_Cookbook]: Chapter Firewall, Penetration testing
[bugtraq id 2003]:
http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D2003
[bugtraq id 2503]:
http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D2503
[bugtraq id 3009]:
http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D3009

[Checkpoint]: http://www.checkpoint.com/techsupport/alerts/
[Checkpoint_RDP]: http://www.checkpoint.com/techsupport/alerts/rdp.html
[Checkpoint_FM]: http://www.checkpoint.com/techsupport/alerts/fastmode.html
[Checkpoint RDP Bypass]:]: http://www.cert.org/advisories/CA-2001-17.html
[CISCO_12]: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/
[Cert]: http://www.cert.org/
[CERT_CISCO_HTTP]: http://www.cert.org/advisories/CA-2001-14.html
[CERT_CISCO_HTTP]: http://www.kb.cert.org/vuls/id/812515
[CISCO_Perimeter_Security]:
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm
[CISCO_Security_Improve]: http://www.cisco.com/warp/public/707/21.html
[CVE-1999-0675]: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0675

[ETHEREAL]: http://www.ethereal.com/

[firewalk] : http://www.packetfactory.net/firewalk/
[Firewall_piercing]: http://www.linuxdoc.org/HOWTO/mini/Firewall-Piercing.html
[Firewall_Tester]: http://sole.infis.univ.trieste.it/~lcars/ftester/
[Firetower]: http://www.firetower.com/demand.html
[FW-1]: http://www.dataprotect.com/bh2000/blackhat-fw1.html

[Hide_n_Seek]:]http://www.fish.com/security/hide-n-seek.html
[Hping2]: http://www.hping.org/

[Integralis_ACE]:
http://www.integralis.ch/products_services/authentication/rsa_ace.php
[Integralis_ID]:

http://www.integralis.ch/products_services/authentication/rsa_secure.php

[Naphta]: http://razor.bindview.com/publish/advisories/adv_NAPTHA.html
[Netcat]: http://www.atstake.com/research/tools/index.html
[Netwhistle]: http://www.netwhistle.com
[NESSUS]: http://www.nessus.org/
[NMAP]: http://www.insecure.org/nmap/
[NMAPFE]: http://www.insecure.org/nmap/nmap_relatedprojects.html

[Packeteer]: http://www.packeteer.com/products/packetshaper/
[PhoneBoy_FW1]: http://www.phoneboy.com/
[PhoneBoy_BH]: http://www.phoneboy.com/docs/bh2000/blackhat-fw1.html
[Practical_Matthew_P._Brown]:
http://www.sans.org/y2k/practical/Matthew_Brown_GCFW.zip

[RFC 1918]: http://www.ietf.org/rfc/rfc1918.txt
[ripe]: http://www.ripe.net/perl/whois

[SANS_router]: http://www.sans.org/infosecFAQ/firewall/router.htm
[SANS_SYN_FLOOD] : http://www.sans.org/infosecFAQ/threats/SYN_flood.htm
[Sean]: http://www.sean.de/Solaris/tune.html
[securityfocus] :http://www.securityfocus.com/
[SecurePoint_FW1]: http://msgs.securepoint.com/fw1/
[Securityspace]: http://www.securityspace.com
[Spitzner_IDS]: http://www.enteract.com/~lspitz/ids.html
[Spitzner_Solaris]: http://www.enteract.com/~lspitz/pubs.html
[Spitzner_Rules]: http://www.enteract.com/~lspitz/rules.html
[Spitzner_Audit]: http://www.enteract.com/~lspitz/audit.html
[Spitzner_FW1]: http://www.enteract.com/~lspitz/fwtable.html
[Spitzner_Router]: http://www.enteract.com/~lspitz/routing.html
[SSH_Cygwin]: http://www.cygwin.com/
[SSH_Cygwin_Install]: http://tech.erdelynet.com/cygwin.asp
[SSL_SUPPORT]: http://www.netcraft.com/sslwhats/
[Stunnel]: http://stunnel.mirt.net/
[SUN_Tune]: http://docs.sun.com/ab2/coll.709.2/SOLTUNEPARAMREF/

[Tannenbaum]: Kapitel 5.2.5.2 Split Horizon Hack (S.388), "Computernetzwerke", Tanenbaum 1998 (3. Aufl.)
[Tcpdump] : http://www.tcpdump.org/
[tripwire]: http://www.tripwire.com/

[University_of_Waterloo_Patch]: http://ist.uwaterloo.ca/security/howto/2000-12-04/

[Whisker]: http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2

[Xprobe]: http://www.sys-security.com/html/projects/X.html