Global Information Assurance Certification Paper

John Jenkinson

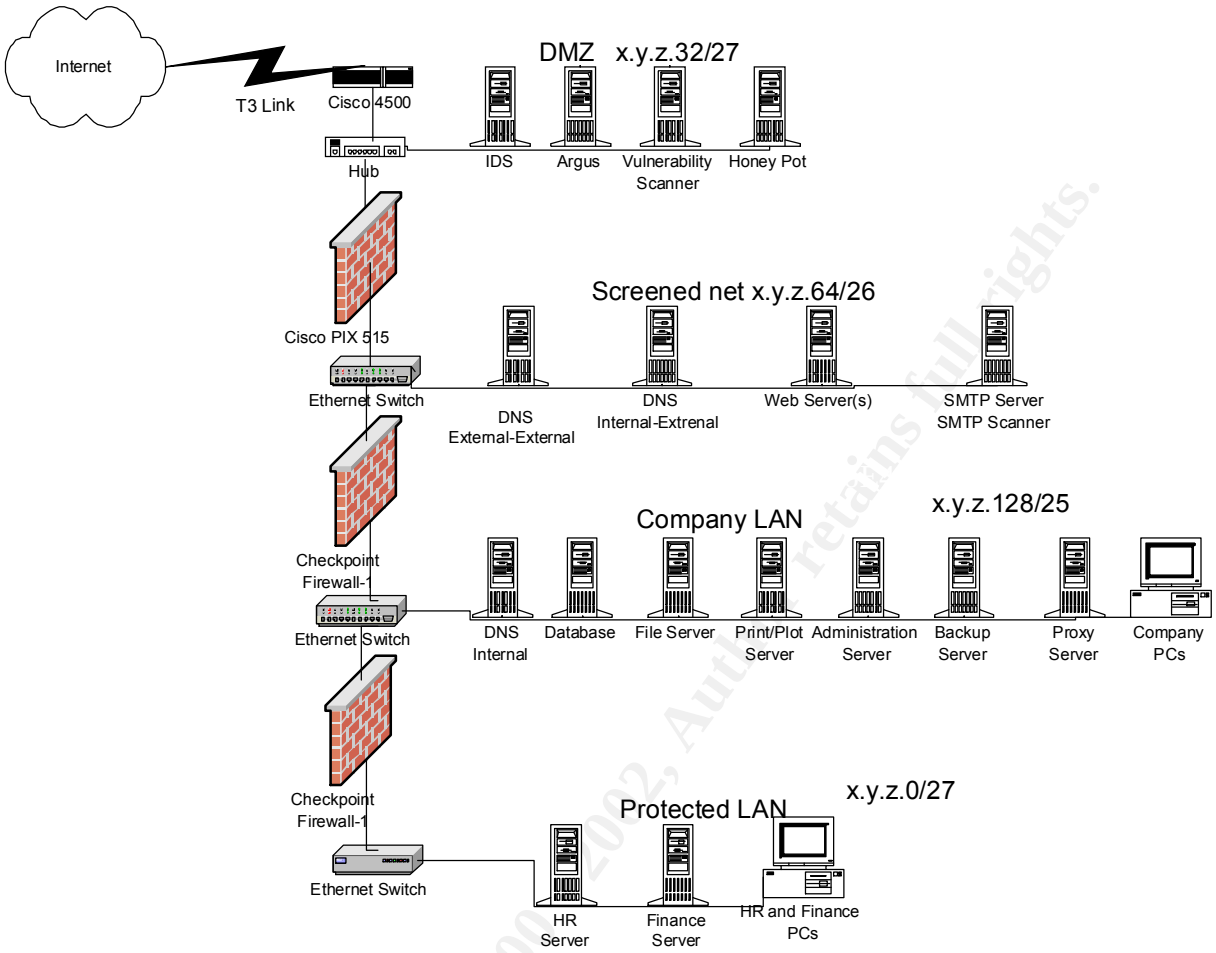
LevelTwo Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5

Assignment 1 - Security Architecture (25 Points)
Define a security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition.
Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.
You must consider and define access for:
- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component.

Some specifics missing from the assignment text that will make a real difference in the depth and scope of the security architecture include:
Is the $200million per year gross or net? i.e., what can we spend?
What is the anticipated traffic volume to and from customers? Suppliers? Partners?
Is the recent merger/acquisition a capital boon or drain to GIAC Enterprises?

Real world thinking would have this Internet startup use a Web hosting service initially, though not one in California. This would get the business going quickly, allow most of the infrastructure cost be expensed instead of using capital money, and give the business an idea of traffic volumes and patterns. Using a web hosting service would also get technical expertise to the business quickly and allow GIAC Enterprises to then bring in-house the functions that suit the business plan and the company's growth. Many other factors given or not given in the assignment suggest web hosting and third party provider care, but not a good response for a practical assignment. These factors do indicate the security architecture should be on the capital conservative lean, but the architecture should allow for growth, as the company could be the next Internet wonder-site.
Security should be strong as the company's assets are fortune cookie sayings and probably not copyright protected. Thus theft from a break-in would mean probably total loss of those assets with very little chance of legal recourse.



GIAC Enterprises

Multiple firewalls would ma keup the architecture in a growth scenario. These firewalls would be from multiple vendors to account for the potential of a compromise in one vendor's offering not allowing the compromise of the internal systems. Firewalls don't work in isolation so we'l lpair the outermost firewall, VPN, and router from Cisco. This places the higher performance firewall at the higher traffic point. The middle firewall will be from Checkpoint as will the innermost firewall. This allows the firewalls most likely to be cha nged and having the larger rule set to be from the vendor that seems to have the better user interface and the larger pool of experience available for technical staff recruiting. We also gain the capability of managing multiple rule sets from a single man agement point. We could further specify one Checkpoint firewall would run on Solaris and the other on AIX to provide the same type of protection from an operating system vulnerability. Cisco was chosen for the VPN due to desired placement and the support in PIX of VPN. We can also upgrade the PIX firewall to one that has hardware acceleration capabilities like the PIX 535.

The LAN segments will be 100Mbit switched Ethernet. Customers won't revisit if they have to wait and 100Mbit switched gear is almost com modity now.

The Internet connection speed will depend on the traffic volume estimate and the location of GIAC Enterprises. This will then dictate the Cisco router configuration. Lets assume a T3 Internet connection and Cisco 7500 series. As Internet volume grows an additional T3 from another provider can be added. The premium router allows more growth, extended

ACLs to provide bandwidth allocations and filtering on destination addresses, and good resale value if the business fails.
We also have the proce ssor power to implement Context Based Access Control to add more to defense in depth once we characterise our traffic.
Assume we have a full class C network assignment irrespective of the acquisition/merger. We will need subnets for the DMZ, Screened Netwo rk, the company LAN and the protected or inner LAN (HR, Finance, etc.) While 63 addresses per subnet is probably enough, we can use variable Length Subnet Masking (VLSM) to take from the more limited potential address segments to give to the more probable growth subnets. Using x.y.z as our network address we could use:

Segment/Subnet	Network/Subnet	Number of hosts	Subnet Mask
Inner LAN	x.y.z.0/27	30	255.255.255.224
DMZ	x.y.z.32/27	30	255.255.255.224
Screened	x.y.z.64/26	62	255.255.255.192
Company LAN	x.y.z.128/25	126	255.255.255.128

We will use split-split DNS with a secondary for the external -external at a service provider for the addresses in the DMZ and the screened network. Split -Split DNS means we have internal DNS server for the inter nal network, and two DNS servers in the screened network. One resolves external addresses for the internal users, and one resolves external addresses (i.e. those in the screened network) for external (Internet) users. This to prevent DNS cache poisoning.

The DMZ subnet will have nodes that provide IDS (intrusion detection), Argus server (for forensic evidence), a means of vulnerability or port scanning from beyond the outer firewall, and the potential for a Honey Pot. These could all be on a few nodes with addresses a liased to the appropriate NIC card. The IDS and Argus NIC would be set -up read-only i.e. receive packets from the probe points via switch in hub mode
.
The screened subnet will have DNS servers, the WEB servers, and the email gateway. Again th ese services can share servers initially and go to separate servers as the company grows.

The company LAN will have backup server, syslog servers, administrative server, database server, the web development and source for a periodic push to the web serve rs in the screened network, and whatever else the business requires as it grows.

The protected LAN will have nodes for HR, financial, and whatever else the business needs to be on a segment with additional protection from the main company LAN

Assignment 2 - Security Policy (25 Points)

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

Border Router
Primary Firewall
VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

Before addressing the specifics of the border router, the firewalls, and the VPN the general aspects of the security policy will be mentioned.

Policies and procedures will be documented and periodically reviewed. Any and all changes will use change control that will reference the appropriate policy and/or procedure.

Security and system administrators will be trained and certified. They will also subscribe relevant security newsgroups and monitor security related sites (SANS, etc.)

The company will use a digital PBX, asynchronous serial ports will be disabled, war dialling will scan for modems in the company's phone number range, an external FAX service will be used, and a bounty will be paid to the employee reporting a modem connection or any other security policy breach.

System integrity checkers will be run twice daily. Systems will be built and monitored with cfengine to conform to the system settings that provide the most hardened system for the vendor platform. This will include issues like minimal services enabled, file owner and permissions, routing tables, etc. The executables for disabled services will be removed or renamed.

Secure Shell will be the method of Telnet-like machine access, Xwindows access, the r-commands, and file copying.

Patches will be kept up to date via a subscription to a vulnerability alerting service. New OS releases will be applied as soon as practical based on application verification, new function, and security improvement.

Virus scans will be conducted on the appropriate platforms, as will scans for Trojans, DDOS tools and other malware. A subscription and update service will be used from the virus vendor

Incoming and outgoing email will be scanned for viruses and other malware signatures.

Syslogs will be captured to a VAX machine, those logs monitored by a process designed to look for suspicious activity, and that activity forwarded to appropriate roles in the company via pager or near-realtime alerting system. These alerts will go to one or more technical security employee and at least one technical manager.

That VAX machine will also control, monitor, and log all console access to every machine with a command line console.

TCPWrappers will be configured and used for all TCP services on the appropriate machines.

IPSec filtering will be configured and used on the appropriate machines
SSL will be used for transactions on the WEB servers.
DNS names will not indicate the machines function except f or the nodes in the screened subnet
Firewall rulesets will conform to a "allow known, deny otherwise" policy
Personal or local host firewalls will be used and those will watch and warn for traffic in and out of the machine.
IT auditing will be done by an e xternal firm twice a year, by internal auditor 4 times a year.
All users will have an account and use only that account to provide accountability. All users will authenticate with the strongest method available.
Password policy will be clear, signed by t he user, and password compliance checked at random intervals.
Machines will be allowed access to applications, data, and users consistent with their function.
Data of any sensitivity will be encrypted and access audited.
Individual Ethernet switches will t ake priority over VLAN configurations where possible.
External use applications and services (DNS, HTTP servers, SSH, SMTP, etc.) will be the latest version possible and will be configured using best practices from the Internet security community.
Privacy policy will be predominately displayed on the company's Web site pages that customers, partners, and suppliers visit. That privacy policy will be acknowledged and adhered to by all employees and partners.
Administrator and root passwords will use stronger authentication via RSA SmartCards or other methods of identifying the individual administrator.
Machines for administration of the company's machines, network, and media robots will be more physically secured.
Sessions to the infrastructure for administrat ion changes will be logged and archived
Backup and archive tapes will be strong encrypted and a copy stored offsite and transported there by secure means.
SMTP server will have message relaying turned off
VPN access requests will require signing an agreeme nt to connect to the company's VPN security gateway. This agreement will detail the company's security policy regarding such connections, the company's privacy policy, and detail the minimum security and privacy standards the connecting VPN party should im plement on the VPN client.

Border Router
We will do most of the filtering at the firewalls, so the border router mostly routes. Thus our router set -up will:

Block company's address range as source inbound
Block private addresses and loopback network (12 7.0.0.x) addresses inbound

```
IP access-list standard INBOUND
      deny 10.0.0.0      0.255.255.255 log
      deny 172.16.0.0    0.15.255.255  log
      deny 192.168.0.0  0.0.255.255   log
      deny 127.0.0.0     0.255.255.255 log
      deny x.y.z.0       0.0.0.255     log
      permit any
```

Block source routed packets inbound

```
router# config t
router(config)# no ip source -route
```

Block non-local addresses outbound

```
IP access-list standard OUTBOUND
      permit x.y.z.0     0.0.0.255
      deny any                          log
```

now apply to the interface

```
router# config t
router (config)#  int s0
router (config-if) # ip access-group INBOUND in
router (config-if) # ip access-group OUTBOUND out
```

Turn on logging and specify syslog destination

```
router# logging on
router# logging x.y.z.a
router# logging trap debug
router# logging console emergenc ies

Now some security to the router set -up
```
Set password
```
router# login
router# password <hard to crack password>
```
Turnoff directed broadcasts (prevents layer 3 to 2 broadcast mapping and smurfs)
```
router# no ip directed -broadcasts
Encrypt service password
router# service password -encryption
```
Disable vulnerable and unneeded services
```
router# no ip http server
router# no ip bootp server
Change snmp community names and limit snmp access to the administration machine
router# snmp -server community <name> RO 21
router# snmp-server community <name> RW 21
router# access -list 21 permit x.y.z.a
```
Add warning banner
```
router# banner \No unauthorised access permitted \
don't respond to echo, chargen, finger, etc.
router# no service udp -small-servers
router# no service tcp -small-servers
router# no service pad
```

Other possible filtering is deferred to the outermost firewall.

Firewalls

Here we want to do most of the filtering and logging. We will control access to and from the screened network and allow other necessary and required traffic from the company LAN and the protected LAN.

The **border router** will be console controlled by the VAX console system and syslog (UDP port 514) to the syslog sever on the company LAN.

The **SMTP server** can connect SMTP (TCP port 25) to the Internet, to the web servers, the company LAN, and the protected LAN. We will allow POP3 (TCP port 110) from the company LAN and the protected LAN. We also allow and encourage the use of PGP. We will also need access to DNS (UDP port 53) on all 3 DNS servers, syslog a ccess to the syslog server and backup to the backup server.

The **external-external DNS server** can accept DNS (UDP port 53) from the Internet, from the SMTP server, the Web server, and the admin server. The server can also zone transfer (TCP port 53) to the secondary at the ISP provider.

The **internal-external DNS server** can accept DNS (UDP port 53) from the company LAN, from the protected LAN, and the SMTP server.

The **internal-internal DNS server** can send DNS (UDP port 53) to the internal -external DNS server .

All **three DNS servers** can send syslog (UDP port 514) to the syslog server and allow backup to the backup server. Console access for maintaining the DNS zone files is via the console server.

The **Web server(s)** accept HTTP (TCP port 80) and HTTPS (TCP port 443) from the Internet, from the company LAN, and from the protected LAN. Console administration is done via the console server, but SSH (TCP port 22) from the company LAN Web development server for maintenance and a scheduled push of the current Web serve r content to overwrite any tampering and provide consistency. The copies are done via scp. The web server(s) access the company database server(s) on TCP port 3306. Web servers also can access the Internal -External and External -External DNS servers (UDP p ort 53), the company syslog server (UDP port 514) as well as backup to the backup server.

The **VPN server** accesses the Internet with IPSec. It is possible that VPN clients will also need access to the company database server via SQL (TCP port 3306). It is i ntended that all partner and client connections to VPN will have their needed services on the screened subnet.

The **database server** accepts MySQL (TCP port 3306) from the VPN servers, the company LAN, and the Web server(s).

The **database server** also is allow ed connections to the backup server and the syslog server. Console access to the database server is via the console server. The database server will have individual accounts for company employees that

require access. That access will be read -only unless the employee requires read -write for their job function. Partner access to the database will also be by individual account on both the database server and the VPN server. Authentication will be required on both servers.
The **Backup server** will access all nodes on the protected LAN, the company LAN, and the screened network. Backup of the nodes in the DMZ will be done via console access to a local removable media that is removed from the machine as soon as the backup task is done.
The rest of the **company LAN** accepts no connection from the Internet nor DMZ. The company LAN nodes are allowed
HTTP, HTTPS, SMTP, POP3 and DNS to the screened network and to the Internet via the proxy server.
The **proxy server** accepts connections from the company LAN and the protected LAN to access the Internet. No unsolicited connections are accepted from the Internet
The **protected LAN** can connect to the screened network and the proxy server for Internet access on HTTP, HTTPS, SMTP, POP3 and DNS.
The only connection allowed to the protected LAN is the port to the backup server on the company LAN.
We then deny everything else.

```
For the PIX 515 firewall:
!set security levels
nameif ethernet0 outside security0
nameif ethernet1 screened  security10
!define interfaces and force speed/duplex
interface ethernet0 100Full
interface ethernet1 100Full
!assign IP addresses
ip address outside x.y.z.o 255.255.255.255
ip address screened  x.y.z.64 255.255.255.192
!setup to perform protocol security checks
fixup protocol ftp 21
fixup protocol http 80
fixup protocol https 443
fixup protocol smtp 25
!don't NAT
nat (inside) 0.0.0.0 0.0.0.0
!for border router  - must be passed by next firewall as well
static (screened, outside)x.y.z.o netmask 255.255.255.255 0 0
conduit permit udp host x.y.z.j netmask 255.25  5.255.255 0 0
!for web server
static (screened, outside) x.y.z.e netmask 255.255.255.255 0 0
conduit permit tcp host x.y.z.e eq http any
conduit permit tcp host x.y.z.e eq 443 any
!for smtp server
static (screened, outside) x.y.z.f netmask 255.255.255.255    0 0
conduit permit tcp x.y.z.d smtp any
!for external -external DNS server
static (screened,outside) x.y.z.h netmask 255.255.255.255 0 0
conduit permit tcp x.y.z.d eq 53 any
conduit permit udp x.y.z.d eq 53 any
!for internal -external DNS server
static (scre ened,outside) x.y.z.i netmask 255.255.255 0 0
conduit permit udp x.y.z.i eq 53 any
!allow IPSec
sysopt connection permit -ipsec
!setup logging
logging on
logging host z.y.z.j
logging facility 20
!disable rip
no rip outside passive
no rip screened passive
no rip outside default
no rip screened default
!set outside default route to the border router
```

```
route outside 0.0.0.0 x.y.z.o 1
```

We don't specify a explicit deny all as PIX has this as default, only specified access is granted, all other is denied.

For the VPN service using the PIX firewall as the VPN Security gateway, we can connect to VPN hosts or other VPN Security gateways. Also placing the VPN at this entry point into the company we gain the protection of the two other firewalls for the internal nodes. Since the screened network is the trusted network to the VPN security gateway we need the services needed by remote employees, the company partners, customers, and the company suppliers to be available on the screened network. With PIX the crypto map entri es are searched in order (first fit) and the entries specify using IPSec or not, so the access/deny to IP addresses or address ranges must be done in the firewall ruleset. As Cisco's PIX implementation allows for both AH (Authentication Header) and ESP (En capsulating Security Payload) we can setup Transform Sets to best suit the connection. AH can be used to connect where DES may not be available (we should need access to China for fortune cookie sayings). Also salesmen on the road may need authentication a nd data encryption when sending in orders, but not so when they're just checking their schedules.
As our methods should be following the culture whence our fortunes came, we'll use SHA (stronger, but slower) over MD5 for authentication. We'll start out not using a CA (Certificate Authority) but can add that capability later. While we can do ad-hoc manual entries to our crypto map, we want to encourage IKE or pre-shared keys for out VPN peer initiated connections.
The recommended order to configure Cisco PIX VPN is IKE, IPSec, IKE Extended Authentication (for user authentication for peer VPN clients), then IKE Mode
(for dynamic IP addressing i.e. the mobile sales force).
IKE as a protocol adds ease of configuration as well as flexibility and features to IPSec . Both Oakley and Skeme key exchanges, lifetime on IPSec security associations, anti-replay, etc. make IKE defined IPSec configurations easier to setup and maintain. But, this requires an IKE policy at both peers. If the partner/customer/supplier has an IKE policy already defined, we can obtain, vet, and then add that IKE policy. If not, we can supply them one of our IKE policies. We would choose the one most closely matching the attributes of the new VPN client.
Multiple IKE policies can be specified for a peer for those VPN connections from
peers that have varying levels of security requirements such as data encryption.
There are 5 components of an IKE policy; the encryption algorithm, the hash algorithm, the authentication method, Diffe-Hellman group iden tifier, and the security association's lifetime. On connection the attempt to find a matching policy starts with the highest priority till a match is found (first match).
Thus our IKE policies will have the more restrictive settings for these components i n the higher priority IKE policies. Given most of the components have only two choices for component values, these policy creations are the balance between speed and security. The lowest priority IKE policy is the VPN vendor supplied default policy.

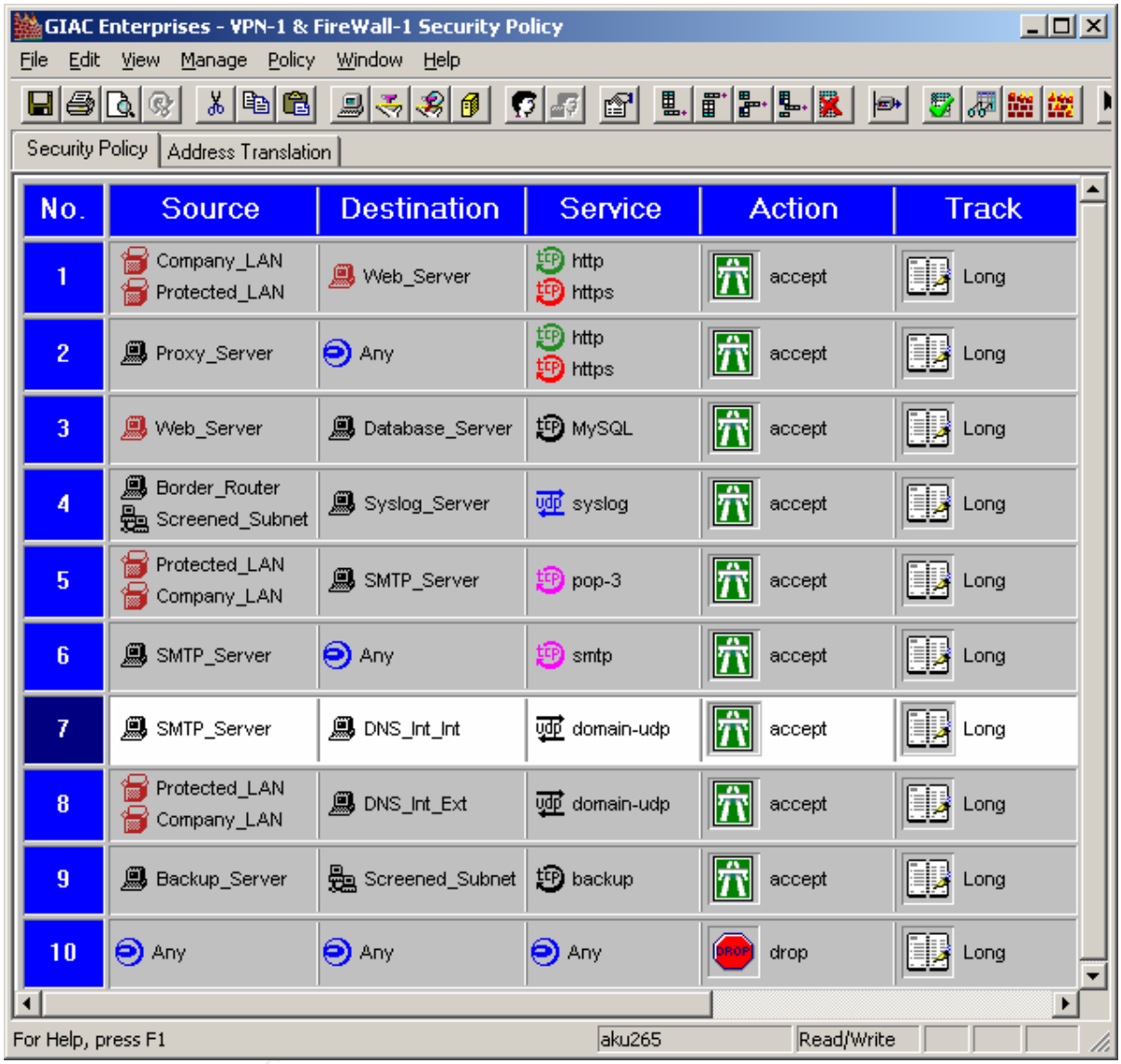
Component	**Possible Values**	**keyword**
Encryption Algorithm	56-bit DEC-CBS *	des
	168-bit Triple DEC	3des
Hash Algorithm	SHA-1 *	sha
	MD5	md5
Authentication	RSA Signatures *	rsa-sig
Method	pre-shared keys	pre-share
Diffie-Hellman	768-bit *	1
Group Identifier	1024-bit	2
Security Association	any number of seconds	-
Lifetime		

where * specifies the default value
NOTE: The lifetime does not have to match
ALSO NOTE: setting up of either authentication method requires steps for that component as well.

```
!turn on debugging  - useful during initial setup
debug crypto isakmp
!enable IKE on interface(s) to evaluate IPSec traffic
isakmp enable ethernet0
isakmp enable ethernet1
!for this example define a priority of 15 (15 also becomes the identifier o   f
!this policy)
isakmp policy 15
```

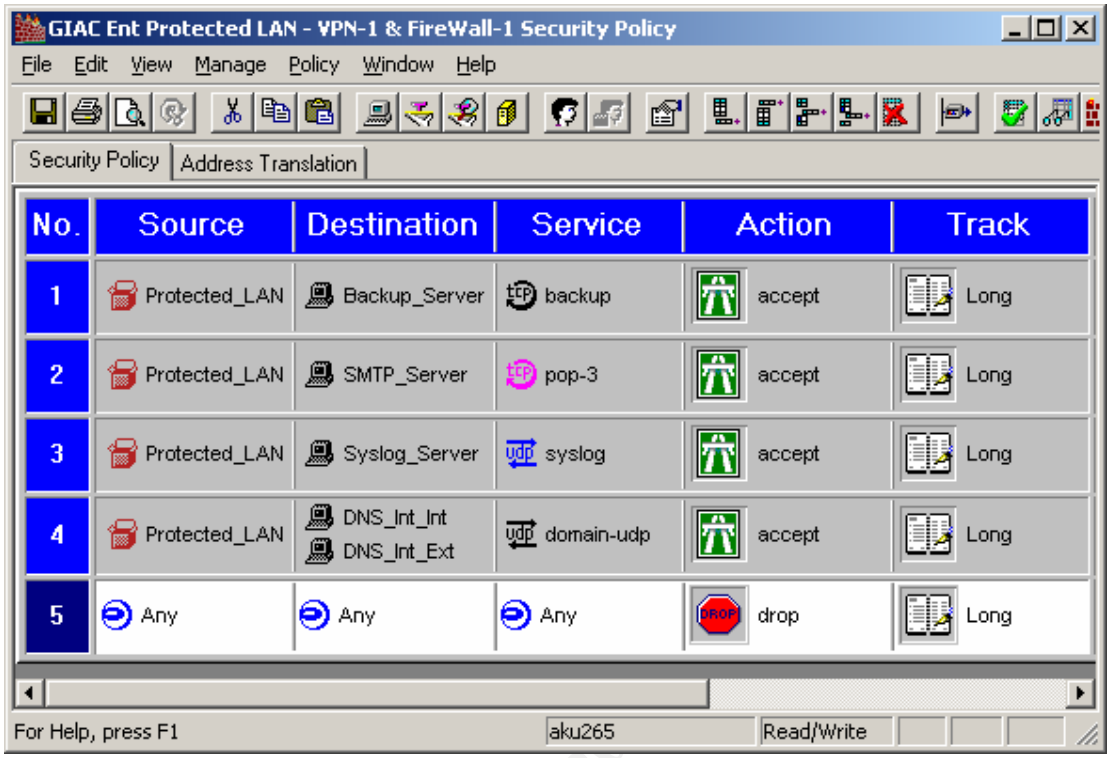
```
isakmp policy 15 encryption 3des
isakmp policy 15 hash md5
isakmp policy 15 authentication pre -share
isakmp policy 15 group2
isakmp policy 15 lifetime 86400
For the pre-shared key, defining one generated key per address or   network
isakmp key <key-string> address <peer-address> netmask <netmask>
Next in order will be configuring IPSec
!turn on debugging for initial setup
debug crypto ipsec
!make the access list
access-list 107 permit ip <src-addr> <src netmask> <dest-addr> <dest netmask>
!the transform set (to be placed in the crypto map entry)
crypto ipsec transform-set set1 esp-des esp-sha-hmac
!create the crypto map entry with a priority of 10
crypto map map10 10 ipsec-isakmp
!assign an access list
crypto map map10 match ad dress 107
!specify the peer to which IPSec traffic will be forwarded
crypto map map10 107 set peer <dest -addr>
!the transform set(s) in priority order
crypto map map10 107 set transform -set set1 set2 set3
!security association lifetime
crypto map map10 107  set security association lifetime 86400
Now extended authorization
!the AAA-server group-tag interface host server -ip key
aaa-server TACACS+ (ethernet1) host <server -ip> <key value>
!enable
crypto map map10 client authentication TACACS+
!for pre-shared ke y
isakmp key <key string> address <ip address> netmask <netmask> no   -xauth
```

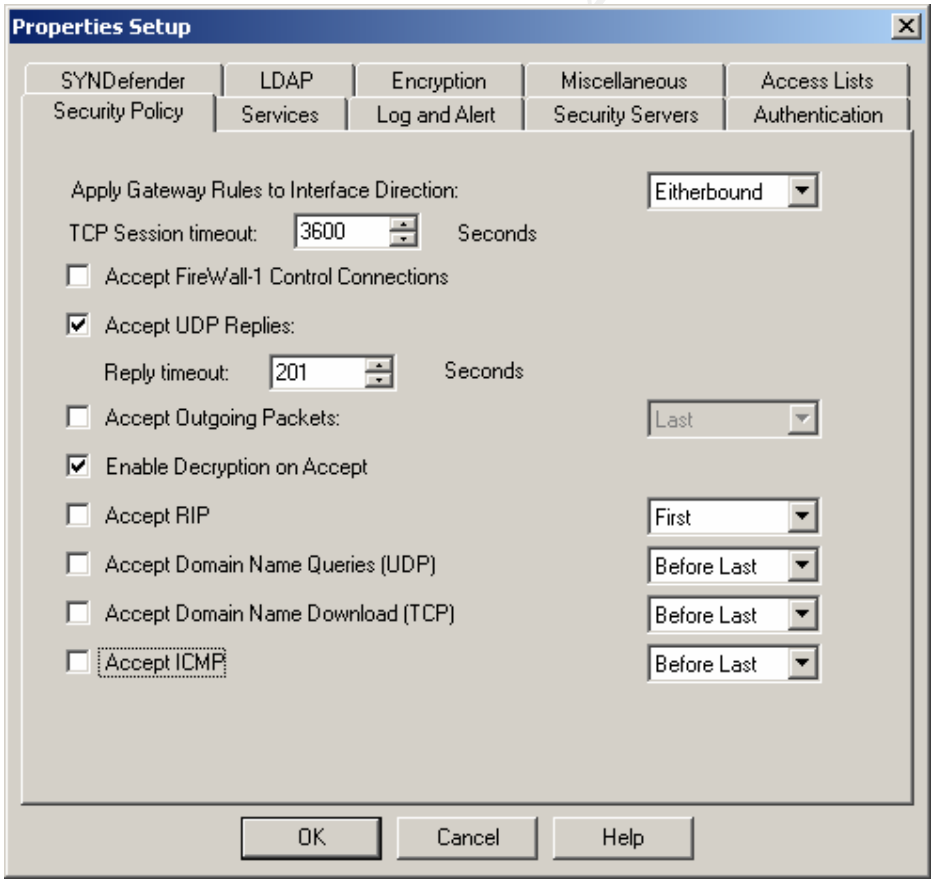
The Checkpoint firewall configurations are now given. First the one between the screened subnet and the company LAN. This is Firewa11 -1 Version 4.1 SP 2 on Solaris 8



No.	Source	Destination	Service	Action	Track
1	Company_LAN Protected_LAN	Web_Server	http https	accept	Long
2	Proxy_Server	Any	http https	accept	Long
3	Web_Server	Database_Server	MySQL	accept	Long
4	Border_Router Screened_Subnet	Syslog_Server	syslog	accept	Long
5	Protected_LAN Company_LAN	SMTP_Server	pop-3	accept	Long
6	SMTP_Server	Any	smtp	accept	Long
7	SMTP_Server	DNS_Int_Int	domain-udp	accept	Long
8	Protected_LAN Company_LAN	DNS_Int_Ext	domain-udp	accept	Long
9	Backup_Server	Screened_Subnet	backup	accept	Long
10	Any	Any	Any	drop	Long

For the protected LAN and Default Propeties for both Checkpoint Firewall -1 configurations:
Firewall-1 V4.1 SP2 on AIX 4.3.3





Assignment 3 - Audit Your Security Architecture (25 Points)

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Border Router and Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Border Router and Primary Firewall are actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Plan

We would do this assessment in two phases. The first would assume we know nothing of the security architecture and thus use generic scans, probes, and attempts to gather information. Once all the generic methods have been used, the specifics of the architecture will be used to attempt to gain further information. This doesn't bias our choice of tools knowing the specifics of the border router or firewall, but then allows us to be more thorough on each filter and rule in the second phase as we know the specifics of the rule and filter and the platform they are implemented on.

The wording of the assignment seems to indicate this assessment should cover the other nodes. A comprehensive information systems audit requiring the border router and primary firewall can be interpreted as just that i.e. all the systems with only the border router and primary firewall being required. Then there is the ambiguity in defining the primary firewall.

We will also bring the collected knowledge of the Internet by searching for the specifics on deja news and several of the major search engines.

We will need access to the IDS logs, the syslogs, and the specific logs of the firewall and border router for periods before the assessment (to gather baseline information) as well as during the assessment. This will help if the assessment causes problems to know if the problem existed before the assessment.

We will also need access to all the policies and procedures concerning the border router and primary firewall to predict staff behaviour during the assessment.

For each component of the border router and primary firewall we will need the company's documentation and the company supplying that component i.e. the component's vendor. Examples are the system hardware vendor, the operating system vendor, the firewall vendor, the network interface card vendors, etc. This allows us to determine the current patch, firmware, microcode, etc. available vs. the ones in place during the assessment.

Once the policies and procedures have been obtained, read, and understood by the assessment team the staff will be interviewed to determine their level of understanding of those policies and procedures. These interviews are best done at the staff member's normal work location and shift to determine how much distraction is in the workplace in a normal day.

The security policy, and its previous versions if available, will be required. The current security policy will be matched against the configurations of the border router and the primary firewall looking for both the aspects of the security policy not implemented or not fully implemented in those configurations and the configuration parameters not in the security policy.

A company supplied network diagram will be requested to be checked against the output of a network scanner set to gather minimum system information in the implementation phase and differences noted.

Best practices procedures for hardware, operating system, and application configurations will be obtained to compare against the current configurations during the implementation phase. Examples are the Solaris hardening guides and CERT documents.

We will request reports from the change control system for the border router and primary firewall to compare with the current configurations during the implementation phase.

We will request accounts on at least one machine on each of the subnets and either administrator access on the key internal machines or access to an administrator to perform tasks needed in the implementation phase. Accounts or access to the IDS, the vulnerability scanner, and the argus servers in the DMZ is requested as well.

A method of accessing the enterprise from an external address that can spoof addresses will be need. We can provide this, but such access at the enterprise's ISP would be preferred. If the test machine is external to the enterprise then the data collected during the assessment must be protected. Using EFS on Windows 2000 is an option.

A listing of accounts on the border router and the primary firewall will be needed as will the implemented password portion of the security policy. This will allow password cracking att empts during the implementation phase. We will check that the policy treats users differently than administrators. Users should be locked out on failed login attempts where administrators should not. Administrators should have stronger password filter rule s and require changing of passwords more often.
A list of current known vulnerabilities from CERT, SANS, Security Focus, etc will be compiled, the exploits built and loaded on the external machine and the vulnerability scanner for running during the implementation phase.
Once the requests for these resources are satisfied or reasons why they are denied are explained, the scope of work w ill be detailed to the company's management that requested the assessment. Costs, risks, and time for the various aspects will be given and options for timing of the assessment will be given. Then the timing of the assessment's various aspects will be sche duled to fit the needs of the business as only they can determine the impact of the assessment on the company's schedule. Thus some aspects of the assessment that have risk of affecting services can be scheduled in light traffic periods, where aspects tha t are designed to trigger alarms or generate log entries that don't have the level of risk can be scheduled on shifts where the employees are monitoring the systems.
As the primary firewall in this instance has the VPN security gateway as well, we need to clear the assessment scope and timing with any partner, supplier, or vendors who might have connections via the VPN.

Implementation

We want to attempt to determine the status and response to the major protocols in the network and transport IP layers. T hus we need to have a method of scanning for TCP, UDP, ICMP, IPSec, IGMP, etc. and the ports in those protocols which have ports. For TCP and UDP nmap is the tool of choice. To add some vulnerability checking on ports found open and to add a sanity check to nmap , SARA and nessus will be used We can also use ISS Scanner and/or Cybercop in this assessment if the company has not u sed the current version of either of these commercial tools recently and wishes to add the cost of the use of those tools to the assessment. Otherwise we'll be telling them what they already should know as these tools are not configurable to add vulnerabil ity checks

For the border router we can use tools that allow IP address spoofing to check the filter denying private addresses into the perimeter. To test the deny of source routing we can use netcat and check the logs and success of the command:
#nc -g x.y.z.o –g x.y.z.b 1200
From an internal node we send a crafted packet with a source address external to the enterprise to the machine we are using to do the assessment to see if it makes it or is dropped and logged
#sirc4 a.b.c.d testhost 23
An attempt to use the small ports (chargen, echo, etc.) should be dropped and logged as part of the nmap or SARA scans.
We will also attempt to telnet, ssh and otherwise connect to the router. We will reset and power cycle the router if our test machine is at the ISP to see if we see packets sent out before the router is initialized and ready.

For the primary firewall we use the nmap commands to map the entire port range for TCP and UDP.
#nmap –sT –p 1-? -P0 x.y.z.64/26
#nmap –sU –p 1-? -P0 x.y.z.64/26
If our test machine and the company's log server aren't full yet we can add the other nmap scans as time, log space, and money allows.

Perimeter Analysis

There is no data from the assessment, as I have not run this assessment on any live network. I can imagine the results and the remedies to apply.
While the mantra of "let routers route and firewalls firewall" has some appeal, defense in depth has some solace. Thus adding configuration changes to the router to block more services (like finger, etc.) would impr ove the perimeter defense.
A reverse proxy server would be a possible addition to the security architecture.
Once IPSec VPNs and NAT play better together we could consider NATing the company and protected LAN subnets.
More IDS systems can be deployed wi th additional machines at the DMZ, the company LAN, and the protected LAN.
Machines in the protected LAN can have personal firewalls added, have EFS (Encrypted File System) configured to hold the sensitive files, and have PGP installed and the users educat ed to its use for signing and /or encrypting email.

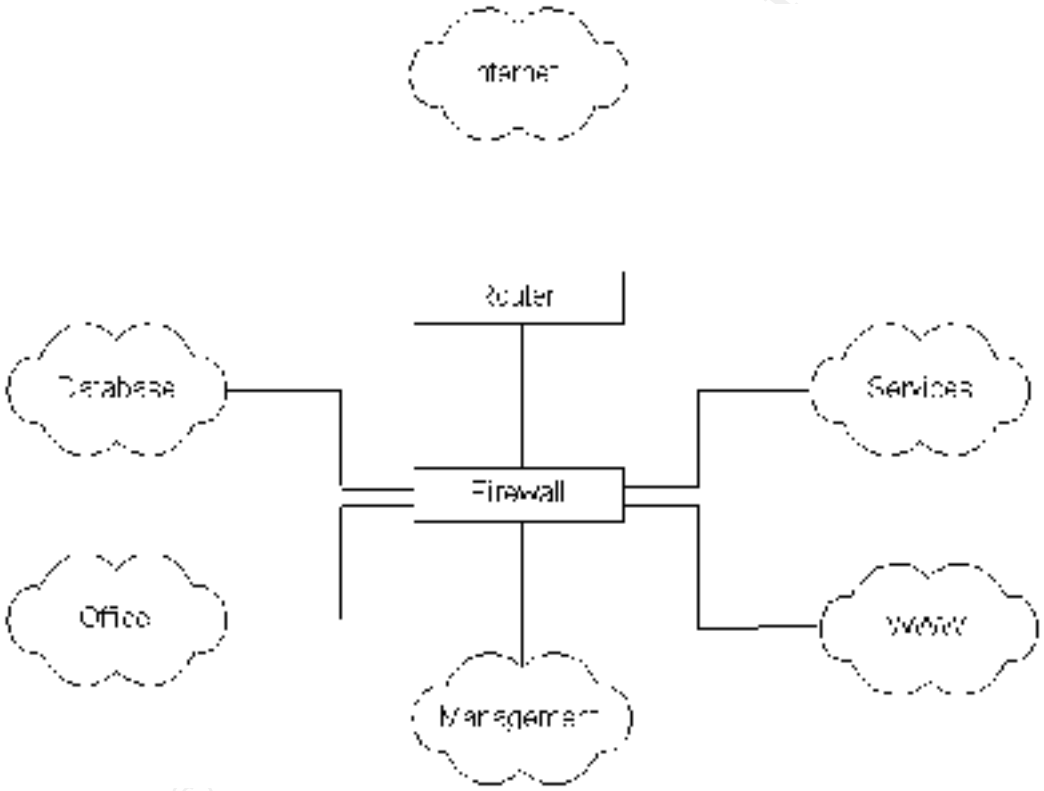
Assignment 4 - Design Under Fire (25 Points)

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!
Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

James McMahon GCFW Practical Assignment

Entire Network



This design was selected for several reasons:
It shows no intrusion detection systems
It uses a single Checkpoint firewall on Solaris 2.6 with 6 interfaces
The Solaris system running Firewall -1 has NIS server and AutoFS packages installed
It specifies a vulnerable version of Firewall -1
It does not specify modifying the default properties setting for Firewall -1

Firewall Attack
Firewall-1 V4.0 and no SP level specified, so our potential vulnerabilities to attempt to exploit:
Default Properties, if unaltered from the installation defaults, allow the following traffic to be accepted and without logging:

UDP/53 DNS to any destination
TCP/53 DNS to any destination
UDP/160 SNMP traffic to the firewall
IP Type=94 (IP within IP encapsulation) traffic sent to firewall
ICMP traffic to any destination
TCP/256 – 259 traffic to firewall
TCP/18,181 traffic sent to firewall

For vulnerabilities the best source is probably the paper presented at Black Hat Briefings 2000 by Thomas Lopatic and John McDonald. For this exercise, download the referenced modules, run against the Firewall-1 at GIAC Enterprises, monitor the results. The IP Address Verification exploit probably won't work, though no information in the paper indicates otherwise, likewise for S/Key. FWN1 will probably work allowing an unload. Firewall to smoke screen without much effort. No fastmode configuration is listed in the paper, but a use of nmap in Stealth FIN mode with the most likely ports to have fastmode turned on can be attempted.

Denial of Service Attack

No information is given on the hardware the Solaris hosted Firewall-1 firewall is using. Most companies use small machines for this function so the recent IP fragment denial of service vulnerability will probably have the desired affect. As this configuration has the firewall as a central routing hub between the database, office, management, web server, services subnets AND the firewall is not unloaded but CPU busy this really impacts the business. Tribe FloodNet 2K or any of the Distributed Denial of Service (DDOS) would be used as we do have 50 compromised cable/DSL systems at our disposal. Other options are Ping of Death, Smurf, LAND, Teardrop, etc. The important point of this exercise is how to prevent such attack from impacting the business. The paper's follow on design using more than one firewall will help to some degree. This design has the advantage of a dedicated firewall management node, but I do not see a method of monitoring the border router. We need such monitoring of the router to alert the administrators of traffic not fitting normal or anticipated traffic patterns. This implies that the administrators are aware of normal traffic patterns, have means of monitoring the traffic patterns, are trained in procedures to recognize and respond to DOS attacks, and methods exist to collect information to find the real source of the attack. If the DOS attack is initiated or transferred to the internal network the design is well suited to survive given the way it is dispersed.

Compromise an Internal System

If we mapped the nodes on the network through the firewall with TCP fastmode and have a tooltalk service that has the buffer overflow vulnerability we can use the ftp-ozone utility from the Lopatic and McDonald paper to exploit that vulnerability. If not and I have to choose just one internal system to attack I would go after something on the management network, probably the FW management system. Usually an attack attempt goes through the phases of:

Phase	Reason	Technique	Tools
footprinting	get target address ranges, node names, contacts, etc.	Open source search whois DNS Zone transfer	USEnet, Internet search engines, http://www.arin.net/whois dig, nslookup ls –d, Sam Spade
scanning	find services that are listening and/or responding	ping sweeps TCP/UPD/ICMP scans	fping, Ping Pack nmap
enumeration	get user accounts, etc.	system utilities	telnet banners, showmount, etc
gaining access	attack most vulnerable services	password file grab, file share listing buffer overflows	snoop legion
escalate privilege	get root or administrator	password cracking	crack, L0phtcrack, getadmin
pilfering	to the next system	find passwords in clear, sniff,	rhosts, configuration files
cover tracks	so we can continue or come back in	clear logs hide tools	zap, edit hidden directories, file streams
back doors	when we return regain regain our privileges	add user accounts infect startup files leave remote controls	administrator privilege, wheel group rc files, registry, rc files netcat, trojans

The assignment implies we have our target and its associated information so our next step would be a vulnerability scanner. For this we use SARA as it is kept current with the recent vulnerabilities. If the firewall is on Solaris 2.6, the firewall management system is probably similar, but nmap in fingerprint mode will confirm that. SARA will show any vulnerabilities,

then it's just a matter of obtaining the corresponding exploit to gain the access. I guess that is why *their* job is easier than *our* job.