



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Table of Contents	1
Scott_Stevens_GCFW.doc.....	2

© SANS Institute 2000 - 2002, Author retains full rights.



GIAC LevelTwo Practical:

Firewalls, Perimeter Protection, and VPNs

*Submitted by Scott C. Stevens
August 27, 2001*

© SANS Institute 2000 - 2002, Author retains full rights.

Introduction

GIAC Enterprises is an up and coming Internet startup that anticipates tremendous growth in the impending years. As a dot-com, it participates in online electronic commerce and accrues all revenue through this channel. Its electronic assets are significant and must be protected through various means and layers of Information Protection, to include firewalls, filtering routers, Virtual Private Network (VPN) devices, and proxy servers. Additionally, other measures may be used, such as Intrusion Detection Systems (IDS) and Sensors, encryption tools, and bastion hosts/honeypot segments.

Assignment 1 - Security Architecture

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn \$200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- *Customers (the companies that purchase bulk online fortunes);*
- *Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);*
- *Partners (the international partners that translate and resell fortunes).*

GIAC Enterprises Security Model

GIAC Enterprises is in the business of electronic commerce and must deal with the tremendous growth that comes with success. As a result, it must plan out a robust and scaleable information security architecture and policy. First however, it must consider who and what it's protecting. This architecture and policy must serve and protect in the following capacities:

Services Offered

Obviously the services center on the ability to successfully and securely transact with business customers, suppliers and partner over the Internet. Additionally, the ability to market our services (e.g. Website) and communicate (e.g. e-mail) must be effectively secured through various layers of information protection.

Customers

This basically represents the general public (or whoever wants to buy fortune cookies). These folks will have Anonymous access to GIAC Enterprise's Web Server.

Business Partners

This represents those folks that basically buy and resell fortune cookies. They will require various services that will be best provided through our VPN solution, thereby allowing them to fully run various applications at their site without any worries to the security of such processing. The VPN will provide high-encryption via IPSec at Layer 3.

Suppliers

These are those folks supplying the product and located outside of our organization. Most likely we will interface with these folks via SSL (over HTTP).

Internal Users

Internal users will have office automation software and all accesses to internal resources as necessary.

Remote Users

Users telecommuting or on the road will have some network services available to them. E-mail will be retrieved via Exchange and IIS's Outlook Web Access over SSL. Additional accesses will require a VPN client laptop to be issued or, where necessary, to install the VPN client on the users home machine. In the latter case, an engineer must be deployed to the users home (or the user must bring in his/her workstation) to be baselined with GIAC's current image. Personal firewall software must also be installed and the user must sign an agreement letter to keep his anti-virus software current. If the user wishes, GIAC will provide AV software for the user.

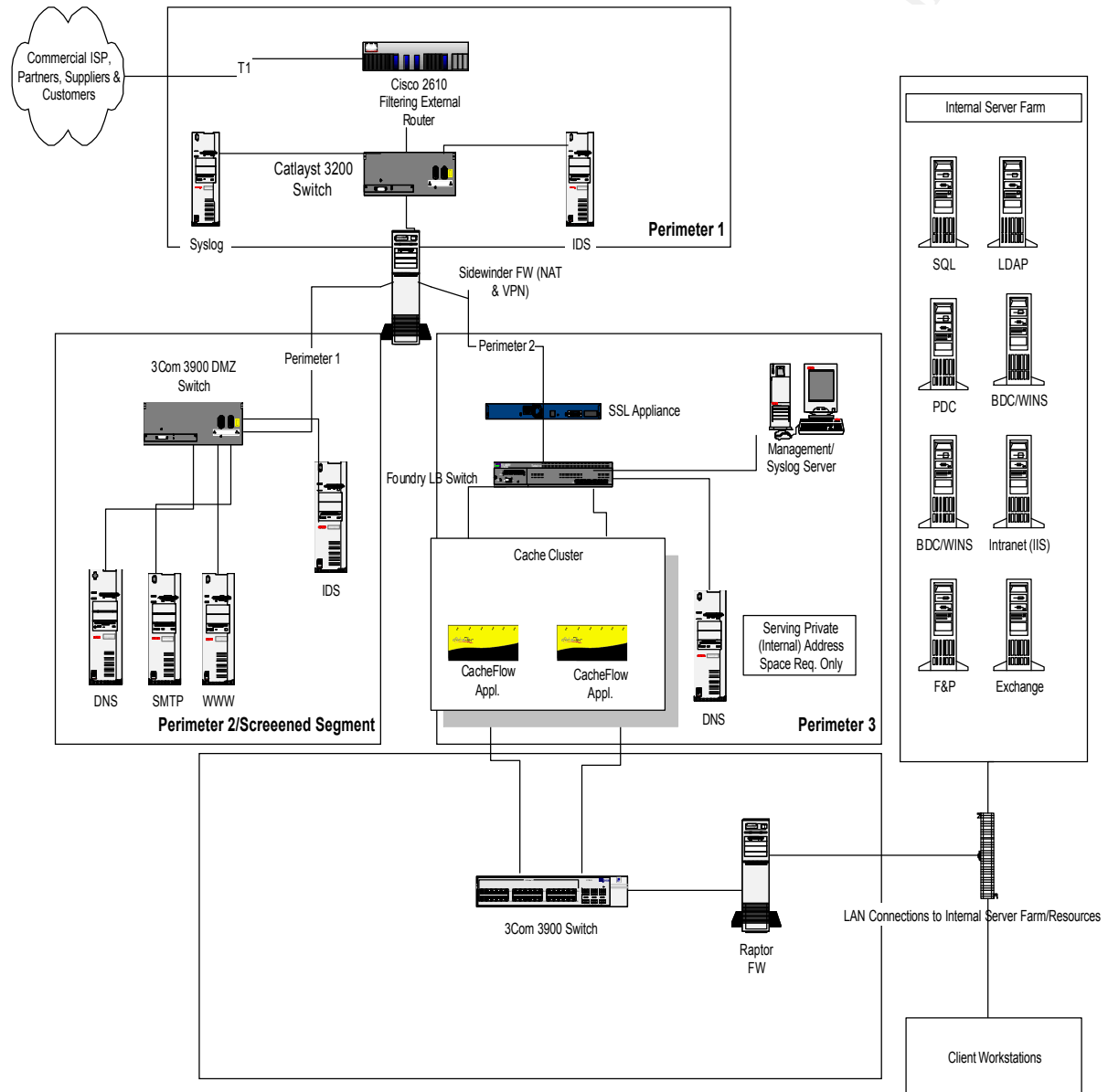
Remote Administrators

Remote administration will occur via SSH and VPN communications. We will attempt to keep remote administration to a minimum.

Architectural Approach

In light of the recent merger, the approach to developing extensive security architecture will be to add on to the existing infrastructure and to ensure its scalability as GAIC Enterprises continues to grow. This is accomplished by extending the existing server farms with scaleable servers, adding a "cache cluster" and load balancer to service inbound/outbound requests to/from the server farm, upgrading the links to Fast Ethernet (100BaseT), and reloading our Sidewinder firewall on a more powerful Sun Enterprise box. The architecture is broken down into three segregated "Perimeters:" Perimeter 1,

consisting of our external filtering router, a switch; and an IDS box; Perimeter 2, consisting of the “screened segment” and housing our Public Servers; and Perimeter 3, consisting of our Load Balancing switch, a management station/Syslog server, and a cache cluster. The GIAC Server Farm and our clients exist behind an additional firewall (Axent Raptor) residing behind Perimeter 3. The illustration is as follows:



Products & Services

The following is a summation of the various products and services used to implement a secure architecture and policy at GIAC enterprises:

Perimeter Router

Our border router serves as our first layer of defense in our security architecture. Our external router is a 2600 series Cisco running the 12.0 Cisco IOS. The router serves as a first defense network layer packet filterer by screening all inbound and outbound communications and will be configured with a fairly simple set of rules to help prevent common attacks such as IP address spoofing, blocking non-routable addresses, controlling ICMP traffic, disabling unnecessary and vulnerable services, and preventing source routing. The router will be configured with the latest security features (e.g., latest IOS security patches, access lists that include most recent malicious addresses/subnets) but will be more open in nature as it sits on the outermost layer of the enterprise (i.e. between our network and our ISP's Gateway). The router will be configured to allow all logs to be sent to the Syslog Server sitting off the Catalyst Switch. The router is configured with static IPs from our provider for its interfaces (S0 and E0). Its ACLs take into consideration all the fundamental security measures for perimeter routers, including egress filtering and denying "private address" ranges (e.g. 10.0.0.0, 192.168.0.0, etc). Our references include:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm>
http://www.sans.org/dosstep/cisco_spoof.htm

Primary Firewall

Secure Computing's *Sidewinder* 5.0 firewall

(<http://www.sctc.com/index.cfm?sKey=232>) is chosen as the primary firewall to segment the trusted network from the untrusted network. Its proxy-based nature offers thorough security for all the major RFC-based protocols (e.g., HTTP, HTTPS, FTP, SMTP, POP3, IMAP, Telnet, DNS, etc.). The firewall will have three NIC's or "Burbs," one to the external untrusted network (to our ISP), one to the screened segment (Perimeter 2), and one to the internal trusted network (Perimeter 3), which eventually interfaces with our back-end Raptor firewall for connectivity to the Server Farm and workstations. The Sidewinder also comes with Network Address Translation (NAT) services which will be used to perform a many-to-one conversion of the private address space to allow for "security by obscurity" as well as conserving our public address space. For those machines that require static addresses for external systems coming inbound, reservations will be made. The Sidewinder allows translation to occur on a per-ACL basis. Additionally, the Sidewinder will be configured with the add-on VPN module to service mobile users requiring internal network resources. Due to extensive processing and I/O as a result of the proxying and VPN services, the Sidewinder

will sit on a 2-way Dell PowerEdge 2450 with 1GB RAM. The operating system is Secure Computing's "*Secure OS*," a locked-down version of BSD with Secure Computing's "Type Enforcement" technology. Subsequent to the initial install of the Secure OS, a BSD-equivalent version of integrity software (e.g., Tripwire) is installed. GIAC Enterprises ensures that an original copy set of configuration files and data is captured, which later scans can be run against to ensure its integrity. Upon changes in the baseline configuration, the integrity software will be re-run.

Cache Appliances and Load Balancing Switch (in Perimeter 2)

The CacheFlow devices residing in Perimeter 2 act as proxies as well and can be configured with access lists similar to a router. Their secure nature (runs a very small OS – CacheOS – that has no exposed vulnerabilities to our knowledge) enhances our "Defense-in-Depth" philosophy as they will proxy all requests to our back-end servers, log against those requests, and will know to only communicate with the back-end Raptor firewall. A potential attacker would have to get past these caches after getting by our external router and Sidewinder firewall, before attempting to hammer away at our internal firewall.

Additionally, the Caches will protect against worm attacks, such as the recent Code Red worm that proliferated throughout the Internet (our hopes are that our SAs have actually already patched their systems however). We will implement this via command lines that we add to the CacheFlow's conf files, such as a *deny* for all HTTP GET /default.ida?XXX... (that are followed by a specific number of characters). These types of modifications are easily implemented on the CacheFlows. Of course, the caches also add a substantial performance gains for requests heading to our backend servers.

A Foundry *Server Iron* load-balancing switch is installed between the firewall and the cache cluster. This device will provide Layer 2 through 7 intelligent switching for the CacheFlow clustering appliances. It will base its decision on content (vice just address) and load balance the switching decisions for the cache appliances.

Because of the nature of the cache appliances, in addition to the LB switch, SSL appliance, internal DNS Server and Management station/Syslog Server that also exist, we like to consider this its own "Perimeter" for clarity.

SSL Appliance and Syslog Server/Management Station (also in Perimeter 2)

As strictly a network performance additive, an SSL hardware accelerator is installed and configured to offload the processing-intensive nature of SSL from the internal WWW Server. This box will sit just off the firewall's second Burb in "Perimeter 2." Just as GIAC Enterprise's external customers securely order bulk fortune cookie sayings, our business partners (i.e. suppliers) route through the

same process. Our internal WWW and SQL Servers service requests from our business partners through web pages. Just like our customers, these requests are encrypted via 128-bit Secure Sockets Layer. The SSL appliance is managed via a Java-enabled browser on a workstation strung off the Load Balancing switch.

A syslog server is installed off the Foundry LB Switch to log certain data passing from and to the back-end systems to the Internet. Information on the server is pulled into the corporate network using freeware SSH (<http://www.openssh.com/>). (A syslog server also exists off the Catalyst switch to collect our external router log data. This data will be pulled, also via SSH, from the Management Station for periodic review).

VPN

We will provide secure communications with our suppliers and partners via Sidewinder's VPN capabilities. With its standards based solution we will be able to establish encrypted sessions with our business partners without an extensive need for reconfiguring on their ends. The VPN services will be provided through the Sidewinder's VPN add-on gateway module, based on the IPsec and Internet Key Exchange (IKE) public key management standards and digital certificates and Certificate Authorities (CAs). Since VPNs (in addition to proxies) are very processing intensive, we'll augment the VPN module with an Intel PA 100 acceleration card. This card redirects much of the processing burden off the Dell's CPUs. The VPN gateway works in concert with the Sidewinder VPN client, which can run on any Windows platform or Java-based client, as well as other IKE-based VPN solutions. For VPN clients, the IP address pool and DNS server list will all be allocated from the gateway.

Screened Segment (Perimeter 2 - DMZ)

The screened network segment (Perimeter 2) consists of those services that are needed for "untrusted" network use but require security to some extent. This segment includes systems that need to be accessible from the Internet but do not require the same protection as those behind our firewall. These services include public DNS requests (e.g. serving requests for www.GIACEnterprises.com or [ftp.GIACEnterprises.com](ftp://ftp.GIACEnterprises.com)), mail relay, File Transfer, and public Web Server requests. The DNS system provides resolution for DMZ hosts and those resolution requests needed from the Internet. The DNS server is an OpenBSD system running BIND. Although BIND has a history of vulnerabilities, we will run it as a non-root user in a "chroot cage" to further protect the system in the event an exploit is discovered. The mail relay on this segment acts as a proxy for all incoming mail. This box runs a Solaris 2.6 with Norton AntiVirus for Gateways, version 2.1. It is used to guard against DoS attacks against the mail system and scans mail attachments for possible viruses. An IDS machine will reside off the switch to monitor suspicious packets and report on possible

hacking attempts. Its logs will be pulled in by the management station in Perimeter 3 via SSH. These servers will be installed with locked down operating systems (e.g. removal of all unnecessary services, scripts, etc., latest patches and hot fixes applied, etc.) as much as possible without disrupting functionality. We may also consider throwing in a honeypot type deception device in the future (e.g. ManTrap from Recourse Technologies www.recourse.com/products/mantrap/trap.html), in order to entice hackers and determine which attacks/probes are being used against GIAC.

Name Servers

Two name servers exist in GIAC Enterprise's design. One DNS (BIND 8.1.2) server exists in Subnet 1 – the DMZ segment. As mentioned above, it provides name resolution for hosts in the DMZ and requests from the Internet. The other DNS server (BIND 8.1.2) responds to resolution requests from the private address space only. It sits in Perimeter 2 off the Load Balancing switch.

Intrusion Detection Systems (IDS)

An Internet Security Systems (ISS) Real Secure box resides off both the DMZ switch as well as the Foundry switch. These devices will have the massive role of listening for common (and not so common as updates are released from the vendor) breaches, including DoS/DDoS attempts, port scans (e.g. NMAP, Ping of Death, etc), and other unauthorized access attempts. The innermost box (i.e. off the LB switch) is configured with a more sensitive logging and reporting set, as it sits behind the firewall and should be acknowledging more legitimate positive hits. The outermost box will be less sensitive as, sitting on the perimeter of our organization, it can generate significant logs of "false positives" if not.

Anti-Virus and Content Filtering Software

All servers and workstations will be respectively imaged with their approved and continuously updated software baseline. Each image will include the latest software release from a major Anti-virus provider (e.g. Symantec/Norton, McAfee, etc.). As part of the image configuration, live update type features will be disabled. Instead, a separate "AV Server" will be setup as a standalone NT Member Server that will pull down updates from the provider. This server will then push out the software and its periodic definition updates to all clients (workstations and servers) via a Management Console located on the AV Administrator's desktop. Additionally, our SMTP Relay machine will be configured with e-mail AV software (e.g. Norton AV for Sendmail) to screen all incoming email that may contain viruses. For an additional layer of mail protection, we'll setup a server, running on top of NT and Exchange 5.5 and added as part of our Exchange Site (but not containing any actual mailboxes) with content filtering software (e.g., MineSweeper or Mail Essentials) to scan mail for malicious content (e.g. Active-X controls, Java Script, etc.), perform dirty word searches, add organizational disclaimers, and, if deemed necessary,

add PGP signatures to outgoing messages. This server will also act as a relay in that it will essentially sit between the Mail Relay and the Exchange Messaging Bridgehead Server and will therefore have the ability to quarantine all “precarious” content and await review from administrators prior to final delivery to individual mailboxes (or deletion).

Password Policy

Strong passwords shall be used at GIAC Enterprises. Below is an outline of GIAC Enterprise’s password integrity implementation, which will help secure its systems. GIAC Enterprises uses a Windows NT architecture for its back-end servers. It maintains and enforces a “strong” password policy for its users with the installation of a popular tool called “Passfilt,” which comes with NT Service Pack 2+. Passfilt is a .DLL file that gets added to the registry of the Domain Controllers (or any Windows NT Server you wish to modify the registry of). It requires a user to specify a password with the following criteria:

- Passwords may not contain your user name or any part of your full name.
- Passwords must be at least six characters long.
- Passwords must contain elements from three of the four following types of characters:

Character types	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric characters (special characters)	\$,!,%,^

Server Farm, Client Workstations and Internal (Back-end) Firewall

Since GIAC Enterprises consists of fairly flat network architecture, its internal servers will reside on their own segment in a “server farm” area. Client workstations are strung off these servers for basic file and print type services. Additionally, we will be deploying an Axent Raptor (sitting on Windows NT) Firewall just outside these switched segments (i.e. Server Farm and workstations) for an added layer of protection. Our intent is not only an additional layer of defense but that, for those exploits that are identified in our primary firewall (Sidewinder) and taken advantage of by attackers, they are *not* exploitable in our Raptor firewall. A differentiation of security products is almost always a positive. Generally, between products that serve the same role, holes and bugs identified in one product version do not apply to another product

version. The Windows NT box will be hardened, patched, and logged for all possible attacks. The firewall's rule-set will consist of little more than those rules necessary for the Caches to communicate with the back-end servers. All other packets will be dropped and logged against.

Abstracts – Training, Security Mailing Lists & Log Review

Ongoing training for the technologies within GIAC Enterprise's architecture is paramount. The training should be a combination of practical "on-the-job" assignments as well as formal classroom training sessions. The administrators must be well versed with the products they are implementing and should weigh vendor (or third party) training heavily prior to purchasing and implementing their products.

Additionally, all engineers and administrators should subscribe to all of the major security mailing lists, including Bugtraq, www.Securityfocus.com, Securifyportal.com, to name a few. Other sites such as www.sans.org and www.incidents.org are other excellent sources for the latest security developments. If available, these folks should also keep current with their implemented technologies as well. This can usually be done through simple website subscriptions that provide mailings from the vendor when an update, patch, or vulnerability is discovered.

Lastly, continuous log review will forever be a necessity to security work. Almost every product and platform offers logging capabilities these days, with some being more robust than others. Firewall, IDS, Server and Router logs should be reviewed as often as possible for suspicious activity. Firewall and IDS logs are of course more sensitive and should be reviewed on a daily basis of possible. When expunging these logs they should first be archived onto permanent media, such as tape or CD, for future retrieval if necessary.

Assignment 2 - Security Policy

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

- *Border Router*
- *Primary Firewall*
- *VPN*

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

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

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

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

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

create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.

Explain how to test the ACL/filter/rule.

Policy Overview

Architecture means nothing without the policies and rule sets to support it. Security policies start out more loosely on the exterior and tighten down as packets make (or attempt to make) their way further in towards protected information assets. I am making the farfetched assumption that GIAC Enterprises does in fact have a written and already approved Corporate Information Security Policy, providing our individual component policies and rule sets with an overall development guidance.

Border Router

As indicated earlier, the border router is a Cisco 3620 running the 12.0 IOS and configured with ACLs based on well-known resources, including SANS. For precautionary purposes, all changes made, particularly to access lists, will be made from the serially connected console port. Furthermore, changes will first be made within Notepad or some other standard ASCII text editor prior to implementing at the command line.

Configuration – Routing, Access Lists, and Blocked Services

First, we must deny “Private” and “Reserve” address spaces, including the Loopback Address, Multi and Broadcast Addresses, and all zero addresses. We will add our implicit “permit ip any any” at the end to allow all other packets through and will log those entries we are denying.

- access-list 110 deny ip 0.0.0.0 0.255.255.255 any log
- access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
- access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
- access-list 110 deny ip 169.254.0.0 0.0.255.255 any log
- access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
- access-list 110 deny ip 192.0.2.0 0.0.0.255 any log
- access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
- access-list 110 deny ip 224.0.0.0 31.255.255.255 any log
- access-list 110 deny ip 240.0.0.0 7.255.255.255 any log
- access-list 110 deny ip 248.0.0.0 7.255.255.255 any log
- access-list 110 deny ip 255.255.255.255 0.0.0.0 any log
- access-list 110 deny host 0.0.0.0 log
- access-list 110 permit ip any any

This access list is then applied Inbound on the external serial interface (We will apply this access list to the *external* interface of the router in order to save us CPU cycles that would accompany the routing involved if it were applied to the internal interface.):

- router(config)# interface s0
- router(config-if)# ip access group 110 in

The "log" at the end of the deny statement in this access list will log any packet that is sent with a source address other than the ones permitted by the previous statement.

After the access list is applied to the interface, the command "show ip access-list <list>" will display counters for each access expression. Confirm that the counter for the expression to pass your address block is incrementing.

If it is necessary to remove the access list due to an error, use the interface command "no ip access-group 110 out" to remove it and confirm with "show ip int <interface>".

Next, all unneeded services are either disabled or blocked altogether. Since we have no use for these services, there is no need to allow them as they can potentially be exploited. All the following are made in Global Configuration mode (router command followed by explanation in parentheses):

- no ip redirect (Some source packets can be crafted or modified to include an alteration to a destination hosts routing table. This command blocks all attempts of a redirect)
- no ip directed-broadcast (Blocks all broadcasted traffic)
- no ip bootp server (Another source of broadcast based traffic will be blocked)
- no ip http server (The web-enabled management interface will not be used)
- no ip finger (Blocks the exploitable Finger service)
- no ip gdp (Blocks gateway discovery protocol)
- no ip irdp (Blocks icmp router discovery protocol)
- no ip mask-reply (Blocks icmp netmask replies)
- ntp disable (Blocks access to external time servers)
- no cdp enable (Blocks Cisco discovery protocol queries)
- no ip proxy arp (Blocks arp service)
- no ip unreachable (Prevents router from accepting packets that may alter the routing tables)

Also, we want to configure the router not to allow any terminal access to the router from anywhere other than the our network. We'll modify the config file as follows:

© SANS Institute 2000 - 2002, Author retains full rights.

```
! Allow traffic from the x.x.x.x/24 network and deny all else
access-list 10 permit x.x.x.0 0.255.255.255
access-list 10 deny any log
! Apply access list to terminal lines
line vty 0 4
access-class 10 in
```

Now we want to turn off common services that we don't want to pass through our router, such as tcp echo, discard, and chargen ports:

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

Additionally, Cisco Discovery Protocol [CDP], which can potentially provide vital information to upstream routers, will be turned off. There is no business need in providing this information:

- no cdp run
- no cdp enable

Logging is implemented to port all logged data to our Syslog Server residing in Perimeter 3. The address of the Syslog Server and the correct router interface must be specified to turn logging on:

- logging source-interface Ethernet1
- logging <ip-address of syslog machine>

Also, we deny and log commonly known Trojan horse and DoS ports:

- access-list 110 deny tcp any eq 33270 log (Trinity DDoS)
- access-list 110 deny udp any eq 12345 log (NetBus)
- access-list 110 deny udp any eq 12346 log (NetBus)
- access-list 110 deny udp any eq 20034 log (NetBus)
- access-list 110 deny udp any eq 31337 log (Back Orifice)
- access-list 110 deny udp any eq 5631 log (PCAnywhere)
- access-list 110 deny tcp any eq 5631 log (PCAnywhere)
- access-list 110 deny tcp any eq 5632 log (PCAnywhere)
- access-list 110 deny udp any eq 5632 log (PCAnywhere)

Access list 110 is then again applied Inbound on the external serial interface.

- router(config)# interface s0
- router(config-if)# ip access group 110 in

SNMP Community is redefined and changed from its default "Public" string.

Additionally, the attributes are changed to reflect “Read Only.” An access list is then created and applied to allow only certain “SNMP Management stations” to interface with the routers SNMP MIB. This access list will be applied to the *internal* interface of the router

- `snmp-server community gcfsnmp RO 20`
- `access-list 110 permit <internal_IP_of_mgt_station(s)>`

By default Cisco does not impose a “Warning Banner” when consoling or remotely accessing the router. A warning banner message is defined and applied to advise all unauthorized users of GIAC Enterprise’s personal property:

- `banner motd ^CC This machine is personal property of GIAC Enterprises, Inc. Any and all unauthorized accesses will be fully pursued and prosecuted. ^C`

IDENT, an easily exploited service (Port 113) that provides one with information about a machine, will also be added to access-list 110 and blocked:

- `access-list 110 deny tcp any any eq 113`

Static and NAT Routes - A static route (ISP’s upstream router) must be defined as a default route as well as routes to correspond to the address range provided by the Network Address Translation performed by the Sidewinder:

- `ip route 0.0.0.0 0.0.0.0 199.220.53.1 (ISP’s address)`
- `ip route 196.24.2.0 255.255.255.0 196.24.1.1`

Source routing shall never be allowed in the GIAC network. Spoofed and source routed addresses will be blocked on the external router. The following implementation is taken from SANS *Anti-Spoof Egress Filtering* article (http://www.sans.org/dosstep/cisco_spoof.htm). All of the changes are assuming that the access list itself has already been created (i.e. access-list 110):

First, we must deny spoofed addresses. Since our Sidewinder firewall is also performing address translation, the Class C address space 196.24.1.0 (0.0.0.255) is used, as registered from our ISP:

- `Access-list 110 deny 196.24.1.0 0.0.0.255 log`

Deny all ICMP requests to prohibit potential eavesdroppers from receiving ICMP information:

- `access-list 110 deny icmp any any log`

We will now apply the list to our Serial 0 (external) interface. We'll also keep this rule near the top of our ACL set:

```
ip access-group 110 in
```

Firewall

The firewall GIAC Enterprises has chosen is Secure Computing's *Sidewinder ver. 5.0* (three hot-fixes have been released for version 5.0 and have been applied to the GIAC firewall). GIAC Enterprises employs several ex-military service members and, with Sidewinder deployments widespread throughout DoD facilities, it was all too familiar of a product for our enterprise and an easy choice to make for our Information Security department staff. Sidewinder is an application proxy based firewall and its configuration is an explicit "deny all" policy. Furthermore, with every major proxy supported, as well as the ability to manually create others (although the packet regeneration is not the same as the natively-supported proxy services), data streams *will not* traverse the Sidewinder without being proxied (unless *IP Filters* are created to tunnel through, which is fundamentally unsound and highly recommended against).

Hardened "Type Enforcement" Operating System & ACLs:

Sidewinder's underlying operating system is a locked down and secured version of Unix BSD. Secure Computing removes all unnecessary services and files and restructures its architecture such that, even with root privileges, modifications that would impact the core BSD kernel are prohibited. This prevents things such as an attacker having the ability to edit the syslog file to cover their tracks. All application-layer elements are less prone to attack when undergoing this lockdown process. Secure Computing likes to call this security through its patented name "Type Enforcement."

<http://www.sctc.com/index.cfm?sKey=738>

Sidewinder is by nature an inherent "deny all" proxy/ACL-based firewall. In other words, unless a proxy (and again, customized proxies can be created as well at the risk of bypassing much of the fine-tuned security that comes with the Sidewinder supported proxies) and corresponding ACL rule is defined in the rule set, the packet is denied and dropped by default. While you can elect to define a "deny all" rule at the end of the ACL set, it provides for a small performance gain only. Whether it exists or not, packets are still dropped when not meeting a rule. Therefore, all "small service" ports and other popularly exploitable "high order" ports are blocked, as there is no reason to create an access control list rule for them. Additionally, the firewall is configured using several popular industry references in determining its open and closed ports/protocols, including Secure Computing recommendations (<http://www.sctc.com/index.cfm?sKey=723>) and SANS Institute resources (<http://www.incidents.org/cid/index.php> and

<http://www.sans.org/topten.htm>).

© SANS Institute 2000 - 2002, Author retains full rights.

Another very useful resource used in building our rule base is Lance Spitzner's "Building Your Firewall Rulebase" white paper (<http://www.enteract.com/~lspitz/rules.html>).

Network Address Translation (NAT)

The firewall will be performing layer-3 address translation for both security purposes – to hide the internal hosts' addresses, as well as to conserve our registered public address space for only those machines that have a genuine need to be static (e.g. a server that requires inbound access but cannot sit out in the DMZ). Internally, we will be implementing the 192.168.0.0 address space, with a Class C mask of 255.255.248.0. This will allow for an abundance of hosts for our few subnets, while still allowing for plenty of growth (i.e., 32 subnets) if we choose to further subnet in the future. Since we will be implementing DHCP from our File and Print Servers, address scopes can be modified on the fly (would only require a restart for hosts configured for DHCP). Incidentally, NAT makes a nice complement to DHCP.

Access Control Lists (ACLs)

The following parameters are allowed to be defined within the Sidewinder ACLs:

- Source Address or Network Object (i.e. Domains, Hosts, IPs, NetGroups, & Subnets)
- Destination Address or Network Object (i.e. Domains, Hosts, IPs, NetGroups, & Subnets)
- Service – Proxy/Server
- Port
- Allow/Deny
- Enabled/Disabled (i.e., you can turn the rule on or off)
- Authentication Type (Password, RADIUS, SecurID, Safeword, SNK)
- NAT (with ver. 5.0+ you can define translation per ACL rule, if desired)

The following ACL set will be created to allow for communications with business customers and suppliers. In addition, Sidewinder is a "stateful packet inspecting" proxy-based firewall. If requests are initiated from the internal side, the replies communication stream is allowed back inbound. There are not very many services that GIAC Enterprises requires for its business. We will keep the rule set as clean and minimal as possible. FTP will *not* be allowed. All file transfer type transmissions will be either via HTTP or HTTPS. As other rules are required down the line, we will address them on a case-by-case basis. Only SRC, DST, Service, Port Number, and Action will be listed in the following ACL table.

SRC	DST	Service	Port	Action
FirewallAdmins	Firewall	scobra	TCP/9003	Allow

- Allow the FirewallAdmins group object “Secured Cobra” access to the Firewall itself.

SRC	DST	Service	Port	Action
FirewallAdmins	Firewall	SSH	TCP/22	Allow

- Allow the FirewallAdmins group object Secure Shell access to the Firewall itself.

SRC	DST	Service	Port	Action
ANY	Firewall	NetBIOS	UDP&TCP/137-139	Reject

- Send “Resets” on chatty NetBIOS traffic. The resets will speed up for performance. We purposely place these *before* our overarching “Deny All” rule to the Firewall.

SRC	DST	Service	Port	Action
ANY	Firewall	IDENT	TCP/113	Reject

- Send “Resets” on IDENT traffic. The resets will speed up for performance. We purposely place these *before* our overarching “Deny All” rule to the Firewall.

SRC	DST	Service	Port	Action
ANY	Firewall	ANY	ANY	Deny

- Drop all other packets destined to the firewall itself.

SRC	DST	Service	Port	Action
Public	Internal	ANY	ANY	Deny

- Deny all traffic originating from the DMZ and destined to the Internal interface. This is a well-known rule in the firewall community. Traffic destined to the Internal side from a screened segment should never be allowed. (NOTE: This is a more specific rule and is therefore added further at the top of the set so that the more general rules below do not supersede it).

SRC	DST	Service	Port	Action
ANY	ANY	SMTP	25	Allow

low mail to flow in all directions.

SRC	DST	Service	Port	Action
ANY	ANY	SSH	TCP/22	Allow

- Allow Secure Shell in all directions.

SRC	DST	Service	Port	Action
ANY	Public WWW Server	HTTP	TCP/80	Allow

- Allow HTTP access to Public WWW Server.

SRC	DST	Service	Port	Action
ANY	Internal WWW Server Group	HTTP	TCP/80	Allow

- Allow inbound WWW access to Internal Web Server Group.

SRC	DST	Service	Port	Action
ANY	DB Server	SQL	TCP/1531	Allow

- Allow access to back-end Database Server (SQL)

SRC	DST	Service	Port	Action
ANY	WebServers	SSL	TCP/443	Allow

- Allow HTTPS access for all interfaces.

SRC	DST	Service	Port	Action
ANY	WebServers	IKE	UDP/500	Allow

▪

SRC	DST	Service	Port	Action
Internal	DNS-Perimeter2	DNS	UDP/53	Allow

- Allow Name Resolution to and from the Internal hosts only.

SRC	DST	Service	Port	Action
Internal	Public	ANY	ANY	Allow

- Allow all traffic stemming from the Internal, trusted network to the DMZ.

SRC	DST	Service	Port	Action
ANY	ANY	ANY	ANY	Deny

- While it is not necessary to add this rule with Sidewinder (Sidewinder drops all packets that don't meet a rule, regardless), it does enhance performance somewhat.

Firewall Management

Only user accounts for the specific firewall administrators and their backups will exist, as well as one account for the IAPM (Information Assurance Program Manager), who reports directly to the GIAC Enterprises VP of Technology. The firewall administrators and the IAPM are granted full root privileges (i.e. “admin” role in Sidewinder speak – there are also “proxyadmins, authadmins, ftpadmins, and so on, to limit peoples administration), which allow them to manipulate all features of the Sidewinder, minus those features that are locked down through “Type Enforcement.” The backups are granted administrative rights but to a slightly lesser degree. Shall these people take on added responsibility of firewall administration, their rights will be increased accordingly.

Sidewinder can be administered via command line through Telnet or Secure Shell (SSH) or a proprietary tool called “COBRA.” For security purposes, telnet is restricted to the internal, protected NIC only. It is not allowed via the external, un-trusted side. Secure Shell (<http://www.openssh.com/>) is used for remote command-line administration and monitoring via un-trusted circuits. COBRA also includes the ability to securely administer Sidewinder via Secure Sockets Layer. This functionality will also be enabled on the external NIC so that administrator can tune and modify the Sidewinder over Internet channels when necessary. The preferred method of administration is through the COBRA utility while on the internal network or at the console itself. Additionally, COBRA comes equipped with a monitoring utility that keeps a close eye on things like Network Connections, CPU usage, Memory usage, and Disk Space on the various mounted file systems. (Unix commands such as *top* will be used as well, when monitoring via command line). COBRA can run on any windows host.

Virtual Private Network (VPN)

VPN Solution Determination, Approach and Assumptions

Because of GIAC Enterprise's role in E-commerce it deals extensively with its suppliers and partners, an easy yet secure means of communication must exist between our organization and theirs. A Virtual Private Network (VPN) is the best way to secure these ongoing lines of communication with these folks.

Like most implementations in IT, there are multiple designs and implementations that an IT architect can take. Many implementations now include actual VPN appliances, which are fairly easy to install, configure and maintain and are often affordable. For example, many Cisco shops install Cisco's VPN Concentrators (e.g. the VPN 3000 Concentrator) to easily integrate with their routers. These appliances can either be installed on a DMZ type segment, in front of the firewall (generally not recommended), or parallel to the firewall on its own interface (most acceptable solution). This would obviously require certain ports to be open on the firewall and filtering routers, for example, UDP 500 (IKE key-negotiation), TCP 51 (Authentication Header). Other implementations can consist of still opening up ports in order to allow traffic to a Windows NT PPTP Server or a Win2K IPSec Server sitting either in the internal network or out in a DMZ (or, again, parallel to the perimeter firewall). Still other implementations can be a VPN module on the firewall itself.

Since we have previously setup VPN solutions with Secure Computing's Sidewinder Firewall with relative ease and success, we will choose it as our solution. Sidewinder supports industry recognized VPN standards (e.g. IKE and IPSec) and allows for an easy and seamless implementation. Sidewinder embeds this VPN solution into its O/S, allowing admins to apply access rules in the same fashion as they do for physically connected networks, as well as giving them the ability to control GIAC Enterprise-wide security policies. Once the encrypted data is decrypted on the gateway it is sent as clear text back to the destination host (and vice versa for outgoing packets). Sidewinder's secure separation between "burbs" protects this information as all decrypting will occur on the internal burb. As far as horsepower, our dual processor PIII CPUs and 1GB memory, in addition to the VPN Accelerator Crypto Card, provides sufficient horsepower for the processing overhead the VPN encryption leverages.

The VPN services can be configured either via command line or through Sidewinder's *Cobra* GUI. Since the options through the BSDI CLI can be extensive and cumbersome, I have decided to use the screen captures which can depict greater detail of what is actually being configured in the underlying O/S. However, at times, tweaking of the Sidewinder *.conf* files (e.g., *ike.conf*, *cert.conf*, etc.) is necessary, if the COBRA GUI tool is not sufficient. This is generally not necessary and is usually only required for unusual troubleshooting scenarios.

VPN Configuration

First, before configuring a VPN, we must ensure certain servers are running on our Sidewinder:

- EGD – Entropy Generating Daemon server is a random number generator used by ISAKMP. The server must be enabled before VPN associations can be created.
- CMD – Certificate Management Daemon server must be enabled before you can configure your certificate server.

We can check the status of these by secure shelling to our Sidewinder BSD box or logging into the console and typing:

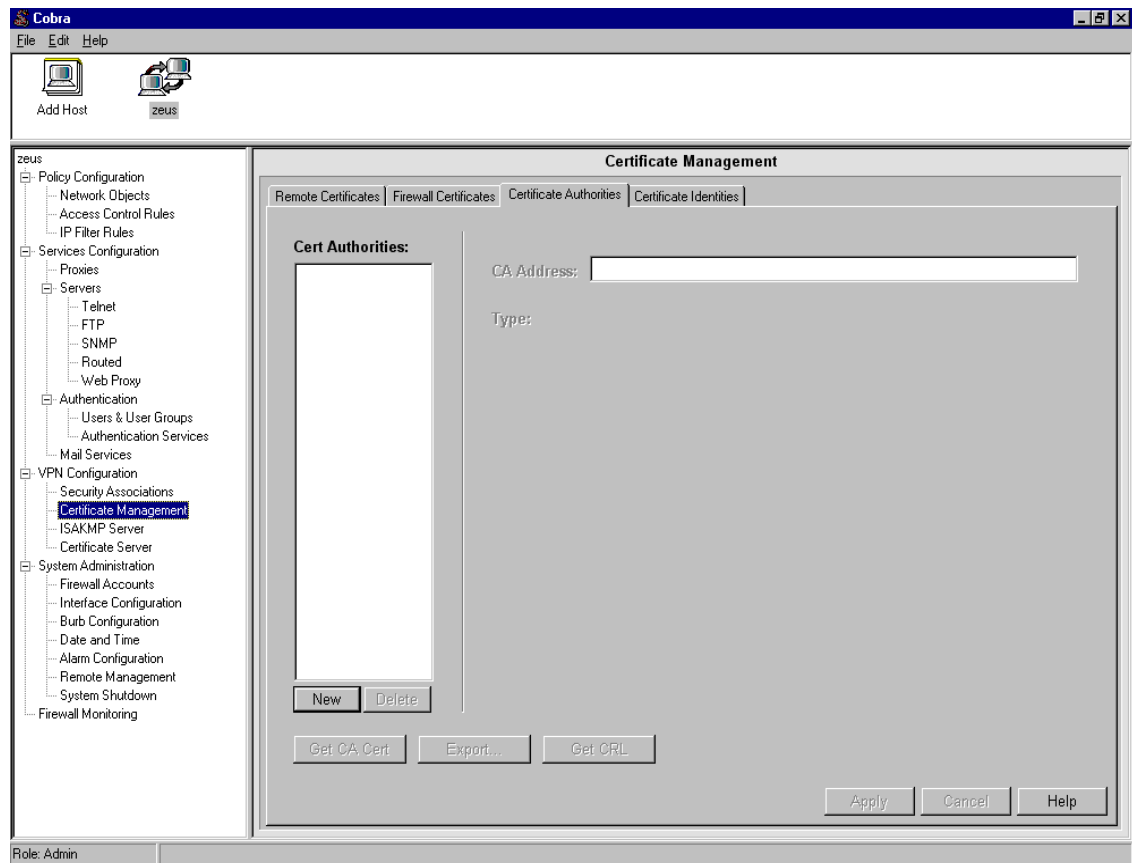
- `cf server status egd`
- `cf server status cmd`

And, if needed, we can enable them by:

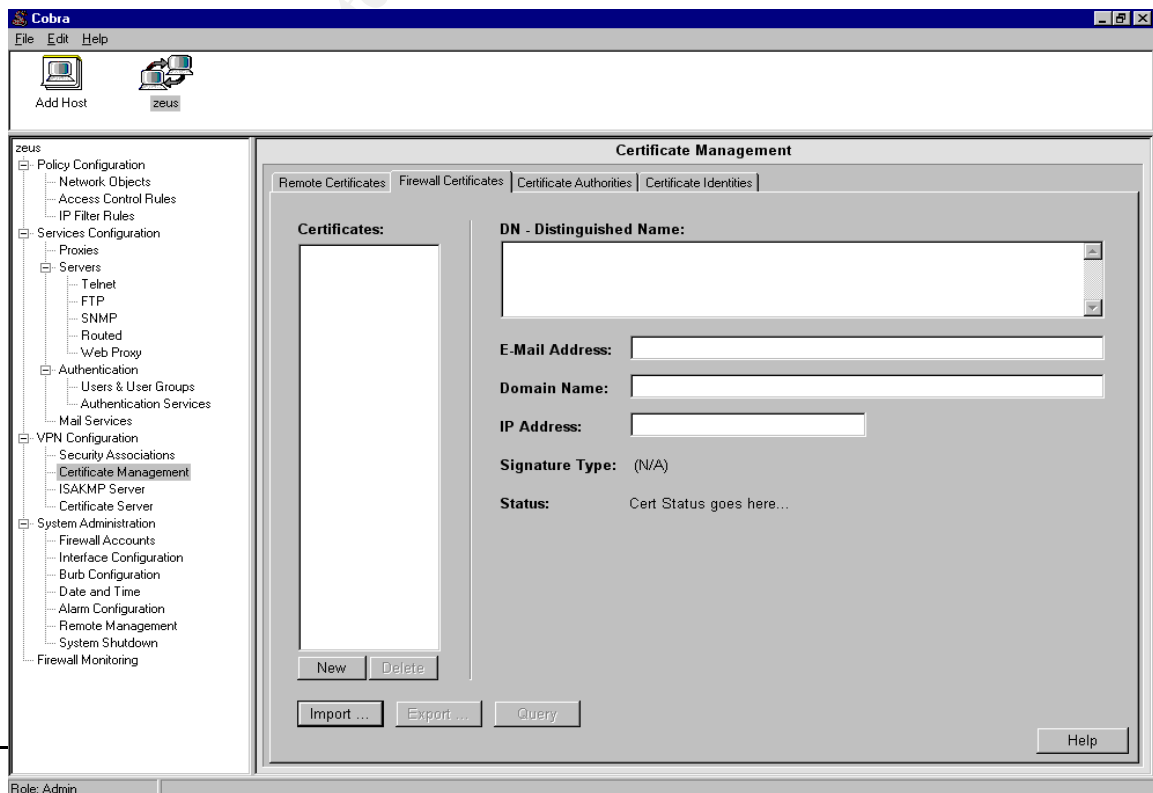
- `cf server enable egd`
- `cf server enable cmd`

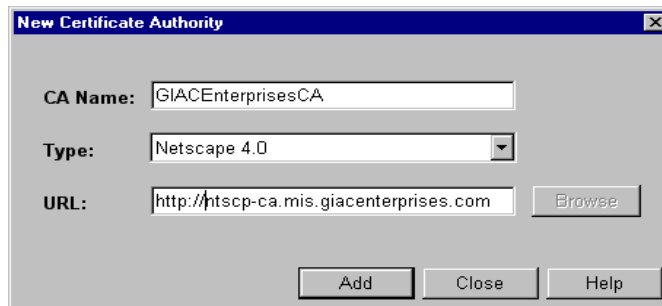
Next, before configuring our VPN settings on the Sidewinder, it is easiest to first define our certificates. Since GIAC Enterprises deals with various suppliers and partners, each of whom may use different types of certificates on the remote end, we decided to go with a Certificate Authority-based implementation. This implementation will use an automatic key exchange solution using Internet Key Exchange (IKE), and allow us to configure it as a Certificate Authority (CA) Policy.

PLEASE NOTE: While I would have preferred to add all parameters to make the VPN configuration as real as possible, I unfortunately did not have the luxury of making such changes on our firewall (i.e. firewall at my work place). I am most familiar with Sidewinder, have been impressed with its Secure O/S, and therefore selected it as my primary firewall. I hope that my explanations that accompany the screen captures will suffice.

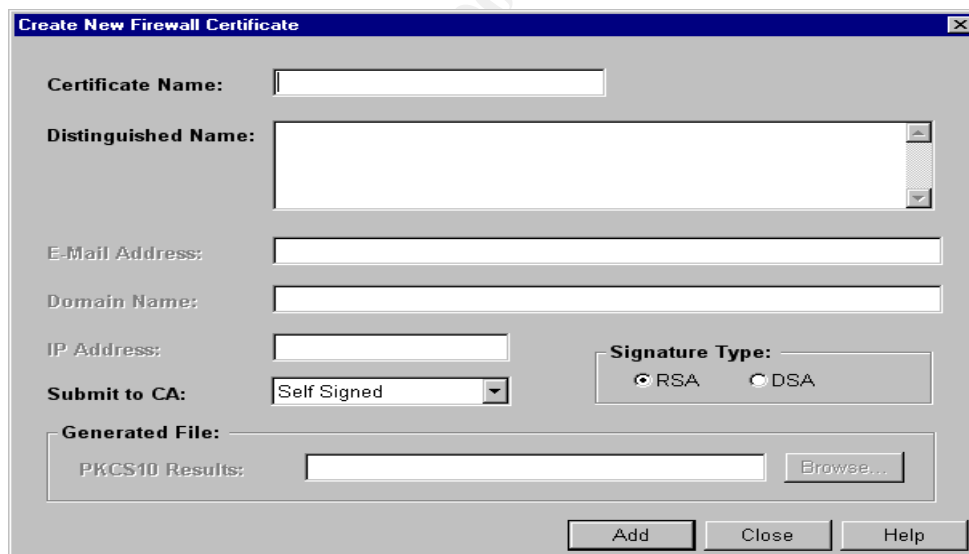


Here, we would create a new **Certificate Authority**. This will be our own private CA server:





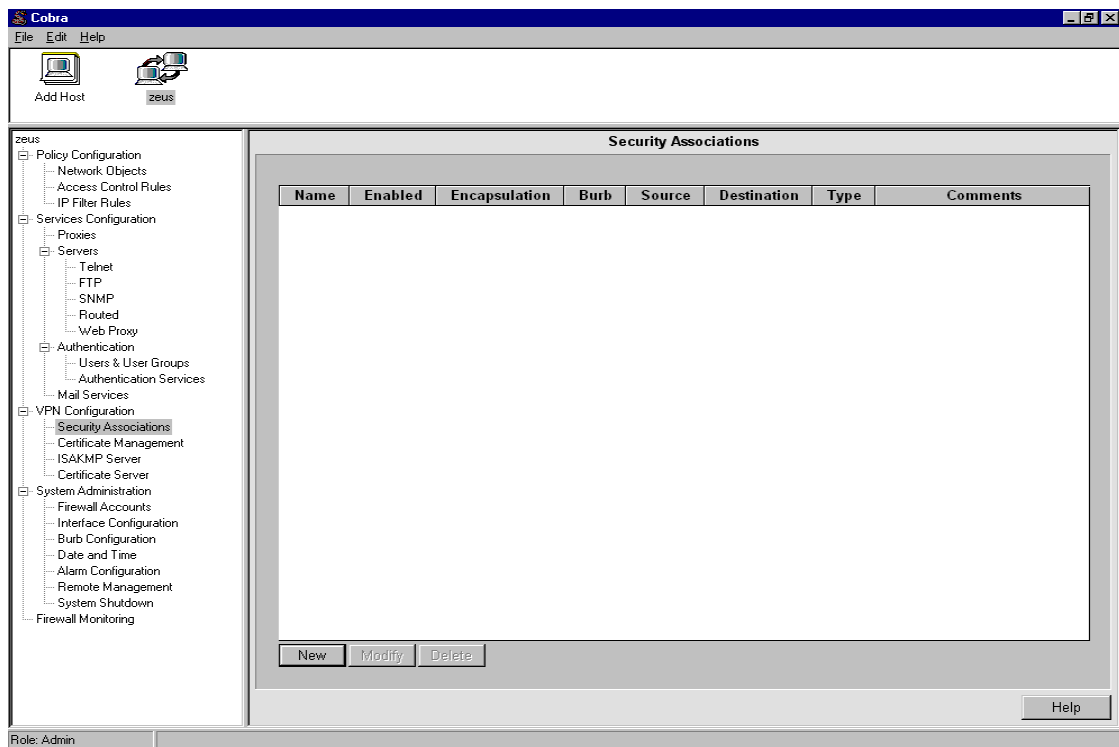
Next, we will define a **new certificate**, which gets sent to our newly defined CA for validation. This certificate gets added into the *Firewall Certificates* list. This would be used to identify the firewall in our “peer-to-peer” sessions in which we were establishing a tunneled connection with another Sidewinder. We will give the certificate a name, Distinguished Name (i.e., one that follows the cn=, ou=, o=, l=, st=, c= naming convention). The key will get submitted our private Netscape CA server (typo in the second window – it will NOT be “self-signed) with the standard RSA encryption format. The other fields are optional.



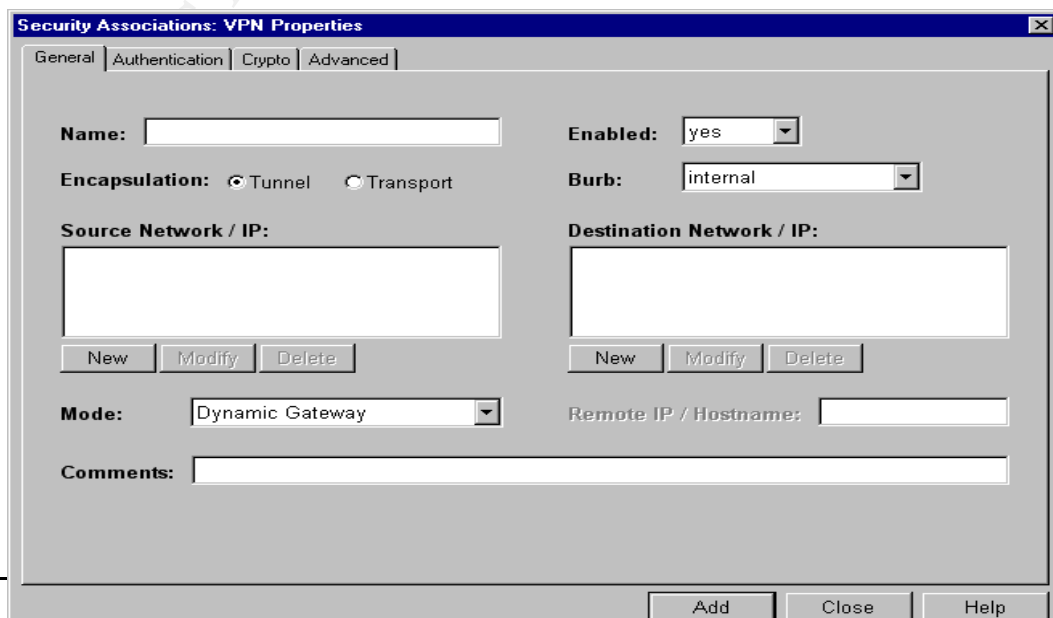
Next, we must define a **Security Association**. A Security Association must be created for each and every remote end “termination” that will exist. However, here we have the opportunity to define different types of association under the *Modes* list. For example, if we are connecting to a channel supplier and establishing a session with various clients (hosts) that reside behind a gateway device, we would select *Dynamic Gateway*

In order to continue, we must now reconfirm that the EDG server is enabled by again typing *cf*

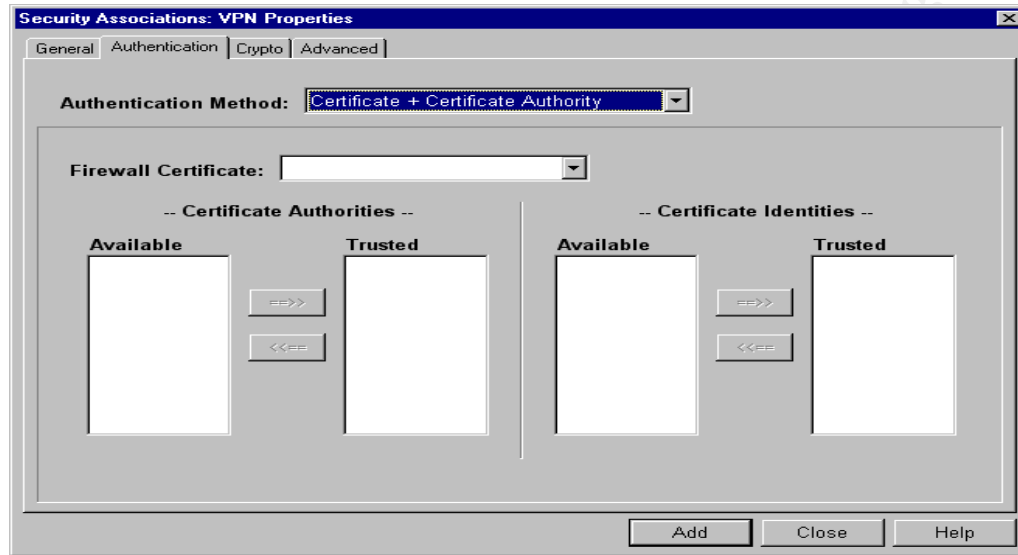
server status egd.



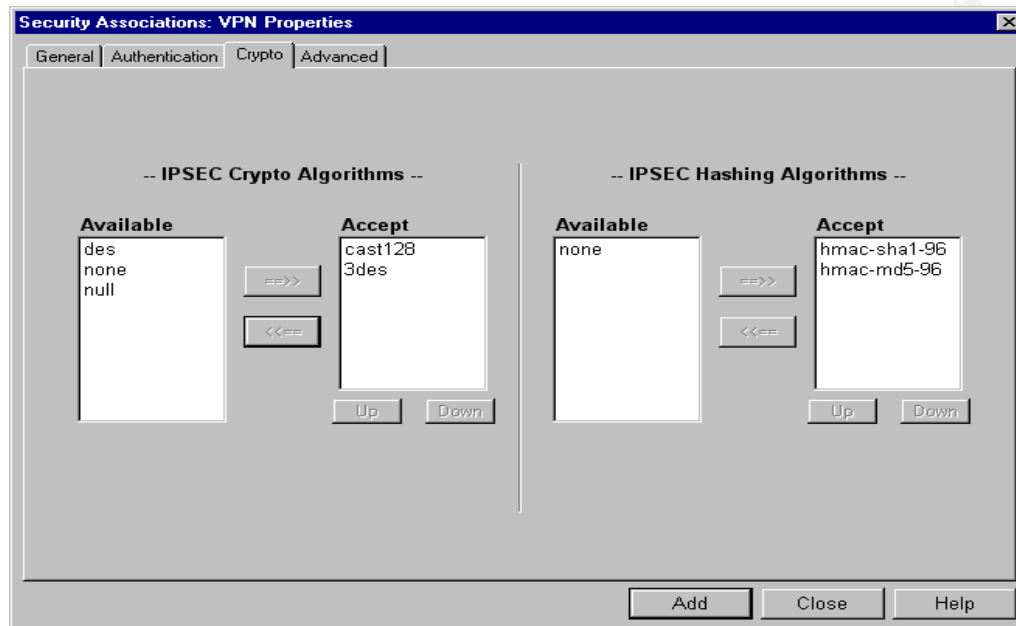
Here we add **basic information** about this VPN association. The IPSec standards define two different modes of encryption processing: tunnel mode and transport mode. In transport mode, the source and destination addresses contained within the packet headers are visible. Only the data portion of the packet is encrypted, not the ip header. We will always be using Tunnel encapsulation as it encrypts both the header and payload, vice transport, which will NOT protect the header information. We also select the “Mode” which I spoke of above. The Association “mode” depends on whether we are tunneling to a gateway or a group of dynamic clients. We can also apply access rules to these associations. <NOTE: we strongly encourage our admins. to use the “Comments” fields. These fields are throughout the Sidewinder COBRA GUI and help clarify when and why things were created.>



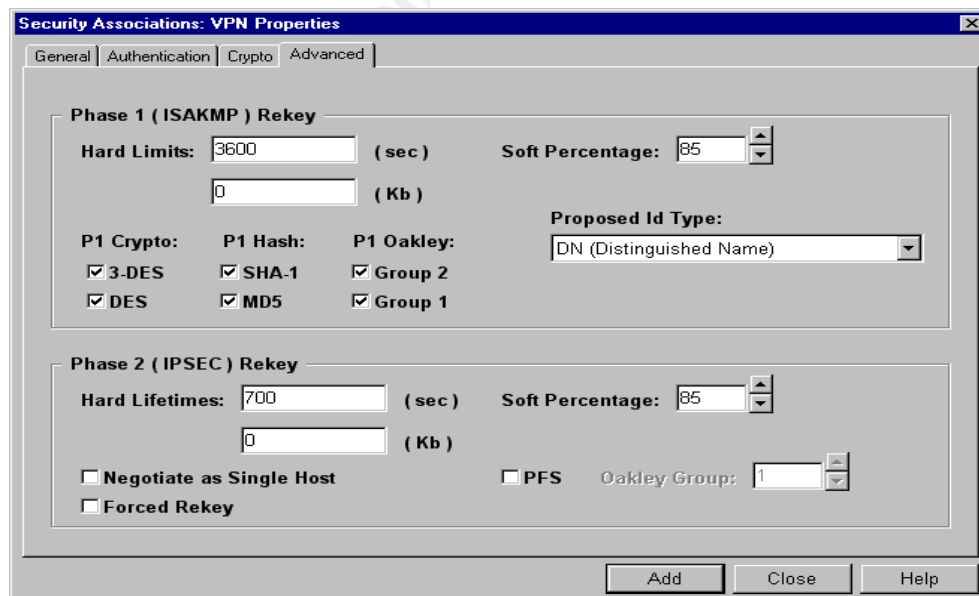
Authentication is provided to prevent hosts from masquerading as a VPN peer of ours. Here we define what type of authentication we prefer. Since we are employing a Private CA server and dealing with an automatic key exchange environment, we are going with the “Certificate + Certificate Authority” option. Our certificate(s) that we defined earlier would appear in this window:



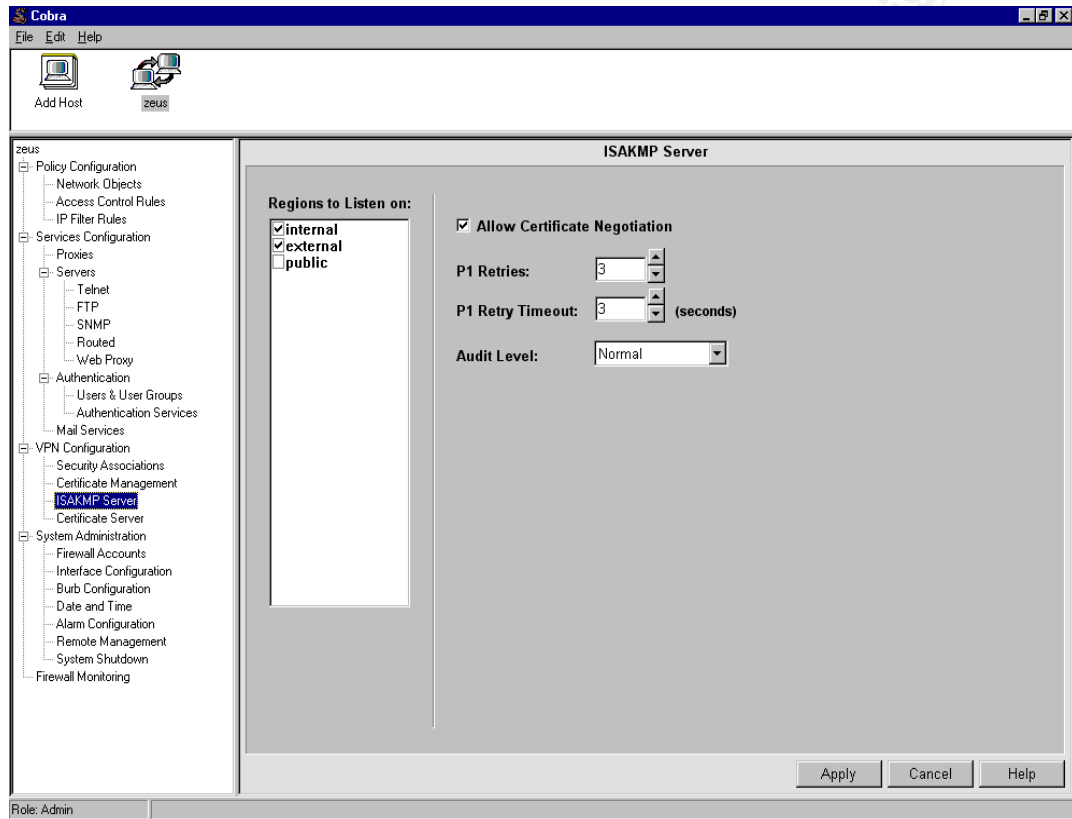
Crypto defines the cryptographic and hashing algorithms used to authenticate our peer(s) in this Association. We will be accepting only Cast128 and Triple-DES encryption and both available Hash types (i.e. sha1-96 and md5-96).



The “**Advanced**” tab is not very necessary to tweak. These settings are pretty much referring to how to narrow down the certificate exchange and re-keying preferences. We are generally going with the defaults, as they are industry-recognized settings, particularly the re-key lifetimes.



Finally, because we are using an automatic key exchange configuration, we must now setup the **ISAKMP Server**. It is this server that generates and exchanges keys for VPN sessions. The Server will be listening on both “Regions.” Since we are not utilizing an LDAP server (or some other certificate database), it is very important to ensure that the “Allow Certificate Negotiation” setting is toggled on. This setting allows ISAKMP to send and receive certificates with remote peers using this protocol (i.e. ISAKMP). Without it, we would have to hold and maintain all peers’ certificates in a database of some sort. The packet retries and timeout are left at the defaults and we’ll keep the audit level at “Normal” unless we run into troubleshooting scenarios.



Conclusion

That will complete our VPN setup. We will have to configure multiple “Associations” as we come across more unique partners and suppliers. More importantly, while VPNs have become much easier to setup, significant research is still required prior to pointing and clicking. While Sidewinder comes with its proprietary *SecureClient* software for clients to use to connect to it directly to tunnel in, providers and suppliers will not necessarily be implementing a Sidewinder VPN solution. Others’ VPN solutions must be given a second look in order to ensure that they’ll integrate with ours.

Assignment 3 - Audit Your Security Architecture

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

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

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

Assessment Plan

Firstly, a comprehensive and thorough security audit must first include a review of all of the actual security-related policies and directives drafted for the organization. We are assuming that GIAC Enterprises already possesses some of these documents and that we must first review them for content and accuracy. This may be the time for extensive edits in order to reflect an accurate portrayal of the current architecture and to structure our policies such that they allow for flexibility and growth within the organization, while still providing for the framework and guidance of a locked down infrastructure. The policies should be articulate and straightforward and shall be signed off by our IAPM as well as our Senior Vice President.

Secondly, due to the sensitive and comprehensive nature of audits – bandwidth intensive probes, network/system fingerprinting tools, password cracking, policy analyses, log analyses, access control analyses, account policies, penetration scenarios, etc. – the impact on operations, both technologically and procedurally, can be substantial. As a result, management buy in is paramount in order to actually follow through with the audit. Full support should be received from the highest possible individual in the organizational hierarchy (e.g. CIO), if possible. System downtime will most likely need to be scheduled, as some systems will not be able to be down or

scanned against during normal operating hours. A kick-off meeting shall be arranged with the highest supporting individual and should include representatives from all affected organization divisions and departments. An agenda can be consummated at this time and include the hours of downtime as well. A follow-on meeting shall be held with the specific auditing team and shall include all of the System Administrators (SAs) needed for support during the audit. In this meeting, the risks involved with the scanning and fingerprinting of the network/systems shall be explained, including the possibility of some systems crashing as a result of the scans. If time permits, a brief “Roles and Responsibilities” memorandum should be drafted to outline the SA’s various responsibilities while the organization undergoes the audit (e.g. IDS analyst, Firewall analyst, Router/Network analyst, Scanning Analyst, NT expert, etc.). Of course, some of these roles will overlap one and other.

Thirdly, the audit costs would mainly consist of the time required for the scans and analysis. A rough approximate of this would be 3-5 full business days (8am-5pm). The time is contingent on a number of conditions, for example, number of hosts to audit/scan, amount of traffic occurring during scans, tools used, availability and access to computers, etc. Heavier scans, including those against the Firewall itself, would need to be scheduled during non-business hours, as they will exert a heavy toll on the equipment. With ideal conditions, 3-4 days should be more than enough. Since the majority of tools used are free or shareware downloadable from the Internet and that, assumingly, the equipment the tools are loaded on is preexisting, the hardware/software costs are minimal. I estimate that a minimum of four employees would be necessary to conduct a thorough assessment and a reasonable rate for this level of work would be \$110/hour. For four employees at approximately 8 hours per day over 4 days, the cost for the assessment will be approximately \$19,200.

Finally, follow-up assessments shall be conducted on an annual basis at a minimum, preferably every six to nine months. An information systems audit does not end with the first one; it is an ongoing living and breathing effort and practice. A neutral third-party shall be brought into the organization to give an unabridged and unbiased analysis of GIAC Enterprise’s current information security posture. In between these third-party audits, GIAC Enterprises shall conduct its own scans using tools such as, Nessus, L0phtcrack, ISS, etc., to ensure the ongoing compliance with the changes that were made as part of the initial assessment and implementation.

Implementation

There are literally countless tools that can be used as part of an assessment, many of which are freeware or shareware, others of which are Commercial-Off-the-Shelf. We will move forward with our implementation with a combination of each.

We can first gather a large amount of basic information about the network through various O/S included tools.

Whois (A free tool – website(s) to gather Domain Name Registration)

(NOTE: The results here are fictitious and for purposes of the assignment only. I'm making the assumption that, like other public Internet websites, Giacenterprises.com will have its basic information listed with the Domain Name databases.)

Domain Name: GIACENTERPRISES.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES
WORLDWIDE
Whois Server: whois.InternetNamesWW.com
Referral URL: http://www.InternetNamesWW.com
Name Server: WWW.3DMEDIATION.COM
Name Server: SIMON.GIACENTERPRISES.COM
Updated Date: 30-mar-2001
The Registry database contains ONLY .COM, .NET, .ORG, .EDU
domains and
Registrars.

Domain Name..... giacenterprises.com
Creation Date..... 2001-02-10
Registration Date.... 2001-02-10
Expiry Date..... 2003-02-10
Organisation Name....Scott Stevens
Organisation Address. 5805 North 26th Street
Organisation Address.
Organisation Address. Arlington
Organisation Address. VA
Organisation Address.22207
Organisation Address. USA

Admin Name..... Scott Stevens
Admin Address..... 5805 North 26th Street
Admin Address.....
Admin Address..... Arlington
Admin Address.....VA
Admin Address..... 22207
Admin Address..... USA
Admin Email..... sstevens@nciinc.com
Admin Phone..... (703) 428-2147
Admin Fax.....

Tech Name..... Scott Stevens
Tech Address..... 5805 North 26th Street

```
Tech Address.....
Tech Address..... Arlington
Tech Address..... VA
Tech Address..... 22207
Tech Address..... USA
Tech Email..... sstevens@nciinc.com
Tech Phone..... (703) 428-2147
Tech Fax.....
Name Server..... simon.giacenterprises.com
Name Server..... www.3dmediation.com
```

Nslookup (to gather IP information about the Name Servers)

(NOTE: The results listed here are fictitious as there is no giacenterprises.com domain. They are for the assignment scenario only).

```
C:\>nslookup
```

```
Default Server: www.3dmediation.com
Address: 208.193.112.3
```

```
> giacenterprises.com (fictitious name obviously)
```

```
Default Server: www.3dmediation.com
Address: 208.193.112.3
```

```
Non-authoritative answer:
```

```
Name: giacenterprises.com
Address: 203.52.96.178
```

```
> set type=ns
```

```
> giacenterprises.com
```

```
Default Server: www.3dmediation.com
Address: 208.193.112.3
```

```
Non-authoritative answer:
```

```
giacenterprises.com nameserver = simon.giacenterprises.com
```

```
simon.giacenterprises.com internet address = 203.52.96.178
```

```
Default Server: www.3dmediation.com Address: 208.193.112.4
```

We'll now attempt a zone transfer from external name servers:

```
> ls -d giacenterprises.com
```

[www.3dmediation.com]

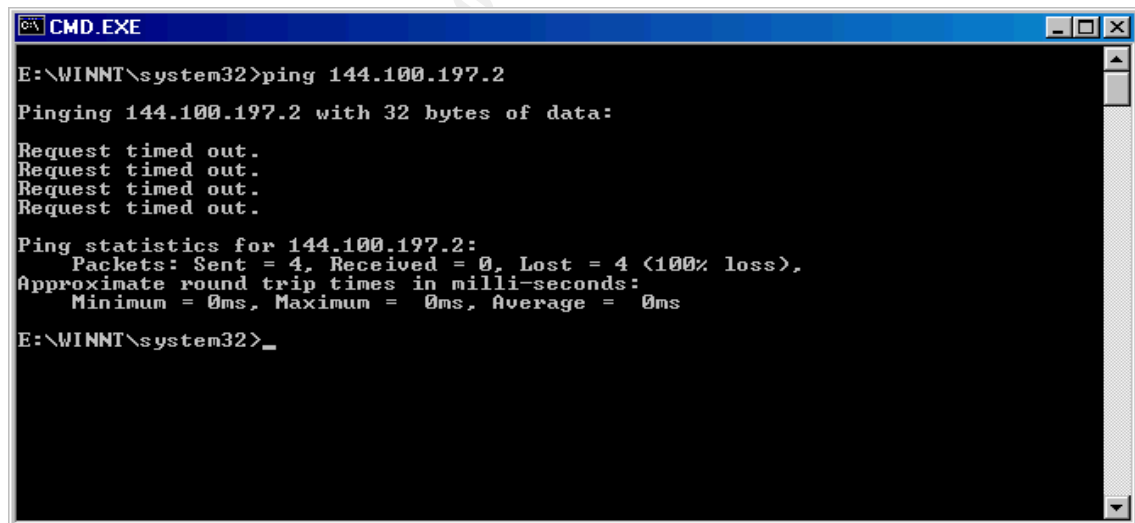
*** Can't list domain giacenterprises.com: Query refused

The zone transfer was obviously unsuccessful.

Ping (To test for connectivity)

NOTE: For these simple connectivity tests I will be “sourcing” from various addresses. Some are from my workplace and others are from my home. Please disregard the source addresses for the purposes of this scenario. Also, when I make the second Telnet attempt from a “DMZ host” please disregard its source address, as its actually from a host at my workplace and not representative of my architecture’s DMZ addressing scheme.

We begin with a simple ICMP echo request to confirm that our firewall policy (specifically, ACL # 5) is properly responding. We’ll assume the below address is the external IP of the primary firewall (Sidewinder) and that the test originates from an external, un-trusted host.



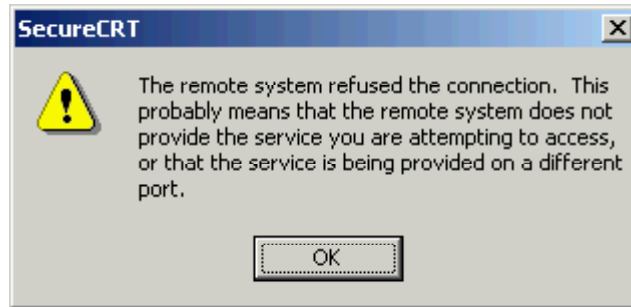
```
CMD.EXE
E:\WINNT\system32>ping 144.100.197.2
Pinging 144.100.197.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 144.100.197.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
E:\WINNT\system32>
```

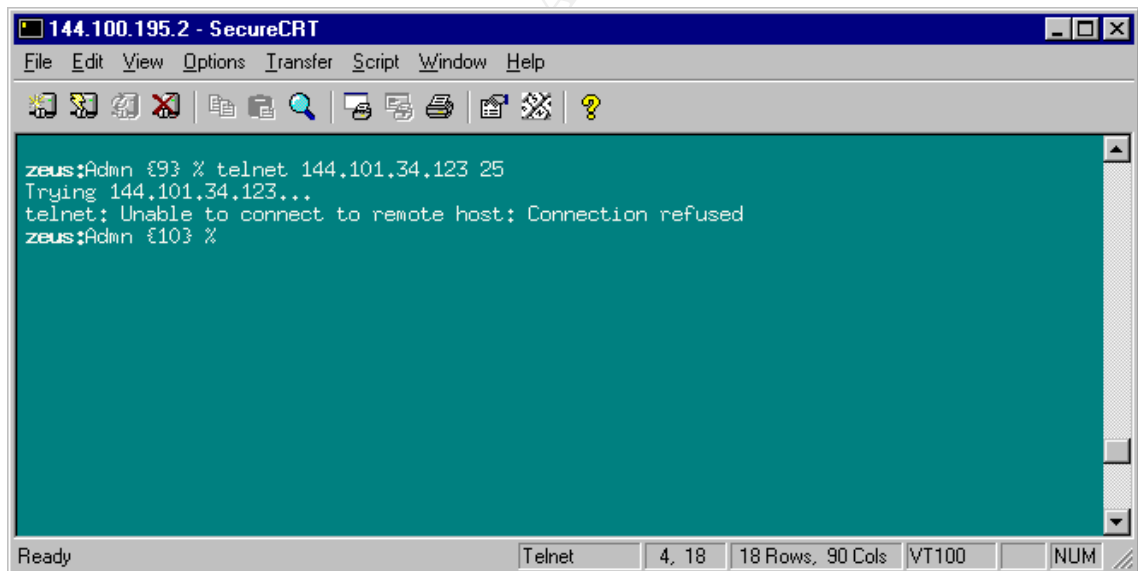
Telnet (To test for connectivity and verify rules)

Telnet is a simple but thorough tool, as it sits at the Application layer, and can therefore test for connectivity through all seven layers. (We will never use Telnet when sensitive machine passwords are to be authenticated). Again, from an external, un-trusted host, we this time make a Telnet attempt to an internal host on various ports (i.e. ports not globally allowed in our Firewall rule-set). What we end up with is basically a connection refused (dialogue box pasted right out

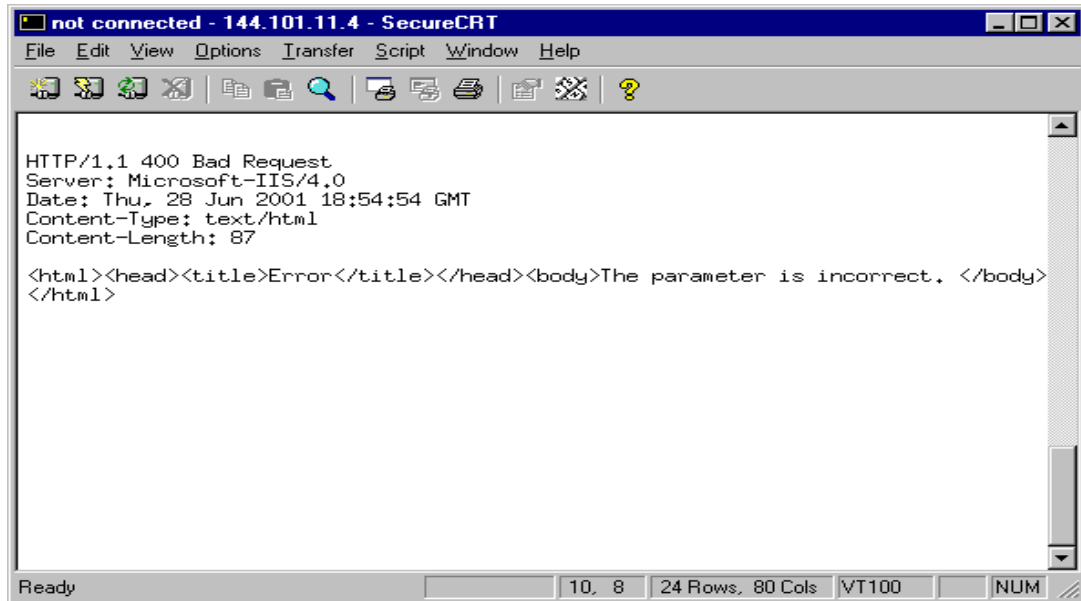
of SecureCRT interface):



We attempt an additional Telnet test to confirm that, from our WWW server on the screened (DMZ) segment (hypothetically), we cannot get to the SMTP port of one of our internal Mail servers. This is in line with our rule early in the set that disallows all traffic stemming from the screened segment, as indicated with another refused connection:



We now attempt a Telnet connection from an external, un-trusted host via Port 80 to our Webserver on the DMZ:



```
not connected - 144.101.11.4 - SecureCRT
File Edit View Options Transfer Script Window Help
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Thu, 28 Jun 2001 18:54:54 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.</body>
</html>
Ready 10, 8 24 Rows, 80 Cols VT100 NUM
```

We're able to see our Web Server's Banner information. While the server is not necessarily vulnerable, we are advertising too much information here and providing a quick starting point for an attacker by identifying the platform type and IIS version. We'll readdress this in Part 3 of this assignment.

Nmap (To identify open ports and fingerprint the network)

NMap is one of the most popular auditing tools available and is a freely downloadable open source utility (<http://www.insecure.org/NMap/>). It is a great starter tool in ones attempts to map out and audit your network. Via Nmap, we can attempt to capture various systems' banners and identify which ports it's listening on. I ran Nmap against the primary firewall. I initially ran Nmap with `-sT` which tells it to perform a basic TCP port scan on all interesting port, generally all ports under 1024. I then used option `-sU` which forces a UDP port scan on all interesting ports. I finally performed an `-sS` which forces a TCP SYN scan – a “half-open” port scan, which should get back a SYN-ACK, indicating the port is listening. The results are as follows:

```
# ./nmap -v -sS -P0 -O x.x.x.x
```

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

Interesting ports on .zeus.giacenterprises.com (x.x.x.x):

(The 2960 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp


```
22/tcp....open.....ssh
25/tcp  open      smtp
80/tcp  open      http
113/tcp open      auth
443/tcp open      https
1531/tcp...open.....sql
```

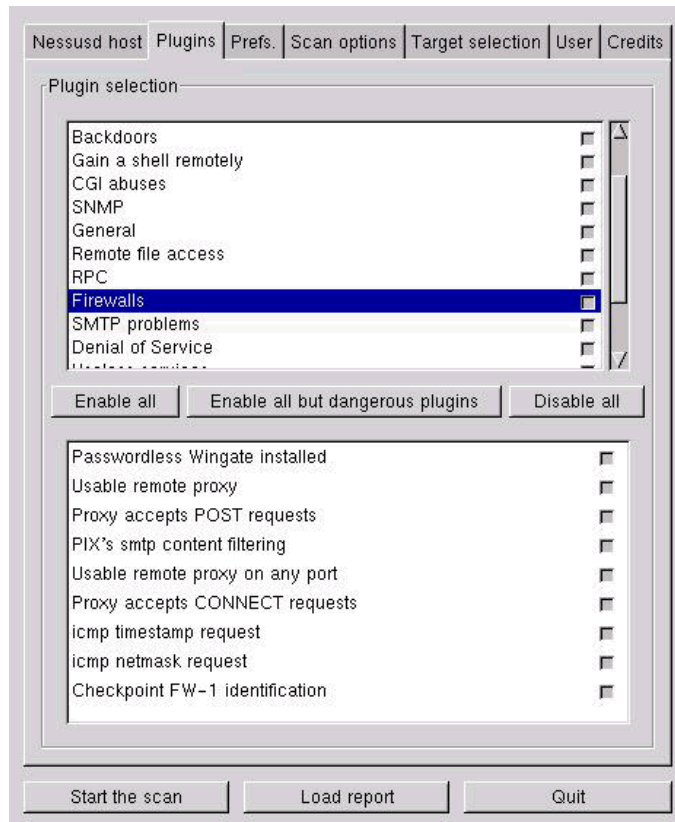
Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds

Our Nmap scan against the Sidewinder was not able to return the Operating System type, which is probably related to its “Type Enforcement” lockdown of the OS.

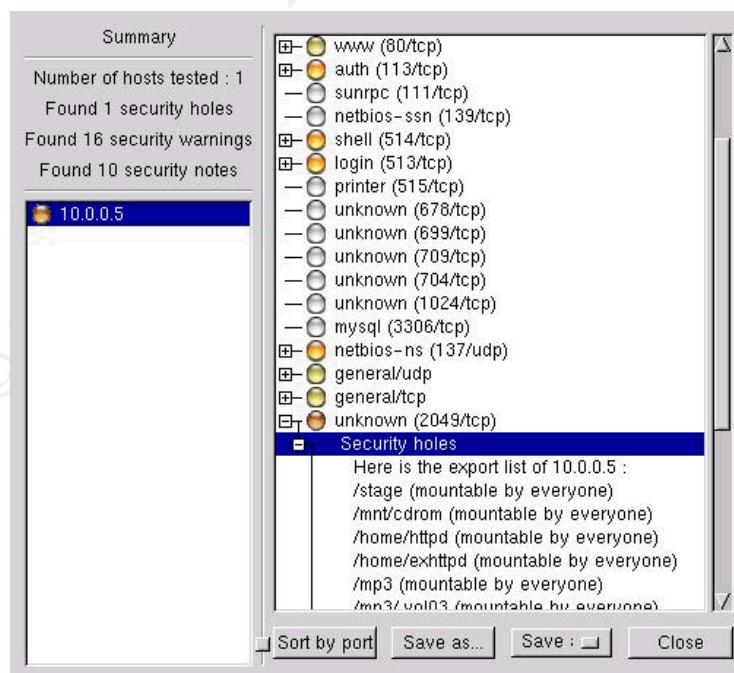
Nessus:

One other open source and popular tool is Nessus (<http://www.nessus.org/>). Nessus does a very good job of protocol/port scanning while providing comprehensive reports, all at no cost as part of our implementation. Nessus is very comparable to COTS scanners such as ISS System Scanner, and, for Unix platforms, probably even holds an edge on a scanner such as ISS’s. Many security industry pundits consider Nessus “the scanner of choice.” With Nessus, we would scan the entire network, segment by segment. As mentioned in our Assessment, we will most likely need to run some of these scans during “non-operational” hours, as they will severely stifle the resources of the systems being scanned.

I was not able to receive permission to actually run Nessus against our firewall. The illustrations below serve as examples only. While Sidewinder is very protective of its OS, I’m confident Nessus would return more results than Nmap based on past experiences of running it against Unix-based hosts. The illustration below outlines the various plugins that we would add. The more plugins added, the more likely the vulnerabilities within systems will be discovered during scans. Specific plugins need to be researched more closely if there appears to be a chance of crashing specific platforms. Below the window are those options respective of the plugin selected.



The next illustration reveals some results of an example scan that we would run against a host on the GIAC Enterprises network. A summation exists in the upper left hand corner outlining the number of security holes, security warnings, and security “notes” discovered.



Nessus scan results.

Perimeter Analysis

As a result of our assessment and resulting implementation, we can now look back and reflect on some architectural and engineering improvements and recommendations to further strengthen our security profile.

So from our scans we can at least start plugging away at those ports that we know are open and start attempting a compromise of the Public WWW IIS Server via all of the exploitable IIS holes (<http://www.securityfocus.com/>). One improvement could be to modify all servers that advertise banner information so that either false information or no information at all appears. We also know the following:

- Router - There are a handful of exploits against Cisco Routers available on the internet (<http://www.securitytracker.com/archives/target/70.html>)
- Firewall – Even though we were unsuccessful in identifying the OS of the firewall, from our scan it appears it is stopping traffic at the perimeter as expected. It is also noted that different scan types had no additional or less effect which should be indicative of the stateful-like nature of the Sidewinder. Our next step would be to attempt to spoof packets to bypass the firewall.
- Internal Services – We know that some servers are providing services on SMTP (25), HTTP (80), HTTPS(443), SSH (22), and SQL (1531). Most of these services have vulnerabilities associated with them. A simple Telnet session will often reveal what is running on these services. Another visit to www.securityfocus.com and other sites will tell us what vulnerabilities are current for the products in use.

Other Recommendations

Host-based Firewalls

Even though we didn't demonstrate an attack and exploit on an internal workstation, a nice additional layer of defense is, as part of the baseline image I referred to earlier, for workstations, or at least more sensitive workstations, such as dedicated security workstations, we could deploy personal firewall software and IDS software installed on them (e.g. Norton's Personal Firewall or Network Ice's Defender), which will further enhance their security posture.

TCP Wrappers & IP Filter/IP Tables

In line with the workstation firewalls, we can also implement TCP Wrappers and IP Filter (or IP Chains/Tables for any Linux-based hosts) to add a layer of security to the our Unix servers. These filters will effectively block attempts to connect to it from unknown addresses. (Spoofed addresses will generally still get by if the TCP Wrapper configuration allows it). SANS publishes excellent resources covering the proper installation of such software for a nominal fee (<http://www.sansstore.org/>).

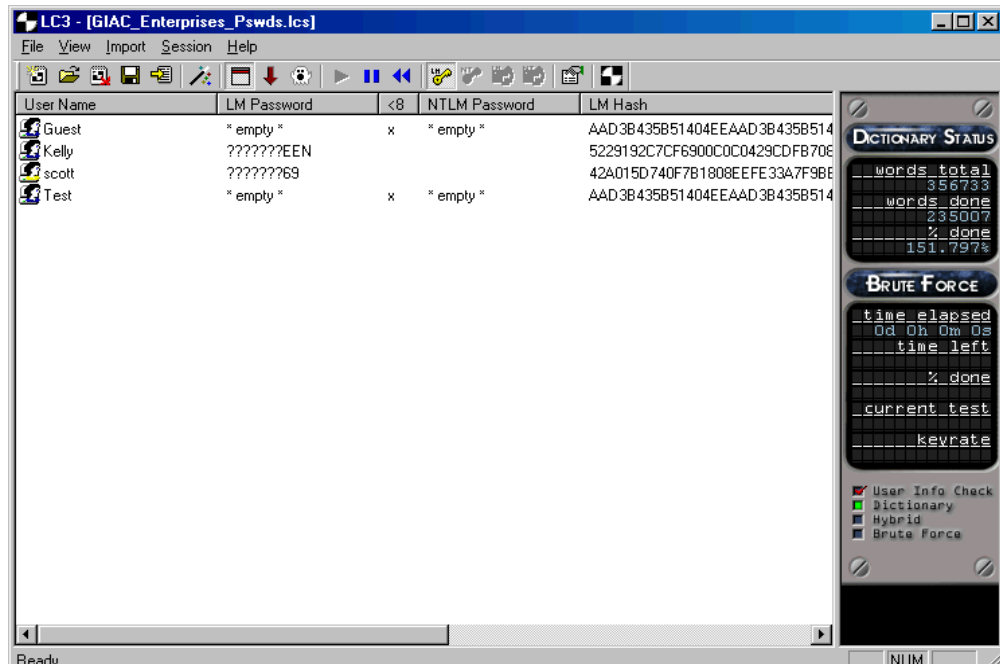
Honeypot/Deception Hosts

Additionally, other deception type hosts, for example, Recourse Technologies ManTrap (represents four hosts or “cages” within one quad-card Solaris machine and advertises certain services). These boxes will pickup on attempted attacks and will then either alert the administrator of the attack and possibly trap the attacker in his tracks. It also gives an organization the ability to stay on top of what real-world attacks are occurring on the Internet and on against the organization’s systems.

Password Integrity

Another subject area that wasn’t addressed as part of the “attack” but certainly is a sensitive area and paramount to a security shop’s success is password integrity. Until biometrics fully takes off in mainstream IT shops, organizations will need to continue to find ways to keep passwords strong.

To be reassured that the *Passfilt* tool is actually enforcing GIAC’s password policy and to assure users are not finding ways of bypassing it, GIAC Enterprises will use the popular *L0phtcrack* utility (<http://www.l0pht.com/l0phtcrack>) to check for password integrity within the Domain Controllers Security Account Manager. While we hope to eventually have all SAs run this locally against their locally established accounts on their NT Member Servers, our focus would first be simply against the Domain Controllers. Below is an example screen capture of the L0phtcrack utility processing against GIAC’s SAM database on its PDC:



GIAC Enterprises also consists of a handful of Unix-based systems for various specialized roles (e.g., Name Server, Mail Relay, Custom Applications and Database Servers). To check for password integrity on these systems GIAC Enterprises will use the popular and freely available Crack for Unix tool (<http://www.users.dircon.co.uk/~crypto/>). Both of these tools will be run against offline copies of the servers' accounts database so that the network is not disturbed as part of this resource intensive process.

Conclusion

The firewall is only opening up the services that are allowed to be accessed. It is a matter of ensuring that these services are secure and up to date with known vulnerabilities. It is much more likely that an attack will come straight through the firewall and hit the web server on Port 80, than it is the firewall itself is attacked. If the web server is compromised, it could then be used to do exploit critical areas of the internal network. The structure however helps to minimize the effect of sniffers, and any tools with known signatures will hopefully appear in the IDSs. The only exception would be if the attacker established a HTTPS session to the Web server.

In short, the results of the scans should be documented, examined closely and patched accordingly. For those that impact functionality of a machine (e.g. a vulnerable Unix daemon that needs to run at startup), alternate workarounds should be explored if no patches have been released. The organization as a

whole should adopt a “disable if not necessary” philosophy. Finally, again, the scans shall be conducted on a regular basis (i.e. at least every 6 mos.) to keep current with the constantly evolving exploits with technology.

© SANS Institute 2000 - 2002, Author retains full rights.

Assignment 4 - Design Under Fire

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (<http://www.sans.org/giactc/gcfw.htm>) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

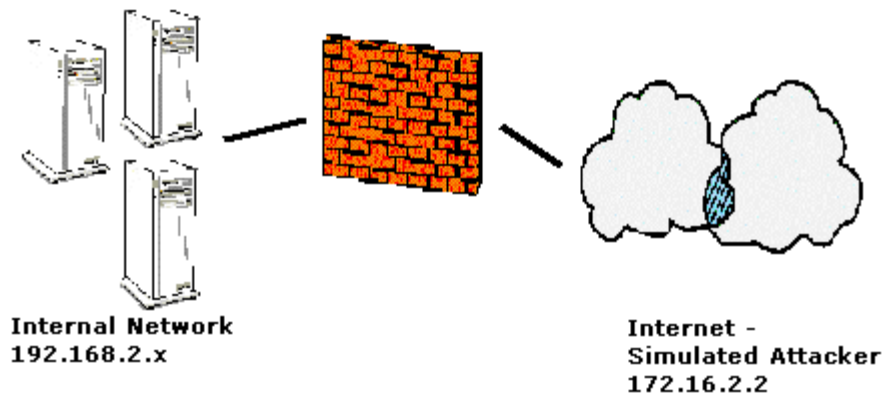
An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.

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.

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.

The purpose of this assignment is to select a previously posted GCFW practical and attack it. The attack will have three parts to it. First, I will attack the firewall itself trying to find vulnerabilities in the product chosen. Next, I will initiate a distributed denial of service (DDoS) attack against the design, limited to tcp SYN, udp, or ICMP floods. Finally, I will attempt to compromise an internal system through the perimeter.

The security chosen is Dujko Radovnikovic's (don't ask me to pronounce it) and can be found at http://www.sans.org/y2k/practical/Dujko_Radovnikovic.doc. He chooses to run his firewall as a Linux IPChains host. His firewall rules, as illustrated below, prevent access to his screened segment. I'm assuming, based on his overall architecture, that he made the mistake of "un-commenting" the access rules for DNS and WWW. I took the liberty of un-commenting out these rules. His design is as follows:



The IPChains rules are as follows:

```
#!/bin/sh
#
# rc.firewall
#
SCREENEDIF="eth1"
SCREENEDNET="192.168.2.0/24"
SCREENEDIP="192.168.2.1"
#
EXTERNALIF="eth0"
EXTERNALNET="172.16.0.0/12"
EXTERNALIP="172.16.2.1"
# Variable used to store location of ipchains binary
IPCHAINS="/sbin/ipchains"
#
# Enable IP Forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
#
# Flush everything
# Incoming packets from outside network
$IPCHAINS -F input
# Outgoing packets from internal network
$IPCHAINS -F output
# Forwarding/masquerading
$IPCHAINS -F forward
#
# Spoofing and Source Route Protection
for x in /proc/sys/net/ipv4/conf/*; do
if [ -f $x/rp_filter ]; then
echo 2 > $x/rp_filter
fi
```



```
if [ -f $x/accept_source_route ]; then
echo 0 > $x/accept_source_route
fi
if [ -f $x/log_martians ]; then
echo 1 > $x/log_martians
fi
done
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
#
## Login Services
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 21 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 22 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 23 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 139 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 512:514 -l -j DENY
#
## RPC and NFS
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 111 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 111 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 2049 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 2049 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 4045 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 4045 -l -j DENY
#
## NetBIOS in Windows NT
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 135 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 135 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 137 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 138 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 139 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 445 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 445 -l -j DENY
#
## X Windows
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 6000:6025 -l -j
DENY
#
## Naming Services
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 53 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 192.168.2.3 53 -l -j
ACCEPT
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 53 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 389 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 389 -l -j DENY
```

```
#
## Mail Services
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 25 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 109 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 110 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 143 -l -j DENY
#
## Web
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 192.168.2.4 80 -l -j
ACCEPT
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 80 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 443 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 8000 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 8080 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 8888 -l -j DENY
#
## Small Services
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 1:20 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 1:20 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 37 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 37 -l -j DENY
#
## Miscellaneous
#
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 69 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 79 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 119 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 123 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 514 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 515 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 161 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 161 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 162 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p udp -s 0/0 -d 0/0 162 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 179 -l -j DENY
$IPCHAINS -A input -i $EXTERNALIF -p tcp -s 0/0 -d 0/0 1080 -l -j DENY
## ICMP
#
$IPCHAINS -A input -i $EXTERNALIF -p icmp --icmp-type 8 -s 0/0 -d 0/0 -l -j
DENY
$IPCHAINS -A output -i $EXTERNALIF -p icmp --icmp-type 0 -s 0/0 -d 0/0 -l -j
DENY
$IPCHAINS -A output -i $EXTERNALIF -p icmp --icmp-type 3 -s 0/0 -d 0/0 -l -j
DENY
```

```
$IPCHAINS -A output -i $EXTERNALIF -p icmp --icmp-type 11 -s 0/0 -d 0/0 -l  
-j DENY  
#  
# All data that is not specified to be accepted, and that does not match any of  
the DENY  
# rules above will be effectively denied by the following rules.  
#  
$IPCHAINS -A input -j DENY  
$IPCHAINS -A output -j DENY  
$IPCHAINS -A forward -j ACCEPT
```

Firewall Attack

The version of IPChains is 1.3.9 and running on a Slackware Linux kernel (version 2.2.16). After a fairly exhausting search for vulnerabilities on the Web, I decided to pursue the *imapd* daemon for possible exploit. (I'm making the sweeping assumption that he left this service on within the Linux box's *inetd.conf* file).

The exploit I chose can be found at www.securityfocus.com and searching on Slackware Linux. This exploit uses the *imap* service to attempt to gain a shell to the server. However, you must first:

- Download the source;
- Compile the source;
- Launch it with the following options: `<host> <login ID> <password> <type> [offset]` - with `<host>` being the hostname (if able to resolve through DNS) or the IP, `<login ID>` being the potential attacker, `<password>` being the password for that account, and `<type>` being choices 0-3 which indicate the various vulnerable distributions of *imapd* on Linux (0=7.0, 1=7.1, and so on). The `<offset>` can be used to further manipulate the exploit.

Its "to be determined" whether this attack will actually work or not. The administrator may not have left this process running in which case it will fail.

Denial of Service Attack

Our next attack stems from the compromise of 50 cable modems on the Internet to construct a traditional DoS against Dujko's network. The DoS can exist in the form of TCP SYN, UPD, or ICMP floods. The 50 high-speed connections should facilitate this attack nicely and should be adequate to bring the network to

a significantly slower speed, if not fulfill the absolute Denial of Service, thereby preventing it from servicing any further customer requests.

The exploit I'll choose is the popular Tribe Flood Network 2000 (tfn2k) to use in the attack. This exploit gained popularity as they were suspected of being used during the popular February 2000 attacks against popular Internet sites. More background on the exploit can be read at:

<http://www.cai.com/virusinfo/encyclopedia/descriptions/t/tfn.htm>. The source code can be found at: packetstorm.securify.com/distributed/tfn2k.tgz. The following must occur to prepare for the attack:

- untar the source code;
- edit src and makefile to uncomment the appropriate O/S for the compiling;
- distribute the server daemon (td) to the 50 compromised cable modem hosts;
- build a file listing fully qualified hostnames/IP addresses of the cable modem hosts;
- startup the client (tfn) on my machine and then instruct the cable modem hosts to point to Dujko's network.

This code is flexible enough to run on multiple platforms. This is a nice plus since it's very likely the cable modem hosts are running different O/S's. I am now capable of performing TCP SYN attacks, UDP floods, and ICMP floods. TFN2K also has options to spoof the source addresses.

While many firewall products may do a very good job of protecting you from these types of DDoS's, with enough resources at your disposal, let's say 500 live high-speed connections, in all likelihood would bring many of these devices to its knees, thereby succeeding in its purpose.

Internal System Attack

I will now choose, like many others submitting their practicals, to attack Dujko's internal Name Server. This of course is somewhat unfair in that I recognize that, based on the submittal date of the paper, it's likely his Name Servers, running BIND, have not been updated past 8.2.3. I will attempt to capitalize on the TSIG bug (packetstorm.securify.com/0102-exploits/tsig_bind.c). If the DNS is in fact exploitable (i.e. not updated past 8.2.3), then, once the source is compiled, this exploit will give me a shell as a result of a buffer overflow. The shell will run with the same privileges as the *named* process.

References/Acknowledgements

Benton, Chris; Northcutt, Stephen; Spitzner, Lance. GCFW Course Materials, The SANS Institute.

Firewalls 24 Seven: Matthew Strebe, Sybex Network Press

Hacking Exposed: McClure, Scambray, Kurtz, Osborne/McGraw-Hill Books.

SSH : <http://www.ssh.com/> - Secure shel remote administration tool for Unix and Windows.

<http://www.sctc.com/> - Secure Computing website for Sidewinder information and references.

<http://www.nmap.org/> - Nmap is a network port scanner – an essential tool for the network security hacker.

www.sans.org - SANS Institute, an all-encompassing website for security information.

<http://www.enteract.com/~lspitz/rules.html> - Lance Spitzner's website with excellent insight into rule sets.

Thank you SANS for this educational, enlightening, and certainly challenging experience.