Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.6a (revised October 26, 2001)

Sans Darling Harbour

January 19-24 2002

Barry Darnton

Security Architecture

Assignment 1 – Security Architecture (15 points)
Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.

Your architecture **must** consider access requirements (and restrictions) 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);
- GIAC Enterprises (the employees located on GIAC's internal network).

You **must** explicitly define how the business operations of GIAC Enterprises will take place. How will each of the groups listed above connect to or communicate with GIAC Enterprises? How will GIAC employees access the outside world? What services, protocols, or applications will be used?

Defining what type of access is required and why is a critical part of this assignment. If you have not thought through how this access will take place, you will not be able to adequately define your security policy and ACLs/rulesets later in the paper.

In designing your architecture, you **must** include the following components:

- filtering routers;
- firewalls;
- VPNs to business partners

Assumptions

I am a consultant that has been called in to GIAC enterprises to design a solution to the above problem. I have no idea of what recourses are available at the company, what is expected or what sort of budget I am limited to. GIAC enterprises will be referred to as "the client".

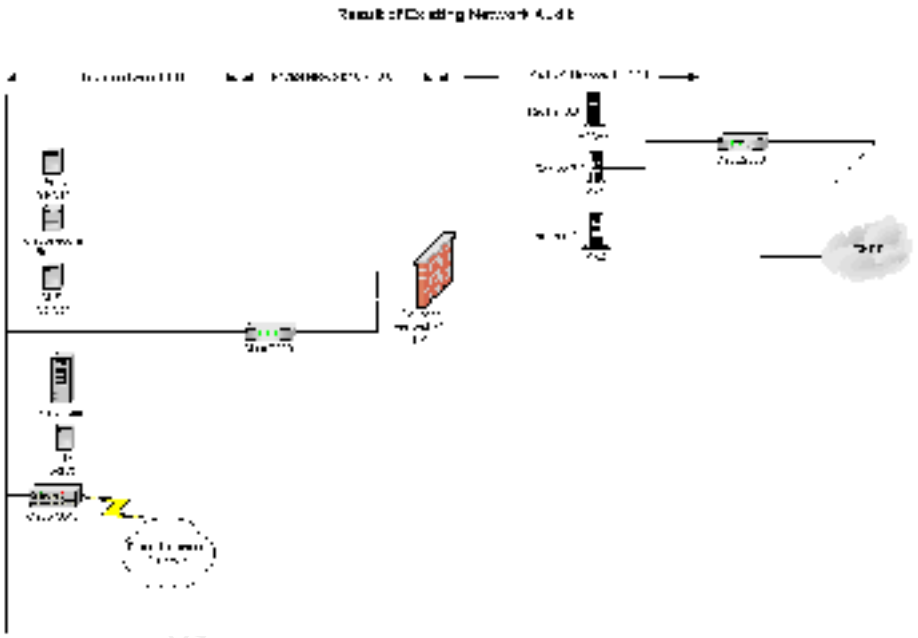
Information gathering

My first point of call would be to do a site visit so that I can clearly define what is required from the client's point of view (get a wishlist). I would also need to audit the current network and external connections if any to ascertain if the proposed solution would work with existing client hardware. There would be no point recommending a solution for remote users that required a Windows 2000 client if the organization only uses windows 98. It would also need to be determined what level of technical expertise exists in the current IT department so that recommendations in regards to required experience and training can be made in order for the client to be able to install and manage the final solution.

Client Requirements

After doing a site visit to GIAC Enterprises I now have the following information.

- The client's desktop environment is aro und 1000 PC's running a mixture of windows 98/2000 software.
- The servers are centralized and managed by a single IT department.
- The IT department has a Database Administrator (DBA), two network administrators familiar with Cisco and Cabletron routers, a VMS administrator and a Unix Administrator with average Unix skills.
- There is currently an old Gauntlet firewall(V3.2), a cisco 2500 border router connected to the Internet via a 128K ISDN line.
- The Internal network uses Non Internet Routable Addresses
- The client has a class C internet address assigned



It would be fairly obvious to most people involved in security that the above design leaves a lot to be desired, old and unpatched Linux machines protected only by a router, a very old version of Gauntlet firewall with an even older version of bind, and Remote access on the Internal network using username/Password via Ciscosecure. This was a real Network prior to doing the Security Essentials track.

Client Access Requirements and Restrictions

Customers

Customers can be anyone, anywhere at anytime, to purchase a fortune , they will not require a username or password, only a valid credit card.

Suppliers

Suppliers are pre-determined and provide confidential information, and will therefore require access via an encrypted link with a username and secure one time password. A separate database for suppliers will be required. Suppliers will Export data from their local database and FTP the Updates to the supplier Database server. A cron job will import the data into the supplier Database. The DBA will import the data into the live Database after the marketing department has approved the new data.

Partners

Partners will require access to the live database, as they are only translating the data at their end only read access will be required. There is no division of data between partners, all partners have access to all the information, therefore once in the database, security is minimal. Access to the network will be via an encrypted link with a username and one time password, access to the database will require another username with a re-usable password, this coupled with read only access and logging should be sufficient. It should be noted that their will be three databases, one for the suppliers, one for the partners and one for customer details and credit card information. The last one will only be accessible from the internal network.

Outbound Access from Client

Users within the clients network require access to the internet for HTTP/HTTPS, FTP and Telnet. It is a requirement that all access is logged by username. No direct mail or pop services are permitted.

Remote Access for Admin Functions

The Administrators and DBA require remote access to all machines for troubleshooting purposes. Direct access via the Internet to hosts outside the Gauntlet firewall will not be permitted. All access to external machines must come from pre-defined internal hosts. This will require secure authentication to the network via an encrypted link, then to the Metaframe server as the jump point. All systems outside the Gauntlet firewall are Unix or Cisco so we can allow access to these systems via SSH where supported and deemed appropriate. Where Access via SSH is not appropriate console port access will be via terminal servers.

Budget & preferences

This is a new venture by the client so money is not unlimited, a reasonable approach to costs must be taken without compromising security. The IT department has requested an application level firewall for the corporate network and has a

preference for Cisco equipment as the support is good and they are familiar with the product already. The bandwidth requirements are uncertain so equipment selection should be done so as to avoid major purchases for the next two years.

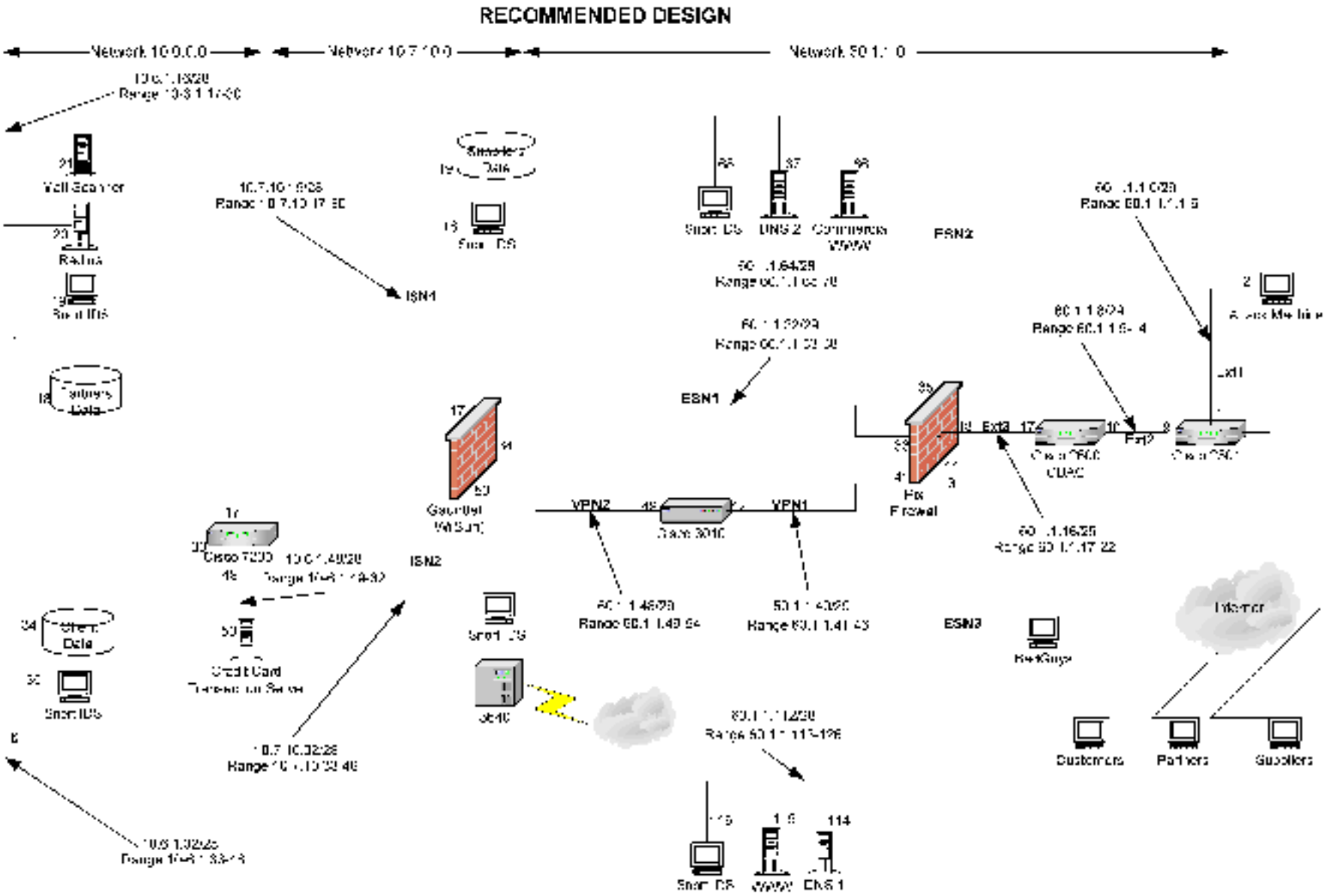
Web Servers

The current web servers are currently free public servers that only have non commercial information stored on them. A new server(s) will be required for the purchase of fortunes, this will need to be secure even though no customer data is stored on this server. If this server is compromised the loss would be revenue rather than customer details. Losing customer Credit card details and personal information is far more likely to put a company out of business than loss of data.

Customer Details and Cred it Card Information

For obvious reasons access to the credit card transaction engine (CCTE) and the customer database will be very restricted. The secure web server will need to pass the customer information to the CCTE for verification of credit card det ails. When checking is complete the CCTE will inform the web server . The CCTE will pass the customer details to the client database. The only server not on the Internal network (10.0.0.0) with any access to the customer database is the CCTE. The Web server will only have access to the CCTE. No customer data is ever stored on the web server or the CCTE except during the transaction processing.

Recommended Design



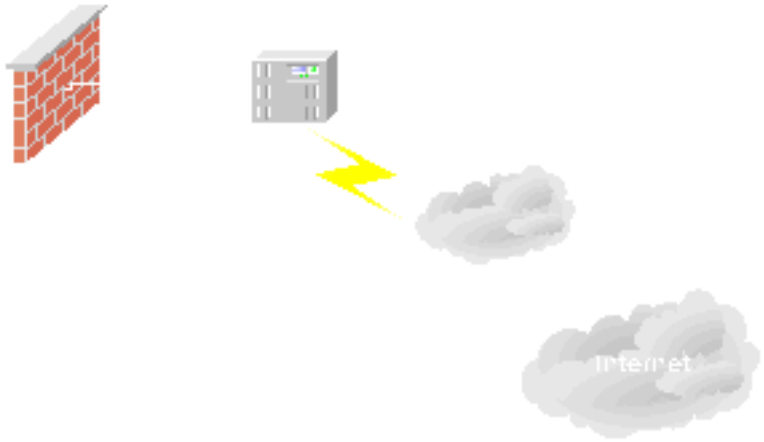
Equipment Selection

Cisco 2500

The Cisco 2500 is an existing piece of equipment and probab ly would not have been included in the design if it was not available. It does offer additional security and act as a choke for the C2600. This router can filter all the common rubbish that you always see in the router logs and reduce the number of alerts on the second router. This router also offers redundancy if the C2600 should fail. A set of ready and tested ACL's for redundancy should be on the router but not applied to any interface. In the event that the C2600 needs to be taken out of service, you would change the Internal IP address and apply the ACL's to the rel evant interface. Under normal operating conditions this router is only running a basic set of ACL's and would not be a bottleneck at the current Internet bandwidth, this would need to be reviewed if the bandwidth was increased.

Cisco 2600

In an effort to keep costs down while still maintaining some level of expansion I selected a Cisco 2611 -RPS. This router will be enough to handle the Frame relay link even if it is expanded to the 2 meg lim it. The 2600 is a modular router and a WAN interface would be purchased so that the C2500 could be removed if required, this would provide additional redundancy. If expansion to multiple E1 links was required the Cisco 3600 with the appropriate module coul d be used. The 3640 was not used initially because this would require all users to have secure one time passwords, this would be cost prohibitive.



PIX Firewall

The recommended firewall is a Pix 515 (current version is 6.1) , this was selected because it supports up to 6 interfaces and we are using 5 already, it also supports failover and has more than enough throughput to handle any load even if multiple E1's were required. The Pix 525 was not chosen even though it support 8 interfaces

as well as Gig because it is unlikely that any more interfaces will be required and with an application level firewall behind it and at best E1's in front the expense of Gig would be wasteful. The Pix is a product of Cisco like the border router's but are completely different animals, you don't use a Pix as a router and you don't use a router as a full blown firewall, both the Pix and the router have very few known exploits and because they are so different, if an exploit was found in one it would not necessarily work on the other. This adds another level of defense. The Pix will be the second line of defense and will primarily keep unwanted traffic from entering the service networks.

Cisco VPN 3015 Concentrator

The Cisco 2610, Pix firewall and the Gauntlet firewall all support encryption but were not selected because it would limit the upgrade path should bandwidth requirements increase. If the bandwidth requirements increased to multiple E1's then hardware encryption would be required later and a full re-design would need to be done. The 3015 concentrator was selected because it can handle up to a 4mB link standard and is upgradeable to 3030, 3060 and 3080 with hardware encryption modules available. The Cisco VPN concentrators also come with a freely distributable VPN client software reducing costs further. The 3015 comes standard with software encryption processing

Gauntlet Firewall

Gauntlet V6.0 was selected primarily for three reasons, first the client was familiar with the product, second they had requested an application level firewall and third a search for known vulnerabilities on www.cert.org found only three, given it's time in the market this is a good indication of it's robustness if configured correctly. Gauntlet supports the standard proxies such as FTP, HTTP, HTTPS, these proxies can also be enabled as adaptive meaning that once authenticated the firewall will pass the rest of the connection at layer three like a packet filtering firewall for enhanced performance. Gauntlet also supports what I would describe as non user type proxies such as DNS and Csmap, the DNS proxy will permit the internal nameserver configured as a forwarder to query the external DNS securely, this means that bind will not need to be run on the firewall itself. The Csmap proxy effectively replaces an MTA such as Sendmail or Qmail from direct access with Internet users. Csmap is the program that listens on port 25 for SMTP messages, the theory is that being a small program of around 300 lines it is easier to secure than a program such as Sendmail that is around 100,000 lines of code. One of the vulnerabilities I found for Gauntlet was for the Csmap proxy but a Patch has been released to fix this, Csmap does not run as root so any exploit has less chance of compromising the root account. Csmap's only job is to accept any SMTP messages, check the formatting and if OK, save the message in a pre-determined directory. The MTA such as Sendmail then picks up any messages in this directory and processes them as normal. Csmap can filter spam and do anti-relay as well, what needs to be remembered is that it is just a basic SMTP handler, if you have requirements to do anything other than accept or reject E-mail in real time then a real MTA such as Sendmail or Qmail should be used. Another useful Proxy is the Syslog proxy, you can configure this to securely permit Syslog messages from specific hosts to your central log server.

Hosts on Service Networks

It would be beyond the scope of this paper to document every host that exists on the service networks as the type of applications that need to run on them would need to be considered. In the design there is currently only Web,DNS and IDS machines, all of which could run under any Unix operating system. My preference would be to run an Open source Unix such as Linux (Current Version 7.2) so that additional security products like Netfilter and tripwire could be used. All of these systems should be locked down as tight as possible by not running any unnecessary services on them and clearly defining what hosts are permitted to talk to who on what ports using Netfilter. Netfilter(iptables) is a bit of a beast to install and configure but is well worth the extra effort involved given it's detailed logging information, if you want a starting place on Netfilter go to http://netfilter.samba.org . Any admin remote access should be via SSHv2 or later, time should be synchronized on all hosts and a central log server put on the internal network for analysis. A certificate should be installed on the SSL server from a registered vendor such as Verisign, you could install your own certificate however some customers may not accept this and business could be lost. Scan each host from the same subnet to determine what services are running and disable or filter any services that are not absolutely necessary. All of the output from your scans should be saved for future audits.

IP Subnetting

Name	Subnet	Net	Range	B/C	Trust Level	Description
Ext1	60.1.1.0/29	0	1-6	7	1	External Net 1 Completely Untrusted Used for Auditing network and sniffing unfiltered Internet traffic
Ext2	60.1.1.8/29	8	9-14	15	2	External Net 2Completely Untrusted, Internet Router Links
Ext3	60.1.1.16/29	16	17-22	23	3	External Net 3 only protected by router ACL's. Used for testing what's actually getting through the Router
Esn1	60.1.1.32/29	32	33-38	39	5	External Service Net 1 all outbound traffic from gauntlet firewall. In/Out SMTP and DNS queries to DNS1 & 2. Connection from Fortune WWW to CCTS
VPN1	60.1.1.40/29	40	41-46	47	5	Encrypted traffic from Suppliers and Partners. Should only see TCP 50,51 and UDP 500
VPN2	60.1.1.48/29	48	49-54	55	6	Unencrypted traffic from Suppliers and partners
Esn2	60.1.32.64/28	64	65-78	79	5	External Service network 2 used for http/https to fortune server, secondary DNS. Connection from fortune server to CCTS
Esn3	60.1.32.112/28	112	113-126	127	5	External Service Network 3, used for HTTP to general Web server and DNS (UDP) from Gauntlet firewall and DNS (TCP) between DNS1 & 2
Isn1	10.7.10.16/28	16	17-30	31	6	Internal Services Network 1 used only for suppliers to put new data into the database. Only ftp traffic should be seen here
Isn2	10.7.10.32/28	32	33-48	49	4	Internal Services network 2 this will be used for Administrators to come in via the internet VPN then to the Met frame server on TCP 1490. For additional redundancy they will be able to dial in over the public telephone network as well. As part of this one time passwords on dialin access will be a requirement. Authentication to the Radius server will also mean that port UDP 1490 will be seen.
I1	10.6.1.16/28	16	17-30	31	6	Internal Net 1, used for the mail scanner, radius server and the partners database. Expected traffic will be SMTP, Radius requests and SQL all from the firewall
I2	10.6.1.32/28	32	33-48	49	5	Internal Net 2, only used for transactions between the CCTS server and the Client database server. In addition to this the DBA machine will need access. Expected traffic will be SQL and SSH from DBA.

NOTE: the 60.1.1.0 subnet is a reserved address and should not be routable across the Internet. The addressing scheme and Subnetting used is for example only. Any valid Class C address could be substituted by replacing the 60.1.1 section w ith a valid address range. A listing of currently assigned and reserved addresses can be found at http://www.iana.org/assignments/ipv4 -address-space.

Could the Subnetting have been done b etter, well that's subjective but it could have been done differently. I purposely used a 29 Bit subnet mask between routers instead of a 30 bit mask so that sensors etc could be placed in these areas later. There is also a big gap between ESN2 and ESN3. E sn2 currently has 14 usable addresses, if I had put ESN3 at the next available subnet I would have not been able to increase the available addresses without configuring secondary addresses on the pix firewall as well as modifications to the routers and Gau ntlet firewall. The way this is designed you can simply change the subnet mask to a 27 bit mask and double the available addresses without changing any existing addresses. I could have started private addressing behind the Pix to save addresses but I chose not to run Nat on the Pix so that the Border router filters could isolate specific hosts and also allow a trace to detect individual traffic at that point.

Security Policy

Assignment 2 – Security Policy (35 points)
Based on the security architectur e 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 Access Control List (ACL), firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider the access requirem ents for internal users, customers, suppliers, and partners that you defined in Assignment 1. The policies you define should accurately reflect those business needs as well as appropriate security considerations.

You **must** include the complete policy (expli cit ACLs, ruleset, IPSec policy) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" etc. The policies may be included in an Appendix if doing so will help the "flow" of the paper.

Defining what's needed where

Before applying any rules to routers or firewalls it is a good idea to do a matrix of what ports, protocols, hosts and direction of traffic flow is required in order to comply with the clients requirements (policy). While a policy needs to be a lot more t han just access controls we have enough information from assignment one to be able to do this part. In the following sections I will systematically go through each firewall and router that needs to be configured to meet the requirements. Host lockdown is a n integral part of this implementation and must be done as part of this installation but is far to involved to do in the time given for this assignment.

Cisco 2500 Choke Router

The first router in the firing line is the Cisco 2500 running a standard IP I OS. The Firewall Feature set would not be put on this router because CBAC is very processor intensive and could cause a bottleneck. The purpose of this router is just to reduce noise by basic filtering of unwanted INBOUND packets such as ICMP and some UDP. Obviously the router itself will need to be protected as well.

Protecting the router

Protecting the router can be put into three categories

- Disabling any unnecessary services
- Setting secure router access controls and passwords
- Filtering unwanted packe ts to and through the router

As this is the first line of defense into the network we have decided not to permit any telnet access to the router at all, only console access will be permitted. According to the clients requirements this is not what they ask ed for, however we

can supply console access via a terminal server. This can be done by using a secured internal Unix host with a second NIC directly attached to the terminal server(s) that are in turn hardwired to the console ports. All routers and hosts that support console ports will have this type of access, the logic behind this decision is that there is nothing worse than configuring a router via telnet and locking yourself out, secondly if only one person can access a router at a time then no mistake s can be made, thirdly , console access via another host requires authentication and is logged. A scripthost could be used to record all changes made to hosts and routers to use as change control and audit trail if deemed necessary. I will include a diagram and brief description of console port access in the appendix.

Disabling unnecessary services

These commands should be set regardless of the IOS, some versions have some services switched of by default but the next version does not

No ip source -route	Don't allow source routed packets
No service finger	Disable finger requests
No ip HTTP server	Disable the routers internal HTTP management process
No ntp enable	Don't act as an NTP server
No cdp enable	Disable the Disco discovery protocol
No ip bootp server	Disable the bootp server
No snmp	Don't answer any SNMP requests
No ip directed -broadcast	Don't be used as a smurf amplifier (applied to interface)
No ip redirects	Disable ICMP redirects
No service tcp -small-servers	Disable TCP services such as Echo and Chargen (great for a DOS)
No service udp -small-servers	Disable UDP services (Echo and Chargen are here as well)

Setting Secure router access controls

Service password -encryption	Encrypt the login password
Enable secret 0 "password"	Encrypt and set the Enable password
Line aux 0 Transport input none	Disable all transports on the Aux line. No transports, no access of any type
Line vty 0 4 Transport input none	Disable all transports on all the Vty lines. No transports, no access of any type
Line con 0 Exec -timeout 15 0 Password 0 "password"	Set the automatic logout to 15 minutes and set password on the console port. No transport is required because it will be a direct serial connection

Packet Filtering

First we will apply filter s to deny any traffic in any direction that are not valid IANA registered addresses. This list is straight out of an article written by Scott Winters and can be found at http://rr.sans.org/firewall/blocking_cisco.php . I won't repeat the explanations for these filters as they are already clearly explained in the above document and just about any other GCFW practical to date.

Access-list 11 deny 10.0.0.0 0.255.255.255
Access-list 11 deny 127.0.0 .1 0.255.255.255
Access-list 11 deny 172.16.0.0 0.15.255.255
Access-list 11 deny 192.168.0.0 0.0.255.255

Access-list 11 deny 224.0.0.0 15.255.255.255
Access-list 11 deny host 0.0.0.0

NOTE: The strange mask that you see above such as 0.15.255.255 is just the inverse of the subnet mask. Why cisco choose to do this is beyond me but it isn't difficult to calculate. The range in RFC 1918 states that 172.16.0.0 to 172.32.0.0 is a reserved address. With a little calculation you will find that this will require a 255.240.0.0 subnet mask. Where you see a 255 you use a 0, where you see a 0 you use 255, to get the 15 you simply subtract 240 from 255.

Next we do a matrix of what traffic we want to let in and out, we will use the policy of least privilege, ie anythin g not explicitly permitted is denied. I have selected the snort sensor on ESN3 as the host for testing network connectivity.

Cisco 2500 Filter Matrix

Cisco 2500 Filter Matrix					
Outbound	IP	Src	Dst	Initiating Host	Description
	All	60.1.1.64	Any	ESN2	Outbou nd from hosts on ESN2
	All	60.1.1.112	Any	ESN3	Outbound from hosts on ESN3
	All	60.1.1.34	Any	Gauntlet F/W	Outbound from Gauntlet
	All	60.1.1.42	Any	Cisco 3010	Outbound from VPN
	ICMP				
Echo		60.1.1.112	Any	ESN3	Outbound Echo from ESN3
Inbound					
	All	Any	60.1.1.64	Internet	Inbound traffic to ESN2
	All	Any	60.1.1.112	Internet	Inbound traffic to ESN3
	All	Any	60.1.1.34	Internet	Inbound to Gauntlet F/W
	All	Any	60.1.1.43	Internet	Inbound to VPN
	ICMP				
Echo -Reply Unreachable		Any Any	60.1.1.112 60.1.1.112	Internet Internet	Inbound Reply to ESN3 Inbound Unreachable to ESN3
Time -Exceed		Any	60.1.1.112	Internet	Inbound Time -Exceeded to ESN3
	Nets				
NON IANA		Any	10.0.0.0	Internet	Inbound Block Net 10
		Any	127.0.0.0	Internet	Inbound block Net 127
		Any	172.16.0.0	Internet	Inbound Block net 172.16 -172.32.0.0
		Any	192.168.0.0	Internet	Inbound block net 192.168.0.0
		Any	224.0.0.0	Internet	Inbound block net 224.0 -224.32.0.0
	Host	0.0.0.0		Any	Block invali d IP address

From the above matrix we can make the following access -list
Ip access-list extended internet

1. deny ip 10.0.0.0 0.255.255.255 any
2. deny ip 127.0.0.0 0.255.255.255 any
3. deny ip 172.16.0.0 0.15.255.255 any
4. deny ip 192.168.0.0 0.255.255.255 any
5. deny ip 224.0.0.0 0.15.255.255 any
6. deny ip host 0.0.0.0
7. permit icmp 60.1.1.112 0.0.0.255 any echo
8. permit icmp any 60.1.1.112 0.0.0.255 echo -reply
9. permit icmp any 60.1.1.112 0.0.0.255 unreachable
10. permit icmp any 60.1.1.112 0.0.0.255 time -exceeded
11. deny icmp any any
12. permit ip 60.1.1.64 0.0.0.255 any
13. permit ip any 60.1.1.64 0.0.0.255 any
14. permit ip 60.1.1.112 0.0.0.255 any
15. permit ip any 60.1.1.112 0.0.0.255
16. permit ip host 60.1.1.34 0.0.0.255 any
17. permit ip any host 60.1.1.34
18. permit ip host 60.1.1.42 any
19. permit ip any host 60.1.1.42
20. deny ip any any log

Apply to interface
Int s0.1
Ip access-group internet in

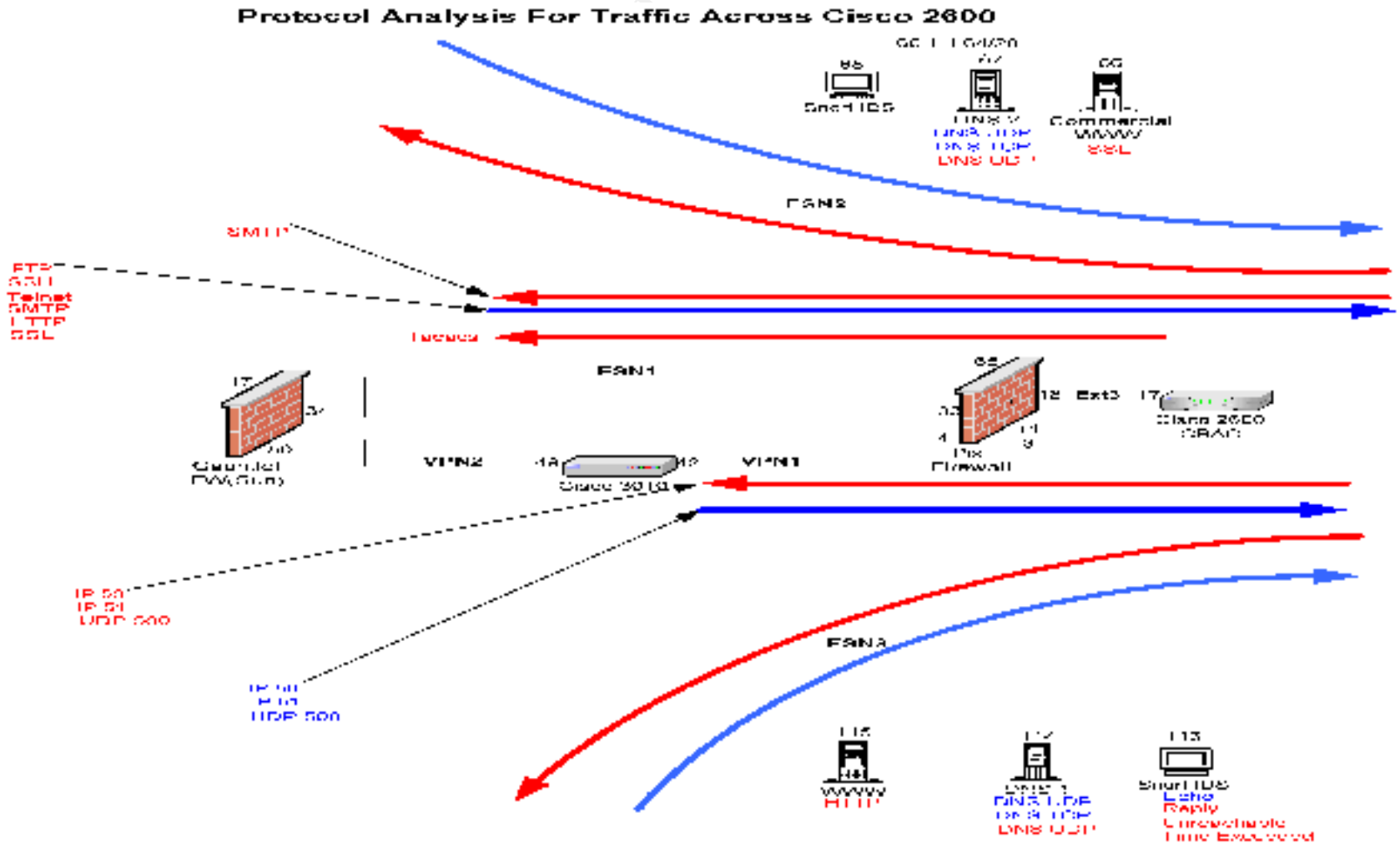
Rule Order

The order in which rules are applied is important as is the type of access list, looking at rules 1 -6 we are denying all IP from those netw orks or hosts, this does not prevent ICMP from those addresses, so after we have permitted the ICMP filters for the network designated as the test network for traceroutes we then need to block all other ICMP traffic. We could have used the following standa rd access-list
Access-list 10 deny 172.16.0.0 0.15.255.255, this would have blocked all traffic from these hosts be it TCP,UDP or ICMP. The type of access list selected will depend on your needs. Keep in mind that this is just a noise reduction router so a broad set of filters have been applied because the next step of filtering will hone in more on what's really needed. Multiple access lists can be applied to router interfaces, so you can separate your Ingress filters from your Egress filters if you like, it is just a matter of choice , again more specific details can be found in Scott Winters paper .

Cisco 2600 Border Router

The router directly behind the C2500 choke router is the Cisco 2611, with the Firewall IOS feature set. The router is the first real line of defense and will need to be well locked down. This ACL's on this router need to be very granular and only permit what is absoloutly necessary. As there are many different hosts and protocols crossing this router I first did a graphical representati on, I find that less gets missed this way. In addition to this the ACL's can be built from this analysis.

Cisco 2600 Protocol Analysis



Cisco 2600 Protocol/Port matrix

Name	**Port**	Src	Dst	Initiating Host IP	Description
IPSec	50	Any	60.1.1.42	External User	Inbound VPN Connection
IPSec	51	Any	60.1.1.42	External User	Inbound VPN Connection
IPSec	50	60.1.1.42	Any	Cisco 3010	Return Traffic for VPN Connection
IPSec	51	60.1.1.42	Any	Cisco 3010	Return Traffic for VPN Connection

TCP					
Name	Port	Src	Dst	Initiating Host	Description
ftp	21	60.1.1.34	Any	Gauntlet Firewall	Outbound FTP Access from client
Telnet	23	60.1.1.34	Any	Gauntlet Firewall	Outbound Telnet Access from client
SMTP	25	60.1.1.34	Any	Gauntlet Firewall	Outbound E-mail
SMTP	25	Any	60.1.1.34	Gauntlet Firewall	Inbound E-mail
DNS	53	60.1.1.67	Any	DNS1	Outbound DNS Query 's (Primary)
DNS	53	60.1.1.114	Any	DNS2	Outbound DNS Query's (Secondary)
HTTP	80	60.1.1.34	Any	Gauntlet Firewall	Client Outbound HTTP access
HTTP	80	Any	60.1.1.115	External User	Inbound access to web general Web server
SSL	443	60.1.1.34	Any	Gauntlet Firewall	Client Outbound SSL access
SSL	443	Any	60.1.1.66	External User	External User SSL to Fortune Server

UDP					
Name	Port	Src	Dst	Initiated By	Description
DNS	53	60.1.1.67	Any	DNS1	Outbound DNS Queries from Primary
DNS	**53**	Any	60.1.1.67	Anyone	Inbound DNS Queries for GIAC Domain (Primary)
DNS	53	60.1.1.114	Any	DNS2	Outbound DNS Queries from Secondary
DNS	**53**	Any	60.1.1.114	Anyone	Inbound DNS Queries for GIAC Domain (Secondary)
Ip-sec	**500**	60.1.1.42	Any	VPN Concentrator	Outbound IPSEC connections
Ip-Sec	**500**	Any	60.1.1.42	External User	Inbound IPSEC Connections

ICMP				
Echo	60.1.1.116	Any	Snort IDS	Let someone ping for troubleshooting
Echo-Reply	Any	60.1.1.116	Any	Let the reply come back (also the badguy)
Unreachable	Any	60.1.1.116	Any	Let error messages come back in
Time-Exceeded	Any	60.1.1.116	Any	And these errors too

Firewall IOS Features

Using the Firewall IOS feature set we are able to use some additional features not currently found on the standard IOS. CBAC allows for filtering at the application layer to learn about the state of the connection for supported applications, CBAC will create temporary openings in access lists to allow return traffic. An exam ple of where this is useful is for is the FTP data session.

Access-list 100 permit tcp 61.1.1.0 0.0.0.255 any
Access-list 100 permit tcp any 61.1.1.0 0.0.0.255 ack

Rough as this is, it will allow all tcp services that originate from network 61.1.1.0 to anywhere, it also lets the bad guys in with the Ack bit set. The above list will not work for Active FTP because it requires the server on the Internet to establish a connection back to the client on port 20. In the initiation the Syn bit would be set and the packet would be dropped by the above list. You can open port 20 back in but this is just another peep hole for the bad guy to look at. Using CBAC you can do the following.

Ip inspect ftp
Apply this to the interface (with the rest of the config of cou rse) and this is what happens.

An outbound packet from the 61.1. 1.0 network is sent to an FTP server on the Internet, the router will modify access lists on the fly based on the state of the connection. For example host 61.1.1.1 connects to 62.1.1.1 usin g ftp, no dynamic access list is created until the receiver sends back the Syn Ack. The router checks this packet for a match in its state table, if one is found it will dynamically create an access list for that specific connection.

Permit tcp host 62.1. 1.1 eq ftp host 61.1.1.1 eq xxxx

Assuming you are using Active FTP, when you do an ls on the FTP server, the server will try to initiate a connection back to 62.1.1.1 on destination port 20. When this packet arrives at the router it will check the state t able to see if there is an FTP session matching that source and destination current. If one i s found, a dynamic access list will be created for this connection only.

Permit tcp host 62.1.1.1 eq ftp -data host 61.1.1.1 xxxxx
This ACL will stay active for as long as the session is current. If you have enabled auditing you will see a log entry similar to %FW -6-SESS_Audit_trail ftp -data session initiator (62.1.1.1:20) sent 400 bytes responder (61.1.1.1:xxxx) sent 0 bytes on the router or log host.

Automatically building access lists on the fly is still not the golden goose of security but is one more level of defense.

Now we have all the information we need to start configuring the router, first we would stop all unnecessary services and secure acces to the ro uter as outlined previously. This router requires telnet (or preferably SSH if your IOS supports it) access from the internal network only . We have an internal Ciscosecure server that we can use to require authentication using the Tacacs protocol.

Lock do wn remote access to the router

Command	Purpose
Service password -encryption	Encrypt the login Password
Enable secret 0 "password"	Encrypt and set the Enable Password
Banner motd / Authorised Access Only /	Set a banner to display whenever router is acces sed from any port
AAA new -model	Enable AAA
AAA authentication login default Tacacs+	The name "default" when applied to an interface will use the Tacacs+ protocol to authenticate
AAA authentication login no_tacacs none	The name "no_tacacs" when applied t o an interface will not require authentication
Tacacs-server host 10.6.1.20 key Tacacs	Tell the router who to send Tacacs requests to and the key required to query that server. In reality no -one would use the word Tacacs as the key
Access-list 10 permit 61.1.1.34	When applied to an interface only the gauntlet firewall will be able to access
Line con 0	Configure the console port
Login authentication no_tacacs	No authentication required on console
Line aux 0	Configure the aux port
Transport input none	No protocols means no access
Line vty 0 4	Configure the vty ports
access-class 10 in	Only the Gauntlet firewall can access
Transport input telnet	Only use the telnet protocol
Exec-timeout 15 0	Time out the connection after 15 minutes
Login authenticat ion default	Use Tacacs to authenticate anyone coming in on the vty ports

Configure timers and thresholds

ip inspect audit-trail ip inspect tcp synwait-time 30	if 3 way handshake is not complete in 30 seconds drop the connection
ip inspect tcp finwait-time 5	The Dynamic ACL will be removed 5 seconds after a FIN exchange
ip inspect tcp idle-time 3600	The TCP connection will be dropped after 1 hour of inactivity
ip inspect udp idle-time 30	The UDP connection will be dropped after 1 hour of inactivity
ip inspect dns-timeout 5	Any DNS query that is inactive for 5 seconds will be dropped
ip inspect one-minute low 900	If there are more than 900 Half open sessions in one minute the oldest ones will be deleted
ip inspect one-minute high 1100	If the rate of half open sessions exceeds 1100 in one minute the oldest ones will be deleted
ip inspect max-incomplete low 900	If half open sessions are being deleted, the router will stop deleting them at 900
ip inspect max-incomplete high 1100	The total number of half open connection that will cause the router to start deleting
ip inspect tcp max-incomplete host 50 block-time 0	If the number of half open TCP connections to the same destination host exceeds 50, the router will start deleting them

Most of the above timers and thresholds are used to help reduce the impact od DOS attacks such as the SYN flood.

Configure the protocols to inspect and the direction

Ip inspect name outbound smtp	Named list Outbound inspect SMTP
Ip inspect name outbound ftp	Named list Outbound inspect FTP
Ip inspect name outbound HTTP java-list 3	Named list Outbound inspect HTTP and apply access list 3 to this traffic
Ip inspect name inbound smtp	Named list inbound inspect SMTP
Ip inspect name inbound http	Named list inbound inspect HTTP

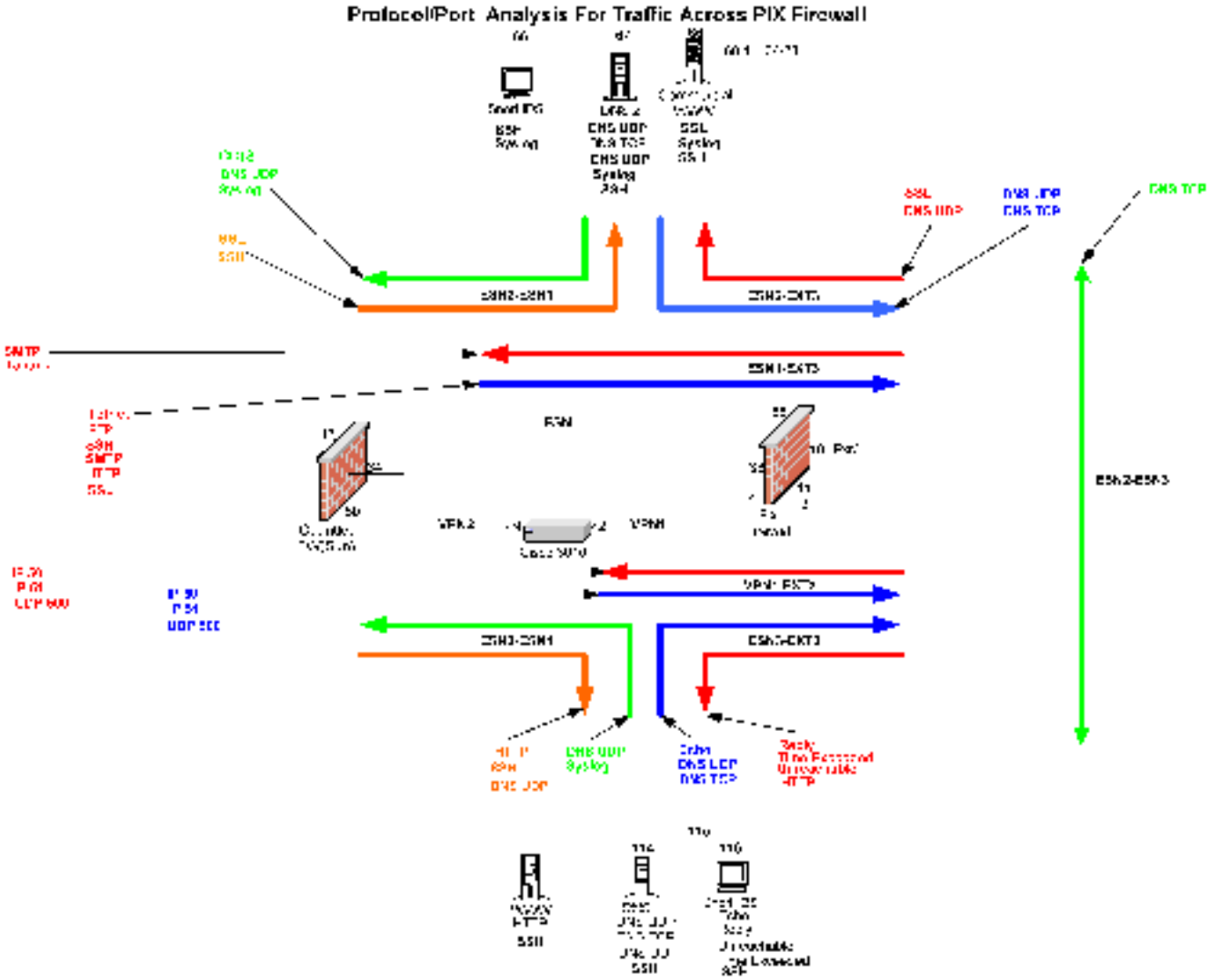
Configure Access lists on the 2600 from Protocol/Port matrix

To and from Gauntlet firewall Access-list 100 permit tcp host 60.1.1.34 any eq ftp	Outbound FTP access from client
Access-list 100 permit tcp host 60.1.1.34 any eq telnet	Outbound Telnet from client
Access-list 100 permit tcp host 60.1.1.34 any eq smtp	Outbound E-mail
Access-list 100 permit tcp host 60.1.1.34 any eq ssl	Outbound HTTPS from client
Access-list 100 permit tcp host 60.1.1.34 any eq http	Outbound HTTP from client
Access-list 100 permit tcp any host 61.1.1.34 eq smtp	Inbound E-mail
To and from DNS1	
Access-list 100 permit tcp host 61.1.1.67 any eq dns	Outbound DNS queries requiring TCP from DNS1
Access-list 100 permit udp host 61.1.1.67 any eq dns	Outbound DNS queries from DNS1
Access-list 100 permit udp any host 61.1.67 eq dns	Inbound DNS queries to DNS1
To and from DNS2	
Access-list 100 permit tcp host 61.1.1.114 any eq dns	Outbound DNS queries requiring TCP from DNS2
Access-list 100 permit udp host 61.1.1.114 any eq dns	Outbound DNS queries from DNS2
Access-list 100 permit udp any host 61.1.114 eq dns	Inbound DNS queries to DNS2
To and from General web server	
Access-list 100 permit tcp any host 61.1.1.115 eq http	Inbound HTTP to general web server
To and from Commercial Web server	
Access-list 100 permit tcp any host 61.1.1.66 eq ssl	Inbound HTTPS only to Fortune Web server
VPN traffic	
Access-list 100 permit 50 any host 61.1.1.42	
Access-list 100 permit 50 host 61.1.1.42 any	
Access-list 100 permit 51 any host 61.1.1.42	
Access-list 100 permit 51 host 61.1.1.42 any	
Access-list 100 permit udp any eq 500 host 61.1.1.42 eq 500	
Access-list 100 permit udp host 61.1.1.42 eq 500 any eq 500	
To and from network test box	
Access-list 100 permit icmp host 60.1.1.116 any echo	Let the test box out for testing network connectivity
Access-list 100 permit icmp any host 60.1.1.116 echo-reply	
Access-list 100 permit icmp any host 60.1.1.116 unreachable	
Access-list 100 permit icmp any host 60.1.1.116 time-exceeded	

Cisco PIX Firewall

The next level of defense is the PIX firewall. This is basically a dumb router specifically designed to manage packet flow at a higher level than a router. It does not make intelligent routing decisions or support any routing protocols so cannot replace a router. Once again the ACL's on this firewall need to be very granular and only permit what is absolutely necessary. Again this has many different hosts and protocols passing through it, so once agai n I will do a graphical representation first.

Pix Firewall protocol/Port analysis



Pix Firewall Protocol/Port Matrix

Traffic on ESN1					
Prot	Src	Dst	Port	Initated By	Description
TCP	61.1.1.34	Any	21	Gauntlet F/W	Outbound FTP from client
TCP	61.1.1.34	Any	22	Gauntlet F/W	Outbound SSH from client
TCP	61.1.1.34	Any	23	Gauntlet F/W	Outbound Telnet from client
TCP	61.1.1.34	Any	25	Gauntlet F/W	Outbound E-mail
TCP	61.1.1.34	Any	80	Gauntlet F/W	Outbound HTTP from client
TCP	61.1.1.34	Any	443	Gauntlet F/W	Outbound SSL from client
UDP	10.6.1.23	61.1.1.67	53	Gauntlet F/W	Outbound DNS from Internal DNS to DNS2
UDP	10.6.1.23	61.1.1.114	53	Gauntlet F/W	Outbound DNS from Internal DNS to DNS1
TCP	61.1.1.66	10.6.1.50	1111	Commercial WWW	Inbound Credit card transactions
TCP	Any	61.1.1.34	25	External	Inbound SMTP
TCP	61.1.1.17	10.6.1.20	49	Cisco 2600	Tacacs Authentication from Cisco 2600 only
UDP	61.1.1.66	10.6.1.22	514	Commercial WWW	Inbound Syslog messages to log server
UDP	61.1.1.67	10.6.1.22	514	DNS2	Inbound Syslog messages to log server
UDP	61.1.1.68	10.6.1.22	514	Snort	Inbound Syslog messages to log server
Traffic on EXT3					
TCP	61.1.1.34	Any	21	Gauntlet F/W	Outbound FTP from client
TCP	61.1.1.34	Any	22	Gauntlet F/W	Outbound SSH from client
TCP	61.1.1.34	Any	23	Gauntlet F/W	Outbound Telnet from client
TCP	61.1.1.34	Any	25	Gauntlet F/W	Outbound E-mail
TCP	61.1.1.34	Any	80	Gauntlet F/W	Outbound HTTP from client
TCP	61.1.1.34	Any	443	Gauntlet F/W	Outbound SSL from client
TCP	61.1.1.67	Any	53	DNS2	Outbound DNS
TCP	61.1.1.114	Any	53	DNS1	Outbound DNS
TCP	Any	61.1.1.66	443	Internet	Inbound SSL to Commercial WWW
TCP	Any	61.1.1.115	80	Internet	Inbound HTTP to WWW
UDP	61.1.1.67	Any	53	DNS2	Outbound DNS
UDP	61.1.1.114	Any	53	DNS1	Outbound DNS
UDP	Any	61.1.1.67	53	External	Inbound DNS to DNS2
UDP	Any	61.1.1.114	53	External	Inbound DNS to DNS1
UDP	61.1.1.42	Any	500	VPN Concentrator	Outbound IPSec
UDP	Any	61.1.1.42	500	VPN Concentrator	Inbound IPSec
IP	61.1.1.42	Any	50	VPN Concentrator	Outbound IPSec
IP	61.1.1.42	Any	51	VPN Concentrator	Outbound IPSec
IP	Any	61.1.1.42	50	External	Inbound IPSec
IP	Any	61.1.1.42	51	External	Inbound IPSec
ICMP	61.1.1.116	Any		Snort	Outbound Echo
ICMP	Any	61.1.1.116		Internet	Inbound Echo-reply to Snort
ICMP	Any	61.1.1.116		Internet	Inbound Time-Exceeded to Snort
ICMP	Any	61.1.1.116		Internet	Inbound Unreachable to Snort
Traffic on VPN1					
IP	61.1.1.42	Any	50	VPN Concentrator	Outbound IPSec
IP	61.1.1.42	Any	51	VPN Concentrator	Outbound IPSec
IP	Any	61.1.1.42	50	External	Inbound IPSec
IP	Any	61.1.1.42	51	External	Inbound IPSec
Traffic on ESN2					
TCP	Any	61.1.1.66	443	Internet	Inbound SSL to Commercial WWW
TCP	61.1.1.34	61.1.1.64	22	Gauntlet F/W	Inbound SSH from Gauntlet
TCP	61.1.1.67	61.1.1.114	53	DNS2	DNS between DNS2 & DNS1
TCP	61.1.1.114	61.1.1.67	53	DNS1	DNS between DNS1 & DNS2
TCP	61.1.1.66	10.6.1.50	1111	Commercial WWW	Inbound Credit card transactions
TCP	10.6.1.50	61.1.1.66	1111	CCTS	Inbound Credit card transactions
UDP	Any	61.1.1.67	53	External	Inbound DNS to DNS2
UDP	61.1.1.66	10.6.1.22	514	Commercial WWW	Inbound Syslog messages to log server
UDP	61.1.1.67	10.6.1.22	514	DNS2	Inbound Syslog messages to log server
UDP	61.1.1.68	10.6.1.22	514	Snort	Inbound Syslog messages to log server
Traffic on ESN3					
TCP	61.1.1.34	Any	22	Gauntlet F/W	Outbound SSH from client
TCP	61.1.1.67	61.1.1.114	53	DNS2	DNS between DNS2 & DNS1

TCP	61.1.1.114	61.1.1.67	53	DNS1	DNS between DNS1 & DNS2
TCP	Any	61.1.1.115	80	Internet	Inbound HTTP to WWW
UDP	61.1.1.114	10.6.1.22	514	WWW	Inbound Syslog messages to log server
UDP	61.1.1.115	10.6.1.22	514	DNS1	Inbound Syslog messages to log server
UDP	61.1.1.116	10.6.1.22	514	Snort	Inbound Syslog messages to log server
ICMP	61.1.1.116	Any		Snort	Outbound Echo
ICMP	Any	61.1.1.116		Internet	Inbound Echo-reply to Snort
ICMP	Any	61.1.1.116		Internet	Inbound Time-Exceeded to Snort
ICMP	Any	61.1.1.116		Internet	Inbound Unreachable to Snort

The problem with specifying individual ports for the outbound access such as permit tcp 61.1.1.34 any eq (21,22,23,80 and 443) is that if an external web server is using a non standard port then access will be denied by this policy. The only way around this is to replace all these statements with a permit tcp host 61.1.1.1.34 any estab. This will work for those sites with non standard ports but permits more ports out. This could have also been solved by running NAT on the Pix. As there is a firewall behind the Pix, control of outgoing ports can be refined there. Another issue arises with HTTP being run on non standard ports is that when gauntlet tries to connect to a non standard port it will do the port translation and try to connect using that port. For e xample if you connect to www.xxx.yyy:8080 then Gauntlet will try to go through the PIX using port 8080, as we did not configure that port in the above table the connection will be dropped by the Pix. To fix this we will need to configure the Gauntlet firewall to "Handoff" all http requests to the internal interface of the Pix (61.1.1.33), doing this will force all HTTP requests to be handed off to the pix on port 80 and the Pix will do the port translation for you.

Configuring the ACL's on the Pix

From the table in 2.4.1 we can make up our Access lists, I will name each list based on the network it services, for example access -list ESN1 will refer to the access to be applied to the ESN1 interface on the PIX (61.1.1 .33). On the PIX you use the nameif command to set up an interface name and security cost

nameif ethernet0 ESN1 security100

this would set the E0 interface to the Highest security Level(most trusted)

nameif ethernet4 EXT1 security 0

This would set the E4 interface to the lowest security level(Untrusted)

All the other interfaces would need to be set between these values to be able to talk to each other using the conduit command for lower value interfaces to communicate with higher value interfaces. Pix su pports SSH and Tacacs for remote access, it would be best to configure this as part of the install.

Depending on how paranoid you are you could just apply one list to the EXT3 interface and let the other service networks talk to each other as they please, doing it on individual interfaces means duplication of ACL's and makes it more complex, but it also means that you have to make the same mistake twice to accidentally let in something unwanted, more complexity but more levels of defense.

NOTE: The following access-lists are shown only for the purpose of describing where I would apply the ACL's, Without access to a Pix firewall I cannot guarantee the ACL's shown are syntactically correct.

ACL's to apply to ESN1	
For the super paranoid apply these to all interfaces	**Non IANA blocking, note the mask is the opposite of cisco IOS, you actually use the subnet mask.**
Access-list ESN1 deny ip 10.0.0.0 255.255.255 any	
Access-list ESN1 deny ip 127.0.0.0 255.0.0.0 any	
Access-list ESN1 deny ip 172.16.0.0 255.240.0.0 any	
Access-list ESN1 deny ip 192.168.0.0 255.255.0.0 any	
Access-list ESN1 deny ip 224.0.0.0 255.240 0.0 any	
Access-list ESN1 permit tcp host 61.1.1.34 any estab	Allows for non standard TCP ports, if you use this you would need to do the same to the routers.
Access-list ESN1 permit udp host 10.6.1.23 host 61.1.1.23 eq 53	Internal DNS queries to Ext DNS (Split DNS)
Access-list ESN1 permit udp host 10.6.1.23 host 61.1.1.114 eq 53	
Access-list ESN1 permit tcp host 61.1.1.66 host 10.6.1.50 eq 1111 log	CCTS transaction port
Access-list ESN1 permit tcp any host 61.1.1.34 eq 25	Outbound SMTP
Access-list ESN1 permit tcp host 61.1.1.17 host 61.1.1.34 eq 49	Inbound Tacacs from C2600
Access-list ESN1 permit UDP 61.1.1.64 255.255.255.240 host 61.1.1.34 eq 514	Syslog for all hosts on Subnet 61.1.1.64
Access-list ESN1 permit UDP 61.1.1.112 255.255.255.240 host 61.1.1.34 eq 514	Syslog for all hosts on Subnet 61.1.1.112
Access-list ESN1 deny IP any any log	
Access-list ESN1 deny icmp any any log	
ACL's to apply to EXT3	
Access-list EXT3 permit tcp host 61.1.1.34 any eq 21	
Access-list EXT3 permit tcp host 61.1.1.34 any eq 22	All outbound from Gauntlet firewall
Access-list EXT3 permit tcp host 61.1.1.34 any eq 23	
Access-list EXT3 permit tcp host 61.1.1.34 any eq 25	
Access-list EXT3 permit tcp host 61.1.1.34 any eq 80	Pix is doing the Port translation so only 80 is needed
Access-list EXT3 permit tcp host 61.1.1.34 any eq 443	
Access-list EXT3 permit tcp host 61.1.1.67 any eq 53	Inbound and Outbound DNS
Access-list EXT3 permit udp host 61.1.1.67 any eq 53	
Access-list EXT3 permit udp any host 61.1.1.67 eq 53	
Access-list EXT3 permit tcp host 61.1.1.114 any eq 53	
Access-list EXT3 permit udp host 61.1.1.114 any eq 53	
Access-list EXT3 permit udp any host 61.1.1.114 eq 53	
Access-list EXT3 permit tcp any host 61.1.1.66 eq 443	Inbound SSL to Commercial WWW
Access-list EXT3 permit tcp any host 61.1.1.114 eq 80	Inbound HTTP to WWW
Access-list EXT3 permit ip any host 61.1.1.42 eq 50	IPSeca
Access-list EXT3 permit ip any host 61.1.1.42 eq 51	
Access-list EXT3 permit udp any host 61.1.1.42 eq 500	
Access-list EXT3 permit ip host 61.1.1.42 any eq 50	
Access-list EXT3 permit ip host 61.1.1.42 any eq 51	
Access-list EXT3 permit udp host 61.1.1.42 any eq 500	
Access-list EXT3 permit icmp host 61.1.1.116 any echo	Traceroute test Machine
Access-list EXT3 permit icmp any host 61.1.1.116 echo-reply	
Access-list EXT3 permit icmp any host 61.1.1.116 unreachable	
Access-list EXT3 permit icmp any host 61.1.1.116 time-exceeded	
Access-list EXT3 deny IP any any log	Deny and log everything else
Access-list EXT3 deny icmp any any log	
ACL's to apply to VPN1	
Access-list VPN1 permit ip any host 61.1.1.42 eq 50	Inbound and Outbound IPSEC
Access-list VPN1 permit ip any host 61.1.1.42 eq 51	
Access-list VPN1 permit udp any host 61.1.1.42 eq 500	
Access-list VPN1 permit ip host 61.1.1.42 any eq 50	
Access-list VPN1 permit ip host 61.1.1.42 any eq 51	
Access-list VPN1 permit udp host 61.1.1.42 any eq 500	
ACL's to apply to ESN2	
Access-list ESN2 permit tcp any host 61.1.1.66 eq 443	
Access-list ESN2 permit tcp host 61.1.1.34 61.1.1.64 255.255.255.240 eq 22	SSH to subnet 61.1.1.64 from Gauntlet
Access-list ESN2 permit tcp host 61.1.1.67 host 61.1.1.114 eq 53	DNS to DNS1
Access-list ESN2 permit tcp host 61.1.1.114 host 61.1.1.67 eq 53	DNS to DNS2
Access-list ESN2 permit tcp host 61.1.1.66 host 10.6.1.50 eq 1111 log	CCTS traffic from WWW to CCTS server
Access-list ESN2 permit tcp host 10.6.1.50 host 61.1.1.66 eq 1111 log	CCTS traffic to WWW from CCTS server
Access-list ESN1 permit UDP 61.1.1.64 255.255.255.240 host 61.1.1.34 eq 514	Syslog for all hosts on Subnet 61.1.1.64
Access-list ESN1 permit UDP any host 61.1.1.67 eq 53	Inbound DNS
Access-list ESN2 deny IP any any log	Deny and log everything else
Access-list ESN2 deny icmp any any log	
ACL's to apply to ESN3	
Access-list ESN3 permit tcp host 61.1.1.34 61.1.1.112 255.255.255.240 eq 22	SSH from Gauntlet to 61.1.1.112 subnet
Access-list ESN3 permit tcp host 61.1.1.67 host 61.1.1.114 eq 53	Zone Transfer DNS2 & DNS1
Access-list ESN3 permit tcp host 61.1.1.114 host 61.1.1.67 eq 53	Zone Transfer DNS1 & DNS2

Access-list ESN3 permit UDP 61.1.1.112 255.255.255.240 host 61.1.1.34 eq514	ESN3 Syslog
Access-list ESN3 permit icmp host 61.1.1.116 any echo	Traceroute Test Machine
Access-list ESN3 permit icmp any host 61.1.1.116 echo-reply	
Access-list ESN3 permit icmp any host 61.1.1.116 unreachable	
Access-list ESN3 permit icmp any host 61.1.1.116 time-exceeded	
Access-list ESN3 deny IP any any log	Deny and log everything else
Access-list ESN3 deny icmp any any log	

Cisco 3015 VPN Concentrator

Partner and Supplier connection

In most cases where business is done on the Internet we are in effect extending our corporate network, you would not put your financial information system in a public area in your company for obvious reasons, what is not so obvious to business managers is that by connecting your company to the Internet with out proper thought is no different t o the above, except many more people can (and will) access it. Using a one time password is one step in the right direction but this is still subject to things like sniffing (if not encrypted), spoofing and man in the mi ddle attacks. What a VPN is trying to achieve is an extension of trust between a remote user or system and your network. As with any remote user you also need to find out who they are (Authenticating), granting them access to defined recourses (Authorizing) and keeping track of what they are doing (Accounting). Authentication is part of the VPN setup, Authorization and Accounting are normally handled by a third party system such as Ciscosecure. If you are able to authenticate yourself in a secure manner th e system will look after the rest and you are then assumed to be as trusted as any user on your corporate network (yeah who trusts them anyway). The difference is that this user is accessing your network via a public network with lots of bad guys on it. Th is is the reason that you would use encryption as an added piece of security to any users accessing your network this way.

Authentication

The primary methods of authentication for VPN's are either passwords or digital certificates. Digital certificates o ffer better security if the certificates are managed correctly because they can verify the identity of the connection. If a digital certificate is stolen or compromised it can be revoked. We will not use the digital certificates primarily for cost reasons, each supplier and partner would need to obtain a certificate from an authority such as Verisign, this coupled with the complexities of deploying a full PKI solution make it an unrealistic option. Using re-usable passwords is not acceptable either as they are usually the weakest link in the chain, users either write them on terminals, use dictionary or obvious passwords. One other type of password that can be used is a one time password such as SecureID, this password is used in conjunction with a shared se cret (password) and changes every 60 seconds. There is a cost to doing this but for the added security it is worth it. We could also setup VPN concentrators at each Partner and supplier but the cost would be prohibitive.

VPN Protocols

PPTP

PPTP is one pr otocol that can be used for a VPN, this is a tunneling protocol and is able to encapsulate other protocols such as IPX within the tunnel. One reason this

is a popular solution is that it is built into NT4.0 and can be downloaded for windows 9X. PPTP was not chosen as the VPN protocol to use because IPSEC is becoming the Defacto standard.

IPSEC

There are a number of steps that need to be taken when establishing a connection with VPN device.

Internet Key Exchange (IKE) . Before any data can be transferred w e need to establish that the connecting system is authorized to connect . This can be done by using names, pre-shared secrets or public key pairs. During this initial setup the two systems must negotiate the encryption algorithm, key length, key life etc. I f both sides of the connection can agree on these parameters and the calling system knows the correct secret then a Security Association (SA) is setup for this connection. A security association is the rules that will be applied to each packet (such as the encryption algorithm and Key parameters) for each connection, these parameters are defined by the VPN administrator, who must setup a policy for each group of users that will be calling the system. The policy for each group will depend on the data being a ccessed and the life of the data. The type of encryption algorithm and key length has a direct impact on the performance and security, so must be chosen wisely. The type of algorithm and key length required will depend on the life of the data being encrypt ed. For example logging into a system and sending an E-mail or two is a short life so even DES would be sufficient (but not necessarily recommended), if the data was to stay encrypted for many years then a stronger algorithm and key length would be used. I KE will come back from time to time and change the keys if the session exceeds the time defined by the policy. All of the communications between partners and suppliers is short term so I would select either DES or 3DES but you may need to check the countri es your suppliers and partners are in for any restrictions on encryption before making a final decision. There are a number of services within the IPSec protocol that need to be negotiated as part of the IKE process, these are the AH and ESP service and th e communication mode.

Authentication Header(AH) ensures that the data within the IP header was not modified and that the origin of the data (source) is correct. AH only provides data integrity, it does not provide any protection for the payload. When using AH both the source and destination must be legal addresses, any changes to the packet going through a NAT device will change the checksum of the packet and will be dropped by the receiving system.

Encapsulating Security Payload(ESP) is the protocol res ponsible for encrypting the data within the packet (payload). Unlike AH, ESP provides limited verification of the source because the entire original packet is encrypted and encapsulated in a normal IP packet and routed as normal. This is the reason that us ing ESP will work if passed through a NAT device. The type of encryption used is determined by the security policy defined by the administrator and implemented using Internet Key Exchange (IKE). The minimum encryption standard that can be used with ESP is DES.

Communication Modes

IPSec support two security modes with a VPN end device such as the Cisco VPN concentrator.

Transport-mode is when the original payload is encrypted and put inside an IP packet. In transport mode the address of the source and destination hosts are not encrypted. Transport mode is usually used for host to host communications and both hosts must have Internet routable addresses. The suppliers and partners will connect to a server in a non routable address range (Private addressing) so it will not be possible for us to use transport mode. When using transport mode both devices must be IPSec compliant.

Transport mode using ESP		
IP Header		Encrypted Payload
Src	Dst	
10.1.1.1	10.7.10.19	Payload

Tunnel-mode is when the entire original packet including the IP headers are encrypted and put inside another packet and routed as normal. Because tunnel mode puts the entire original packet inside another IP packet routing the packet through a NAT will work because when it reaches the destination VPN device, the original packet will not have been modified in any way by the NAT device.

Tunnel Mode using ESP			
		Encrypted Header and Payload	
IP Header		Original IP Header	
Src	Dst	Src	Dst
62.1.1.1	61.1.1.42	10.1.1.1	10.7.10.19 Payload

Looking at the above you can see that using transport mode the destination host will receive an encrypted packet, this means that to use transport mode both ends of the connection must be IPSec compliant. Even if our internal systems did support IPSec and public addresses, we would not want Encrypted traffic going to them as it would defeat the purpose of any IDS systems put in place. This is the primary reason we selected Tunnel mode to connect partners and suppliers using ESP.

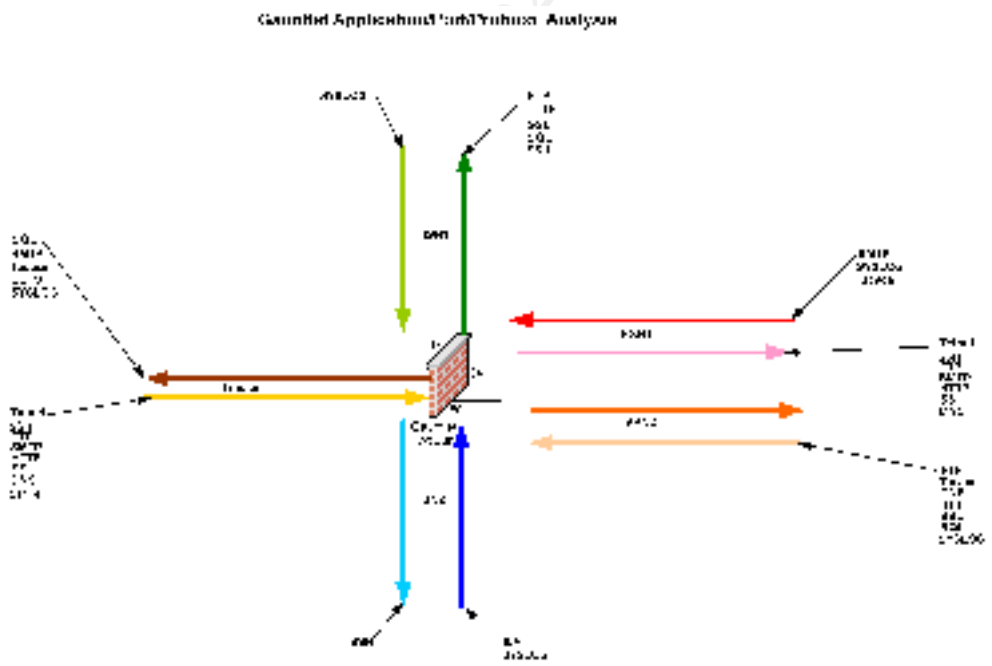
The client software supplied by Cisco also supports authentication authorization and accounting using the Ciscosecure server already installed. The VPN client also support split tunneling so the client will be able to send encrypted packets to the VPN and still be able to send unencrypted packets over the internet, this feature would be disabled. The best client solution would be one that supports remote policy enforcement, this way you can be sure that the user on the remote client has not enabled features or installed software that you consider to be unsafe, you must always keep in mind that the remote machine may have been compromised.

Gauntlet Firewall.

Installation of SunOS 5.8 is a little tricky as you need to remove all components relating to X and CDE. Download the recommend ed patches from sun for the version of OS and apply them. After these two steps are done you need to either run a hardening script such as YASP (www.yassp.org) or you can get a complete set of instructions step by step from Sans (www.sans.org/newlook/resources/hard_solaris.htm#3_). Once this is done run Nmap on the Server and see what services are listening, if you see anything running like LPD,CDE or X ports then you need to start again. Install Gauntlet and the GUI manager on a PC and do the basic setup to allow dedicated machines to access the Firewall configuration via the GUI. Download all the patches for Gauntlet and install them and run Nmap again to see if anything new has appeared. One word of caution in regards to application level firewalls, if you need to apply an OS patch after the firewall is installed you should check with you firewall vendor first, some patches modify the kernel and c an stop your firewall from working (if your lucky) or punch a hole right through the thing. If you are happy with your Nmap scan on the outside interface you can now connect your firewall to the Internet (you didn't install it connected did you??) and use the GUI to configure outbound access without authentication for testing.

Gauntlet firewall unlike a router uses policies rather than Access control lists to control who has access to what recourses, you still need to do a traffic flow analysis to help en sure that you comply with the policy of the company.

Gauntlet Port/Protocol Analysis



Gauntlet Policies

Using the above analysis we can define our policies on the Gauntlet firewall

Application/Port	Source	Destination	Gauntlet Proxy Type	Comment
Policy trusted- For general users on the Internal network				
Telnet	Internal Network	Any	Application	Internal users can telnet anywhere except to the service networks
FTP	Internal Network	Any	Application	Internal users can FTP anywhere except to the service networks
HTTP	Internal Network	Any	Application	Internal users can HTTP anywhere except to ISN1,ISN2 and VPN2
SSL	Internal Network	Any	Application	Internal users can use SSL anywhere except to ISN1,ISN2 and VPN2
Policy services-out --- For outgoing Host to Host services				
DNS	10.6.1.23	DNS1-DNS2	UDP-Plug	Permit the internal nameserver(s) only to do DNS lookups
SMTP	10.6.1.21	10.7.10.11	Application	Only the mail scanner can deliver mail to the firewall for final delivery
CCTS	10.6.1.50	61.1.1.66	TCP-Plug	Replies to the Commercial WWW about Transactions
Policy Services-in ---For incoming Host to Host Services				
Syslog	10.7.10.18	10.6.1.22	UDP-Plug	Syslog from Host IDS on ISN1
Syslog	10.7.10.34	10.6.1.22	UDP-Plug	Syslog from Host IDS on ISN2
Syslog	60.1.1.35	10.6.1.22	UDP-Plug	Syslog from Host IDS on ESN1
Syslog	60.1.1.64	10.6.1.22	UDP-Plug	Syslog from Hosts on network ESN2
Syslog	60.1.1.112	10.6.1.22	UDP-Plug	Syslog from Hosts on network ESN3
Syslog	60.1.1.33	10.6.1.22	UDP-Plug	Syslog from Pix Firewall
Syslog	60.1.1.17	10.6.1.22	UDP-Plug	Syslog from Cisco 2600
SMTP	Any	60.1.1.34	Application	Incoming Mail
CCTS	61.1.1.66	10.6.1.50	TCP-Plug	Queries from Commercial WWW to CCTS
Tacacs	61.1.1.49	10.6.1.20	TCP-Plug	Tacacs Authentication for Partners, Suppliers and administrators
Tacacs	61.1.1.17	10.6.1.20	TCP-Plug	Tacacs Authentication for admin access to Cisco 2600
Policy-Dialin --- For users and admins that dial in				
ICA	100.100.100.0	Met frame	TCP-Plug	General users are assigned PPP addresses in the 100.100.100 network and can only access the Internal Met frame server using the ICA client
ICA	100.100.101.0	Met frame	TCP-Plug	Admins are assigned a 100.100.101 network address and can only access the Met frame server
HTTP	100.100.101.0	10.6.1.20	Application	Admins can connect to the Ciscosecure Web interface
SSH	100.100.101.0	Console-Host	Application	Admins can connect to a predefined console host. This is explained in the appendix but is a dedicated host for accessing router and host consoles.
Policy VPN --- Incoming from partners, suppliers and Admins				
Tacacs	172.16.1,.2,.3	10.7.10.9	TCP-Plug	Tacacs Authentication Suppliers Assigned 172.16.1, Partners 172.16.2, Admins 172.16.3
HTTP	172.16.1.0	10.7.10.19	Application	Http access to Supplier Database
SSL	172.16.1.0	10.7.10.19	Application	SSL access to Supplier Database
FTP	172.16.1.0	10.7.10.19	Application	FTP access to Supplier Database FTP-Put only restrictions can enforced by Gauntlet proxy
HTTP	172.16.2.0	10.6.1.18	Application	HTTP access to Partner Database
SSL	172.16.2.0	10.6.1.18	Application	SSL access to Partner Database
SQL	172.16.2.0	10.6.1.18	TCP-Plug	SQL access to Partner Database
ICA	172.16.3.0	Met frame	TCP-Plug	ICA access to Met frame Server
Telnet	172.16.3.0	Console-Host	Application	Telnet access to Console Host
HTTP	172.16.3.0	10.6.1.20	Application	HTTP access to Ciscosecure Web Interface
Policy Admin ---Administrators need full access to all the service networks, Access to this policy is controlled by IP address				
Telnet	Internal Network	Any	Application	Admins can telnet anywhere
FTP	Internal Network	Any	Application	Admins can FTP anywhere
HTTP	Internal Network	Any	Application	Admins can HTTP anywhere
SSL	Internal Network	Any	Application	Admins can use SSL anywhere
SSH	Internal Network	Any	TCP-Plug	Admins can SSH to anywhere
SQL	Internal Network	Any	TCP-PLUG	Admins can use SQL anywhere

Application and Plug Proxies

The Gauntlet firewall is an application level firewall, this means that if you have an application proxy for a particular service like HTTP then the proxy understands the application and can make decisions based on more than just rules. For example if you use the HTTP proxy and craft a packet so that the data within the packet is not part of the HTTP specification then the firewall will drop and log the packet regardless of the rules. A plug proxy does not do this, a plug understands the protocol but not the application, so will pass the packet if it meets the rules. Before applying any plug proxies to a firewall the risks need to be evaluated first.

Ciscosecure

Ciscosecure is a software product supplied by Cisco Systems, it can be used as a RADIUS compliant server, a Tacacs server or both concurrently. We chose Ciscosecure because the Gauntlet firewall supports Radius whereas the Cisco routers, access servers and Pix firewall support both Radius and Tacacs. Tacacs is the preferred option where supported because it has more features than Radius. The Ciscosecure server can assign IP addresses to individual users and groups as well as different access control lists when using an access server such as the Cisco 3640. Usernames and passwords can be obtained from various systems such as NT,Ldap and NDS, so the product goes a long way to supporting a single sign on. A user can be permitted to have a reusable password if connecting from one network such as the internal one, but need to use a one time password if connecting from an access server or the Internet. Ciscosecure also support database replication so two servers can be setup for redundancy, unfortunately I have not been able to find a way to configure a Cisco router to query a second server if the primary has failed without reconfiguring the router. Ciscosecure provides a further level of defense against configuration errors because it can deny access to a network for a group. If I somehow got a rule wrong and permitted the Suppliers access to the Partners database the Ciscosecure server would not permit access to that network because of it's rules, once again this means that you need to make the same mistake twice before access to the wrong network is permitted. One important point to keep in mind when using any product that claims to Authorize users is that if you permit telnet access to host "A" but not host "B" then after login, the host access takes over. If Host "A" can telnet to Host "B" then Ciscosecure cannot prevent this.

Rule Testing

Testing of the rules for each system is an essential part of the installation to make sure that your filters are working as expected. This process will be covered in the Audit assignment so repeating it here is not necessary.

Assignment 3-Audit Your Security Architecture

Assignment 3 – Audit Your Security Architecture (25 points)
You have been asked to conduct a technical audit of the **primary firewall** (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

1. Plan the audit. Describe the technical approach you recommend to assess th e firewall. 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. Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' 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. Evaluate the audit. Based on your assessment (and refe rring 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 you must annotate/explain the output.

Assumptions

Giac enterprises now has a working solution as proposed in assignment II and has been running for some time now. The system was installed and is being managed by the internal IT department. No changes have been made to the design so my audit will produce the same diagram as shown in 1.5. I have had nothing to do with the original design or implementation. All Nmap scans requested a s part of the design spec have been done and are available.

Cost of Audit

The audit can be broken down into the following phases

- Network design Audit
  Verifying that the design in 1.5 is accurate @0.5 Days
- Hardware/Software Audit
  Identifying t he Router/Firewall hardware/Software versions
  Identifying the Host Hardware/Software versions
  Identify known vulnerabilities in Software Versions @2.0 Days
- Internal Audit
  Scanning and testing any Internal Hosts that are accessible from remote user s
  Scan the entire internal network for unwanted services or Trojan ports @1.0 Days
- Inside out scan
  Local scanning and penetration testing hosts on service networks
  Test what services are available from each Service network both inside and outside @1.0 Days
- Review Firewall Policies
  View and check the policies applied on the firewalls @0.25 Days

- VPN Configuration
  Verify that encrypted traffic only is seen on the outside interface
  Verify that no encrypted traffic is seen on the inside interface
  Verify what services are available from the inside interface @0.5 Days

- Dialin
  Crack the NT passwords to check for poor passwords
  Wardial the entire number range assigned to test for unauthorized modems
  Test what services are available from each dialin g roup @1.25 Days
- Ciscosecure
  Review the Groups, policies and direct access restrictions @0.5 Days
- Write report on findings and recommendations @3.0 Days
- Audit Central Log server @1.0 Days

Total time for the Audit will be 11 days. 5 days have b een allocated as level 1 service at a rate of $150.00/Hour and 6 days at level 2 service costing $250.00/Hour. The total cost for the Audit will be $AU18000.00 The estimated time from the start date to completing the final report will be 30 Days. The info rmation gathering and manual vulnerability assessment can be done during normal business hours, the scanning, war -dialing and actual vulnerability probes will need to be scheduled for a quiet time as determined by the customer once the possible ramifications have been explained.

Before proceeding with any audit the customer must be made aware that the potential exists that confidential data may be obtained and that services may be affected during the Audit. The customer must sign off prior to any audit agr eeing to the above and indemnifying you of any responsibility for lost revenue etc during the audit.

Tools

Vulnerability scanners range from the outrageously expensive Internet Security Scanner (http://www.iss.net) to free scanners such as Nessus (http://www.nessus.org). A vulnerability scanner has a database of known vulnerabilities for as many Operating systems that it knows about. These databases are constantly changing and need to be updated frequently to keep the tools useful. Even with a vulnerability scanner you still need to check sites like http://www.cert.org and http://cve.mitre.org and do a search for any OS, application or service that you are auditing.

Port scanners, well the most widely used one is Nmap so I will stick to that, you can find it at http://www.insecure.org/nmap .

Password crackers l0phtcrack can break any NT password given enough time by generating passwords and applying the same algorithm done by NT to generate the hash. By comparing the two hashes for a match you can eventually get any password. As we are running a legitimate audit we would have access to the domain and therefore the hashed database. While this tool can break any password if you wait long enough we will run the tool in hybrid mode which is like a dictionary attack but with the ability of adding numbers to the words. A ll the audit is intended to do is detect weak passwords not crack every password. L0phtcrack is available from http://www.atstake.com/research/lc3/

Brutus is a remote brute force password cracker, it can be used for brute forcing a system when you find a service such as telnet running. Brutus can be found at http://www.hoobie.net/brutus .

Sniffers free tools like tcpdump (http://www.tcpdump.org) is a basic packet sniffer and is useful for capturing packets based on a command line specification. To use Tcpdump you need to be familiar with the structure of the protocol you want to look at. Tcpdump is useful for seeing what's happening on the other side of a device when certain traffic is sent to the opposite side. For example you may have a rule that filters Echo requests but if you don't send an Echo request and monitor the other side , to make sure it does not appear t hen you are blindly accepting the filter is working. If you need to do higher level packet monitoring with added decoding (saves you a lot of work) you need a commercial sniffer such as the sniffer pro product from http://www.sniffer.com .

War-Dialers are programs designed to dial a range of numbers you determine and look for modems answering. Most organizations have internal faxes so the program you use must be able to distinguish between a fax and a modem. My tool o f choice is Phonesweep (http://www.sandstorm.net) because it is a cost effective tool (average site cost is $3K), it has automated penetration testing and can detect over 200 systems when they answer.

The Audit

Desktop Audit

The desktop audit was carried out over a period of seven days . Nmap was run on the entire internal address range excluding the range designated for the servers. A cron job was scheduled every 6 hours to scan this range, the purpose was to ens ure that every desktop possible was scanned.

A file called desktops was created with the desktop ranges
10.6.20.0/24
10.6.21.0/24
.
.
10.6.50.0/24

the cron job ran every 6 hours and output to a file
Nmap –sS –Su –O –iL /tmp/desktops –oN /tmp/desktops.txt

This will do a TCP and UDP scan, try to fingerprint the operating system and output the results as a normal readable file called desktops.txt in the /tmp directory. Obviously you will need to be sure that sufficient disk space is available first. The file after seven days was very large and needed to have the duplicate scans removed before we could analyse the results. The result was mostly positive as the customer had a standard operating environment (SOE) that required the users to launch applications f rom a NAL screen. If you installed your own OS you could not get access to the applications or upgrades easily and the Helpdesk would not assist for problems on non standard desktops.

Internal Server Audit

The internal server audit revealed a few problem s mainly to do with unpatched NT systems, to many unnecessary services running and no logging of the scans..

```
# Nmap (V. 2.54BETA8) scan initiated Sun Feb 10 15:25:24 2002 as: Nmap -sS -sU -O -oN
exchange -vv exchange.giac
Interesting ports on exchange.giac (10.7.1.5):
(The 3082 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
27/tcp     open        nsw-fe
110/tcp    open        pop-3
119/tcp    open        nntp
135/tcp    open        loc-srv
135/udp    open        loc-srv
137/udp    open        netbios-ns
138/udp    open        netbios-dgm
139/tcp    open        netbios-ssn
143/tcp    open        imap2
161/udp    open        snmp
389/tcp    open        ldap
427/tcp    open        svrloc
427/udp    open        svrloc
563/tcp    open        snews
593/tcp    open        http-rpc-epmap
636/tcp    open        ldapssl
993/tcp    open        imaps
995/tcp    open        pop3s
1083/udp   open        ansoft-lm-1
1084/tcp   open        ansoft-lm-2
1103/udp   open        unknown
1112/tcp   open        msql
2301/tcp   open        compaqdiag
6050/tcp   open        arcserve
6050/udp   open        unknown

TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=3 (Trivial joke)
```

There are a lot of services on this mac hine that should be shutdown as well as some that need investigating such as 1083, a portsearch on http://www.treachery.net/security_tools/ports/lookup.cgi says this port could be th e Anasoft License manager or it could be the winhole Trojan. We can also see that this server has an SNMP service running we will try to use the public community string to see what happens.

Snmpwalk exchange –c public

The resulting file was very large an d contained lost of juicy free information.

```
system.sysDescr.0 = Hardware: x86 Family 6 Model 7 Stepping 2 AT/AT
COMPATIBLE
Software: Windows NT Version 4.0  (Build Number: 1381 Multiprocessor Free
) system.sysObjectID.0 = OID: enterprises.311.1.1.3.1.3
system.sysUpTime.0 = Timeticks: (2421748) 6  :43:37.48 system.sysContact.0
sytem.sysName.0 = Exchange
system.sysLocation.0 =
system.sysServices.0 = 76
interfaces.ifNumber.0 = 2
interfaces.ifTable.ifEntry.ifIndex.1 = 1
interfaces.ifTable.ifEntry.ifIndex.  2 = 2
interfaces.ifTable.ifEntry.ifDescr.1 = MS TCP Loopback interface
interfaces.ifTable.ifEntry.ifDescr.2 = Compaq Ethernet/FastEthernet or
Gigabit NIC
interfaces.ifTable.ifEntry.ifType.1 = softwareLoopback(24)
interfaces.ifTable.ifEntry.ifType.2 = eth  ernetCsmacd(6)
Etc
```

Telnet exchange 25

```
Trying 10.7.1.5...
Connected to exchange.giac.
Escape character is '^]'.
220 exchange.giac ESMTP Server (Microsoft Exchange Internet Mail Service
5.5.2653.13) ready
helo you
250 OK
mail from:<me@here>
250 OK -
rcpt to:<santa@northpole.com
250 OK - Recipient <santa@northpole.com >
data
354 Send data.  End with CRLF.CRLF
i win u loose
.
250 2.0.0 Message received OK
quit


The server is an open relay.

Similar tests were carried out on the rest of the hosts  .
This server along with some others are a hackers dream come true.
```

Logging: The port scans were not recorded in the event log, however any brute forcing attempts using Brutus to the FTP port were logged but not noticed.

Recommendations: Install NTsyslog or a similar product to have all NT servers forward there log information to a central log server. Disable all unnecessary ports on all servers and Investigate the Ports that are left running for possible backdoors. Configure the SMTP service to only accept mail from specific hosts and to/from specific domains. Patch all systems as far as possible and investigate the possibilities of applying the SYSKEY SAM database encryption utility (search Microsoft for Q143475). Investigate the cost effectiveness of installing the commercial version of tripwire onto at least the NT systems. NT security is an art all in itself, a good place to start would be in the Sans reading room at http://rr.sans.org/index.php . Investigate the possibility of putting the Servers on Switched ports and applying ACL's, this will depend on the volume of traffic and the size of the Switch purchased. Investigate the option of installing a host based firewall such as Black Ice defender (http://www.networkice.com/products/blackice_defender.html

Gauntlet Firewall Audit(from Internal Network)

Nmap –sS –sU –O –oN gauntlet gauntlet

```
# Nmap scan initiated Sun Feb 10 16:49:18 2002 as: Nmap -sS -sU -O -oN gauntlet
Interesting ports on gauntlet.giac (10.7.10.11):
(The 3084 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
49/tcp     open        Tacacs
80/tcp     open        http
443/tcp    open        https
1112/tcp   open        msql
53/udp     open        dns
514/udp    open        Syslog
1494/tcp   open        citrix-ica

TCP Sequence Prediction: Class=random positive increments
```

```
Difficulty=72358 (Worthy challenge)

Sequence numbers: 7CD6B8FA 7CDB7F68 7CDD1F7D 7CE09828 7CE3257C 7CE55539 Remote operating
system guess: Sun Solaris 8 early access beta through actual release OS

# Nmap run completed at Sun Feb 10 16:54:24 2002 -- 1 IP address (1 host up) scanned in 306
seconds
```

These ports are as expect ed

Open relay test
Telnet gauntlet 25
Connection closed by foreign host
The firewall would not accept connections from any system other than the mail scanner.
Firewall Policies
The policies on the firewall were checked against the design and appeared to b e correct.

User access, any attempt to use any service such as HTTP and FTP to the Internet was challenged with a username and password.

Logging: The firewall logged all the probes and forwarded them to the log server.

Recommendation: None

ISN1 Audit

There were two machines on this network a Windows 2000 server running the latest Microsoft patches and Microsoft SQL server Version 7.0 with SR1 applied and a Redhat 7.2 Snort sensor.

Windows 2000
(The 3075 ports scanned but not shown below are in state: closed)

Port	State	Service
7/tcp	open	echo
7/udp	open	echo
19/tcp	open	chargen
19/udp	open	chargen
80/tcp	open	h ttp
135/tcp	open	loc -srv
135/udp	open	loc -srv
137/udp	open	netbios -ns
138/udp	open	netbios -dgm
139/tcp	open	netbios -ssn
443/tcp	open	https
1433/tcp	open	ms -sql-s

TCP Sequence Prediction: Class=random positive increments
Difficulty=15974 (Worthy challenge)

Sequence numbers: 194A868E 194B 30DA 194BC2BB 194C82F3 194DC900 194E9BC9
Remote OS guesses: Windows 2000 RC1 through final release, Windows Millennium Edition v4.90.3000 OS Fingerprint:

Snort Sensor
Interesting ports on (10.7.10.18):
(The 3102 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open SSH

TCP Sequence Prediction: Class=random positive increments
Difficulty=6038468 (Good luck!)

The Linux machine only has the SSH port open as expected, attempts to connect to this port from an address other than the nominated IP addresses of the Admin machines failed.

Logging the snort sensor logged all the probes but the NT system did not, this is expected from NT. The snort sensor is doin g it's job.

Recommendation: all ports except HTTP,SSL and ms -sql be closed and authentication be done using the IIS server installed. Logging and scan detection as per the recommendations the Internal server audit .

ISN2 Audit

The snort sensor was scanne d and had the same results as in the ISN1 audit .
The Cisco 3600 scan produced the following results

Interesting ports on 3640.giac (10.7.10.33)
(The 3103 ports scanned but not shown below are in state: closed)
Port State Service
23/tcp open telnet
49/tcp open Tacacs
49/udp open Tacacs
67/udp open bootps
161/udp open snmp

TCP Sequence Prediction: Clas s=random positive increments
Difficulty=2893 (Medium)
Logging As expected the snort sensor detected and logged all the scans but the Cisco logged nothing.

Recommendation: Disable the bootp service and change the community string to something a little more secure than public. Add a deny ip any any and deny udp any any with the log option and configure a logging host.

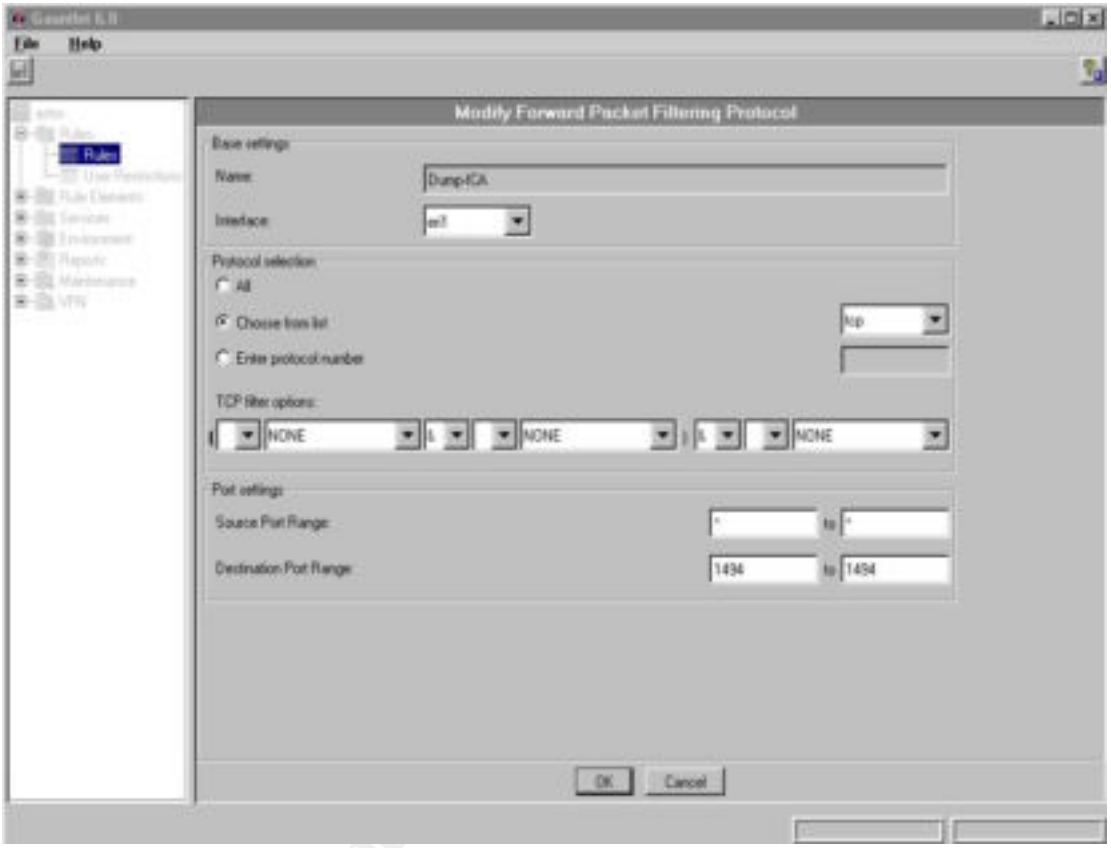
ESN1 Audit

The scan on the Gauntlet firewall produced the same results as the internal scan. The Pix scan said that all ports were closed using various scan options.

Logging Both the Pix and Gauntlet recorded the probes, the Pix however reported far less than Gauntlet.

Recommendation: The Gauntlet firewall is showing services such as the ms -sql and citrix_ica on the outside interface. This is common for this type of firewall as prior to Ver 6.0 the proxy c ould not be configured on an interface basis. Access to that proxy is

determined by the policy on the firewall. Gauntlet does support packet filtering that takes precedence over the proxy rules. My recommendation would be to use the packet filter to drop and log any packets on each interface where a listed service is not required.



The above filter done with the Gauntlet Gui will prevent any packets destined for the Citrix-Ica port on the Eri1 Interface, this is the interface on ESN1. Using Gauntlet v6.0 you can bind some services to a specific interface. If the proxy does not support this then you would need to apply packet filters to each proxy.

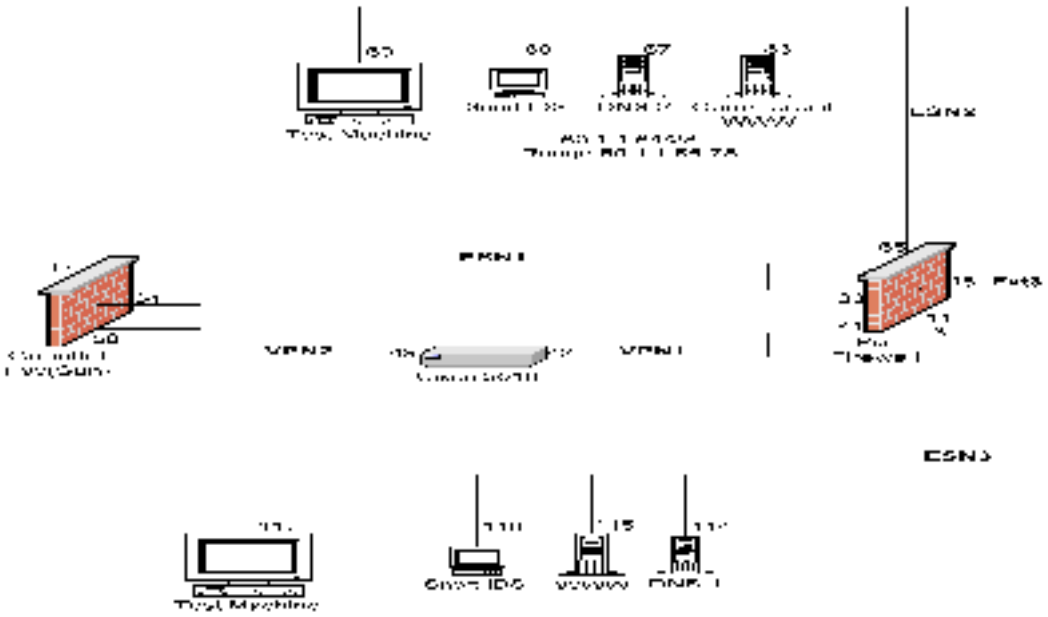
VPN2 and VPN1 A udit

The Snort sensor was tested with the same results as the previous sensors . A tcpdump trace with a partner connected could only see unencrypted traffic as expected. A trace on VPN2 revealed only encrypted traffic was seen.

Logging: The probes produced the results expected in the log server.

Recommendations: A Snort IDS should be placed on the VPN2 network.

ESN1 and ESN2 Audit



The three servers in these networks were running Redhat Linux 7.2 with Netfilter. All services that could be disabled w ere disabled and strict ACL's were applied. The apache server was version 1.3.23, It would be beyond the scope of this audit to verify the apache.conf file setup for problems but a search on bugtraq did not find any vulnerabilities for this version. The OS search did not find any vulnerability for any of the services that were running.

A test machine was installed on each network and the following tests were done

- Nessus scan on each system
  Results
  The Snort sensors refused any connections from the test m achine
  The DNS servers only gave up port 53 UDP and no vulnerabilities were detected.
  The web server on ESN3 only gave up port 80 and an apache/1.3.6 banner.
  The Web server on ESN2 only gave up port 443 and no banner
  Nmap Successfully identified the oper ating system fingerprint.
  All scans were detected and logged
  Any attempts to access the internet were denied and logged
  Any attempts to access the other service networks was denied and logged
  Note The above tests were denied because the IP address of the t est machine was not authorized to access any services.

- Each system in the service networks was disconnected one at a time and the test server assumed the Ip address of the disconnected server. Attempts to access the internet and other service networks was then attempted

  Results
  The test machine was only able to access services as stated in the policy
  No outbound Access to the internet was permitted except when the test machine assumed the IP address of either DNS1 or DNS2.

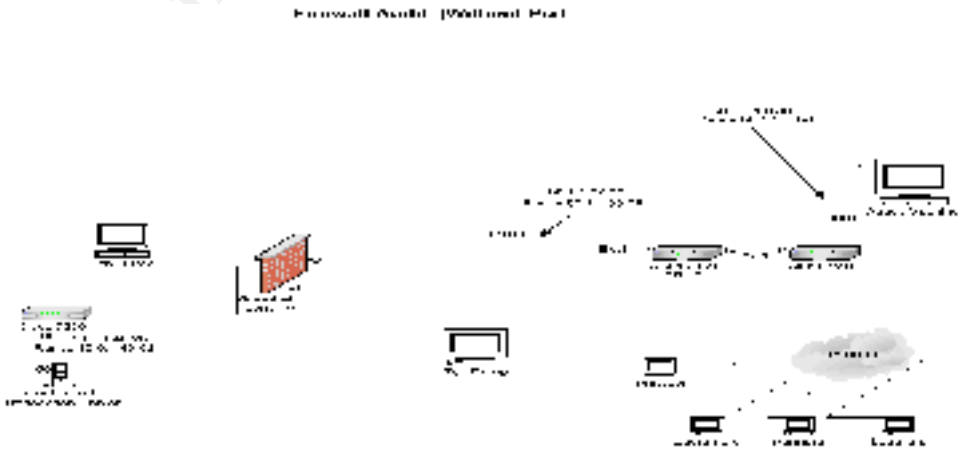
Logging: All logging was as ex pected and forwarded to the log server

Recommendations: Remove the Apache Banner from the Web server

Primary Firewall Audit

In the design we have a Pix firewall in front of a Gauntlet firewall, arguably the Pix would be considered the primary firewall b ecause it is the first line of defence (After the border router). I however believe that the firewall that is protecting the most critical data is the primary firewall. If the Pix or any of the hosts on the service networks attached to the Pix are compromised the loss to the business is revenue. Without revenue most companies cant survive very long, if however the internal systems are compromised and the entire company's secrets and plans are made public and the hosts trashed, most companies will go out of business immediately if not sooner. It is for this reason I have chosen to audit the Gauntlet firewall as the primary for this assignment (besides I have access to a Gauntlet firewall but not a Pix). In a real Audit both firewalls would be audited in the s ame way.

Outside the border router I setup the attack machine with Nessus and Nmap installed,
Inside the Border router I setup a machine running tcpdump, on the internal interface of the Gauntlet firewall was another tcpdump machine.
The attack Machine is 61.1.1.2
The External router address is 61.1.1.3
The internal border router interface address is 61.1.1.17
The Gauntlet firewall outside interface is 61.1.1.34



The following Nmap scans were made and the traffic that passed through the border router and any packets that passed through the firewall was monitored. No useful results from the scans except from the connect scan were expected, the purpose was to check that the filters

on the Border router were functioning as expected. The –P0 option was used in all Nmap scans to prevent the scan from failing.

```
# Nmap (V. 2.54BETA25) scan initiated Tue Feb 12 11:09:18 2002 as: Nmap -sT -sU -vv -P0 -oN 61.1.1.34.nmap.connect.scan.txt
61.1.1.34
Interesting ports on 61.1.1.34 (61.1.1.34):
(The 3129 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
```

Connect scan

```
# Nmap run completed at Tue Feb 12 11:20:38 2002 -- 1 IP address (1 host up) scanned in 680 seconds
```

Tcpdump From ESN1

```
10:25:32.421334 61.1.1.2.48350 > 61.1.1.34.smtp: S 3593455717:3593455717(0) win 5840 <mss 1460,sackOK,timestamp 799577[|tcp]>
(DF)
10:25:32.421769 61.1.1.34.smtp > 61.1.1.2.48350: S 2040897307:2040897307(0) ack 3593455718 win 24616 <nop,nop,timestamp
223804923 799577,nop,[|tcp]> (DF)
10:25:32.443432 61.1.1.2.48350 > 61.1.1.34.smtp: . ack 1 win 5840 <nop,nop,timestamp 799581 223804923> (DF)
10:25:32.450832 61.1.1.2.48350 > 61.1.1.34.smtp: R 1:1(0) ack 1 win 5840 <nop,nop,timestamp 799581 223804923> (DF)
```

The 3 way handshake to the SMTP port on the Gauntlet firewall were the only packets detected

No packets were received on the internal interface of the Gauntlet firewall

Border Router Logs(snipped)

```
Feb 12 11:09:28 61.1.1.17 1087169: *Mar 6 20:45:45: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(46936) > 61.1.1.34(1549),
1 packet
Feb 12 11:09:30 61.1.1.17 1087186: *Mar 6 20:45:48: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(46940) > 61.1.1.34(2600),
1 packet
Feb 12 11:09:33 61.1.1.17 1087201: *Mar 6 20:45:51: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(46946) > 61.1.1.34(1549),
1 packet
Feb 12 11:09:36 61.1.1.17 1087216: *Mar 6 20:45:54: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(46936) > 61.1.1.34(1549),
1 packet
```

The router detected and dropped any packet that did not match the criteria

Gauntlet Firewall Logs

```
Feb 12 10:08:34 gauntlet.giac Csmap[29036]: [ID 174344 daemon. notice] permit host=nodnsquery/61.1.1.2
Feb 12 10:08:34 gauntlet.giac Csmap[29036]: [ID 898782 daemon. notice] nuisance logging is ON
Feb 12 10:08:34 gauntlet.giac Csmap[29036]: [ID 205199 daemon. notice] connection OK nodnsquery/61.1.1.2 passed nuisance check
Feb 12 10:08:34 gauntlet.giac Csmap[29036]: [ID 325624 daemon. notice] exit host=nodnsquery/61.1.1.2 messages=0 bytes=0
```

The Gauntlet firewall detected a completed connection to the SMTP proxy

SYN Scan

```
# Nmap (V. 2.54BETA25) scan initiated Tue Feb 12 11:24:46 2002 as: Nmap -sS -sU -vv -P0 -oN 61.1.1.34.nmap.syn.scan.txt
61.1.1.34
Interesting ports on 61.1.1.34 (61.1.1.34):
(The 3129 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
```

Tcpdump From ESN1

```
10:44:20.167047 61.1.1.2.60626 > 61.1.1.34.smtp: S 1318752675:1318752675(0) win 4096
10:44:20.167382 61.1.1.34.smtp > 61.1.1.2.60626: S 2873507420:2873507420(0) ack 1318752676 win 24656 <mss 1460> (DF)
10:44:20.308832 61.1.1.2.60626 > 61.1.1.34.smtp: R 1318752676:1318752676(0) win 24656
10:44:20.315042 61.1.1.2.60626 > 61.1.1.34.smtp: R 1318752676:1318752676(0) win 0 (DF)
```

No packets were received on the internal interface of the Gauntlet firewall

Router Logs(Snipped)

```
Feb 12 11:24:56 61.1.1.17 1094681: *Mar  6 21:01:14: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(60626) >
61.1.1.34(951), 1 packet
Feb 12 11:25:02 61.1.1.17 1094701: *Mar  6 21:01:20: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(60627) >
61.1.1.34(951), 1 packet
Feb 12 11:25:14 61.1.1.17 1094740: *Mar  6 21:01:32: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(60626) >
61.1.1.34(1671), 1 packet
Feb 12 11:25:20 61.1.1.17 1094810: *Mar  6 21:01:38: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(60627) >
61.1.1.34(1671), 1 packet
```

Once again the router dropped packets as expected

Gauntlet did not detect the connection to the SMTP proxy, my assumption here is that the 3 way handshake must be completed for this to be logged.

Fin Scan

```
# Nmap (V. 2.54BETA25) scan initiated Tue Feb 12 11:46:28 2002 as: Nmap -sF -sU -vv -P0 -oN 61.1.1.34.nmap.fin.scan.txt 61.1.1.34
All 3130 scanned ports on 61.1.1.34 (61.1.1.34) are: filtered

# Nmap run completed at Tue Feb 12 12:49:22 2002 -- 1 IP address (1 host up) scanned in 3774 seconds
```

Tcpdump From ESN1

```
11:07:12.586035 61.1.1.2.62913 > 61.1.1.34.smtp: F 0:0(0) win 1024
11:07:18.504945 61.1.1.2.62914 > 61.1.1.34.smtp: F 0:0(0) win 1024
```

The Fin scan did not get a reply from the firewall

No packets were received on the internal interface of the Gauntlet firewall

Border Router Logs

```
Feb 12 11:46:49 61.1.1.17 1103911: *Mar  6 21:23:07: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(62913) >
61.1.1.34(2025), 1 packet
Feb 12 11:47:20 61.1.1.17 1104084: *Mar  6 21:23:37: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(62914) >
61.1.1.34(540), 1 packet
Feb 12 11:47:26 61.1.1.17 1104110: *Mar  6 21:23:43: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(62913) >
61.1.1.34(1988), 1 packet
Feb 12 11:48:25 61.1.1.17 1104506: *Mar  6 21:24:44: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(62913) >
61.1.1.34(344), 1 packet
Feb 12 11:48:37 61.1.1.17 1104583: *Mar  6 21:24:56: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(62913) >
61.1.1.34(1987), 1 packet
```

The router dropped packets as expected

Gauntlet Firewall Log reported nothing

```
# Nmap run completed at Tue Feb 12 11:44:15 2002 -- 1 IP address (1 host up) scanned in 1169 seconds
```

Xmas scan

```
# Nmap (V. 2.54BETA25) scan initiated Tue Feb 12 12:51:26 2002 as: Nmap -sX -sU -vv -P0 -oN 61.1.1.34.nmap.Xmas.scan.txt
61.1.1.34
All 3130 scanned ports on 61.1.1.34 (61.1.1.34) are: filtered

# Nmap run completed at Tue Feb 12 13:54:21 2002 -- 1 IP address (1 host up) scanned in 3775 seconds
```

Tcpdump From ESN1

```
12:11:23.487129 61.1.1.2.47024 > 61.1.1.34.smtp: FP 0:0(0) win 3072 urg 0
12:11:29.502621 61.1.1.2.47025 > 61.1.1.34.smtp: FP 0:0(0) win 3072 urg 0
```

The Xmas scan did not get a reply from the firewall

No packets were received on the internal interface of the Gauntlet firewall

Router Logs(Snipped)

```
Feb 12 12:51:42 61.1.1.17 1130178: *Mar 6 22:28:00: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(47025) >
61.1.1.34(1667), 1 packet
Feb 12 12:53:25 61.1.1.17 1130634: *Mar 6 22:29:42: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(47024) >
61.1.1.34(444), 1 packet
Feb 12 12:54:07 61.1.1.17 1130827: *Mar 6 22:30:25: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(47025) >
61.1.1.34(913), 1 packet
Feb 12 12:54:18 61.1.1.17 1130897: *Mar 6 22:30:37: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(47025) >
61.1.1.34(694), 1 packet
```

The router dropped packets as expected

Gauntlet Firewall Log reported nothing

Null Scan

```
# Nmap (V. 2.54BETA25) scan initiated Tue Feb 12 14:02:33 2002 as: Nmap -sN -sU -vv -P0 -n -oN 61.1.1.34.nmap.null.scan.txt
61.1.1.34
All 3130 scanned ports on  (61.1.1.34) are: filtered

# Nmap run completed at Tue Feb 12 15:05:34 2002 -- 1 IP address (1 host up) scanned in 3781 seconds
```

Tcpdump From ESN1

```
13:35:25.907177 61.1.1.2.59443 > 61.1.1.34.smtp: . win 4096
13:35:31.914413 61.1.1.2.59444 > 61.1.1.34.smtp: . win 4096
```

The Null scan did not get a reply from the firewall

No packets were received on the internal interface of the Gauntlet firewall

Router Logs(Snipped)

```
Feb 12 14:02:56 61.1.1.17 1158103: *Mar 6 23:39:14: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59443) >
61.1.1.34(171), 1 packet
Feb 12 14:03:01 61.1.1.17 1158124: *Mar 6 23:39:20: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59444) >
61.1.1.34(171), 1 packet
Feb 12 14:03:07 61.1.1.17 1158161: *Mar 6 23:39:26: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59443) >
61.1.1.34(2047), 1 packet
Feb 12 14:03:19 61.1.1.17 1158311: *Mar 6 23:39:38: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59443) >
61.1.1.34(970), 1 packet
Feb 12 14:03:25 61.1.1.17 1158384: *Mar 6 23:39:44: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59444) >
61.1.1.34(970), 1 packet
```

The router dropped packets as expected

Gauntlet Firewall Log reported nothing

The Next step was to run a scan on the Gauntlet Firewall using Nessus

Results

```
61.1.1.34|smtp (25/tcp)|10324|
REPORT There is a buffer overflow when this MTA is issued the 'HELO' command issued by a too long argument.
This problem may allow an attacker to execute arbitrary code on this computer, or to disable your ability to send
or receive emails.

Solution : contact your vendor for a patch.
Risk factor : High

61.1.1.34|smtp (25/tcp)|10256|
REPORT There is a buffer overflow when this MTA is issued the 'HELO' command issued by a too long argument.
This problem may allow an attacker to execute arbitrary code on this computer, or to disable your ability to send
```

or receive emails.

Solution : contact your vendor for a patch.
Risk factor : High
CVE : CAN-1999-0284

61.1.1.34|smtp (25/tcp)|10353|
REPORT It was possible to perform a denial of service against the remote Interscan SMTP server by sending it a special long HELO command. This problem allows a cracker to prevent your Interscan SMTP server from handling requests.

Solution : contact your vendor for a patch.
Risk factor : Serious

61.1.1.34|smtp (25/tcp)|10050|
REPORT There is a buffer overflow when this MTA is issued the 'HELO' command
issued by a too long argument (12,000 chars) This problem may allow an attacker to
execute arbitrary code on this computer, or to disable your ability to send or receive emails.

Solution : contact your vendor for a patch.
Risk factor : High
CVE : CAN-2000-0042;

61.1.1.34|smtp (25/tcp)|10047|
REPORT There seems to be a buffer overflow in the remote SMTP server when the server is issued a too long argument to the 'MAIL FROM' command, like :MAIL FROM: AAA[...]AAA@nessus.org Where AAA[...]AAA contains more than 8000 'A's.
This problem may allow a cracker to prevent this host to act as a mail host and may even allow him to execute arbitrary code on this system.

Solution : Contact your vendor for a patch
Risk factor : High

61.1.1.34|smtp (25/tcp)|10249|INFO|
The remote SMTP server answers to the EXPN and/or VRFY commands.
The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.
Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

Solution : if you are using Sendmail, add the option O PrivacyOptions=goaway in /etc/sendmail.cf.

Risk factor : Low;CVE : CAN-1999-0531;

61.1.1.34|smtp (25/tcp)|10260|INFO|
The remote STMP server seems to allow remote users to send mail anonymously by providing a too long argument to the HELO command (more than 1024 chars). This problem may allow bad guys to send hate mail, or threatening mail using your server and keep their anonymity.

Risk factor : Low.
Solution : If you are using Sendmail, upgrade to version 8.9.x. If you do not run Sendmail, contact your vendor.
CVE : CAN-1999-0098

61.1.1.34|smtp (25/tcp)|10263|NOTE|
Remote SMTP server banner gauntlet.giac SMTP/smap Ready.
214-Commands-HELO MAIL RCPT DATA RSET
NOOP QUIT HELP VRFY EXPN

61.1.1.34|general/tcp|10336|NOTE|
Nmap found that this host is running Sun Solaris 8 early access beta through actual release;

Router logs during Nessus scan<snipped>

Feb 12 14:02:56 61.1.1.17 1158103: *Mar 6 23:39:14: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59443) > 61.1.1.34(171), 1 packet
Feb 12 14:03:01 61.1.1.17 1158124: *Mar 6 23:39:20: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59444) > 61.1.1.34(171), 1 packet
Feb 12 14:03:07 61.1.1.17 1158161: *Mar 6 23:39:26: %SEC-6-IPACCESSLOGP: list 100 denied tcp 61.1.1.2(59443) > 61.1.1.34(2047), 1 packet
Feb 12 15:10:24 61.1.1.17 1179532: *Mar 7 00:46:42: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 61.1.1.2 > 203.34.41.34 (3/3), 1 packet
Feb 12 16:53:03 61.1.1.17 1214345: *Mar 7 02:29:21: %FW-3-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (61.1.1.2:57229)
Feb 12 16:53:03 61.1.1.17 1214346: *Mar 7 02:29:21: %FW-6-SESS_AUDIT_TRAIL: smtp session initiator (61.1.1.2:57229) sent 17 bytes – responder
Feb 12 16:57:47 61.1.1.17 1216066: *Mar 7 02:34:06: %FW-3-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (61.1.1.2:57238)
Feb 12 16:57:48 61.1.1.17 1216067: *Mar 7 02:34:06: %FW-6-SESS_AUDIT_TRAIL: smtp session initiator (61.1.1.2:57238) sent 0 bytes -- responder (61.1.1.34:25) sent 39 bytes
Feb 12 17:06:37 61.1.1.17 1218378: *Mar 7 02:42:55: %FW-3-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (61.1.1.2:57253)

Feb 12 17:06:37 61.1.1.17 1218379: *Mar 7 02:42:55:%FW-6-SESS_AUDIT_TRAIL: smtp session initiator (61.1.1.2 57253) sent 14 bytes -- responder (61.1.1.34:25) sent 0 bytes
Feb 12 17:06:37 61.1.1.17 1218380: *Mar 7 02:42:55:%FW-6-SESS_AUDIT_TRAIL: smtp session initiator (61.1.1.2 57254) sent 0 bytes -- responder (61.1.1.34:25) sent 39 bytes
Feb 12 17:09:06 61.1.1.17 1218987: *Mar 7 02:45:24:%FW-3-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (61.1.1.2 57255)
Feb 12 17:09:06 61.1.1.17 1218989: *Mar 7 02:45:24:%FW-6-SESS_AUDIT_TRAIL: smtp session initiator (61.1.1.2 57256) sent 0 bytes -- responder (61.1.1.34:25) sent 39 bytes
Feb 12 17:09:07 61.1.1.17 1218993: *Mar 7 02:45:24:%FW-6-SESS_AUDIT_TRAIL: smtp session initiator (61.1.1.2 57257) sent 0 bytes -- responder (61.1.1.34:25) sent 39 bytes

The router dropped packets as expected, there are also log entries for the SMTP connections. These alerts appear when an invalid SMTP command is issued and terminates the connection. This shows that the SMTP inspection is working.

Logging: All logs were sent to the Syslog server as expected but the time stamps are not correct. One system appears to be running in daylight savings time and the others are not. The cisco router is even showing the wrong month.

Recommendation: The SMTP problems appear to be quite serious, however the firewall has the latest patches applied for both the OS and Gauntlet. I would recommend that the report be forwarded to the support company for clarification/explanation. At least one NTP central time server should be installed and all systems should query this system for time. The Router ACL's appear to be functioning as expected however fragmented packets did pass through the router, although no extra information was gleaned using this method. I would also recommend that an IDS be installed on this network.

Social Engineering

This is only a scenario of a possible way to social engineer a site, it is obviously fictitious but is here as it should be part of an audit.
A visit to the Giac web site revealed lots of useful information such as the CEO's name and Email address along with departments, contact names and telephone NO's. Using this information I found that the IT helpdesk was a 24X7 operation. I called on a Saturday on purpose expecting that only a junior support person would be on hand. I then called the main switch telephone NO and asked for IT services, I then had the following conversation.

ME: Hi, my name is Josephine smith, I am john smith's (the CEO) new temporary personal assistant while she is on holidays. John has just called me and said that I need to finalize a PowerPoint presentation for him by Monday morning but my dialin account is not working. I really need to get this done today can you help me out please.

Helpdesk: What's your user ID
ME: JosieS (got that from everyone's E-mail address)
Helpdesk: Your dialin account looks OK what's the problem.
ME: It keeps asking me for my password
Helpdesk: Are you sure you are using the right password
ME: Well I am only new and I have not dialed in before so I am not sure, can I change it to something else.
Helpdesk: I cant do that unless you come here in person
ME: I live 30 miles away I cant come all that way just to do that, if I don't get this done John will be very upset with IT services.
Helpdesk: But I am not allowed to do this if you are not here.
ME: look me up in the phone book or the Intranet you will see that I am on ext 5123.
Helpdesk: Yes you are here but I cant do it over the phone.

ME: OK, can I have your name please, I will call John back and tell him that you wont help me get this presentation done, I don't think he is going to be very happy.
Helpdesk: I am sorry about this my name is Tony smith (lots of smith's at Giac)

A few Minutes later the phone rings.

Partner in crime(male): It John Smith here, is Tony smith there please.
Helpdesk: Speaking Mr Smith
Partner in crime: I understand that my secretary Jose phine is having problems with her dialin account
Helpdesk: Yes she just called
Partner in crime: Look I really need her to make these changes, can you do whatever is needed to get her working.
Helpdesk: Yes Mr Smith now that you have authorized it.
Partner in crime: Ok I will get her to call back

Call back
…..
Helpdesk: OK what do you want your password changed to.

Etc etc

ME: OK thanks now I just want to confirm that the number I am calling is correct, it 555 - 11256 (got that from the main switch NO and guessed the range)
Helpdesk: Oh maybe that's the problem the number is 555 -32000
You get the point

While the above may or may not have worked in reality there is a lot of information on web sites that should not be there, If I found a site such as this t hen I would recommend that the Email address be different from the username (Email=Joesphine_smith Username - JoesP) and that publicly available information is approved by management prior to publication. Also Helpdesk procedures need to be very clear so tha t the helpdesk operator knows that they cannot be disciplined for following procedure. If this is clear then intimidation from a senior person real or not, is not possible.

Report

NOTE: This is just a summary of the findings in the full report all of the problems and recommendations listed throughout the audit would be included.

The review conducted tested the major operating systems and networking components used to support the administrative functions of Giac enterprises. The configuration of the appli cations running on these systems was outside the scope of this audit. The security environment within GIAC enterprises is not within the range expected for most companies with external connections.

As is common with many organizations Giac enterprises is skewed towards internal users, the outside world has few points of entry and those points are protected within the range expected. Internal users will always be the largest exposure and the audit revealed that the procedures to monitor this group are outsi de of what is expected.

Although several exposures were noted only one could cause significant loss, a poorly configured administrator account on the NT Domain controller. I would

recommend that a full time resource be allocated to the role of Security Manager, this person should have the day to day responsibilities for the creation and implementation of security policies procedures and tools.

KEY Findings

The internal workstations were mainly Win95X and provide no security to application data stored on them. Files or data on these systems are vulnerable and passwords are passed in clear text, so are vulnerable to sniffing by tools such as l0phtcrack.

The Windows NT primary Domain controller had an easily guessable password and another server had it's registry available to remote users.

All NT servers were not patched to the latest security patches and are vulnerable to DOS attacks as can be found on the Microsoft web site www.microsoft.com/technet/security/default.asp

The Unix systems were mixed with the servers on the service networks being very secure to some internal servers running old Operating Systems without any patches. Most are running default installation services such as Sendmail and POP that are unnecessary.

Networks security provides the greatest internal exposure as any device can connect and obtain an IP address via DHCP without any verification or authentication. Where possible ports should be disabled or where permanent desktops are situated the port locked to that MAC address.

Procedures The service network hosts have all been configured to log messages to a central log server but most internal ones do not. During brute force scans any logging that did take place was not noticed because there is no resource or procedure to review them on a regular basis.
No procedures are in place for the identification and installation of security hotfixes from application or OS vendors. No procedures exist for the obfuscation of plain text passwords on systems where supported. While a procedure existed for users requesting password changes it was not difficult to circumvent this procedure with intimidation. A very clear policy on any user changes needs to be written and implemented. No procedure existed to track breaches should they be identified. No procedure exists for remote access systems setup by users.

Remote Access The dialin system employs re-usable passwords and is an area that could be easily exploited using brute force software. As a minimum the network access server (NAS) needs to be monitored very closely and account lockout enforced, with follow on all locked out accounts. The Wardial revealed a number of modems requesting authentication that were not in the range allocated to the NAS, these numbers need to be traced and their purpose identified as a matter of urgency.

Logging from the service networks was fully implemented and operational. Internal hosts did not do any central logging at all. The timestamps on a number of systems was of by months in some cases, this makes cross referencing the logs impossible. The NT event logs have effectively been disabled probably in an effort

to conserve disk space. NTsyslog or a similar product should be installed and logging turned back on to a central log server. All systems should have their time synchronized. http://www.sabernet.net/software/ntsyslog_src.zip

Gauntlet firewall: The SMTP vulnerability need s to be investigated to ensure that a real buffer overflow or DOS does not exist.

Redundancy. A failure of either firewall will have a significant impact on business. Both the PIX and Gauntlet support a failover option and this could be implemented but at a significant cost. The impact on business and associated costs would need to be evaluated to justify this expense. I have provided two alternate designs that will provide redundancy, the first one will require manual intervention , the second one is autom atic, but takes about 30 seconds for failover to activate.

Low Cost Redundant Design

The Commercial web server has been moved to the ESN3 interface on the PIX firewall and a mirror of both web servers would need to be purchased . In the event that the PIX fails, you would need to patch the cable from the switch to the Cisco 2600 and change the IP address accordingly. The ACL's would not need to be modified as the hosts that are not down would still be in the current ACL's. All DNS and Web traffic would be diverted through the Gauntlet firewall. Email would be an issue so I would recommend that the DNS servers be configured as the MTA's and secured accordingly. Some modifications to the current PIX ACL's and Gauntlet policies would need to be done prior to m oving the service networks.

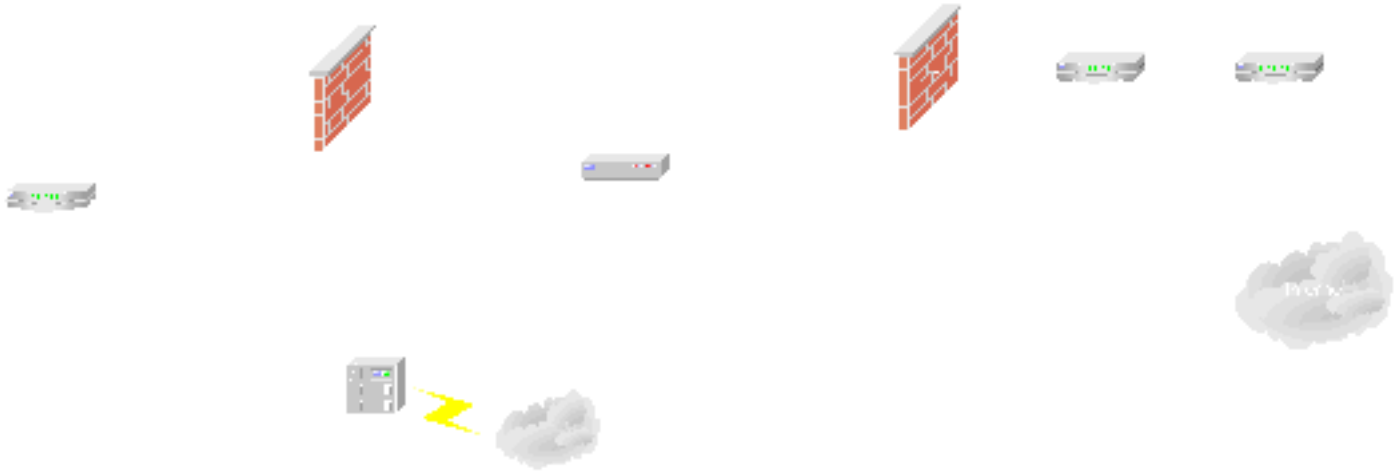
In the event of the Gauntlet firewall failing you would need to patch a cable from the 7200 to the supplier database network and patch from the VP N switch to the 7200. Configure these interfaces to the same IP addresses as the current firewall and things will continue to run. If you need Dialin redundancy as well then a similar option with another switch to the 7200 could be used or the 3600 could be positioned as in the second design. Obviously if the 3600 fails then Dialin acc ess is lost.

This is obviously just an emergency patch and would not be used long term, a detailed analysis would need to be done first to ensure that nothing has been missed. This would require quite a bit of re -configuration and testing to be done. Obviously the redundant firewalls are the better option as the failover is automatic and basically transparent to the users, this design is only an option if money is tight.

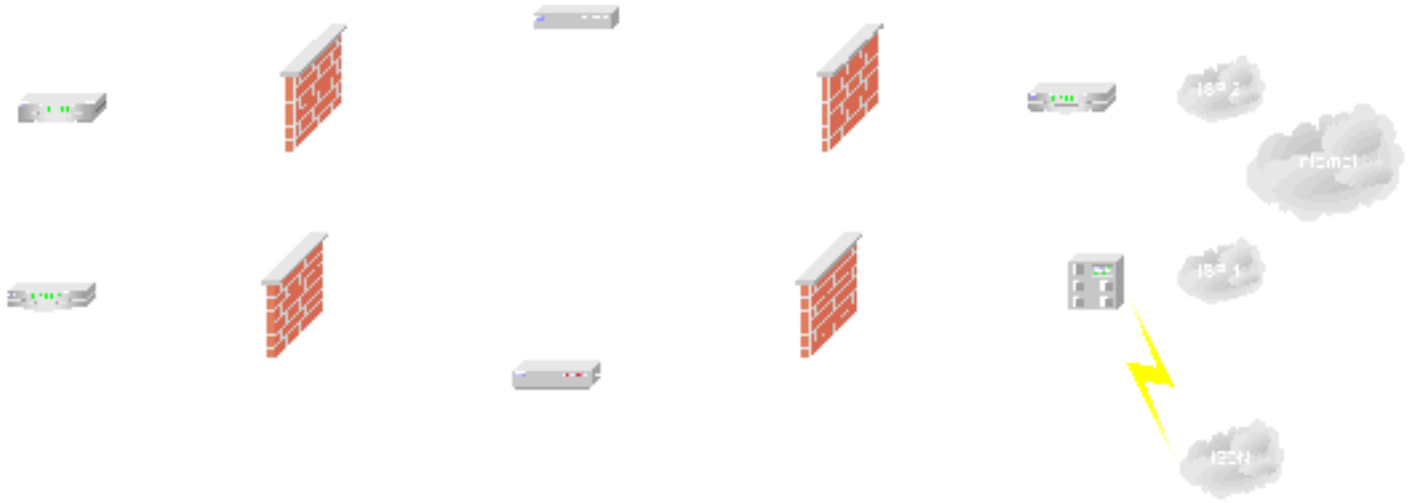
High cost Redundant Design

As with the previous design the Web server s are mirrored and ESN2 moved an interface on the Gauntlet firewall. By moving this service network to the Gauntlet firewall each service network is available for use all the time so mirroring and DNS updates can take place . When a failure occurs, one service network will become unavailable but operations are not affected . You will see by the design a number of switches need to be purchased, two additional firewalls with failover software/hardware and a second ISP . The basic design is still there and this could be implemented with minimal downtime to the current system.

Low cost redundant design



High cost Redundan t design



Design Under Fire

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.giac .org/GCFW.php) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Research and design two of the following three types of attacks against the architecture:

1. An attack against the firewall itself. Researc h and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design. Choose **one** of the vulnerabilities, design an attack based on the vulnerability, and explain the results of running that attack against the fi rewall.
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.

Chosen design

If you are so inclined that you want to break into a network that you are not authorized to do, you would not normally have the luxury of having the design in front of you. I reviewed many other practicals and noticed that nearly all of them tried to attack the firewall directly from the internet. Th e only problem I see with this approach is that a firewall is more likely to be the one piece of hardware/Software that has been scrutinized the most, and as such is more likely to have probes noticed, and less likely to be compromised than systems on a se rvice network. It's even harder to crack an appliance type firewall that does not run any services, on an operating system that nobody knows about. The common belief is that access to systems on a service network is far more restricted because they are pro tected by the firewall. This is a good assumption, the chances of you finding a router letting in traffic to the Imap port and the firewall permitting the same is probably very low. If you do happen to find one though then it is likely that there is a lot more open the administrator does not know about. It is highly likely that the external interface of the firewall is very hard, but the inside interface is a little softer, after all no bad guys should be on your inside interface should they. With the bugs that have been found in Microsoft outlook in recent times an attack with a high probability of success would be to use E -mail with some active content . The aim would be to send the E-mail to an unsuspecting user such as a non IT person and compromise that system by installing a program such as HTTPtunnel (www.nocrew.org/software/httptunnel.html), then tunnel back through the firewall. I wasn't able to find any code to install a Trojan using E -mail but I know that it is around, so I will stick to a more conventional method and try and compromise a host on a service network and use this to attack the firewall from a hopefully softer side. I have chosen Frank Meylan's practical for a couple of reason s. (http://www.giac.org/practical/Frank_Meylan_gcfw.zip)

- It offers services such as DNS,WWW,FTP and POP from the outside
- The Internal network is connected via a Gauntlet firewall throu gh the network of the host that I hope to compromise. This will give me a great place to sniff the network looking for things like telnet access to the outside firewall.

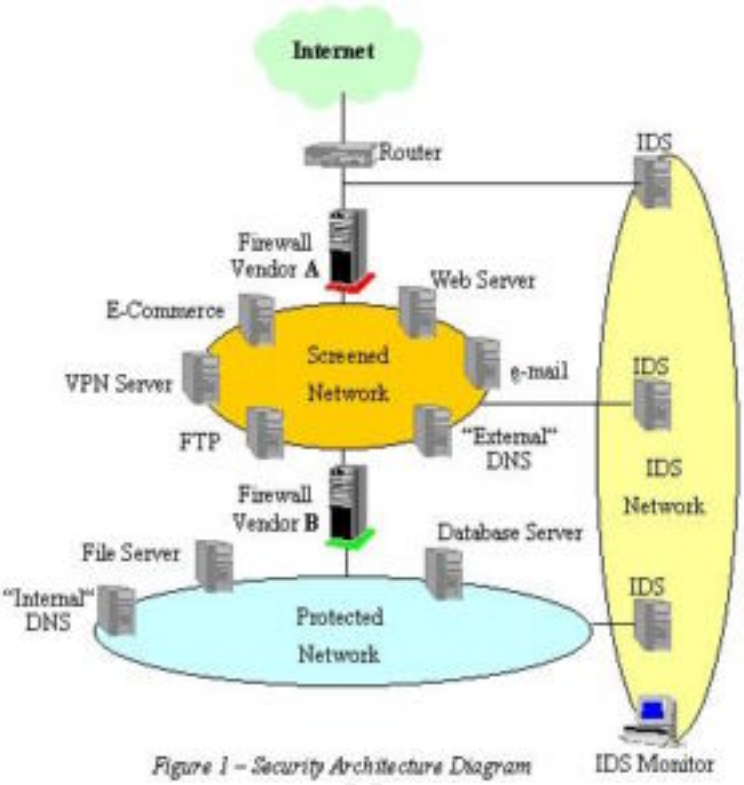


Figure 1 – Security Architecture Diagram

Reconnaissance

As stated previously you are not normally given a network design fo r a network that you are going to attack so you need to create your own map and gain as much knowledge as possible about the victim before you start. After scanning the Internet and obtaining your list of possible sites to attack you would be wise to use N slookup to find the domain name of the address from your scans. It would be very unwise to start attacking an address to find out later that it was in the .mil domain. A tool such as Whois which is found on most UNIX systems or web based sites such as http://us.mirror.menandmice.com are useful for finding out the administrator names , contact details and addresses for a domain, this information can be used for social engineering and the addresses used as the base scan area. Ping and traceroute can be used to test routing information and connectivity, it is also useful to gauge the experience of the people running the system, if you can ping every host in a domain then either you have found a honeypot or the sys tem may be poorly configured, either way you can start drawing yourself a pretty comprehensive network map when you get the OS versions from scan tools such as Nmap. Before scanning the network a search engine can be used to search for things like "@giac.o rg", it is amazing what comes back from this type of search. Web links, departments within the organization, upcoming events etc. Perhaps one of the most interesting things I have found is that most mailing lists have archives, and any messages from these archives come up in the search. Once you have the Email address of the domain admin from Whois you can search for this

address for messages on mailing lists. For example you find a message on a firewall list from the domain admin at giac.org

> Hi guys,
>
> I need some help with my PIX firewall. Outside address is 61.1.1.1 inside address is 61.1.2.1 and I am trying to get mail to pass through to my Linux Sendmail machine at 61.1.2.2. I have put in a rule to allow all IP traffic from the internet to this box but my mail is just queuing on the box.

Realistically would you see such a dumb message, maybe not this dumb but you would be surprised at what information some people are prepared to give away publicly. Searching the mailing lists will give you a pretty good idea as to what is working and what is not as well as the relevant experience of the administrator. In addition to this you can find recent messages and reply to the user only, asking for confidential information under the guise of helping them find a solution.

Host Selection

Before you can decide on a victim you first need an exploit, once you have an exploit you only need to scan the networks found during your Reconnaissance for hosts that are listening on that port. This will reduce noise and may not be noticed. If you don't care about the noise then you just scan all ports and see what comes back. You can reduce noise by using stealth techniques in scanners such as the Syn scan or avoid being identified by blasting the site with hundreds of spoofed addresses, either way if an IDS is installed 99% of scans will be detected unless you are very patient and scan only a few times a day. Once you have your list of hosts and available ports you then need to check the version of software listening on that port. For example if you have an exploit for the POP service after your scan you could telnet to port 110 and see what version information it gives you if any.

```
Escape character is '^]'.
+OK giac.org POP3 v6.50 server ready

Telnet to the Mail port

Escape character is '^]'.
220 giac.org ESMTP Sendmail 8.8.7/8.8.7; Sun, 03 Feb 2002 18:33:23
+1100

ftp to the ftp host
220 ftp.giac.org FTP server (Version wu -2.4.2-academ[BETA-18](1) Sun
Feb 3 19:17:20 EDT 2002) ready.
```

We now have three possibilities to look for remote root exploits. After searching various sites such as http://insecure.org , http://online.securityfocus.com and www.cve.mitre.org I found only a few possibilities. Most of the exploits were local or DOS attacks. I did however find one called wu-ftpd-exp.c on http://anticode.online.com in the download area but a valid username and password on the FTP server was required. One option was to use a program such as Brutus and try to brute force a valid username and password. This would be extremely noisy and would probably attract some attention. If however anonymous login was available then this was enough for the exploit to work. To check this you just need to FTP to the server and login as anonymous, if it lets you in, then you

have a go, if not it's back to the search engine. I will assume in this case that the FTP server in Franks design e ither accepted anonymous logins or was misconfigured.

Remote Root Exploit

Output from running exploit code on vulnerable FTP server

```
[root@hacker.com root]# ./wu -ftp-exploit giac.org -l
anonymous -p hacker@hacker.com


logging in with anonymous hacker@ha cker.com
logged in.
250 CWD command successful.
257 "/home/anonymous/ -l///" new directory created.
250 CWD command successful.
257 "/home/anonymous/ -l////" new directory created.
250 CWD command successful.
VÍè¬ÿÿÿ" new directory created.À°Í1À1Û°.ÍëO1À1É^° '
250 CWD command successful.
VÍè¬ÿÿÿ/bin" new directory created.À1Û°.ÍëO1À1É^°'
250 CWD command successful.
VÍè¬ÿÿÿ/bin/sh" new directory created.°.ÍëO1À1É^°'
250 CWD command successful.
VÍè¬ÿÿÿ/bin/sh/¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ
¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿcd /; uname -a; pwd; id;
¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨
ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿¨ÿ¿
¨ÿ¿¨" new directory created.
Linux giac.org 2.0.36 #1 Sun Feb 24 22:17:11 EDT 2002 i586
unknown
/
uid=0(root) gid=0(root) groups=401(anonymous)

ls
bin
boot
cache
dev
etc
home
internet
lib
lost+found
mnt
proc
proxy
root
```

We have root-Now what

We have root, so now we need to quickly install a rootkit and stop logging our activity. One would assume that this has already gone to a log host so the idea is to minimize the alerts. The only thing that showed up on my logs for this exploit was a log entry showing an anonymous login with my real IP address. In addition to this a 'who' revealed that anonymous was logged in on a tty port, again with my IP address. Installing a rootkit will prevent any further logging and stop me showing up in the who, last etc commands.

Assuming that I have installed a rootkit I can now start sniffing the network to see what's happening. I would be looking for things such as a telnet connection to the external firewall and what traffic from other servers are permitted back in through the second firewall. I can then use this information to compromise further hosts that have access. An example host would be the mail server, this would probably have direct access to the internal mail server, perhaps they are not so diligent with the internal systems and have an exploitable Sendmail I could use. The DNS server may permit TCP 53 to the internal name server, if an exploit is available for this then I can go through the firewall and start looking for NT machines to install tunnel software on. Scanning from this host would be a last resort as it would probably attract attention very quickly.

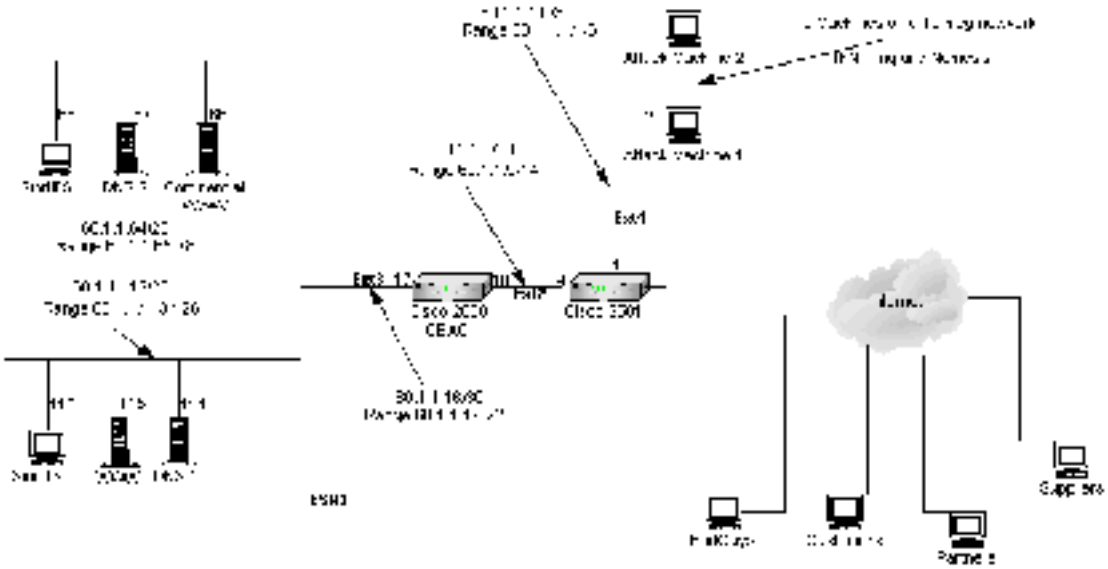
If you cant Hack'em, DOS'em

DOS selection

Denial of Service (DOS) attacks have been around for quite some time with the tools and methods getting more sophisticated all the time. There are literally hundreds of DOS attacks available on the Internet, but if you want to take down a big site like Microsoft etc you need more bandwidth than they have. Even if you had the bandwidth available tracking you down would be fairly trivial. So how do you hit a big bandwidth site and get away with it, you would use a Distributed Denial of Service (DDOS) such as Trinoo or Tribal Flood Network(TFN).

To simulate a DDOS I have used the following setup. I don't need to use my chosen design to simulate the DOS because the basic theory is the same for any DOS attack, I used the following setup as I was able to get real statistics from the attacks.

DDOS Simulation setup



I have also written a quick and dirty Perl program that you will find in the appendix. What the program does is use SNMP to get the Inoctets and OUToctets of each of the Ethernet interfaces on the Cisco 2600 every 60 seconds. It then subtracts the current octet count from the previous octet count and gives a current utilization in Kilobytes/S. Using this I will be able see the effects of different types of DOS attacks on each interface. The program writes the results to a file so I will import this file into excel and graph the results for each attack, this way you can see the effect of the filters on the router for each type of attack. During the time of writing this assignment a new vulnerability for SNMP was released, I would not recommend using SNMP on a border router, however the above design has a choke router that does not run SNMP and can filter any SNMP traffic to the 2600. Using the above method with the Perl pr ogram will allow me to identify the possibility of a DOS attack without seriously compromising security.

Common DOS attacks . In order to deny services to users you either need a vulnerability that stops a host from working such as winnuke, Pong and the Ping-of-death programs that utilize a vulnerability in the way that some systems handle fragmented ICMP packets causing the system to die , or you need to consume all of the bandwidth available to the target network.

Vulnerability attacks are known floors in software that have been found by various people. For example if you have a Windows NT server on the Internet and you allow port 139 in, it is only a matter of time before someone nukes it by running a program such as Stream3 on it (http://downloads.securityfocus.com/vulnerabilities/exploits/stream3.c) Stream3 sends a stream of empty TCP packets on destination port 139 to the target. Each packet consumes a little of the ta rgets memory, if you send enough of these packets fast enough you will consume all available memory and crash the target. While

applying the latest service pack for the OS will fix this you really need to evaluate if you need this port open as it is only a matter of time before a new vulnerability is found.

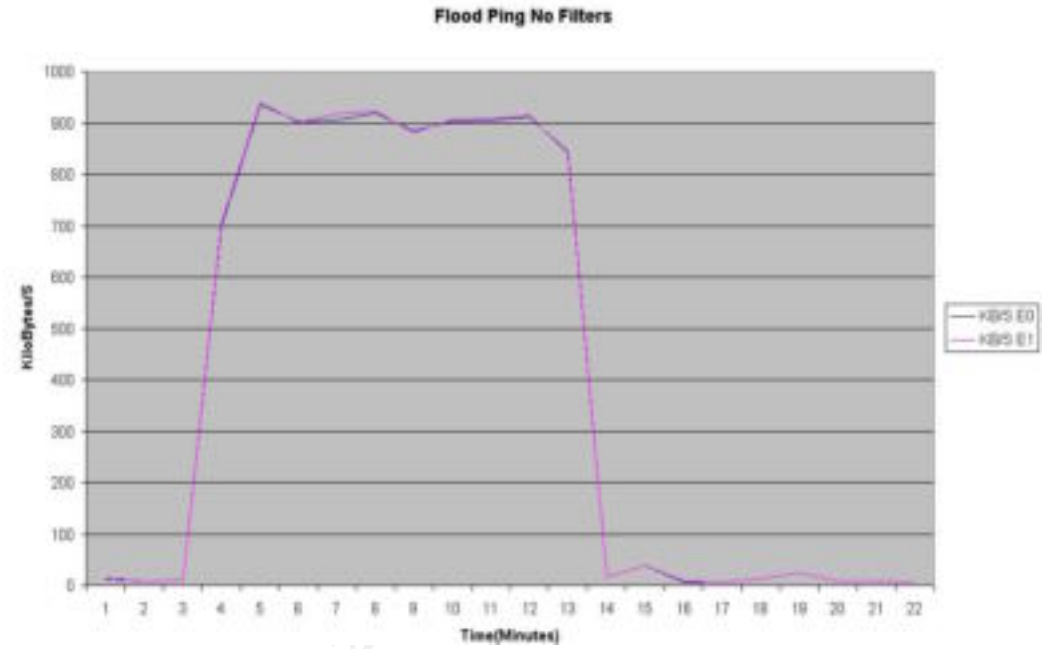
Bandwidth based DOS attacks are reasonably hard to orchestrate; they require one key item not available to everyone, lots of bandwidth. If you want to take out a site with a 100meg link to the Internet then you need at least 100 meg available to you. At first glance one would think that there is no way to do this, but the hackers came up with an ingenious way of achieving massive bandwidth at no cost to them. The DDOS is the best way to attack any site, large or small, however you need to be able to compromise many machines in the Internet first. With the original TFN program this was more difficult because it only ran on Unix , so you needed to compromise a number Unix hosts. DDOS programs such as Trinoo and TFN2K work on UNIX and windows hosts and open up a lot more possibilities than the original TFN. Scan the Internet looking for open windows shares, you may be surprised at what you find. If you can find a share and place the right file in the Windoze directory you have yourself another agent that you can use for an attack. There are many articles on the Internet about TFN and other DDOS attacks so I wont repeat what these already say, it is enough to say that if you can get access to enough machines the re is no site that you cannot take down.
How do you compromise enough machines to have a good attack platform, well we can thank Microsoft for most of that. It is not difficult for those in the know, to get hundreds of thousands of E -mail addresses and send an E-mail with active content or an attachment that sends you to a Website with malicious code using Java or ActiveX. If you let this code run automatically then these applications can basically do whatever they like including the installation of an app lication or Trojan. A demo on this vulnerability can be found on the Finjian website (http://www.finjan.com/attack_release_detail.cfm?attack_release_id=67) .
What is very scary about these DDOS tools is what the author of TFN2K has to say about the program (From the Readme file of TFN2K) .

> TFN can be seen as the yet most functional DoS attack tool with the best performance that is now almost impossible to detect. What is my point in releasing this? Let me assure you it isn't to harm people or companies. It is, however, to scare the heck out of everyone who does not care about systematically securing his system, because **tools sophisticated as this one are out, currently being improved drastically, kept PRIVATE, and some of them not with the somewhat predictable functionality of Denial Of Service**. It is time for everyone to wake up, and realize the worst scenario that could happen to him if he does not care enough about securit y issues. Therefore, this program is also designed to compile on a maximum number of various operating systems, to show that almost no modern operating system is Specifically secure, including Windows, Solaris, most UNIX flavours and Linux.

TFN already ha s a root access command and communicating with it is done using a variety of protocols. If functional enhancements are being made to this program and they already have full access to the machines they are on it is a little scary to say the least as to what these people may be up to next.

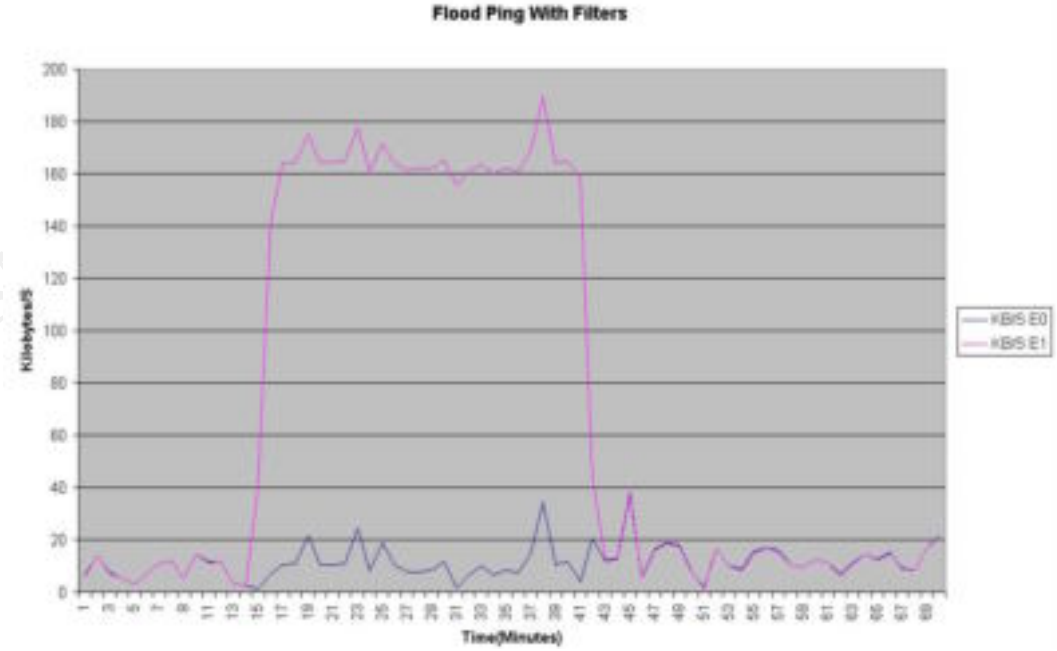
ICMP Flood Attack

The TFN program has an option that allows you to ping a target and set the packet size. If you tell the agent to ping a host or network with a 1500 byte packet, this would be the equivalent of running a flood ping from my attack machines on the border router. The first graph is a flood ping to a host with no filters on the router.



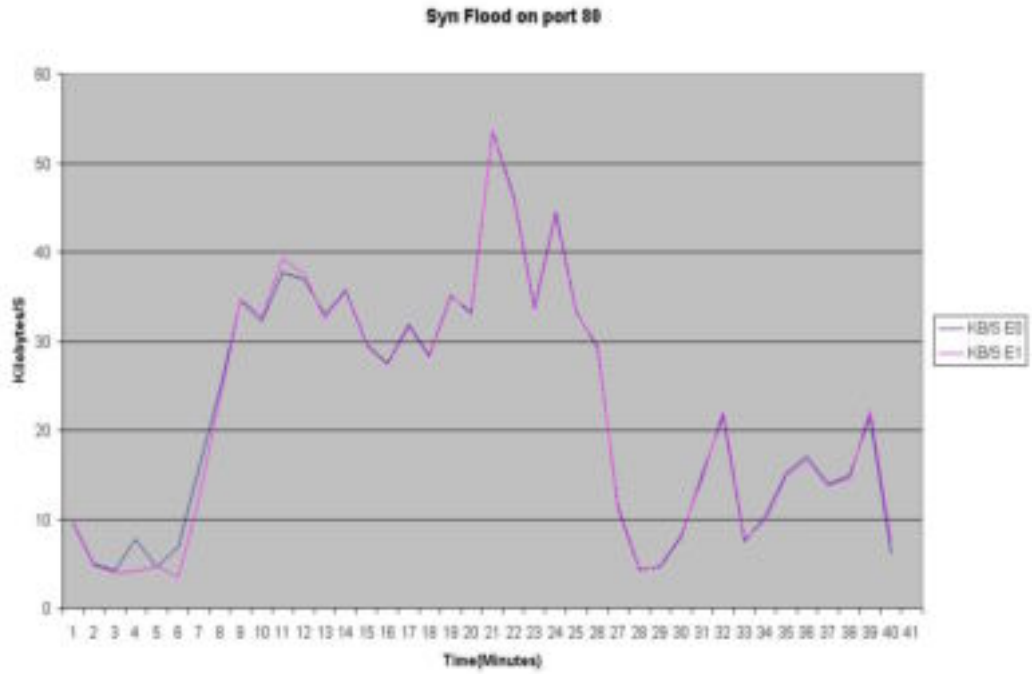
Although Difficult to see, both Interfaces are utilised at around the 8 -900K/S. In reality the External interface would ha ve peaked at the available bandwidth.

The same as above but with ICMP filters applied



It is obvious from the above graph that the filters are working. The traffic is being dropped by the external interface (E1) and are not seen by the Inside interface. The downside is that you have still been DOSsed, the bandwidth on the external interface has all been used , but at least you still have control of your systems behind the router.

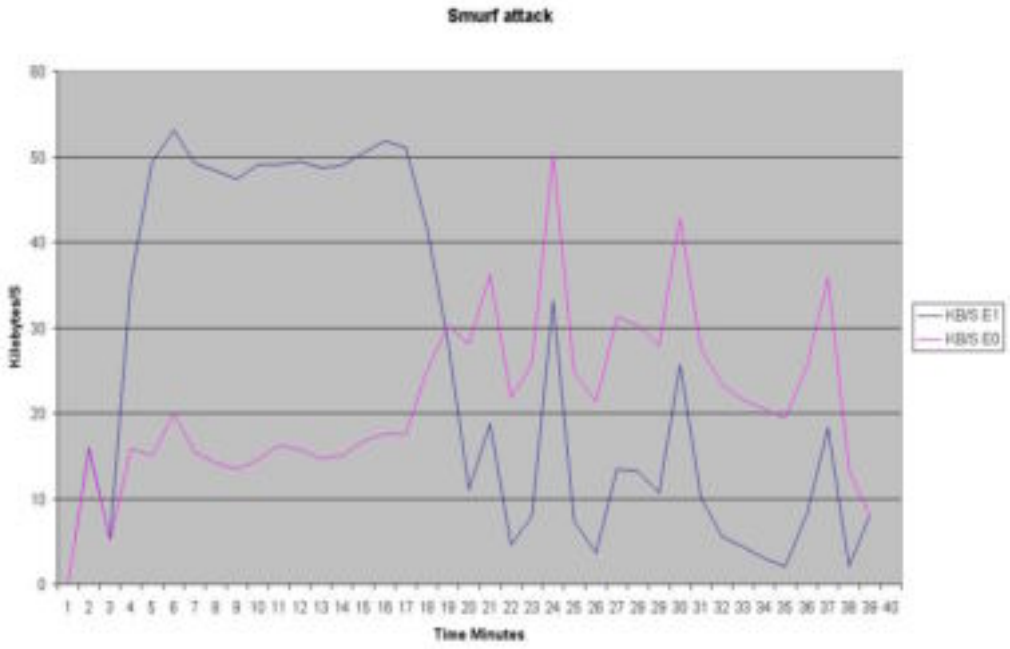
In order for a business to function you need services available to internal and Internet users such as mail and WWW. It is a fact of life that this can be exploited quite easily. TFN supports a SYN attack to try and use up all available connections on a target. On my test attack machine I used Nemesis to simulate a SYN attack against the publicly available web server. I just used a quick shell script to loop continuously with the following command ./nemesis -tcp –v –S 60.10.10.10 –D 60.1.1.115 –fS –y 80. This tells the program to send a TCP packet to 60.1.1.115 with the SYN flag se t and Destination port 80. This packet would be accepted because it would be a standard packet when starting a TCP connection with the publicly available web server.



Again the traffic is equal on both interfaces and the DOS would have been successful as the bandwidth on the external interface would have all been consumed. Similar attacks could have been done on the mail servers or any other publicly available service.

A Smurf attack is when you forge ICMP packets and send them to a broadcast address. If you have a class C network with 200 IP hosts on it and ping the broadcast address say 61.1.1.255, you will get 200 replies to that one ping. You can imagine the effect that this has on a network of you let these forged packets in. In the following graph I had 6 hosts behind the router and I removed the no ip directed-broadcast command from the interfaces and the filter for traffic from my

own network coming in. I then used nemesis -icmp to ping the broadcast address with the following results.



You can see that the internal interface (E1) had more than twice the traffic on it during this attack. After approximately 20 minutes I re -applied the filter and put back the no ip directed -broadcasts, you can see the change to the traffic flow instantly. I used nemesis-icmp to do this attack but could have just as easily use a DDOS tool like TFN to do this from multiple hosts as well.

Preventing DOS attacks

Simple statement but hard to achieve, while there are some things we can do to prevent DOS attacks in re ality you cant stop them. If your having a water fight and you have a garden hose while your opponent has a fire hose, it doesn't take a genius to figure out who will win. The community at large can only stop this happening. If all systems on the Internet were secure the Hackers would not have the bandwidth and the attacks would stop. While this will probably never be a reality it is up to anyone interested enough to do their part and secure their systems as far as possible so that they do not contribute to the problem, not securing your systems could make you liable if you are used to launch any type of illegal activity on the Internet. As a minimum the following steps should be taken to help reduce this problem.

- All systems should be patched on a regular basis, while this does not prevent you being attacked it does increase the likelihood that you will not be compromised and used as a launching pad.
- Limit the amount of bandwidth available to services that are targeted such as SMTP and HTTP. This will only reduce the impact and may still deny legitimate

users access to services but at least you will be able to access your systems to make changes or check logs so that you can liase with your ISP to block any known addresses that are attacking. Establish a rel ationship with you ISP and clarify what they are prepared to do in the event of a DOS attack. Ensure that thresholds are configured appropriately or use TCP intercept to protect hosts running Internet available services.

- Only allow services that you must r un, the more services you have the more th at can be attacked or compromise d.
- Configure your router to block non routable addresses, unwanted ICMP traffic and only allow very specific traffic in and out.
- Install both host and network Intrusion Detection Sys tems and scan the network regularly for changes. Use a log analysis tool and tune it to reduce false positives so that you don't become complacent. Familiarity breeds contempt.
- Run vulnerability scanner(s) both Internally and externally tools such as Nessu s and SARA are free and regularly maintained. Run DDOS scanners on a regular basis especially on internal hosts.
- If possible run an application level firewall, DDOS and Trojans have less chance of going through these systems especially if linked to a conte nt scanner
- Install an E-mail content scanner a keep up to date with any new vulnerability when found.
- Join security newsgroups and mailing lists like bugtraq, SANS and sourceforge.

Finding and installing TFN2K was far easier than I would have thought poss ible, this program can be run by the simplest of script kiddies and there are far to o many easily compromised home machines on fast cable networks available as agents, not to mention the warning from the writer of TFN2K.

References

WEB SITES

Vulnerabili ty search engines
http://www.iss.net/security_center/search.php

General search site for security related Papers
http://searchsecurity.tech target.com/

Whitepapers and RFC's for VPN and IPSEC
http://www.ietf.org/ids.by.wg/ipsec.html

Cisco 3000 series VPN Concentrators
http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm

Ciscosecure Installation/Configuration
http://www.cisco.com/univercd/cc/td/doc/product/a ccess/acs_soft/csacs4nt/csnt30/index.htm

Cisco Pix Installation and Configuration guides
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/index.htm

Ports Database
http://www.treachery.net/security_tools/ports/lookup.cgi

TOOLS

Exploit code
http://www.phreak.org/archives/e_xploits
http://insecure.org
http://online.securityfocus.com
http://anticode.online.com
http://downloads.securityfocus.com/vulnerabilities/exploits/

Vulnerability search engines
www.cve.mitre.org
http://insecure.org
http://online.securityfocus.com
http://www.cert.org

Intrusion Detection Systems And personal Firewalls
Blackice Defender
http://www.networkice.com/products/blackice_defender.html
ZoneAlarm
www.zonealarm.com
Snort IDS
www.snort.org

Password Crackers
Lophtcrack
http://www.at stake.com/research/lc3/
Crack
ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack/
Brutus
http://www.hoobie.net/brutus

Network Scanners

Nmap
http://www.insecure.org/nmap
.
Sniffers
Tcpdump
www.tcpdump.org
Sniffer Pro
www.sniffer.com

War Dialers
Phonesweep
http://www.sandstorm.net

Vulnerability scanners
http://www.iss.net
Nessus
http://www.nessus.org .

Logging
NTSyslog
http://www.sabernet.net/software/ntsyslog_src.zip
Kiwi Syslog Daemon
http://www.kiwi-enterprises.com/
Syslog-ng (Syslog over TCP)
http://www.balabit.hu/en/downloads/syslog-ng/

Log analysers
Webtrends
www.webtrends.com
webalizer
http://www.mrunix.net/we balizer/
analog
www.analog.cx
Scanlogd
http://www.openwall.com/scanlogd/
Swatch
ftp://ftp.stanford.edu/general/security-tools/swatch/swatch-3.0.4.tar.gz,

Online References

Winters Scott , "Securing the Perimeter with Cisco IOS 12 routers ", Aug 15 2000
http://rr.sans.o rg/firewall/blocking_cisco.php

Brett and Variable K. "Building Bastion Routers Using Cisco IOS" Phrack Magazine Vol. 9, Issue 55 9 ", September 1999.
http://www.insecure.org/news/P55_-10.txt

Books

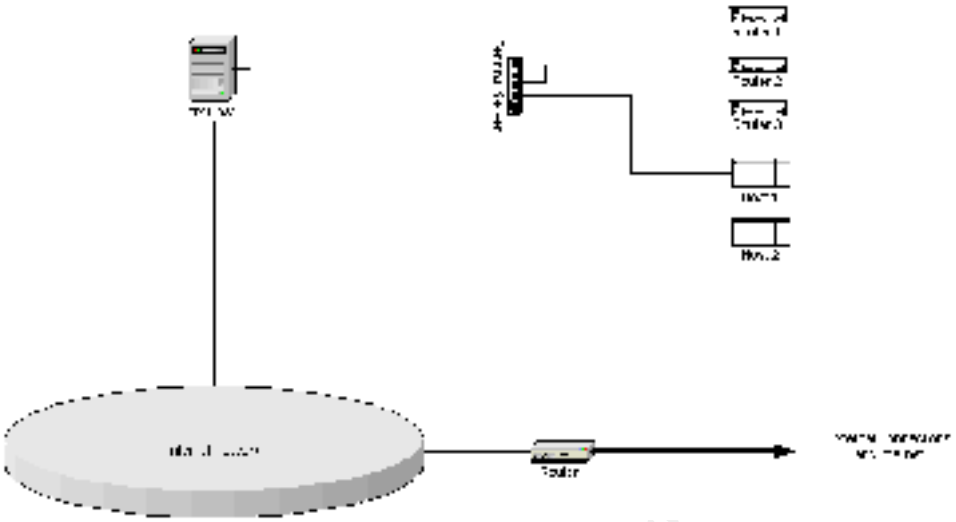
Cole Eric, "Hackers Beware" New Riders Publishing Aug 2001
Chapter 3 Information Gathering Page 21

Chapter 6 Denial of service attacks Page 177

Wenstrom Michael, "Managing Cisco Network Security" Cisco Press Apr 2001
Chapter 8 Configuring the Cisco IOS Fi rewall Page 258
Chapter 9 Configuring the CiscoSecure PIX firewall Page 288

APPENDIX

Console Port access on Routers and hosts supporting console ports.



Most Unix systems support a serial connection as a console port as routers do. The Unix system connected to the terminal server can be secured by only permitting access from designated workstations on the Internal network. Each port on the terminal server is assigned a unique IP address and you would need to telnet to the IP address of the host that you want to manage. Only the Unix host directly connected to the terminal server would be able to connect to these hosts so routing would need to be disabled. This will prevent any direct telnet access from the internal network as you would need to authen ticate to the Unix host first. Logging monitoring and reviews would all need to be part of the process for this system.

Perl program to monitor router interfaces

A program such as MRTG http://people.ee.ethz.ch/~oetiker/webtools/mrtg/ can be used to monitor and graph router utilization constantly, this is an excellent tool and should be used by everyone. The problem with MRTG for the purpose of this exercise was that it uses the 5 minute average counter in the router for the graph. I used this program initially but found the results not a real as the perl program below. This is because it takes the average utilization over 5 minutes, to produce any graphs with meaning necessitated me running the attack for around an hour at a time, not very pleasing for my users even though it was a weekend.

```
#!/usr/bin/perl
###############################################################################
# This program uses SNMP to get the value of  a MIB for the total NO of octets In and
#OUT on an interface
#The mib on this router is .1.3.6.1.2.1.2.2.1.10.X for octets IN, where the X is the
#interface NO .1.3.6.1.2.1.2.2.1.16.Y is the octets OUT where Y is the Interface NO
#use snmpwalk on your ro uter to determine the Interface No's that you want to monitor
#The program collects the data every 60 seconds and subtracts the total octets on an
#interface from the previous value. This gives you the total Bits/Second across the
```

```
#router. This information  is useful as you can see straight away if you are being
#Dos'ed by someone
#If the External Interface has a very high utilisation for Inbound traffic without
#any #corresponding traffic  on the Internal Interface  then you have a problem.
#If you are being  dosed using a valid service then the utilization will be equal
#Basically what you are looking for is no bandwidth available B/W on the Ext Int
#
#I am not a programmer and wrote this program specifically for this assignment
#I knew  nothing  about progra mming when I started and I don't think I know  any more
#now. If you want to clean it up and change the output so that a program like
#Webalizer or RDPtool can use it then go for it. Just don't complain to me about the
#crappy programming.
#Required: SNMP a nd Perl
################################################################################

sub openfile
     {
       #Append to a file and get the current date and time for the log
        #wait for the clock to get to :00 seconds before reading the st   ats
       open(OUTFILE,">> stats.txt");
     }
sub gettime
     {
      #get the time and extract the NO of seconds
      $now=`date`;
      $now=~ tr/ \n//d;
      $delim1=index($now,":");
      $eos=length($now);
      $sec=substr($now,($delim1+4),2)  ;
      $sec=~ tr/ //d;
      }
sub E0in
      {
       $tempE0in=`$E0in`;
       $startloc=index($tempE0in,"=");
       $eos=length($tempE0in) -$startloc;
       $bitsinE0=substr($tempE0in,$startloc+1,$eos);
       $bitsinE0=~ tr / //d;
       $bitsinE0=~  tr /\n//d;
      }

sub E0out
     {

       $tempE0out=`$E0out`;
       $startloc=index($tempE0out,"=");
       $eos=length($tempE0out) -$startloc;
       $bitsoutE0=substr($tempE0out,$startloc+1,$eos);
       $bitsoutE0=~ tr / //d;
       $bitsoutE0=~ tr  /\n//d;
    }

sub E1in
    {

       $tempE1in=`$E1in`;
       $startloc=index($tempE1in,"=");
       $eos=length($tempE1in) -$startloc;
       $bitsinE1=substr($tempE1in,$startloc+1,$eos);
       $bitsinE1=~ tr / //d;
       $bitsinE1=~ tr / \n//d;
```

```
    }

sub E1out
    {

       $tempE1out=`$E1out`;
       $startloc=index($tempE1out,"=");
       $eos=length($tempE1out) -$startloc;
       $bitsoutE1=substr($tempE1out,$startloc+1,$eos);
       $bitsoutE1=~ tr / //d;
       $bitsoutE1=~ tr / \n//d;
    }

sub totals
    {
       $totalE0=$bitsinE0+$bitsoutE0;
       $totalE1=$bitsinE1+$bitsoutE1;
    }

sub history

         {
           $lastoutE0=$bitsoutE0;
           $lastoutE1=$bitsoutE1;
           $lastinE0=$bitsinE0;
           $lastinE1=$bitsinE1;
           $lasttotE0=$totalE0;
           $lasttotE1=$totalE1;
           $loop=1;

         }

sub subtract
      {

       $INpersecE0=sprintf("%3.2f",$bitsinE0  -$lastinE0);
       $INpersecE1=sprintf("%3.2f",$bitsinE1  -$lastinE1);
       $OUTpersecE0=sprintf(" %3.2f",$bitsoutE0 -$lastoutE0);
       $OUTpersecE1=sprintf("%3.2f",$bitsoutE1  -$lastoutE1);
       $totpersecE0=sprintf("%3.2f",$totalE0  -$lasttotE0);
       $totpersecE1=sprintf("%3.2f",$totalE1  -$lasttotE1);
     }

sub utilisation
    {

       $utilE0=spr intf("%3.2f",($totpersecE0)/60);
       $utilE1=sprintf("%3.2f",($totpersecE1)/60);
       #$util=($insec+$outsec);
       $KBE0=sprintf("%3.2f",$utilE0/1024);
       $KBE1=sprintf("%3.2f",$utilE1/1024);
       $line_utilE0=sprintf("%3.2f",(100/$BWE0)*$KBE  0);
       $line_utilE1=sprintf("%3.2f",(100/$BWE1)*$KBE1);
     }

sub writefile
     {
       print OUTFILE ("$now;$INpersecE0;$OUTpersecE0;$KBE0;$line_utilE0;");
       print OUTFILE ("$INpersecE1;$OUTpersecE1;$KBE1;$line_utilE1   \n");
       #print OUTFI LE ("$bitsoutE0;$total_bitsout;$util \n");
       print ("E0 Utilisation=$line_utilE0  \%  E1 Utilisation= $line_utilE1 \% \n");
```

```
       close OUTFILE;
     }
sub savestats
      {

           $lastoutE0=$bitsoutE0;
           $lastoutE1=$bitsoutE1;
            $lastinE0=$bitsinE0;
           $lastinE1=$bitsinE1;
           $lasttotE0=$totalE0;
           $lasttotE1=$totalE1;
           sleep(1);
       }

#Program starts here
$loop=0;
$inE0= " .1.3.6.1.2.1.2.2.1.10.1";
$inE1= " .1.3.6.1.2.1.2.2.1.10.2";
$outE0=" .1.3.6.1.2.1.2.2.1.16.1";
$outE1=" .1.3.6.1.2.1.2.2.1.16.2";
#$brioutavg=" .1.3.6.1.4.1.9.2.2.1.1.8.3";
$community=" MYCOMMUNITYSTRING ";
$get="/usr/bin/snmpget 61.1.1.1 ";
$E0in=$get .$community .$inE0;
$E1in=$get .$community .$inE1;
$E0out=$get .$comm unity .$outE0;
$E1out=$get .$community .$outE1;
#Bandwidth is roughly calculated as 1Mbytes/Sec on 10meg link and 51.2Kbytes/Sec on
#frame Link
$BWE0=10000;
$BWE1=51.2;
$count=0;
&openfile;
$a=100;
 do
      {
        &gettime;
        #Wait till sys tem seconds =00 before reading router stats
        if ($sec == 0 )
           {
              &E0in;
              &E1in;
              &E0out;
              &E1out;
              &totals;
              if ($loop == 0 )
                 {
                  &history;
                 }
               else
                 {
                  &subtract;
                  &utilisation;
                  &writefile;
                  &savestats;
                 }

           }
      }
while ($a == 100) ;
#loop never ends
```