Global Information Assurance Certification Paper

GIAC Level Two Firewalls, Perimeter Protection, and VPNs

Practical Assignment for SANS Security New Orleans

January 28- February 2, 2001

By Robert (Bob) Grill, GSEC, GCIA, GCIH
Other Certifications: CISA, CISSP, SSCP, CCNA, CNA

INDEX

Hi, I am the founder, CEO, CTO, CIO and CFO of Giac Enterprises. For business reasons (See Appendix: A), I used the following principles to design my security architecture:

- Spend as little as possible on a monthly basis to preserve cash.
- Make the auditors happy by purchasing "popular" products that they have a checklist for, regardless of cost or functionality.
- The goal is to receive a favorable SAS 70 http://www.sas70.com review to support an unqualified opinion on my financial statements and to go public with an IPO stock price 200 times what the company is worth.

SECURITY ARCHITECTURE (25 Points)

Assignment 1 – 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).

The objective of this architecture section of the paper is to provide the high level laws that which all detail configurations will flow down from. In this case the high level law or policy will be the Visa ten commandments.

All of the network components will be configured to meet the ten simple minimum requirements that Visa Corporation requires that that vendors follow, also known as the "Visa Ten Commandments", as follows:

1. Install and maintain a working firewall to protect data accessible via the Internet.
2. Keep security patches up-to-date.
3. Encrypt stored data accessible from the Internet.
4. Encrypt data sent across open networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data on a "need to know" basis.
7. Assign unique IDs to each person with access to data.
8. Track access to data, including "read only", by unique ID.
9. Don't use vendor-supplied defaults for system passwords and other security parameters.
10. Regularly test security systems and processes.

In addition the following principles will be followed:

- The architecture will be based on attack detection and risk mitigation (elimination will never be assumed).
- Security implementation will be throughout the Giac Network Infrastructure to achieve "defense in depth".
- Implementation of secure management and reporting for network devices.
- Intrusion detection, both host and network based, will be used.

Giac Enterprises will achieve the control objectives outlined in the Information Systems Audit and Control Association (ISACA) – Control Objectives for Information and Related Technology http://www.isaca.org/cobit.htm, the British Standard 7799 for Information Security Management http://www.c-cure.org/bsframes.htm and, RFC 2196 "Site Security Handbook" at http://www.ietf.org/rfc/rfc2196.txt. Those who read this paper can easily go to the links provided if they want to read the high level security policies. This paper addresses security policy at a level closer to the actual implementation.

The two expanded Visa commandments and its effect on the paper.

At recent Internet Security presentation sponsored by the California Bankers Association, a representative from Visa presented "understanding technology risks". Visa reported that they have expanded the 10 commandments by two; accordingly, they now call their minimum security requirements for their vendors the "digital dozen" (catchy?). The two additional requirements are:

- Implement a management policy that addresses information security
- Restrict physical access to information

Implementing a management policy that addresses information security is vital to a secure network. Policies are the glue that holds everything together; security is not achieved by hardware and software alone, it relies significantly on people and their actions. People can only be changed by policies that provide upper management directives, indicators of areas needing attention and general statements of accountability, ethics, goals and objectives and, controls and procedures. To guide the implementation of the Giac architecture a security policy will be supported by:

- Standards
- Contingency Plans
- Standard Operating Procedures
- Job Descriptions
- Mission Statements
- Management Committee Charters

Policies and procedures provide for enforcement of the intentions of the Giac Enterprises' top management.

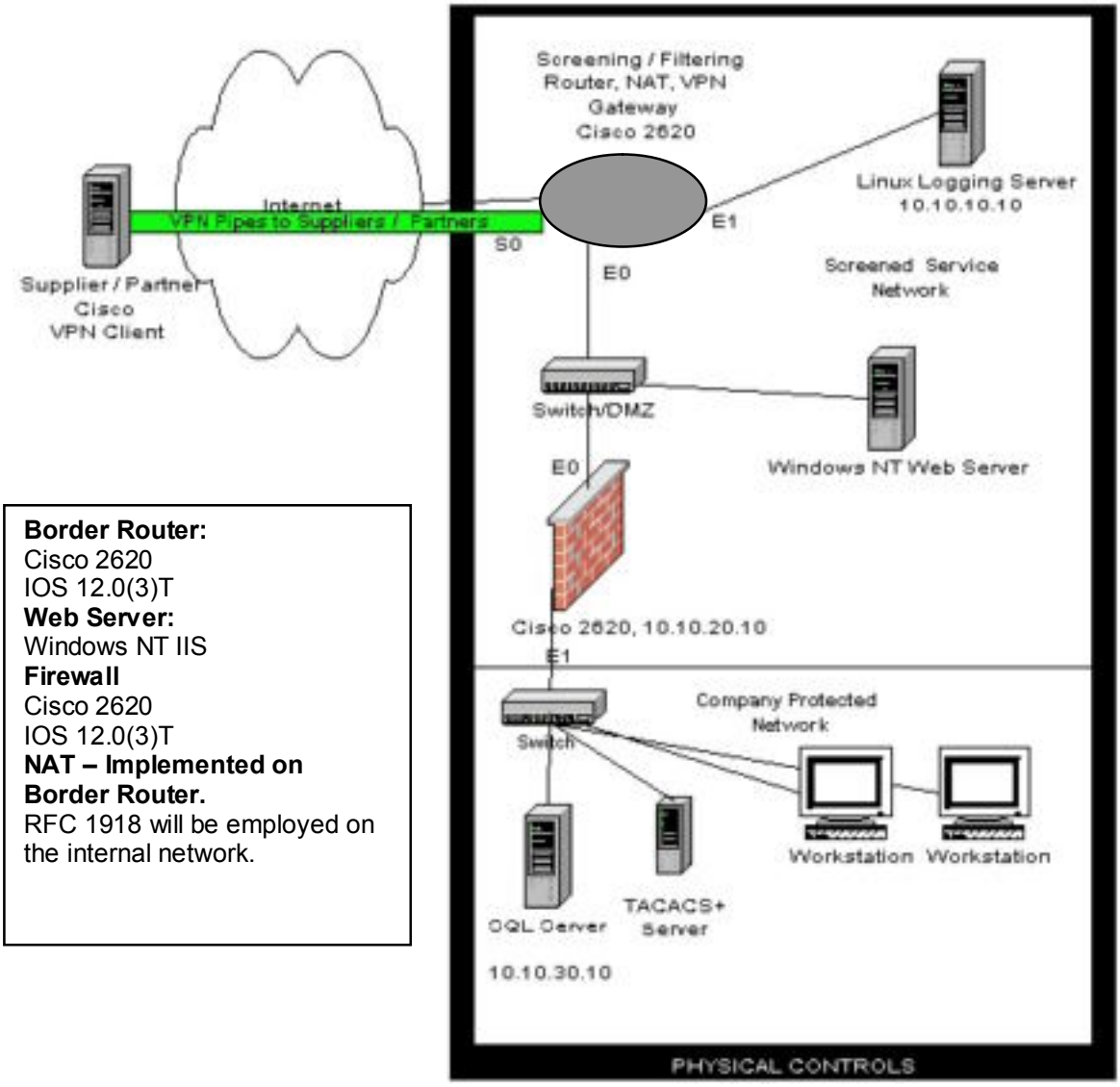
Restricting physical access to information is often overlooked, as it was when the original Ten Commandments were written. However, it is one of the most important. What good is the best firewalls if a hacker can walk in your front door and put a sniffer on your network. It has been my observation that when physical access is achieved, logical access controls are not likely to be effective. Therefore, physical access controls must be included in every information architecture. ISACA recommends physical security control objectives that take into consideration: [3.1]

- Access to facilities
- Site identification
- Physical security
- Inspection and escalation policies
- Business continuity planning and crisis management
- Personnel health and safety
- Preventive maintenance policies
- Environmental threat protection
- Automated monitoring

SANS has an excellent article on this topic at http://www.sans.org/infosecFAQ/firewall/phys_sec.htm. To illustrate how a company without physical controls is vulnerable I would do the following:

Step 1: Go to a Whois database (use the one at http://samspade.org) to find out where the information the company maintains is physically stored.

Step 2: Call the person listed in the Whois database and use "social engineering". Say I am Joe from the backup company and I need to know where to pick up the backup tapes, do you know who I should call. Then call that person and say the first person you contacted told you to call to confirm the physical location.



Border Router:
Cisco 2620
IOS 12.0(3)T
Web Server:
Windows NT IIS
Firewall
Cisco 2620
IOS 12.0(3)T
NAT – Implemented on Border Router.
RFC 1918 will be employed on the internal network.

Step 3: Getting into the building should be easy, just piggy back on someone else, wear a suit, and people will think you are important.

Step 4: Smile and ask a friendly person to show you where the computer room is, use the technical contact for authoritative name dropping. When you see the machine, unhook it and put it in your car, you can then work on getting logical access at home.

The following narrative describes how the architecture on the proceeding page satisfies all of the requirements of the VISA Ten Commandments. The Visa Ten commandments are the basis for security standards being developed by SANS and other organizations (see http://www.cisecurity.org/). Without standards it is difficult to objectively measure the security of an organization. You can't control what you can't measure. The following is a checklist I used to ensure that Giac Enterprises follows the 10 commandments.

1. **Install and maintain a working network firewall to protect data accessible via the Internet.** Yes - This Architecture has a screening router for ISO level 3 and 4 filtering and a stateful firewall.

2. **Keep security patches up-to-date.**

   Daily checks of the following sites are made to ensure GIAC Enterprises stays on top of all security advisories and patches:
   http://www.microsoft.com/technet/security/
   http://www.securityfocus.com
   http://www.cisco.com/warp/public/707/advisory.html
   http://www.cert.org

3. **Encrypt stored data accessible from the Internet.**

   No data will be stored on our web servers as per corporate policy.

4. **Encrypt data sent across public networks.**

   Confidential data sent across public networks will be encrypted with 128 bit SSL or with 3DES with the Giac Enterprises VPN as described later in this paper.

5. **Use and regularly update anti-virus software.**

   On servers and client workstations, McAfee Anti-Virus is used and virus definition (DAT files) are updated regularly.

6. **Data access is restricted on a "need to know" basis.**

   Our partners and suppliers offices utilize VPN software, which is described later in this paper, allows for secure VPN connections back to our VPN gateway.

7. **Assign unique IDs to each person with computer access to data**

   All users are assigned unique login IDs and strong passwords are generated by our servers. No "shared" or "role-based" accounts are allowed.

8. **Track access to data by unique ID.**

   Web and internal network access is logged, allowing us to track access to data by userid. File system auditing is turned on where appropriate to allow for file system auditing. Logs are protected on a secured server and reviewed by a Giac Certified employee on a daily basis.

9. **Don't use vendor-supplied defaults for system passwords and other security parameters.**

L0phtCrack (NT and Unix) and Internet Security Scanner will be used for all of our servers. Network devices such as switches, routers and firewalls are audited to ensure unique strong passwords are used, and any default admin accounts are renamed or disabled.

10. Regularly test security systems and processes

Penetration testing is performed regularly to confirm that configurations are adequate.

Customers (The companies that purchase bulk online fortunes)

The external firewall will be configured to allow only those applications and related protocols with a legitimate "business need". Accordingly, only the TCP protocol will be allowed, with a port of 80 for HTTP or 443 for SSL. To avoid E-Mail hassles HTML based mail will be used by accessing www.hotmail.com, also, it's free - every employee will set up an account. To do business Giac Enterprises will need incoming connections for http and https from the internet to selected hosts on the screened service network. New protocols will be evaluated individually in keeping with Giac corporate policy. Customers will authenticate to our server using HTML based forms, utilizing the POST method only. Giac Enterprises has a strict rule that no data will be stored on the screened network, it will all be pulled back to the corporate protected network by CGI scripts running on the internal network that are never executed by external users or invoke shells. Giac Enterprises will extend credit to all customers, as long as they include a name and address so we can ship the fortune cookie sayings. Credit worthiness will be irrelevant, credit cards will be accepted only after an HTTPS connection is established. Fortune cookie sayings are also available for download, regardless of whether the customer downloaded the fortunes or not all will be shipped to prove sale and thus recognition of revenue. Read Appendix A: Support for $200 million a year in on line sales., for additional explanation of why this approach is followed.

Suppliers (the authors of fortune cookie sayings that connect to supply fortunes)

Suppliers consist of two types anonymous and known. Anonymous suppliers connect to a web interface using an SSL session. They submit their fortune cookie saying ideas through a HTML form. Their address and other contact information are also captured by HTML forms. No data is stored on the web servers. Data is immediately pulled from the data base in the protected network by a CGI script. Known suppliers have Cisco VPN clients set up as outlined in this paper. Company policy is that all data transmitted over public networks will be encrypted.

Partners (the international partners that translate and resell fortunes)

In general, services provided to business partners will be limited to only those services needed, and only to those network devices (servers, routers etc) required. Otherwise, partners will be treated like suppliers. Blanket access shall not be provided for anyone. By default the Giac Enterprises network will deny all access and then allow only those specific services that are needed.

Physical Security

Physical security is often overlooked but all other efforts can be easily defeated if a critical server is located under someone's desk. Card locks will be used to monitor access into restricted areas. The only entry to the server room will be highly visible from the work area and all visitors must sign in and display a visitor badge. All servers, blades and other networking devices will be located in a secure room. Card locks are also used to monitor access to the computer room. Visitors to the computer room must be supervised at all times. Servers and network devices will be locked in separate racks to further restrict access to authorized personnel only.

DNS

Giac Enterprises is a small cheap company, we rely on our ISP for our internet DNS services. Accordingly, there will be no DNS server in our DMZ. WINS will be used for our internal network with the Linux logging machine referenced by IP address only. We will require our ISP to have a SAS70 level 2 review. Hopefully the SAS70 process will force them to harden their DNS servers. Accordingly, the GIAC DHCP server will be configured to point all workstations to the ISP's DNS for name resolution. The Giac NAT will prevent mapping of our internal network.

DMZ

Our DMZ are machines that are exposed to the internet. If they are compromised they will not effect our internal network because of our stateful filtering router (firewall).

SECURITY POLICY (25 Points)

To start out with, all routers and firewalls will be configured to use a TACACS+ server for secure authentication. All ports that have a specific business purpose will be permitted through the border router and firewall. All others will be blocked by the Cisco implicit deny all statement and logged. All configurations will be tested through penetration attempts, with instructions given in the audit program in section 3.

Border Router

Only policy related configurations will be shown for brevity. A "defense in depth" policy will be employed on the Giac Enterprises network. Accordingly, the first layer of defense will be the configuration of the border router. A Cisco 2620 was used because:

- I am a CCNA and I would not have to learn a new system to configure this router. I also don't have time because this paper is due soon.
- This router is also highly expandable and includes firewall and VPN functionality. Relying on one product for router, VPN and firewall does not constitute "defense in depth". Accordingly, two 2620's will be purchased, one as a router and VPN gateway and one as a firewall. Both serve as backups to each other to provide a disaster recovery plan. Now when the auditor asks if I have a disaster recovery plan I can say yes for their checklist. Having all of the network components in one device represents a single point of failure from a reliability standpoint. The brochure is at http://www.cisco.com/univercd/cc/td/doc/pcat/2600.pdf
- It meets the basic objectives I set out at the beginning of this paper.
- When people hear Cisco they think quality, this should help with our pending SAS70. It is also easier to find certified Cisco employees than for other router brands so the risk is lower.
- Supporting Cisco makes my certification more valuable.
- I have had Cisco routers that last over 5 years and the cost is over the capitalization threshold, so I can capitalize the cost per corporate accrual accounting policy. This would make my yearly expenditures lower than with a cheaper router like Juniper that must be expensed by corporate policy.
- It's the cheapest Cisco router I can get with all these features.
- This router is expandable and can grow with the business.

Routers route and firewalls firewall, which means that the more you use your router as a firewall the slower you make it. Accordingly, I just put enough ACLs on the router to protect my DMZ. According to SANS the number one priority of routers is routing but they can be used to perform the following:

- **Block Private Addressing –** There is no reason for packets with a private address (RFC1918) to originate from outside the network. Accordingly, they are illegal traffic that should be blocked.
- **ICMP Traffic –** Applications that work with the ICMP protocol include PING.
- **Block Source Routing -** Source routing is an option in IP that allows the source of a packet to specify the path it will take on the network. Each router hop is included in the packet's header.
- **Application Blocking –** There is a lot to worry about with applications for example:
  - X Windows – tcp port 6000 – 6255.
  - Remote Applications -- telnet – tcp port 23, SSH - tcp port 22, FTP- tcp port 21
  - Windows NT NetBIOS Culprits --137 tcp/udp, 138 – tcp/udp, 139 – udp/tcp.
  - Naming services-- DNS udp 53, DNS zone transfers tcp - 53tcp, LDAP 389 tcp/udp
  - Other HTTP port choices – tcp 8000, 8080, 8888
  - Misc. Services - ports < tcp 20 and < udp 20, graphics – tcp port 41.
  - On and On looking at 65 thousand potential ports.
  - Deny ICMP packets (9th byte in the IP header decimal =1)
  - Block ARP and RIP, EGRP

See http://www.isi.edu/in-notes/iana/assignments/port-numbers for port numbers

Logging will be set up for all deny events and will be pointed to a logging server in the Giac company DMZ on its own interface. The reason I put it on its own interface is to isolate it with my router in case a machine in the screened service network is compromised.

Egress Filtering

The company policy is to block outgoing:

- echo replies
- time exceeded
- unreachable messages
- Traffic with a source address not within the internal network. Since we are employing RFC1918 and 10.0.0.0 255.0.0.0 this is easy.
- All other UDP and ICMP protocol based messages.

To do this, the following inbound ACL will be applied to E1 in on the firewall and E0 on the border router. Throughout this paper, applying to an interface is done by configuring the appropriate interface with an access group, walking the reader through the commands is to basic for this paper. Inbound and outbound are explained in a moment.

Access-list 102 permit tcp 10.0.0.0 0.255.255.255

Everything else will be denied by default.

First the Key to reading CISCO ACL(s) –

- IP Standard access lists - These use only the source IP address in an IP packet to filter the network. This permits or denies an entire suite of protocols.
- Extended access lists - These check for both source and destination IP address, protocol field in the Network layer header, and port number at the Transport layer header.
- For Access Control List (ACL(s)) masks, a 0 means match exactly and a 255 means any.

Once you create an access list, you apply it to an interface with either an inbound or outbound list. With inbound access lists packets are processed through the access list before being routed to the outbound interface. At Giac all ACLs will generally be applied to the inbound interface because it saves on CPU cycles in the router by not allowing the packets to enter the router. With outbound access lists packets are routed to the outbound interface and then processed through the access list. Cisco uses this numbering standard:

<1-99>IP standard access list
<100-199>IP extended access list

This eliminates the majority of the noise originating from the Internet. This configuration is added to block all IANA reserved addresses in the ingress filter. These addresses are (from http://www.arin.net/whois/index.html):

Access lists applied to an inbound serial interface (s0).
Standard Access List (filter on source IP packets)

- **Block Private Addresses (RFC1918) coming from the internet**

access-list 10 deny ip 192.168.0.0 0.0.255.255 any log-input
access-list 10 deny ip 172.16.0.0 0.0.15.255 any log-input
access-list 10 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 10 deny ip 127.0.0.0 0.255.255.255 any log-input
access-list 10 deny ip 0.0.0.0 0.255.255.255 any log-input
access-list 10 deny ip 169.254.0.0 0.0.255.255 any log-input
access-list 10 deny ip 240.0.0.0 15.255.255.255 any log-input

If you are new at this check out Vicki Irwin and Hal Pomeranz's paper at http://www.psionic.com/papers

Extended Access List (100-199) (Filter on address, protocol or TCP port)

- **Block loopback addresses**

Access-list 101 127.0.0.0 0.255.255.255

- **Block Broadcast Addresses Behind the Router**

Access-list 101 deny ip any host 10.10.255.255 (10 is the class B DMZ subnet)
Access-list 101 deny ip any host 10.10.0.0

I can go crazy with deny lists for protocols and 65,535 potential applications. Really all I want to get from the internet to my screened network is HTTP - tcp port 80, SSL – tcp port 443

The following ACL will be listed right after my source address deny (AKA. Standard Access Lists) statements to accomplish this: (by allowing these ports I am not simply blocking everything, as is not allowed by the assignment.)

Access-list 101 permit tcp any any eq 80 - This is for my WWW application. I can use the "any" wildcards here because the packet already went through my source port ACLs above.
Access-list 101 permit tcp any any eq 443 This is for the SSL application

Prevention of Denial of Service Attacks

To prevent SYN flooding attacks TCP intercepts will be used at the border router in watch mode. The timeout will be set to 2 seconds. With TCP intercepts when the router receives a SYN packet it gives the connection 2 seconds (in this case) to establish a connection if it doesn't then it drops the connection. As an added protection aggressive thresholds will be set. With aggressive thresholds, when a router thinks it is under attack it begins to drop connections, either the oldest first or in random order, until the amount of free connections falls below a threshold that is set by the router administrator. The commands look like this:

Ip tcp intercept max-incomplete low number 900

Ip tcp intercept max-incomplete High number 1100
Ip tcp intercept one-minute low number 900
Ip tcp intercept one-minute high number 1100

Logging

The following command starts logging on the border router and sends the messages to our Linux server in the DMZ.

Logging 10.10.10.10

10.10.10.10 is the address of our logging server. See the link below for configuration reference: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/logging.htm.

The logging level on the router has been set to log everything at level 7 with the following command as the router console:

Set logging server severity 7

We will do further filtering after it goes to the logging server. It can be verified with the show logging command.

The following command is entered in the Linux file /etc/syslog.conf file to accommodate the log:

user.debug /var/log/Cisco.log

Everything else is denied by default on a Cisco Router and logged according to our logging level.

Other Router hardening commands

From the interface configuration mode (commands in **Bold)**. See Assignment 1 for the applicable company policy statements to justify these commands. All the commands below are going to be applied to interface S0 IN (the interface to the Internet), when they are not global (entered in global configuration mode). These commands were selected from http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/12cmdsum/12cssec/index.htm I only picked the security options that were relevant to the Giac Enterprises Architecture. I did not turn anything off that was disabled by default, if it was disabled and included because of criticality it was noted in the narrative.

- Disable the generation of ICMP unreachable messages. This can't be done with Access Lists because the messages originate at the border router. Without this command attackers can use this for Ddos attacks and or consume the router's CPU to exhaustion.

  no ip unreachables

- Disable the source routing - can avoid IP address spoofing attacks. Cisco enables (allows) source routing by default.

  no ip source-route

- disable the sending of redirect messages to neighboring routers for less than optimal routes. There are denial of service risks associated with using IP redirects.

  no ip redirects

- Directed broadcasts can be used to multiply the power of denial-of-service attacks (A.k.a Smurf Attacks) and should be disabled on any interface where they're not actually needed.

  no ip directed-broadcast

- Disable Cisco discovery protocol, OSPF updates routing tables itself so CDP is not needed. Don't know of any exploits based on this but it is not needed for the internet.

  no cdp run
  no cdp enable

- Disable proxy Arp, this is not global it must be entered at the S0 interface configuration prompt. This function is disabled to prevent arp related exploits.

  no ip proxy-arp

- Disable multicast route caching – Don't know any exploits related to this, Cisco recommends turning ip mroute-cache off or certain important messages are not logged.

  no ip mroute-cache

- Disable TCP and UDP small services SNMP and Finger – Small service are TCP and UDP ports used for diagnostic services. The services include echo, chargen, and discard. There are allot of Denial of Service attacks using these ports and they are not necessary.

  no service tcp-small-server
  no service udp-small-servers
  no service finger
  no SNMP

- Disable server services for obvious reasons.. (common exploits and not needed)
  No ip http
  No ip bootp

We are using TACACS+ for password management so we do not have to disable virtual terminal access or limit it to one IP address. If we were not using TACACS+ then this would have to be done.

Egress Filtering

This network employs egress filtering to prevent risks from Trojan horse programs like back orifice, firewalk scanning and prevent any unnecessary pollution to the Internet. The access group will be applied to E0 IN on the border router and E1 IN on the firewall.

- **Prevent outgoing ICMP traffic**

Access-List 101 deny icmp any any

- **Prevent outgoing UDP and ICMP packets (UDP is prohibited on our network by corporate policy, no business need)**

Access-List 101 deny udp any any

NAT

Our Cisco base image supports NAT. I have decided to implement it on the border router to hide the addresses of devices behind the router and provide protection against a direct attack from the internet to the screened and trusted network from direct internet attacks. Implementing NAT at

the border router also prevents many VPN hassles, as discussed later in this paper. As mentioned earlier the private addressing scheme will follow RFC 1918. Cisco gives you the choice of translating outgoing addresses by a pool of source addresses or using one source address and keeping track by port number. Since Giac Enterprises can only afford one IP address, the port number option was taken. Below is the commands for the router to make this happen: (Assume the Giac external IP address is 167.216.133.33)

Ip nat pool 1600net 167.216.133.33 167.216.133.33 prefix-length 304
Ip nat inside source list 1 pool 160net overload

These were of course configured on S0.

In addition to the above configuration, only Open Shortest Path First will be the routing protocol implemented on the border router S0 interface. Enhanced Interior Gateway Routing Protocol will be used on the screened service and internal network. Auxiliary ports will also have strong passwords set.

Primary Firewall

The Cisco documentation for using the 2620 router as a Firewall is summarized at http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/f2600_rg.pdf

The primary difference between the border router and the firewall is the sophistication of the filters. The more sophisticated the filter the more processing and memory is required. In this section of the paper the commands for statefull packet inspection will be illustrated. Cisco calls this feature content based access control (CBAC). The CBAC will be configured on the interface to the screened service network – E0 IN. See the Border Router configuration for an explanation if it is not noted below. See Cisco's white paper at http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm for more information.

- The command to define the router name:

  hostname Giac-Firewall

The following commands enable inspection for the protocols we are using on the network and define session timeouts.

ip inspect name from_internal http
ip inspect name from_internal tcp

ip inspect name from_external http
ip inspect name from_external tcp

Apply the following commands to the from_internal and from_external interface so the router knows what which way to enforce state.

Interface Ethernet1

Ip inspect from_internal in

Interface Ethernet1

Ip inspect from_external in

State tables can fill up quickly with syn flood attacks. To prevent this Cisco put timeout settings on TCP connection parameters. When these thresholds are reached the router starts to drop connections not completed to avoid a denial of service.

In addition, the Giac firewall router was set up with more memory. The Giac firewall will have two interfaces. One interface connects to the DMZ switch, and one interface connects to the internal network.

In our example the Cisco router provides additional perimeter defense as well as an internal firewall.

VPN

To ensure confidentiality, data integrity, non-repudiation of source (unlike SSL), protection against replay attacks and prevention against some denial of service attacks, Giac enterprises will incorporate Virtual Private Networking (VPN) using IPSec. IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion. The Tunnel mode encrypts both the header and the payload. Giac Enterprises has selected the Tunnel mode because it is more secure. For example, Giac enterprises has heard every excuse why customer's can't pay their bills. With the Authentication Header (AH) Giac's customers can't deny they placed orders because someone on the internet altered the data they sent to us. With Encapsulating Security Payload (ESP) data is encrypted so our competitors can't read our transmissions with packet sniffers and steal our fortunes. Here is an example of our creative talents – "We are the future, you are, for the past you wanted me to be", is that deep or what. If I would have encrypted the fortune you would have to pay for it to read it. With this in mind, this is why and how we implemented our VPN.

Cisco has the option to use a public or private key infrastructure to encrypt information. We chose the private key method. Using this method, each party shares a secret key that has been exchanged out-of-band and configured into the router. The ability for each side to demonstrate knowledge of this secret key authenticates the exchange. Accordingly, IKE (Internet Key Exchange) will not be employed. This also means that Security Association does not have to be employed.

With Authentication Header (AH) computing a cryptographic function over the datagram with the use of the secret key is performed. The second security mechanism is a encapsulating security payload (ESP), at a high level, this is encryption of the payload.

The Cisco 2620 will be used as the VPN gateways for this network.
http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/vpn26_rg.pdf

This hyperlink tells what commands to enter into the router to start it up.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t2/3desips.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scipsec.htm#4921
and
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/12cmdsum/12cssec/csipsec.htm

When entering the configuration into the router you indicate which IP addresses you want a VPN tunnel with. You also have to enter the keys manually, which is a disadvantage of not employing IKE. The person at the other end of the tunnel has to have a Cisco VPN client already loaded, so this solution will only work with suppliers that you know and are willing to load the client. SSL

would be better in instances where the suppliers and customers are anonymous. With SSL you can't be sure the people you are talking to are who they say they are.

Other design considerations for the VPN will be that it will be filtered first by the Giac border router security policy (implemented by Cisco Access Control Lists). As the SANS GCFW materials point out, putting the VPN outside the firewall has some drawbacks. For example, if the border router gets compromised VPN functionality is compromised, and you have no way of knowing this through monitoring. The decision was made for this architecture by using the Giac Enterprise design principles (cost and audit), this was the cheapest route because it made use of existing equipment and gets me a Yes in the auditors checkbox for VPN's.

Split horizon will be disabled with this VPN scheme because it is not needed.

Host Hardening

Host hardening was not part of this assignment. The Windows NT and LInux hosts will be hardened using the Windows NT and Linux hardening step by step manuals that were provided by SANS when I took the GSEC course. However, I would like to let the reader know that I know of weaknesses in the architecture that I have addressed on my hosts. The architecture does not enable intrusion detection and the screened network machines are not protected by statefull packet inspection. The network also relies on one manufacturer "Cisco" to do all of the protecting, if a major bug was found in Cisco machines, my whole network could be compromised. For this reason IPChains was installed and configured on the logging server, and another host based firewall called Black Ice for the NT (http://www.networkice.com/products/blackice_defender.html) in the DMZ. The Ipchains configuration included logging of unsuccessful connection attempts to act as an intrusion detection system and continually test the border router rule sets.

No customer confidential information will be kept on the DMZ servers. Accordingly, if by the slim chance the DMZ machines are compromised the perpetrators will get no confidential information. The statefull firewall will then prevent them from penetrating the internal network.

Query of the server in the DMZ will be initiated from inside the corporate network using port 80 so no additional holes had to be made in the stateful functionality of the firewall.

Another control that will be implemented is an incident definition and response process.

AUDIT YOUR SECURITY ARCHITECTURE (25 Points)

Audit Planning

The first step in audit planning is risk analysis. I've survived as an auditor for a long time, and the only real way to do this is to select items where the consequence and likelihood of a costly lapse in control is high and it does not cost a lot of time or effort to test. In the business we call this low hanging fruit. Since we are about to have a SAS70 audit we are going to use the guidelines set out by the AICPA for a SAS70 to prevent the auditors from finding anything. A few obvious minor exceptions will be left in the control structure and hinted to the auditors so they can show they "did some work" by finding something. Since a Type I report describes the service organization's controls at a specific point in time and no test work is performed than just having all of the buzz words, the Visa ten commandments and cutting a larger than market value check to our auditors for 'other consulting services' should get us through it.

As a general rule all security at Giac Enterprises will be tested and certified by penetration analysis. Actually trying to break the security will cover all compliance issues.

The following audit program employs NMAP (get NMAP from http://www.insecure.org/nmap) to test our border router and firewall. If I was going to test host security I would use Internet Security Scanner http://www.iss.net to audit our network. You can download the software and audit a single host for free.

Implement the Assessment.

Here we go….Happy audit trails…..

Border Router Testing

Since our border router is used as a pseudo firewall it will be tested as if it was a firewall. I plan to use this audit program so I set it up so it can be pasted into my workpapers. A good audit is 2.5 pounds or more.

Step	Objective and instructions (Nmap and Windump Commands **in Bold)**	Conclusion Done = no exceptions.
	MAKE SURE YOU HAVE WRITTEN PERMISSION FROM MANAGEMENT BEFORE PERFORMING YOUR WORK.	
1.	Verify that the router is reasonably physically secured.	Done
2.	Try to Telenet to the router, if you can, and if so is it is password protected and the password is not Cisco. Telnet should not be enabled at the router.	Done
3.	Verify the Cisco passwords are set at both levels and the privileged "EXEC" mode level is encrypted.	Done
4.	Verify that the password is set on the auxiliary and console port by hooking up to them and trying to enter the router.	Done
5.	Type the command Show Run into the router console determine if the passwords for user mode and enable are encrypted. (the enable secret password is protected by default)	Done
6.	Compare the router configurations on each interface to the security policies outlined in this paper. First type sh int ? to find out what interfaces are on	Done

	the router.	
7.	If the company configuration has not been updated regularly, make sure that security patches and release level of the IOS are up to date. Go to Cisco.com to see the latest IOS.	Done
	Testing From Internet Attempting to Penetrate Border Router – Interface S0	
8.	Type *Sh int* with an interface name for each interface. For example, type sh int S0 to view the ACL s on the interface to the Internet.	Done
8.5	ACLs can be scene with the *Sh run* command (short for show running configuration). This command is run at the enable prompt. This configuration should be compared to an approved configuration with exceptions noted. If the configuration is not documented this can be an issue. Every firewall rule should be documented and it's reason understood. This documentation should include a rationale for the order of the rules.	Done
9.	When reviewing the running configuration ascertain what routing protocols are activated. Verify the RIP is disabled and unneeded protocols are disabled such as IPX.	Done
10.	Verify that the TACACS+ server is enabled for centralized password management. Review the Running configuration and verify the a line like enable use-tacacs, tacacs-server host 10.xx.xx.xx the command to activate this is tacacs-server host 10.xx.xx.xx where xx is the address of the TACACS server, the enable tacacs command and a few other configuration commands must be made first. Verify that the TACACS server has controls outlined in the Host Hardening section of this paper.	Done
11.	Since we are performing penetration analysis we are going to use the SANS 5 step process that I learned while getting the GCIH certification. The 5 steps are Recognizance, Scanning, Exploit systems, keeping access and covering tracks.	Done
12.	First we see what information we can get from the whois database http://www.arin.net/whois/arinwhois.html. Since Giac put all false information to avoid creditors, we should be safe here. Normally you can get contract names for social engineering, addresses of data centers so you can break (or just walk) in, internal telephone prefixes for war dialing, etc…	Done
13.	Start up Nmap ether for NT or Linux and open up an Internet connection. You can get it from http://www.insecure.org for Linux.	Done
14.	Set up Windump and put the sniffer on the DMZ side of the firewall. http://netgroup-serv.polito.it/windump/ We will put it on a W/95 machine. The objective of running Windump is to act as an intrusion detection system to ascertain if our Border Router ACLs are working.	Done
15.	Below is the command lines for Nmap but normally I would use the Gui. First I want to find out what ports are open at Giac Enterprises. www.Giacfortunes.com IP 167.216.133.33, the NMAP command for this is: **Nmap –v –sS -p 1-65535 -oN /nmap/logs 167.216.133.33** - v – Verbose mode. This option tells nmap to give status messages on the screen as you run the scan. -oN /nmap/logs – this command sends the results of the scan to a log file for later analysis. -sS – This is to tell nmap to do a SYN scan. If a SYN|ACK is received we know the port is listening, if a RST is received we know the port is closed. This scan will usually show up on IDS systems and router logs. -p 1-65535 – this tells nmap that I want to scan every port possible. The argument ends with the address you want to scan.	No exceptions noted.

	For this example Nmap will come back with something like this (abbreviated) Interesting ports www.giacfortunes.com(167.216.133.33): Port State Service 80/tcp open http 443/tcp open https	
16.	The above was a tcp scan, the same scan should be done for UDP. This is done using the –sU switch instead of -sS. This type of scan is very slow.	No UDP services noted.
17.	Time to pull out the GCIA skills. I configured Windump to look for any packet that was not approved Command 1: **Windump –I –F /usr/local/logger/filters/tcp.filter** Command 2: **Windump tcp[13] & 3 != 0 and not serc and dst net 10.*.*.*** -i - tells windump to listen on th first interface it finds. Since our machine only has one interface I did not have to specify one. Windump puts the interface into promiscuous mode automatically. -n – I want this to be fast so I told windump not to convert address and port numbers to names. Command 1 looks for TCP packets with protocols that are not approved in this case if they are <> 80, 443. A complete list of the filters I set up in the TCP filter file is beyond the scope of this audit program. In summary, all protocols and ports for these protocols would appear if on the DMZ. Command 2 looks for TCP packets with source addresses outside the local network. Note: looking for the UDP protocols will be accomplished by ipchains and Black Ice installed on each DMZ server. A log review will be included as part of this audit.	Done
18.	We now know what ports are open on Giacfortunes.com the next step is to see if the statefull packet inspection is working - go to the next section – auditing our Firewall. Because of our NAT on our border router we are going to do this from an address in the DMZ.	Done
19.	Comment on network design such as single points of failure or reliance on a single vendor or device type, etc…	Done
	Assuming a machine in the DMZ gets compromised the following series of tests in the firewall audit program are designed to ascertain if the statefull packet inspection is working.	

Audit of Primary Firewall

Note the firewall has the exact configuration as the border router except for the addition of statefull packet inspection.

Step	Objective and instructions (Nmap and Windump Commands **in Bold)**	Conclusion
	We now know what ports are open on Giacfortunes.com the next step is to see if the statefull packet inspection is working by auditing our Firewall.	
	Assuming a machine in the DMZ gets compromised the following series of tests is designed to ascertain if the statefull packet inspection is working.	
1.	Perform all the steps outlined in the border router audit program.	Done
2.	Start a Linux box with NMAP loaded from the DMZ and type the following	Since

	command **Nmap –sA -p 1-65535 10.10.30.10** (an address behind the firewall) What this command does is an ACK scan of the IP address of the behind the firewall. Since I turned off ICMP unreachables on this firewall this scan should turn up no responses. This will be especially critical when Nmap hits port 80 or 443. If the packet gets thought the firewall, the NT SQL server at 10.10.30.10 should not send back a reset (RST), this should not happen because the connection was not initiated from the protected network. I was going to use firewalk at http://packetstorm.securify.com/UNIX/audit/firewalk to enumerate my firewall ruleset but I just want to see if stateful packet inspection is working so Nmap will do. Besides ICMP TTL Exceeded messages would not come from my firewall because they are filtered by egress filtering.	Nmap came up with no responses it suggests that statefull packet inspection is working.
3.	To double check this assertion Windump was set up inside the corporate protected network to sniff all ACK packets coming from the machine with Nmap on my DMZ. The command looked like this: **Windump src net 10.10.10.11** (the address of the nmap machine in the DMZ)	No ack messages were detected from this address.

Analysis of Firewall, Server, IDS and Router Logs

Logfiles are to be removed from the logging servers daily. Logfiles should be analyzed by the security administrators to ensure no intrusions and have occurred and router ACL's are working to assess whether changes to the firewall/router filter policies are required. The logfiles can be quickly analyzed by using the Grep like tool at http://www.funduc.com/index.html the tool to eliminates unnecessary lines in log files and makes them easy to search and report on. This log analysis should occur weekly and a comprehensive incident response process set up for responding to incidents.

Conduct a Perimeter Analysis

Below are the weaknesses found with the internal network.

- The biggest weakness of the design in this paper is the dependence on one type of device (a Cisco 2620, IOS 12.0(3)T) is to act as a border router and firewall. If an exploit such as a buffer overflow was found than the entire network would be vulnerable. If Giac had the money they should replace the firewall protecting the internal network with an application proxy firewall from a different vendor.

- A additional Cisco 2620 border router should be set up at the border router with load balancing to prevent bottlenecks and provide additional redundancy.

- If the primary route to the internet became a victim of a distributed denial of service attack, Giac Enterprises could not function. For this reason a secondary path to the internet is recommended. This secondary path will also provide additional bandwidth.

Looking in bugtrack for a vulnerability related to this router and IOS version I only found one ID1161. It is called “Cisco Router Online Help Vulnerability”. This vulnerability allows an attacker to view the configuration of a Cisco Router. Cisco suggests that a security-conscious administrator should perform the following actions:

- Set the default privilege level for access lines to 0 (rather than leave at 1, the default)

- Using "privilege exec", specify which commands a user at level 0 can use.

DESIGN UNDER FIRE (25 Points)

As assigned I decided to attack the design at http://www.sans.org/y2k/practical/Eric_Rupprecht_GCFW.doc for the following three attacks:

- **Attack Against the Firewall Itself**
- **A Denial of Service Attack**
- **An attack plan to compromise an internal system through the perimeter system.**

Attack Against the Firewall Itself

The firewall used in the Rupprecht paper was Gauntlet 5.5 Application Proxy firewall. An application proxy firewall actually examines, to an extent, the payload of the packets to restrict the functionality of certain applications. It does provide a greater degree of security than a statefull or packet filtering firewall but also results in increased processing loads. According to www.securityfocus.com only one known vulnerability exists for Gauntlet firewall version 5.5. The vulnerability is called “Gauntlet Firewall Remote Buffer Overflow Vulnerability” (CVE-2000-0437, Bugtraq ID 1234 www.securityfocus.com/vdb/bottom.html?vid=1234). Since I can’t get to the underground because my company filters these sites as “criminal” the only resource I had was “known” exploits. The attack is a buffer overflow attack (see http://www.sans.org/infosecFAQ/threats/buffer_overflow.htm – Written by Nicole LaRock Decker, Published by Sans in 2000 for a great tutorial on buffer overflows.) This buffer overflow is not against the Gauntlet firewall itself, but like in many cases, the attack is against a program or utility that comes with the firewall. The utility program is called Cyber Patrol, it is installed by default with a 30 day license. So after 30 days of installation the system is not vulnerable to this attack. The code to carry out this attack is also posted at security focus. The results of the attack are very bad, as is the nature of buffer overflow attacks, once a buffer overflow is found and successful exploit is achieved, the exploit can then be used multiple times and even be used to establish administrative (or Root) command authority on the server that runs the Firewall. To fix this apply the patch from Network Associates.

A Denial of Service Attack

A common denial of Service attack is the SYN flood attack. For the sake of this paper, our perpetrators have hijacked 50 compromised Cable modems. The machines attached to the cable modems were victims of the Tribe Flood Network 2000 (TFN2K) Trojan available at http://packetstorm.securify.com/distributed/ . In this attack the attacker initiates a TCP connection (with a SYN packet) with a TCP based service on the targets network. The Giac machines would then respond with a SYN-ACK. Since the attackers address cannot be reached and a the final ACK of the three way handshake cannot be received. The connection remains in a half-open state until it times out. To achieve a denial of service the attacker floods the server with SYN

packets faster than the connection times out on the Giac machines. Eventually, the attacker exhausts the resources of the Giac server and no one else could connect to the server

Thresholds on Cisco machines could be set to avoid SYN flood attacks. These thresholds were described earlier in the paper.

An attack plan to compromise an internal system through the perimeter system.

The weaknesses this attack exploits is that routers do not reassemble packets before passing them on and the host based Intrusion Detection System (IDS) is not specifically configured to prevent fragmentation attacks.

To get past the border router filters, I would do a fragmentation attack with Fragrouter. (I borrowed some of this stuff from the SANS GCIH training materials, not copied just paraphrased.) Fragmentation attacks exploit the weakness in a firewall and other packet filters that they do not have the complete picture of how a packet will be treated and reassembled at the end system. To get through the non statefull firewall I would implement a fragment overlap attack. In this attack a tool called fragrouter creates two fragments for each IP packet. One fragment has the TCP header, including the port number for a service allowed by the filter (TCP port 80 will be used since we know that the network has a web server). The second fragment has an offset value that is a forged. The offset is smaller than reality, so that when the fragments are reassembled, the second fragment overwrites part of the first, particularly the part of the first fragment including the port number. The two fragments arrive at the targeted protected server and they are reassembled. The reassemble overwrites the port number of fragment 1 with the port info from fragment 2, and the TCP/IP stack passes the packet to the application listening on the protected port. See http://www.anzen.com/research/nidsbench for more. The instructions for fragrouter to carry out this attack would be:

Step: 1 Perform a syn scan of the network address for all port numbers.

Nmap –v –sS eric_rupprecht.com

Step: 2 -. The OS fingerprinting function of Nmap will also be used. The command to do this is:

Nmap –v –o eric_rupprecht.com

Step 3 – Once I have enumerated the web server or mail server Operating System (OS) I would visit www.securityfocus.com and try the latest exploits for that server OS.

Step 4 – Once I gained root on one of the service network servers, I would install a NetCat on the machine to move packets into the internal network to gain root on more hosts without altering the IDS. http://www.l0pht.com/users/10pht/nc110.tgz

Appendix A: Support for $200 million a year in on line sales.

Our 5 months of operation we generated $500 thousand in on line sales. Based on this growth pattern of 100 % per month we will earn 200 million a year.

Our sales are based on shipments we made to random names in the New York phone book, charging $500 per fortune cookie saying.

We get 500,000 original hits per hour to our web site, and this has been confirmed by double click. Advertising revenues for displaying banners at our web site are actually the only cash flow we have. The majority of the hits are generated from the following redirection and other features of the internet:

- Url redirection by cross site scripting see the paper I wrote on this topic at http://www.sans.org/y2k/practical/Robert_Grill_GCIH.doc
- Bogus links placed around the internet that say "Free Live Porn"
- DNS Cache Poisoning
- Denial of Service attacks on competitors

Since we are going public next month and expect to raise 2 billion dollars to finance future growth and stick in our pockets, a big 5 public accounting firm is here performing an audit of our financial records. To verify our sales, a 22 year old good looking woman who knows everything compares our fed x receipts to sales invoices to verify that we are recording our sales in the right period. She selected a sample of these shipments by a formula that I did not understand and made a copy of everything for her workpapers (a good audit is 2.5 pounds). She then sent out confirmation letters to a sample of our customers to verify our accounts receivable amounts. None have answered, which she stated was normal, she called the customers to verify the accounts receivable amounts. By coincidence all our vendors of the same phone number. She called two of the largest sales accounts receivable account holders and noted in her workpapers that the rest was TSTI (Too Small to Investigate), for which she had a rubber stamp so she would not have to write this notation repeatedly. I never met her boss but I hear his name is Fagan.

Our business partners required a SAS 70 review because it was required by their auditors. This review is required because we act as a servicer for our fortune cookie writers. To preserve cash we don't pay for fortune cookie sayings until we sell them. Since some of the publishing firms that supply our sayings have already gone public, their auditors required as SAS70 from us to prevent their auditors from coming out and auditing us and it will also be used to support an unqualified opinion on our financial statements. See http://www.sas70.com for the double talk, smoke and mirrors.

Our recent purchase of a rival pyramid scheme was financed by using an inflated valuation of the target companies assets as the collateral for a leveraged buyout.

References

I try not to ever use verbatim quotes, except for things like the Visa Ten Commandments, where I have no choice. Since Visa wrote these commandments I put the reference in the context of the body of the paper. No specific pages are sited since there are no verbatim quotes. I simply checked my work through a variety of sources.

1. Books

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

Cole, Eric and Skoudis, Ed. GCIH Course Materials, The SANS Institute.

Kurtz, George; McClure, Stuart; Scambray, Joel. Hacking Exposed, Osbourne, 1999

Held, Gil and Hundley, Kent. Cisco Security Architectures, McGraw-Hill 1999

2. Presentation

2.1 Mallet, Pamela (Director, E-Commerce Risk Issues, Visa U.S.A). "Understanding Technology Risks." California Bankers Association - Internet Security Workshop February 27, 2001

3. Web Sites

Web sites were listed in this paper in context for the reader's convenience. When I knew the information I followed the SANS guidelines. When the information is missing it is because I could not determine the author or other information by looking at the web site. If the link points directly to the page, I did not include the page number.

1. Information Systems Audit and Control Foundation. "Control Objectives for Information Technology (COBIT)." COBIT Framework. Version 3.0, July 2000. http://www.isaca.org/cobit.htm (February 17, 2001). Page 52.

2. Cisco Systems. "IOS 12.0 Configuration Guide and Command Reference." November 2000. http://www.Cisco.com (February 26, 2001). See the various links throughout the document for page numbers.