Global Information Assurance Certification Paper

SANS GCFW PRACTICAL ASSIGNMENT
Version 1.7

GIAC Fortune Saying Enterprises
"*Let the wisdom of Confucius enlighten your mind*" ä

By James Giesecke
Oct 28th, 2002

Background:

GIAC Enterprises has a fortune cookie saying business, which is looking for ways to expand and reach more customers. For the first 100 years of its existence the company had been operating as a small business in San Francisco selling to local businesses and restaurants. In the past 10 years the company has been increasing the number of mobile sales force and teleworkers and building its list of suppliers and partners.

GIAC Enterprises also works closely with two fortune cookie sayings suppliers, Confucius Wisdom, Inc. and Paper Wisdom, Inc. One company provides sayings in Chinese and the other in English. GIAC Enterprises international partners, Tastytreats, a German conglomerate, and LeFortune, a French company, resell GIAC Enterprises fortune cookies saying products.

Since the market is becoming saturated and very competitive, the company has decided to take their business "on-line". They have asked JDG Incorporated to design a security architecture for their new online business so customers, suppliers, partners and both internal and external employees can safety and securely access the GIAC Enterprise network and web site. Also, since this company is new to network security, they have also asked that JDG Inc. provide them with a security policy and tutorial so they have a baseline to work with and can learn how to manage their network. As part of the design, JDG Inc. will also conduct a technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced.

Assignment 1 – Security Architecture

GIAC Enterprises is new to on-line e-commerce so they are quite concerned about their web services succeeding. They believe the core of their business sales will be produced from these web services so security is an important issue to be addressed, but as they also point out - "don't build a $1000 fence for a $100 horse".

Assumptions

- GIAC Enterprises stresses the need for security balanced with some budgetary constraints and of the network personnel's network security knowledge level. It's better to build a simple, secure network than one that is difficult to manage and could result in security problems due to complexity. They would also rather pay more for a solution that is sound than trying to cut costs and possibly have their network adversely affected later.
- GIAC Enterprises has registered address space 150.150.1.0/24.
- There are no specific requirements for internal users, but a basic secure infrastructure is specified for their external employees, suppliers, customers, and partners.
- VPN connections are low at the present time (less than 100 simultaneous connections) but are expected to grow in the future.
- There will be no dial-up connectivity to the network. All remote connections must go through the network VPN.
- FTP and remote commands are not allowed. If this type of service is required then the Secure Copy Protocol (SCP) will be used.
- No Web based email services such as Yahoo, Microsoft Hotmail, etc. will be allowed to be accessed from within the GIAC Network.

Guiding general principles of GIAC network:

Layered Network Defense

The network will have multiple layers of protection to increase the difficulty of breaking into the network and to reduce the exposure to hosts from the Internet. Security on external service, such as the web server, is our main focus but not to the point that other services or host(s) are open to compromise.

Various network components will be installed and procedures implemented in this network to provide the needed defenses. A list is provided below of the components and techniques along with any procedures used. A more in-depth explanation of how they will be used in the network can be found in the body of the report:

- Firewalls
- Intrusion Detection Systems (IDS)
- Virtual Private Networks VPN(s)
- Host Hardening
- Vulnerability Scanning
- Anti-virus Protection
- Data Storage and Backups

Silent Runner

This network isn't going to be hastily designed and installed. GIAC Enterprises is concerned about security so initially all ports will be closed and services will be opened as required after the pros and cons have been evaluated so no surprises due to security lapses occur.

Full Speed Ahead!

Once the network is deployed and services are open, the next requirement is to ensure ease of use for the customers. What good is tightening the security of the network if no one can access it? Customers should find the web site easy to access while the GIAC partners and suppliers who need a greater degree of access to the network must use SSHv2 to access the internal GIAC Network.

Test and Re-Test!

Once the network and the security measures are in place doesn't mean the work is done! Testing the security of the network goes on daily on the perimeter and critical devices. And don't just trust the results! An independent audit must be done on the network periodically. This unbiased report will help validate the network security policy and possibly find errors that hadn't surfaced.

Network Access and Restrictions

There are four groups of users that need different access and restrictions applied to them for this network: GIAC employees which can be sub-divided into internal and external groups, Customers that need access only to our web site, Suppliers who need to send new sayings and store them on our servers, and Partners who will download sayings for translation and resale.

GIAC Employees

Remote Employees

Sales Force and Teleworkers

The GIAC mobile sales force and teleworkers will employ laptops running Windows 2000 professional with Norton's Internet Security host-based personal firewall software. Given the inexperience the GIAC employees have with network security, Norton's software provides the fire-up and forget features they need versus BlackICE defender, which is for aligned for technical users wanting to dig into the details of the packets. Other software that needs to be loaded from a security standpoint includes Norton AntiVirus Professional Edition 2003 software for virus protection. The VPN software used will support IPSec to provide confidentiality, authentication, integrity, access control, and some protection from traffic flow analysis. The GIAC network VPN must support Encapsulating Security Payload (ESP) and validate users with SecureID. Also, users will require access to UDP port 500.

The Windows 2000 Pro laptops will be configured to use TCP port 80 (HTTP), TCP port 443 (SSL), port 25 (SMTP), IMAP or POP for email retrieval.

In addition, a limited number of Information Systems (IS) staff will need remote access via VPN to the servers and equipment from home for administration and troubleshooting. For them BlackICE defender, which is for aligned for technical users wanting to dig into the details of the packets will be installed since Norton's Internet Security host-based personal firewall software is probably to tame for them.

Internal Employees

The employees are located on the internal company users network. They connect to the external server located in the service network via SSH to process new fortunes from the suppliers. After reviewing the new deliveries, the internal servers are updated and copies are loaded on the external servers so the partners can download the new fortunes and customers can make purchases. For internal networking the employees need to perform their Windows 2000 logins, file sharing and resource browsing and will require authentication from a Domain Controller. The following services and ports will be required:

- SSH (TCP port 22)
- DNS (port 53)
- HTTP (TCP port 80)

Like the external users, each user will have Norton's Internet Security host-based personal firewall software along with Norton AntiVirus Professional Edition 2003 software.

A subset of the internal users is the IT employees that maintain the GIAC network. This department will require TCP port 22 (SSH) and UDP 514 for management of the servers and Firewalls.

Customers

As important as security is to GIAC Enterprises, it business relies on selling its fortunes using its website, so the website must be accessible. To achieve this goal the following is required:

- Use Secure Sockets Layer (SSL) for transactions. This will require opening TCP port 443.
- Use HTTP reverse cache proxy. All requests to port 80 are redirected to TCP port 8000 or 8080.
- Provide an external DNS server (UDP port 53) for name resolution.
- Install an Oracle database server on the Services network
- All customer personal and credit card information must be protected. Therefore, this information will be located on the Internal network.

Suppliers

Confucius Wisdom, Inc. and Paper Wisdom, Inc send in their sayings to the GIAC external server via SSH (TCP port 22). They will upload their submissions via Secure Copy Protocol (SCP) and receive an email receipt to track whether the submissions were accepted or rejected and also to track Electronic Funds Transfers (EFT) to their accounts. They will provide us with their registered IP address space so we can allow them access to server.

Partners

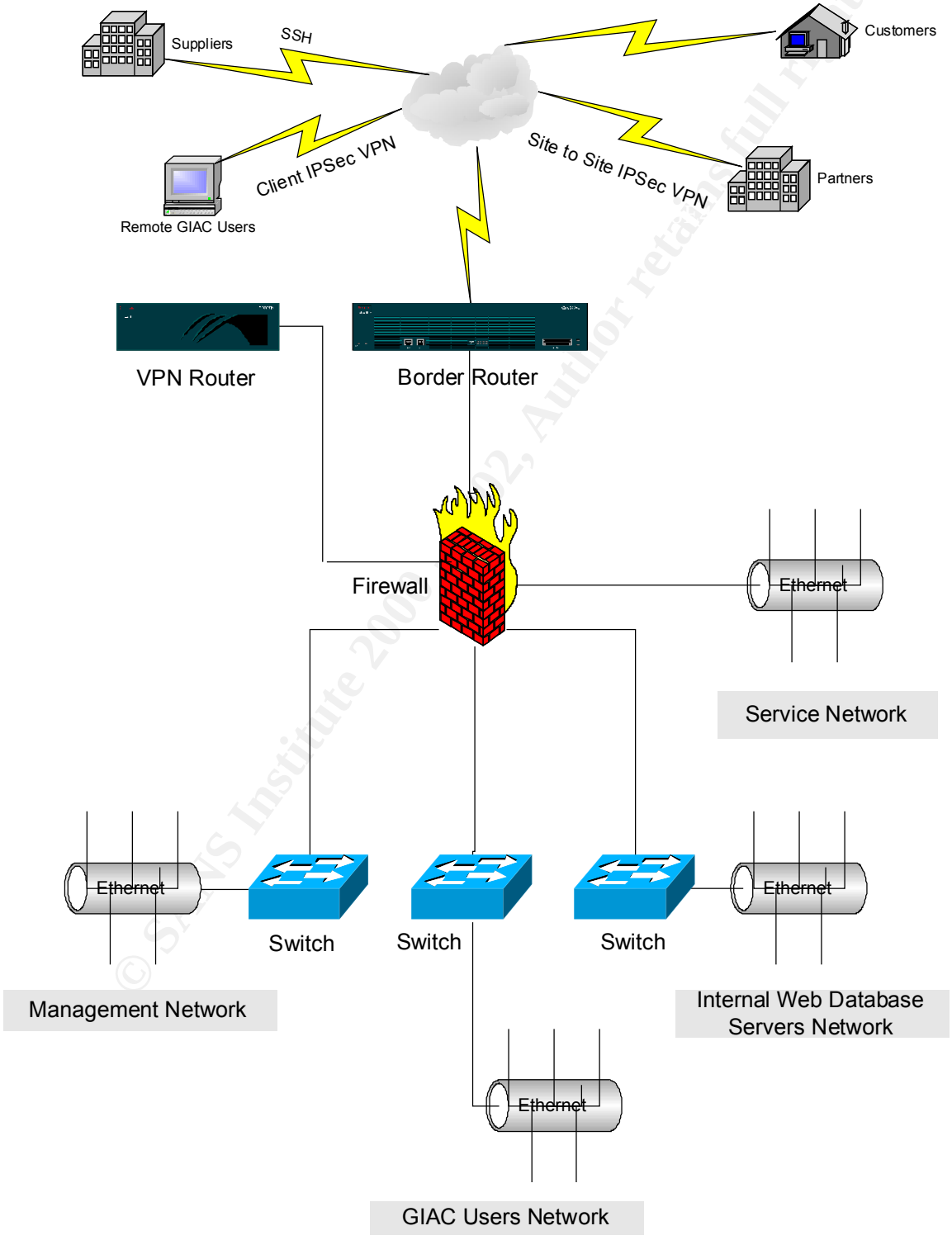
GIAC Enterprises international partners, Tastytreats, a German conglomerate, and LeFortune, a French company, resell GIAC Enterprises fortune cookies saying products by accessing the

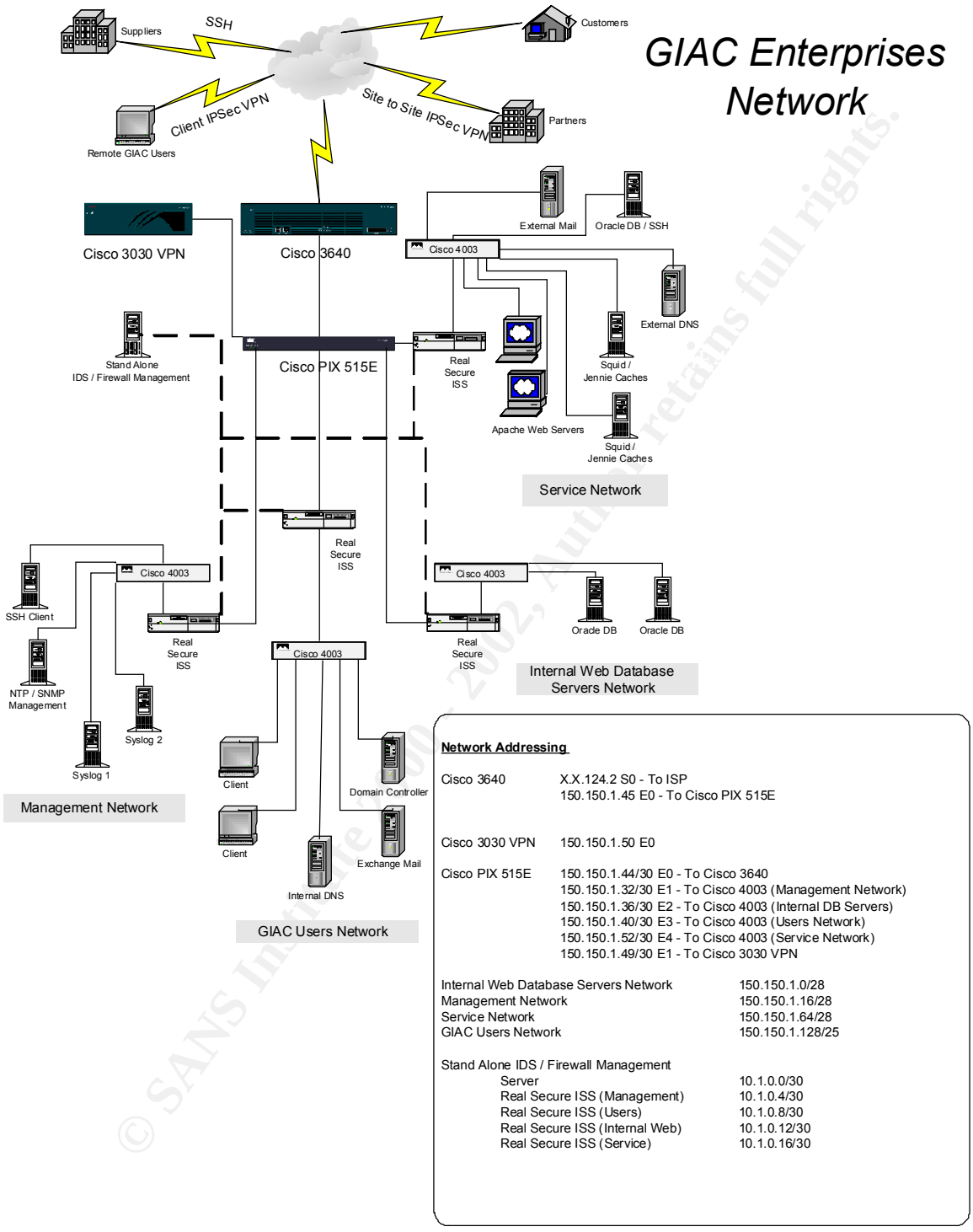
server repository using SSH. They will download and translate the sayings before processing them through their various channels. Like our partners, to tighten-up our security, we will allow only IP addresses provided by our partners through the firewall.

The partners retrieve the sayings using Oracle SQL Net client, TCP port 1521.

The GIAC Network

GIAC Logical and Physical Network Architecture





IP Network Addressing

GIAC Enterprises has been assigned 150.150.1.0/24 by IANA, which is enough address space for the current network. Their ISP is a large national ISP which provides them with 1-800 number to dial into to access

the companies VPN router from anywhere in the world. They also supply the IP address for the Border Router Internet interface (X.X.124.2).

Defense in Depth

The concept of "Defense In-Depth"[1] has been incorporated into the GIAC security architecture. The goal of this concept is to create multiple layers of protection so as to avoid relying on a single firewall against a security lapse occurring.

These layers are built by using routers, IDS with centralized logging and alerting, log analysis, and active scanning of clients. It's important to go through the various security components that make up the GIAC security architecture and explain the role of each component.

Network Border Router

All good network security architecture starts with a border router. For the GIAC network a Cisco 3640 running IOS 12.2 will be employed. This router was chosen to meet the following requirements:

- **Security**. Among the security features required are IOS Firewall Features, DES, and 3DES data encryption, extended access lists, violation logging.

- **Performance**. The router must be able to support WAN interfaces up to T-3 and security features without dropping packets.

- **Availability**. Though not part of the present solution to keep cost down, a second redundant router can be used to ensure minimum downtime by using Hot Swappable Routing Protocol (HSRP). This Cisco protocol provides automatic router backup when the primary router fails. Along with a backup router, there would be connections to two ISPs limiting connectivity failures. Also, having a redundant power supply along with Uninterrupted Power Supply (UPS) support is required.

- **Scalability**. The router selected must support the expected growth that GIAC Enterprises predicts for its network. Cutting corners here cause a bottleneck in the network, to packets being dropped and possibly leading to Denial of Service (DoS) attacks.

[1] **The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.3.1, Bethesda, MD: SANS Press, p. 2 (2002)**

- **Management**. The router must be manageable using HTTPS, SSH, and console port.

The Cisco 3640 is an excellent choice for our medium-range router requirements. Even though it does support an OC-3 interface, given the added burdens from security features that will be implemented, it best not to overly tax the routers CPU.

The router's security function will be to filter out large amounts of unwanted inbound traffic using an standard and extended Access Control Lists (ACL) as well as traffic leaving the GIAC network. Ingress filtering is used to deny spoofed IP packets sourced from unused and private IP ranges, inbound packets using an IP address of the internal network, unneeded service ports, or ports used for known attacks. Egress filtering is used to prevent unwanted traffic (web based email as an example) from leaving our network. The CBAC (Content Based Access Control) feature set is available if needed but it consumes significant amount of CPU cycles so it must be determined that the router can handle normal traffic and ACL's before this feature is enabled. It would allow a stateful inspection of the packets traversing the router. Source routed packets won't be allowed to enter the network and IP unreachable and ICMP time exceeded messages to external hosts will also be prevented. The purpose of the router's ACL filtering is to filter out the "absolutes"[2] – Traffic that obviously has no reason to enter the network. Any traffic that does pass the ACLs will be subject to a more thorough evaluation by the Cisco PIX, which will perform stateful packet filtering and finally employ proxies to filter out any remaining malicious packets.

VPN / Firewall Router

VPN Router

The Cisco 3030 VPN running Concentrator release 3.5.2 was picked as the VPN device. It meets the expected current user needs of less than 100 simultaneous connections and can be upgrade to support up to 1500 connections if necessary. This VPN router was chosen to meet the following present and future requirements:

- **Security**. Support RADIUS, NT Domain Authentication, Digital Certificates, IPSec and RSA SecurID. Also allow for integration of external authentication systems and be interoperable with third-party products

[2] The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.3.1, Bethesda, MD: SANS Press, p. 7 (2002)

- **Performance**. Meet the current and predicted VPN connection requirements, and support hardware-based encryption. It must also support bandwidth requirements from a full T1 to a fractional T3.

- **Availability**. Fail-over and monitoring capabilities.

- **Scalability**. The ability to upgrade the VPN router to meet future requirements.

- **Management**. Capable of being managed by HTTPS, as well as by SSH, and via a console port.

The Cisco 3030 VPN is a platform for a medium- to large-sized company and is field-upgradeable to the 3060 if required. The 3030 is a VPN platform designed for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through fractional T3 (50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. It should be noted that the Cisco VPN client provides support for Windows 95, 98, ME, NT 4.0, and 2000 only.[3]

Firewall

The Cisco PIX 515E using v6.2 was selected because it is a hardware-based firewall removing chances of attacks against an underlying operating system which it doesn't have since the operating system is only in firmware. These are the reasons for selecting this firewall:

- **Security**. Proprietary, hardened system that eliminates security holes typically found in general-purpose software-based operating systems

- **Performance**. Throughput of more than 50 Mbps and at least 1,500 IPSec tunnels.

- **Availability**. Support for a redundant hot standby unit, which will maintain concurrent connections through automatic stateful synchronization.

- **Scalability**. Support for no less four interface so allow for present and future requirements.

[3] **Cisco Corp., "Cisco VPN 3000 Concentrator Series" 4 September 2002 URL:http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm (6 Sep 2002)**

- **Management**. Need a wide variety of methods to remotely configure, monitoring, managing and troubleshooting PIX firewalls using a convenient command-line interface (CLI) through a variety of methods including Secure Shell (SSH) and an out-of-band console port.

The Cisco PIX 515E is a small- to medium business and enterprise device that meets the specified requirements. The unrestricted license (PIX 515E-UR) is purchased to provide a hot-standby (if a second PIX is purchased later), support for additional interfaces (PIX-4FE card) and increased VPN throughput.

Intrusion Detection Servers (IDS)

RealSecure Network Sensor v7.0 Workgroup Manager

There will be a RealSecure network engine monitoring each of the sub-networks or areas in the GIAC network. Each sensor will have two interfaces with one connected to the network set in promiscuous mode with no IP address bound to the interface to analysis the data entering and leaving the area. The second is on a private "10" network separate from GIAC network connecting to a stand alone IDS / Firewall Management station. To accomplish this a SSL session is established to communicate between the manager and the sensor using TCP ports 901 902, 903 & 2998. Version 7.0 of RealSecure Network Sensor integrates BlackICE technology into the analysis portion of the agent and supports full-duplex connections.

Listed below is the full-blown protection system that can be implemented on the GIAC network. For this network and the level of security required, the full rollout might not be needed but these options can be provided to the customer to determine where the threshold between security and cost lie.

Agents

They are a class of modules that provide automated detection and response to threats.

Server Sensor

Monitors both inbound and outbound network traffic directed at a single host as well as the operating system log entries and key system files for indications of intrusion or unauthorized activity. One useful reason to

purchase the Server Sensor component is it ability to monitor SSL traffic for signs of malicious traffic. The Squid Proxy Server mentioned later can only provide pass-through support. So Server Sensor would compliment Squid.

OS Sensor

Monitors operating system log entries and key system files for indications of unauthorized activity and responds automatically.

Workgroup Manager

The RealSecure located on the Management station provides for configuration of the agents as well as detailed management and storage of the threat data generated by the agents. All management of RealSecure agents is accomplished across secure communications channels. Workgroup Manager modules include:

- A Console that allows centralized control of remote sensors and provides for centralized display of alerts and reporting.
- Event Collectors, which collect data from any sensors in real-time and send it to the Enterprise Database and Console.
- An Enterprise Database that stores the sensors' event data.
- An Asset Database that contains information about assets including Event collectors and sensors.[4]

Workgroup Layer 3 Switches

The various GIAC networks are connected to the Cisco PIX Firewall via Cisco 4003 Catalyst switches (IOS V7.3). This switch was selected because it provides added security to the network through port security, VLANs, Secure Shell, ACLs (Layers 2-4) and supports SNMPv3. Layer 3 static routing and VLANs will be configured on the switches using 10/100Mb ports. Autonegotiation is not needed since these are permanent links and so will be disabled. All ports will use the available port based security that only accepts connection from one MAC address. All unused ports will be shut down.

[4] **Internet Security Systems. "RealSecure Protection System FAQ" 21 May 2002 URL:http://documents.iss.net/literature/RealSecure/RS_FAQ.pdf (4 Sep 2002)**

Service Network

The Service Network is connected to one of the Cisco PIX firewall Fast Ethernet Interfaces. This network includes servers that are publicly accessible to the Internet. The servers provide a variety of services including External SMTP Mail, SSH Database services for partners file retrieval and file depository for suppliers, and External DNS. These servers need to be hardened to ensure that only the minimum required services are enabled. We will use Security-Enhanced Linux from NSA (v2.4) on Red Hat 7.1 since it not only secure, reliable and easier to configure for our requirements than Windows, but has been tested by NSA who have combed extensively through the Linux kernel to ensure it is secure.

Squid/Jeanne Web Caching

Two clustered servers will provide proxy caching. Again, the NSA approved kernel of Red Hat will be used. These servers will be administrated by the IS department using SSH and will handle proxy inbound requests to the GIAC. They will also be run in a cluster formation so to increase the GIAC response time and act as a redundant backup to each other in the event one of them has a failure and goes down. They can also provide filtering and access control by preventing attempts from outside users to write to the web server using certain HTTP commands such as GET, and POST. Squid can proxy SSL but can't do access control checking since SSL is encrypted. One of the most important features of Squid is that it isolates the client from the server thus preventing direct communication between the two. This feature results in protecting against certain HTTP based attacks.[5]

Squid will be configured in the squid.conf file to listen on TCP port 80 versus the default port of 3128 and proxy hierarchy will be turned off. As explained later, Squid's http-accelerator mode will be turned on. Also, the GIAC local network is defined as the only IP addresses with access granted to the proxy. This will prevent Internet users from launching HTTP based attacks anonymously against remote hosts.

There are various add-ons that can be used with Squid. The selection for the GIAC network is to use "Jeanne" developed by Vincent Berk. Jeanne allows for content filtering when integrated with Squid's http-accelerator mode. It acts as a redirector to control which files and directories can be accessed on the Web server. The benefit of this is the increased security it provides against such exploits as oversized URLs to access long

[5] The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.2.4, Bethesda, MD: SANS Press, p. 142 (2002)

forgotten administration scripts. Jeanne works with Squid to prevent URLs requests that aren't explicitly defined as being accessible from being forwarded to the Web server.[6]

Web Servers

The GIAC network will employ two Apache web servers using the aforementioned Red Hat v7.1 in the cluster setup. A VeriSign certificate will be installed on it to ensure authenticity of the server. Squid will service the HTTP and HTTPS requests coming from the Internet. These servers will be administrated by the IS department using SSH. Logging are forwarded to the Syslog server in the Management network. No outbound traffic can be initiated from these servers and the procedures securing the Apache servers follow:

- Use the "chown" command for these tasks:
  - All web server files are owned and can be changed only by the root.
  - All scripts and binaries have permissions of 755 (read and executed by anybody and can also be changed by the owner of the file.) while text and graphics have 644 (file can be read. For most HTML files (744 is also fine, but redundant, for this)).
    $ chmod 755 *.css
    $ chmod 744 *.html

- The httpd process is run as user nobody.

- Audit CGI scripts for bound checking and scrubbing of the data.

- Go to the httpd.conf file and limit directory access by the Web server.

- Limit the amount of information supplied by the server to any hackers through a Telnets to port 80 by inserting "ServerTokens Prod" to the httpd.conf file

As an added measure of protection the web server, "security through obscurity" is employed. By configuring the web server to respond to queries for the version of OS running on the box, it will provide a misleading string. This won't stop a determined attack but will work

[6] **The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.2.4, Bethesda, MD: SANS Press, p. 148 (2002)**

against people who run scripts looking for specific versions of OS and bypassing all others.

The Apache server was selected over Microsoft's Internet Information Services 5 (IIS5) on a Windows 2000 due to its higher reliability, better security than the IIS5 implementation, and better performance. An added bonus is the cost. It's free!

External DNS server

The GIAC network will have two split DNS systems running BIND v8.3.3 using the Security-Enhanced Linux from NSA (v2.4) on Red Hat 7.1. This might not be the latest version but it is a mature version. This server will provide non-recursive name resolution services from all external queries for giac.com, and recursive services for hosts on the DMZ and VPN device.

The software won't run in root mode, but in some configured user account, so if the server was broken into the account is compromised and not the root account. The information contained in the external DNS server will include the publicly accessible servers in the service network, but no information about the internal GIAC network. Zone transfers from the internal DNS will be forbidden as well as from the external DNS server to the ISP's DNS servers just encase they become compromised. Logging will be forwarded to the Syslog server located in the Management network.

Database / SSH Server

An Oracle9*i* database server will run on the GIAC Service Network on Red Hat 7.1. The suppliers will access the server by using SSH running on the server while the partners connect to the GIAC network via a VPN to download fortune sayings from the server. By using SSH suppliers can connect via SSH and upload the fortunes sayings while internal GIAC employees will use SSH to process supplier's sayings and to also post new sayings to the database server.

To increase security there won't be any direct access from the external server to the internal one. Instead, the internal employees will move data from the internal to external server. This is to isolate the outside users from requiring access to the internal database server.

External Mail Server

The mail server will run Postfix from http://www.postfix.org/ using Postfix Version 1.1 Patchlevel 11. "Postfix attempts to be fast, easy to administer,

and secure, while at the same time being sendmail compatible enough to not upset existing users. Thus, the outside has a sendmail-ish flavor, but the inside is completely different".[7] Its purpose is to relay all inbound mail to the internal mail server and sending outbound mail from it to the appropriate addresses. The IS department will check the sendmail web site periodically to ensure the latest version / patch is installed.

Internal Web Database Servers Network

The internal Web database servers will use the same platform as the external database server. The only difference between the two is the internal network will have a primary and secondary/backup server. A RAID device is connected between the two internal servers along with a tape backup device and steps are taken following industry specified procedures to ensure the safe storage and recovering of the data.

[7] **Wietse Zweitze Venema, The Postfix Home Page, URL: http://www.postfix.org/start.html (18 Sep 2002)**

GIAC Users Network

Clients

GIAC users will use Windows 2000 PCs and login through the Windows domain controller. All PCs will have Norton's software that provides the fire-up and forget features they need versus BlackICE defender, which is for aligned for technical users wanting to dig into the details of the packets. Other software that needs to be loaded from a security standpoint includes Norton AntiVirus Professional Edition 2003 software for virus protection and propagation.

The PCs are updated with the latest patches and software versions by using an automated program that examines the users PC and performs the needed updates. Most users will not have administrative control of the computer and strong password settings will be enforced.

On a periodical basis employees will access the external Oracle server to retrieve the new fortune sayings provided by the suppliers using SSH. They will move the sayings onto the internal Oracle server for review and processing the sayings. Once this is completed, the sayings are uploaded via SSH to the Web servers.

Internal DNS

The DNS in the Users Network will not be externally accessible and will be configured to provide recursion for internal clients. This Windows Dynamic DNS server will forward lookups to the external DNS when it isn't authoritative and won't allow zone transfers.

Exchange Mail

Microsoft Exchange 2000 is the choice for the internal mail system due to its expected tight integration with Windows 2000 and Outlook. Users will use Outlook to connect to the Exchange server for sending and receiving emails. Patches will be installed with the latest service pack and hot fixes as required. Emails to the Internet are passed to the McAfee Active VirusScan Suite loaded on the Exchange server, which includes NetShield to scan files on the email servers.

Domain Controller

The Domain Controller will run Windows 2000 Active Directory supporting Windows 2000 Print, File and DHCP server.

Management Network

SSH Client

The SSH server will run on the hardened Red Hat mentioned before to support the various SSH-enabled servers and devices on the GIAC network.

NTP / Network Management

The synchronization of the system clocks is critical for precise time stamping of the log files. When these logs are reviewed on the Syslog server, having accurate time stamps helps with correlating events[8] across all devices and servers.

The NTP server will run version 4.1.1a of XNTPD available from www.eecis.udel.edu/~ntp. There will be two NTP servers using hardened Windows platforms synchronizing their time from two stratum 2 servers (216.27.190.202 and 207.126.97.57) that are less than 100 ms away from the GIAC network.

The GIAC Network will run HP Openview, Cisco Works and Cisco Security Policy Manager. Openview will provide alerts of devices and network trouble while Cisco Works support the administration of the Cisco devices. Cisco Security Policy Manager allows for the management of Cisco Secure PIX Firewalls and IOS Routers and to create and manage IPSec tunnels.

All Cisco devices will have their configuration files and IOS images tftped to the SNMP management platform for assisting recoveries and comparing configuration changes.

SiteScope Management software from Freshwater software will provide support to monitor URLs, DNS Monitor, Mail Monitor, Service Availability, Apache web server, Cisco Works, Oracle databases, and much more.[9]

Syslog Server

A very important piece of the GIAC Security architecture is the Syslog server. All devices will send its logs to the server for review and it is this

---

[8] The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.3.6, Bethesda, MD: SANS Press, p. 237 (2002)

[9] Freshwater Software, Inc., "SiteScope Monitor Types" 3 Sep 2002 URL:http://www.sitescope.com/MonitorTypes.htm (3 Sep 2002)

critical information that tells us about the network and whether attacks have occurred or are occurring on the network. Attackers will attempt to break into these servers to erase or cover-up their actions. The consolidating of the logs allows us to find trends occurring across multiple devices, which not have been missed if the logs had to be read separately.

There will be two servers running hardened Red Hat using the Syslog service on UDP port 514. They will run the latest version of Syslog-ng (syslog-ng 1.5.14), which is a syslogd replacement, but with new functionality. The original syslogd allows messages only to be sorted based on priority/facility pairs; syslog-ng adds the possibility to filter based on message contents using regular expressions. The new configuration scheme is intuitive and powerful. Forwarding logs over TCP and remembering all forwarding hops makes it ideal for firewalled environments.[10]

[10] **IT Security Solutions, "Syslog-ng" URL: http://www.balabit.hu/en/downloads/syslog-ng (5 Sep 2002)**

Assignment 2 – Security Policy and Tutorial

Introduction

The security policies define the operational strategy that a company will follow to implement their strategic network security architecture. Having the best components available won't be of much use if lapses in security implementation occur! The devices in the security design must be evaluated and used as a team and not thought of as a separate, discrete piece of the security solution.

The first component of the GIAC security architecture is the Cisco 3640 boarder router which will handle the more basic filtering while the Cisco PIX 515E will provide the bulk of the filtering. Finally, we define the security policy of the Cisco 3030 VPN device that is positioned behind the border route.

Cisco 3640 Border Router

The Cisco 3640 router will run 12.2 of the Cisco IOS. The router will off-line during the initial configuration since putting it on the GIAC network without the proper access control would make the network vulnerable to attacks. All access control information will be document and reviewed before configuring the router. Also, the configuration information is written in a simple text editor first and then after validating the ACL's is loaded onto the router via TFTP on a laptop connected to the console port. Once the process is done the startup configuration is saved to the TFTP server.

General Recommendations

The following is the NSA/SNAC Router Security Configuration general principles for maintaining good router security:[11]

1. Create and maintain a router security policy. The policy should identify who is allowed to log in to the router, who is allowed to configure and update it, and should outline the logging and management practices for it. [Section 3.4]

2. Comment and organize the offline edition of router configuration file! This sounds fluffy despite being a big security win. Also, keep the off-line copy of all router configurations in sync with the actual

[11] **National Security Agency, "Router Security Configuration Guide" 9 July 2002 URL: http://nsa1.www.conxion.com/cisco/download.htm#Zipped%20Archive (11 Sep 2002)**

configuration running on the routers. This is invaluable for diagnosing suspected attacks and recovering from them. [Section 4.1]

3. Implement access list filters by permitting only those protocols and services that the network users really need, and denying everything else. [Section 3.2, 4.3]

4. Run the latest available General Deployment (GD) IOS version. [Sections 4.5.5, 8.3]

5. Test the security of your routers regularly, especially after any major configuration changes. [Section 6]

General Configuration

- Commands begin with "Giac01(config)#" once the hostname is set

- To set the hostname using the hostname command (in privileged mode (config)#) which won't have a password yet)

  hostname Giac01

- Set the privileged configuration mode password.

  enable secret 0 <password>

  Enable secrets are hashed using the MD5 algorithm. As far as anyone at Cisco knows, it is impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks).[12]

- Next encrypt the password stored in the config file since it normally stored as plain text.

  service password encryption

[12] **Cisco Corp., "Cisco IOS Password Encryption Facts" 13 Feb 2002 URL: http://www.cisco.com/warp/public/701/64.html (9 Sep 2002)**

Locking Down Access to Router

- Assign passwords to the console port and session timeouts.

  line console 0
  exec-timeout <time>
  login
  password <console password>
  transport input telnet

- Block telnet access to the router from the Management Network. Setting an ACL locks down access.

  line vty 0 4 ! Applied to telnet vty's 0, 1, 2, 3, 4
  exec-timeout 5 0
  access-class 1 in
  login
  transport input telnet
  access-list 1 deny ip any any log
  ip access-group 1 in

- Block all access to the aux port on the router.

  line aux 0
  no exec
  transport input none
  access-class 2 in
  transport input all
  access-list 2 deny 0.0.0.0 255.255.255.255 log
  ip access-group 2

Logging & Debugging

- Configure the system to timestamp logging and debugging.

  service timestamps debug datetime msec localtime show-timezone

  service timestamps log datetime msec localtime show-timezone

- Send the logs to the Syslog servers

  logging on

logging buffered
logging 150.150.1.20
logging 150.150.1.21
logging trap emergencies
logging trap debugging
logging trap alerts

- Use the NTP server to synchronize the router's clock

  ntp server 150.150.1.26

Shutdown Unneeded Servers on the Router

There are a number of servers that are clearly unneeded. Use the command "show proc" to see the various facilities and services. Servers listed below should practically always be disabled:

- Disable Echo, Discard, Daytime and Chargen which run on port numbers lower than 20. They should be disabled by default, but this will ensure these services are turned off. IP finger will also be removed since the finger daemon provides a list of users logged in to a host and can lead to planning attacks when users aren't on the router. Also, do not allow name resolution.

  no service tcp-small-servers
  no service udp-small servers
  no service finger
  no ip domain –lookup
  no ip http server
  no snmp-server

- Bootp won't be run on this router, so it will be disabled.

  no ip bootp server

- Cisco routers auto-load their startup configurations from local the network. This isn't a secure method, so it will be disabled.

  no boot network
  no service config

- We don't want anyone specifying the path a packet takes since an attacker can use this to spoof a valid IP address of a host, so it's disabled.

no ip source-route

- Cisco Discovery Protocol (CDP). There isn't a need for this router to discovery other Cisco switches or routers (we are using static routing information), it will be disabled.

  no cdp run

- To block services that might be used to gain information about the network and prevent the router from sending unknown subnets of directly connected networks from using the default route.

  no ip classless

Setup Static Routing

- We will use static addressing on the GIAC network and setup the default route. Note that proxy ARP is disabled by the router when the default gateway command is used. The network is rather simple in design so we'll use RIP as the routing protocol. If problems occur later, then another routing protocol like OSFP could be employed.

  router rip
  no ospf
  ! IP Address for GIAC Network
  ip address 150.150.1.0 255.255.255.0
  ! set default gateway
  ip default-gateway S0

Other / Miscellaneous

- Add a banner to inform anyone who accesses this router that access is restricted. This is also important if litigation is required. This banner would also be applied to the vty and aux ports.

  banner %
  This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
  In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

%

Interface Specific Configuration

The interfaces on the router must now be configured to secure the router. Any interfaces, which are not going to be used, will be put in administrative shutdown.

Each interface is configured separately by first selecting the interface: **(config)# interface "interface"**

- Disable the transmission of directed broadcasts passing through the interfaces. This will prevent Smurf attacks by stopping broadcast traffic.

  no ip directed-broadcast

- We want to prevent the router from sending back ICMP error messages that could be used to map the GIAC Network.

  no ip unreachables

- Block the router from sending redirect packets back out to the Internet.

  no ip redirects

- To prevent ad-hoc routing.

  no ip proxy-arp

- All unused interfaces will be s ecured.

  Shutdown

Access Lists

The next step in securing the GIAC network requires the implementation of access lists. Without any access lists, a router forwards all traffic, but once a list is added to an interface, packets not matching any of the rules is dropped by the implicit deny at the end of the access list. It is important to note that the placement of the various rules in the access list can affect the router performance. Since the router must find a rule that the packet matches before it will forward the packet, if it must go through many rules before it finds a match then performance will suffer. It's usually best to put rules that are matched the most often or most specific at the top or beginning of the access list.

Cisco allows for two different types of IP access lists, Standard and Extended. The standard lists are numbered from 1-99 and only filter packets based on source address. A more robust list is the extended list that along with filtering on source address also filters by destination address, protocol, the TCP or UDP port and the ICMP type. The SYN or ACL TCP flags in the packet can also be examined. As of Cisco IOS 11.2, standard and extended access lists can be referred to by a name versus a number. Another type of access list is the Reflexive access list, which is referred to by name only, and they are able to maintain a state table but has the highest CPU and memory requirements of the three.

Below is the format for the Extended Access List:

access-list access-list-number [**dynamic** dynamic-name [**timeout** minutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name][13]

When comparing performance and features of the three access list types, they are, not surprisingly, inverse to each other. The Standard list can only filter "absolutes" while Reflexive list are the slowest but the most comprehensive because state table must be maintained and reviewed for every packet. And in the middle is the Extended list that is a mix between features and performance. It is important to pick the right access list since only one list can be applied to an interface per direction (that being outbound and inbound).

The GIAC Network will use Extended Named Access Lists since Standard lists don't provide enough security while we don't need another device (the Cisco PIX being the other one) performing stateful packet filtering.

Inbound vs. Outbound Filters

Filters can be applied to packets as they enter or exit an interface. Inbound packets are from the Internet to the GIAC network while outbound packets flow through the router towards the Internet. An advantage of applying the filters to packets inbound is it prevents using up memory while transferring packets through the router to just reject them on the outbound (i.e. internal) interface.

Internet, Serial 0 Interface Access List

[13] **Cisco Corp., "Configuring Commonly Used IP ACLs" URL: http://cco-rtp-1.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml (2002)**

The first access that will be applied to the router is Serial 0, which connects to the ISP.

Logging of all rejected packets will be enabled so a review of possible user intent can be done later. Logging can always be turned off if we decide that the data does not provide not enough useful information given the amount of work required to analyze the data.

- To go into ACL configuration mode.

  (config)# ip access-list extended Border_in

- Deny all traffic of addresses from reserved private, internal addresses (RFC 1918).

  deny ip 10.0.0.0 255.255.255.255 any log
  deny ip 172.16.0.0 0.15.255.255 any log
  deny ip 192.168.0.0 0.0.255.255 any log

- Deny all traffic of addresses from the loopback address (1), all broadcast addresses (2), SMURF attacks using the broadcast and subnet address of the GIAC network (3), all multicast addresses (4), Class E reserved IP address space (5), originating traffic with GIAC internal (should be coming from the internal interface) (6), traffic without an IP address (7), and reserved addresses (8).

  deny ip 127.0.0.0 0.255.255.255 any log ! (1)
  deny ip 255.0.0.0 0.255.255.255 any log ! (2)
  deny ip any host 150.150.1.255 log ! (3)
  deny ip any host 150.150.1.0 log ! (3)
  deny ip 224.0.0.0 7.255.255.255 any log ! (4)
  deny ip 240.0.0.0 15.255.255.255 any log ! (5)
  deny ip 150.150.1.0 0.0.0.255 any log ! (6)
  deny ip host 0.0.0.0 any log ! (7)
  deny ip 0.0.0.0 255.255.255.255 any log ! (8)
  deny ip 1.0.0.0 255.255.255.255 any log! (8)
  deny ip 2.0.0.0 255.255.255.255 any log! (8)
  …

- ICMP host-unreachable messages have been disabled earlier. Some services and email use the “packet too big” message when packets can’t be sent from source to destination so we will enable that ICMP message.

  permit icmp any any packet-too-big
  deny icmp any any host-unreachable

- Allow any established session. This will block packets from the Internet that have only the SYN flag set.

  permit tcp any 150.150.1.0 0.0.0.255 established
  deny ip any any log

  This is a simplistic filtering effect since a packet-crafting tool could easily by-pass this rule, but it blocks the less serious attacker.

- The following rules allow HTTP (1) and SSL (2) access to the Squid web caching address and deny HTTP and SSL to all other servers. These rules should be close to the front of the ACL because they are frequently accessed. Also permit access to the external mail server (3) and DNS queries to the external DNS server (4).

  permit tcp any host 150.150.1.67 eq 80 log ! (1)
  permit tcp any host 150.150.1.68 eq 80 log! (1)
  deny tcp any any eq 80 log! (1)
  deny tcp any any eq 80 log! (1)
  permit tcp any host 150.150.1.67 eq 443 log! (2)
  permit tcp any host 150.150.1.68 eq 443 log! (2)
  deny tcp any any eq 443 log! (2)
  permit tcp any 150.150.1.71 eq 25! (3)
  deny tcp any any eq 25! (3)
  permit udp any 150.150.1.69 eq 53! (4)
  permit tcp any 150.150.1.69 eq 53! (4)
  deny udp any any eq 53! (4)
  deny tcp any any eq 53! (4)

- Block telnet (1), FTP (2), SSH except to the SSH server (3), NetBIOS (4), SMB (5), Kerberos (6), rlogin (7), RPC (8) all NFS (9) and lockd (10) (prevents remotely mounting drive).

  deny tcp any any eq 23 log! (1)
  deny tcp any any eq 21 log! (2)
  permit tcp any host 150.150.1.70 eq 22 log! (3)
  deny tcp any any eq 22 log! (3)
  deny tcp any any range 135 139 log! (4)
  deny udp any any range 135 139 log! (4)
  deny tcp any any 445 log! (5)
  deny udp any any 445 log! (5)
  deny tcp any any eq 88 log! (6)
  deny udp any any eq 88 log! (6)
  deny tcp any any range 512 514 log! (7)
  deny tcp any any eq 111 log! (8)

dent udp any any eq 111 log! (8)
deny tcp any any eq 2049 log! (9)
deny udp any any eq 2049 log! (9)
deny tcp any any eq 4045 log! (10)
deny udp any any eq 4045 log! (10)

- Block all X windows traffic, external LDAP queries

  deny tcp any any range 6000 6255
  deny tcp any any eq 389 log
  deny udp any any 389 log

- Some other miscellaneous unneeded protocols to be blocked; SOCKS (1)– deny external proxy service, Line printer daemon (LDP) (2) – deny external UNIX printing service, NNTP (3) – newsgroups, external SNMP (4), Syslog from outside GIAC (5), TFTP (6), and BGP (7) – our ISP doesn't require this service on the border router.

  deny tcp any any eq 1080 log! (1)
  deny tcp any any eq 515 log! (2)
  deny tcp any any eq 119 log! (3)
  deny tcp any any range 161 162 log ! (4)
  deny udp any any eq 514 log! (5)
  deny udp any any eq 69 log! (6)
  deny tcp any any eq 179 log! (7)

- Block Land Attacks. This attack has the same IP address in the source and destination address fields as the router and also with the same port number in the source and destination port fields. This attack could cause a DOS (Denial of Service) or degrade the capability of the router.[14]

  deny ip host x.x.124.2 host x.x.124.2
  permit ip any any

- If problem sites occur, then they would be blocked also.

  deny ip x.x.x.x 0.0.0.255 log

- At the end of the Access List.

  deny ip any any log

[14] **National Security Agency, "Router Security Configuration Guide" 9 July 2002 URL: http://nsa1.www.conxion.com/cisco/download.htm#Zipped%20Archive p. 79 (11 Sep 2002)**

- Apply the access list to the interface access group.

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

Egress Filter on Border Router

Interface Ethernet 0

The next step is to apply an egress access list to the GIAC internal network interface for traffic leaving the network towards the Internet. We choose to apply the ACL to the Ethernet interface versus the serial interface since the ACL will drop the denied packets before they are routed through the router. This will save memory and CPU cycles.

(config)# access-list extended GIAC_out in

- First allow GIAC IP address space to exit the network and deny the rest. This will block traffic of addresses from reserved private, internal addresses (RFC 1918), the loopback address, the broadcast address.

permit ip 150.150.1.0 0.0.0.255 any
deny udp any range 0 65535 any log
deny tcp any range 0 655535 any log

- Allow some ICMP messages then deny access for the rest

permit icmp 150.150.1.0 0.0.0.255 packet-too-big
permit icmp 150.150.1.0 0.0.0.255 echo
permit icmp 150.150.1.0 0.0.0.255 parameter problem
permit icmp 150.150.1.0 0.0.0.255 source-quench

The packet too big message is needed for MTU path discovery, while echo allows users to ping external hosts. Parameter problem and Source Quench packets improve connections by informing about problems with packet headers and by slowing down traffic when it is necessary.[15]

deny icmp any any 3 0 ! network unreachable
deny icmp any any 3 1 ! host unreachable
deny icmp any any 3 3 ! port unreachable
deny icmp any any 3 4 ! DF bit

[15] **National Security Agency, "Router Security Configuration Guide" 9 July 2002 URL: http://nsa1.www.conxion.com/cisco/download.htm#Zipped%20Archive p. 80 (11 Sep 2002)**

deny icmp any any 3 13 ! Admin prohibited
deny icmp any any 5 ! Redirect
deny icmp any any 11 0 ! ttl-expired
deny icmp any any 17 ! Address mask request
deny icmp any any 18 ! Address mask reply

- Deny all traffic of addresses from the loopback address, all broadcast addresses, all multicast addresses, Class E reserved IP address space, originating traffic with GIAC internal (should be coming from the internal interface), traffic without an IP address, and reserved addresses.

  deny ip 127.0.0.0 0.255.255.255 any log
  deny ip 255.0.0.0 0.255.255.255 any log
  deny ip 224.0.0.0 7.255.255.255 any log
  deny ip 240.0.0.0 15.255.255.255 any log
  deny ip host 0.0.0.0 any log

- Deny everything that's is left or missed.

  deny ip any any log

- Apply the access list to the interface access group.

  (config)# interface e0
  (config-if) # ip access-group GIAC_out in

Configuration of the Cisco PIX

This section describes the basic configuration of the Cisco PIX that will provide the stateful inspection of the packets entering and leaving the GIAC network. The Cisco web site provides the guidelines to accomplish this work and is a good site to reference for assistance:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm

General Configuration

The first step is to set the enable password for the PIX to ensure there's secure access while performing configuration and administrative activities on the firewall.

enable password <password>

Set the ARP timeout. This keeps the entries in the ARP table for four hours before flushing.

arp timeout 14400

Enable paging. This will display 24 lines of information before pausing the listing and waiting for a prompt.

pager lines 24

Enable Syslog messages to provide diagnostic information and status on the firewall.

logging buffered debugging
logging timestamp
logging host 150.150.1.20 udp
logging host 150.150.1.21 udp

Disable SNMP access and SNMP traps generation.

no snmp-server location
no snmp-server contact
snmp-server community public

The following lists the default **fixup protocol** values (those enabled when a PIX Firewall is first installed). The PIX firewall supports stateful inspection of packets using Cisco's Adaptive Security Algorithm (ASA). The algorithm "fingerprints" every outgoing packet and then stores that information in a state table.[16]

The purpose of the fixup protocol command is to exam outbound traffic on the protocol types listed below. The source and destination address, port number, TCP flags and sequence numbers of the outbound packets are put into state tables. These tables contain the ASA hashes, which are referenced when the reply returns. If the information matches the table then the packets pass through while all other information is dropped.

fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521

[16] **The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.2.5, Bethesda, MD: SANS Press, p. 189 (2002)**

fixup protocol sip 5060[17]

We will edit the list to remove ftp, h323, and sip which are not required for the GIAC network

no fixup protocol ftp 21
no fixup protocol rsh 514
no fixup protocol h323 1720
no fixup protocol sip 5060

Two statements will be added – domain 53 and ntp 123

fixup protocol domain 53
fixup protocol ntp 123

Assigning an IP address and Subnet Mask

In the IOS configuration mode, set the default route to the interface of the PIX firewall.

ip route 0.0.0.0 0.0.0.0 *pix_inside_interface_ip_address*

Set the interface IP address and mask. Note that for unused interfaces, PIX assigns 127.0.0.1 to each interface and a subnet mask of 255.255.255.255 that does not permit traffic to flow through the interfaces.[18] There are six interfaces that will be used on the PIX firewall – Outside, Service, VPN and Inside (3).

ip address outside 150.150.1.45 255.255.255.252
ip address inside_management 150.150.1.34 255.255.255.252
ip address inside_users 150.150.1.42 255.255.255.252
ip address inside_servers 150.150.1.38 255.255.255.252
ip address service 150.150.1.54 255.255.255.252
ip address vpn 150.150.1.50 255.255.255.252

---

[17] **Cisco Corp., "PIX Firewall Quick Reference, Version 6.1" 10 June 2002 URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/cmd_ref/qref.htm (13 Sep 2002)**

18 **Cisco Corp., "Basic Firewall Configuration" 10 June 2002 URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm p. 2-7 (12 Sep 2002)**

Identifying the Interface Type

The interfaces on the PIX firewall are shutdown by default. By using the **interface** command, the interface becomes enabled. The GIAC PIX firewall will have 10/100 BaseT Ethernet interfaces, but gigabit Ethernet is also available. Also, auto-negotiation is disabled and the interface is set to full-duplex.

interface ethernet0 100full – Connection to Outside
interface ethernet1 100full – Connection to Management Network
interface ethernet2 100full – Connection to GIAC Users Network
interface ethernet3 100full – Connection to Internal Web Servers
interface ethernet4 100full – Connection to Service Network
interface ethernet5 100full – Connection to VPN

We want to ensure to set the MTU to 1500 bytes per Cisco guidance.

mtu outside 1500
mtu inside_management 1500
mtu inside_users 1500
mtu inside_servers 1500
mtu service 1500
mtu vpn 1500

Set Interface Names and Security Levels

The interfaces each have a unique name and security level. By default, Ethernet 0 is named outside and is assigned the security level 0, while Ethernet 1 is named inside with a security level of 100.

nameif ethernet0 outside security0
nameif ethernet1 inside_management security100
nameif ethernet2 inside_users security100
nameif ethernet3 inside_servers security100
nameif ethernet4 service security25
nameif ethernet5 vpn security50

The purpose of the security levels is to control access between systems on different interfaces and the relative security levels of the interfaces either enable or restrict access. There are two different types of access to consider:

For access to a higher security level interface from a lower level interface – use the **static** and **access-list** commands.

To allow access to a lower security level interface from a higher-level interface – use the **nat** and **global** commands.[19]

Therefore the lowest security level would be outside the GIAC network and since outside users have easy access to the service network, its security level is also lower, but not as low as the outside since there is an ACL in place on the border router. Of the four different zones, we would trust out inside network the most so it gets the highest security level while the VPN zone is rated somewhat lower.

Configure the Firewall for Routing

The PIX firewall interfaces need to be configured for route and RIP information. The route information will specify which interface to forward packets and more than one route can specified per interface. The PIX learns the location of devices of the network by passively examining RIP traffic and then updating its routing tables.

The first interface to configure is the outside one connected to the Cisco 3640 Border Router.

route outside 0 0 150.150.1.45 1

This tells the router to send the default route to the router (**1.45**) through the **outside** interface and it is **1** hop away. The **0 0** is shorthand for a 0.0.0.0 IP address and mask.

The next step is to configure the other interfaces that connect to the firewall which have other subnets behind them. The VPN router has already been defined with no other network addresses behind it so this step isn't require for it.

route inside_management 150.150.1.16 255.255.255.240 150.150.1.34 1

route inside_users 150.150.1.128 255.255.255.128 150.150.1.42 1

route inside_servers 150.150.1.0 255.255.255.240 150.150.1.38 1

route service 150.150.1.64 255.255.255.240 150.150.1.54 1

---

[19] Cisco Corp., "Basic Firewall Configuration" 10 June 2002 URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm p. 2-9 (12 Sep 2002)

Establishing Outbound Connectivity

The PIX firewall has the ability to associate internal addresses with global addresses using a NAT identifier (NAT ID).[20] For the GIAC Network, we have decided for now to forgo NAT since we feel there is minimal loss in security by not implementing it. It would be easy enough to use NAT later if the need arises.

The higher-level security interfaces are configured first so devices on those interfaces can start connections to interfaces with lower security levels and be recognized on the outside network.

The NAT format is as follows:

nat (interface_name) nat_id local_ip netmask
A nat_id of 0 causes NAT to be disabled

nat (inside_management) 0 150.150.1.16 255.255.255.240

nat (inside_users) 0 150.150.1.128 255.255.255.128

nat (service) 0 150.150.1.64 255.255.255.240

nat (inside_servers) 0 150.150.1.64 255.255.255.240

The internal database servers should not have the ability to connect to any device other than the external database to only push new information onto the server. Any packets going anywhere else would be blocked by a access list.

Configuring Inbound Access to Network

The firewall requires a rule to allow outside users to access the Services Network and VPN router. For this the **static** command is used to protect inside addresses (or zones with higher security levels) by not providing access to them without explicitly specifying the IP address space or device (mail server, DNS). Along with the static command the **access-list**

[20] **Cisco Corp., "Basic Firewall Configuration" 10 June 2002 URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm p. 2-12 (12 Sep 2002)**

command is needed since without it, the inside host isn't accessible from the outside, therefore, its invisible to the outside world.[21]

The Static command format:

static (*high_security_zone, low_security_zone*) *ip_address_visible_ to outside actual_ip_address* netmask *mask*

Traffic to Services Network

The web servers in the services network needs to be accessible to outside users.

```
static (service, outside) 150.150.1.67 150.150.1.67 netmask 255.255.255.255
static (service, outside) 150.150.1.67 150.150.1.68 netmask 255.255.255.255

access-list acl_to_web permit tcp any host 150.150.1.67 eq 80
access-list acl_to_web permit tcp any host 150.150.1.68 eq 80

access-group acl_to_web in interface outside
```

The static command allows outside users to see the IP address of the Web proxy server which is also the IP address that is set as being visible to the outside (this differs from the NAT enabled procedure which would have two different addresses listed).

The access-list specifies who can access the web server, its address and port.

The access-group command applies the access-list to the outside interface for packets coming into the PIX firewall from the router.

The same would be done for the other web server as well as the External DNS, and External Mail with an access list allowing access to the appropriate protocol and service port.

Traffic to Management, Users, and Internal Database Networks

For traffic coming from the VPN to the three internal networks, another static rule is needed so packets can go to the Management, Users and Internal Database networks.

```
static (inside_management, VPN) 150.150.1.16 150.150.1.16 netmask 255.255.255.240
```

[21] **Cisco Corp., "PIX Firewall Command Reference" 10 June 2002 URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/cmd_ref/s.htm#11459 p. 8-23 (13 Sep 2002**

access-list acl_to_management tcp any host 150.150.1.16 255.255.255.240

access-group acl_to_management in interface VPN

For the other networks to connect to internal GIAC services such as email, and DNS the commands would be similar. Caution should be applied when considering allowing access to the internal database servers and should possible be denied.

Access Lists

The PIX firewall can have only one access-list applied to any interface per direction like the Cisco router. To lessen the use of memory, the access lists will be on the inbound side of the interface so if unwanted packets are to be dropped it is done when they reach the firewall and not when they exit.

It should be noted to avoid confusion, that the Pix Firewall uses a subnet mask versus the wildcard mask (i.e. don't care) mask. This can be confusing if not explained.

PIX Firewall

access-list acl_grp permit tcp any 209.165.201.0 255.255.255.0

Cisco router

access-list acl_grp permit tcp any 209.165.201.0 0.0.0.255

Fortunately the format of the access-list follows an expected pattern.

access-list acl_ID [permit|deny] protocol source_address port destination_address port

Though there are other options available, these are ones we will use.

Traffic From the Internet

The access-list will control unwanted packets that might have somehow passed through the router's "absolute" access-list. We do expect a lower percentage of traffic hitting our outside firewall interface versus the total traffic that hit our outside interface of the border due to the ACL. We could take the approach that the router will do its job and we can believe nothing we intended to block will get through. But since nothing can be absolute here, we'll take the layered approach that if the border route didn't do its

job or was compromised, then we still have an layer to protect the GIAC network.

Private Addresses

As on the Router outside interface, RFC 1918 private addresses are blocked.

access-list from_router deny ip 10.0.0.0 255.0.0.0 any
access-list from_router deny ip 172.16.0.0 255.240.0.0 any
access-list from_router deny ip 192.168.0.0 255.255.0.0 any

DNS Server

Allow access to the DNS server so others can look up the web and mail servers IP addresses plus the VPN router.

access-list from_router permit udp any host 150.150.1.69 eq 53
access-list from_router permit tcp any host 150.150.1.69 eq 53

Mail Server

Next open access to the external mail server, which opens security holes in the network – namely email viruses and spam. We limit our exposure by employing a mail filter but it will have limited success against spam. Anti-Spamming software should be purchased to combat this problem.

access-list from_router permit tcp any host 150.150.1.71 eq 25

Web Servers

We need to allow access to the web severs which is the core to the GIAC business. Just incase the web servers do get compromised; we will also block the web servers from initiating connections out toward the Internet - using the access-list from_sevices later.

access-list from_router permit tcp any host 150.150.1.67 eq 80
access-list from_router permit tcp any host 150.150.1.68 eq 80
access-list from_router tcp any host 150.150.1.67 eq 443
access-list from_router tcp any host 150.150.1.68 eq 443

VPN Router

Traffic from our employees, partners and suppliers will be allowed. We will use a Class C address for partners and suppliers. Key exchange will use port 500 and 50 for ESP.

Allow access to the Cisco VPN 3030 but only for the protocols used for key exchange, key management and encapsulating the payload. This would all be for IPSEC. Port 500 is used by IKE (key exchange protocol), port 50 is ESP that allows encapsulation of the security payload while port 57 is SKIP, the key management protocol. Finally, deny all other types to access to the VPN

permit tcp any host 150.150.1.50 eq 500 log
permit 50 any host 150.150.1.50 log
permit 57 any host 150.150.1.50 log
deny ip any host 150.150.1.50 log

Accurate timestamps are required to mark packets entering and leaving the network, so the VPN will synchronize with the NTP server located on the Management Network.

access-list from_vpn permit udp host 150.150.1.50 host 150.150.1.18 eq 123

Lastly, log messages to the Syslog server and deny all other traffic that hasn't been explicitly allowed.

access-list from_vpn permit udp host 150.150.1.50 host 150.150.1.21 eq 514
access-list from_vpn deny ip any any log-input

Router Logging Traffic

Allow the router logging traffic to reach the Syslog server.

access-list from_router permit udp host 150.150.1.45 host 150.150.1.20 eq 514

The last line in the access list is to deny all other traffic, which might inadvertently block services we do need. But for now we'll side with caution and open ports on a need to use basis after reviewing all security issues.

Other Access-list Entries

access-list from_router deny ip any any log-input

Configuring Access Between Zones on Network

There isn't a lot of access we have to control here. The only traffic that is initiated from a lower security level (Services network) to a higher level (Users network) would be email. We need to allow the external email server to send traffic to the internal email server.

static (inside_users, service) 150.150.1.135 150.150.1.135 255.255.255.255

access-list acl_to_mail tcp 150.150.1.71 150.150.1.135 255.255.255.255 eq 25

access-group acl_to_mail in interface service

Traffic From the Service Network

An access list allowing traffic from our DNS, and Mail Server.

DNS Server

The DNS server needs to query other Internet DNS servers.

access-list from_service permit tcp host 150.150.1.69 any eq 53
access-list from_service permit udp host 150.150.1.69 any eq 53

Mail Server

The mail server must be able to pass so the mail can be send to other mail servers and to the internal mail server. From a security standpoint, we have to be concerned about email viruses and must employ the industry specified software to combat this. If problems by occur later, we will as part of the fix process, remove this rule both for outbound and inbound email traffic.

access-list from_service permit tcp host 150.150.1.71 any eq 25
access-list from_service permit tcp host 150.150.1.71 host 150.150.1.135 eq 25

Access-list

Again, the last line in the access list is to deny all other traffic, which might inadvertently block services we do need. But for now we'll side with caution and open ports on a need to use basis after reviewing all security issues.

access-list from_router deny ip any any log-input

Traffic From the GIAC Users Network

Now we have to specify which traffic will be allowed out of the network.

The exchange of mail from internal to external requires the two to talk to each other through the firewall. Of course, we employ a virus scanner to eliminate viruses as much as possible and ensure the servers have the last patches.

access-list from_users permit udp host 150.150.1.135 150.150.1.71 eq 25

The internal DNS server is used recursively. So when internal devices need to communicate with devices outside the GIAC network, the DNS server must know the IP address of the destination.

access-list from_users permit udp host 150.150.1.134 any eq 53
access-list from_users permit tcp host 150.150.1.134 any eq 53

The new fortune sayings provided by the suppliers must be retrieved from the Service Network database and put on the internal database. Once there, the sayings are reviewed, edited and then put on the web site for purchase. To control who has access to do this, we will assume only a few selected users of the whole GIAC Users Network are allowed access.

access-list from_users permit tcp 150.150.1.136 255.255.255.248 150.150.1.70 eq 1521

access-list from_users permit tcp 150.150.1.136 255.255.255.248 150.150.1.9 eq 1521

There won't be any restrictions on the users' access to the Internet but will block web sites in the future if inappropriate sites (To be defined by Customer) become a problem.

access-list from_users permit ip 150.150.1.128 255.255.255.128 any

Again, as with the other access list, we block all other access unless a compelling reason is given for access and security concerns are reviewed first.

access-list from_users deny ip any any log-input

Traffic From the Management Network

The next to the last access list needed is for the Management Network. This is where the Syslog, NTP, SMTP servers are located and from here the IS department will monitor and fix the GIAC network. They will need access to all sub-networks in the GIAC network.

A limited number of IS devices need access to the GIAC network, so we will limit which ones have access and log their activity. We want to be able to review the logs to ensure these boxes don't become compromised.

access-list from_management permit ip host 150.150.1.17 150.150.1.0 255.255.255.0 log-input

access-list from_management permit ip host 150.150.1.17 150.150.1.0 255.255.255.0 log-input

The NTP server will synchronize with the servers mentioned in the earlier to ensure all logging devices have accurate timestamps. This will allow us to review files from the devices and make correlating packet activity much easier.

access- list from_management permit udp host 150.150.1.18 host 216.27.190.202 eq 123

access- list from_management permit udp host 150.150.1.18 host 207.126.97.57 eq 123

Again, block all other traffic not specified earlier.

access-list from_management deny ip any any log-input

Traffic From the Internal Database Network

The access list for the Internal Database Network is short. We just want to allow the database to push the new fortune sayings to the GIAC external server, which will provide the web server with new sayings.

access-list from_database permit host 150.150.1.9 host 150.150.1.70 eq 1521

Deny all other services and log blocked packets.

access-list from_database deny ip any any log-input

Tutorial on the Cisco Concentrator 3000 Series VPN

This tutorial will focus on configuring the Cisco 3030 to communicate with the VPN clients using certificates.[22]

The first step is to configure the IKE policy. The type(s) of certificates to use must be set and this is accomplished by accessing the IKE proposals screen. This screen is accessed by going to **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** and is displayed in the below screenshot.

Screen 1

This screen allows for the activation or deactivation of multiple IKE (Internet Key Exchange) proposals. These proposals will help us provide an IPSec VPN for the remote GIAC users, partners and suppliers. All use 3DES, which uses 3 keys and provides for confidentially of the data. DES is the most used encryption algorithm in the world[23] but is slow to implement in software. Fortunately, we are using the Cisco VPN 3030 that implements encryption in hardware to greatly improve performance. This will ensure the packets sent and delivered are

---

[22] Cisco Corp., "Configuring the VPN 3000 Concentrator to Communicate with the VPN Client Using Certificates" 23 Sep 2002 URL:http://www.cisco.com/warp/public/471/installboth.html (24 Sep 2002)

[23] The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.4.1, Bethesda, MD: SANS Press, p. 21 (2002)

protected from being unencrypted without a hacker using a great deal of effort. For the GIAC network, 3DES provides more than the needed protection.

Now that the packets are encrypted, we need to know that the message actually came from the sender. The options are either MD5 or SHA used for data integrity. Message-Digest Algorithm (MD5) is used to create a "digital signature" of the message using a one-way hash.[24] This method doesn't involve any keys so only brute force attacks using text combinations continuously will retrieve the original message digest. SHA or SHA-1 is used with the DSA (Digital Signature Algorithm) in electronic mail, electronic funds transfer, software distribution, data storage, and other applications, which require data integrity assurance and data origin authentication.[25] The algorithm takes a message of less than 2^{64} bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.[26] Given the two choices, MD5 would be selected since it's faster (16 Bytes digest vs. 20 Bytes for SHA-1) and we probably don't need the added security that SHA-1 provides. But we would support both so as not to prevent users from accessing the network.

The next option(s) in the IKE proposal list is to select RSA or Diffie-Hellman for authentication. Authentication validates that both ends of a session are in fact who they claim to be.[27] Which one to use is debatable with Roger Schlafly[28] stating, "The asymptotics are similar. But breaking DH (ElGamal or DSA) requires some large tables. Much larger RSA keys have been broken than DH keys." But M.J. Wiener states, "The most important factor in choosing a public-key technology is security. Based on the best attacks known, RSA at 1024 bits, DSA and Diffie-Hellman at 1024 bits, and elliptic curves at about 170 bits give comparable levels of security."[29] We will again support both to prevent blocking user access by not supporting the needed authentication option. The left side of the proposals list shows the Cisco-supplied default active proposals.

---

[24] The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.4.1, Bethesda, MD: SANS Press, p. 33 (2002)

[25] Federal Information Processing Standards Publications, "SECURE HASH STANDARD" 17 April 1995 URL: http://www.itl.nist.gov/fipspubs/fip180-1.htm (25 Sep 2002)

[26] RSA Security, "What are SHA and SHA-1?" 2002 URL:http://www.rsasecurity.com/rsalabs/faq/3-6-5.html (25 Sep 2002)

[27] The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.4.1, Bethesda, MD: SANS Press, p. 32 (2002)

[28] Roger Schlafly, "Opinions on S/MIME" 30 Dec 1998 URL:http://groups.google.com/groups?oi=djq&selm=an_427312947 (25 Sep 2002)

[29] M.J.Wiener, "Performance Comparison of Public-Key Cryptosystems", RSA CryptoBytes, Volume 4, Number 1, Summer 1998

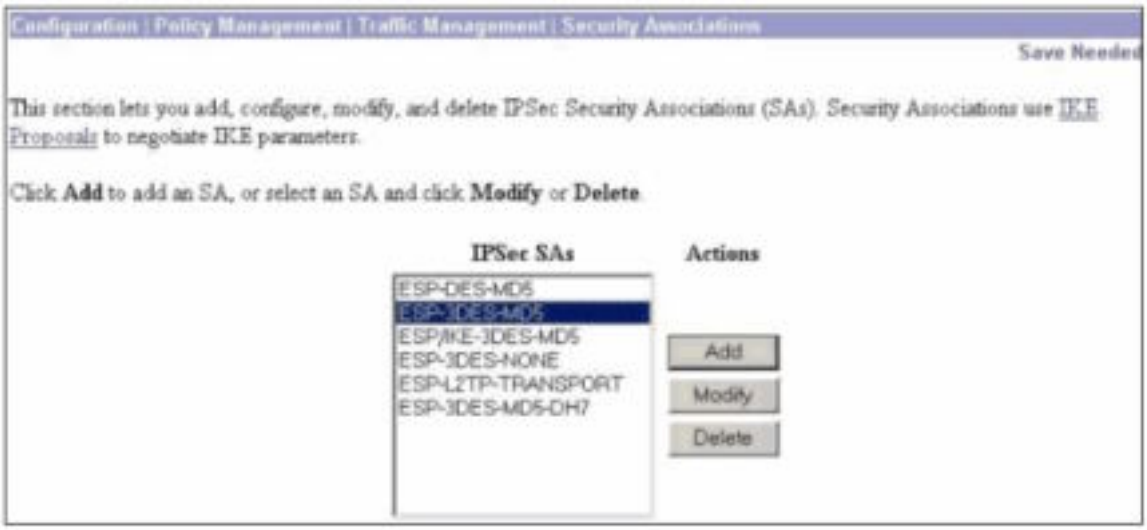
- CiscoVPNClient-3DES-MD5 – This selection uses preshared keys and MD5/HMAC-128 for authentication. 3DES with 168 bits encryption used with Diffie-Hellman Group 2 (1024 bits) to generate SA keys. This option allows for user-based authentication and is the default.

- IKE-3DES-MD5 – Use preshared keys and MD5/HMAC-128 for authentication. Again use 3DES and D-H group 2 for generatingSA keys.

- IKE-3DES-MD5-DH1 – This differs from the last proposal only by the bits used to generate the SA keys (768 vs. 1024).

- IKE-DES-MD5 – This differs from the second proposal by using DES vs. 3DES and using D-H group 1.

- IKE-3DES-MD5-DH7 – Similar to the third proposal but uses D-H group 7, which uses ECC (Elliptic Curve Cryptography).



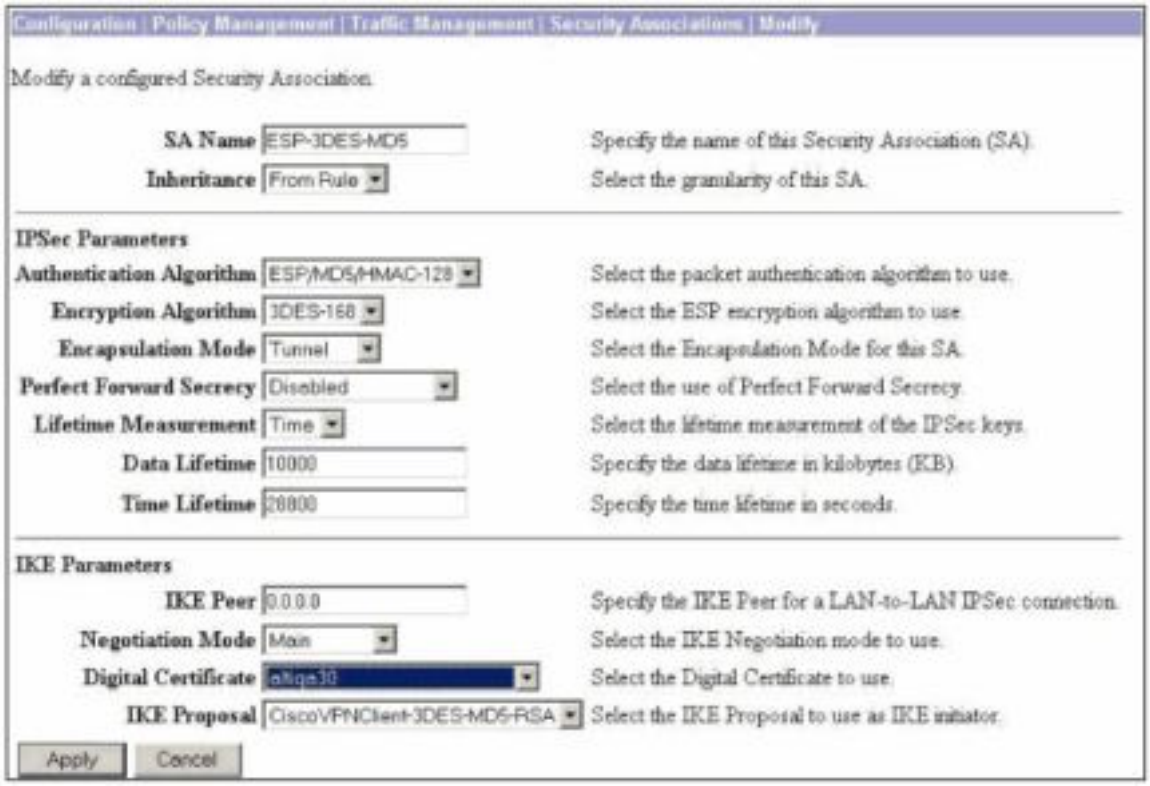
Screen 2

The next step in the process of configuring the VPN to communicate with a VPN client is to setup the IPSec policy to use certificates. The above list of IPSec SAs polices only displays ESP (Encapsulated Security Payload) as an option and not AH (Authentication Header). AH was designed to provide data origin authentication, connectionless integrity, and optional protection against replay attacks.[30] But unlike ESP, AH doesn't protect the data through encryption and it

[30] **The SANS Institute, Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track 2.4.3, Bethesda, MD: SANS Press, p. 102 (2002)**

may break NAT implementations. The reason AH is a problem with NAT is that AH authenticates the source and destination IP addresses but NAT will then change those values so when the receiving device performs an integrity check on the packet it fails. To eliminate problems that could occur with NAT (partners or suppliers using NAT), the GIAC network won't support AH.

The choice we will select to use is "ESP-3DES-MD5". ESP like AH provides authentication, though unlike AH it doesn't authenticate the IP headers. This authentication can occur by one-way hash functions or the use of manual key changes. ESP provides confidentiality by encrypting the TCP header and data portion of the packet either by DES or 3DES. The last three features of ESP are the ability to provide connectionless integrity using the authentication service and protection against replay attacks by using sequence numbers and finally limited flow confidentiality through the use of padding in the protocol.



Screen 3

The modify screen has a number of parameters that can be changed. The first is to set the SA name, which is a unique name for this Security Association. Maximum is 48 characters and inheritance. Inheritance has two options: [31]

[31] **Cisco Corp., "VPN 3000 Concentrator Series User Guide – Policy Management" URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcoug/usr_3_0/ (30 Sep 2002)**

- **From Rule** = One tunnel for each *rule* in the connection. A rule can specify multiple networks, thus many hosts can use the same tunnel. This is the default—and recommended—selection.
- **From Data** = One tunnel for every *address* pair within the address ranges specified in the rule. Each host uses a separate tunnel, and hence, separate keys. This selection is more secure but requires more processing overhead

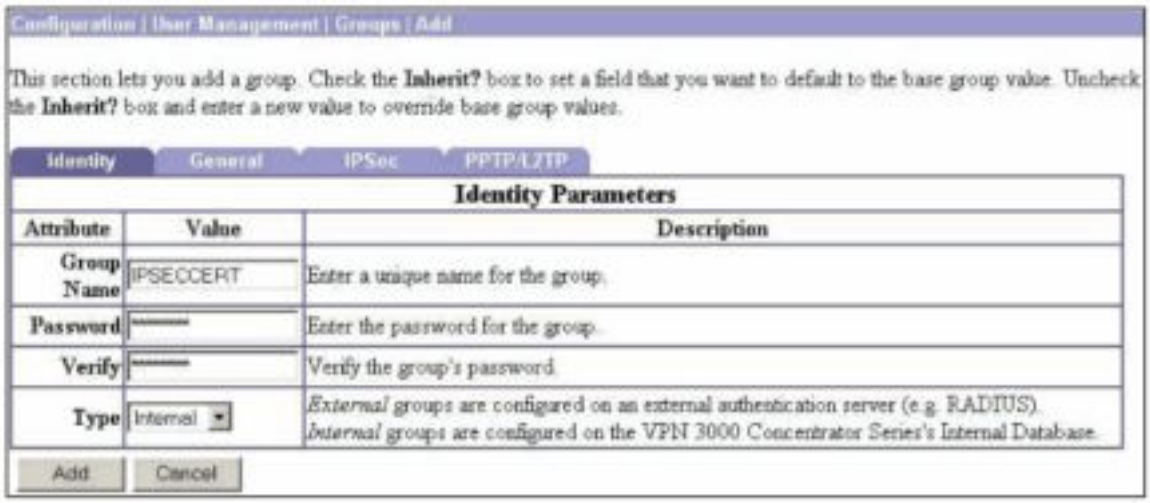
Under the IPSec parameters section we can select which **Authentication Algorithm** to use. The two attributes that Cisco supports are ESP-MD5-HMAC-128 (default selection) and ESP-SHA1-HMAC-160 (Hash Message Authentication Code) – more secure but requires more processing overhead. There are three **Encryption Algorithms** – Null for no packet encryption, DES-56 using DES encryption with a 56-bit key and 3DES-168, which use triple-DES encryption with a 168-bit key (Default selection). For **Encapsulation Mode** the choices are Tunnel or Transport. With tunnel mode ESP encryption and authentication is applied to the entire original IP packet (Default selection and most secure). Transport mode only applies ESP encryption and authentication to the transport segment so the source and destination addresses are exposed. This mode should be used for Windows 2000 client compatibility. **Perfect Forward Secrecy** is a cryptographic concept where each new key is unrelated to any previous key. During IPSec negotiations, the Phase 2 keys are based on the Phase 1 keys unless Perfect Forward Secrecy is specified. Diffie-Hellman techniques are employed to generate the keys. It is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel.

There are four options for this drop-down: Disabled (default selection), Group1, Group2 and Group7. The mentioned groups use Diffie-Hellman to generate IPSec session keys, where the prime and generator numbers are 768 bits (Group 1), or 1024 bits (Group 2). Group 2 is more secure but it also requires more processing overhead. Victor Miller and Neal Koblitz proposed ECC (Elliptic Curve Cryptography) in the mid 1980s[32] using an elliptical curve field size of 163 bits. This group is the fastest of the three and requires the least overhead. For the GIAC network we will follow the Cisco recommended default selection.

The next parameters of interest are in the IKE section. These parameters govern IKE SAs, which are Phase 1 SAs negotiated under IPSec. For this IKE SA the two parties exchange automated key management information. Cisco recommends using the default parameters where possible for the best performance and interoperability. The **IKE PEER** parameter is used only for IPSec LAN-to-LAN connections. We will ignore this since we are configuring for a VPN client but would use it for configuring a VPN for the GIAC suppliers and

[32] **Elliptic Curve Cryptography, 18 Sep 2002 URL:http://www.isg.rhul.ac.uk/~sdg/ecc.html (1 Oct 2002)**

partners. **Negotiation Mode** deals with the exchanging of key information and setting up the SAs. The initiator of the negotiation process uses it and then the responder would auto-negotiate the parameter. There are two modes: Aggressive which is the faster of the two since it sends fewer packets and exchanges but it doesn't protect the identity of the parties involved. Main mode uses more packets and exchanges than Aggressive mode and protects user identities and is the default selection. The **Digital Certificate** parameter specifies whether to use preshared keys or a PKI digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. The drop-down menu will display any digital certificates that have been installed. The default selection is none meaning that preshared keys will be used and we will accept that selection. The last parameter for this section is the **IKE Proposal**, which specifies the set of attributes that govern Phase 1 IPSec negotiations. These negotiations, also known as proposals, were selected on the **Configuration | System | Tunneling Protocols | IKE Proposals** screen earlier. We will use the default setting **CiscoVPNClient-3DES-MD5**.


Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | PPTP/L2TP

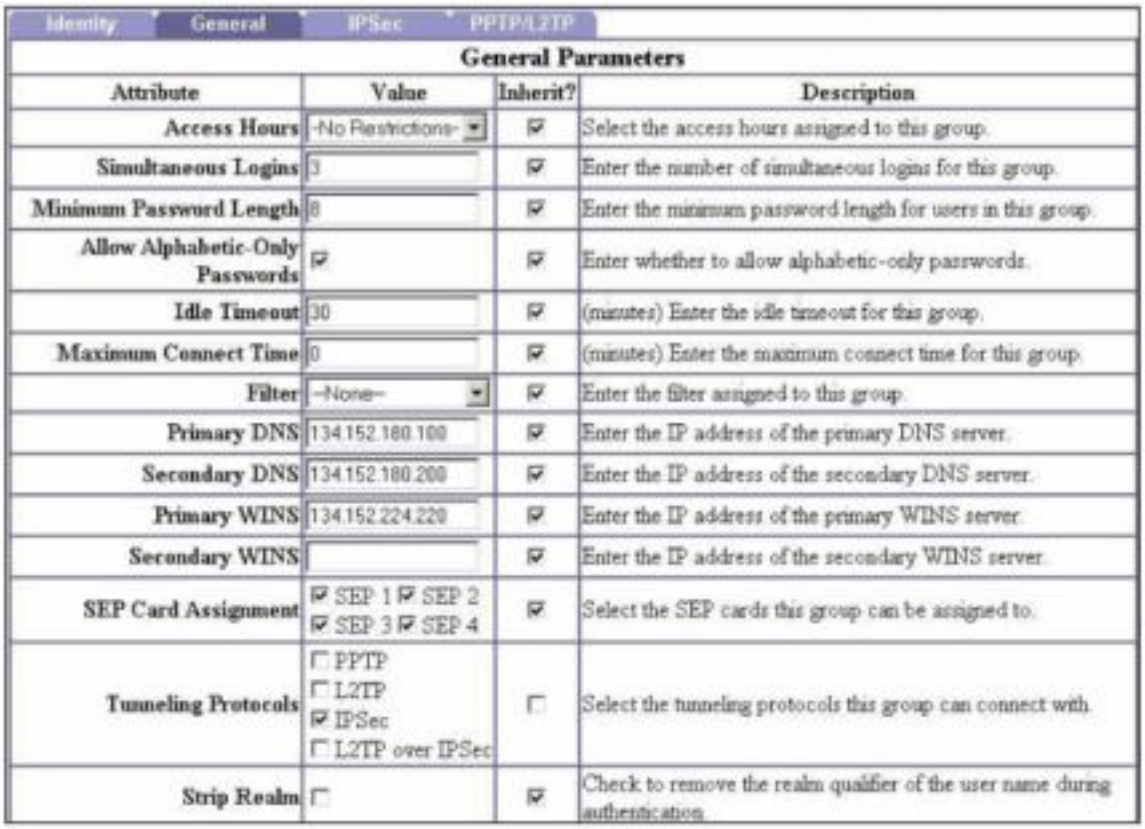
Identity Parameters

Attribute	Value	Description
Group Name	IPSECCERT	Enter a unique name for the group.
Password	********	Enter the password for the group.
Verify	********	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator Series's Internal Database.

Add | Cancel

Screen 4

The following screens require just a few inputs and allow us to double check that the options selected are the ones we want. This next screen allows a group to be added. In the **Group Name** IPSECCERT is inputted. It matches the Organizational Unit in the identity certificate. Next a password is entered. The **Type** of group is either external (RADIUS server) or internal (Cisco VPN concentrator). Internal is selected.



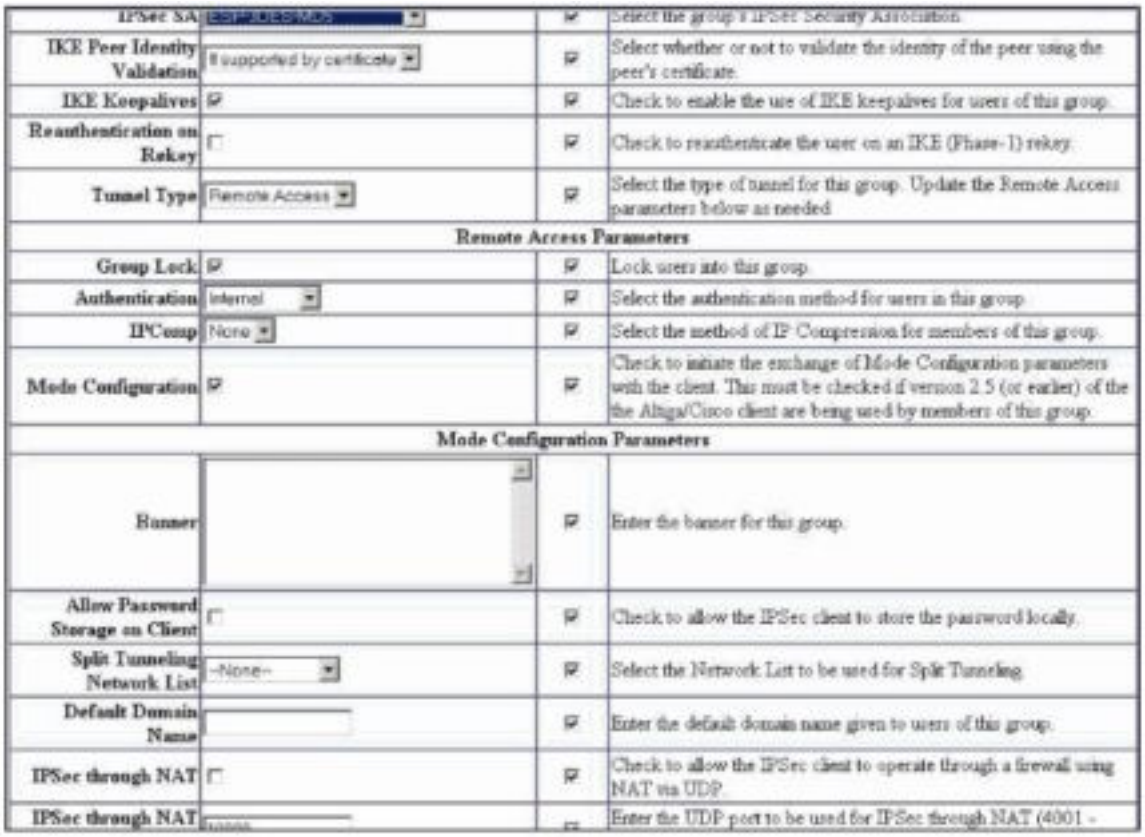
Identity | General | IPSec | PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	-None-	☑	Enter the filter assigned to this group.
Primary DNS	134.152.180.100	☑	Enter the IP address of the primary DNS server.
Secondary DNS	134.152.180.200	☑	Enter the IP address of the secondary DNS server.
Primary WINS	134.152.224.220	☑	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☐	Select the tunneling protocols this group can connect with.
Strip Realm	☐	☑	Check to remove the realm qualifier of the user name during authentication.

Screen 5

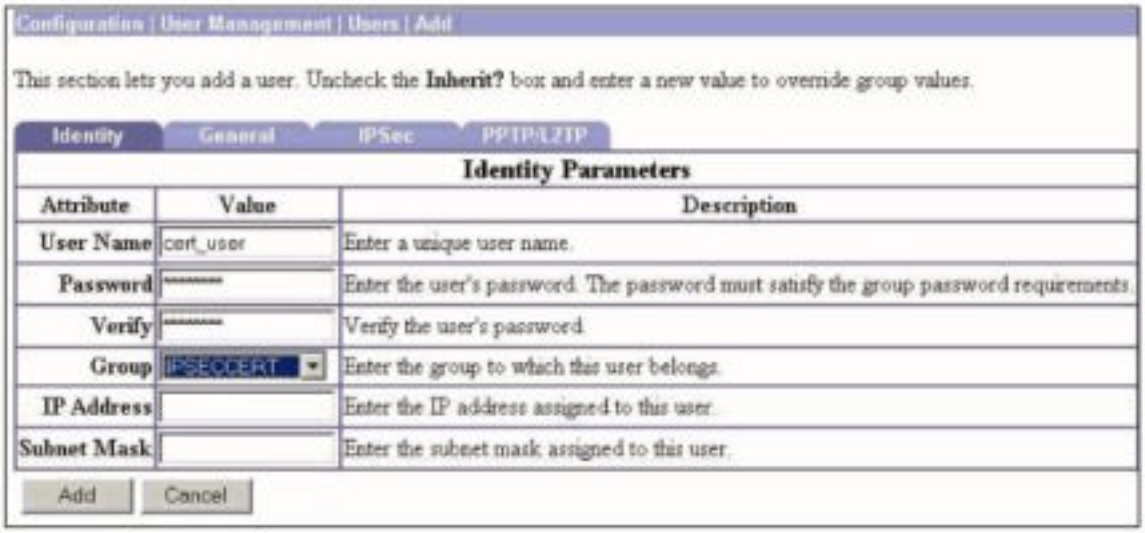
Once the group is identified, we want to set the Primary and Secondary DNS if available. We will have only a Primary DNS found on our Service network (150.150.1.69). The only other option we want to check is IPSec under Tunneling Protocols. All the other default options will be left unchanged.



IPSec SA	[illegible]	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for users of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	☑	☑	Lock users into this group.
Authentication	Internal	☑	Select the authentication method for users in this group.
IPComp	None	☑	Select the method of IP Compression for members of this group.
Mode Configuration	☑	☑	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Altiga/Cisco client are being used by members of this group.
Mode Configuration Parameters			
Banner		☑	Enter the banner for this group.
Allow Password Storage on Client	☐	☑	Check to allow the IPSec client to store the password locally.
Split Tunneling Network List	--None--	☑	Select the Network List to be used for Split Tunneling.
Default Domain Name		☑	Enter the default domain name given to users of this group.
IPSec through NAT	☐	☑	Check to allow the IPSec client to operate through a firewall using NAT via UDP.
IPSec through NAT	[illegible]	☐	Enter the UDP port to be used for IPSec through NAT (4001 -

Screen 6

Of the various options on this screen, we just need to make sure that the configured IPSec SA is selected under **IPSEC SA**. The selection should be the same as the one selected in the IPSec Security Association screen earlier (Screen 2).



Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPSec | PPTP/L2TP

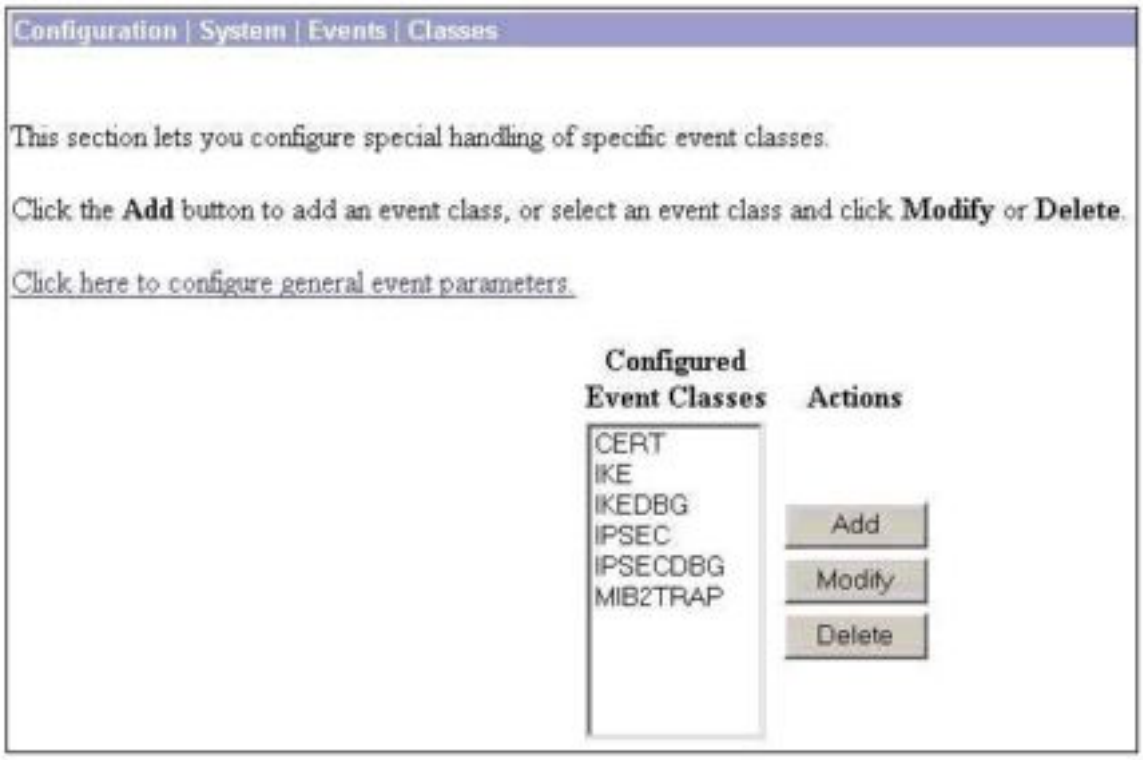
Identity Parameters

Attribute	Value	Description
User Name	cert_user	Enter a unique user name.
Password	********	Enter the user's password. The password must satisfy the group password requirements.
Verify	********	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add | Cancel

Screen 7

Screen 7 is used to configure an IPSec group on the VPN concentrator. A unique user name is entered, along with a password and the **Group** inputted before.



Screen 8

Now that most of the configuration work has been completed, we now have options to enable debugging on the VPN. The Cisco VPN allows for various event classes and severity levels and these are the default values:

CERT	1-13	Digital certificates subsystem including SCEP
IKE	1-6	ISAKMP/Oakley (IKE) subsystem
IKEDBG	1-10	ISAKMP/Oakley (IKE) debugging
IPSEC	1-6	IP Security subsystem
IPSECDBG	1-10	IP Security debugging

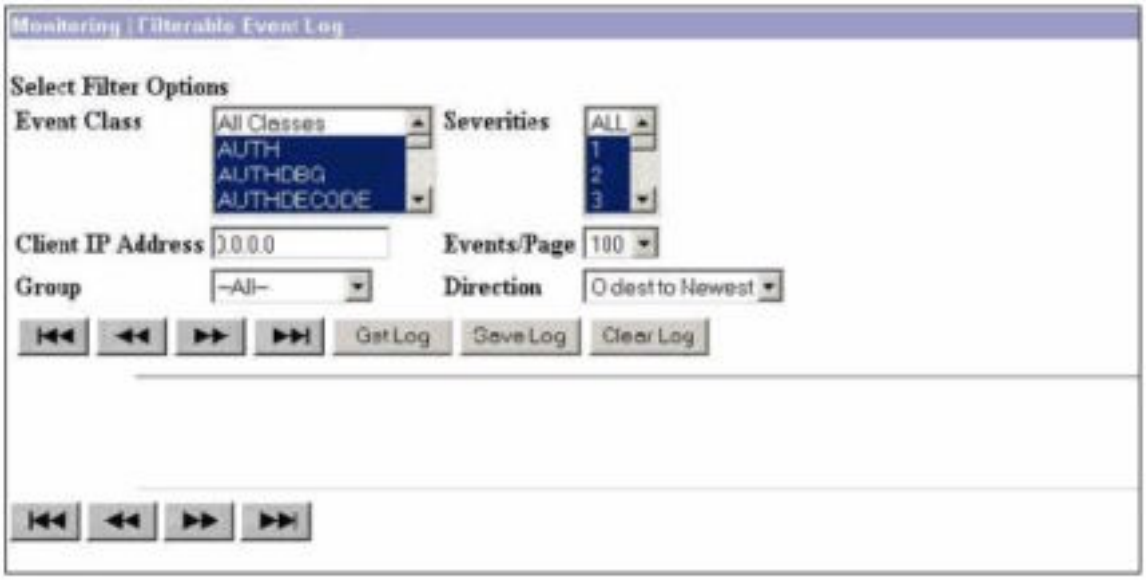
VPN Concentrator Event Severity	Category	Description

Levels Level		
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that might require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.
6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding
11	Packet Decode	Low-level packet header decoding
12	Packet Decode	Hex dump of header
13	Packet Decode	Hex dump of packet

An event is classified by Cisco as “any significant occurrence within or affecting the VPN 3000 Concentrator, such as an alarm, trap (an event message sent to an SNMP system is called a "trap"), error condition, network problem, task completion, threshold breach, or status change. The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. You can also

specify that certain events trigger a console message, a UNIX syslog record, an e-mail message, or an SNMP management system trap."

"Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator**."**[33]



Screen 9

The final screen sets the event classes to view by filtering the event log.

[33] **Cisco Corp., "Table of Contents – Events" 7 Aug 2002 URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/rel3_5_1/config/events.htm (1 Oct 2002)**

Assignment 3 – Verify the Firewall Policy

Plan the Audit

Audits of the GIAC network are an essential part of ensuring it stays secure. We want to go through and sure that no obvious security errors have occurred and use the audit to help strengthen the security policy. Verifying that what we had planned to do has been implemented, the documentation is accurate, and any areas that need improvement are brought to light does this.

As mentioned at the beginning of this report, an independent audit should be done to remove any bias. This will give the auditors a fresh prospective of the network, and remove any personal blind spots of the persons implementing the security policy. For this paper, the scope of the audit will only be on the Cisco PIX Firewall, which is the primary firewall for the GIAC network. A more comprehensive audit would examine all devices, software, polices, traffic flows, etc.

Estimated Cost of Audit:

Table of The Audit Expenses: (Billing rate of $200/hr)

Task	Required Hours
Review documentation – Firewall, Network, Security Policies, etc.	5 hrs.
Examine physical security of Firewall	1 hr.
Review IOS version and patches levels on Firewall System	2 hrs.
Equipment configuration for audit	6 hrs.
Run scanning tools against Firewall and interfaces	15 hrs.
Review results and find reason(s) for identified rule(s) shortcomings	15 hrs. (Estimate- depends on how secure the network really is)
Documentation and Meeting to present report	10 hrs
Total Hours	54 hrs
Total Audit Cost	**$10,800**

Risks and Considerations

Since e-commerce is GIAC Enterprise primary business, we can't have the audit interfere with the on-going business needs. So the security audit

will be planned for a time when there is little traffic, which is determined by looking at the traffic patterns, and Syslogs. From that information, Sunday at 12 midnight until 9AM was selected. All important systems and devices will be backed-up and baselined before the audit just encase problems do occur while running the audit. The software used for the audit is intended to test the security of the network and not the performance of the firewall, so there isn't a concern about affecting performance of the firewall and e-commerce traffic will still be possible. We will however monitor the audit with SiteScope so watch for noticeable slowing of the network that could affect end-user performance. Since this is a test of the security of the network, unexpected events such as Denial of Service or crashing the firewall. This is why we backup and baseline before the test. We will have the appropriate personnel on-site during the audit fix any problems that might pop-up.

Technical Approach

The audit of the PIX firewall will follow a series of stages and events:

1) Brief GIAC management on the audit, explaining its purpose, duration, cost, inherent risks, and expected results.
2) Develop a written audit strategy and plan that compares the security policy against the firewall rule set. This information should be gathered and verified from talks with network, security and administrators of the GIAC network. Have a logical diagram of the flow of traffic required for the GIAC business needs.
3) Perform a physical review of the network equipment to ensure only authorized personnel have physical access to the firewall.
4) Review documentation related to the Cisco PIX firewall. Review installation and configuration guides and documentation related to the firewall rule set.
5) The rule base will be examined and tested to ensure it is working properly and the rules successfully restrict unauthorized access.

General Audit Plan

Two laptops are employed and positioned so the firewall is between them as we examine the traffic as it attempts to go from one area of the network to another. These areas include the Internet, the Service, Management, User and Internal Server Networks plus the VPN.

The first step is to ensure the PIX isn't mistakenly listening on ports previously identified. Then the networks behind the firewall are tested to see if we find any hosts or open ports.

We will go through the firewall to various networks trying to ping any hosts on another network. Nmap is a useful tool to accomplish this task.

For any host we do find using nmap or decide to add to our list since we do know the active ones, we will attempt to gather more information using nmap, nessus, nslookup, telnet, Sam Spade.

Audit Tools

The auditing software will be run on two or three laptops, which will allow them to be connected to various locations on the network to gather information.

We will also take advantage of the Real Secure IDS boxes in the network along with the Syslog files to detect and analyze traffic.

The actual software used in the audit is readily available from various web sites as shareware or open source with each having certain network analyzing abilities we can take advantage of. Nmap will scan the firewall by passing packets through it from a laptop PC on one side to another one on the other side. Nessus will examine the firewall and provides a report on any vulnerabilities. Sam Spade is used to initiate a DNS zone transfer so we can test the zone transfer drop rule. Firewalking will be employed as we attempt to map the firewall using Hping2, which we will use to craft ICMP error messages.

Scanning Tool	Type of Scan
Nmap	Port Scan
Nessus	Denial of service attack
Hping2	TTL-ICMP error message
Sam Spade	TCP DNS Zone
tcpdump	Network Sniffer
Bindview Internet Security	Vulnerability scan and DOS

nmap (www.insecure.org/nmap)

Nmap was the first software tool selected since it seems to be the most prevalent network security scanner used by network security people and hackers alike. The nice thing about nmap is that it "uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and

dozens of other characteristics."[34] Nmap has some great features and explains in its manual page that nmap is "*Nmap* is designed to allow system administrators and curious individuals to scan large networks to determine which hosts are up and what services they are offering. N*map* supports a large number of scanning techniques such as:

UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, IP Protocol, and Null scan. Nmap also offers a number of advanced features such as remote OS detection via TCP/IP fingerprinting, stealth scanning, dynamic delay and retransmission calculations, parallel scanning, detection of down hosts via parallel pings, decoy scanning, port filtering detection, direct (non-portmapper) RPC scanning, fragmentation scanning, and flexible target and port specification."

This tools offers more than enough features to test the GIAC PIX firewall, but it always nice to have lots of choices! Nmap will be used to find open ports which it does by sending various types of TCP, UDP and ICMP packets with numerous combinations of TCP flags, ICMP types options set. We will also try the OS detection against the PIX to see if nmap can fingerprint our firewall. It should be noted that nmap can be run as non-root and root but many critical kernel interfaces like raw sockets require root privileges (but make sure not to be setuid root).

Below is a table of the options and a description of the purpose of each option: (from the nmap manual page)

Options	**Explanation**
sS	TCP SYN scan: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets. This is the default scan type for privileged users. – **This scan is not usually caught by TCP Wrappers, but we expect the firewall to detect them.**
sT	TCP connect() scan: This is the most basic form of TCP scanning. The connect() system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable. One

[34] **Insecure.org., "Nmap" 12 Nov 2001 URL:http://www.insecure.org/nmap/ (8 Oct 2002)**

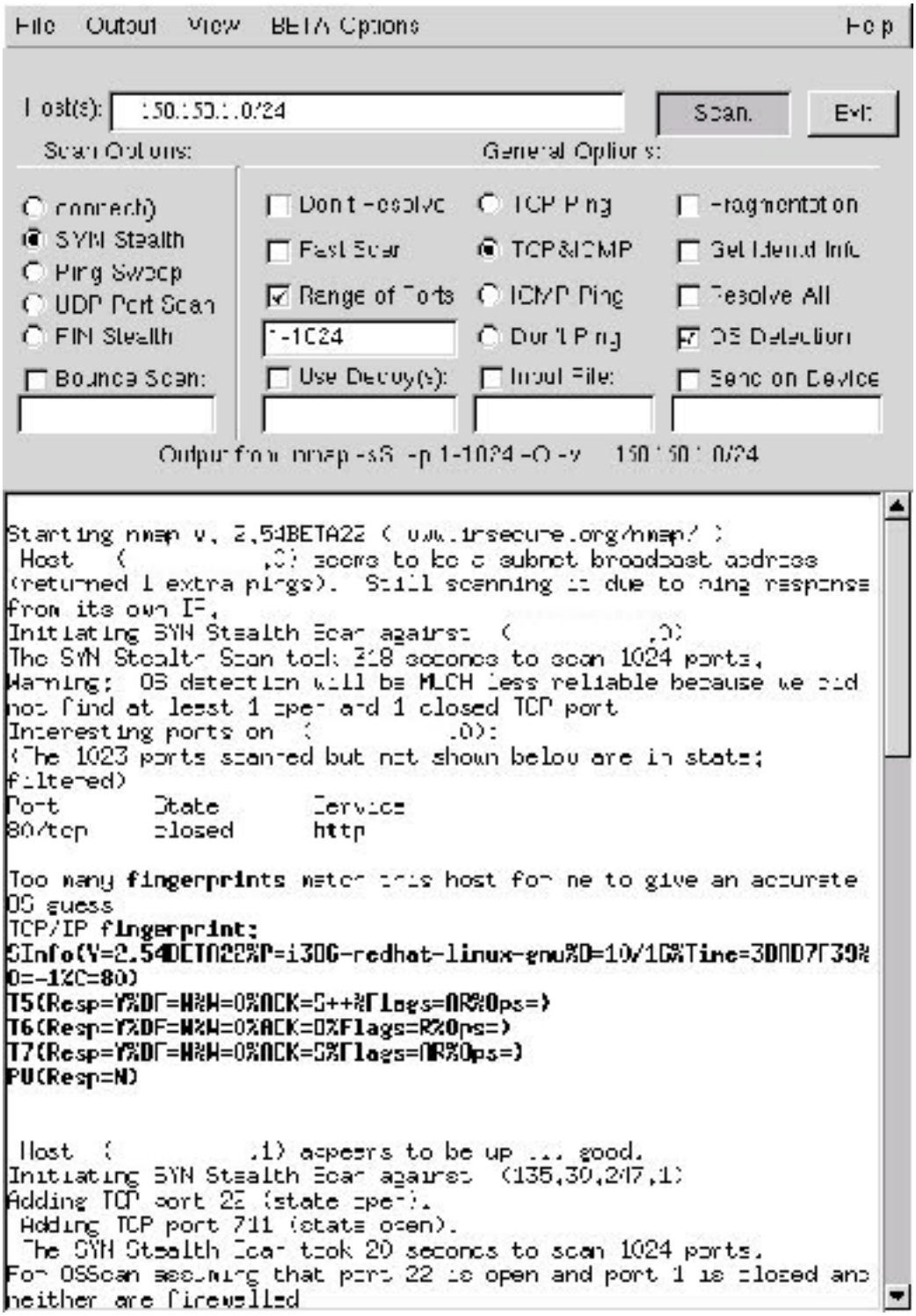
	strong advantage to this technique is that you don't need any special privileges. Any user on most UNIX boxes is free to use this call. This sort of scan is easily detectable as target host logs will show a bunch of connection and error messages for the services which accept() the connection just to have it immediately shutdown. This is the default scan type for unprivileged users.
sF -sX	Stealth FIN, Xmas Tree, or Null scan modes: There are times when even SYN scanning isn't clandestine enough. Some firewalls and packet filters watch for SYNs to restricted ports, and programs like Synlogger and Courtney are available to detect these scans. These advanced scans, on the other hand, may be able to pass through unmolested. The idea is that closed ports are required to reply to your probe packet with an RST, while open ports must ignore the packets in question (see RFC 793 pp 64). The FIN scan uses a bare (surprise) FIN packet as the probe, while the Xmas tree scan turns on the FIN, URG, and PUSH flags. **TCP FIN scan (-sF) might be able to get through undetected by firewall if the firewalls don't properly filter this type of scan.** **TCP FIN URG PUSH (-sX) scans again might not be properly filtered**
sP	Ping scanning: Sometimes you only want to know which **hosts on a network are up**. Nmap can do this by sending ICMP echo request packets to every IP address on the networks you specify. Hosts that respond are up. Nmap can also send a TCP ack packet to (by default) port 80. If we get an RST back, that machine is up. A third technique involves sending a SYN packet and waiting for a RST or a SYN/ACK. For non-root users, a connect() method is used. By default (for root users), nmap uses both the ICMP and ACK techniques in parallel though you have the option to change this. Note that pinging is done by default anyway, and only hosts that respond are scanned. **Only use this option if you wish to ping sweep without doing any actual port scans.**
sU	UDP scans: This method is **used to determine which UDP ports are open on a host**. The technique is to send 0 byte udp packets to each port on the target machine. If we receive an ICMP port unreachable message, then the port is closed. Otherwise we assume it is open. Some people think UDP scanning is pointless, but a Solaris rcpbind hole shows the scans value. Rpcbind can be found hiding on an undocumented UDP port somewhere above 32770. So it doesn't matter that 111 is blocked by the firewall. But can you find which of the more than 30,000 high ports it is listening on? With a UDP scanner you can!

	There is also the cDc Back Orifice backdoor program that hides on a configurable UDP port on Windows machines. Not to mention the many commonly vulnerable services that utilize UDP such as snmp, tftp, NFS, etc. **This scan can produce false positives if ports are packet filtered.**
-sA	ACK scan: This advanced method is usually **used to map out firewall rulesets**. In particular, it can help determine whether a firewall is stateful or just a simple packet filter that blocks incoming SYN packets. This scan type sends an ACK packet (with random looking acknowledgement/sequence numbers) to the ports specified. If a RST comes back, the ports are classified as "unfiltered". If nothing comes back (or if an ICMP unreachable is returned), the port is classified as "filtered". Note that *nmap* usually doesn't print "unfiltered" ports, so getting no ports shown in the output is usually a sign that all the probes got through (and returned RSTs).
-P0	Nmap **won't ping a host to see if it's alive before scanning it**. Useful if the firewall filters out normal ping traffic.
-O	Nmap tries to **determine the operating system running** on the target host.
-f	This option causes the requested SYN, FIN, XMAS, or NULL scan to use tiny fragmented IP packets. The idea is to split up the TCP header over several packets to **make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing**.
-v	Verbose mode. Provides more information. Use it twice for greater effect!
-p < >	Use only these ports or port ranges for scanning
-oN	Log results to a human readable form
-oX	Logs results into grepable form

A list of ports scanned is provided by nmap once the scan is completed. The list will include the port's "well known" service name, number, protocol and state. The various states are 'open' meaning the port will accept connections, 'filtered' for ports that namp can't determine if they are open due to a firewall, filter or some other network obstacle. 'Unfiltered' results show that ports known to be closed by nmap and no firewall or filter is blocking nmap's attempts to determine this.

The following screen shot shows the nmap gui-frontend (nmapfe) with the target host inputted (GIAC.org network) while the scan results are from an actual live network scan with the IP addresses blocked. The output is intended to show the type of information provided by nmap. Notice nmap will state the scan used, how long it took to perform the scan on the

selected ports, and how reliable the OS detection will be. A nice feature is the listing of interesting ports, their state and the service running on that port. While nmap doesn't always determine what OS is running on the host, it provides an output of its scan results that can be added to its library. So if you know the target was a PIX firewall then these results could be put into the library labeled as such. So when another scan is done it will have this new information to use to try to match up the scan results with its library information.



Nessus (www.nessus.org)

Nessus is a tool like nmap that probes for services listening on a device, but Nessus also has the ability to detect what kind of server is running on that port.

Nessus utilizes an up-to-date security vulnerability database that is updated daily and has a client-server architecture. The Nessus Security Scanner is made up of two parts: a server, which performs the attacks, and a client, which is the frontend or the server and the client on different systems. That is, you can audit your whole network from your personal computer, whereas the server performs its attacks from the main frame located somewhere else: one for X11, one for Win32 and one written in Java.

This tool can be configured as **Non-destructive**: If you don't want to take the risk to bring down services on your network, you can enable the "safe checks" option of Nessus, which will make Nessus rely on banners rather than exploiting real flaws to determine if a vulnerability is present.

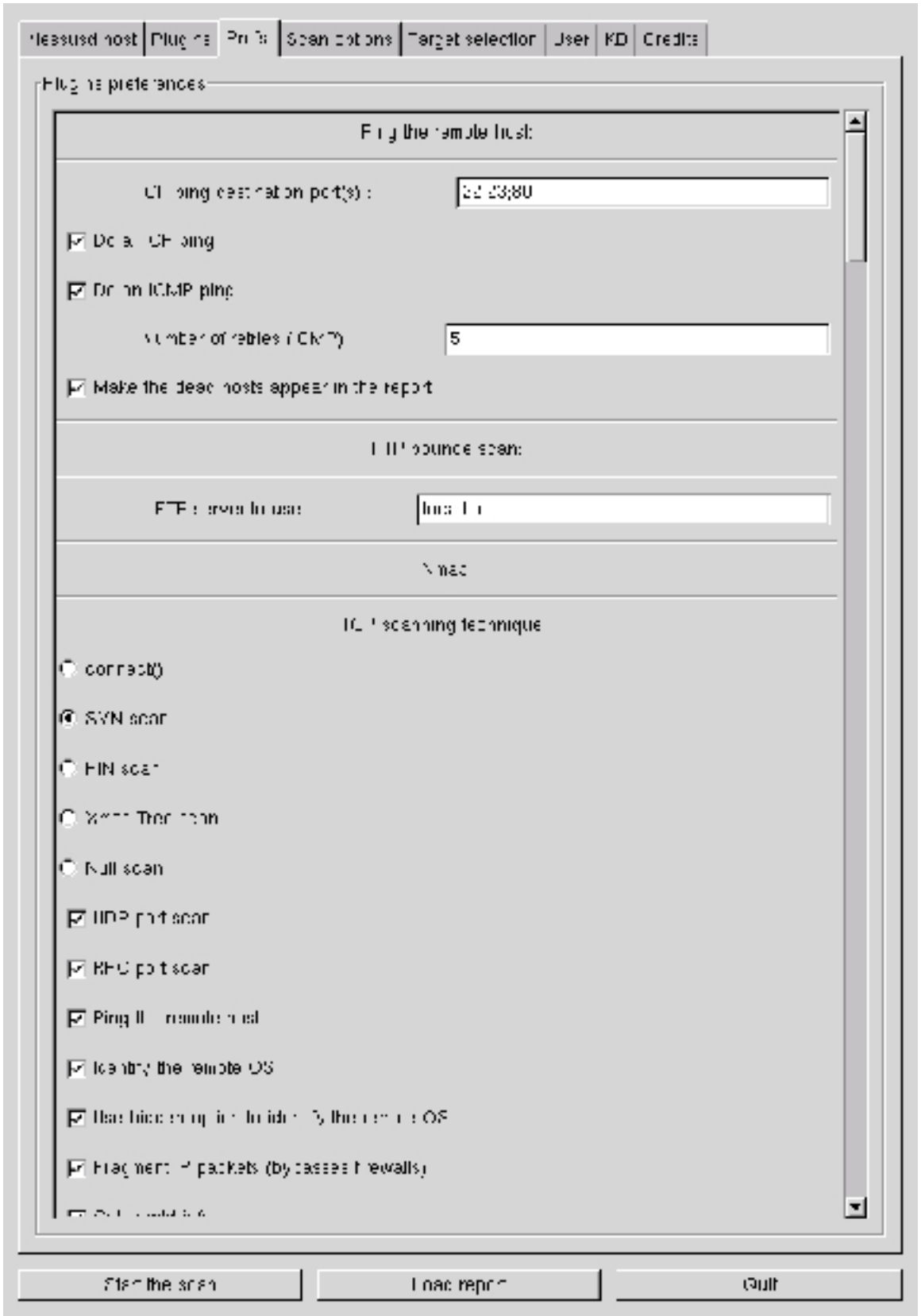
Nessus provides **Full SSL support**: Nessus has the ability to test SSLized services such as https, smtps, imaps, and more. You can even supply Nessus with a certificate so that it can integrate into a PKI-fied environment.

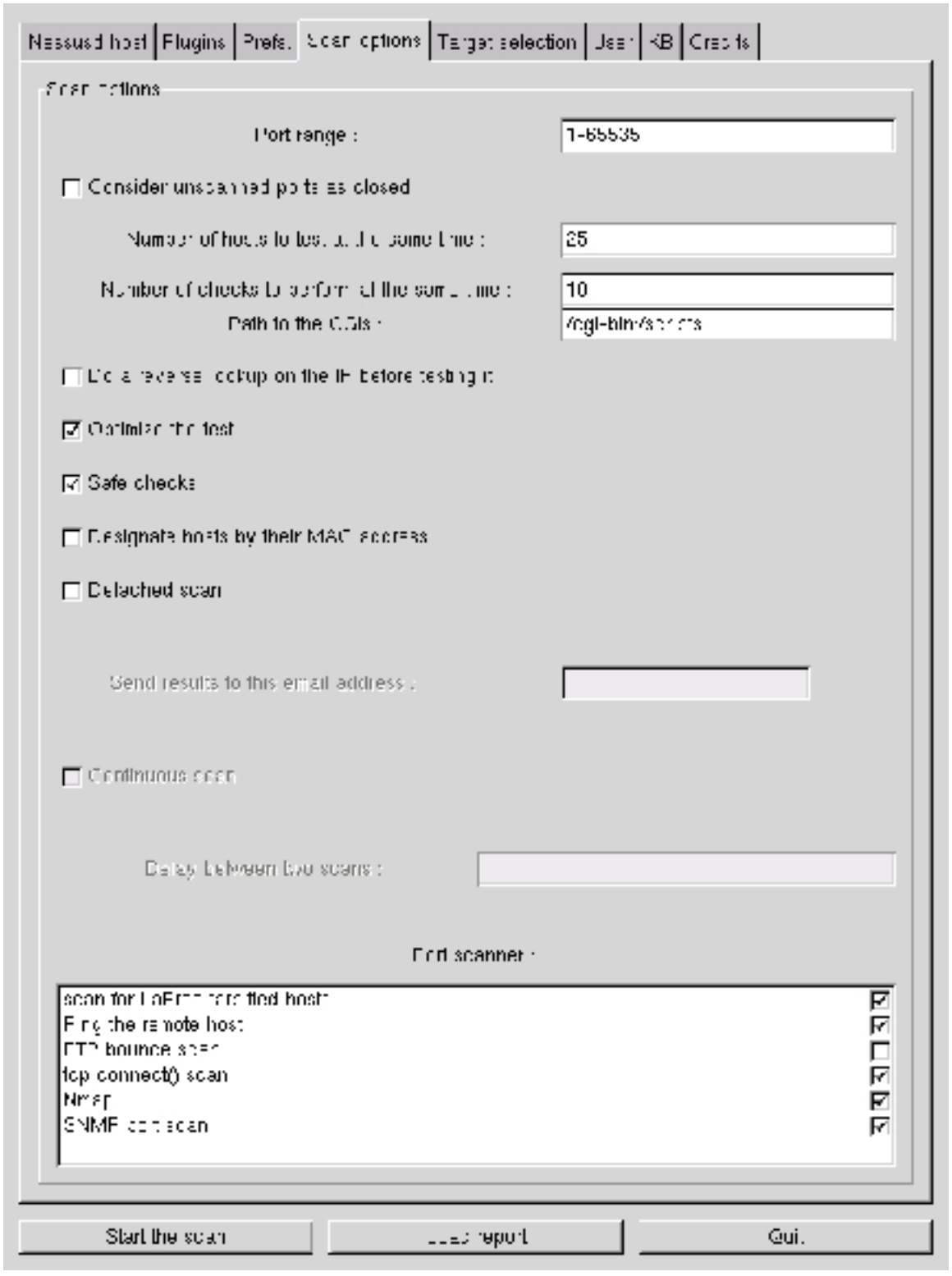
Nessus provides reports that tell not only what's wrong on with the network, but will, most of the time, tell how to prevent crackers from exploiting the security holes found and will give you the risk level of each problem found (from *Low* to *Very High*)

Lastly, Nessus' reports are exportable. The Unix client can export Nessus reports as ASCII text, LaTeX, HTML, "spiffy" HTML (with pies and graphs) and an easy-to-parse file format.

For those interested in seeing the full list of checks Nessus executes by default, go to http://cgi.nessus.org/plugins/dump.php3

It's interesting to note that Nessus actually uses nmap to scan for open ports.

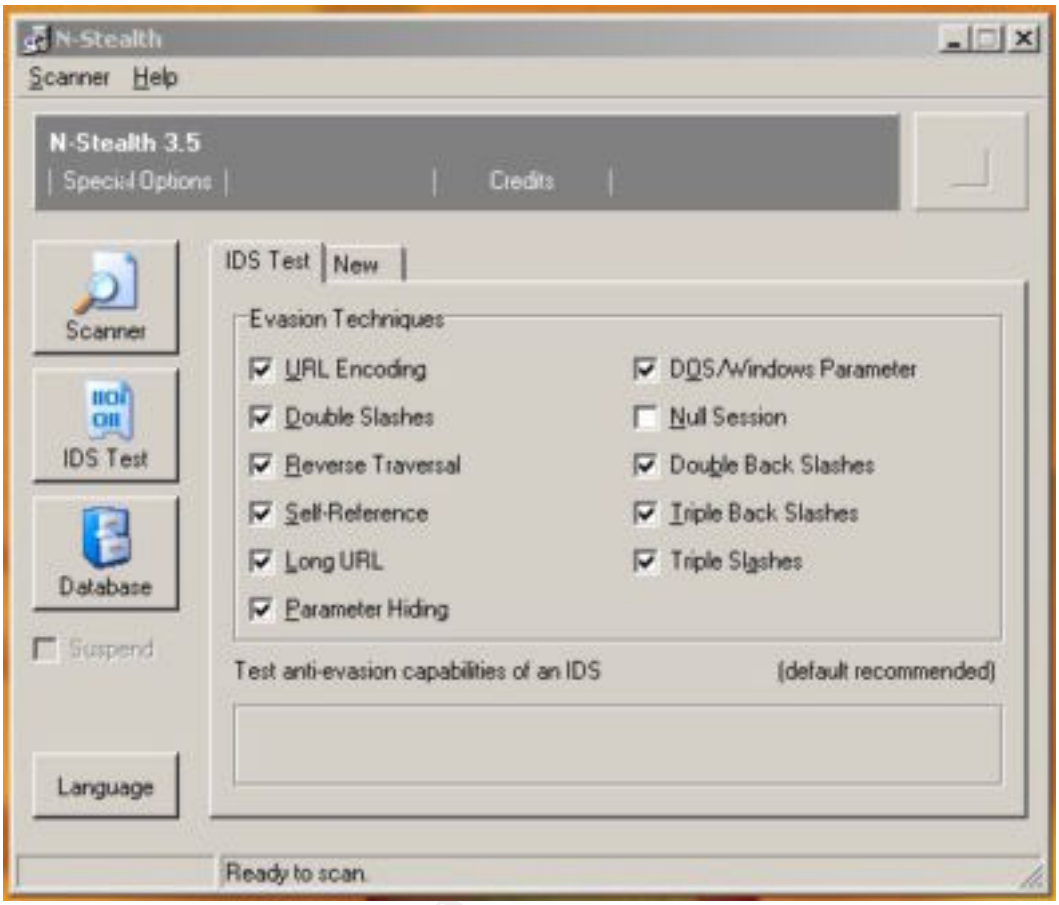




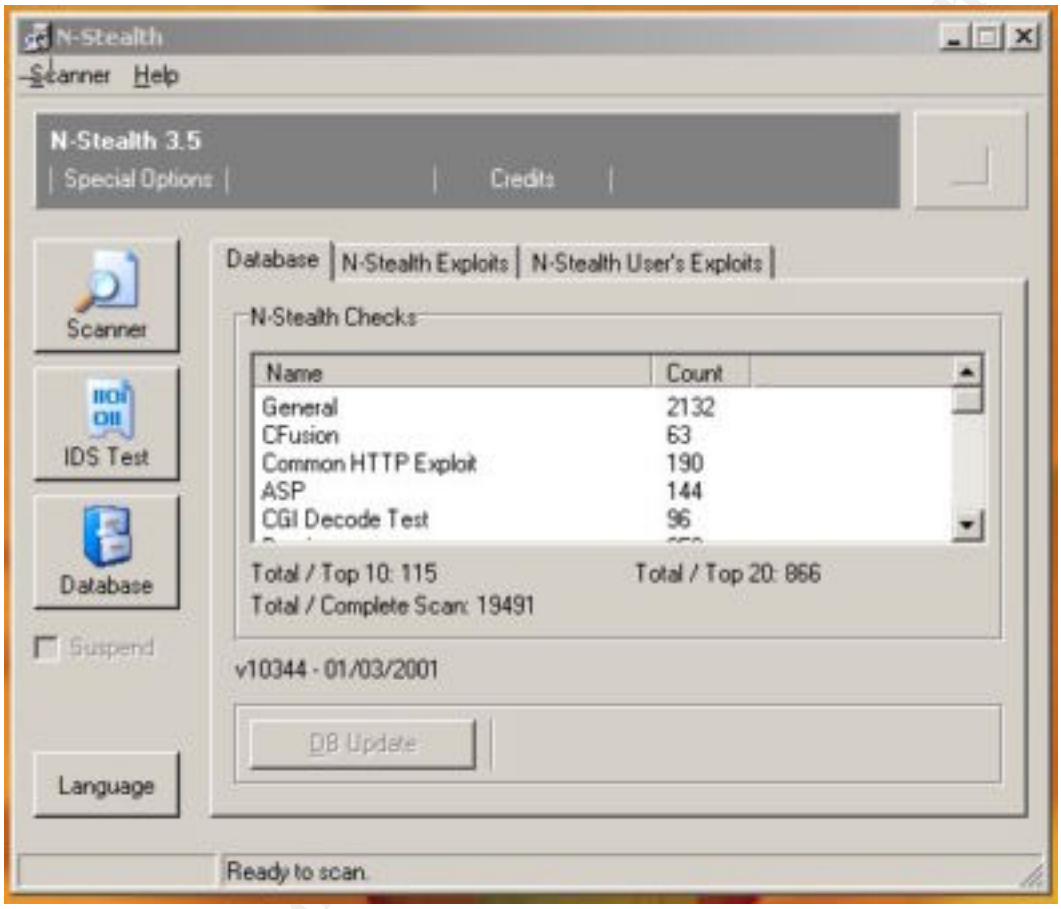
N-Stealth 3.5 Build 62 (www.nstalker.com/nstealth)

N-Stealth was selected to perform a vulnerability assessment against the web servers to help identify security problems and other weaknesses, which could allow unauthorized privileged access to these servers. N-Stealth can do over 19,000 vulnerability checks, be alerted for new checks added to the database and a scan rule option (bottom right in picture below) that scans all vulnerabilities, top 10 or top 20 SANS/FBI holes. Nessus also has this ability but having tools that have overlapping capabilities is seen as a good thing since this will help reinforce the results. N-Stealth is Windows based and can be installed and up and running in minutes while Nessus will take some time to install. Nessus will return at times false positives that can be certainly annoying, but N-Stealth has the ability to filter false positives.

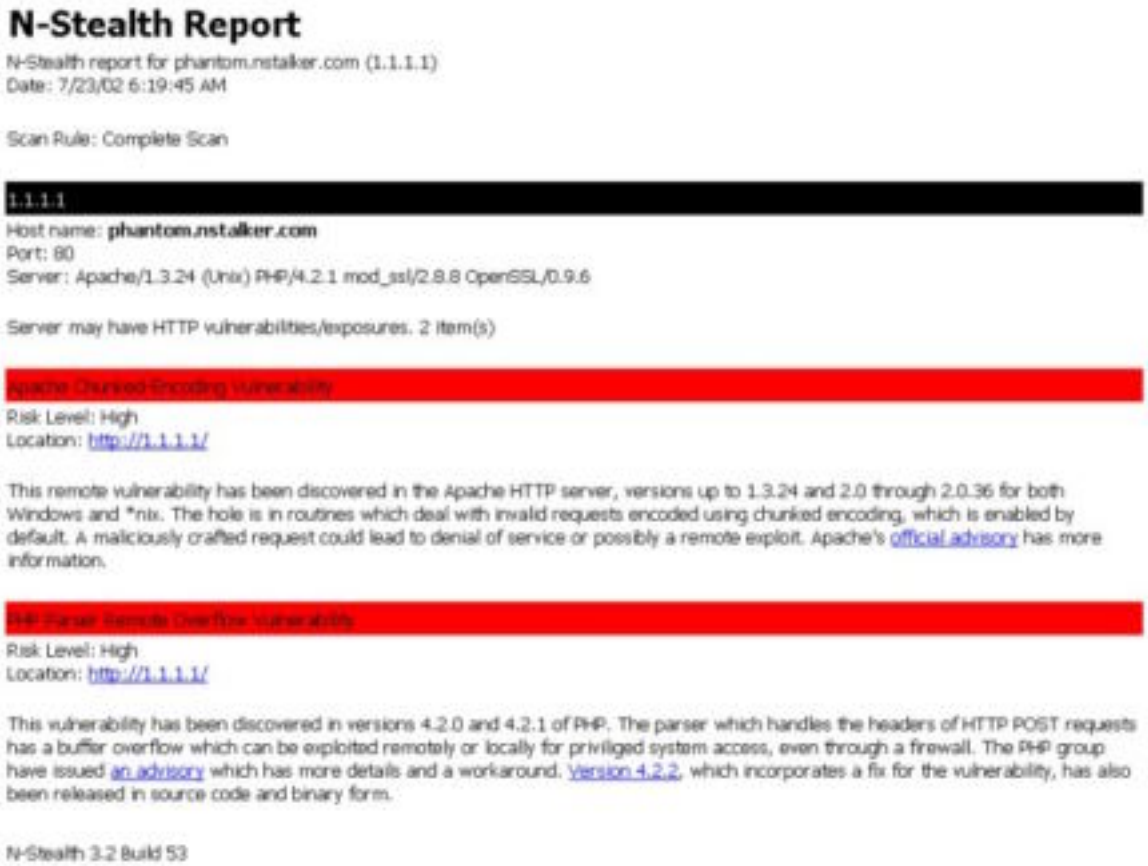
N-Stealth has multiple IDS Test evasion techniques allowing for a quite comprehensive test.



The Database screen shows all the vulnerabilities that N-Stealth checks and how many vulnerabilities are associated with each. By clicking on the "DB update" button, you can ensure the software has the latest checks, which increase 5-10 per day.



Below is a sample report from N-Stealth. The report provides the vulnerabilities detected along with the risk level of the vulnerability. The explanation of the vulnerability helps the user understand the problem, which version of OS it affects and a location and/or a newer OS that fixes this vulnerability.



N-Stealth Report

N-Stealth report for phantom.nstalker.com (1.1.1.1)
Date: 7/23/02 6:19:45 AM

Scan Rule: Complete Scan

1.1.1.1

Host name: **phantom.nstalker.com**
Port: 80
Server: Apache/1.3.24 (Unix) PHP/4.2.1 mod_ssl/2.8.8 OpenSSL/0.9.6

Server may have HTTP vulnerabilities/exposures. 2 item(s)

Apache Chunked-Encoding Vulnerability

Risk Level: High
Location: http://1.1.1.1/

This remote vulnerability has been discovered in the Apache HTTP server, versions up to 1.3.24 and 2.0 through 2.0.36 for both Windows and *nix. The hole is in routines which deal with invalid requests encoded using chunked encoding, which is enabled by default. A maliciously crafted request could lead to denial of service or possibly a remote exploit. Apache's official advisory has more information.

PHP Parser Remote Overflow Vulnerability

Risk Level: High
Location: http://1.1.1.1/

This vulnerability has been discovered in versions 4.2.0 and 4.2.1 of PHP. The parser which handles the headers of HTTP POST requests has a buffer overflow which can be exploited remotely or locally for priviliged system access, even through a firewall. The PHP group have issued an advisory which has more details and a workaround. Version 4.2.2, which incorporates a fix for the vulnerability, has also been released in source code and binary form.

N-Stealth 3.2 Build 53

Sam Spade (www.samspade.org/ssw/)

Sam Spade for Windows is a freeware network query tool that has quite a number of features that we can use in addition to the tools mentioned earlier. We will use it to try to perform a DNS zone transfer, and a dig. The zone transfer request asks a DNS server for all the information it has about a domain. It automatically finds the authoritative servers for a domain and will query one or all of them. A dig is a more advanced DNS query tool. Dig asks a DNS server for all the information it has about a host.

tcpdump (www.tcpdump.org)

tcpdump is a network sniffer which is used to capture traffic on the network while we are actively probing. This tool will allow us to examine the packets later to determine if the firewall failed to block packets that were denied in our rule set or ACLs.

Conducting the Audit

Auditing from the Internet

All listening services on the PIX firewall have been disabled and even though it is a hardware based OS and therefore more hardened against attack versus others which are software based running on top of an operating system, we will treat as a software based one for testing purposes. It came as no surprise that scans against the PIX IP address found no ports in listen mode.

We then tried to connect to any hosts located on the Service Network. Scanning the addresses provided the following boxes and ports:

Device Found	Listening Ports
Proxy Web Server	TCP 80 (HTTP) & 443 (SSL)
Mail Server	TCP 25 (smtp)
DNS Server	TCP & UDP 53 (Domain)
Database Server	TCP 22 (SSH)

Now knowing that those services are available, we try to determine the OS, which could be then exploited if vulnerabilities exist for that type of OS. We use nmap using the OS-detection option, but the firewall blocks these attempts. Responses received back are actually from the firewall as port filtered – we never make it to the target hosts. This means that any UDP scans aren't trustworthy since we don't make it to the targets, which is a positive sign that our rule sets are working.

We also review the Syslog data that came from our firewall and see that our scanning has been detected and logged, just as expected.

Web Server Scan

Nessus is used against the web server to try to determine what it is running and its version of OS. If Nessus can determine this it can then check its database of vulnerabilities. Since we have setup the web server to respond to such queries with a version obscuring string, Nessus won't have accurate information therefore thwarting this type of attack against our web servers. Nessus might determine we are using Linux on the servers, which is a hardened version from the NSA, but that is all it was able to find out.

DNS Server Scan

The next target is our DNS server, which is listening on port 53. Sam Spade is run against the DNS server to try to get it to do a zone transfer.

10/17/02 11:36:10 Zone transfer giac.com@150.150.1.69
Zone transfer giac.com@150.150.1.69 ...
Query refused. Nameserver won't talk to me for policy reasons

We also run dig to see if we can get the server to perform a transfer. The results looked like this:

$dig giac.com axfr
;<<>>DiG 9.1.3 <<>>giac.com axfr
;;global options:printcmd
;Transfer failed.

Lastly, running a DNS-specific scan using Nessus against the server resulted in the version obfuscation feature we setup earlier defeating Nessus effort to perform some checks against the server.

Mail Server Scan

The mail server is vulnerable to exploitation from the outside if the commands VRFY and EXPN are allowed. These commands are used to validate an address and accepting mail and also to expand aliases. If these commands were allowed a hacker could learn what are the valid email addresses at GIAC and could provide useful to employ some social engineering. As an additional layer of protection, the firewall filters inbound connections to the mail server to allow through only MAIL, RCPT, HELO, DATA, NOOP, RSET, and QUIT commands.

Past PIX firmware versions up to 6.0 were found to have vulnerabilities in this type of filter. Cisco has addressed this problem in 6.1, which we are running, but we will still test to make certain this is indeed the case.

This vulnerability will be tested with Nessus but we also want to test manually just ensure Nessus might miss it. We telnet to port 25 of the mail server and issue an EXPN command to expand the “all” alias, but get back a “500 command unrecognized”. Checking our logs we see that this error message is coming from the PIX versus the mail server and that a denied query was indeed logged. So it seems like the vulnerability has indeed been fixed. As an added layer of protection, the mail sever was configured to not relay messages so attempts to send mail from an outside account to another fail.

Oracle Database

Scans of the service network found the SSH port open for the database but we alerted the query responses the server might send out. The scan results show that this is indeed the case and since we are using the hardened OS from the NSA, the scans found no vulnerabilities.

VPN Server

Scanning the VPN server from the Internet requires the probes to pass through the router ACL and the PIX firewall rule set. The VPN device is detected by the scans since we do allow valid connections to it but any packets intended to actively probe the VPN are blocked. So the two levels of security eject probes of UDP port 500 on the VPN IP address.

Auditing from the Service Network

We want to test our rules to ensure only approved connections that initiate from the service network out to the Internet and other networks of the GIAC network occur. The test laptop that is given an IP address available in the service network is connected on the service network to a port on the switch which we'll enabled since all unused ports have been previously disabled for security reasons.

The first audit will be to the GIAC networks behind the Firewall. We've blocked most connections that initiate from the area, but we do see one types still occurring. This connection is to the internal Syslog server on UDP port 514. This is an expected and allowed event and shows that our Syslog functions are working properly.

Now what about connections out to the Internet? To confirm that we have restrictions in place by trying to telnet to a known mail server, FTP server and to SSH to a system provided by the external auditors. Then we attempt to access the Web, which should be the most likely service we could have access to. Results from the PIX and Syslog server show all attempts were blocked by the PIX.

The audits perform next require the replacement of the devices in the service network with the test laptop.

Mail Server

First we took the mail server and replaced it with laptop, which will perform the scanning so it in effect becomes the mail server. We then test to see what hosts the server can access on TCP port 25. From the results we

see that the server can access any host on the Internet but internally only the Syslog server on UDP port 514 and the GIAC internal mail server on TCP port 25. This is the correct and expected results given what we have setup in our firewall rule sets.

DNS Server

For the DNS server we did the same procedure as with the mail server and then tried to access hosts on the Internet using TCP & UDP port 53. This like the mail server tested showed it was possible so then we looked inward. We would have been concerned if the DNS server was able to access our internal DNS so it shouldn't, but we were glad to see that access to the internal DNS was blocked again by the Firewall. Only access to the Syslog server was allowed.

Oracle Database

For this test we want to ensure that the server can't initiate any Internet- or internal-bound connections. The only inbound connections should be SSH from our Partners and Suppliers and the selected few internal users who retrieve new fortune sayings from the server. The web server is allowed to access the database but we locked down the IP addresses so only the web server and the internal database server can access it on TCP port 1521 (SQLNET). We'll blocked access to all Internet & internal devices from the server with the firewall so scans don't produce any results.

Web Server

When auditing the external web server, the scans showed that it couldn't initiate any Internet-bound connections while it could talk to the external Oracle Database on TCP port 1521 for SQLNET traffic and the Syslog server.

Auditing from the VPN

Since we are using a "/30" subnet for the connection between the firewall and the VPN, we don't have any other IP addresses to use like we did on the service network. So we will replace the VPN with our laptop to perform the scans.

The first scan will be towards the Internet using all the various service ports (i.e. SSH, Telnet, FTP, Web, etc.). Then the scans are directed to the internal GIAC network.

From these scans we found that access out wasn't allowed to the Internet but packets could go to the internal NTP server and Syslog server.

Auditing from the Internal Network

The audits will try to access the hosts on the service network, and then the Internet. We also want to ensure only the selected users can access the internal and external database servers. Not everyone requires access to these servers. Since the employees haven't been complaining about their access, it could be assumed that things work properly. But since one of the reasons for doing an audit is to reinforce our security implementations, it clearly makes sense to be safe and run our checks.

All users can access the web server, which comes as no surprise. But attempts to the database server fail except for the few users that have permission in the access list. If we replace the internal mail server with our scanner, it is only able to connect to the external mail server on port 25 and not to the Internet or VPN. The internal DNS server could only initiate connections with hosts on the Internet on either TCP or UDP port 53.

Auditing from the Management Network

The management network has the NTP server and Syslog server locate in it plus the IS people will use SSH to connect to other hosts in the GIAC network for servicing.

The NTP server is able to connect with the NTP servers that were identified earlier in the access list (216.27.190.202 & 207.126.97.57) using port UDP port 123. The Syslog server won't "pull" information from other devices but instead receives information so we don't see any successful connections initiating from the server.

Evaluate the Audit

Firewall Performance

The firewall rule sets and access lists did a good job at controlling whether to allow or deny packets from entering or leaving the GIAC network. One area to correct is the performance of the firewall in terms of the location the rules in the lists. We noticed that the rules for the external web server were mistakenly put lower than the VPN, which had few connection requests. Also, DNS request were quite high but less the web server ones

so it should be placed below it in the list. Since the PIX will go through the access list until it finds a match, if possible, it's best to put the most frequently used rules at the top of the list.

CISCO PIX Vulnerabilities

Arguably the most important piece of the GIAC network in terms of security is the PIX firewall so we want to be sure that it is as secure as possible. Therefore we want to examine websites for the latest vulnerabilities to make sure that the latest patches are installed.

We reviewed SecurityFocus' database for the latest information:

http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

For the PIX 515 Firewall there were two notable vulnerabilities:

Cisco SSH Denial of Service Vulnerability[35]

Discussion:
"While addressing vulnerabilities described in http://www.cisco.com/warp/public/707/SSH-multiple-pub.html, a denial of service condition has been inadvertently introduced into firmware upgrades. Firmware for routers and switches (IOS), Catalyst 6000 switches running CatOS, **Cisco PIX Firewall** and Cisco 11000 Content Service Switch devices may be vulnerable.

Solution:
Cisco has reported that scanning for SSH vulnerabilities on affected devices will cause excessive CPU consumption. The condition is due to a failure of the Cisco SSH implementation to properly process large SSH packets.

Repeated and concurrent attacks may result in a denial of device service. As many of these devices are critical infrastructure components, more serious network outages may occur.

Cisco has released upgrades that will eliminate this vulnerability."

From the Cisco Web site:

[35] **SecurityFocus Online, "**Cisco SSH Denial of Service Vulnerability"
URL:http://online.securityfocus.com/bid/5114 (21 Oct 2002)

Security Advisory: Scanning for SSH Can Cause a Crash

http://www.cisco.com/warp/public/707/SSH-scanning.shtml#Software

The firmware versions affected includes version 6.2 which we have on our PIX but the vulnerability is for the ED (Early Deployment). We, as a company policy, don't go "bleeding-edge" and wait until the GD (General Distribution) is available. So having the 6.2(1) maintenance release fixes this vulnerability. We have 6.2.2.

Cisco IOS Malformed SNMP Message Denial of Service Vulnerabilities[36]

Discussion:
"Cisco products contain multiple vulnerabilities in handling of SNMP requests and traps. A general report for multiple vendors was initially published on February 12 (Bugtraq IDs 4088 and 4089), however more information is now available and a separate Bugtraq ID has been allocated for the Cisco IOS vulnerabilities.

It is reportedly possible for a remote attacker to create a denial of service by transmitting malformed SNMP packet to a device running a vulnerable version of IOS. The affected device may reset, or (under rare circumstances) require a manual reset to regain functionality.

The nature of this denial of service conditions is not known. They may be due to exploitable buffer overflow conditions."

Solution:
Cisco has released firmware upgrades.

Cisco provided various fixes for vulnerability:
http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtml

Product	Defect ID	Intended First Fixed Releases*
PIX	**CSCdw63021, CSCdw75833**	**4.4(9), 5.2(8), 5.3(4), 6.0(3), 6.1(3) (available 2002-02-28)**

Again, the PIX 515 is using firmware version 6.2.2 so the vulnerability doesn't exist for this particular version.

[36] **SecurityFocus Online, "**Cisco IOS Malformed SNMP Message Denial of Service Vulnerabilities" **URL:http://online.securityfocus.com/bid/4132/info/ (22 Oct 2002)**

General Information:

SNMP on the PIX is DISABLED by default, and warning messages are displayed to the administrator when SNMP is configured to listen on the OUTSIDE interface. [writer's note – SNMP is disabled on the GIAC network PIX]

SNMP is enabled on the PIX when the Firewall administrator enters the snmp-server ... command.

The PIX is not vulnerable if the PROTO test suite is run from a server whose IP address is not explicitly defined in the snmp-server host command. The results of current testing show that the PIX is only vulnerable if SNMP data is received from a host defined in the snmp-server host ... command.

Please review the configuration of your PIX and make sure that each of the IP addresses listed in the snmp-server host ... command is a legitimate SNMP host. Customers should review configuration for lines such as the following: *snmp-server host outside ip-address* which would permit SNMP queries from the unprotected interface. If they find these commands in the configuration, they should carefully evaluate the necessity for them and the protection offered by other devices upstream to ensure that spoofing of the SNMP host cannot take place.

Best Practices:

Firewall Administrators should evaluate their site security policy and consider implementing SNMP egress filtering (deny UDP port 161 and 162 and TCP and UDP ports 1993) on the PIX Firewall. If your organization does not manage any device that is not on your network, you may want to consider blocking SNMP at your Internet Firewall so that future SNMP exploits cannot be launched from your network.

Change the snmp-server community string to something else other than "public".
snmp-server community somethingotherthanpublic

Workarounds:

Disable SNMP. You can do this by removing all snmp-server host commands.
no snmp-server host inside ip-address
no snmp-server host inside ip-address
no snmp-server location

no snmp-server contact
no snmp-server community public
no snmp-server enable traps
Note: Other PIX SNMP commands including the snmp-server community may still appear in the PIX configuration after the no snmp-server host ... command has been executed.

While going through the Cisco web site we found Cisco software caveats for version 6.2.2. We noted some items that are known bugs or problems with the software with no fix action available:

CSCdw0435 – PIX authentication is vulnerable to incomplete authentication

CSCdv91040 – Slow response to write mem command when heavy traffic load

CSCdx85168 – When you type show ssh session in your browser you fail to get debug

CSCdx91760 – Reload hangs PIX515. This is after upgrading new bupgisk.[37]

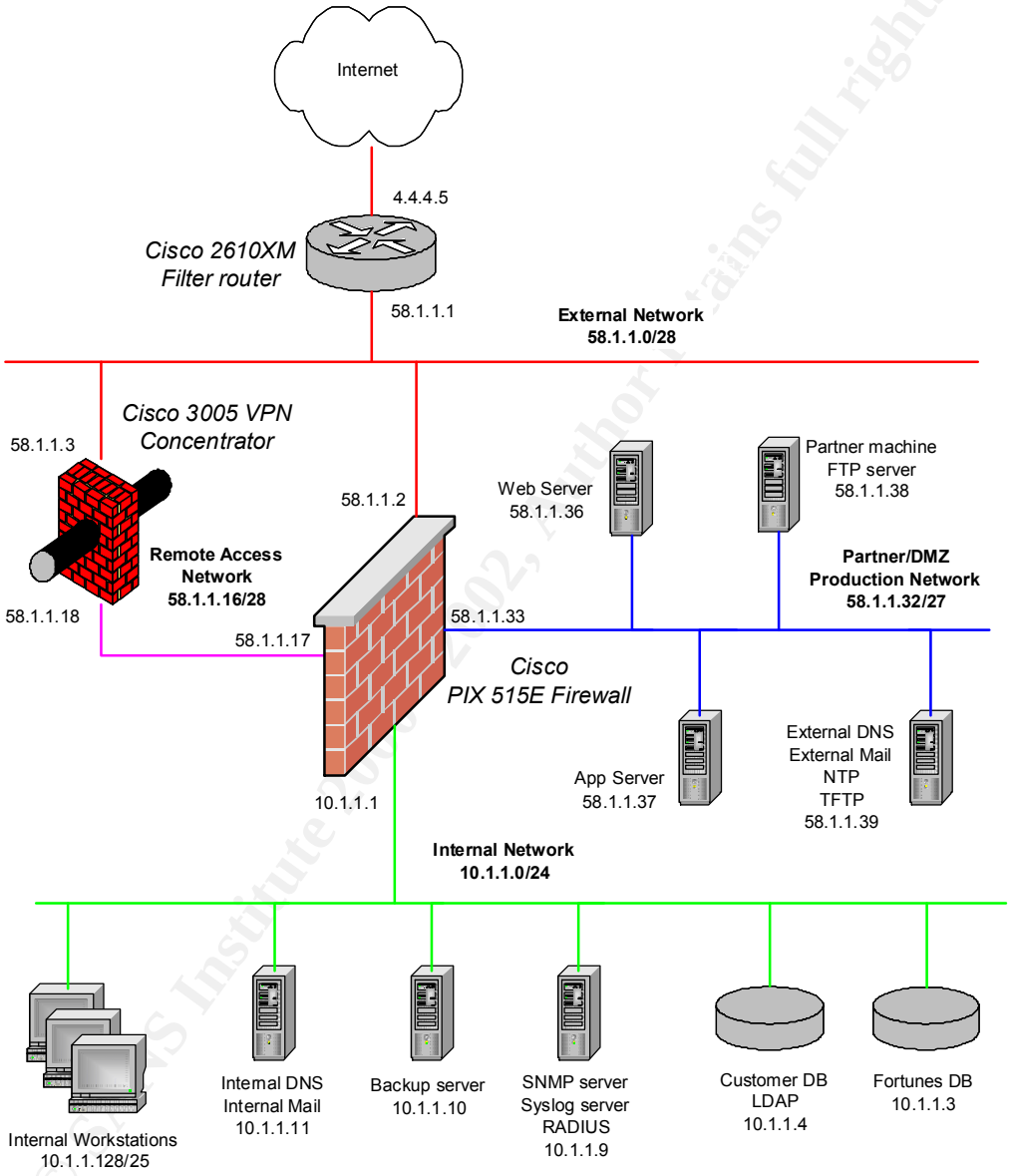
The point of these items is to examine these caveats when you notice problems with the PIX. Many times you might think the problem you are experiencing is due to user error, but by looking at the database of known problems, the problem might be found there.

One item came to light from the audit, which is the need to ensure security people are on a mailing list for bug alerts. When vulnerabilities are found with equipment, which is also used on the GIAC network, multiple people should receive an automatic alert. This does two things: it ensures that if a person is "out-of-pocket" that someone else will also receive the message. Also, an automatic alert ensures timely fixes to the software so the amount of time the network might be vulnerable to attack is limited.

[37] **Cisco Corp., "**Cisco PIX Firewall Release Notes Version 6.2(2)**"**
URL:http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note09186a00800b1138.html **(21Oct 2002)**

Assignment 4 - Design Under Fire

The design selected for this assignment is the practical by Steve Keifling submitted on June 5th, 2002.[38]



Attack Against the Firewall

Before attacking the Cisco PIX 515E Firewall a search of known vulnerabilities is done at SecurityFocus Online (http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl).

[38] **Steve Keifling GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.7 URL:www.giac.org/practical/Steve Keifling_GCFW.zip (22 Oct 2002)**

As mentioned earlier in the practical, Cisco along with many other vendors released an advisory in February '02 concerning the SNMP vulnerabilities, which was found in most of their networking products.

The last updated advisory, 2002-04-02, details the vulnerability and its impact:

Detail:

> SNMP defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network.
>
> There are three general types of SNMP operations: "get" requests to request information, "set" requests which modify the configuration of the remote device, and "trap" messages which provide a monitoring function. SNMP requests and traps are transported over User Datagram Protocol (UDP) and are received at the assigned destination port numbers 161 and 162, respectively.
>
> The largest group of vulnerabilities described in this advisory result from insufficient checking of SNMP messages as they are received and processed by an affected system. Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which may result in a system crash and reload (or reboot) in most circumstances. Some Cisco products may not reload but will become unresponsive instead. Some of the affected products are not directly vulnerable to malformed SNMP messages, but fail under extended testing or large volumes of SNMP messages due to memory leaks or other unrelated problems.

Impact:

> The vulnerabilities can be exploited to produce a Denial of Service (DoS) attack. When the vulnerabilities are exploited, they can cause an affected Cisco product to crash and reload.
>
> SNMP messages are transported using User Datagram Protocol (UDP) and are subject to IP source address spoofing which could be used to circumvent the access control mechanisms.
>
> If an attacker is able to guess or otherwise obtain a read-only community string for an affected device, then he or she could bypass SNMP access control relying on the community string.

The PIX OS versions that are vulnerable are versions through 5.3(3), 6.0(2) and 6.1(2). A simple fix is the disable SNMP or to ensure the SNMP packets' address isn't specifically listed in the "snmp host" command.

To test this vulnerability against the targeted PIX we could the exploit program written by kundera@tiscali.it. This program is written for a Cisco 2600 IOS 12.0(10) but can be used also against the PIX.

http://downloads.securityfocus.com/vulnerabilities/exploits/ciscokill.c

Of course this vulnerability won't work unless this criteria is met:

- Know the IP address of the firewall, or at least that of the network.
- The firewall must be running a vulnerable version of the OS.
- SNMP must be turned on.
- Have the IP address of the SNMP management host
- The router must allow SNMP packets spoofed as the SNMP management host.
- Know the SNMP community string.

Against Steve Keifling's design, we don't meet the second criteria since he is using OS 6.2(1), which isn't vulnerable to this exploit. Also the router's ACL would block spoofed internal IP addresses coming into the GIAC network from the Internet. So having depth of defense helps protect PIXs that might be vulnerable.

Denial of Service Attack

The GIAC network has only a T1 ISP network connection while we have at our disposal 50 cable modem/DSL systems, which can easily overwhelm that link. A favorite tool to produce the DDoS is TFN2K (Tribe Flood Network 2000). (http://packetstorm.decepticons.org/distributed)

The list of options for the program is as follows:

```
% ./tfn
usage: ./tfn <options>
[-P protocol]          Protocol for server communication. Can be ICMP, UDP or TCP.
                       Uses a random protocol as default
[-D n]                 Send out n bogus requests for each real one to decoy targets
[-S host/ip]           Specify your source IP. Randomly spoofed by default, you need
                       to use your real IP if you are behind spoof-filtering routers
[-f hostlist]          Filename containing a list of hosts with TFN servers to contact
[-h hostname]          To contact only a single host running a TFN server
[-i target string]     Contains options/targets separated by '@', see below
[-p port]              A TCP destination port can be specified for SYN floods
```

```
<-c command ID> 0 - Halt all current floods on server(s) immediately
                1 - Change IP antispoof-level (evade rfc2267 filtering)
                    usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
                2 - Change Packet size, usage: -i <packet size in bytes>
                3 - Bind root shell to a port, usage: -i <remote port>
                4 - UDP flood, usage: -i victim@victim2@victim3@...
                5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
                6 - ICMP/PING flood, usage: -i victim@...
                7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
                8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
                9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
                10 - Blindly execute remote shell command, usage -i command
```

There are multiple targets that can be targeted here. We could go after the web server.

% ./tfn –f owned_boxes –c 5 –P tcp –p 80 –l www.giac.com

Or the GIAC router.

% ./tfn –f owned_boxes –c 8 –l 4.4.4.5

The first choice would instruct the 'owned boxes' to send out tcp packets to port 80 of the web server. It's possible that the web server won't become overwhelmed but the 50 boxes would quickly eat-up all available bandwidth between the ISP and the GIAC router preventing legitimate traffic from passing through.

The second attack would work also given that the owned boxes can push at least 25 Mbits/sec at the link (50 boxes at 500Kbits/sec).

The countermeasures against this type of attack can be found out on the Internet.
http://packetstorm.decepticons.org/distributed/TFN2k_Analysis.htm

Jason Barlow and Woody Thrower of the Axent Security Team describes how to detect and defeat TFN2K:

Detecting TFN2K – The Signature

All control communications are unidirectional, making TFN2K extremely problematic to detect by active means. Because it uses TCP, UDP, and ICMP packets that are randomized and encrypted, packet filtering and other passive countermeasures become impractical and inefficient. Decoy packets also complicate attempts to track down other *agents* participating in the denial-of-service network.
Fortunately, there are weaknesses. In what appears to be an oversight (or a bug), the Base 64 encoding (which occurs after encryption) leaves a

telltale fingerprint at the end of every TFN2K packet (independent of protocol and encryption algorithm). We suspect it was the intent of the author to create variability in the length of each packet by padding with one to sixteen zeroes. Base 64 encoding of the data translates this sequence of trailing zeros into a sequence of 0x41's ('A'). The actual count of 0x41's appearing at the end of the packet will vary, but there will always be at least one. The padding algorithm is somewhat obscure (but predictable) and beyond the scope of this document. However, the presence of this fingerprint has been validated both in theory and through empirical data gathered by dumping an assortment of command packets.
A simple scan for the files tfn (the *client*) and td (the *daemon*) may also reveal the presence of TFN2K. However, these files are likely to be renamed when appearing in the wild. In addition to this, both *client* and *daemon* contain a number of strings that can be found using virus scanning methods. Below is a partial list of some of the strings (or sub-strings) appearing in TFN2K:
NOTE: Scanners should look for pattern combinations unlikely to appear in legitimate software.

TFN2K Client (tfn)

[1;34musage: %s <options>
[-P protocol]
[-S host/ip]
[-f hostlist]
[-h hostname]
[-i target string]
[-p port]
<-c command ID>
change spoof level to %d
change packet size to %d bytes
bind shell(s) to port %d
commence udp flood
commence syn flood, port: %s
commence icmp echo flood
commence icmp broadcast (smurf) flood
commence mix flood
commence targa3 attack
execute remote command

TFN2K Daemon (td)

fork
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123
456789+/
/dev/urandom
/dev/random
%d.%d.%d.%d
sh*
ksh*

command.exe**
cmd.exe**
tfn-daemon***
tfn-child***

* Unix and Solaris systems only
** Windows NT systems only
*** This text is likely to have been changed in many TFN2K installations

TFN2K Daemon and Client (tfn and td)

security_through_obscurity *
D4 40 FB 30 0B FF A0 9F **
64 64 64 64 ... ***

* This is a function whose definition is generated at compile time. This is a strong (and probably unique) signature.
** This byte pattern is present in both *client* and *daemon*, and represents the first eight bytes in the CAST-256 encryption table (assumes little-endian byte ordering).
*** A contiguous 128-byte sequence of 0x64 values reveals the presence of the static table used in the Base 64 decoding algorithm.

Defeating TFN2K – A Strategy

There is no known way to defend against TFN2K denial-of-service attacks. The most effective countermeasure is to prevent your own network resources from being used as *clients* or *agents*.

Prevention

Use a firewall that exclusively employs application proxies. This should effectively block all TFN2K traffic. Exclusive use of application proxies is often impractical, in which case the allowed non-proxy services should be kept to a minimum.
Disallow unnecessary ICMP, TCP, and UDP traffic. Typically only ICMP type 3 (destination unreachable) packets should be allowed.
If ICMP cannot be blocked, disallow unsolicited (or all) ICMP_ECHOREPLY packets.
Disallow UDP and TCP, except on a specific list of ports.
Spoofing can be limited by configuring the firewall to disallow any outgoing packet whose source address does not reside on the protected network.
Take measures to ensure that your systems are not vulnerable to attacks that would allow intruders to install TFN2K.

Detection

Scan for the *client*/*daemon* files by name.
Scan all executable files on a host system for patterns described in the previous section.
Scan the process list for the presence of daemon processes.
Examine incoming traffic for unsolicited ICMP_ECHOREPLY packets containing sequences of 0x41 in their trailing bytes. Additionally, verify that all other payload bytes are ASCII printable characters in the range of (2B, 2F-39, 0x41-0x5A, or 0x61-0x7A).
Watch for a series of packets (possibly a mix of TCP, UDP, and ICMP) with identical payloads.

Attack Internal System

The plan to compromise an internal system will require a combination of methods to increase the likelihood of succeeding. We will target a user's PC since we feel it's typically less secure than servers. The information gathered from the PC will then allow us to leapfrog into other sensitive and more secure systems and the chances of being detected are less. The idea is to use social engineering, a Trojan program and a little bit of luck!

Social engineering takes advantage of the general desire of people to be helpful. It might be the least technical, but it is often the most successful.

The first phase is to go to www.arin.net and do a "whois" on giac.com and examine the information for POCs and email addresses. Add to the list of information you gather any names and email addresses found on the companies web site. As a shot in the dark also look for GIAC employee posting in chat rooms and bulletin boards. From the list of information, you might be able to see a pattern with email addresses and phone numbers. By calling at night to phone numbers one or two off of your known phone number list, you can possibly get the voice mail of other employees. The purpose for this step is to have as big a list as possible. Once you feel that the list is as complete as it's going to be then we move onto the next step.

This step works on the employees' lack of safeguarding company assets. By dressing so we present a clean, professional appearance, we will lower employees' suspicions and simply let them open doors for us! We'll wait by the door of GIAC's data center until an employee approaches. Then pretend to have forgotten the numeric password if it has a keypad or our card for a card-swiping security system. So as good as the security might be, people (that is the company employees) are the most useful tools for hacking into networks!

Another step worth pursuing is to simply call a person preventing to be from the IT department. This can often get you the user name and password

In phase two we craft a Trojan program to email a rather benign email to the targeted list of GIAC employees (if getting the user name and password didn't work earlier). We don't want to outsmart ourselves by trying to make it look like an email to a group of people unless we are sure these people would normally receive such emails (putting the CEO and Billy the new intern on the same email might raise suspicions!). Once the user opens the email, a small program is a loaded onto the PC. Since users usually have the ability to access the Internet through port 80, we will use that port as the method to get out to an already "owned" box.

The problem with many employees is that they can be characterized as sheep while the hacker is the wolf. Employees don't properly protect themselves from falling victim to social engineered attacks. Users tend to be infatuated with the technology such as firewalls, IDS, anti-virus, etc. Raising their awareness of security is an essential first step to combat this problem. This must be done so it integrated into their day-to-day behavior. Having a once-a-year presentation on raising security awareness is not effective. The educational programs should be creative to keep them alert and aware of smart security practices. Sending out security-related emails either daily or weekly helps remind users of important security issues. Another tool would measure your programs effectiveness by sending users a software program to test users' security knowledge. Using the results, you can then focus on areas that need more education. The security people must realize that the key to the success of their education program is communication.

List Of References

IT Security Solutions, "Syslog-ng" URL:http://www.balabit.hu/en/downloads/syslog-ng (5 Sep 2002)

Internet Software Consortium, "ISC BIND" URL:http://www.isc.org/products/BIND (4 Sep 2002)

December Communications Inc., "File Permissions in Your (Expanding) Web Space" 30 Aug 2002 URL:http://www.december.com/html/tutor/permissions.html

Internet Security Systems, URL:http://www.iss.net/ (2 Sep 2002)

Cisco Corp., URL:http://www.cisco.com/

National Security Agency, "Downloading Security-Enhanced Linux" URL:http://www.nsa.gov/selinux/download.html

Hyperlative Ltd., "UNIX commands for Web developers" (1997) URL:http://www.sofer.com/research/unix.html

National Security Agency, "Security Recommendation Guides Cisco Router Guides" 9 Jul 2002 URL:http://nsa1.www.conxion.com/cisco/download.htm

The SANS Institute, "Firewalls 102: Perimeter Protection with Firewalls, SANS Firewall Track", Bethesda, MD: SANS Press (2002)

Wietse Zweitze Venema, "The Postfix Home Page", URL:http://www.postfix.org/start.html

Freshwater Software, Inc., URL:http://www.sitescope.com

Federal Information Processing Standards Publications, "SECURE HASH STANDARD" 17 April 1995 URL: http://www.itl.nist.gov/fipspubs/fip180-1.htm

RSA Security, URL:http://www.rsasecurity.com

Roger Schlafly "Opinions on S/MIME" 30 Dec 1998 URL:http://groups.google.com/groups?oi=djq&selm=an_427312947

M.J.Wiener, "Performance Comparison of Public-Key Cryptosystems", RSA CryptoBytes, Volume 4, Number 1, Summer 1998

Elliptic Curve Cryptography, 18 Sep 2002 URL:http://www.isg.rhul.ac.uk/~sdg/ecc.html

Insecure.org., “Nmap” 12 Nov 2001 URL:http://www.insecure.org/nmap/

SecurityFocus Online, URL:http://online.securityfocus.com

Steve Keifling GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.7 URL:www.giac.org/practical/Steve Keifling_GCFW.zip