Global Information Assurance Certification Paper

GIAC Enterprises: Fortunes Hot Off the Press

GIAC Certified Firewall Analyst Practical (GCFW)

Practical Assignment v.3.0

Global Information Assurance Certification (GIAC) Program

Bryan Feltin

Version 1.1.01
May 5, 2004

TABLE OF CONTENTS

ABSTRACT

As part of the Global Information Assurance Certification (GIAC) program, this paper is the practical assignment required to obtain the GIAC Certified Firewall Analyst (GCFW) certification. The assignment is intended to demonstrate a high level of understanding of the information provided within the GIAC Track 2 program: *Firewalls, Perimeter Protection, and Virtual Private Networks (VPNs)*. This assignment will apply obtained knowledge regarding firewalls by designing a secure perimeter defense architecture for a fictional company called GIAC Enterprises.

ASSUMPTIONS

- The following assignment is based on a fictional company called GIAC Enterprises. Any references made to this company are not to be taken seriously outside the GIAC Certification circle.
- In order for GIAC Enterprises to have a web presence a domain must be registered. The following document assumes the domain giacenterprises.com is registered to GIAC Enterprises with the primary and secondary DNS servers configured properly.
- The public IP addresses used were fabricated and are not meant to reference any actual registered IP subnet.
- It is also assumed that the appropriate DNS entries for www.giacenterprises.com and the mail exchanger recorder smtp1.giacenterprises.com have propagated properly.
- A code of conduct policy and a nondisclosure agreement are assumed to be in place between GIAC Enterprises and customers, partners, suppliers and employees.

ASSIGNMENT 1

SECURITY ARCHITECTURE

Business Operations

GIAC Enterprises is a well-experienced, successful company that deals with the online sale of fortune cookie sayings. The company delivers great returns to its investors, suppliers and partners in three countries. Even though the company of roughly 1000 employees is relatively small for the fortune cookie industry, GIAC Enterprises business goal for 2005 is to double its net profit. In order for the company to achieve its extremely aggressive goal, GIAC Enterprises has reviewed and revamped its business processes, which now includes targeting

the large wholesale customers, suppliers and partners. The company has also invested a large amount of money into architecting the entire perimeter security for its new on-line presence.

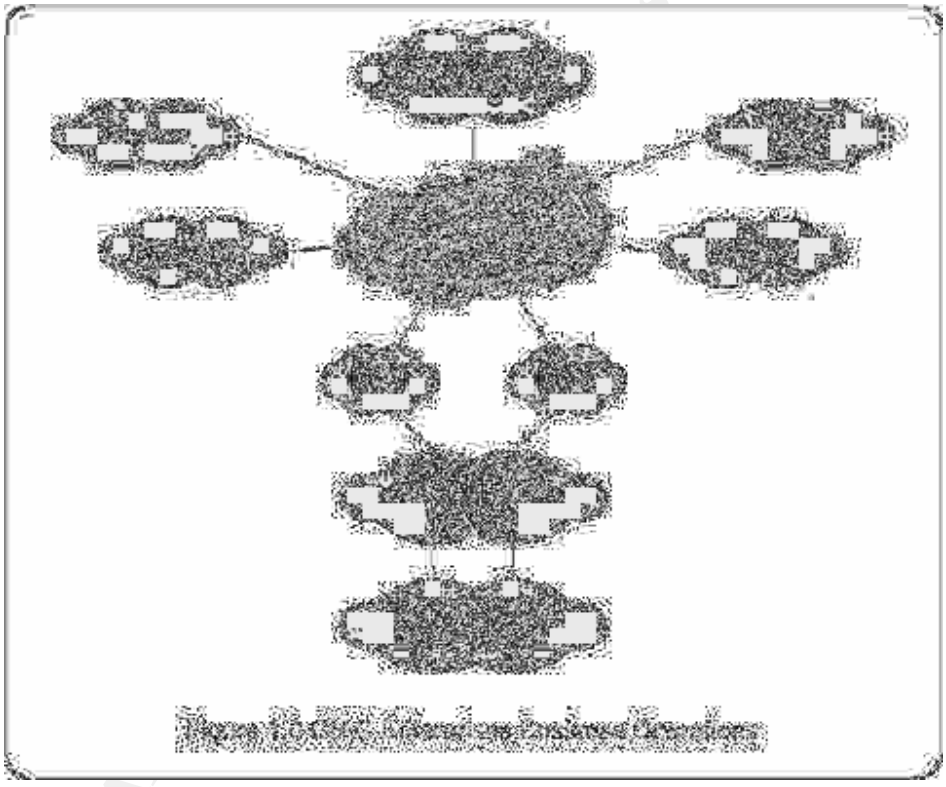
For GIAC Enterprises to be able to expand its employee base and overall revenue, a popular and well-received on-line presence is required. This is expected to happen by increasing the company's customer base, as well as by increasing the number of suppliers that it deals with. Since the demand for fortune cookie sayings has sky rocketed, suppliers have been very particular with who and how they do business. Suppliers now require customers to have a strong security focus and a transaction interface that is easy to use.

The Internet is becoming a highly infectious medium for operating a business. Viruses, worm, Trojans, and other malicious software make it possible for one company's lax security policies to have detrimental affects on another company's business. Company reputation is vital to the future success of GIAC Enterprises.

Access Requirements

Overview

The business process analysis of how GIAC Enterprises conducts its business was performed two years ago and several changes were made. These changes focused on improving old processes and developing new ones to better position GIAC Enterprises for conducting its new on-line business. One change made was to organize the company's business transactions into one of six categories: customers, suppliers, partners, internal employees, remote employees, and the general public. The high-level relationship between the different categories is displayed in Figure 1.0. Once the reorganization task was complete, a high level overview of how each group conducts business was developed.



Customers

Overview

Customers are individuals or companies that purchases bulk on-line fortunes. The company's new business model is to target large customers, wholesalers and repeat customers. The company plans to move away from smaller clients. This decision was made to functionally reorganize the company as a productive e-business and to avoid the "one-time" customers.

Business Process

A company interested in becoming a customer accessed the required information, such as a salesperson's contact information, from the public GIAC Enterprises' website by using any current web browser. The public website is accessible by using the HTTP protocol on TCP port 80. If the application requirements are met, the customer is given a specific username and password, along with the address to the secure private web server that is not accessible by the general public.

The private or e-business website is accessible with the HTTPS protocol on TCP port 443. Since the secure web server is using a 128bit certificate, the web browsers must also support 128bit encryption. The 128bit encryption prevents sensitive data from falling into the wrong hands. 128bit encryption also meets the fortune cookie industry standards required to conduct business. The private website is configured with virtual sites to provide a different web interface for customers, suppliers, partners and GIAC Enterprises employees.

Suppliers

Overview

Suppliers are companies that provide GIAC Enterprises with fortune cookie sayings. In the new business model, it is a common occurrence to deal with suppliers of other nationalities and to purchase fortune cookie sayings in other languages. This is one of the key requirements that needed to be established in order to double GIAC Enterprises' revenue in 2005.

Business Process

Suppliers interact with GIAC Enterprises very frequently. Similar to customers, suppliers are provided their own specific username and password to a separate virtual website for suppliers. Here they are able to upload their data to GIAC Enterprises. Once the data is uploaded, GIAC employees can manipulate the data and resell the fortune cookie sayings.

The same access requirements exist for suppliers as they do for customers. The suppliers virtual website is accessible with the HTTPS protocol on TCP port 443 using a 128bit certificate. This also requires suppliers to use 128bit compliant web browsers in order to perform on-line transactions.

Partners

Overview

Partners are international companies that translate and resell fortune cookie saying. They buy English fortune cookie sayings from GIAC Enterprises, translate them to their local language and resell them. GIAC Enterprises also uses partners to translate fortune cookie saying that were supplied by international suppliers.

Business Process

Similar to customers and suppliers, partners are provided their own secure virtual website along with their own user ID and password. Their website interface, however, is slightly more complicated. Partners, unlike customers and suppliers, have the ability to download fortune cookie sayings that need translating as well as the ability to upload translations that have already been translated.

The same requirements exist for partners as they do for suppliers. The partners virtual website is accessible with the HTTPS protocol on TCP port 443 using a 128bit certificate. This also requires suppliers to use 128bit compliant web browsers in order to perform on-line transactions.

GIAC Enterprises Internal Employees

Overview

GIAC Enterprises employs people for various functions within the company. The sales division is often away from the office trying to generate new business by signing and renewing contracts with customers, suppliers and partners. The development department focuses on creating new fortune cookie sayings. The publishing department, updates the website when new fortune cookie saying are available. The information technology department is responsible for the entire network infrastructure. As any other business, the usual departments, such as human resources, finance, etc., are all present

Business Process

The only department that requires access to the secure web server is the publishing department. When new fortune cookie sayings are created by the development department or when data is uploaded from suppliers and partners, it is the responsibility of the publishing department to reflect the changes on the website.

GIAC Enterprises' employees are also provided Internet access to perform research for new fortune cookie sayings. To segregate the e-business traffic from internal employee traffic, GIAC Enterprises decided to install two connections to the Internet. One, from ISP1, handles all e-business web traffic from customers, suppliers, partners and the general public. The second Internet connection, from ISP2, handles all regular day-to-day Internet traffic. Day to day employee Internet traffic includes outgoing web browsing, inbound and outbound email, externally hosted DNS traffic and incoming VPN traffic from remote GIAC employees.

GIAC Enterprises employee Internet policy is to deny all inbound and outbound traffic except for what is explicitly permitted. Currently, only the following reports are required for outbound Internet access:

HTTP – TCP port 80 (Hypertext Transfer Protocol)
HTTPS – TCP port 443 (Hypertext Transport Protocol (Secure)
FTP - TCP port 21 (File Transport Protocol)
FTP Data – TCP port 20 (File Transport Protocol)

On the Internal GIAC Enterprises network, the following protocols are also required:

SMTP – TCP 25 (Simple Mail Transfer Protocol)
DNS – UDP 53 (Domain Name Server)
DNS – TCP 53 (Domain Name Server)
SSH – TCP 22 (secure shell)
Microsoft Windows Domain:

- TCP 139 (File Sharing, Logon Sequence, Printing)
- UDP 137, 138 (Browsing, Logon Sequence, Printing)
- TCP 445 (SMB without NetBIOS)

GIAC Enterprises Remote Employees

Overview

GIAC Enterprises also provides its employees remote access to internal network resources to allow employees to work at home or away from the office. This was originally designed for the mobile sales force, but it has been expanded to all employees if required.

Business Process

In order to be able to use VPN, the IT department has installed the VPN client on the employee's laptop. The personal firewall program called Zone Alarm is also installed. Zone Alarm must be running in order to connect via VPN and this policy can be enforced by the VPN endpoint. The user is supplied an RSA secure ID token in order to authenticate against the RSA server.

The following ports are required to establish the VPN connection:

ISAKMP - UDP port 500
IPSec NAT - UDP port 10000

Once an employee is connected via VPN, the same protocols used for internal employees apply:

SMTP – TCP 25 (Simple Mail Transfer Protocol)
DNS – UDP 53 (Domain Name Server)
DNS – TCP 53 (Domain Name Server)
SSH – TCP 22 (secure shell)
Microsoft Required

- TCP 139 (File Sharing, Logon Sequence, Printing)
- UDP 137, 138 (Browsing, Logon Sequence, Printing)
- TCP 445 (SMB without NetBIOS)

Security Architecture Analysis

The choice to host a secure website for customers is based on the easy to use requirement for the fortune cookie industry. All that is needed to conduct business is access to the Internet and a 128bit web browser. There is no client software to install, administer, support, or upgrade. This allows GIAC Enterprises to be able to make sure that its architecture and components are secure, without having to worry about the security processes of companies it does business with. Most companies allow their employees port 80 and 443 access to the Internet. By using the standard ports, customers, suppliers, or partners do not need to modify their firewall rule set to access the GIAC Enterprises' website.

The design of having two Internet connections is primarily to prevent a problem with one link having an adverse affect on the other. In the event that GIAC Enterprises is hacked or infected with a new worm, the safeguard is in place so the primary business function is not affected. Two ISPs is a great blueprint for a failover solution. GIAC Enterprises will be looking failover and redundancy in the near future.

Security Architecture Design

Overview

GIAC Enterprises has taken a scaled back approach to implementing its new on-line presence. Due to budgetary constraints, certain key components do not have the failover ability as recommended by the business process review committee. The architecture does provide expansion and scalability. Pending the 2005 Q4 results and budgetary approval, the ability to implement a complete failover plan is possible. Since GIAC Enterprises already has a well-developed core network infrastructure, the next section of this document focused on detailing the perimeter security architecture.

IP Addressing Scheme

In order to understand how GIAC Enterprises' network is configured, it is important to understand the various networks that exist within the corporation. As Table 1.0 shows, there are three general networks - the Internet, the perimeter security network and the internal network. Within each of these general networks resides smaller subnets divided by function.

Table 1.0 GIAC Enterprises IP Subnetting Scheme

Network	Subnet Name	Subnet
Internet		
	ISP1	201.201.201.0/24
	ISP2	202.202.202.0/24
Perimeter Security Network		
	Proxy DMZ	192.168.101.0/24
	VPN DMZ	192.168.102.0/24
	Web Server DMZ	192.168.103/24
	Firewall Subnet 1	10.10.100.0/24
	Firewall Subnet 2	10.10.200.0/24
Internal Network		
	Servers VLAN 100	172.20.100.0/24
	IDS VLAN 150	172.20.150.0/24
	Research and development VLAN 200	172.20.200.0/24
	Information Technology VLAN 210	172.20.210.0/24
	Marketing/Sales Department VLAN 220	172.20.220.0/24
	Other departments VLAN 230	172.20.230.0/24
	Remote VPN Users	172.20.240.0/24

Multiple subnets make a hacker's reconnaissance more difficult, as possible hackers need to know what the IP address scheme is on each side of a router, a firewall, a DMZ or an Internal network. It is very important to not leak any non-public IP addresses. Figure 2.0 shows how

the subnets listed in Table 1.0 are logically configured on the GIAC Enterprises' network.

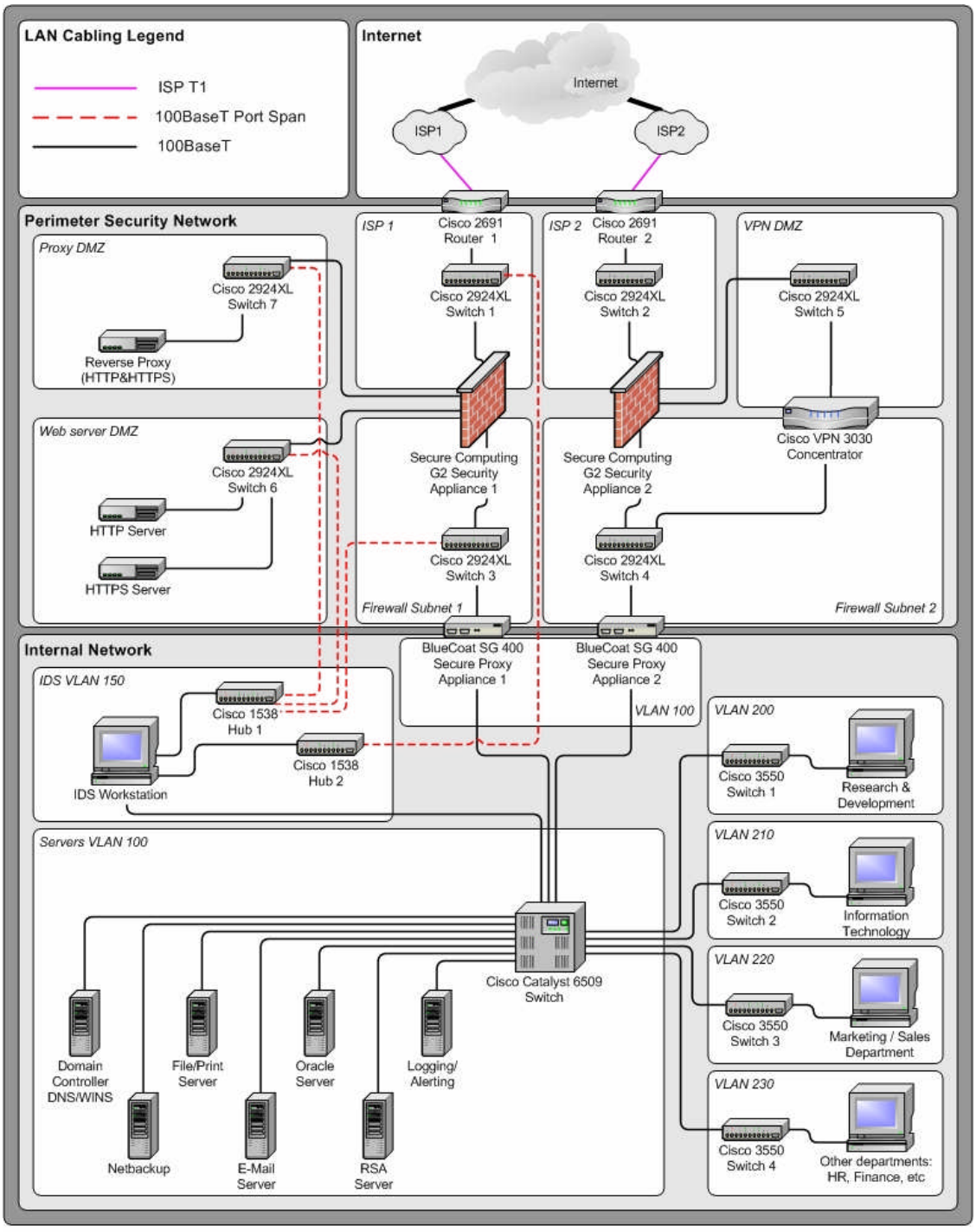


Figure 2.0 GIAC Enterprises Security Architecture

Internet Service Providers

Previously mentioned and as Figure 2.0 shows, GIAC Enterprises decided to incorporate two Internet connections into its network, each from a different ISP. The decision was made to keep e-business traffic (transactions from customers, partners and suppliers) separate from general employee Internet traffic (e-mail, web browsing, etc.). Since spam, worms, Trojans, or user negligence can have a negative impact on a company's Internet connection, it can be a good idea to keep the traffic segregated. As well, having the two Internet connections greatly positions GIAC Enterprises to add failover, fault tolerance or load balancing to its Internet presence.

The ISP1 connection is used to host GIAC Enterprises' websites. The ISP1 link is also be the secondary entry point for email and DNS traffic in the event that ISP2 is unavailable. The ISP2 link is used for incoming and outgoing SMTP traffic, general web browsing, hosting a primary DNS server, as well as incoming VPN traffic from remote GIAC Enterprises VPN users.

Border Routers

The first line of defense that GIAC Enterprises incorporated is the placement of routers between each ISP and the firewalls. Even though a router's primary purpose is it simply route traffic, it still has a significant contribution to perimeter security. The routers are used to perform packet filtering and are configured to block unwanted traffic. The routers block all private addresses, spoofed packets, packets that have a source destination of the Internal network and much more non-legitimate traffic. Routers also maintain logs, which may come in handy in the event of a security breach.

The ideal location for traffic blocking routers is outside the firewalls. This prevents unnecessary traffic from getting to the firewall freeing up processing time. A downside of performing packet filtering with a router is that "state" may not be kept. This however, is not a serious concern as Cisco routers have become more robust and are starting to contain "stateful" features. Having a stateful firewall as a second layer of defense greatly increases the overall security.

Since GIAC Enterprises already has a well-established relationship with Cisco, the border routers are Cisco 2691 Multiservice Routers. This model delivers extended performance, higher density, enhanced security performance and increased concurrent application support. The routers are able to meet the growth demands of GIAC Enterprises, which may include the addition of branch offices. The 2691 routers are running the Cisco IOS version 12.3, which is the latest release that incorporates a

number of features important to GIAC Enterprises. One feature, the ability to perform stateful inspection of ICMP traffic, prevents attackers from using "ping" to gain knowledge of network resources or to map out the perimeter security architecture. IOS version 12.3 includes Cisco's IOS IDS signature enhancements that detect 101 of the most common intrusion attack signatures. The ability is there to enable or disable any one of the signatures the company believes to be the most dangerous.

Stateful Inspection Firewalls

The most important security component of GIAC Enterprises perimeter security is the firewalls. The firewalls are the first real aggressive layer of security that protects the resources of the private network from unauthorized access and potentially harmful users. The firewalls also protect the web servers located in the Web Server DMZ by controlling the kind of traffic able to access the servers.

There are several key networks in the overall architecture design: three DMZs, two ISPs, and two firewall subnets. Each network is protected by the firewalls. The firewalls contain a separate network interface for each network connected. This is important because if a host in the DMZ is compromised, the hacker must still try to circumvent the firewall again to access the other networks.

Firewalls, important as they are, should not be a company's sole means of defense because they do have flaws. Even though firewalls are improving every day, the majorities of them are still simply port and IP based and are poor at controlling content. This has become a concern for GIAC Enterprises because almost any Internet application can be configured to traverse the Internet over port 80, which is required for normal web browsing. A major concern is when internal employees run applications such as Kazaa or Bit Torrent and download programs that are infected with backdoors, viruses, Trojans or whatever malicious program is floating around on the Internet. Also, firewalls do not protect against social engineering attacks. If an internal employee divulges certain information regarding a firewall's configuration, the firewall may be able to be exploited either internal or externally. GIAC Enterprises requires the ability to allow people that are members of the domain group Internet-Sales access to port 80 and 443 yet only give the group Internet-Marketing access to the Internet on port 80. Firewalls have historically lacked to provide this functionality. Although this is starting to change, the ability to permit or deny outbound traffic based on Windows domain account privileges is very important to the company.

The flaws and lack of features of firewalls can be fixed by leveraging the "defense in depth" concept. The introduction of an additional layer of security based on a proxy technology placed behind the stateful inspection firewall provides the flexibility to control access and contain any intrusions that do occur. GIAC Enterprises has implemented a secure proxy to mitigate these risks and add the domain group policy features.

GIAC Enterprises purchased two Sidewinder G2 Security Appliances from Secure Computing. The appliances are running the latest version of software, which is currently 6.1 shipped with the appliance. SideWinder G2 is the latest firewall product from Secure Computing (a hybrid of the purchased Gauntlet firewall and their own SideWinder firewall).

The SideWinder G2 appliances were chosen because of their advanced feature set. It is based on the BSD operating system and provides tremendous flexibility, performance and security. Secure Computing still claims that it is the world's strongest firewall that has never been compromised. It also has the ability to host Secure Mail, Web, and DNS gateway services and also has embedded anti-spam and anti-virus engines. The G2 appliance also contains an integrated IDS system with real-time alerts. One of the most useful and important features is the built-in file integrity checking. If a firewall does get compromised, it is easy to determine which files were modified. Many network analysts do not agree with hosting key services such as e-mail and DNS on the firewall itself but this is not a concern with the Sidewinder G2. The SMTP relay is based on "sendmail" and there are actually two different Sendmail servers that must be exploited to reach the internal network. With two ISP connections to the Internet, there is fault tolerance with the email and DNS. For GIAC Enterprises, the ability to do virus scanning and anti-spam tasks at the firewall layer of defense is huge! Internal email resources can remain focused on processing legitimate email.

Secure Proxy Appliances

GIAC Enterprises is using two BlueCoat SG 400 secure proxy appliances, one on each ISP connection. On the ISP2 link, used for outbound web traffic, the appliance provides the ability to have multiple users on the Internal network access the Internet by using a single IP address. The BlueCoat appliance also logs all employee transactions. Monthly Internet reports, provided to management, are generated from the log files.

The Bluecoat appliance has many security features that are implemented by GIAC Enterprises:

1. Supports the "deny all traffic except what is explicitly allowed" policy on a per-user or group basis.
2. Performs as a web proxy-caching server to cache and server commonly requested sites to increase page load time for users.
3. Implements content filtering to block employees from improper Internet sites and potentially infecting the network with malicious software resulting in network downtime.
4. Carries out web virus scanning on active connections to the Internet as well web-based email such as yahoo and hotmail. The Bluecoat appliance also performs virus scanning on web based email attachments.
5. Operates as an application firewall. Only Internet Explorer is able to connect to the Internet over port 80. This prevents other Internet applications such as peer-to-peer applications from using port 80 to connect to the Internet.

The proxy appliance on the ISP1 link creates symmetry, which is required for a future failover implementation. It also creates another network that must be breached if the firewall or server in the DMZ is compromised.

Since proxy appliances accept requests from internal users, one interface of the appliance is connected to the Internal network and the other interface is connected to the same subnet as the internal interface of the firewalls creating the firewall subnets.

Proxy servers and appliances do have a downfall. In order for inbound connections to be allowed, the ports on the external interface of the proxy must be opened which means the ports are always listening. These open ports make the proxy vulnerable to attack; however with a stateful inspection firewall with no listening ports placed a level in front of the proxy appliance, a secure architecture is created.

Virtual Private Networks

GIAC Enterprises required a secure method for remote working employees (people working from home or the mobile sales force) to connect to the internal network and access local resources. A VPN solution was proposed and implemented. VPNs use encryption to provide secure communication over a non-trusted medium such as the Internet.

GIAC Enterprises, decided to use a Cisco VPN 3030 Concentrator as its secure VPN gateway appliance. The VPN Concentrator uses a different IOS scheme than routers and switches. The latest version provided by Cisco is IOS 4.1.2 for the VPN 3030 Concentrator. The design shows that the concentrator is located in its own DMZ, behind the primary firewall. Having the concentrator behind the firewall adds another level of security by only allowing the required ports to connect to the concentrator. This should avoid, many common attacks and network reconnaissance of the DMZ. If the concentrator does get compromised, the hacker must be able to traverse the second layer of defense, the BlueCoat proxy appliance, in order to connect to internal, confidential information.

The Cisco concentrator requires the Cisco VPN client software to be installed on any client computer trying to connect. The latest version of the client is 4.0.4 for the VPN 3030 Concentrator. This is the version used by GIAC Enterprises. One potential problem may be the maintenance of the client software on remote machines. If new versions of software become available that fix vulnerabilities, it must be applied to VPN user's laptops. The later releases of the Cisco VPN Concentrator IOS have a feature that provides the ability to notify clients when their version is outdated and to provide them with the new software to install. The VPN concentrator also requires a group name and password to authenticate and, based on which group is authenticated, can change what access permissions the user has. The problem with this is that normally it is the responsibility of the users to remember the group name and password, which is sometime difficult for many users. GIAC Enterprises has decided to create obscure group names and long passwords (32 characters) and hard code the information in the group profile file. This concern is mitigated by the use of an RSA authentication server. Each user is provided a secure ID token, which has a rotating PIN, that changes ever 60 seconds synchronized with the RSA server. Another concern with VPN traffic is that once a tunnel is established, usually any traffic is allowed to traverse the two networks, even worms or malicious software. To mitigate this risk, GIAC Enterprises forces all VPN users to run Zone Alarm, a personal firewall application, on their laptops. The VPN concentrator is configured to create a successful connection only if it detects that Zone Alarm is running.

Web Environment

The web environment consists of three servers. One, a web server, running strictly as an information website accessible on port 80. Another, the e-business web server, is for performing transactions between customers, partners and suppliers. The third web server is a reverse proxy server placed in a separate DMZ (for both the HTTP and HTTPS web servers).

All three servers run Red Hat Enterprise Linux version 3 as well as the latest release of the Apache HTTP Server. According to http://httpd.apache.org/download.cgi the latest version is 2.0.49. The reverse proxy server runs the Squid reverse proxy server. According to http://www.squid-cache.org/ the latest stable release is version 2.5. Squid is a key portion of the entire web environment (it proxies the clients from the servers and prevents them from communicating directly). This helps protect the servers from HTTP based attacks. One thing to note is since HTTPS traffic in encrypted, Squid is not able to perform access control checking against the traffic. However, squid can still forward unchecked requests to the HTTPS server. This has been accepted by GIAC Enterprises.

One issue that concerns GIAC Enterprises is that there is only one reverse proxy server for both web servers. The company eventually agreed that with proper backups, should the server fail, it is easy to rebuild the Linux server and restore the configuration. GIAC Enterprises will look into redundancy and failover in the future with the other components.

Intrusion Detection

Previously discussed in the security architecture were filtering routers, firewalls, VPN and proxy servers. All these devices perform similar functions. They control how traffic is to be handled, denied or passed, based on an established set of rules. An intrusion detection system is another layer of defense that can be used to alert support staff when abnormal traffic does occur even though it may still adhere to the rules of the previous devices. Intrusion detect systems are able to detect known attack patterns called signatures and send alerts based on a defined set up rules.

Since IDS is new to GIAC Enterprises, the company decided to take a low cost approach for the time being to determine if IDS will really benefit the company. GIAC Enterprises focused on traffic coming in through the ISP1 Internet connection, as it is the E-business link. GIAC Enterprises decided to implement a Linux Red Hat workstation with three network cards running the IDS software SNORT. One interface, connected to the Internal network, provides the ability to send alerts. The other two

interfaces are each connected to a Cisco 1538 series Micro Hub 10/100. As Figure 2.0 shows, the Cisco 1538 Hub 1 is used to monitor traffic behind the firewall and the Cisco 1538 Hub 2 is used to monitor external traffic. This combination allows GIAC Enterprises to deduce what traffic is passing through its firewall. If malicious traffic is detected on the outside of the firewall but not on the inside, then the traffic can be explicitly blocked or simply ignored. If for some reason the traffic is detected on both the outside and the inside, the IDS system should send an alert. The connection from the Cisco 2924XL switches to the hubs is a standard port span, which allows the Snort workstation to monitor all traffic to the various subnets.

There are several problems with IDS systems. The first is the sheer number of alerts that the system detects. It takes a lot of time and administration to tweak the system. Often, IDS systems alert on false positives or network activity that the sensor thinks is abnormal but which may be legitimate. A solid administration process should address these issues.

Security Architecture Review

GIAC Enterprises has taken a fairly aggressive approach to developing an e-business architecture that provides perimeter security as well as an easy to use business interface. It is evident that security is taken seriously as demonstrated by the various layers of protection provided by the defense in depth concept. Failover and hardware redundancy is still missing, but will be addressed at a later date. Most of the devices mentioned have failover capabilities, such as the G2 security appliances and the BlueCoat secure proxy appliances, but more hardware needs to be purchased which is not in the budget for this project.

ASSIGNMENT 2

SECURITY POLICY AND COMPONENT CONFIGURATION

Overview

The intended purpose of this section is to define the security policies as well as the detailed component configuration of the Cisco 2691 border routers, the Secure Computing G2 Security Appliances, the BlueCoat Secure Proxy Appliances and the Cisco 3030 VPN Concentrator. The template used for the following policies is based on the DMZ Lab Security Policy (*SANS Security Policy Project, p.1*).

Border Router Security Policy

1.0 Purpose

The purpose of this policy is to define standards that all networking devices located on the public Internet and owned by GIAC Enterprises must meet. These standards are defined to reduce the public exposure of the Internet and to protect GIAC Enterprises private information from malicious traffic.

2.0 Scope

Devices that are connected to the Internet and are located outside the firewall subnets are considered part of the "hostile zone" (Internet). Devices located on the Internet are highly vulnerable to attack and therefore must abide by this policy. This policy details the hardening requirements to secure the two Cisco 2691 border routers shown in Figure 2.0.

3.0 Border Router Security Requirements and Configuration

The following security requirements are based on Cisco Security Device Manager (*Cisco Security Device Manager, p.1*) and the recommendations that it has provided. The Security Audit feature examines a routers configuration and then updates the configuration in order to make the router more secure.

3.01 Disable Finger Service
The Finger protocol is used to gather information about users on a remote system. Finger servers can usually provide either a list of logged-in users or detailed information on a single user. It is required that this reconnaissance method be blocked

The Finger service can be used as a Denial-of-Service (DoS) attack called "Finger of death." It is required that this DoS attack be prevented.

In order to disable the Finger service on a Cisco router enter the following command from configure terminal mode:

no service finger

3.02 Disable PAD Service
The packet assembler/disassembler service is used to connect simple devices (like character-mode terminals) that do not support the full functionality of a particular protocol to a network. Since this service is not used, it needs to be disabled.

In order to disable the PAD service on a Cisco router enter the following command from configure terminal mode:

no service pad

3.03 Disable TCP/UDP Small Servers Service
The small services refer to simple services such as echo, chargen and discard. These services are infrequently used but can be used to launch DoS and other attacks. It is required that both the TCP and UDP versions of these services be disabled.

In order to disable the small servers service on a Cisco router enter the following command from configure terminal mode:

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

3.04 Disable IP BOOTP Server Service
The BOOTP server service permits computers and other routers to automatically configure necessary Internet information from a centrally administered server upon startup, including downloading Cisco IOS software. This means that an attacker could download a copy of a router's Cisco IOS software using the BOOTP service. The BOOTP service is also vulnerable to DoS attacks and therefore it is required to be disabled.

In order to disable the BOOTP server service on a Cisco router enter the following command from configure terminal mode:

no ip bootp server

3.05 Disable IP Identification Service
The Identification service allows a user to query a TCP for identification. This information returned, such as the router's model number, is very valuable information in reconnaissance. This service is required to be disabled.

In order to disable the IP Identification Service on a Cisco router enter the following command from configure terminal mode:

no ip identd

3.06 Disable CDP
The Cisco Discovery Protocol allows for routers to identify themselves on the network. This information is also very important for reconnaissance as it may deliver a router's model number and IOS version making it vulnerable to attack. CDP is required to be disabled.

In order to disable CDP on a Cisco router enter the following command from configure terminal mode:

no cdp run

3.07 Disable IP Source Route
IP source routing allows the sender of an IP datagram to control the route or path that the packet will travel. This is rarely used for legitimate purposes, as it is possible to crash machines with IP source routing enabled. IP source routing is required to be disabled.

In order to disable IP source routing on a Cisco router enter the following command from configure terminal mode:

no ip source-route

3.08 Enable Password Encryption Service
Password encryption is useful for preventing people from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder. It is required that password encryption be enabled.

In order to enable the password encryption service on a Cisco router enter the following command from configure terminal mode:

service password-encryption

3.09 Enable Sequence Numbers and Time Stamps on Debugs
Time stamps on debug and log messages record the time and date that the event is created. Sequence numbers indicate the sequence in which messages that have identical time stamps were generated. Knowing the timing and sequence that messages are generated is an important tool in diagnosing potential attacks.

In order to enable sequence numbers and time stamps on debugs on a Cisco router enter the following command from configure terminal mode:

service timestamps debug datetime localtime show-timezone msec

service timestamps log datetime localtime show-timeout msec
service sequence-numbers

3.10 Enable IP CEF
Routes configured for Cisco Express Forwarding (CEF) perform better under SYN attacks than routers using the traditional cache.

In order to enable CEF on a Cisco router enter the following command from configure terminal mode:

ip cef

3.11 Disable IP Gratuitous ARPs
A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. A spoofed gratuitous ARP message can cause network-mapping information to be stored incorrectly which can result in a network malfunction.

In order to disable IP gratuitous ARPs on a Cisco router enter the following command from configure terminal mode:

no ip gratuitous-arps

3.12 Set Minimum Password Length
Longer passwords have exponentially more possible combinations of characters, making a brute force password attack much more difficult.

In order set the minimum password length to at least six characters on a Cisco router enter the following command from configure terminal mode:

security passwords min-length <6>

3.13 Set Authentication Failure Rate
Setting the authentication failure rate causes access to the router to be locked for 15 seconds after three unsuccessful login attempts. This protects against the dictionary method of attack. It is required that the authentication failure rate be set to three.

In order set the authentication rate to three on a Cisco router enter the following command from configure terminal mode:

security authentication failure rate <3>

3.14 Set TCP Synwait Time
The TCP synwait time is a value that is useful in protecting against SYN flooding attacks. Setting the TCP synwait time to ten seconds causes the router to shut down an incomplete connection after ten seconds, preventing the buildup of incomplete connections. It is required to have the synwait time set to ten seconds.

In order set the TCP synwait time to ten seconds on a Cisco router enter the following command from configure terminal mode:

ip tcp synwait-time <10>

3.15 Set Banner
The text banner is one method of informing users that the system they have connected to is private and that only authorized employees are allowed to connect to this host. It is required to have a banner that reads: "Authorized employee access only. This system is the property of GIAC Enterprises. Inappropriate use will be prosecuted!"

In order to create a banner on a Cisco router enter the following command from configure terminal mode:

banner ~
Authorized employee access only
This system is the property of GIAC Enterprises. Inappropriate use will be prosecuted!"
~

3.16 Enable Logging
Logging is critical to recognize and to respond to events. Time stamps and sequence numbers provide information about the date and time and sequence in which events occur. It is required that logging be enabled, however as a border router, logging only takes place locally on the router rather than opening a port on the firewalls.

In order to turn on logging on a Cisco router enter the following commands from configure terminal mode:

logging console critical
logging trap debugging
logging buffered 2048

3.17 Disable SNMP
The Simple Network Management Protocol provides a method for gathering data about network performance and processes. Since SNMP uses community strings which are stored and sent across the network in plain text and it is an easily spoofable protocol, it is required that it be disabled

In order to disable SNMP on a Cisco router enter the following commands from configure terminal mode:

no snmp-server

3.18 Disable IP Redirects
Hackers often use ICMP as a reconnaissance tool. Disabling ICMP redirects causes no operational impact to the network but it protects from several attacks. It is required that IP redirects be disabled.

In order to disable IP redirects on a Cisco router enter the following commands from configure terminal mode:

no ip redirects

3.19 Disable IP Proxy ARP
The Address Resolution Protocol converts IP addresses into MAC addresses. Routers can act as a proxy for ARP requests making ARP queries able to cross multiple networks but it also increases the chance for malicious use on the network. It is required that proxy ARP is to be disabled.

In order to disable IP proxy ARP on a Cisco router enter the following commands from configure terminal mode:

no ip proxy-arp

3.20 Disable IP Directed Broadcast
Directed broadcasts allow for the ability to broadcast packets across multiple subnets. This is very useful for DoS style attacks. For this reason it is required that IP directed broadcasts be disabled.

In order to disable IP directed broadcasts on a Cisco router enter the following commands from configure terminal mode:

no ip directed-broadcast

3.21 Disable IP Unreachables
ICMP unreachables can be used be used by hackers to perform reconnaissance and network mapping. This is why IP unreachables are required to be disabled.

In order to disable IP unreachables on a Cisco router enter the following commands from configure terminal mode:

no ip unreachables

3.22 HTTP Server Service
The HTTP service permits remote configuration and monitoring using a web browser. Since remote administration is done via SSH or the console port, it is required that the HTTP server service be disabled.

In order to disable IP unreachables on a Cisco router enter the following commands from configure terminal mode:

no ip http server

3.23 Enable SSH
Remote administration is conducted by using an SSH client to make Telnet access much more secure. Set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds. Also set the maximum number of unsuccessful SSH login attempts to two before locking access to the router.

In order to enable SSH with the required parameters on a Cisco router enter the following commands from configure terminal mode:

ip ssh time-out 60
ip ssh authtication-retries 2
!
line vty 0 4
transport input ssh
!

3.24 Outbound Traffic Access Control List (ACL)
The following is a list of requirements to block all non-compliant traffic originating from the GIAC Enterprises networks. The firewalls are used to restrict IP port and destinations.

Create an access control list for outbound traffic:
ip access-list extended outbound

Block all ICMP error packets that may leak information:
deny icmp any any time-extended unreachables echo-reply

Block all outbound NetBIOS/IP, SMB/IP and Windows services:
deny tcp any any range 135 139
deny udp any any range 135 139
deny udp any any range 445

Block all outbound TFTP, Syslog and SNMP:
deny udp any any 69
deny udp any any 514
deny udp any any range 161 162

Permit outbound IP traffic:
permit ip 201.201.201.0 0.0.0.255 any reflect ip-filter

Permit outbound replies to inbound SMTP connections:
evaluate smtp-filter

Block the remaining outbound traffic:
deny ip any any log-input

3.25 Inbound Traffic Access Control List (ACL)
The following is a list of requirements to block all non-compliant traffic destined for the GIAC Enterprises networks.

Create an access control list for inbound traffic:
ip access-list extended inbound

Block all packets with a source IP of a private addressing space:
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any

Block all packets with a source IP of a multicast or engineering address space:
deny ip 224.0.0.0 0.255.255.255 any

Block all packets with a source IP of localhost:
deny ip 127.0.0.0 0.255.255.255 any

Block all inbound NetBIOS/IP, SMB/IP and Windows services:
deny tcp any any range 135 139
deny udp any any range 135 139
deny udp any any range 445

Block all inbound TFTP, Syslog and SNMP:
deny udp any any 69
deny udp any any 514
deny udp any any range 161 162

Block all host-redirect requests as well as echo-request packets:
deny icmp any any host-redirect echo

Permit return traffic to outbound IP traffic:
evaluate ip-filter

Permit hosted traffic (DNS, SMTP, HTTP, HTTPS, IKE, IPSEC):
permit udp any 201.201.201.3 eq 53 reflect dns-udp-filter
permit tcp any 201.201.201.3 eq 53 reflect dns-tcp-filter
permit tcp any 201.201.201.3 eq 25 reflect smtp-filter
permit tcp any 201.201.201.3 eq 80 reflect http-filter
permit tcp any 201.201.201.3 eq 443 reflect https-filter
permit udp any 202.202.202.3 eq 500 reflect ike-filter
permit udp any 202.202.202.3 eq 10000 reflect ipsec-filter

4.0 Enforcement

GIAC Enterprises will take disciplinary action against employee found in violation of this policy (including termination of employment).

5.0 Revision History

Version:	*Date:*	*Revised by:*	*Approved by:*	*Comments:*
01:00:00	April 18, 2004	Bryan Feltin	CIO, CEO	New Policy

Format: xx.yy.zz
Where:
- xx – is the major revision number (usually used to indicate complete policy revisal).
- yy – is the minor revision number (usually used to indicate a section policy revisal).
- zz – is the revision in process number (used to keep track of changes during revision)

Firewall Security Policy

1.0 Purpose

The purpose of this policy is to define the standards of how GIAC Enterprises configures, secures, and installs any new firewall like devices into the corporation. These standards are defined to reduce the public exposure of the Internet and to protect GIAC Enterprises private information from malicious traffic.

2.0 Scope

This policy is aimed at firewall like devices that's purpose is to protect GIAC Enterprises from a third party and potentially hostile network. This policy focuses on the two Secure Computing G2 Security Appliances.

3.0 Firewall Security Requirements and Configuration

The following security requirements are based on industry best practices as well as GIAC Enterprises functional requirements. Since this policy covers two specific firewalls, bother general and specific requirements are discussed.

Interface Configuration:
Each interface or network card is connected to a separate network or "burb." Basically, the term "burb" is used to correlate an interface with a network.

Table 3.0 Secure Gateway Appliance 1 Interface Configuration

Interface	Burb Name	Burb Number	IP Address	Subnet Mask
exp0	Internal	1	10.10.100.1	255.255.255.0
exp1	External	2	201.201.201.3	255.255.255.0
eb0	ProxyDMZ	3	192.168.101.1	255.255.255.0
eb1	WebServerDMZ	4	192.168.103.1	255.255.255.0

Table 4.0 Secure Gateway Appliance 2 Interface Configuration

Interface	Burb Name	Burb Number	IP Address	Subnet Mask
exp0	Internal	1	10.10.200.1	255.255.255.0
exp1	External	2	202.202.202.3	255.255.255.0
eb0	VPNDMZ	3	192.168.102.1	255.255.255.0

DNS Service:
Both G2 Security Appliances are running the Domain Name Server (DNS) service. They are configured as a single-hosted DNS, which means there is no split DNS and the internal corporate DNS server is not accessible by the firewalls. This keeps external DNS traffic from internal and vice versa. Hosting DNS provides each subnet the ability to use a DNS server with centralized administration. It also allows GIAC Enterprises the ability to host its own Internet DNS server and to make DNS changes at its own will. The G2 Security Appliance 2 is the primary DNS server for giacenterprises.com, hosting the master database files. ISP1 and ISP2 both have slave DNS servers for backup.

See Appendix B, for the detailed DNS configuration.

SMTP Service:
The firewalls handle email with their hosted SMTP service, which uses sendmail as the SMTP agent. Using the hosted features allows for increase email security because of the "secure split" mail servers hosted on the firewall itself. There are actually three separate sendmail servers running on the firewall and each has to be configured properly to process mail. As well, by default the G2 Security Appliances reject relayed emails.

G2 Security Appliance 2 handles the majority of the email traffic and the G2 Security Appliance 1 is used as a backup if primary is unavailable. This is shown in Appendix B.1.2 by the DNS entries:

```
3600   IN    MX    5      smtp1.giacenterprises.com.
3600   IN    MX    10     smtp2.giacenterprises.com.
```

These two entries, known as mail exchange records, indicate which servers are responsible for handling email for the specified domain. Since smtp1.giacenterprises.com has a lower value (5 is lower than 10) it actually has a higher priority, but either mail server can accept mail.

The G2 Security appliances have a spam control ability enabled. This is simply and extension of the sendmail's feature set. It requires a configuration change and a real-time black hole list subscription from MAPS http://www.mail-abuse.org. Ideally, this will prevent a large amount of junk email from entering the corporation and protect it against malicious traffic.

According to The G2 Administration guide (*Secure Computing Corporation, p.286*), configure the firewall to use the Realtime Blackhole List, follow the steps below:

1. Log in to the Admin Console and select Services Configuration -> Servers
2. Select sendmail and click the Configuration tab. Separate configuration files are maintained for each burb.
3. Select the M4 Config File in the external burb list and click Edit File.
4. Add the following line to the file.
5. FEATURE('dnsbl', 'blackholes.mail-abuse.org') dnl
6. Save the changes you made to file and then close the file.
7. Click the Save icon to save the configuration changes and rebuild the configuration and database files. This automatically restarts the sendmail servers.

The G2 Security appliance forwards incoming email to the BlueCoat Secure Proxies, which proxies the inbound connection to the appropriate email server. Outbound email originated from the email servers is also proxied through the secure proxies to the firewalls.

See Appendix C, for the detailed SMTP configuration.

Web Traffic:
The website that is used for general information is http://www.giacenterprises.com and is hosted on TCP port 80. The website used for E-business transactions is https://www.giacenterprises.com and is hosted on port 443. The G2 Security Appliance 1 accepts port 80 and port 443 traffic, and passes it to the reverse proxy server. The reverse proxy, located in the Proxy DMZ, handles all web requests. The firewall is also configured to allow only the reverse proxy server a direct connection to the HTTP and HTTPS servers located in the Web Server DMZ.

VPN Traffic:
The remote user VPN solution requires the G2 Security Appliance 2 to allow two ports through to the VPN DMZ. The two ports are Internet Key Exchange (UDP 500) and IP Security or IPSec (UDP 10000). Since the standard Encapsulation Security Protocol, normally used in a VPN, does not work well through a NAT firewall, IPSec is used to encapsulate the VPN tunnel over UDP port 10000.

Access Policy:
All firewall devices have a "deny all except for what is explicitly allowed" access control policy. GIAC Enterprises is aware that this can be a more complex solution for administration but is willing to accept this to make its network more secure and controllable.

Access Control Lists:
Both G2 Security Appliances and both BlueCoat Secure Proxy Appliances have similar Access Control Rules for common traffic such as SMTP, HTTP, HTTPS and FTP. Since ISP1 hosts the websites and ISP2 hosts the VPN, these access control rules reside only on its specific appliance.

See Appendix D, for the detailed Access Control Lists

As shown in Table 5.0 in Appendix D, each access control list is numbered. The G2 Security Appliance processes the ACLs consecutively starting with 0. Once a traffic patter matches a rule, the traffic is passed and the appliance stops processing the ACLs. If no traffic pattern matches any ACLs, then ACL 100, the default "deny all" blocks the unwanted traffic.

As a precaution, both G2 secure appliances have a block rule as ACL 0. This ACL blocks the Dshield Top 10 Internet offender IP addresses. The network group called "Hostile" contains the IP addresses and the security appliance blocks all traffic from those addresses.

On the G2 Security Appliance 1, the next two ACLs (1 & 2) are next so the ACL processing takes as little time as possible to pass the traffic. This should keep the website responding as quickly as possible. These ACLs allow Internet users to connect to the reverse proxy server to view the web pages on ports 80 and 443 respectively.

The next two ACLs (3 & 4), are also placed close to the beginning of the list to maintain good performance. These two rules allow the reverse proxy server to connect to the web servers when the web sites content has changed. They use ports 80 and 443 respectively.

The remaining ACLs (5, 6, 7, 8, & 9) allow the BlueCoat secure proxy to access the Internet on ports 53(DNS), 80(HTTP), 443(HTTPS) and 20 & 21(FTP). These ACLs are placed lower in the list because employee web browsing is not as important as e-business transactions.

The main difference between the ACLs on the G2 Security Appliance 2 is that the web hosting ACLs are not required, but there are ACLs for VPN access. The two ACLs for VPN access (1 & 2) are also at the top of the order for performance. These rules allow two ports UDP 500 and UDP 10000 to pass through to the VPN concentrator. The security appliance protects the VPN endpoint from unnecessary traffic.

The BlueCoat Secure Proxy Appliances operate in a similar manner to the security appliances in that they process the rule set top down or ACL 0 first. The secure proxies have the same rule set so they can be used for redundancy if the other fails or if one ISP experiences problems. They currently provide access to

the Internet on ports 80(HTTP), 443(HTTPS), 20&21(FTP) as well as 25(SMTP) for email. Port 25 is also allowed through the Bluecoat for incoming emails.

4.0 Enforcement

GIAC Enterprises will take disciplinary action against employee found in violation of this policy (including termination of employment).

5.0 Revision History

Version:	*Date:*	*Revised by:*	*Approved by:*	*Comments:*
01:00:00	April 18, 2004	Bryan Feltin	CIO, CEO	New Policy

Format: xx.yy.zz
Where:
- xx – is the major revision number (usually used to indicate complete policy revisal).
- yy – is the minor revision number (usually used to indicate a section policy revisal).
- zz – is the revision in process number (used to keep track of changes during revision)

VPN Security Policy

1.0 Policy

The purpose of the virtual private network is to provide the GIAC Enterprises employees, such as the sales force, to remotely connect to the internal corporate network anywhere with Internet access.

2.0 Scope

Devices that provide a secure encrypted communication channel for GIAC Enterprises remote employees must abide by this policy. This includes the Cisco VPN 3030 concentrator and any software required in order to establish the secured channel.

3.0 Configuration

VPN users are required to have an RSA account and SecureID token synchronized with the RSA server. The user's laptop also requires the Cisco VPN client software and personal firewall Zone Alarm to be installed. The VPN software client is used to establish a secure encrypted tunnel from the client device to the VPN concentrator. The VPN concentrator applies filters and traffic management polices to authenticated users. Split tunneling is disabled making it necessary for all remote users to access the Internet via the corporate connection when they have a tunnel established. The client laptops are also running the Zone Alarm personal firewall and antivirus software to protect against unauthorized access, viruses, Trojans and worms.

GIAC Enterprises is using the latest version of Cisco VPN Client software for Windows 2000/XP laptops which can be downloaded from Cisco's website with the proper account login. Currently, the latest version posted on Cisco's web site is vpn-client-win-4.0.4.Rel-K9.exe and was posted on April 16, 2004. As well, the latest version of the Cisco 3030 Concentrator IOS image is being used. The most recent version of IOS software is vpn3000-4.1.3.Rel-K9.bin and was posted on April 14, 2004. This IOS image file is designed for the Cisco VPN Concentrator model 3015-3080.

In response to Bug ID CSCed41329 and Cisco Document ID: 50600 (http://www.cisco.com/warp/public/707/cisco-sn-20040415-grppass.shtml), there is currently an exploitable feature when using group usernames and passwords. GIAC Enterprises has considered this vulnerability to be low risk for various reasons. The group username and password is not the sole means of authentication. It is strictly used to provide filtering and policy management to end-users based on the group that the user is a member. The primary means of authentication is the RSA Secure ID tokens, a device with a six number liquid crystal display that changes every 60 seconds. Remote users need an account on the RSA server that is synchronized to their RSA SecureID token.

See Appendix E, for the detailed VPN configuration.

4.0 Enforcement

GIAC Enterprises will take disciplinary action against employee found in violation of this policy (including termination of employment).

5.0 Revision History

Version:	*Date:*	*Revised by:*	*Approved by:*	*Comments:*
01:00:00	April 18, 2004	Bryan Feltin	CIO, CEO	New Policy

Format: xx.yy.zz
Where:
- xx – is the major revision number (usually used to indicate complete policy revisal).
- yy – is the minor revision number (usually used to indicate a section policy revisal).
- zz – is the revision in process number (used to keep track of changes during revision)

ASSIGNMENT 3

DESIGN UNDER FIRE

Overview

The purpose of this exercise is to evaluate the security architecture of GIAC Enterprises as designed by a previous GCFW graduate. The approach is to be taken from a "black hat" or hacker perspective. The architecture that is to be evaluated was designed by William K. Hollis and was submitted on January 7, 2004. Here is the related URL: http://www.giac.org/practical/GCFW/William_Hollis_GCFW.pdf. William's diagram is also shown in Figure 3.0.

Goal

The end goal of this security evaluation an attempt to compromise and to retain access to the GIAC Web/Mail server located in William's DMZ. The process of compromising a web server also demonstrates different types of reconnaissance performed by hackers and what countermeasures can and should be taken to secure perimeter protection architecture.

Assumptions

- The domain giac.org is properly registered with Network Solutions.
- The website for GIAC Enterprises is www.giac.com.
- GIAC Enterprises public IP addresses are a class C provided by the ISP.

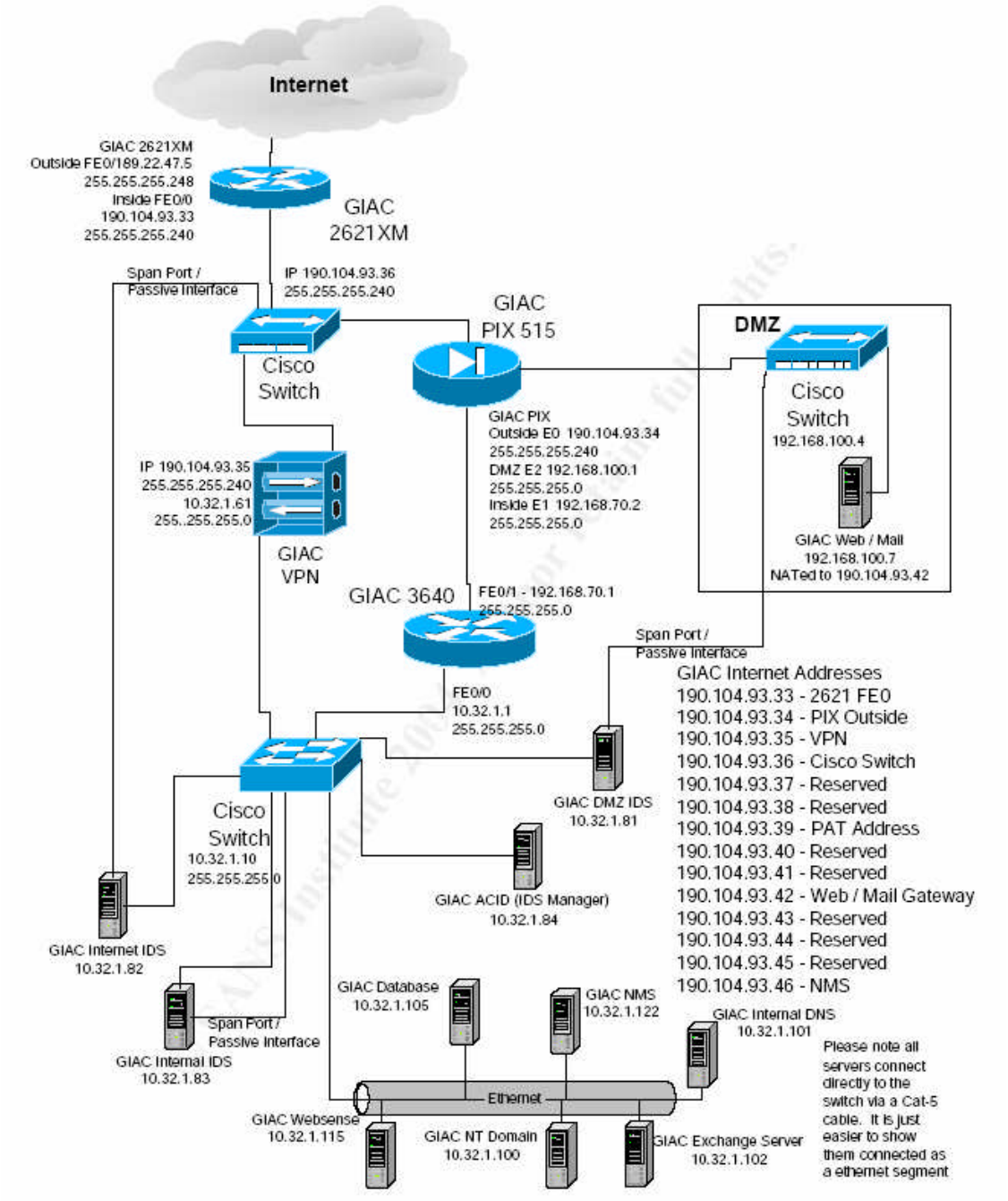


Figure 3.0 – GIAC Enterprises Security Architecture by William K. Hollis

Reconnaissance

Target Selection

GIAC Enterprises was chosen as a target due to its latest publicity in the media. At this stage we determine the city and the time zone that the company is located. This is needed to pick an ideal time for the attack. It is preferred to attack when no support staff is on site, if possible. This could be determined with social engineering but it does not have a large impact as the attack will take place whether or not there is support staff on site.

Determine Addresses

Since the goal is to eventually compromise the web server we have to verify that a web server does exist and is online. An anonymous proxy, located at http://johnny.ihackstuff.com was used to do this. The web site is active and browsed from an anonymous IP address to help cover any tracks that may indicate that we ever viewed the web site. Even though it is a public web site, the web logs never record our, the attacker's, actual IP address. It also provides a graphical view of the webpage that may have a banner on it stating which web server software they are running, such as "Powered by Apache."

Now that we know the website is located at www.giac.com, because we tried it in a web browser, we can perform an "nslookup" or "dig" to find the IP addresses. Or better yet, let's use a website like http://www.samspade.org to once again do our reconnaissance anonymously. With these tools we have determined that the IP address for www.giac.com resolves to 190.104.93.42 and that the server is available on TCP port 80.

The output from nslookup looks similar to the following:

```
C:\>nslookup
Default Server:  NS1.DNSMANAGED.COM
Address:  192.5.6.34

> www.giac.com
Server:  NS1.DNSMANAGED.COM
Address:  192.5.6.34

Non-authoritative answer:
Name:    www.giac.com
Addresses:  190.104.93.42
```

By performing a "whois 190.104.93" on the website http://www.arin.net, It may also be possible to determine if this address is owned by GIAC Enterprises or simply provided to it by an upstream ISP. The output looks similar to the following:

Search results for: 190.104.93.

ISPxxx (NET-190-104-0-0-1)
190.104.0.0 - 190.104.255.255
GIAC Enterprise Corporation (NET-190-104-93-0-1)
190.104.93.0 - 190.104.93.255

 # ARIN WHOIS database, last updated 2004-04-29 19:15
 # Enter ? for additional hints on searching ARIN's WHOIS database.

There are other DNS queries that we could use like trying to perform zone transfers or listings of the entire domain. Instead we focus on a specific DNS type, the mail exchanger or MX record. We use nslookup to see what the MX record is for giac.com. The commands below were performed on a Windows XP computer. We assume the output to be correct.

C:\>nslookup
Default Server: dns2.ispx.com
Address: 123.123.123.123

> set type=mx
> giac.com
Server: dns2.ispx.com
Address: 123.123.123.123

Non-authoritative answer:
giac.com MX preference = 10, mail exchanger = mail1.giac.com

giac.com nameserver = ns1.giac.com
giac.com nameserver = ns2.giac.com
giac.com nameserver = ns2.homepc.org
ns1.giac.com internet address = 213.213.213.213
ns2.giac.com internet address = 132.132.132.132

An nslookup for mail1.giac.com reveals the IP address to be 190.104.93.42. This is the same IP address that the web server is listening on. This is key because now we now that the target is a web/mail server that will have access through the firewall on port 25 in order to send and receive email traffic. We can use this knowledge later.

Determine the Operating System

Determining the OS is important because, once we know what the OS is we can find out how it is vulnerable and exploit it. The first attempt to determine what the web server is running, is to visit the website http://uptime.netcraft.com and query for www.giac.com. Normal results from netcraft.com look similar to the following:

OS, Web Server and Hosting History for www.giac.com
www.giac.com was running Apache on unknown when last queried at 30-Apr-2004 19:39:29 GMT

OS	Server	Last changed	IP address	Netblock Owner
unknown	Apache	30-Apr-2004	190.104.93.42	IP Services
Linux	WebServer	24-Jul-2003	190.104.93.42	Unknown

We assume that by changing the default error messages, like William has done in his design, has fooled netcraft.com so it cannot make a valid guess of what operating system the server is running. This means that more investigation is required.

Next we try OS Fingerprinting, the process of sending active packets to the target host and analyzing the responses. Since the program Nmap (http://www.insecure.org/nmap) contains the fingerprinting ability, this is the tool that is going to be used to do our scanning.

Nmap can be a real noisy scanner, which can be detected by IDS systems. The following command is run in paranoid mode to try to determine the operating system of the web server without setting off alerts. This scan will be performed with the Windows version 3.50 of Nmap during the early morning hours of 2:00am to reduce the probability of a quick response from support staff.

C:\nmap-3.50\nmap –O –T 0 –P0 –D11.11.12.13 www.giac.com

This command tells Nmap to perform an OS fingerprinting attempt (-O), in paranoid mode (-T 0) to be less noisy, do not perform a ping request (-P0) and use a decoy IP address of 11.11.12.13. The results of the command are assumed to be as follows:

C:\nmap-3.50>nmap -O –T 0 –P0 –D11.11.12.13 www.giac.com

Starting nmap 3.50 (http://www.insecure.org/nmap) at 2004-04-30 15:01 Canada Central Standard Time

Interesting ports on www.giac.com (190.104.93.42):
(The 1649 ports scanned but not shown below are in state: filtered)
PORT STATE SERVICE
80/tcp open http

Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or Windows XP

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

As shown highlighted above, we now know that the server is a windows server. An educated assumption is that that target is a server class computer running Windows 2000 Server or Advanced server. This gives us our first attack vector, the operating system.

Nmap Countermeasures

Since William's web server sits behind a firewall the accuracy of the Nmap query is reduced. Without the proper test environment, we assume that the Nmap scan did return Windows 2000 Server as the operating system. To add to the assumption, the Cisco PIX is not very "feature rich" when it comes to firewalls therefore it is assumed the OS fingerprint is successful.

Another countermeasure that Williams deployed is the intrusion detection system. Since we used Nmap in paranoid mode, it is assumed that the IDS system did not set off any alerts. Chances are the IDS administrator may notice strange traffic in the morning or over a couple of days.

There is another method, available for Windows 2000 and XP servers, to fool or confuse OS fingerprinting scanners. The Windows registry can be modified to change its characteristics for the way that it handles and responds to traffic. Settings such as the TCP window size, the time to live value and the maximum segment size are very specific to Windows. When these settings are modified it greatly increase the possibility of fooling a scanner. The detailed information on how to do this is provided by Microsoft (*Microsoft Corporation, p.1*).

Determine Web Server Software

Next we want to determine what kind of web server software is running on the web server. Since we know the server is running Windows, there is a good chance that it is running Microsoft's Internet and Information Services or IIS, but this is not certain.

Again we can use the web site http://uptime.netcraft.com as a first attempt. We used the same output shown earlier when trying to determine the OS but this time focusing on the "Server" section.

OS, Web Server and Hosting History for www.giac.com
www.giac.com was running Apache on unknown when last queried at 30-Apr-2004 19:39:29 GMT

OS	Server	Last changed	IP address	Netblock Owner
unknown	**Apache**	30-Apr-2004	190.104.93.42	IP Services
Linux	**WebServer**	24-Jul-2003	190.104.93.42	Unknown

Again we assume that Netcraft.com detected the server type as Apache due to the precautions that William has taken. If further investigation is not performed, hackers may try to attack the site with an Apache vulnerability. This is futile, as we know his web server is running IIS.

To verify if the web server is actually Apache, we can try a couple more techniques. One is to simply visit the web page with an invalid URL such as http://www.giac.com/notvalid.pdf. The goal here is to see what the error message looks likes.

For example, the default IIS 404-error message looks similar to the following (notice the error contains Internet Information Services which is a dead give away):

> *The page cannot be found*
> *The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.*
> *---*
> *Please try the following:*
> *If you typed the page address in the Address bar, make sure that it is spelled correctly.*
> *Open the www.giac.com/notvalid.pdf home page, and then look for links to the information you want.*
> *Click the Back button to try another link.*
> *HTTP 404 - File not found*
> ***Internet Information Services***
> *---*
> *Technical Information (for support personnel)*
> *More information:*
> *Microsoft Support*

As we already know, William has modified his default error messages and they may now look similar to the following (notice it says Apache when it is really running IIS):

> *The page cannot be found*
> *The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.*
> *---*
> *Please try the following:*
> *If you typed the page address in the Address bar, make sure that it is spelled correctly.*
> *Open the www.giac.com/notvalid.pdf home page, and then look for links to the information you want.*
> *Click the Back button to try another link.*
> *HTTP 404 - File not found*
> ***Apache 1.3.29***
> *---*
> *Technical Information (for support personnel)*
> *More information:*
> *Microsoft Support*

Since the error message we get from William's server was changed to make us think it is an Apache web server actually makes us a more suspicious that it is in fact NOT an Apache web server. This is because after testing other sites that are known to be running Apache such as http://www.apache.org, when an invalid URL is entered, the output did not inform us that it is an apache server. This is shown in the output below:

The page cannot be found
The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:
If you typed the page address in the Address bar, make sure that it is spelled correctly.
Open the www.apache.org/notvalid.pdf home page, and then look for links to the information you want.
Click the Back button to try another link.
HTTP 404 - File not found

Technical Information (for support personnel)
More information:
Microsoft Support

Error Message Countermeasures

Although William is on the right track to hide the fact that the server is running IIS, instead of forcing it to say Apache he should have simply removed all references to IIS and leave it at that. Another option he has is to redirect all invalid URLs to a valid one. For example, we typed in the URL http://www.giac.com/notvalid.pdf. Had he simply redirected that request to http://www.giac.com, no error messages are displayed and this type of reconnaissance is thwarted.

Now that we are suspicious to the web server being IIS after all, we try one more technique called "banner grabbing" to verify. To perform banner grabbing a telnet client is required.

This example is performed using a Windows XP telnet client. Run the following command to connect to the web site www.giac.com on port 80:

C:\telnet www.giac.com 80

A blank command prompt screen appears and depending on the screen echo setting you may or may not be able to see what you type. Type the following command:

GET / HTTP/1.0

This is a valid "GET" request and the very first few lines should give us what we need. The output is below:

HTTP/1.1 200 OK
Content-Length: 238
Date: Sat, 01 May 2004 15:32:36 GMT
Content-Location: http://www.giac.com/Default.htm
Content-Type: text/html
Server: Microsoft-IIS/5.0
Accept-Ranges: bytes
Last-Modified: Wed, 24 Mar 2004 22:13:36 GMT
ETag: "f046c540ed11c41:ab1"

Notice the server section in the above output. According to Microsoft (*Microsoft Corporation, p,1*), IIS 6.0 is included with Windows Server 2003, IIS 5.1 is included with Windows XP Professional and IIS 5.0 is included with Windows Server 2000. We can now conclude that William's server is running IIS 5.0 on Microsoft's Windows 2000 Server.

Finding Vulnerabilities

Now we need to decide how we are going to exploit the Windows 2000 Server running IIS 5.0. We know Microsoft has been getting a reputation of continually releasing security fixes for its products. Windows 2000 and IIS 5.0 are no exception. There are several ways to find vulnerabilities for these products. A simple search with Google can reveal a lot of interesting information as explained in "The Google Hacker's Guide" (*Long*) as available to registered users of the web site http://johnny.ihackstuff.com. But as a first means of research we try the vendors website to see if there is any mention of new vulnerabilities. New vulnerabilities are usually more successful as it takes time for system administrators to test and patch their systems.

On Microsoft's website we find the following Microsoft Security Bulletin:
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

> *Microsoft Security Bulletin MS04-011*
> *Security Update for Microsoft Windows (835732)*
> ***Issued: April 13, 2004***
> *Updated: April 28, 2004*
> Version: 1.2
>
> Summary
> Who should read this document: Customers who use Microsoft® Windows®
>
> **Impact of vulnerability: Remote Code Execution**
>
> *Maximum Severity Rating: Critical*
>
> *Recommendation: Customers should apply the update immediately.*
>
> *Security Update Replacement: This bulletin replaces several prior security updates. See the frequently asked questions (FAQ) section of this bulletin for the complete list.*
>
> *Caveats: The security update for Windows NT Server 4.0 Terminal Server Edition Service Pack 6 requires, as a prerequisite, the Windows NT Server 4.0 Terminal Server Edition Security Rollup Package (SRP). To download the SRP, visit the following Web site. You must install the SRP before you install the security update that is provided in this security bulletin. If you are not using Windows NT Server 4.0 Terminal Server Edition Service Pack 6 you do not need to install the SRP.*

This bulletin contains a couple of key pieces of information critical to our decision. The release date is April 13, 2004 so it is a very new vulnerability and the impact is rated as Remote Code Execution, which is our end goal.

The website http://packetstormsecurity.org is very helpful for us to achieve this goal. It has a searchable database of vulnerabilities as well as the exploit code. This is where we start by searching for the phrase "IIS Remote Command Execution." Several results are returned but the one of interest is shown below.

/// File Name:	iisex.c
Description:	iisex.c is a remote command execution exploit for Microsoft iis 4.0 and 5.0, as discussed in and iis-unicode.txt which attempts to provide an interactive cmd.exe shell.
Author:	Incubus
Homepage:	http://www.securax.org
MD5 Checksum:	459afc044268c9b7a2672e4e8ec28bf1

As we look into the details of the exploit code, we determined that this is a fairly old exploit and that the server is probably patched and not vulnerable. For the purpose of this exercise, we assume that the exploit code we found and downloaded from Packetstormsecurity.com is valid exploit code.

The Exploit

The IIS Unicode exploit code allows an attacker to remotely execute commands against IIS as the local account IUSR_<computername>. The information provided with the exploit code explains how to use cmd.exe to echo the contents of a hacker's constructed .asp file to the target system. Ideally this is done from obscured or spoofed IP and MAC addresses. Then from an anonymous proxy website, http://johnny.ihackstuff.com/, browse to the target website and specify the hacker.asp file (http://www.giac.com/hacker.asp). Once the file is launched the code in hacker.asp is executed on the system.

Once we can do this we can make the server do also anything want. As mentioned earlier we know that the web server is also a mail server or relay and it is able to connect outbound on port 25. We could have the exploited server connect to our hostile server on port 25 and potentially download malicious files or code that we could execute in the same manner as above. Now that we can remotely execute commands on the server and want to retain control we need to determine some information.

Let's start by running the command:

C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : webserver
Primary Dns Suffix . . . . . :
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : giac.prv

Ethernet adapter Local Area Connection 1:

Connection-specific DNS Suffix . :giac.prv
Description . . . . . : 3COM something PCI Card
Physical Address. . . . . : 00-01-1D-34-82-47
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.100.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DNS Servers . . . . . : 123.123.123.123

Here we can see the DNS suffix, which we can use to possibly create Windows domain accounts. We also see the Internal IP addressing scheme of the DMZ. This can be used to attack the firewall from the inside or try to get a hold of resources on the internal network.

The next thing we do is to create a new local account with administrative privileges. A quick search on Google tells us how to create accounts from the command line:

```
NET USER [username [password | *] [options]] [/DOMAIN]
username {password | *} /ADD [options] [/DOMAIN]
username [/DELETE] [/DOMAIN]
```

We could change the administrator password to something different with this command as well, but an administrators would notice that more easily. Instead we create an account that may get over looked by administrators, which may allow us to retain control of the server for a longer time.

net user IUSR_IIS password /ADD /Fullname:"IIS Default Account"

To finish off, we leave a backdoor program on the target web server. Again we check Google and Packetstormsecurity to see what various backdoor programs are currently available. This provides us access to the system whenever we want to play havoc until the backdoor is detected. Here is a good article for attempting how to do this http://www.thc.org/papers/fw-backd.htm.

Exploit Countermeasures

To avoid this exploit, the most obvious countermeasure for this scenario would have been to apply the patches sooner. That is assuming that a patch is available from the vendor in time, which is not always the case.

Another option is to place the proper permissions on the cmd.exe file on the IIS server so IUSER_<computername> cannot launch it. This would have prevented this exploit. So a properly locked down server would have helped.

Administrators of web servers should also make sure unnecessary services are disabled and unnecessary programs are removed. Antivirus software running on the web server should detect common back door applications but might not detect “home-brew” applications.

ASSIGNMENT 4A

FUTURE STATE OF SECURITY TECHNOLOGY

Overview

Several years ago the Internet was new, exciting and its full potential was unknown. Fast-forward several years. The Internet has evolved from dial-up Internet access to high-speed modems. It has become a low cost investment reaching the stages of a mission-critical medium for business and employee transactions.

The low cost investment and large amount of resources on the Internet attracts high employee usage. The different services provided by the Internet make it difficult for employees to remain focused on work related usage. Employees find the Internet too convenient to play games, watch videos, chat with friends, send and receive emails and more.

Not only does this cause a loss in employee production but some material on the Internet can be harmful to computers, networks and even the company's reputation. Peer-to-peer applications such as Kazaa or streaming audio websites can saturate a company's connection to the Internet. Bandwidth saturation can have a negative impact on the company if it relies on the Internet to perform business transactions.

Even though allowing employee access to the Internet is valuable, there are ways of minimizing and controlling end user abuse. The purpose of this paper focuses on how organizations can use new technologies to combat this problem. Some points may seem common sense and some technologies mentioned are fairly new to the industry.

Education

The first place to start is with education. Everyone from management to end users need to understand the implications of using unauthorized software, such as peer-to-peer and instant messaging applications. The latest versions of these programs can be configured to access the Internet on any port, even port 80. This means that the applications are able to connect to the Internet, even if it is against our wishes.

Many viruses, worms, Trojans and other malicious software are disguised as fun games or cool programs, especially on peer-to-peer networks. When these malicious programs are downloaded and launched on a company's network, anything can happen. Perhaps a virus runs havoc on the network requiring the servers to be shut down or a network disruption occurs. Perhaps the program installs a backdoor to the Internet providing a hacker complete access to the computer. The hacker may then be able to access confidential information.

These malicious programs can also be received in emails from friends, from spam or junk mail or even from a web based email account. Web based email viruses are becoming commonplace.

Educating people will help, but it is not a cure. Security policies must be in place in order to enforce users to a specific set of rules. Security it not a technology, it is a policy. There are however, technologies available to help augment education and to help enforce security policies. The focus of security was once to keep the hackers out. The trend now is to prevent employees from behaving improperly. It was once acceptable to allow port 80 to all destinations but this is no longer acceptable in today's security conscious world.

Technology

Web applications that run over port 80 are everywhere. Since TCP port 80 is most commonly opened on firewalls for all users to any destination, firewalls alone cannot prevent users from configuring an application to use port 80. New technologies are available that can help prevent employees from improper use of the Internet. The technologies are often referred to as "port 80" firewalls or application firewalls. A more preferred term could be "IP Port Firewalls" as the devices can firewall more than port 80.

Assume we have a firewall with TCP port 80 open for all users to all destinations. There are a lot of programs on the Internet that can be downloaded, installed and reconfigured to use port 80. Applications such as Winamp, Kazaa, AOL Instant Messenger, Real One Player as well as peripheral auto update software, can be troublesome. Not only can these programs be used to download malicious files but they can also have security vulnerabilities. If an employee uses an application that is vulnerable to some form of attack, it can put the entire company at risk. If the company knows that the user is running the software, it can be upgraded or patched to remove the vulnerability. If an end user installs the application, and the company does not know about it, it may never get patched. If a software inventory program such as Microsoft's SMS Server is in place, it may be easy to determine who has the software installed and what version. If there is no such software inventory program, then how can an organization fix a vulnerability that they do not even know they have?

Imagine a device placed between the end users and the perimeter security firewall that analyzes the passing traffic and based on established policies affects the way that the traffic gets handled. The traffic policies could either deny the traffic completely or simply reduce the amount bandwidth the traffic is utilizing. There are several companies that provide such a device. One is already mentioned in this paper and it is BlueCoat Systems (http://www.bluecoat.com). This type of technology may seem commonplace in the industry but not to the extent of these new types of appliances.

The BlueCoat Systems (*BlueCoat Systems*, *p.1*) secure proxy appliance feature list includes, Content Filtering, Instant Message Control, Web proxy, Content Security, Web Virus Scanning and bandwidth management. As noted, the BlueCoat system is a secure proxy appliance. It is not a firewall nor is it meant to be. The BlueCoat appliance used in a layered architecture in conjunction with a stateful firewall is very solid and secure solution. A layered defense adheres to the defense in depth concept and to not rely on a single security technology to protect a network. There are other proxy server appliances and software on the market, but the feature set is lacking compared to these new appliances.

The BlueCoat appliance has some interesting features applicable to this discussion. There are other technologies available that perform similar functions but the BlueCoat's primary purpose is for perimeter network security. The first feature that is becoming more requested by management is content filtering. Content filtering is a method to block users that attempt to access inappropriate web sites. Just because a firewall configuration allows end users to view improper web sites does not means that employees should. Even if policies are in place stating that users are to use the Internet for work related usage only, inappropriate usage will still occur. There are a lot of valuable web sites on the Internet but there is an enormous amount more that are garbage.

Employees are allowed full access because it is nightmare for firewall administrators to maintain a list of acceptable Internet sites that employees can access. It is just not feasible. Content filtering can help with this by restricting employees from accessing inappropriate sites based on category. For example, categories such as porn, hate speech, gambling, dating and so on could be blocked 24 hours a day or only during working hours. By blocking user access to these sites help prevent the users from downloading malicious software. It is also possible to add non-categorized sites such as a local ISP's web mail server to a specific category.

Content filtering also provides a "coaching" feature. If the sports category is coached, a warning message appears stating that the user is entering a non-work related site and that their usage is being monitored. It then asks if the user is sure they want to continue. There is other content filtering software that has a delay option where an administrator could add a five or ten second delay to the sports category. The goal here is that the site takes so long to load the user simply gives up.

There are many companies that provide URL and content filtering software but more popular ones are Secure Computing's SmartFilter and Websense. The following is a list of growing risks of Internet abuse according to Websense (Reference Websense).

- 77% of companies have at least one peer-to-peer file sharing application on their network.
- 1 in every 5 corporate users is using instant messaging tools.
- 44% of employees run streaming media applications during the workday
- As many as 9 out of every 10 computers are infected with spyware.
- The Nimda virus affected more than 2 million servers and PCs worldwide.
- In the last 12 months, 45% of businesses detected unauthorized access by insiders.

Websense not only provides URL filtering it has several other useful features such as blocking the launch of malicious or illegal software applications on desktops, blocking employee hacking, keyboard piracy, spyware, peer-to-peer file sharing, manage instant messaging and more.

Another technology of interest is web virus scanning. The ability to perform on the fly virus scanning at the perimeter security level can be extremely useful. It can prevent web-based viruses from even getting through to the corporate network. This even applies to attachments found in web-based emails. Web-based email is a relatively new service being provided by more and more companies and ISPs. This service allows an end user at work to connect to a web page on port 80 and read and download their home email. This is a handy service but it can also be very dangerous.

Corporate email systems usually have virus scanning incorporated and scan new email as it arrives. When users bypass the antivirus safe guard and download malicious software from a web mail site, it circumvents security precautions already in place. I know of a company that runs a non-Microsoft email server and email viruses were few and far between. The company never had network downtime due to an email virus. The local ISP did have a web mail service but it was hosted on port 1623. That is good news because that port is blocked outbound on the firewall. Several users complained to the help desk that they could not log into their web mail from work. When these users were asked for a business case to open the port on the firewall, not one business case was submitted. As soon as the local ISP changed their web mail server from being hosted on port 1623 to port 80, the web mail viruses started. This goes to show the power of allowing anything to run over port 80. This needs to be controlled.

The most useful feature provided by the BlueCoat appliance is the ability to apply Content Security based on users or groups. This is very important to tackling the port 80 problems. The BlueCoat appliance can be configured to only allow a specific browser and version, such as Internet Explorer version 6 SP1, access to the Internet on port 80. This is huge! The BlueCoat appliance just disabled thousands of applications from traversing the Internet on port 80.

Content security can also be configured to allow specific users or groups the ability to download certain type of files. Some file types on the Internet are often associated with worms and other malicious software. The ability to prevent these files from reaching the internal network is very important in maintaining a secure environment. If an employee does manager to browse to a malicious web site, content security can strip and replace potentially dangerous active content from the web page and still serve the remainder of the web content. This removes any harmful material from getting to the internal network and the user may still get the information they require. Content security can also perform granular stripping of active content, such as stripping Visual Basic scripts for all users, but allow ActiveX for certain ones.

Web based email does have a valid purpose but it needs to be controlled. Many email viruses are in the form of attachments. It is ideal to prevent or limit which users can download attachments from web mail servers. Content security performs this function based on users or groups.

Final Thoughts

As discussed, security policies are put in place to protect and to provide guidance to employees in how they interact with the Internet. The Internet can be a dangerous place for employees and misuse can result in termination. Firewalls in conjunction with secure proxy appliances help enforce security policies. Secure perimeter architectures can actually protect end users by preventing them from breaking the policies. A secure perimeter however, is not a silver bullet. New sites are always being added to the Internet and there are new worms and malicious code released every day. Policies and security technology configurations need to be maintained, reviewed regularly and updated as the Internet evolves.

APPENDIX A – Domain Registration

GIAC Enterprises decided to register the domain giacenterprises.com to have as its Internet presence. Below is the current registration as hosted by Network Solutions http://www.networksolutions.com.

giacenterprises.com

Registrant:
GIAC Enterprises
ATTN: GIACENTERPRISES.COM
c/o Network Solutions
P.O. Box 447
Herndon, VA. 20172-0447

Domain Name: GIACENTERPRISES.COM

Administrative Contact:
Admin, FIrewall pf54c36k4t3@networksolutionsprivateregistration.com
ATTN: GIACENTERPRISES c/o Network Solutions
P.O. Box 447
Herndon, VA 20172-0447
570-708-8780

Technical Contact:
Network Solutions, LLC. (HOST-ORG) customerservice@networksolutions.com
13200 Woodland Park Drive
Herndon, VA 20171-3025
US
1-888-642-9675 fax: 571-434-4620

Record expires on 26-April-2010.
Record created on 26-April-2004.
Database last updated on 28-Apr-2004 11:13:58 EDT.

Domain servers in listed order:

DNS1.GIACENTERPRISES.COM 202.202.202.3
DNS1.ISP1.COM xxx.xxx.xxx.xxx
DNS1.ISP2.COM xxx.xxx.xxx.xxx

This listing is a Network Solutions Private Registration. Mail correspondence to this address must be sent via USPS Express Mail™ or USPS Certified Mail®; all other mail will not be processed. Be sure to include the registrant's domain name in the address.

APPENDIX B – GIAC Enterprises DNS Configuration

B.1.0 Primary DNS Server – G2 Security Appliance 2

Configuration Files:

1) */etc/named.conf.u* – This file controls how BIND operates by maintaining the global BIND parameters as well as the zones for which the server is master or slave.
2) */etc/namedb.u/giacenterprises.com.db* – This is the zone database file for giacenterprises.com. This file controls how www.giacenterprises.com gets resolved to an IP address.

B.1.1 named.conf.u

```
#include "/etc/rndc.key";
controls {
        inet 127.0.0.1 allow { localhost; } keys { "rndc-key"; };
};
// named configuration file
options {
        directory "/etc/namedb.u";
        dump-file "named_dump.db.u";
        statistics-file "named.stats.u";
        allow-transfer {127.0.0.1; dns1.isp1.com.; dns1.isp2.com.; 201.201.201.3;};
};
zone "100.10.10.in-addr.arpa" {
        type master;
        file "100.10.10.db";
};
//
zone "202.202.202.in-addr.arpa" {
        type master;
        file "202.202.202.db";
};
//
zone "102.168.192.in-addr.arpa" {
        type master;
        file "102.168.192.db";
};
//
zone "giacenterprises.com" {
        type master;
        file "giacenterprises.com.db";
};
//
zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.db";
};
//
zone "." {
        type hint;
        file "root.cache";
};
```

B.1.2 giacenterprises.com.db

```
; *** NOTE: Serial number is in the format YYYYMMDD##
; where ## starts at 01 and is incremented by 1 each time a change is made for that day
$ORIGIN com.
;
giacenterprises   3600   IN     SOA     dns1.giacenterprises.com. postmaster.giacenterprises.com. (
                2004042001 3600 1800 1728000 3600 )
        3600    IN      NS      dns1.giacenterprises.com.
        3600    IN      NS      dns2.giacenterprises.com.
        3600    IN      NS      dns1.isp1.com.
        3600    IN      NS      dns1.isp2.com.
        3600    IN      MX      5 smtp1.giacenterprises.com.
        3600    IN      MX      10 smtp2.giacenterprises.com.
;
$ORIGIN giacenterprises.com.
dns1    3600    IN      A       202.202.202.3    ; ISP 2 Firewall 2
dns2    3600    IN      A       201.201.201.3    ; ISP 1 Firewall 1
smtp1   3600    IN      A       202.202.202.3    ; ISP 2 Firewall 2
smtp2   3600    IN      A       201.201.201.3    ; ISP 1 Firewall 1
www     3600    IN      A       201.201.201.3    ; ISP 1 Firewall 1
vpn     3600    IN      A       202.202.202.3    ; ISP 2 Firewall 2
```

B.2.0 Slave DNS Server – G2 Security Appliance 1

Configuration Files:

1) */etc/named.conf.u* – This file controls how BIND operates by maintaining the global BIND parameters as well as the zones for which the server is master or slave.
2) */etc/namedb.u/giacenterprises.com.db* – This is the zone database file for giacenterprises.com. This file controls how www.giacenterprises.com gets resolved to an IP address. Since G2 Security Appliance 1 is a slave DNS server, this file is actually a copy from the G2 Security Appliance 2.

B.2.1 namedb.u

```
#include "/etc/rndc.key";
controls {
        inet 127.0.0.1 allow { localhost; } keys { "rndc-key"; };
};
// named configuration file
options {
        directory "/etc/namedb.u";
        dump-file "named_dump.db.u";
        statistics-file "named.stats.u";
        allow-transfer {127.0.0.1; dns1.isp1.com.; dns1.isp2.com.; 202.202.202.3;};
};
zone "200.10.10.in-addr.arpa" {
        type master;
        file "100.10.10.db";
};
//
zone "201.201.201.in-addr.arpa" {
        type master;
        file "201.201.201.db";
};
//
zone "101.168.192.in-addr.arpa" {
        type master;
        file "101.168.192.db";
};
//
zone "103.168.192.in-addr.arpa" {
        type master;
        file "103.168.192.db";
};
//
zone "giacenterprises.com" {
        type slave;
        file "giacenterprises.com.db";
        masters {
                202.202.202.3;
        };
};
//
zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.db";
};
zone "." {
        type hint;
        file "root.cache";
};
```

APPENDIX C – GIAC Enterprises SMTP Configuration

C.1.0 Primary SMTP Server – G2 Security Appliance 2

Configuration Files:

3) */etc/mailertable.mta1* – tells sendmail to which server to route incoming mail.
4) */etclmailertable.mta2* – tells sendmail to only accept email for the domains listed.

C.1.1 mailertable.mta1

```
#####################################################################
# /etc/mailertable.mta<burb>
#
#  On the INTERNAL side of the Sidewinder, this file is used to
#  map
#  domain names to delivery-agent:relay-host name pairs.
#  For example:
#
#  my.domain     smtp:mailhost.my.domain
#  .my.domain    smtp:mailhost.my.domain
#
#  would direct Sendmail to use the smtp mailer to send mail
#  addressed  #  to the my.domain domain to the
#  mailhost.my.domain mailhost.
#
#####################################################################
#
giacenterprises.com     smtp:bluecoat2.giacenterprises.dmz
. giacenterprises.com    smtp: bluecoat2.giacenterprises.dmz
#
#####################################################################
#  The above two lines indicate that the firewalls will relay all
#  inbound SMTP traffic the BlueCoat Secure Proxy appliance 2
#  which will in turn deliver the email to the Email server.
#####################################################################
```

C.1.2 mailertable.mta2

```
######################################################################
# On the EXTERNAL side of the network, /etc/mailertable.mta<burb>
# is used to direct incomming mail to the internal Sendmail
# processes.  This is accomplished using the SCC-defined "mfil"
# mailers.
#
# For example:
#                sctc.com      mfil-21:firewall.domain
#                .sctc.com     mfil-21:firewall.domain
#
# would direct all incomming mail from the burb 2 network to a
# Sendmail process running in burb 1, which would, in turn,
# examine its mailertable.mta<burb> file to determine where to
# deliver the
# message.
#
######################################################################
#
giacenterprises.com     mfil-21:G2SA2.giacenterprises.prv
. giacenterprises.com    mfil-21:G2SA2.giacenterprises.prv
#
######################################################################
#  The above two lines tell the external Sendmail process to
#  forward email for giacenterprises.com to the internal sendmail
#  server on G2 Security Appliance 2
######################################################################
```

C.2.0 Secondary SMTP Server – G2 Security Appliance 1

Configuration Files:

5) */etc/mailertable.mta1* – Tells Sendmail which server to route incoming mail to.
6) */etclmailertable.mta2* – Tells Sendmail to only accept email for the domains listed.

C.2.1 mailertable.mta1

```
###################################################################
# /etc/mailertable.mta<burb>
#
#  On the INTERNAL side of the Sidewinder, this file is used to
#  map
#  domain names to delivery-agent:relay-host name pairs.
#  For example:
#
#  my.domain     smtp:mailhost.my.domain
#  .my.domain    smtp:mailhost.my.domain
#
#  would direct Sendmail to use the smtp mailer to send mail
#  addressed  #  to the my.domain domain to the
#  mailhost.my.domain mailhost.
#
###################################################################
#
giacenterprises.com     smtp:bluecoat1.giacenterprises.dmz
. giacenterprises.com    smtp: bluecoat1.giacenterprises.dmz
#
###################################################################
#  The above two lines indicate that the firewalls will relay all
#  inbound SMTP traffic the BlueCoat Secure Proxy appliance 1
#  which will in turn deliver the email to the Email server.
###################################################################
```

C.2.2 mailertable.mta2

```
######################################################################
# On the EXTERNAL side of the network, /etc/mailertable.mta<burb>
# is used to direct incomming mail to the internal Sendmail
# processes.  This is accomplished using the SCC-defined "mfil"
# mailers.
#
# For example:
#                sctc.com      mfil-21:firewall.domain
#                .sctc.com     mfil-21:firewall.domain
#
# would direct all incomming mail from the burb 2 network to a
# Sendmail process running in burb 1, which would, in turn,
# examine its mailertable.mta<burb> file to determine where to
# deliver the
# message.
#
######################################################################
#
giacenterprises.com     mfil-21:G2SA1.giacenterprises.prv
. giacenterprises.com    mfil-21:G2SA1.giacenterprises.prv
#
######################################################################
#  The above two lines tell the external Sendmail process to
#  forward email for giacenterprises.com to the internal sendmail
#  server on G2 Security Appliance 1.
######################################################################
```

Appendix D – GIAC Enterprises Access Control Lists

Table 5.0 G2 Security Appliance 1 Access Control List

ACL Name	*ACL #*	*Action*	*Source Burb*	*Source IP*	*Destination Burb*	*Destination IP*
Block-Hostile IPs	0	deny	External	Netgroup:Hostile	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	all	all	Denys all traffic from hostile IP addresses
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTP-Inbound(00080)	1	allow	External	all	External	201.201.201.3
			Redirect to:	***Service***	***Service name***	***Comments***
			192.168.103.3	proxy	http	Allows the Internet to http://www.giacenterprises.com
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTPS-Inbound(00443)	2	allow	External	all	External	201.201.201.3
			Redirect to:	***Service***	***Service name***	***Comments***
			192.168.103.3	proxy	https	Allows the Internet to https://www.giacenterprises.com
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTP-Proxy(00080)	3	allow	ProxyDMZ	192.168.101.2	WeServerDMZ	192.168.103.2
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	http	Allows the reverse proxy server to connect to the http server
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTPS-Proxy(00443)	4	allow	ProxyDMZ	192.168.101.2	WeServerDMZ	192.168.103.3
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	http	Allows the reverse proxy server to connect to the https server
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
DNS-Outbound(00053)	5	allow	Internal	10.10.100.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	dns	Allows DNS resolution to be performed by the BlueCoat appliance for SMTP traffic as well as web traffic
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTP-Outbound(00080)	6	allow	Internal	10.10.100.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	http	Allows Internal users proxied through the BlueCoat appliance Internet Access on port 80
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTPS-Outbound(00443)	7	allow	Internal	10.10.100.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	http	Allows Internal users proxied through the BlueCoat appliance Internet Access on port 443
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
FTP-Outbound(00021)	8	allow	Internal	10.10.100.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	ftp	Allows Internal users proxied through the BlueCoat appliance FTP Access on port 21
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
FTP-Outbound(00020)	9	allow	Internal	10.10.100.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	ftp-data	Allows Internal users proxied through the BlueCoat appliance FTP Access on port 20
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
Deny-all	100	deny	any	all	any	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	all	all	Default deny all traffic

Table 6.0 G2 Security Appliance 2 Access Control List

ACL Name	*ACL #*	*Action*	*Source Burb*	*Source IP*	*Destination Burb*	*Destination IP*
Block-Hostile IPs	0	deny	External	Netgroup:Hostile	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	all	all	Denys all traffic from hostile IP addresses that are members of the network group "Hostile"
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
VPN-IKE-Inbound(00500)	1	allow	External	all	External	202.202.202.3
			Redirect to:	***Service***	***Service name***	***Comments***
			192.168.102.20	proxy	IKE	Allows remote users to connect to the Cisco VPN Concentrator
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
VPN-IPSec-Inbound(10000)	2	allow	External	all	External	202.202.202.3
			Redirect to:	***Service***	***Service name***	***Comments***
			192.168.102.20	proxy	IPSec	Ecapsulates VPN traffic over UDP port 10000 in order for VPN to work through a NAT firewall
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
DNS-Outbound(00053)	2	allow	Internal	10.10.200.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	dns	Allows DNS resolution to be performed by the BlueCoat appliance for SMTP traffic as well as web traffic
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTP-Outbound(00080)	3	allow	Internal	10.10.200.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	http	Allows Internal users proxied through the BlueCoat appliance Internet Access on port 80
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
HTTPS-Outbound(00443)	4	allow	Internal	10.10.200.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	http	Allows Internal users proxied through the BlueCoat appliance Internet Access on port 443
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
FTP-Outbound(00021)	5	allow	Internal	10.10.200.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	ftp	Allows Internal users proxied through the BlueCoat appliance FTP Access on port 21
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
FTP-Outbound(00020)	6	allow	Internal	10.10.200.1	External	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	proxy	ftp-data	Allows Internal users proxied through the BlueCoat appliance FTP Access on port 20
ACL Name	***ACL #***	***Action***	***Source Burb***	***Source IP***	***Destination Burb***	***Destination IP***
Deny-all	100	deny	any	all	any	all
			Redirect to:	***Service***	***Service name***	***Comments***
			NA	all	all	Default deny all traffic

Table 7.0 BlueCoat Secure Proxy Appliance 1 Access Control List

ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
HTTP-Outbound(00080)	0	allow	Internal	Internet-Web	Internal - 172.20.100.1
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.100.1	http	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 80 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
HTTPS-Outbound(00443)	1	allow	Internal	Internet-Web	Internal - 172.20.100.1
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.100.1	https	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 443 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
FTP-Outbound(00021)	2	allow	Internal	Internet-Web	Internal - 172.20.100.1
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.100.1	ftp	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 21 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
FTP-Outbound(00020)	3	allow	Internal	Internet-Web	Internal - 172.20.100.1
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.100.1	ftp-data	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 20 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
SMTP-Outbound(00025)	4	allow	Internal	172.20.100.5	Internal - 172.20.100.1
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.100.1	smtp	Relays outbound mail from giacenterprises.com to the G2 Security Appliance 1
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
SMTP-Inbound(00025)	5	allow	External	10.10.100.1	External - 10.10.100.2
			Forward request to:	***Protocol Definition***	***Comments***
			172.20.100.5	smtp	Relays inbound mail for giacenterprises.com to the email server
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
Deny-all	100	deny	any	any	any
			Forward request to:	***Protocol Definition***	***Comments***
			NA	any	Default deny all traffic

Table 8.0 BlueCoat Secure Proxy Appliance 2 Access Control List

ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
HTTP-Outbound(00080)	0	allow	Internal	Internet-Web	Internal - 172.20.100.2
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.200.1	http	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 80 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
HTTPS-Outbound(00443)	1	allow	Internal	Internet-Web	Internal - 172.20.100.2
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.200.1	https	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 443 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
FTP-Outbound(00021)	2	allow	Internal	Internet-Web	Internal - 172.20.100.2
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.200.1	ftp	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 21 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
FTP-Outbound(00020)	3	allow	Internal	Internet-Web	Internal - 172.20.100.2
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.200.1	ftp-data	Verifies the requesting user is a member of the Internet-Web group and permits or denies port 20 access based on the results
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
SMTP-Outbound(00025)	4	allow	Internal	172.20.100.5	Internal - 172.20.100.2
			Forward request to:	***Protocol Definition***	***Comments***
			10.10.200.1	smtp	Relays outbound mail from giacenterprises.com to the G2 Security Appliance 1
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
SMTP-Inbound(00025)	5	allow	External	10.10.200.1	External - 10.10.200.2
			Forward request to:	***Protocol Definition***	***Comments***
			172.20.100.5	smtp	Relays inbound mail for giacenterprises.com to the email server
ACL Name	***ACL#***	***Action***	***Source Interface***	***Source Domain Group***	***Destination Interface***
Deny-all	100	deny	any	any	any
			Forward request to:	***Protocol Definition***	***Comments***
			any	any	Default deny all traffic

APPENDIX E – GIAC Enterprises VPN Configuration

E.1.0 Cisco VPN Client Profile File

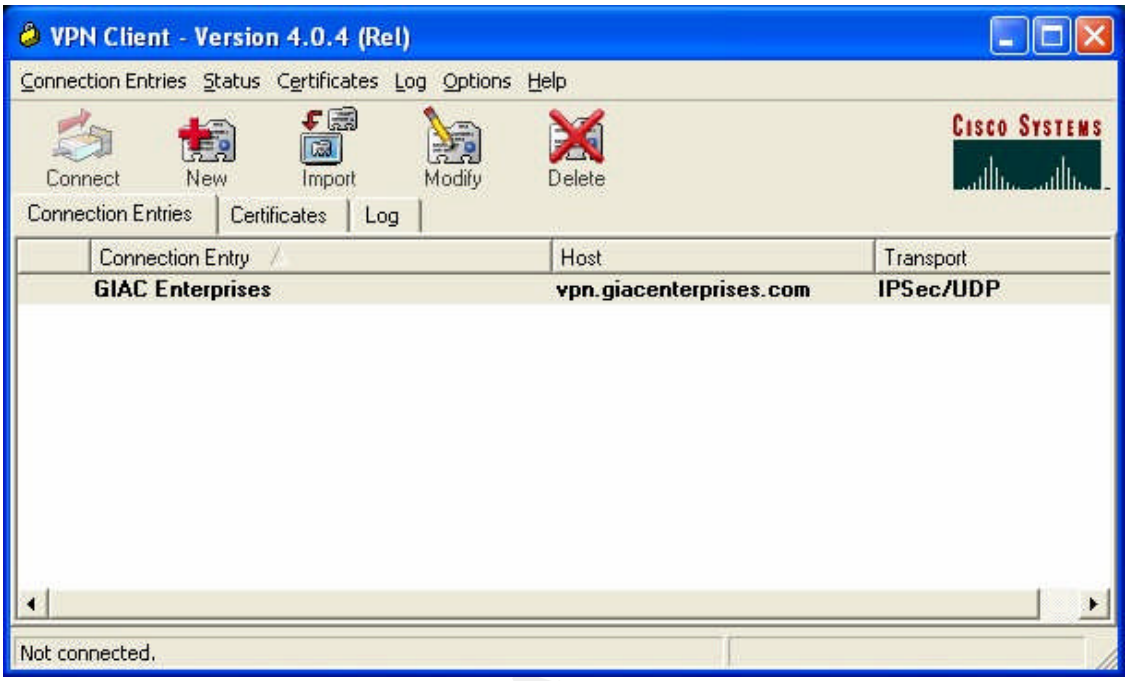
The Cisco VPN client software stores the connection configuration in a profile configuration file (.pcf). The default install path is "c:\program files\cisco systems\VPN Client\." There are only a few settings specific to GIAC Enterprises. The host is set to vpn.giacenterprises.com which resolves to 202.202.202.3. The group name is hard coded to GIACEnterprises and the group password is an encrypted 32 character ambiguous password that makes it extremely difficult to guess and hack. This decision was made because the main authentication process will be the RSA Secure ID token.

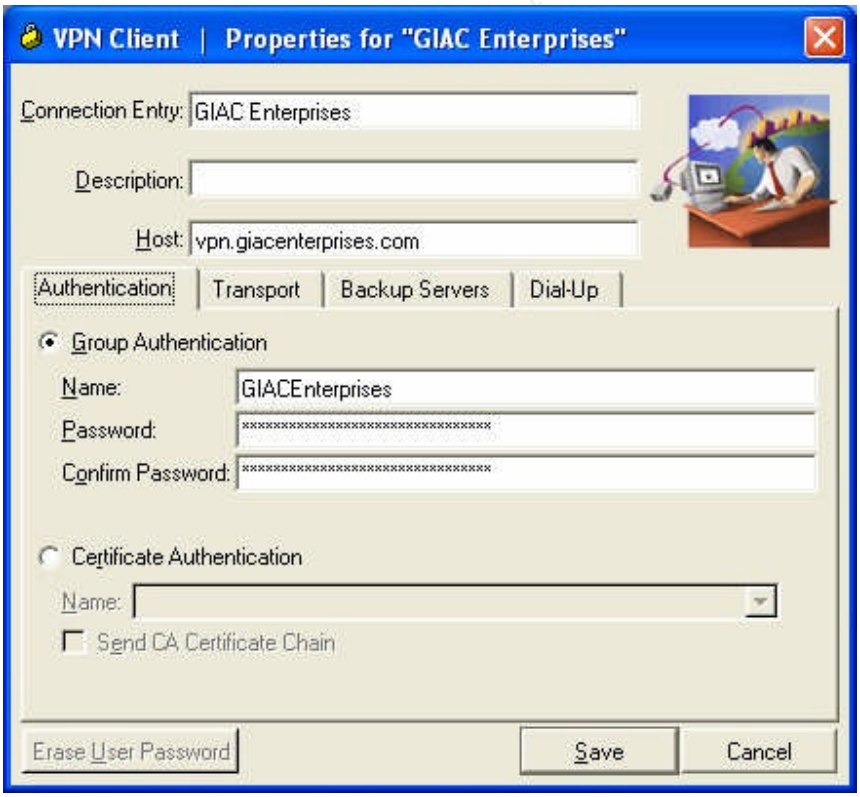
E1.1 GIAC Enterprises VPN Profile File Text Configuration

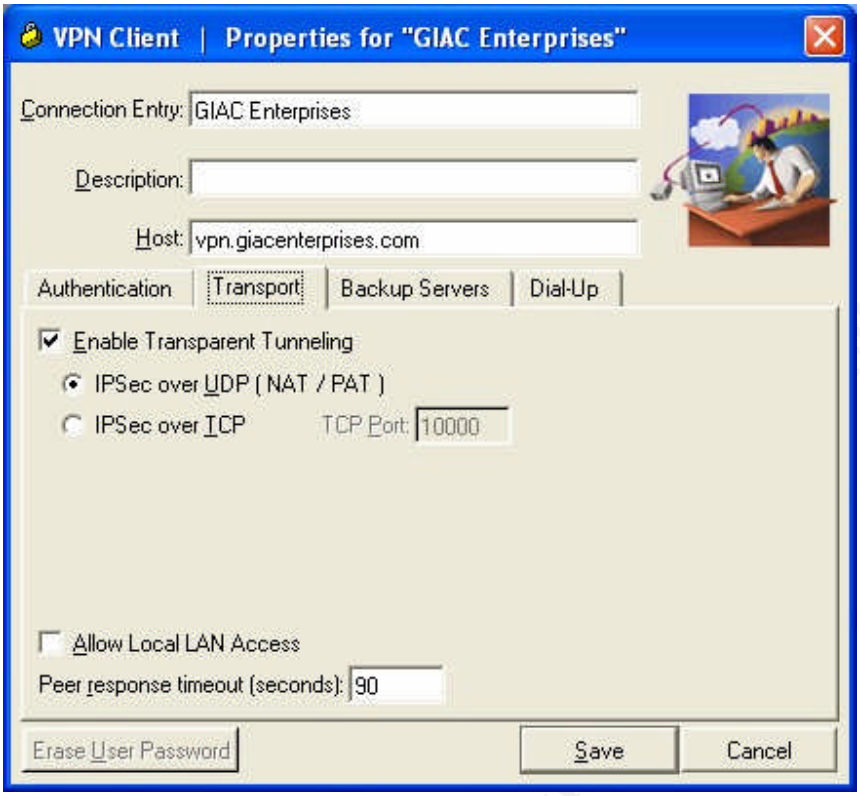
```
[main]
Description=GIAC VPN Connection
Host=vpn.giacenterprises.com
AuthType=1
GroupName=GIACEnterprises
GroupPwd=
enc_GroupPwd=0B947893054FE64192EB18CF5411A1DD5A2D8874686AF1A8
9452A06C0450F065B08AAAECDFF3983F4657766B6774EA9139C259EA0D73
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=1
BackupServer=
EnableMSLogon=1
MSLogonType=1
EnableNat=1
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
PeerTimeout=90
```

E1.1 GIAC Enterprises VPN Profile File GUI Configuration

The VPN Dialer is launched from the Programs menu.

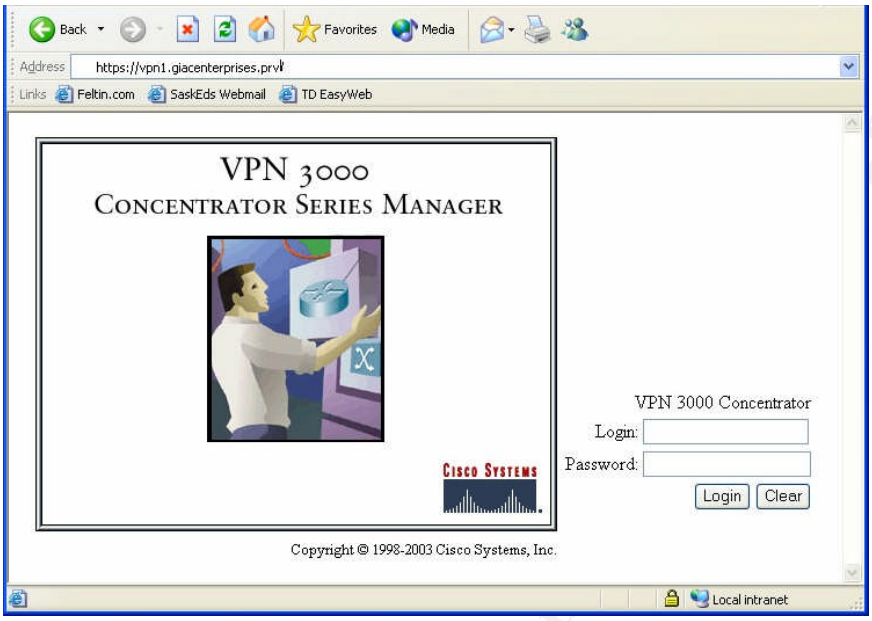






E2.0 Cisco VPN Concentrator IOS Configuration

The Cisco VPN Concentrator will be managed on its internal interface with the graphical user interface using the HTTPS protocol.



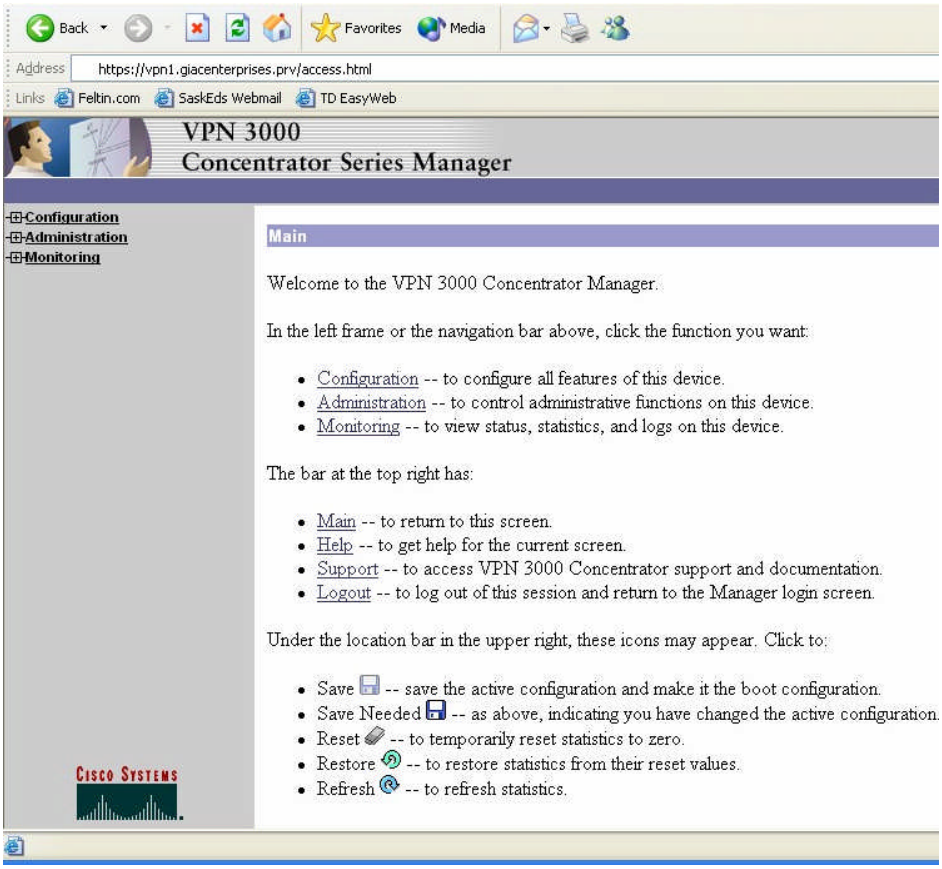


Table 9.0 Concentrator Interface Configurations

Configuration Items		
	Ethernet 1 (Private)	Ethernet 2 (Public)
IP Address	10.10.200.3	192.168.102.2
Subnet Mask	255.255.0.0	255.255.255.0
Public Interface	No	Yes
Filter	None	Public
Speed	10/100 Auto	10/100 Auto
Duplex	Auto	Auto
Inbound RIP	Disabled	Disabled
Outbound RIP	Disabled	Disabled
OSPF	Disabled	Disabled

Table 10.0 Server Configurations

Servers		
Authentication Servers	(Only SDI, delete internal authentication service)	
	Server Type	SDI
	Authentication Server	172.20.100.3
Accounting Servers		
	Accounting Server	172.20.100.3
	Server Secret	<password>
	Verify	<password>
DNS Servers		
	Enabled	Yes
	Domain	Domain Controller / DNS
	Primary DNS Server	172.20.100.7
	Secondary DNS Server	

The authentication and accounting server are both the RSA server located on the internal network. It provides the primary authentication with the use of the RSA SecureID tokens.

Table 11.0 Address Management

Address Management		
Assignment		
	Use Address Pools	Enabled
Pools		
	Range Start	172.20.240.1
	Range End	172.20.240.254

When VPN users authenticate, they are provided an IP address on the internal network by the concentrator via DHCP. The IP range is 172.20.240.1 – 172.20.240.254

Table 12.0 Tunneling Protocols

Tunneling Protocols		
	PPTP Enabled	FALSE
	L2TP Enabled	FALSE
	IPSec Enabled	TRUE
IKE Proposals		
	CiscoVPNClient-3DES-MD5	
	IKE-3DES-MD5	
	IKE-3DES-MD5-DH1	
	IKE-3DES-SHA-DSA	
	IKE-3DES-MD5-RSA-DH1	

Table 12 indicates that PPTP and L2TP are disabled and that IPSec will be used to create the VPN. The IKE proposals available are listed above, but the client and the concentrator will negotiate to use the CiscoVPNClient-3DES-MD5 with pre-shared secrets.

Table 13.0 Management Protocols

Management Protocols		
FTP	Enabled	FALSE
HTTP/HTTPS	HTTP Enabled	FALSE
	HTTPS Enabled	TRUE
TFTP	TFTP Enabled	FALSE
Telnet	Telnet Enabled	FALSE
	Telnet/SSL Enabled	FALSE
SNMP	SNMP Enabled	TRUE
	Port	161
	Max Queued Requests	4
SNMP Communities	SNMP String	"giacREAD"
SSL	Enryption Protocols	RC4-128/MD5
		3DES-168/SHA
		DES-56/SHA
		RC4-40/MD5 Export
		DES-40/SHA Export
	Client Authentication	Disabled
	SSL Version	Negotiate SSL V2/V3
	Gen Certificate Key Size	768-bit RSA Key
SSH	Enable SSH	TRUE
	SSH Port	22
	Max Sessions	4
	Key Regen Period	60
	Excryption Protocols	3DES-168
		RC4-128
		DES-56

Table 13.0 indicates that the only ways to manage the concentrator are through HTTP and SSH on the internal interface. SNMP is also enabled for monitoring purposes.

Table 14.0 Event Management

Events		
General	Save Log on Wrap	Not Checked
	Save Lof Format	Multiline
	FTP Saved Log on Wrap	Not Checked
	Email Source Address	vpn1.giacenterprises.prv
	Syslog format	Cisco IOS compatible
	Severity to Log	"1-3"
	Severity to Console	"1-3"
	Severity to Syslog	"1-3"
	Severity to Email	"1-3"
	Severity to Trap	"1-3"
FTP Backup	FTP Server	Blank
	FTP Directory	
	FTP Username	
	FTP Password	
	Verify	
Trap Destinations	Destination	172.20.100.8
	SNMP Version	SNMPv2
	Destination	172.20.100.8
	SNMP Version	SNMPV1
Syslog Servers	Syslog Server	172.20.100.8
SMTP Servers	SMTP Server	172.20.100.5
Email Recipients	Email Address	admin.giacenterprises.prv
	Max Severity	"1-3"

Table 14.0 shows how logging is configured and that alerts and traps are send to the internal logging server.

Table 15.0 User/Group Management

User Mangement		
Base Group - General	Access Hours	No Restriction
	Simultaneous Logins	3
	Min Password Length	8
	Allow Alphabet Only PW	Enabled
	Idle TimeOut	0
	Max Connect Time	0
	Filter	None
	Primary DNS	172.20.100.7
	Secondary DNS	
	Primary WINS	172.20.100.7
	Secondary WINS	
	SEP Card Assignmnet	SEP 1, 2, 3, 4
	Tunneling Protocals	Only IPSec
	Strip Realm	Disbaled
Base Group - IPSEC	IPSec SA	ESP-3DES-MD5
	IKE Peer Identity Validiatio	If supported by certificate
	IKE Keepalives	Enabled
	Reathorization on Rekey	Disabled
	Tunnel Type	Remote Access
	Group Lock	Disbaled
	Authentication	None
	IPComp	None
	Allow Password Storage	Disbaled
	Split Tunneling Network	None
	Default Domain Name	giacenterprises.prv
	IPSec through NAT	Enabled
	IPSEC NAT UDP Port	10000
Groups	Group Name	GIACEnterprises
	Password	
	Type	Internal
	Authentication	SDI
	Idle TimeOut	30
	Filters	None

Table 15.0 shows how the VPN groups are configured. The group used by remote users is GIACEnterprises. Notice that authentication is set to SDI and idle users are disconnected after 30 minutes. The GIACEnterprises group also inherits properties from the Base Group. One of the most important properties to note is that split tunneling is not allowed. This means once a user connects to GIAC Enterprises via VPN, they can no longer connect to their own private internal network. This prevents a third party from hijacking the laptop when connected via VPN, to try to gain access to corporate resources.

Table 16.0 Policy and Traffic Management

Policy Management		
Traffic Management		
Filters	Filter Name	Filter Rules Assigned to Filters
	Public (rules allowed)	IKE In from 192.168.102.1
	Private (default)	Any In
		Any Out
	External (deafult)	No Rules
NAT	NAT operation	Enabled

Table 16.0 lists the filter or ACL that is applied to each interface. Each filter is composed of filter rules. The only rule on the external or public interface is to allow in IKE from the G2 security appliance 2. This is because inbound traffic gets network address translated as it passes through the firewall. As a part of the internal network, the private interface allows all traffic for remote users to have unrestricted access once the tunnel is established.

REFERENCES

The SANS Institute. Track 2.1 TCP/IP for Firewalls. The SANS Institute, 2003.

The SANS Institute. Track 2.2 Packet Filters. The SANS Institute, 2002.

The SANS Institute. Track 2.3 Firewalls. The SANS Institute, 2003.

The SANS Institute. Track 2.4 Defense in Depth. The SANS Institute, 2003.

The SANS Institute. Track 2.5 VPNs. The SANS Institute, 2003.

The SANS Institute. Track 2.6 Network Design and Assessment. The SANS Institute, 2003.

The Apache Software Foundation, "Downloading the Apache HTTP Server Project." Retrieved 1 May 2004 < http://httpd.apache.org/download.cgi>.

"Stable Releases Suitable for Production Use." Squid version 2.5. Retrieved 1 May 2004 < http://www.squid-cache.org/Versions/v2/2.5/>.

"The SANS Security Policy Project." SANS Institute. Retrieved 28 Apr. 2004 < http://www.sans.org/resources/policies>.

Secure Computing Corporation. SideWinder G2 Administration Guide. Secure Computing Corporation, 2003

Microsoft Corporation. "Microsoft Windows 2000 TCP/IP Implementation Details." Retrieved 5 May 2004 <http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.mspx>.

Microsoft Corporation. "Internet Information Services." Retrieved 2 May 2004 <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/internet_information_services_start_page.asp>.

Long, Johnny. The Google Hacker's Guide. Version 1.0.

BlueCoat Systems. “Proxy Solutions to Control Web Communications.” Web Server Appliances. Retrieved 1 May 2004 < http://www.bluecoat.com/solutions/index.html>.

Websense. “The Growing Risks of Internet Abuse.” Websense Internet Filtering Products Stop Internet Abuse. Retrieved 4 May 2004 < http://www.websense.com/products/>.

Cisco Systems. “Cisco VPN 3030 Concentrator.” Cisco Systems. Retrieved 5 May < http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/ps2292/index.html>.

Cisco Systems. “Cisco 2600 Series Multiservice Platforms.” Cisco Systems. Retrieved 5 May 2004 < http://www.cisco.com/en/US/products/hw/routers/ps259/index.html>.

Cisco Systems. “Cisco IOS Software Release 12.3 Mainline.” Cisco Systems. Retrieved 10 Apr. 2004 <http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin09186a0080199900.html#wp42180>.

Cisco Systems. “Cisco Security Device Manager.” Cisco Systems. Retrieved 11 Apr. 2004 <http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a00801eb26f.html>.

Cisco.com. Retrieved 11 Apr 2004 <http://www.cisco.com>

RSASecurity.com. Retrieved 12 Apr 2004 <http://www.rsasecurity.com/>.

Spangler, Ryan. “Analysis of Remote Active Operating System Fingerprinting Tools.” Retrieved 15 Apr 2004 < http://www.net-security.org/dl/articles/osdetection.pdf>.

SecureComputing.com. Retrieved 1 May 2004 <http://www.securecomputing.com>.

Chuvakin, Anton. “Complete Snort-based IDS Architecture, Part One.” Security Focus Home Infocus. Updated 6 Nov. 2004. Retrieved 20 Apr. 2004 < http://www.securityfocus.com/infocus/1640>.

Chuvakin, Anton. “Complete Snort-based IDS Architecture, Part Two.” Security Focus Home Infocus. Updated 6 Nov. 2004. Retrieved 5 May 2004 < http://www.securityfocus.com/infocus/1643>.

Snort.org. Retrieved 12 Apr 2004 < http://www.snort.org/docs/>.

"Exploits and Tools." Digital Information Society. Retrieved 1 May 2004 < http://www.phreak.org/html/exploits.shtml>.

"How to Cover Your Tracks." Retrieved 2 May 2004 < http://www.thc.org/papers/COVER-1.TXT>.

ihackstuff.com. Retrieved 1 May 2004 <http://johnny.ihackstuff.com>.

"Microsoft Security Bulletin MS04-011." Microsoft.com. Retrieved 2 May 2004 <http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx>.

"Net User Options." Retrieved 3 May 2004 <http://www.ss64.com/nt/netuseroptions.html>.

"Placing Backdoors Through Firewalls." Retrieved 3 May 2004 <http://www.thc.org/papers/fw-backd.htm>.

Samspade.org. Retrieved 3 May 2004 <http://www.samspade.org/>.

Packetstormsecurity.org. Retrieved 3 May 2004 < http://www.packetstormsecurity.org/>.

Netcraft.com. Retrieved 3 May 2004 <http://uptime.netcraft.com>.

Insecure.org. Retrieved 3 May 2004 <http://www.insecure.org/nmap/index.html>.

Guffey, Mary Ellen, "MLA Style Electronic Formats." MLA Style Electronic Formats. Updated Aug. 2001. Retrieved 5 May 2004 < http://www.westwords.com/guffey/mla.html>.