Global Information Assurance Certification Paper

GIAC CERTIFIED FIREWALL ANALYST PRACTICAL

VERSION 1.7

Submitted By Greg Surla

TABLE OF CONTENTS

Tables of Figures

BACKGROUND

The GIAC Corporation is one of the world's largest suppliers of fortune cookie sayings. The company's world headquarters is located on a vast 5-acre campus in the heart of what is commonly referred to as the "Silicon Alley" of the southeastern part of the United States – Yeehaw Junction, Florida. GIAC employs approximately 350 employees at its world headquarters with an additional 150 employees based out of their homes around the country. Recent mergers of various fortune cookie saying companies have caused a much tighter and more competitive marketplace. With over 500 million in annual sales up for grabs, GIAC requires a thorough security policy for its computer network connections in order to maintain and grow its 12% market share.

The GIAC network was built up from a small Novell Netware 3.11 network to an all-Microsoft network in the mid to late 90's. In the early 2000's, GIAC Enterprises began the migration from one OS vendor to multiple OS vendors. This was due to increasing licensing costs in a growing company as well as using the process of selecting the best tool for the environment and not just settling on a tool because it ran on a certain operating system.

As the GIAC network grew, the I.S. department began to take notice of the increasing risk of performing business over the Internet. In 2001, a complete reworking of the Internet security services. In order to take a more active role in protecting the GIAC information infrastructure, more attention was paid to the security default operating system installations, containing Internet mail viruses and worms and overall company border security.

The contents of this paper outline the border security implementation that GIAC has undergone over the past couple of years. It also includes the results of the network audit conducted 12 months after the implementation of the GIAC border security components.

ASSIGNMENT 1 – SECURITY ARCHITECTURE (15 POINTS)

Define a network security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.

Your architecture must consider access requirements (and restrictions) for:

- Customers (Companies or individuals that purchase bulk online fortunes)
- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)
- Partners (International companies that translate and resell fortunes)
- GIAC Enterprises employees located on GIAC Enterprise's internal network
- GIAC Enterprises mobile sales force and teleworkers

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

Defining access requirements and the reasoning for those requirements is **critical** to this assignment. If you have not thought through how this access will take place, you will not be able to adequately define your security policy and ACLs/rulesets later in the paper.

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

- Filtering Router(s)
- Firewall(s)
- VPN(s)

Your architecture may also include the following **optional** components if they are appropriate to your design:

- Internal firewalls (Are internal firewalls appropriate for additional layered protection; to segment internal networks…?)
- Additional secure remote access (Is additional remote access – other than the VPN – required by administrators, salespeople, telecommuters…?).
- Intrusion detection systems

You must include a diagram or set of diagrams that shows the layout of GIAC Enterprise's network and the location of each component listed above. You must provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

The network can be as complex or as simple as you like as long as it meets the functional requirements that you define according to the guidelines given above. The important thing is not how elaborate your network is, but that your design actually works.

You must justify the appropriateness of your design. Is it both technically reasonable and financially feasible? Are you building a $1000 fence to contain a $100 horse? You may provide a cost or bill of materials if you wish.

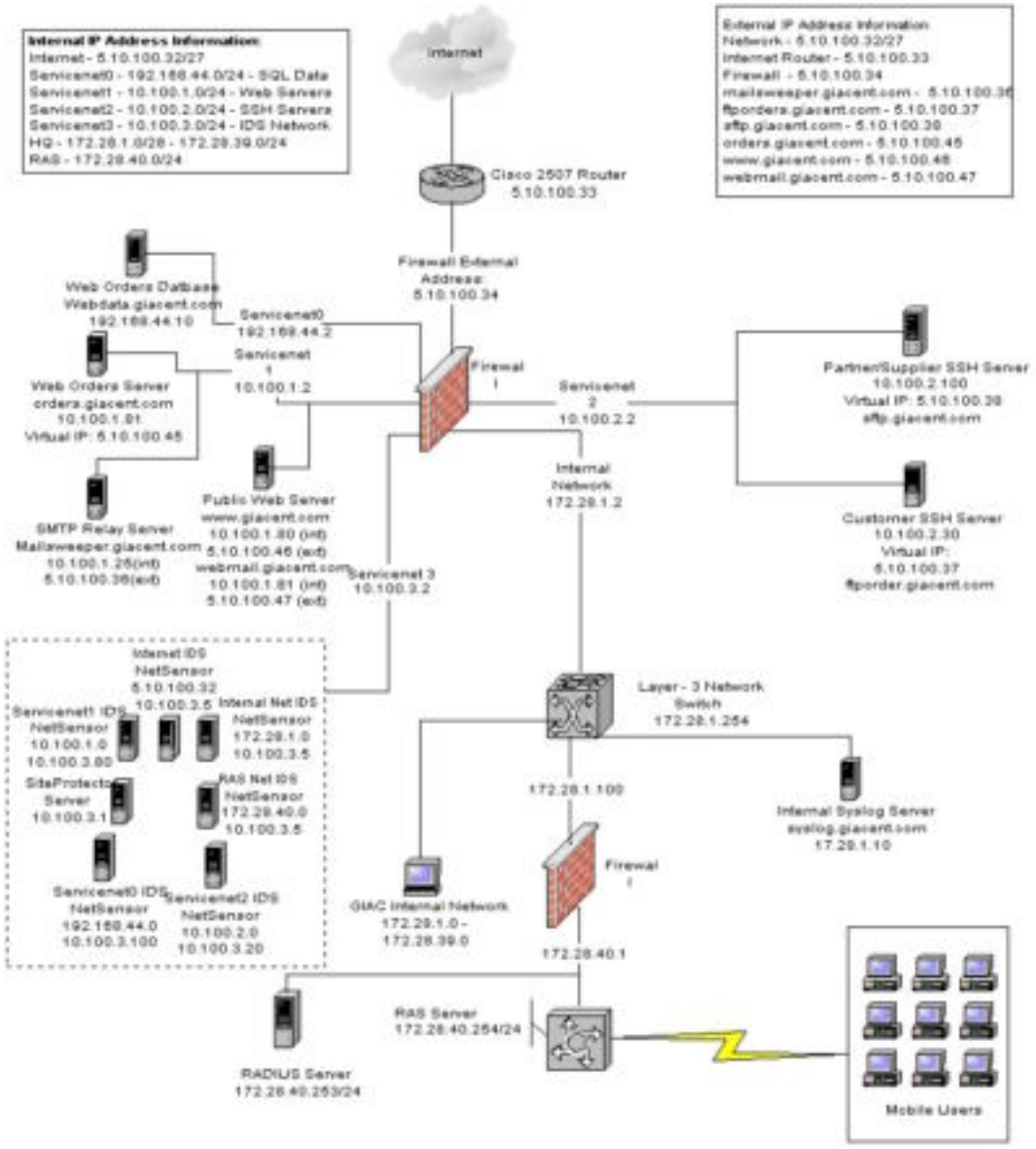


Figure 1 - GIAC Network Overview

1.1 INBOUND CONNECTIONS

1.1.1 CUSTOMERS

Most customers will order their sayings online through a secure web server. For individuals and businesses without established accounts, all purchasing will take place through a secure web page. For customers with accounts, the primary method of submitting order information is through the secure web server but an SFTP over SSH connection will be available to those wishing to automate their ordering process. Those with the inability to connect with an SSH client will be allowed to connect using a host-to-host VPN connection.

1.1.2 WEB-BASED CUSTOMERS

Customers utilizing the web interface to purchase sayings will connect to orders.giacent.com. The web server at this address uses a 128-bit SSL certificates. Any client connecting over standard http-80 will not get the 403.5 error page. Instead, the client will be redirected to the appropriate secure web page. Customer data is not stored on the web server. All data entered into the web interface from a customer is sent to a separate database server on a different subnet.

1.1.3 FTP SERVER CUSTOMERS

Since established customers generally submit bulk orders, a process has been developed to allow those customers to send a text file formatted to allow for easy entry into the servers processing those bulk orders. Those customers lacking the ability to perform IPSec connections will be permitted to submit their orders via Secure FTP. All SFTP Server customers are required to supply at least one static IP address that they will use to connect to GIAC. This is to prevent unknown hosts from accessing the server.
The Secure FTP session will take place over an SSH connection utilizing public key authentication. The public key will be generated by the GIAC Enterprises network department and mailed to the customer using snail mail. All SSH customers connect to ftporders.giac.com (5.10.100.37) over port 1984/tcp.

1.1.4 VPN CUSTOMERS

For customers wishing to use VPN connections, IPSec VPN is enabled on the firewall to allow those VPN connections into the FTP order server. The VPN connection allows for strictly a host-to-host connection with the VPN client connecting to ftporders.giac.com (5.10.100.37). Once the VPN connection has

been established, an FTP session is setup to 10.50.15.100 and FTP PUTS to the server are performed by the customer. All FTP GET attempts by VPN customers are blocked in order to prevent the stealing of data in case an unknown vulnerability has been exploited on the FTP server.

1.1.5 INBOUND SERVER ARCHITECTURE

Customer Orders SFTP Server (ftporders.giac.com) Architecture

The FTP Server is running Red Hat Linux 7.2 with kernel 2.40-18. This server has been patched with the latest updates. The Bastille Linux Hardening System[1] has also been implemented on this server to try to "lock down" the server as best as possible. The Tripwire system integrity-checking tool is installed to audit changes to the server.

The FTP Server is running WU-FTPD[2] for its VPN clients. Patches have been applied to the WU-FTPD server that fix the known vulnerabilities of the server. All logging needed to go to the central syslogd server so the WU-FTPD has been recompiled with the appropriate options to allow for this logging configuration. FTP connections to this server are not available over the Internet without connecting over a VPN session.

The server is running OpenSSH 3.4p1 for SSH client connections. All logging is sent to the internal syslogd server. The SSH clients will need to configure their connection go through port 9287/tcp instead of the standard 22/tcp.

Web Server (orders.giac.com) Architecture

The web server is running on Microsoft Windows 2000 using the Internet Information Services 5.0. The server contains one NIC, which is set to 10.100.2.80/24. The server has been patched with the latest service pack and updates.

All transactions will be stored on the data server located on a separate machine in a separate DMZ network. This is to add an extra layer of protection between the Internet and the valuable financial data. A hacked web page may provide a little embarrassment to a company in the short term but a hacked credit card database will cause much greater harm, not only to reputation and confidence but also to the company's bottom line in the cost of litigation and lost customers.

The web server is running the Tripwire (www.tripwire.com) system integrity-checking tool as well as the ISS RealSecure Server Sensor (www.iss.net).

---

[1] See http://www.bastille-linux.org for more information

[2] Information on wu-ftpd can be found at http://www.landfield.com/wu-ftpd/

These two products should provide enough information to detect a hacking attempt in time to stop or reduce the damages that could occur.

A connection to the Microsoft SQL Server database (webdata.giac.com) occurs over port 1776/tcp3. This is a custom port number. The default port of 1433 is well known and exploits have been developed that attack this port. By changing the default port that SQL Server communicates through, the vulnerability is reduced. Unfortunately, all a hacker needs to do is run a network sniffer on the network segment containing the SQL Server in order to find the port established for SQL traffic.

Database Server (webdata.giac.com) Architecture

The database server is running Microsoft Windows 2000 with Microsoft SQL Server 2000. The server has one NIC, which is set to 192.168.30.50. As stated previously, connectivity from the web server to the SQL Server data will occur over through the firewall over port 1776.

The database server has a RealSecure server sensor installed to detect changes and intrusions on the server. In addition, the following steps has been performed on the SQL Server to help cure some known vulnerabilities:

- All patches and service packs were applied. Patching to the server occurs on an as-needed basis.
- Internet Information Services has been removed.
- The SA password has been reset to a hard-to-guess non-English password containing at least 15 characters, which utilizes upper and lower case letters, symbols, and numbers[4]. The SA password is not given to developers who, in their laziness, might use the SA account in their software to access databases.
- All logins to the SQL Server are audited.
- The SQL services run as a specific user and not the 'LocalSystem' account. LocalSystem has rights "to act as part of the operating system".
- Disable unnecessary and insecure stored procedures[5].

[3] Port 1776 is assigned to the Federal Emergency Management Information System (http://www.pnl.gov/femis/). GIAC will not be allowing this system into its network therefore, it can be used as the port for SQL communications to/from the customer web server.

[4] http://www.kb.cert.org/vuls/id/635463 - CERT Vulnerability Note (VU#635463) Microsoft SQL Server and Microsoft Data Engine (MSDE) ship with a null default password

[5] Microsoft SQL 2000 Security Whitepaper - http://www.microsoft.com/sql/techinfo/administration/2000/securityWP.asp

- xp_cmdshell -- This procedure allows someone (among other things), the ability to add users to the server or domain if the SQL server is a domain controller.
- Registry Access stored procedures – The ability to read the registry is also available by running the 'xp_readreg' stored procedure.

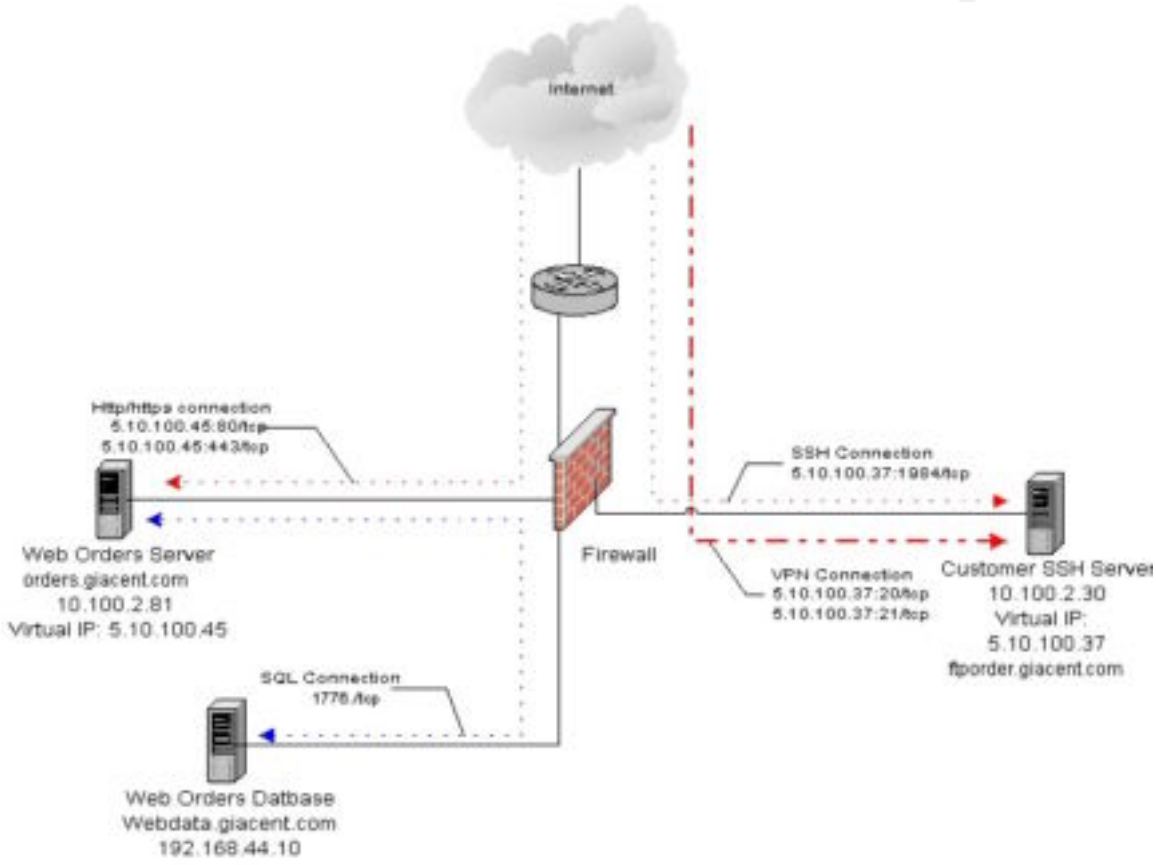


Figure 2 - Customer Connections

1.2 - SUPPLIERS AND PARTNERS

1.2.1 - Suppliers

Suppliers transfer sayings in bulk to the server located at GIAC Headquarters via the Internet. Suppliers are generally philosophers, theologians, or comedians who write or study insightful text. These suppliers are mostly individuals working at home or small offices and do not have access to a technical support staff.

GIAC has developed a script that automates the process for suppliers to send their files to the GIAC server. Suppliers create text files containing the quips and phrases. When the supplier is ready to send their file to GIAC for processing, the supplier runs the script that first encrypts the file with GPG, compresses the encrypted file and then finally it runs an SCP command to send the file to the GIAC SSH server using public-key authentication. The only interaction that is required by the user is the password that needs to be typed in once the SCP connection is made. The public and private keys for both SSH and GPG are created by the GIAC security department. The public key is placed on the server and the private key is snail mailed to the user along with the private key password. Most requests for help from suppliers is centered on the supplier needing to copy their private key to a newly acquired PC as well as the installation of the SSH client and the GPG software.

1.2.2 - Partners

Partners connect to the GIAC network in order to retrieve English language versions of the sayings that need to be translated to other languages for use domestically and in other countries. As with suppliers, but not nearly as abundant, partners may work either at home or in small offices without the luxury of an on-site computer support staff. In most cases, partners are also suppliers.

As with Suppliers, partners run a script, which will copy the file or files from the GIAC server containing the phrases that need translations using the SCP program and public-key authentication. Once copied down to the local machine, the script then decrypts the file. The process for obtaining keys for SSH and GPG are the same as the supplier – GIAC creates the keys and sends out the keys to the partner for installation on their local machine.

1.2.3 - Supplier and Partner SSH Server (sftp.giacent.com)

This server is nearly identical to the customer SSH server. This server is running Red Hat Linux 7.2 with the latest kernel and software updates. The Bastille Linux Hardening System has also been implemented on this server to try to "lock down" the server as best as possible. The Tripwire system integrity-checking tool is also installed to audit changes to the server. The server is located on the Servicenet2 network at IP address 10.100.2.100 and on the public IP address at 5.10.100.38.

For SSH clients, the server is running OpenSSH 3.4.p1. All logging is sent to the internal syslogd server. The SSH clients will need to configure their connection go through port 9278/tcp instead of the standard 22/tcp. While a telnet connection to the port will result in the OpenSSH banner being displayed, changing the port number may help prevent lazy "script kiddies" from using known exploits against the OpenSSH server.

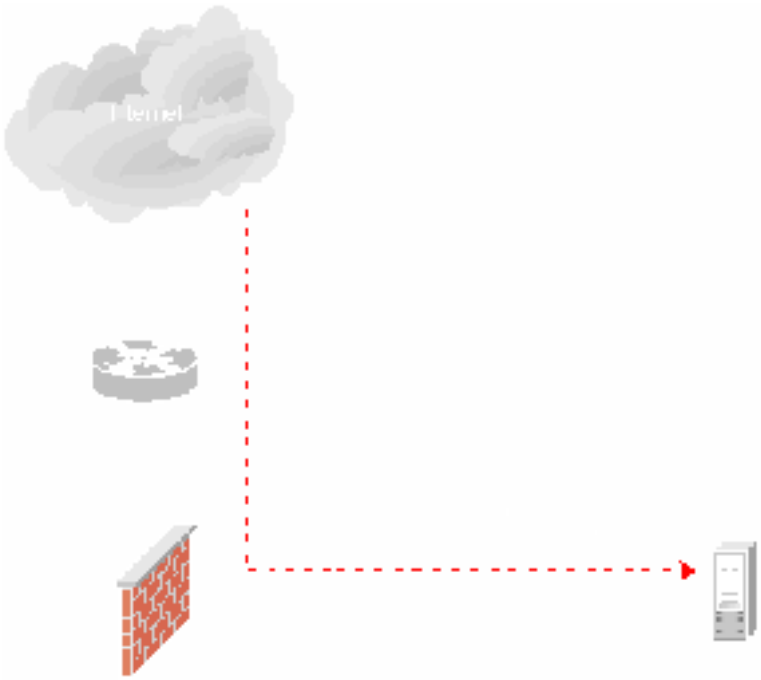


Figure 3 - Partner and Supplier connections

1.3 - INBOUND EMPLOYEE CONNECTIONS

GIAC employees connect to the GIAC network remotely in one of two ways: Dial-in RAS or VPN.

1.3.1 - DIAL-IN ACCESS

Accessing the GIAC Enterprises network via telephone connection is the failsafe method of remote connection in case VPN connections do not work. All RAS users connect via their operating system's RAS client. The RAS Server is placed on its own subnet to allow for the filtering of unnecessary protocols by the RAS Firewall as well as only allowing traffic to the Windows server network located at 172.28.1.0/24. In order to permit RAS clients to connect to the Microsoft Exchange Server located in the Windows Server network, the Exchange Server computers require a registry edit that sets the client communication ports to 6000/tcp and 6001/tcp. By default, Exchange Server assigns a random port number that the client uses in order to communicate with the Exchange Server.

The Cisco Secure Access Control Server for Windows provides the RADIUS authentication services for RAS users. To alert on an attack originating from the

RAS network, the RAS network is monitored by a RealSecure Network Intrusion Detection sensor.

1.3.2 - VPN CONNECTIONS

All remote GIAC employees with appropriate rights are to connect to the GIAC network through the VPN connection provided by the Symantec Enterprise Firewall VPN component. The client workstations should be running a version of Microsoft Windows 98 or newer in order to be able to run the Symantec VPN Client. Other VPN client software may be able to connect the VPN server but it is not supported and is not recommended. All employees that require inbound VPN access are issued the client with their username and secret key. The usernames and passwords do not correspond with the GIAC network logon ID. The accounts names and passwords are randomly generated in order to guarantee uniqueness.

1.3.3 - WEB-BASED E-MAIL SERVER

Most employees will access the network remotely in order to read e-mail. To make life easier for employees on the road, a web-based mail system has been deployed. This service is deployed on the public web server as a virtual directory. The web mail service is running SquirrelMail. SquirrelMail is an open source web-based mail solution running on an Apache web server, it contains Spam filtering and supports SSL connections. It runs as an IMAP mail client to the mail server, which cuts down on the overhead of a dedicated web-based e-mail server. The external IP address for webmail.giac.com is 5.10.100.47. Since the addition of webmail.giac.com, GIAC has seen a 60% reduction in VPN and RAS traffic from GIAC employees.

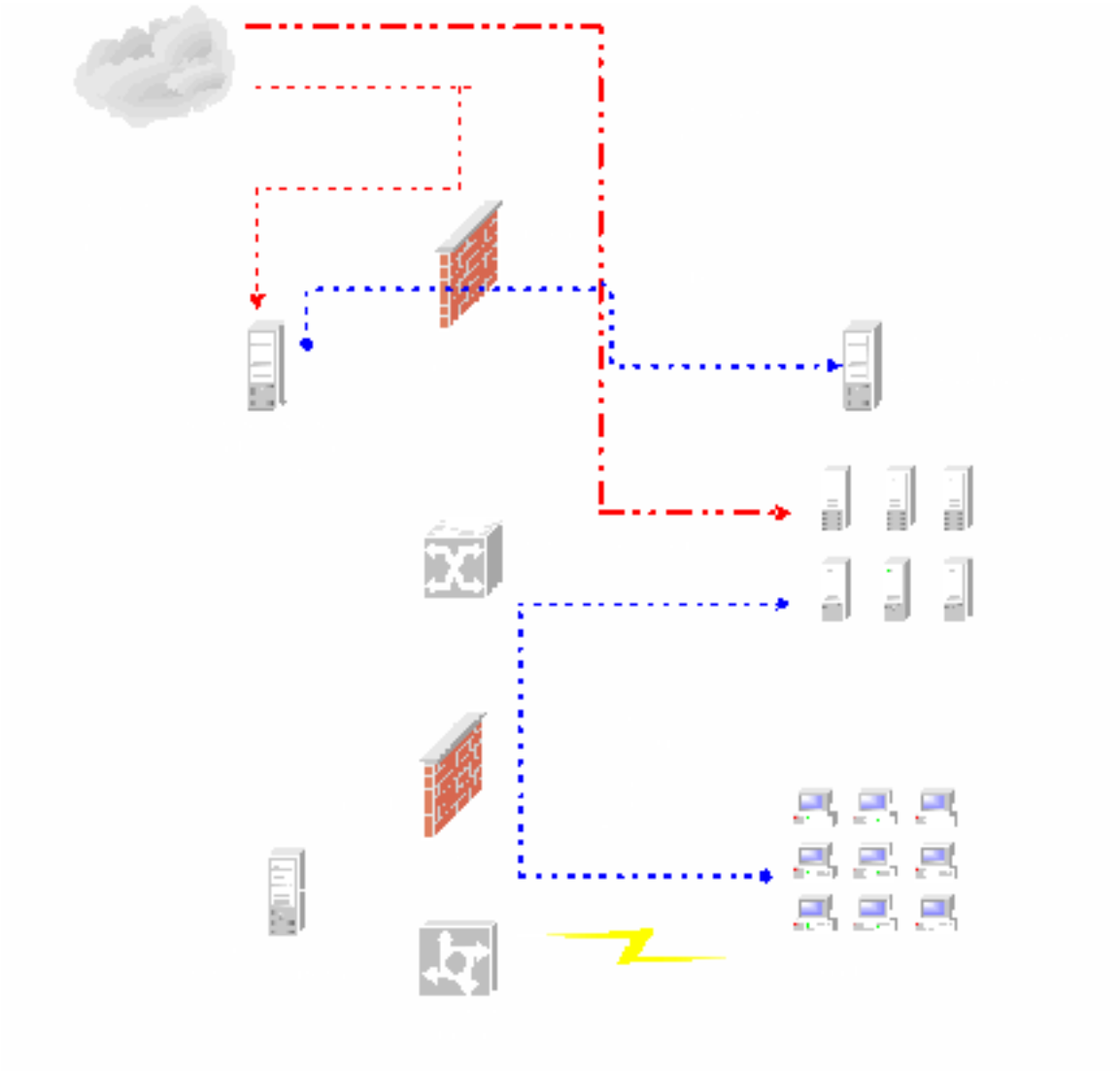


Figure 4 - Employee Connections

1.4 - OTHER SERVICES

1.4.1 - SMTP MAIL

With the threat of viruses on the Internet being a major concern for the GIAC I.S. staff, GIAC has installed the Clearswift Mailsweeper for SMTP. This software scans for viruses, certain file type attachments and Spam. Rather than letting the anti-virus engine on the Mailsweeper server detect and contain the virus attachment, GIAC filters all .com, .vbs, and .pif files in e-mail as a precaution. The Mailsweeper server utilizes the Real-time Blackhole List provided by MAPS[6] in order to prevent Spam mail from open SMTP relay servers. The anti-Spam

[6] http://mail-abuse.org/rbl/

engine also searches for certain keywords in e-mail messages that are generally used by spammers to send out porn and other types of unwanted messages. The anti-virus engine is provided by Command Software. Updates occur at least on a weekly basis.

The Mailsweeper for SMTP (Mailsweeper.giacent.com) service runs on a Microsoft Windows 2000 server. The server is placed in Servicenet1 with the internal IP Address of 10.100.2.25 and the external IP address of 5.10.100.36. In order to send e-mail to the Internet, the internal Microsoft Exchange 5.5 mail server running the Internet Mail Service for Exchange (mailrelay.giacent.com) will forward all mail to the MAILSWEEPER server via the SMTP protocol. The MAILSWEEPER server will then send all mail out to the appropriate destination server on the Internet after scanning the messages. Receiving Internet mail is the inverse of outbound e-mail from GIAC. Any mail received by MAILSWEEPER is first scanned then sent to the internal mailrelay.giacent.com server.

1.4.2 – USENET NEWS

GIAC Enterprises employees are allowed access to Usenet newsgroups through their NNTP client. GIAC downloads the appropriate newsgroups to their Microsoft Exchange server (mailrelay.giacent.com), which then serves those newsgroups to the employees. The firewall allows the NNTP port (119) for only exchange.giacent.com to the ISP's Usenet server (news.ackmee.net). GIAC does not filter Usenet messages but does filter all newsgroups that are primarily used to distribute binary files.

1.4.3 - PUBLIC WEB SERVER

The GIAC Enterprises public web server is used to disseminate Public/Investor Relations and Marketing information along with other information regarding the GIAC Enterprises Corporation. This website contains the typical marketing data that the public accesses to gather more information about the company. Since there is a high probability that potential investors and customers will access the web site, security on that machine is a high priority.

The public web server runs Red Hat Linux 7.2 with the Apache web server and Bastille Hardening System loaded. The server has been patched with the latest updates and kernel. Logging for this server will point to the internal syslog server at 172.28.1.10. The web server is attached to the Servicenet1 network on IP address 10.100.2.80 with a public IP address of 5.10.100.46. This server is running Tripwire as well as a RealSecure server sensor for host security management.

1.5 - OUTBOUND EMPLOYEE CONNECTIONS

1.5.1 - PROXY SERVER CLIENTS

Most employees on the internal GIAC network are assigned an IP address via DHCP. Connection to the Internet is limited to http, https and ftp access via the proxy server (proxy.giacent.com – 172.28.1.80) for most employees. Any other service connections will bypass the proxy server.

1.5.2 - SPECIAL ACCESS CLIENTS

For those employees wishing to access protocols outside of those serviced by the proxy server, individual requests are reviewed for impact and business justification. Some employees have a requirement to connect to other Internet servers on special ports for specific services. These employees may be assigned a static address. In the case of whole departments requiring special access to a port, subnets and, if necessary, the entire network will be allowed through the firewall for specific ports.

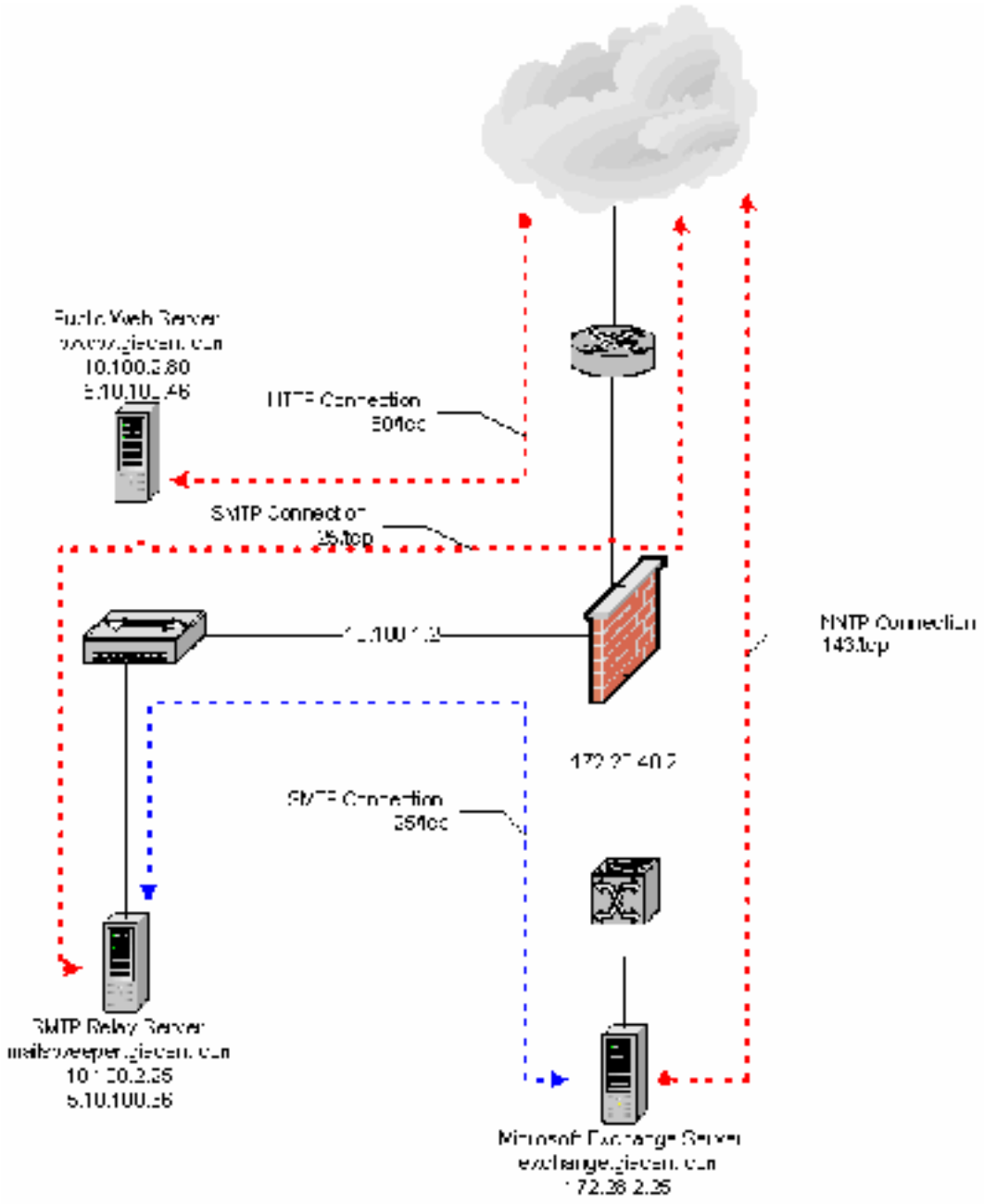


Figure 5 - Other Connections

1.6 - PERIMETER SECURITY

1.6.1 - BORDER ROUTER

The border router at GIAC is a Cisco 3620 Router with IOS version 12.2. The Cisco 3620 was chosen because of it is a feature-rich router with support for multiple interface types on two separate interfaces, allowing GIAC to modify its Internet access based on bandwidth requirements that may increase in the future.

The router contains one Ethernet interface for the GIAC network and one T1 interface for Internet WAN connection. It also contains the standard serial console port for local management. The Ethernet interface address is set to 5.10.100.33 and the external WAN interface address is set to 5.4.36.22.

1.6.2 - PERIMETER FIREWALL

The firewall managing traffic on the Internet is the Symantec Enterprise Firewall (formally known as Axent's Raptor) version 7.0. This firewall is running on a Windows 2000 Server machine. The firewall contains six network interfaces in order to accommodate the following networks:

- Internal network (172.28.1.2/24)
- Internet (5.10.100.34/27)
- Web services network (10.100.1.2/24)
- SSH and FTP services network (10.100.2.2/24)
- SQL data services network (192.168.44.2/24)
- Intrusion Detection System network (10.100.3.2/24).

Symantec Enterprise Firewall has been chosen over other vendor solutions because it is an Application Proxy as opposed to a packet filtering firewall such as Checkpoint's FW-1 and Cisco's PIX. Application Proxy firewalls tend to be more secure than stateful inspection firewalls but are slightly slower in performance[7]. The slight performance decrease is not a concern for GIAC since security is more important than speed. The Symantec Enterprise Firewall's history as a solid firewall solution for the medium to large business environment was also a major factor in the decision to deploy this solution.

1.6.3 - RAS FIREWALL

The firewall that provides protection on the Remote Access side of the GIAC network is also a Symantec Enterprise Firewall version 7.0. This firewall is also running Microsoft Windows 2000 as its operating system. The RAS firewall contains two network interface cards. One NIC (172.28.1.100/24) is connected to the internal switch, while the other NIC is connected to the RAS network (172.28.40.1).

1.6.4 - INTRUSION DETECTION SYSTEM

The Intrusion Detection System on the GIAC network is RealSecure by Internet Security Systems. RealSecure monitors the subnets as well as managing the servers that contain sensors such as the orders.giac.com web and database servers.

[7] Application Layer Firewalls vs. Network Layer Firewalls: Which Is the Better Choice?

Monitoring of the RealSecure Intrusion Detection System is centralized on an ISS Site Protector system. This allows for centralized deployment of XPUs (sensor updates) to the various sensors as well as a centralized repository of information captured. The Site Protector server runs on Windows 2000 service pack 2 with Microsoft SQL 2000 server. The server sits on the IDS DMZ located on the 10.10.60.0 network.

The ISS RealSecure system was chosen for its reputation as a leader in the Intrusion Detection Systems marketplace. Its cross-platform deployment capabilities and centralized reporting features make RealSecure ideal in an environment such as GIAC's.

IDS Network Sensor Servers

The Intrusion Detection System has agent machines that monitor network segments. These machines have common hardware makeup and OS requirements. All systems run Windows 2000 workstation and contain two Network Interface Cards. Each network sensor machine has a NIC running TCP/IP with an address on the 10.100.3.0 network. The additional NIC is not bound to a protocol so that it may capture traffic in promiscuous mode. The sensors report matched patterns back to the Site Protector management server. Each sensor is also responsible for alerting based on policies set by the security administrator. Network sensors are placed in the following locations:

- Firewall internal subnet
- RAS Server subnet
- All firewall Servincenets

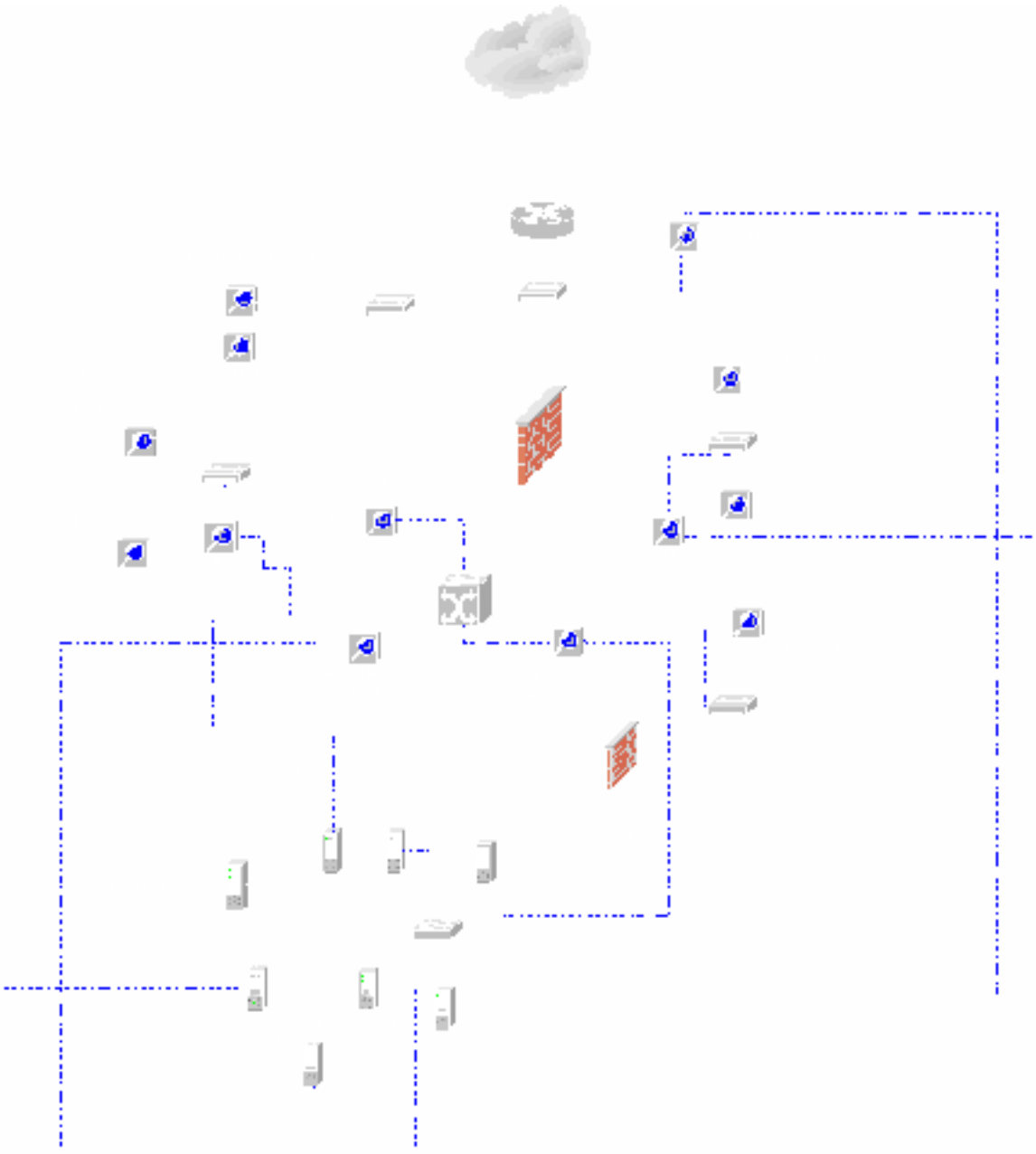


Figure 6 - IDS Sensor and Tripwire placement

1.7 - OTHER SYSTEMS - INTERNAL SYSLOG SERVER, LOG MANAGEMENT AND ALERT NOTIFICATION & TIME SERVICES

1.7.1 – Syslog Services

Reviewing system logs is a time-consuming and often boring process. The need to determine whether problems are occurring on a particular system is paramount to any network or security administrator trying to perform his job effectively. For this purpose, and where possible, all systems logs will be sent to a centralized log server that acts as a clearinghouse for the log files. The review process is consolidated to one or more servers allowing for alerts via e-mail and paging. This syslog server (syslog.giacent.com) is located at 172.28.1.10.

Syslog.giacent.com is running on a Red Hat Linux computer that has been hardened by the Bastille Linux Hardening System. Tripwire is installed on this system to monitor any changes made to the server. The systems that send their log files to the syslog server include:

- All UNIX-like hosts
- The Internet router
- Windows NT/2000 hosts (utilizing third party software to capture Event Log notifications)
- Any system running Tripwire

Not all systems are capable of sending their log files to the syslog server. For these systems, the primary method used to review logs is noted below.

1.7.2 – Symantec Enterprise Firewall (SEF)

All daily logs files are archived on a separate server each night for disaster recovery purposes. In order to review the gigs of data contained in the logs, a product called the Firegen Log Analyzer[8] is used. This software allows an administrator to generate a web page based on SEF log files. The web page outlines all messages that have occurred in the log files. Firegen categorizes log messages by severity and contain links to the Firegen web site that explains what a message could possibly mean. Since the majority of messages on a SEF system are non-threatening to the environment, the ability to filter this information and concentrate solely on what is important is invaluable for time management.

Alerts are handled by the SEF paging and e-mail alert systems. All Emergency (700), Critical (600) and Alerts (500) messages are sent to the firewall administrator's pager. These indicate that there is a serious problem or a

[8] http://www.eventid.net/firegen

potential firewall breech that requires immediate attention 24 hours a day. Alerts at the Error (400) and Warning (300) levels are sent to the administrator's e-mail box for further review. Anything below these levels is ignored by the alerting system on the firewall.

The syslog.giacent.com server acts as the repository for the log files for centralized retrieval. The SEF log files are copied to the syslog server via the scheduler service and a script utilizing the robocopy command found in the Windows NT Resource Kit. The Vulture service on SEF will shutdown all unauthorized services on the firewall. In order to be able to run the scheduler service on the firewall, the SEF configuration file named *vulture.runtime* needs to be edited. Two Windows 2000 service names will need to be added to this file – *schedule* (The Scheduler service) and *protected storage* (Stores security information for programs).

1.7.3 – Intrusion Detection Systems

By it's very nature an IDS requires alerting to occur on a constant basis. Without the alerting feature, an IDS is useless to most companies. With this in mind, alerts are generated based on the policy that is created by the IDS administrator. With false positives occurring constantly within IDS, an administrator needs to determine the level of alerting based on the signatures that are appropriate for their environment. There is no need to enable detection for Coldfusion exploits if a Coldfusion server is not in the environment. Chasing false positives all day long is counter-productive to an efficient security administrator. Therefore, it is recommended that in order to gauge what is required to be monitored, an IDS should be run with all signatures enabled for approximately a week. This will allow the administrator to determine what generates false detections and he or she can modify the alert policy based on the trial run. After the trial run has been completed with the IDS logging set at full, the level of alerting is dependent upon what the environment calls for. An EHLO command sent to the mail relay server isn't nearly as important if that server rejects the command than if a SYN flood attack is detected. Both attacks are considered high risk but the SYN flood is a higher risk and requires more immediate attention. In this case, the SYN flood detection should be set to page the administrator while the EHLO command detection can safely be logged or ignored altogether.

The Site Protector administration program provides a central console for managing and reviewing IDS alerts. All alerts are sent to a Microsoft SQL Server database in order to store the data for later analysis and to generate the reports that management loves to peruse.

1.7.4 – Time Services

In order for alert notification to be useful, the system clocks of the computers on the network should be accurate. In order to do this, GIAC has installed a Network Time Protocol (NTP) server on the network. This service is running on syslog.giacent.com. All other servers on the network will connect to syslog.giacent.com to update its clocks every hour. Syslog.giacent.com will synchronize its clock with the Internet firewall located at 172.28.1.2.

ASSIGNMENT 2 – SECURITY POLICY AND TUTORIAL (35 POINTS)

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

- Border Router(s)
- Primary Firewall(s)
- VPN(s)

You may optionally include policy for other devices (i.e., - internal firewalls).

By "policy", we mean the specific set of ACLs, ruleset, or IPSec policy for that device – **not** corporate or organizational policy (though note that organizational policy may dictate the specific ACLs or ruleset in effect).

For each component, be sure to consider the access requirements for customers, suppliers, partners, remote users, and internal users that you defined in Assignment 1. The policies you define must accurately reflect those business needs as well as appropriate security considerations.

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

For each rule in all policies, you must include the general purpose of the rule and why it is important.

You must also include a discussion of the order of the rules, and why order is (or is not) important.

For **one** of the three security policies defined above, you must incorporate a tutorial on how to implement the policy. Clearly separate and label your tutorial. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information to clarify your instructions. Be certain to include a general explanation of the syntax or format of the ACL, filter, or rule for your device, as well as a general explanation of how to apply a given ACL, filter, or rule.

Be certain to point out any tips, tricks, or potential problems.

2.1 – BORDER ROUTER CONFIGURATION

GIAC has a Cisco 3620 router with one Ethernet connector and one T1 frame relay connector. The Ethernet segment that GIAC has leased resides on the 5.10.100.32/28 network. GIAC connects to their ISP via a frame relay T1 connection using the address of 5.4.33.22. The router performs filtering on as many potential TCP/IP exploits as possible.

All logging is sent to the internal syslog server located at address 172.28.1.10. In order for the router to "see" this address, a virtual IP address of 5.10.100.40 has been set up on the firewall located at 5.10.100.34. The virtual IP address for the syslog server allows the router to send its logging to the proper location.

GIAC has based its router ACLs on the suggestions made by the United States National Security Agency in their published papers – *The 60 Minute Network Security Guide*[9] and the *Router Security Configuration Guide*[10].

2.1.1 – INGRESS FILTERING ON THE ROUTER

The border router performs ingress filtering by blocking the following:

- Known unassigned IP Addresses
  - 10.0.0.0/16
  - 172.16.0.0 – 172.31.0.0
  - 192.168.0.0/20
  - 192.0.2.0/24
    - "test" network
  - 169.254.0.0/24
    - Address used by a machine whenever a DHCP client machine fails to lease an address.
  - 224.0.0.0/24
    - Multicast network
- Network file sharing protocols
  - CIFS (445/tcp)
  - NetBios (137-139/tcp)
  - NFS (2049)
- TCP and UDP ports that are generally not implemented for use over the Internet
  - TCP and UDP Small Servers
  - Finger
  - http server
  - bootp server
  - X11

[9] http://nsa2.www.conxion.com/support/guides/sd-7.pdf

[10] http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

    - RPC
- Other known tcp/ip exploits such as LAND attacks and certain DoS attacks

2.1.2 – EGRESS FILTERING

Egress filtering on the router denies the following outbound:

- RFC 1918 address in order to prevent, among other problematic addresses, DDoS Zombies that will spoof addresses (ex. TFN, TFN2K, Stacheldraht)
    - 10.0.0.0/16
    - 172.16.0.0 – 172.31.0.0
    - 192.168.0.0/20
    - Network file sharing protocols
        - CIFS (445/tcp)
        - NetBios (137-139/tcp)
        - NFS (2049)
    - UNIX services (512-518/tcp) that do not need to speak to the Internet
        - Rexec
        - Who
        - Syslog
    - NFS (2049/tcp)
    - Anything outside the local network
    - Known attacks and exploits
        - Netbus
        - Backorifice
        - Etc…

2.1.3 – THE GIAC BORDER ROUTER CONFIGURATION

```
Current configuration : 2708 bytes
!
version 12.2
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname GIACBR
```

The router needs to specify its timeserver. In the case of the GIAC network, the firewall (5.10.100.34) acts as the NTP server.

```
!
! Set NTP server
ntp source Ethernet0/0
```

```
service timestamps log datetime localtime show-timezone
service timestamps debug datetime localtime show-timezone
clock timezone EST -5
clock summer-time EDT recurring
! set NTP Server to firewall
ntp server 5.10.100.34
```

In the next section, we will configure the router to send its syslog messages to the internal syslog server. The virtual address of 5.10.100.40 is routed to 172.28.1.10 on the internal network.

```
! Configure Logging
logging on
logging console informational
no logging monitor
logging 5.10.100.40
logging trap debugging
logging facility local7
logging source interface Ethernet0/0
!
enable secret 5 $1$ZuRD$YBaAh3oIv4iltIn0TMCUX1
!
no ip source-route
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 description connected to Ethernet LAN
 ip address 5.10.100.33 255.255.255.240
 ip access-group 150 in
 keepalive 10
!
interface Serial 0/0
.
.
.
.

!
interface Serial 0/0.1 point-to-point
 no shutdown
 description connected to Internet
 ip address 5.4.36.22 255.255.255.252
 ip access-group 100 in
 frame-relay interface-dlci 1003
!
interface Ethernet 1/0
.
.
.
!
!
! access-list 100 is used to filter external network traffic
!
! Reset ACL 100
no access-list 100
! Deny LAND Attack
```

```
access-list 100 deny ip 5.4.36.22 0.0.0.3 any log
! Deny broadcast
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
! Deny localhost
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
! Deny RFC1918 Addresses
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 192.0.2.0 0.0.0.255 any log
! Deny failed-to-lease DHCP addresses
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
! Deny Multicast
access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
! Deny network and broadcast
access-list 100 deny ip any host 5.4.36.20 log
access-list 100 deny ip any host 5.4.36.23 log
! Allow already established connections
access-list 100 permit tcp any 5.4.36.20 0.0.03 established
! ICMP traffic
access-list 100 deny icmp any any echo log
access-list 100 deny icmp any any redirect log
access-list 100 deny icmp any any mask-request log
access-list 100 permit icmp any 5.4.36.20 0.0.0.3
! Deny NetBIOS
access-list 100 deny tcp any any range 135 139 log
! Deny CIFS
access-list 100 deny tcp any any eq 445 log
! Deny NFS
access-list 100 deny tcp any any eq 2049 log
access-list 100 deny udp any any eq 2049 log
! Deny X11
access-list 100 deny tcp any any range 6000 6063 log
! Deny irc
access-list 100 deny tcp any any range 6665 6669 log
! Deny NetBus
access-list 100 deny tcp any any range 12345 12346 log
! Deny Backorifice
access-list 100 deny tcp any any eq 31337 log
access-list 100 deny udp any any eq 31337 log
! Deny RPC
access-list 100 deny tcp any any range 32700 32900 log
access-list 100 deny udp any any range 32700 32900 log
! Attempt to block DDOS Attacks
! the TRINOO DDoS systems
access-list 100 deny tcp any any eq 27665 log
access-list 100 deny udp any any eq 31335 log
access-list 100 deny udp any any eq 27444 log
! the Stacheldraht DDoS system
access-list 100 deny tcp any any eq 16660 log
access-list 100 deny tcp any any eq 65000 log
! the TrinityV3 system
access-list 100 deny tcp any any eq 33270 log
access-list 100 deny tcp any any eq 39168 log
! the Subseven DDoS system and variants
access-list 100 deny tcp any any range 6711 6712 log
access-list 100 deny tcp any any eq 6776 log
access-list 100 deny tcp any any eq 6669 log
access-list 100 deny tcp any any eq 2222 log
access-list 100 deny tcp any any eq 7000 log
!
! access-list 150 applies to traffic from the internal network
```

```
!
! Reset ACL
no access-list 150
! Block LAND attack
access-list 150 deny ip host 5.10.100.33 host 5.10.100.33 log
! Allow some ICMP
access-list 150 permit icmp 5.10.100.32 0.0.0.15 any echo
access-list 150 permit icmp 5.10.100.32 0.0.0.15 any parameter-problem
access-list 150 permit icmp 5.10.100.32 0.0.0.15 any packet-too-big
access-list 150 permit icmp 5.10.100.32 0.0.0.15 any source-quench
! Block small servers
access-list 150 deny tcp any any range 1 19 log
! Block Supdup
access-list 150 deny tcp any any eq 93 log
! Block NetBIOS
access-list 150 deny tcp any any range 135 139 log
! Block CIFS
access-list 150 deny tcp any any eq 445 log
! Deny NFS
access-list 150 deny tcp any any eq 2049 log
access-list 150 deny udp any any eq 2049 log
! Block more problematic services
access-list 150 deny tcp any any range 512 518 log
! Block uucp
access-list 150 deny tcp any any eq 540 log
! Permit the rest
access-list 150 permit tcp 5.10.100.32 0.0.0.15 gt 1023 any lt 1024
! Permit DNS requests
access-list 150 permit udp 5.10.100.32 0.0.0.15 gt 1023 any eq 53
access-list 150 permit udp 5.10.100.32 0.0.0.15 any range 33400 34400 log
! Block anything not on the 5.10.100.32/28 network
access-list 150 deny tcp any range 0 65535 any range 0 65535 log
access-list 150 deny udp any range 0 65535 any range 0 65535 log
access-list 150 deny ip any any log
!
! access-list 175 applies to remote access from specific hosts
! (172.28.1.100 and 172.28.1.101) to the router for mgmt.
no access-list 175
access-list 175 permit tcp host 172.28.1.100 host 0.0.0.0 eq 23 log
access-list 175 permit tcp host 172.28.1.101 host 0.0.0.0 eq 23 log
access-list 175 deny ip any any log
!
! Turn SNMP off
no snmp
no snmp-server location
no snmp-server contact
!
line vty 0 4
access-class 175 in
password 7 123456789012345678901234
login
transport input telnet
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 5.3.36.22
no ip http server
banner #unauthorized access prohibited.#
!
line console 0
 exec-timeout 0 0
```

```
 password 2manysecrets
 login
!
line vty 0 4
 password 2manysecrets
 login
!
end
```

2.2 – VPN CONFIGURATION

GIAC provides VPN access for its end users, customers and partners/suppliers for various services on the GIAC network. The VPN device used by GIAC is the Symantec Enterprise VPN (SEVPN) running on Windows 2000. This VPN server was chosen because of it ease of use as well as the scalability for the number of VPN users on the GIAC network.

2.2.1 – TYPES OF ENCAPSULATION PROTOCOLS ON THE SYMANTEC VPN GATEWAY

SEVPN supports three types of VPN encapsulation protocols:

- IPSec/IKE
- IPSec Static
- SwIPe

GIAC uses the IPSec/IKE protocol for its VPN tunnels because it supports multiple configuration parameters in a single policy. The configuration parameters are dynamically negotiated thereby reducing the number of connection problems associated with statically assigned parameters. When using statically assigned configuration parameters, mistakes can be made by the administrator when setting up the parameters. If both the client and the server do not have matching parameters, the VPN connection fails. With dynamically assigned parameters, the problems are reduced once the first VPN client is work because all subsequent VPN clients can utilize the known working configuration and make a connection.

2.2.2 – VPN POLICIES

SEVPN ships with default IPSec/IKE policies that have been modified by GIAC for use in the VPN policies for its users. The options chosen for the VPN policies are as follows:

Data Integrity Preference – Data Integrity is used in authenticating packets.

- SHA1 – slower than MD5 but is more secure
- MD5

Data Privacy Preference

The Data Privacy option is the encryption algorithm that encrypts the actual data packet. The encryption options chosen by GIAC are:

- 3DES – slower than DES but more secure
- DES

Diffie-Hellman Preference

Diffie-Hellman is the standard by which shared keys are established. For more information on Diffie-Hellman, see the RSA Cryptography FAQ at http://www.rsasecurity.com/rsalabs/faq/3-6-1.html.

- Group2
  - Group2 Diffie-Hellman utilizes 1024 bits. It is more secure but takes up more CPU time.
- Group1
  - Group1 Diffie-Hellman utilizes 768 bits.

Tunnel and Transport Mode

All VPN tunnels use what is known as Tunnel Mode encapsulation. SEVPN allows for two types of encapsulation modes – Tunnel and Transport. Transport mode is only allowed between two entities with the same address as their external gateway address or between an entity with the same address as its external gateway address and a SEVPN Client entity. All endpoints in GIAC VPN tunnels include either a specific host entity or a subnet entity.

2.2.3 – GIAC VPN CONFIGURATION

The following lists the VPN configuration on the SEVPN for each of the tunnels:

Common Criteria
Security Gateway
Name: SG_Ext
IP Address: 5.10.100.34
VPN Policy: GIAC_Default_VPN_Policy

Customers
Secure Tunnel
Name: Customer_Secure_Tunnel
Local Entity: Hst-ftporder.giac.com
Local Gateway: SG_Ext
Remote Entity: VPN_CustomerGroup

Address Transform
Name: Customer_Gateway_Address_Transform

Coming In Via: Customer_Secure_Tunnel
To Server: Hst-ftporder.giacent.com
Going Out Via: Servicenet2
Client Address Transform: Use Gateway Address

Rule
Description: Allow VPN Customers
For Connections Coming In Via: Customer_Secure_Tunnel
Destined For: Hst-ftporder.giacent.com
Coming Out Via: Servicenet2
Services: FTP Ping ssh-customers

Supplier/Partners
Secure Tunnel
Name: SP_Secure_Tunnel
Local Entity: Hst-sftp.giacent.com
Local Gateway: SG_Ext
Remote Entity: VPN_SPGroup

Address Transform
Name: SP_Gateway_Address_Transform
Coming In Via: SP_Secure_Tunnel
To Server: Hst-sftp.giacent.com
Going Out Via: Servicenet2
Client Address Transform: Use Gateway Address

Rule
Description: Allow VPN Supplier/Partners
For Connections Coming In Via: SP_Secure_Tunnel
Destined For: Hst-sftp.giacent.com
Coming Out Via: Servicenet2
Services: FTP Ping ssh-sp

Employees

User Group
Name: VPN_Employees

VPN Network Parameters
Primary Nameserver: 172.28.1.53
Secondary Nameserver: 172.28.1.54
Primary Wins Server: 172.28.1.29
Secondary Wins Server: 172.28.10
PDC: 172.28.1.10

Secure Tunnel
Name: Employee_Secure_Tunnel
Local Entity: Sub_172.28.1.0
Local Gateway: SG_Ext
Remote Entity: VPN_Emloyees

Address Transform
Name: Employee_Gateway_Address_Transform
Coming In Via: Employee_Secure_Tunnel
To Server: Sub-172.28.1.0
Going Out Via: Internetnet
Client Address Transform: Use Gateway Address

Rule
Description: Allow VPN Employees
For Connections Coming In Via: Employee_Secure_Tunnel
Destined For: Sub-172.28.1.0
Coming Out Via: Internalnet
Services: Ping Nbdgram Cifs*

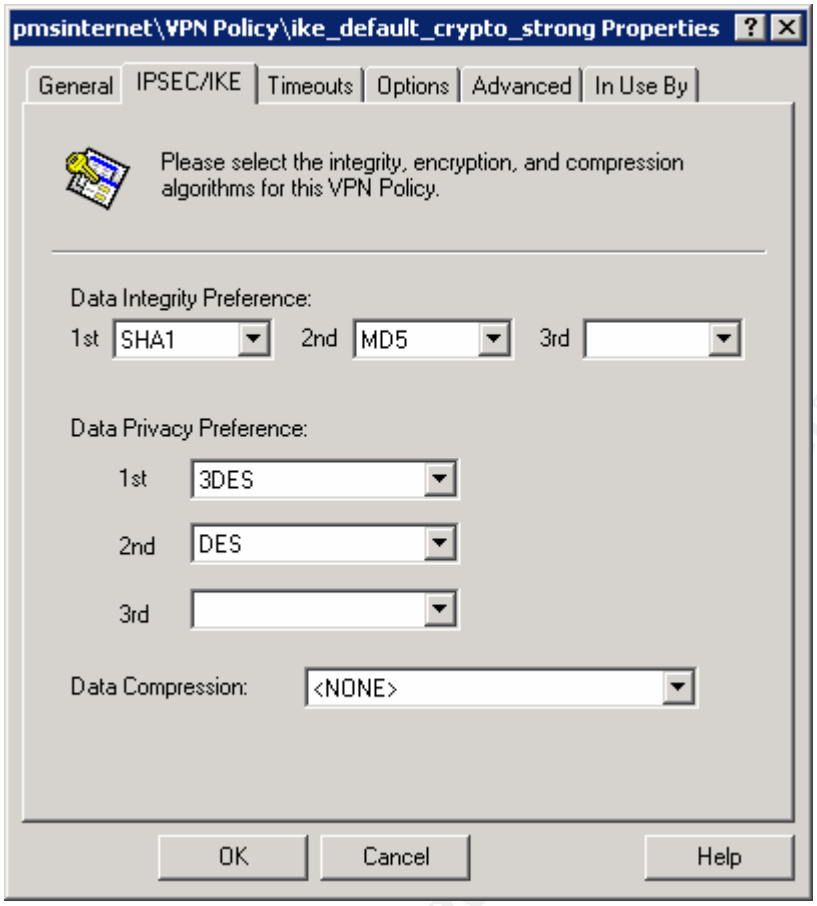


Figure 7 - Example of the IKE Properties dialog

2.3 – TUTORIAL ON THE INSTALLATION AND CONFIGURATION OF THE SYMANTEC ENTERPRISE FIREWALL

2.3.1 – INSTALLATION OF THE SYMANTEC ENTERPRISE FIREWALL

Installation of the Symantec Enterprise Firewall (SEF) on the Windows 2000 is a relatively straightforward procedure. However, certain tasks need to be performed prior to installing the software.

The Symantec Enterprise Firewall Installation Tasks:

1. Format your system drive(s) with the NTFS file system.

2. Install all network interface cards with the latest drivers.

3. Install at least Windows 2000 Service Pack 2. Check with Symantec Support prior to installing any later service packs.

4. If you wish to receive audible alerts, verify that your sound card is functional.

5. Verify that your modem is Hayes compatible and is functioning if you wish to receive pager alerts.

6. Verify that your system's routing tables are correct.
    a. If you are running on a routed network, verify that your machine can ping the other networks in your environment if they are going to be accessing the Internet through your firewall.
    b. Verify that the separate networks can ping the internal network card on the SEF machine.

7. Request a license key from Symantec.
    a. You will need the volume ID from your system drive.
    b. Type **vol %systemdrive%** at the command prompt on the computer you will be installing SEF.
    c. The volume serial number is what is needed for Symantec Licensing

Once the prerequisites have been performed, navigate to \SYMC_fw_vpn\3DES (for High Encryption) or the \SYMC_fw_vpn\DES on the CD drive and double-click the "SETUP.EXE" file.

You will be led through a series of screens that will, most notably, take you

through reading the license agreement, inputting your license key (if you have one), and whether you want to install the documentation and the Symantec Raptor Management Console (SRMC). You will also need to indicate which drive you would like to install the firewall. If you choose to install the SRMC, you will also be prompted with the license agreement for this software as well as the installation destination for the SRMC. Once you have indicated your willingness to agree with the license and the installation directory, the actual installation of the software will commence on your hard drive.

After the firewall software has gone through the software installation process, you will then be prompted to specify your internal and external network addresses. All networks that contain addresses that are assigned by you and not your Internet Service Provider are considered internal networks. This includes any service networks that you will be using.

Finally, the installation program will prompt you to create your SEF Local Management password. This password is used to access the SEF through the SRMC on the local machine. If you wish to manage the firewall from remote machines, you will need to assign those passwords later. All passwords on the SEF are case-sensitive.
.

2.3.2 – CONFIGURATION OF THE SYMANTEC ENTERPRISE FIREWALL

LOGGING ONTO THE SYMANTEC RAPTOR MANAGEMENT CONSOLE

The installation process places an icon called "Symantec Raptor Management Console" on your desktop and an icon in your Start menu under Start | Programs | Symantec Raptor Management Console called "Raptor Management Console".

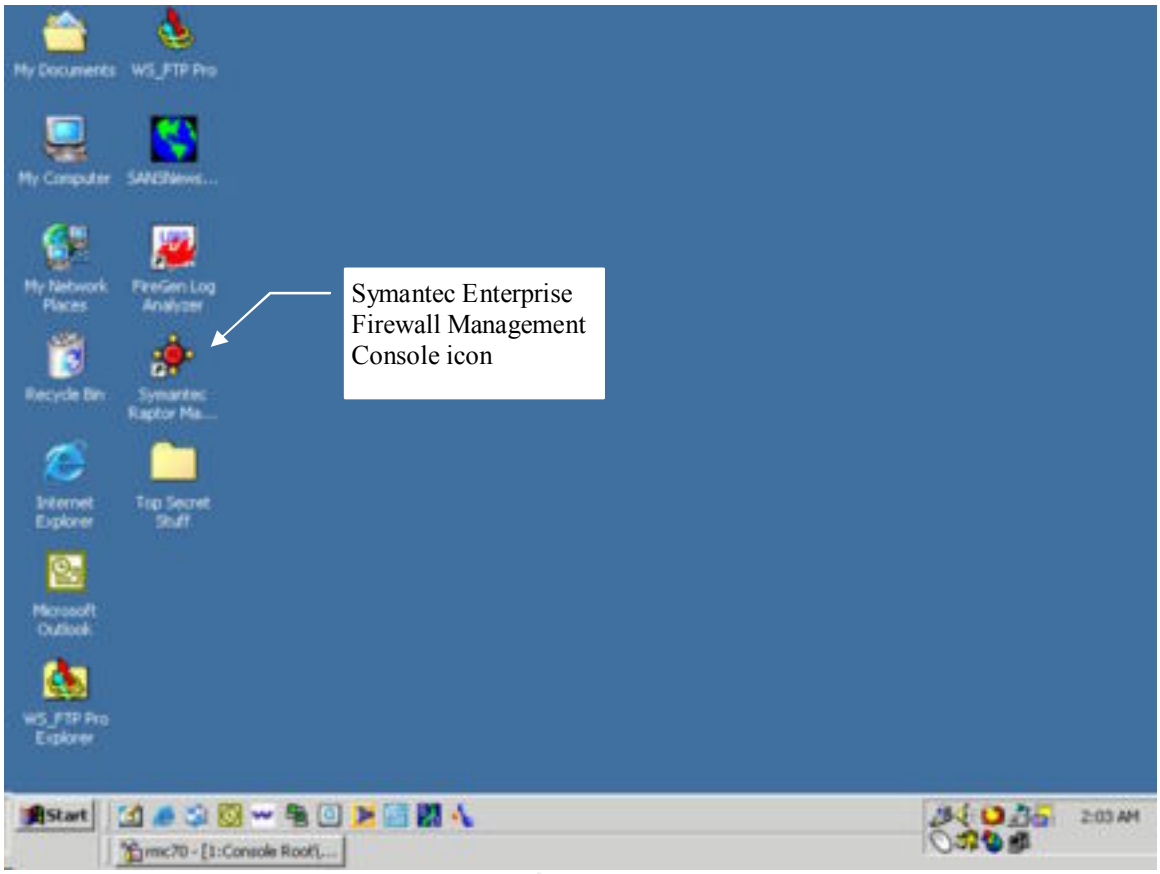


Figure 8 - Symantec Raptor Management Console desktop icon

These two icons perform the same task; they start the Microsoft Management Console application for the Symantec Enterprise Firewall.

Open the SRMC by using one of the two methods above. You will be shown the screen in figure 8.

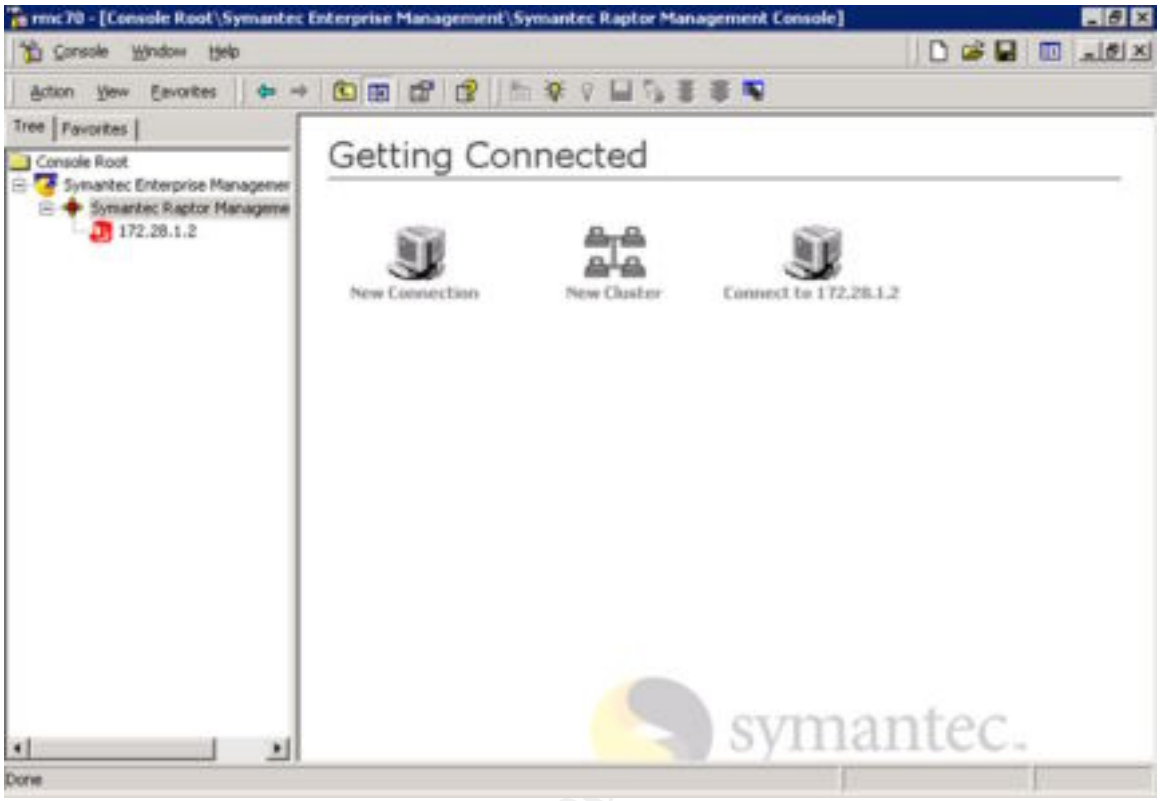


Figure 9 - Symantec Raptor Management Console

The GIAC firewall resides at the internal address of 172.28.1.2. We will need to connect to that address on the SRMC by clicking the icon that states "Connect to 172.28.1.2".

Next, we will be prompted for the console password. The installation program had asked for this same password. Type this password in the appropriate place and click OK. Remember that all passwords on SEF are case-sensitive.

Figure 10 - SRMC login screen

If you typed in the correct password, the management console address will now have a green icon (instead of red) and you will now have access to the management portion of the console.

2.3.3 – CONFIGURING THE FIREWALL

SEF Routing Table

The first step in configuring the SEF is to verify that your routing is setup correctly. If you haven't set up static routes within the Windows 2000 operating system, you can configure routing tables through the SRMC.

The steps to configure routing through the SRMC are as follows:

1. Click the plus (+) sign next to the firewall name or IP address. In the case of the GIAC network, the firewall name is GIACFW.

2. Next, either click the plus sign (+) next to Base Components on the left pane or click Base Components itself.

3. Click Routes on either the left pane or the right pane. The location of your click is dependant upon where you clicked in the previous step.

4. We will set the following routes for the GIAC firewall:
    a. 0.0.0.0 will route out through the external interface
    b. 172.28.0.0 will route through the internal interface
    c. 192.168.44.0 will route through the servicenet0 interface
    d. 10.100.1.0 will route through the servicenet1 interface
    e. 10.100.2.0 will route through the servicenet2 interface
    f. 10.100.3.0 will route through the servicenet3 interface

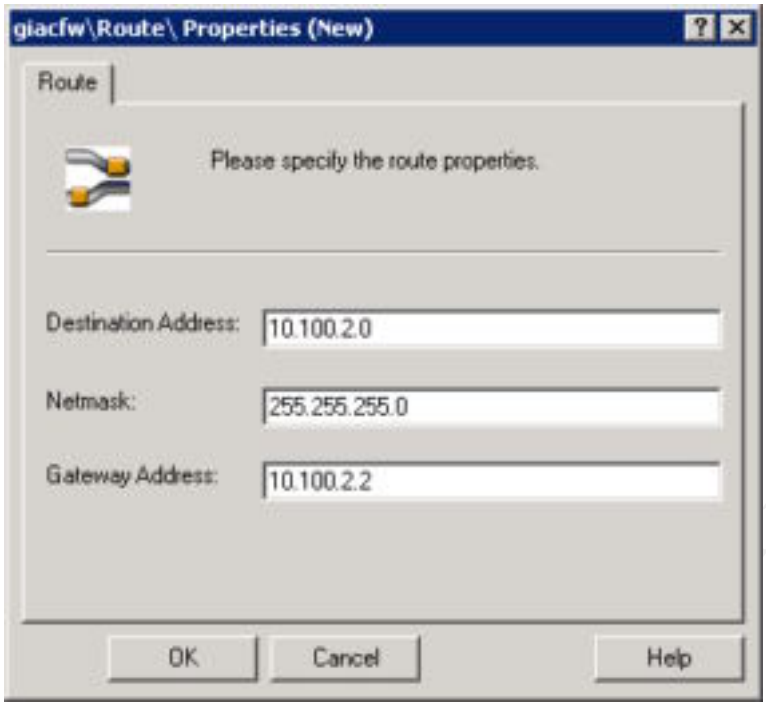


Figure 11 - Configuring the 10.100.2.0 route

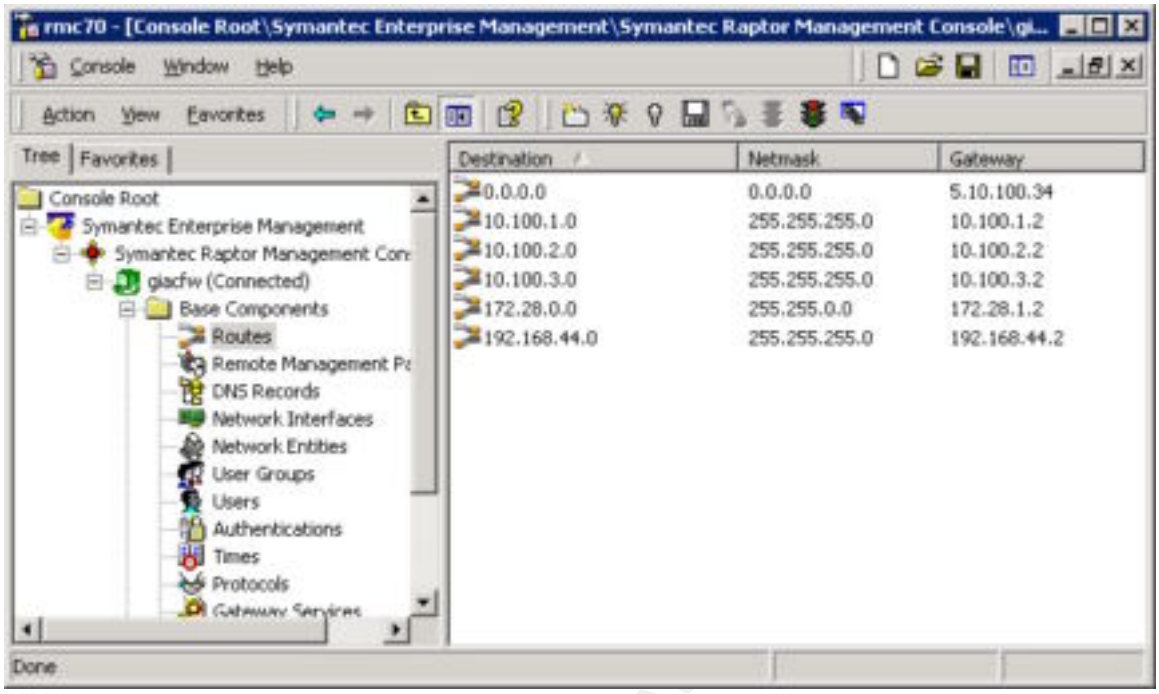


Figure 12 - GIACFW Routing Table

Remote Management and Log Retrieval Configuration

GIAC has a remote management station for the network administrator located at 172.28.1.50, 172.28.40.13 and 10.100.3.50. We will need to configure the SEF to allow access to the firewall for management from these workstations. GIAC also has a log server located at 172.28.1.10. Access to the log files needs to be allowed for the machine located at that address.

Steps for setting up remote management permissions:

1. Under Base Components, click Remote Management.

2. Right click in the right pane and choose New > Remote Management Password.

3. The Remote Management option is selected by default; if this isn't the case, click the radio button for this selection.

4. For Remote Management System, type 172.28.1.50.

5. Type the password that will be used to access the firewall from this workstation. All passwords are case-sensitive.

6. Click OK.

7. Repeat 1-6 for 10.100.3.

All management machines will need to run the SRMC setup program from the SEF CD in order to install the management program.

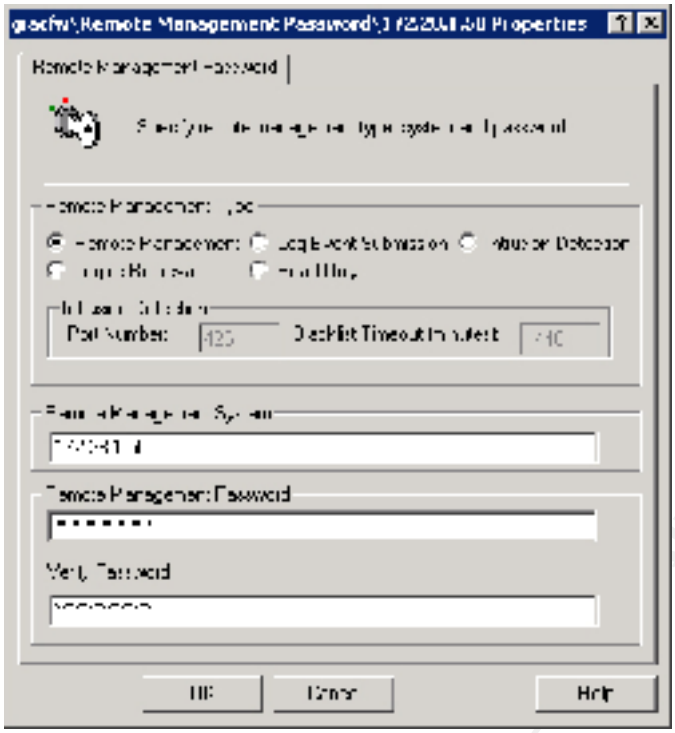


Figure 13 - Configuring A Remote Management Password

Next, we will need to configure the firewall to allow syslog.giacent.com access to the firewall for logfile retrieval.

The steps to be followed in order to allow the syslog server the ability to access firewall logs:

1. In the right-hand pane of the SRMC under Remote Management Passwords, right-click and choose File > New > Remote Management Password

2. Click Logfile Retrieval.

3. Under Remote Management System, type 172.28.1.10

4. Type the password that will be used by syslog.giacent.com to access the firewall logs.

5. Click OK.

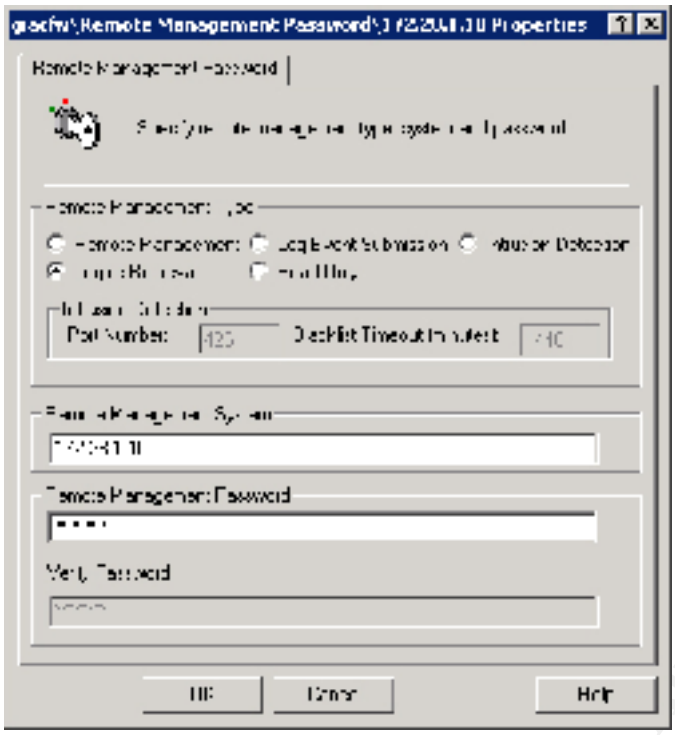


Figure 14 - Configure the logfile retrieval workstation password

The other options, Log Event Submission, Intrusion Detection and Read Only will not be used at GIAC at this time.

DNS Configuration

GIAC uses two separate domain names to distinguish between the internal network (giacent.com) and the external network (giac.com). This was designed in this manner in order to prevent confusion when configuring the DNS structure for GIAC. Figure 8 illustrates the location of the DNS servers for the two domain names used by GIAC.

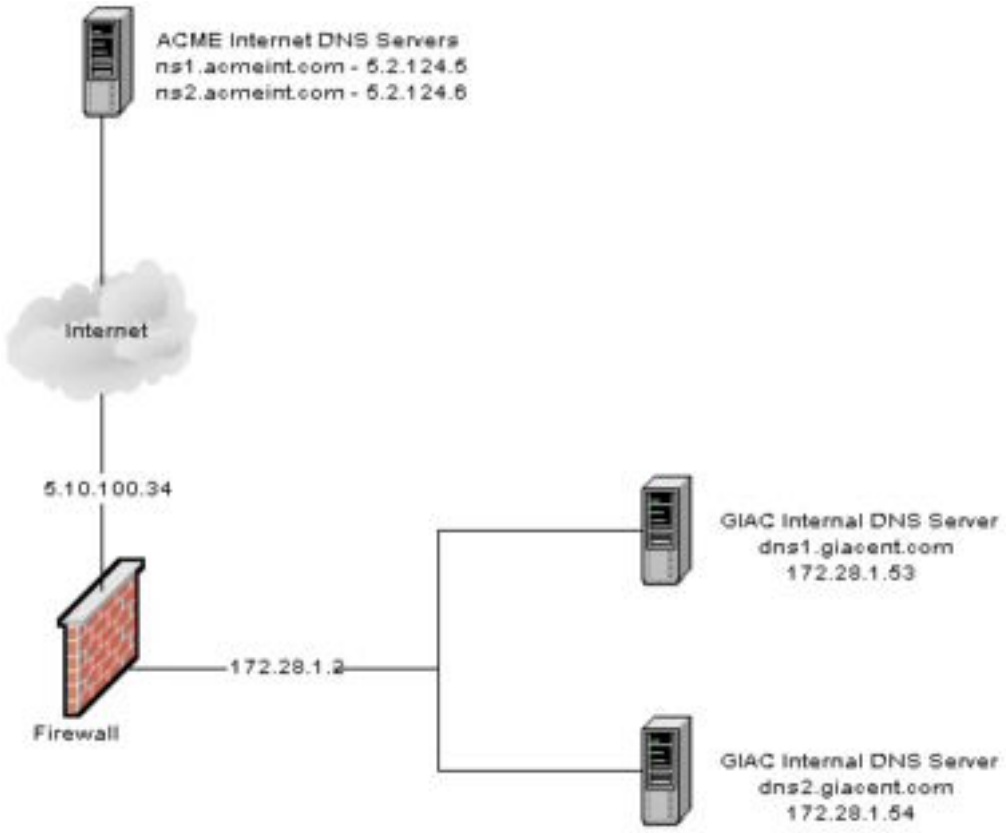


Figure 15 - GIAC DNS Configuration

GIAC uses a split-level DNS configuration . The internal DNS servers are located on the 172.28.1.0 network and the ISP hosts the external DNS for giac.com. Giacfw acts as a forwarder for the Internal DNS requests to the outside. All DNS configuration for giac.com for the outside world is managed by ACKME Internet Services.

The Internal DNS servers need to be specified in the SRMC in order for split-level DNS to occur.

The steps to adding the internal DNS servers to the SRMC:

1. Right click on DNS Records and select New > Name Server.

2. Select the Private radio button

3. Type in the FQDN (fully qualified domain name) of the internal DNS server. Ex. dns1.giacent.com

4. Type the IP address of the dns server

5. Add the domain and and reverse zone for the internal network.
    a. giac.com 28.172.in-addr.arpa

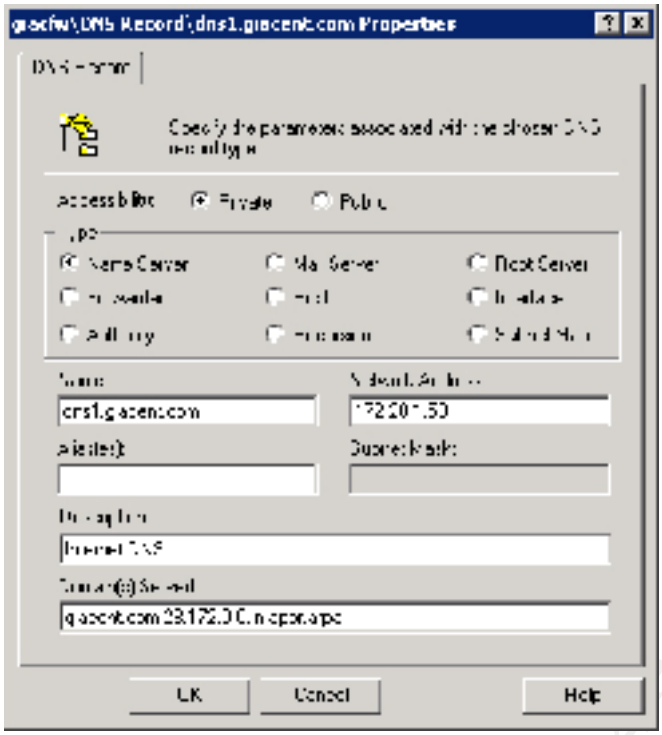


Figure 16 - Configure internal DNS servers

In order for giacfw to act as a DNS forwarder for the internal DNS servers, the DNS servers on the internal network need to add to their DNS tables a forwarder record for giacfw. The steps to accomplish are dependent upon the DNS server software. The following line has been added to the internal DNS servers' configuration file on the GIAC network:

```
options {
     forwarders { 172.28.1.2; };
```

The giacfw computer needs to specify its forwarders as well. This is accomplished by adding a forwarder record to the firewall configuration.

Steps to specify DNS forwarders on the firewall:

1. Under Base Components, select DNS Records.
2. Right-click in the right hand pane and choose New > Forwarder
3. Type the IP Address of ns1.ackme.com (5.2.124.5)
4. Type Ackme Internet Services NS1 in the Description box.
5. Click OK.

6. Repeat steps 2-5 for ns2.ackmee.net

Network Interfaces

The next section covers the configuration of the Network Interfaces with the SRMC.

The following steps have been performed on the giacfw SEF:

1. Click Network Interfaces on the left pane of the SRMC.

2. Right click on the interface you wish to configure and select properties

3. In the *Name* field, type a name for the interface that best describes the location of the network the interface is located.
    a. 172.28.1.2 – Internalnet
    b. 10.100.1.2 – Servicenet1
    c. 10.100.2.2 – Servicenet2
    d. 10.100.3.2 – Servicenet3
    e. 192.168.44.2 – Servicenet0
    f. 5.10.100.34 – Externalnet

4. In the *description* field, type a description for the Network Interface.
    a. Internalnet – "Internal GIAC Network"
    b. Servicenet1 – "Hosts public web servers"
    c. And so on…

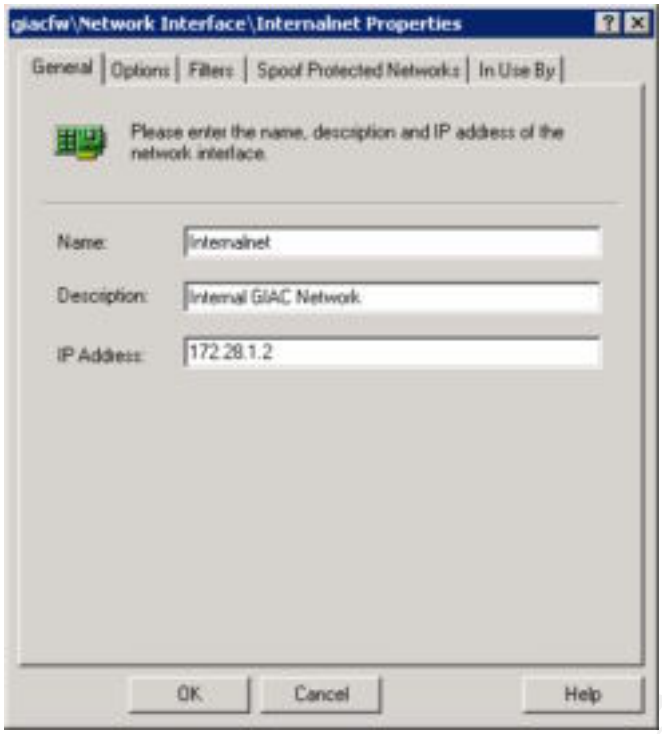


Figure 17 - Network Interface properties

5. Click the Options tab.

6. For the internal and service networks, verify that *This address is a member of the internal network* is checked.

7. Leave *Allow Multicast (UDP-based) Traffic* and *Enable SYN Flood Protection* unchecked.

    a. Multicast traffic will not be passing through any of the Interfaces on the firewall.
    b. SYN Flood Protection should only be enabled whenever an attack has been detected by the IDS since SYN Flood Protection is known to take up a large amount of resources on the firewall.

8. Check *Enable Port Scan Detection*

    a. Multiple log messages with the ID of 347 indicate that a port scan is taking place on the interface.

9. Filters will not be applied to the GIACFW firewall. Click the *Spoof Protected Networks* tab.

10. For the external Network Interface select all internal

networks and service networks

11. Highlight the appropriate subnet in the *Excluded Members* and click the button labeled ">>"

12. Repeat the above steps for each interface.

Network Entities

We need to identify all Hosts, Groups of Hosts, Subnets, Gateways, Domains and Workgroups that will be passing through the firewall. This is performed on the SRMC under the *Network Entities* section.

Below is a list of types of Entities with the description of the entity, the identifier that GIAC will be using during the configuration of the firewall entities and an example of setting up an entity if it applies to the GIAC environment:.

Note: When describing the steps to perform when created entities, I will take one entity as an example. The remaining entities will follow the same procedures.

Host Entities

Individual machines with either IP addresses or DNS host names. IP addresses are the preferred method of specifying the entity location but DNS host names will be acceptable for hosts that change without the GIAC Security Department's knowledge such as websites with multiple IP addresses in a round robin DNS setup.
A special host entity is created upon installation. This entity is named Universe*. The Universe* entity specifies everything on the network in which the entity appears in the firewall rule.
The format we use to specify a host entity in the firewall is **Hst-***entityname*
Steps outlining the creation of a host entity for Internal mail server (exchange.giacent.com):

1. Click Network Entities in the left pane of the SRMC

2. Right click in the open space and click *New* > *Host*

3. In the *Name* field, type **Hst-exchange.giacent.com**

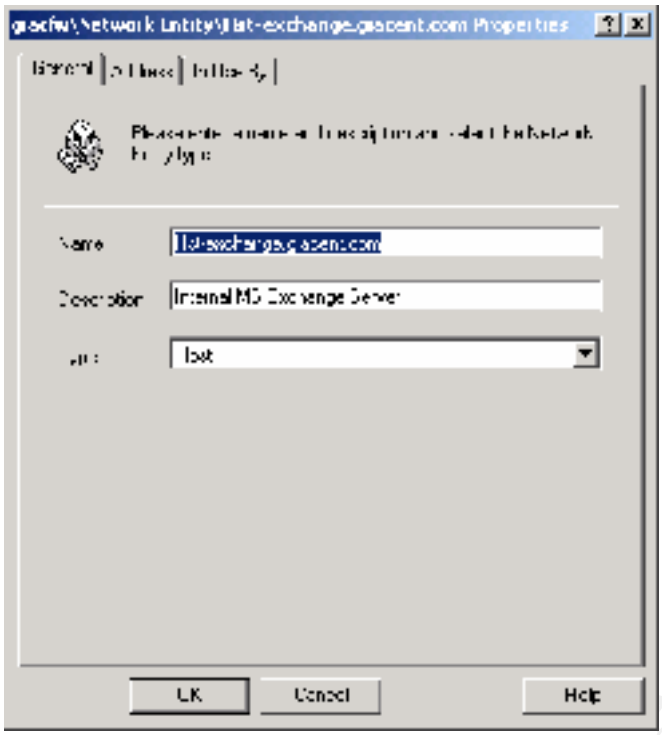


Figure 18 - Host Entity

4. In the *Description* field, type "Internal MS Exchange Server"

5. Click the *Address* tab

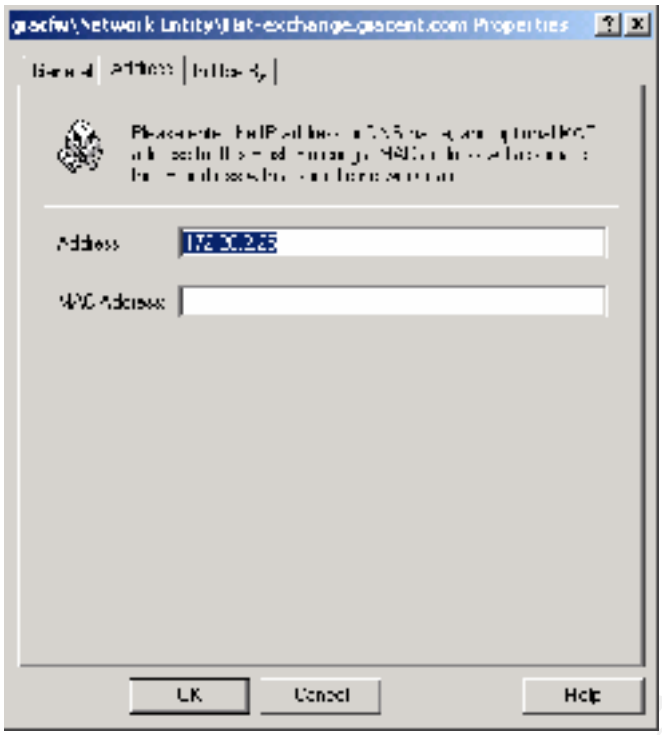


Figure 19 - Host IP Address

6. Type **172.28.2.25**
7. Click OK to exit
8. Click Save and Reconfigure

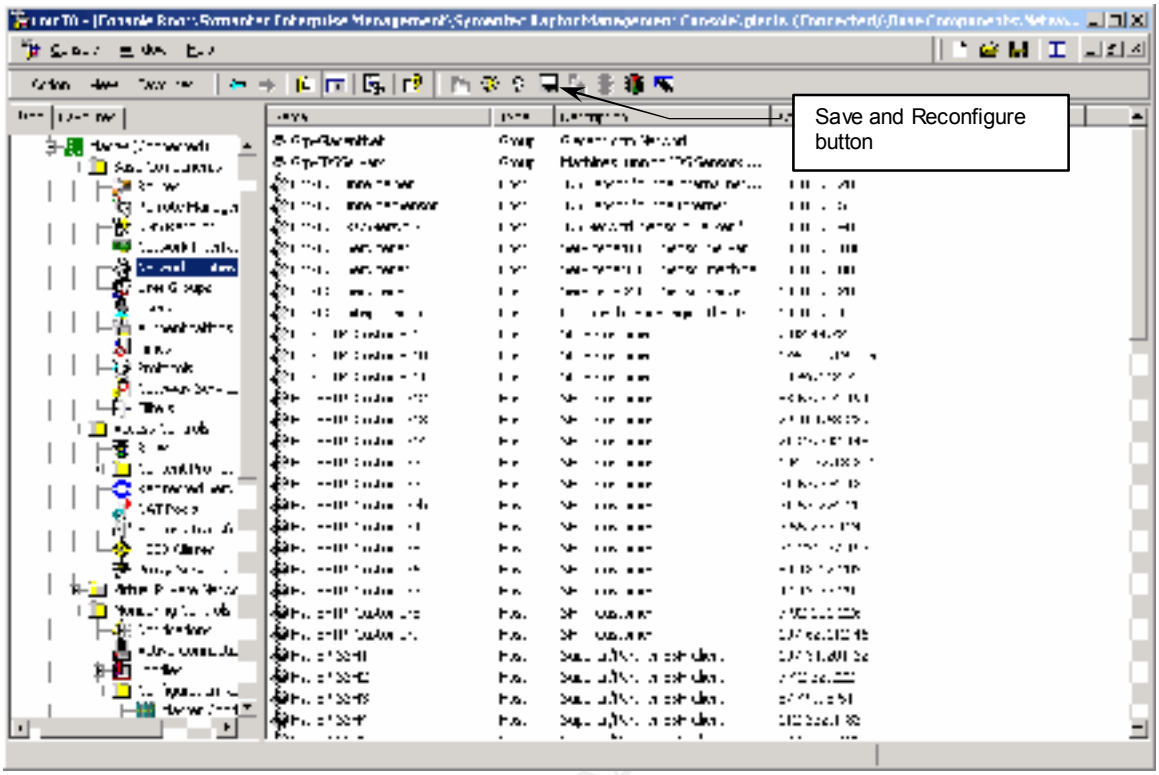


Figure 20 - Click the Save and Reconfigure button after each update

Subnet Entities

Subnet entities are those that specify an IP subnet. These entities are helpful when you'd like to add groups of computers to the firewall without specifying each individual machine on the firewall.
The format used by GIAC to specify a subnet in the firewall entity list is **Sub-*subnet***

Steps to create subnet entity on the firewall:

1. Click Network Entities in the left pane of the SRMC
2. Right click in the open space and click *New* > S*ubnet*
3. In the *Name* field, type **Sub-Servicenet1**
4. In the *Description* field, type **Servicenet1 subnet**

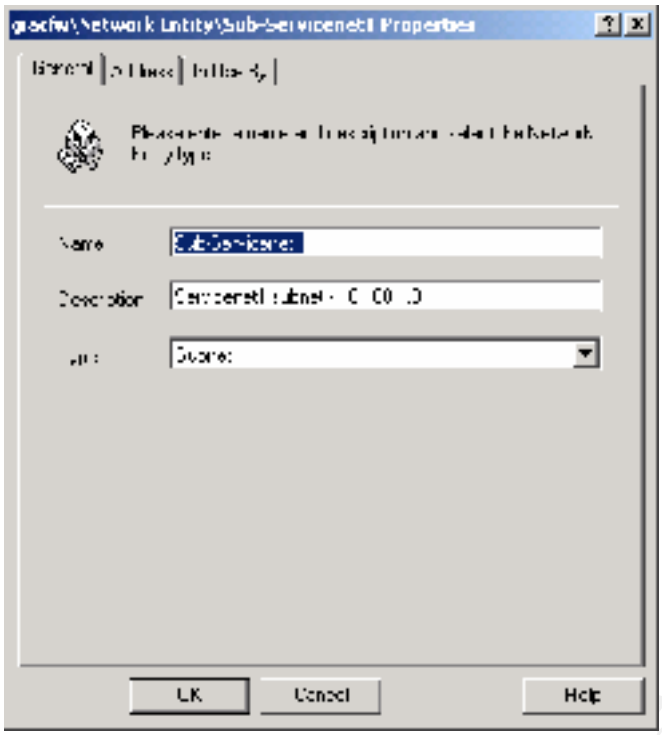


Figure 21 - Subnet Entity

5. Click the *Address* tab
6. In the *Address* field, type **10.100.1.0**
7. In the *Subnet* field, type **255.255.255.0**

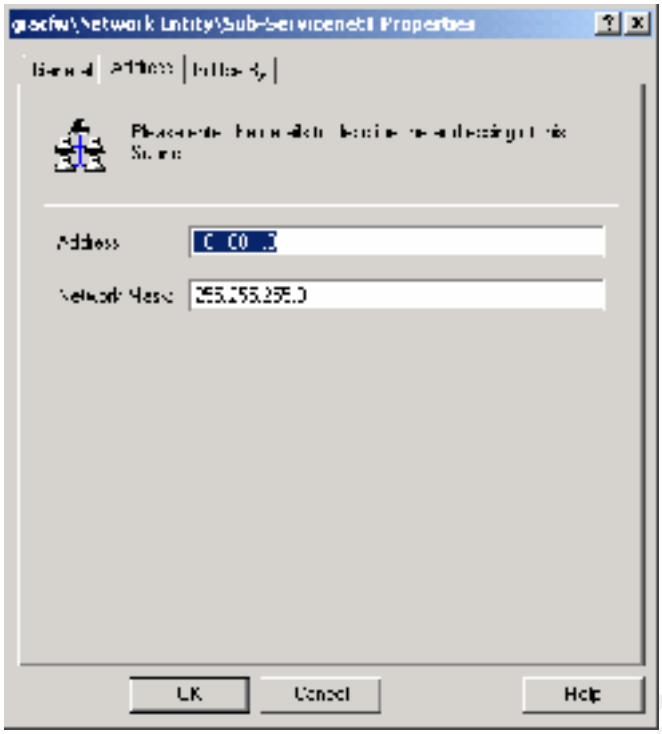


Figure 22 - Subnet Entity Network Address Screen

8. Click OK to exit
9. Click *Save and Reconfigure*

Domain Entities

Domain entities are used to specify a DNS domain name in the firewall. For example, if you want to group all computers in the giac.com domain, you specify giac.com as a Domain entity.
The format GIAC uses to specify a domain entity in the firewall SRMC is **Dom-*domain***

Steps to add a Domain entity:

1. Click Network Entities in the left pane of the SRMC
2. Right click in the open space and click *New* > Domain
3. In the *Name* field, type **Dom-giac.com**
4. In the *Description* field, type **giac.com domain**

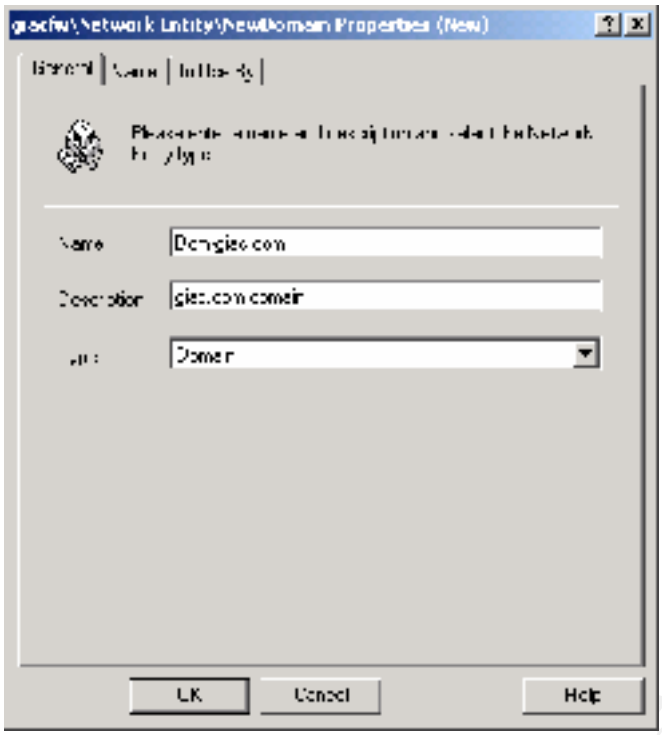


Figure 23 - Domain Entity

5. Click the *Domain* tab
6. In the *Domain* field, type **giac.com**

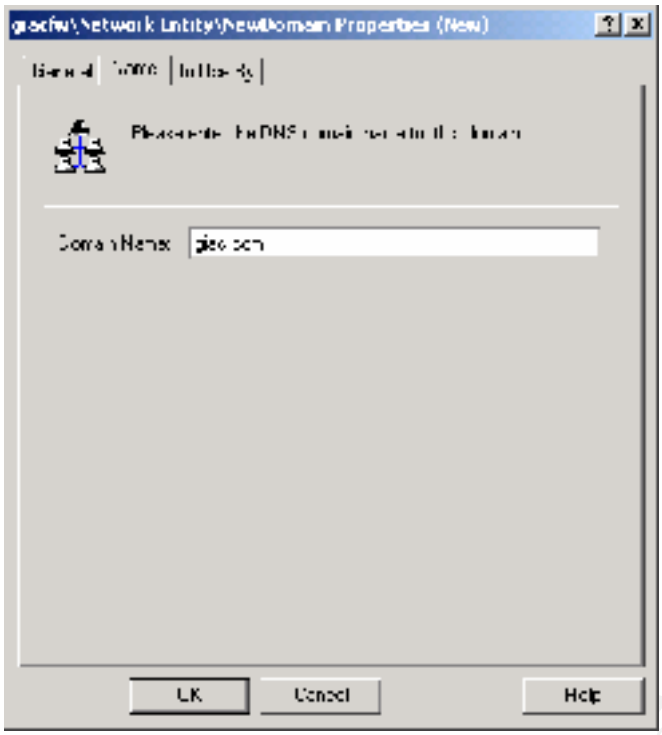


Figure 24 - Specifying the domain name

7. Click OK to exit

8. Click *Save and Reconfigure*

Groups

- Group entities group together hosts, subnets and domains as a single entity. This makes writing rules easier as multiple entities may use similar rules to access through the firewall.
- The format used by GIAC to specify a group name in the firewall is **Grp-***groupname*

To create a group of entities, use the following procedure:

1. Click Network Entities in the left pane of the SRMC

2. Right click in the open space and click New > Group

3. In the Name field, type Grp-IDS_Servers

4. In the Description field, type Machines running IDS Sensors or Software

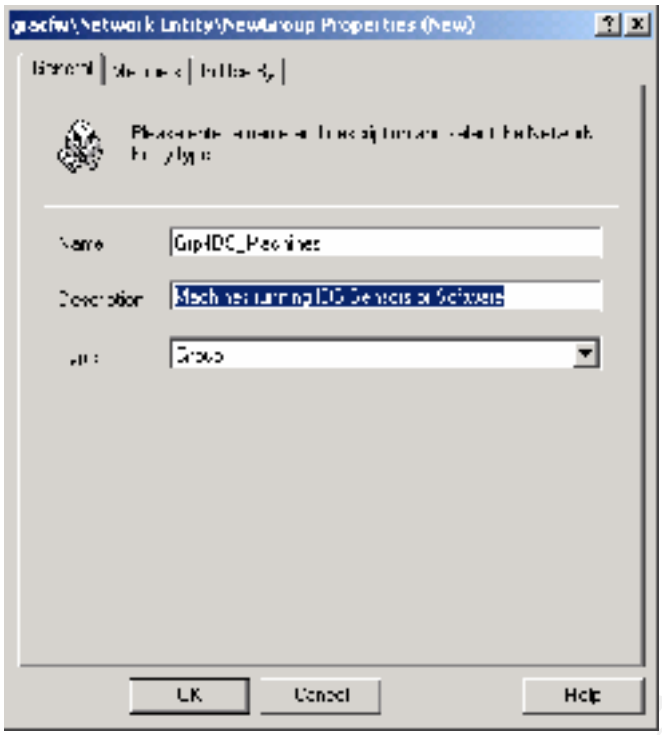


Figure 25 - Group Entity

5. Click Members

6. Highlight the IDS host machines on the right side of the screen

   - Hst-IDS_InternalNet
   - Hst-IDS_InternetSensor
   - Hst-IDS_RASNetwork
   - Hst-IDS_Servicenet0
   - Hst-IDS_Servicenet1
   - Hst-IDS_Servicenet2
   - Hst-IDS_Siteprotector

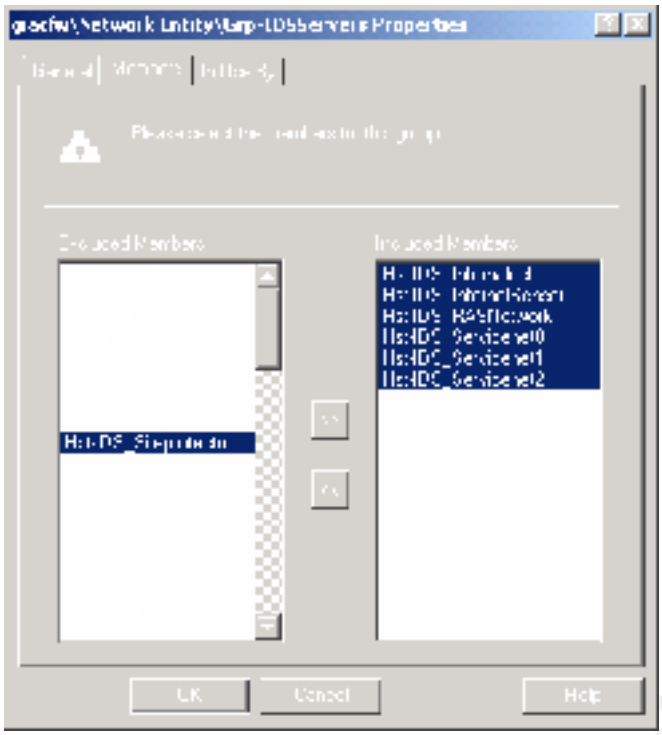


Figure 26 - Selecting Entities for a group

7. Click the **>>** button to move the entities to the *Included Members* side of the dialog box.

8. Click **OK**

9. Click Save and Reconfigure

Security Gateways

- The entities are used to establish secure tunnels through the firewall. A Security Gateway acts as an endpoint in a VPN connection.

- GIAC uses the format of **Sg-***securitygateway* when specifying security gateways in the firewall.

Steps to create a Security Gateway

1. Click Network Entities in the left pane of the SRMC

2. Right click in the open space and click New > Security Gateway

3. In the Name field, type Sg-VPN1

4. In the Description field, type *GIAC Security Gateway*

Figure 27 - Create a new Security Gateway

5. Click the *Security Gateway* tab

6. Select the IP address for the gateway. This is usually the IP address for the external (Internet) network.

7. Type an optional password in the Shared Secret field.

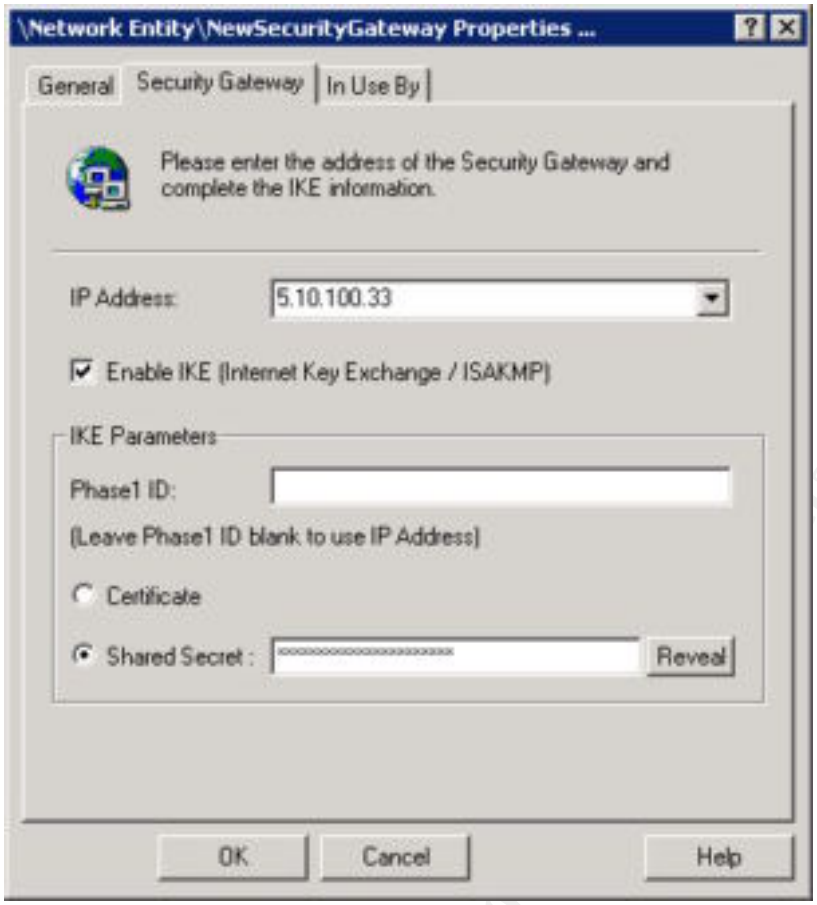


Figure 28 - Specify the gateway address

8. Click OK

9. Click Save and Reconfigure

Workgroup

- A workgroup entity is a pairing of a network entity with a security gateway entity to create an endpoint for use in secure tunnels that use IKE authentication.

- If used, GIAC will specify the workgroup as **Wg-workgroup** in the entities list.

Steps to create a Workgroup Entity

1. Click Network Entities in the left pane of the SRMC

2. Right click in the open space and click New > Workgroup

3. In the Name field, type Wg-VPN_Workgroup

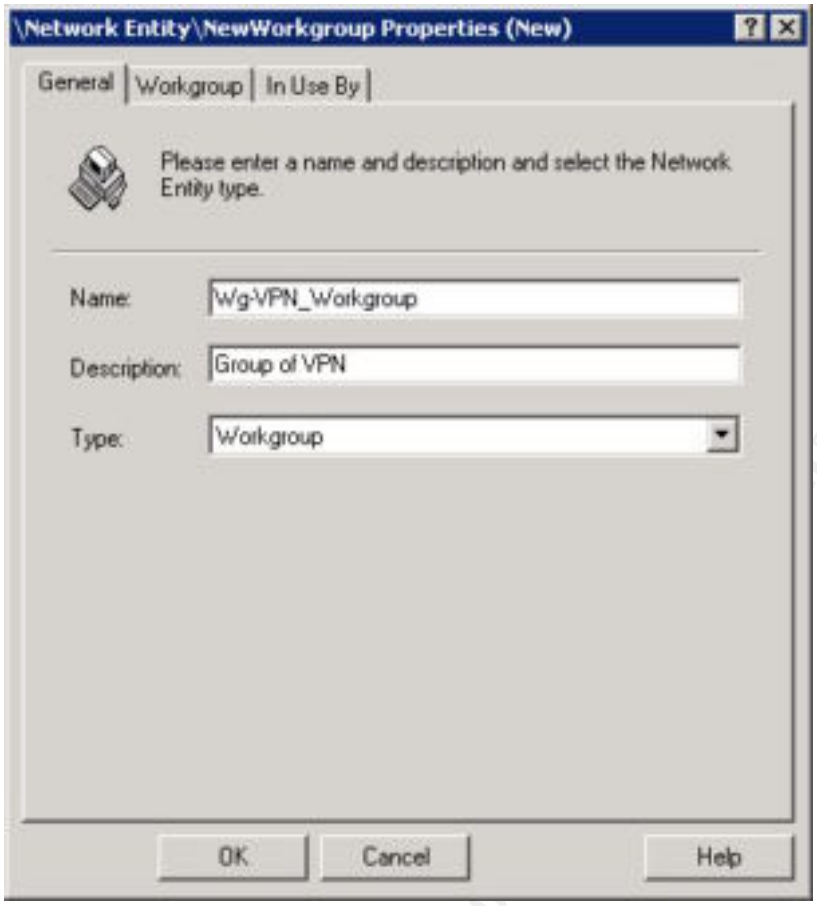


Figure 29 - New Workgroup

4. In the Description field, type Group of VPN entities
5. Click the Workgroup tab.
6. Select the Entity/Gateway combinations for your workgroup.

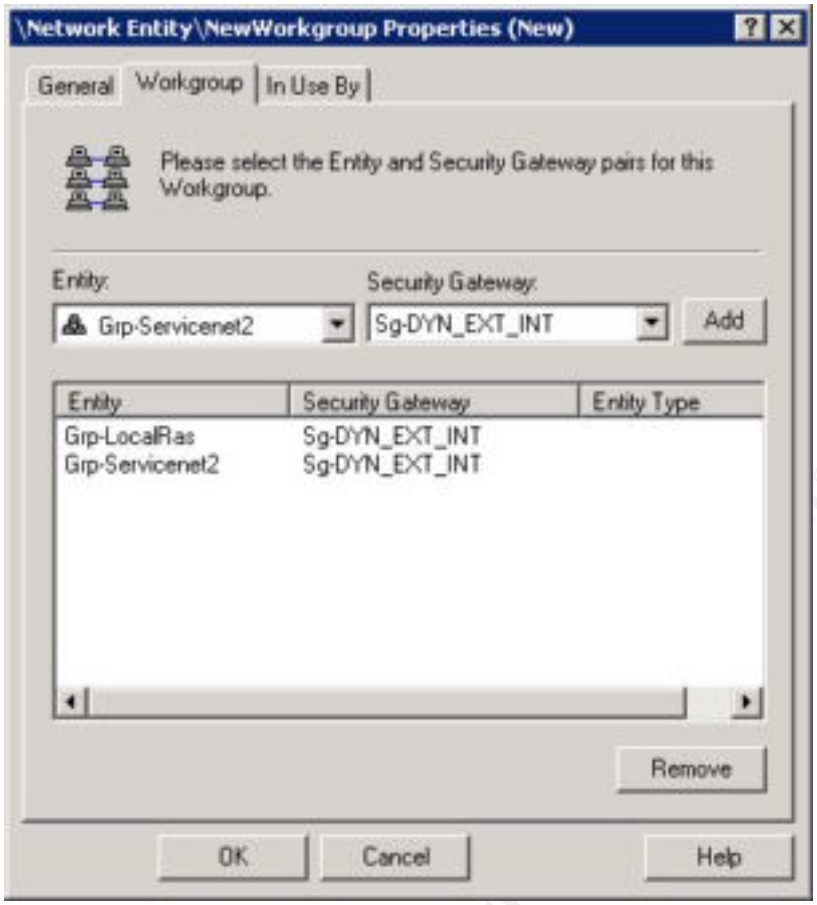


Figure 30 - Specify Workgroup Entity/Gateway pairs

7. Click OK

8. Click Save and Reconfigure

Another network entity is not covered in this tutorial. It is the Raptor Mobile entity. This entity is used by older Raptor VPN clients that must be specified in the firewall.

A listing of all entities on the GIACFW firewall can be found in Appendix A.

2.3.5 – Protocols

SEF protocols are a listing of network ports that can be specified in a rule to either block or allow. An example of a protocol is HTTP or port 80/tcp. "New" protocols can be specified in the firewall if they do not appear in the list already.

GIAC has created custom protocol to allow connections to the two SSH servers that are not running on the assigned 22/tcp port. The GIAC network

administrators felt that running on these ports may invite “script kiddies” to try out the latest tools on the GIAC network to attack an open well-known port. Therefore, the port in which SSH is running has been changed to 1984/tcp on the customer SSH server (ftporder.giac.com) and 9278/tcp on the Partner/Supplier SSH Server.

Custom port numbers are not limited to just the SSH servers. The customer order web server (orders.giac.com) communications with the Microsoft SQL Server (webdata.giacent.com) over port 1776/tcp. Other custom protocols will undoubtedly be required for outbound access by the users at GIAC. For example, there may also be time when a web-based training company requires the use of a custom port in order to connect to their presentation server.

To add the custom protocol 1984/tcp for the customer SSH server, perform the following steps:

1. Right-click *Protocols* in the left pane of the SRMC. You may have to click the plus (+) sign next to *Base Components* first in order to expand the group of objects.
2. Click *New* > *Protocol*

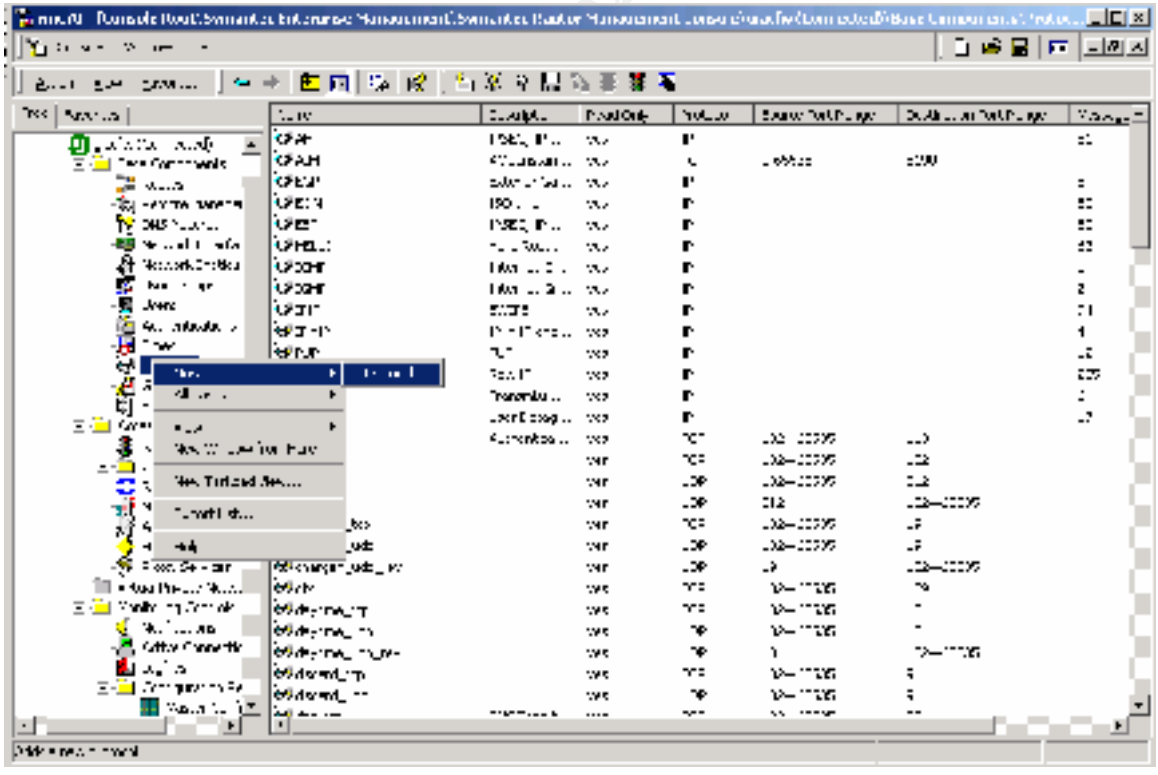


Figure 31 - New Protocol

3. In the *Name* field, type **customer-ssh**

4. In the description field, type **Protocol used by customers accessing the SSH Server**

5. Under *Base Protocol*, select **TCP**

6. We want to use this protocol in our rules so click *Display in Rule Window*

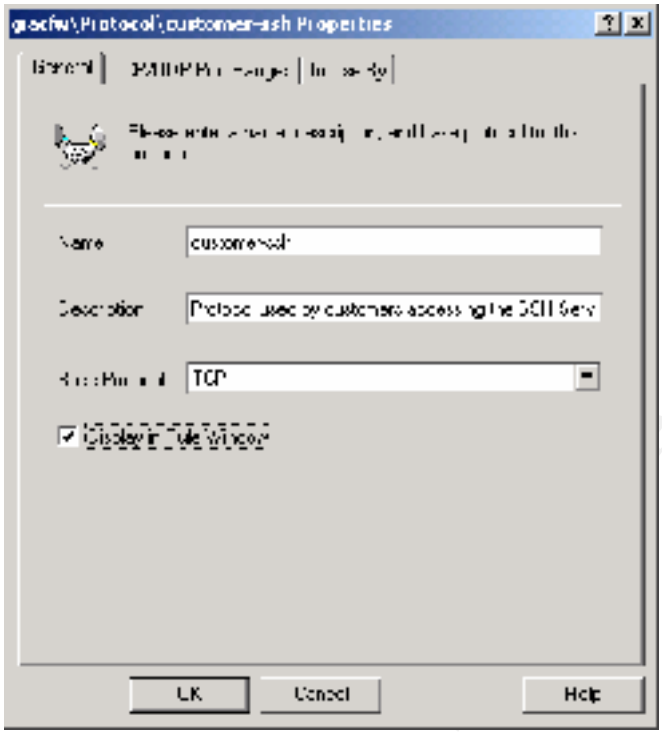


Figure 32 - New Protocol General tab

7. Click the *TCP/UDP Port Ranges* tab

8. In the *Destination Port Range* field, type **1984**

9. In the *Source Port Range* field, type **1024-65535**

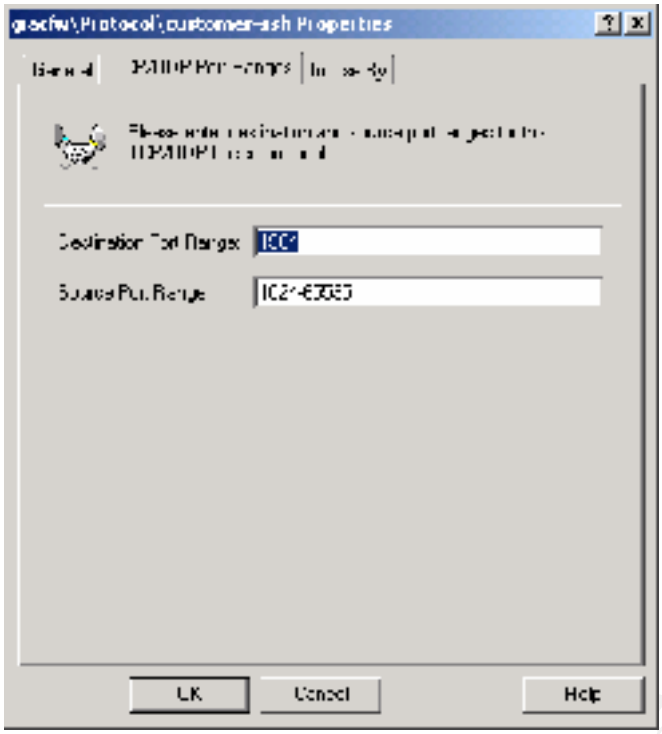


Figure 33 - Specify Source and Destination Ports

10. Click OK

11. Click *Save and Reconfigure*

Note: There is a service named all available when creating a rule. This service acts as a "hole" in the firewall as it represents all protocols and services. It is highly recommended that administrators avoid utilizing this service in permanent rules and should only be used when troubleshooting connection problems. In addition to the potential security lapses it may generate, the any* service also negatively affects overall rule processing performance on the SEF server.*

This concludes base component configuration for the GIACFW firewall. The next step covers the actual firewall rule base.

2.3.6 – FIREWALL RULES

How to write a ruleset for the Symantec Enterprise Firewall

Firewall rules decide what is passed or blocked with regards to network traffic. These rules use the entities, protocols, and network interfaces outlined in previous paragraphs. In addition to the items above, other configuration variables such as *time of day, users and user groups, content profiles* and *authentication methods* are also used in setting up SEF rules.

Whenever a network connection is attempted through the firewall, the SEF will

select the rule that most likely applies. This can either be an ALLOW or DENY rule, meaning the traffic is permitted through the firewall in the ALLOW state or is blocked in the DENY state. By default, the firewall will DENY all traffic unless there is a rule specifically allowing traffic through.

SEF looks at various amounts of information in the ruleset to decide whether or not a rule applies to the traffic attempting to pass. The following outlines what needs to be present in a rule before the firewall will allow (or deny) traffic to pass:

a. *Source and Destination entities*. This requirement is lightened a bit with the Universe* entity. The Universe* entity specifies everything on the network.

b. *Allow or Deny must be specified.* Since all traffic is denied by default, most rules will be Allow rules. A Deny rule should be used whenever you'd like to prevent a certain host or group of hosts from using a broad rule that covers a large amount of hosts that also includes the host or hosts you wish to prevent. An example of this would be if you gave access to the http protocol out to the Internet for everyone in the company but you'd like to prevent the HR group of computers from accessing http. To do this, you would write a DENY rule specifically blocking the http protocol out to the Internet for the HR computers. This rule specifically listing the HR department computers overrides the ALLOW rule.

c. *Protocols must be specified.* Since SEF acts as an application proxy for certain services, a service can also be specified. For example, SEF has an application proxy for FTP. Instead of permitting port 20/tcp and 21/tcp, you should select the FTP* service. This will proxy FTP connection and as an administrator, you can limit the FTP connection to PUTs or GETs depending on the reason for the connection.

d. *Access times must be present.* By default, all rules have a range of time set to ANYTIME. SEF also allows you to limit access by time of day, day(s) of the week, and a specific date range. A typical reason for limiting traffic to specific days would be whenever auditors will be utilizing your Internet connection while they are conducting an on-site audit. By specify the dates they will be on-site in your rule, this prevents temporary rules inadvertently becoming permanent. Granted, a good firewall administrator will keep track of temporary rules but this is an excellent safeguard against those temporary/permanent rules.

e. *Optional Users and User Groups*. While primarily utilized by the VPN connections, users and user groups can be specified in the

firewall rule to prevent anyone from passing traffic even though their network entity is specified in the rule. An administrator can assign users/user groups to a rule that includes every entity on the local network for the FTP protocol. Only certain users may require access through this rule but by specifying users/user groups in the rule, only those with the correct authentication information can utilize the rule.

f. *Data scanning and optional parameters*. SEF allows for additional parameters on rule in order scan the traffic for specific patterns or types of traffic. For example, SEF allows you to deny certain patterns of http traffic through the firewall. The Nimda worm passes the url pattern "/winnt/system32/cmd.exe?/c+dir" to web servers when trying to infect them. By adding this url pattern to the httpurlpattern.cf file and then specifying the file in the *Advanced Services* tab of the firewall rule permitting access to local web servers, you will block a version of the Nimda worm while allowing other "legal" traffic through.

g. *Alerting via Traffic Thresholds*. Traffic thresholds can be used to alert the administrator whenever excessive traffic patterns are occurring in a rule. For example, multiple SSH connections in a short period of time may indicate a hacking attempt. By setting the threshold of 10 connections attempts in a five minute period for a relatively low traffic SSH server, such as the GIAC customer SSH server, an administrator will be alerted to this and can react appropriately.

Using Source and Destination Interfaces

SEF also allows the administrator to create rules that specify the network interface in which the traffic will flow through. It is important to remember that when writing a rule, the administrator should specify this source and destination interface as often as possible. This limits where traffic originating from a hacked server can travel. For example, let say that there is a rule that allows an FTP server in Servicenet1 to access the FTP protocol to the entity Universe* because someone decided that outbound FTP doesn't pose a risk to the GIAC network. Let's also state that the rule allows the FTP access on the <Any> source and destination network interfaces. If a hacker gains control of that FTP server, he or she can now FTP into the GIAC network. This presents a big problem to the Security Department's future with the company. To prevent this nightmare from occurring, the SEF administrator should specify the Source Interface as Servicenet1 and the Destination Interface as External. This limits traffic to those networks that are accessible by the interfaces specified.

Rule Application

Unlike other firewalls, the Symantec Enterprise Firewall does not initially apply its rules to traffic in a top-to-bottom hierarchy. Instead it ranks the rules it will choose to apply based on how specific the rule has been written. SEF follows the hierarchy of Host > Subnet > Domain > Universe* when determining which rule is more specific. More specifically:

- A rule containing a host entity is more specific than a rule with a subnet entity.
- A rule with a subnet entity is more specific than a rule with a domain entity.
- A Domain entity is more specific than the universe* entity.

Groups are handled differently. A group is handled as if each entity in the group had its own rule. However, if there are two rules, one with a host and a subnet in a Group entity and another rule with only the host, both rules are considered equal. The tie-breaker occurs on the location of the rule in the rule base. A rule with a lower number is the rule that is followed in this case. Since you cannot change the order of rules without deleting other rules once they are written, it is a good idea to be aware of the method SEF uses when applying rules with Group entities when planning your ruleset.

2.3.7 – THE GIAC FIREWALL RULESET

Next, we will write out our access requirements through the firewall. Beginning with the most basic services and ending with the most complex methods of access.

Outbound Connections

SMTP traffic must be able to travel between the mailsweeper.giacent.com server to the Internet

- Source: Hst-mailsweeper.giacent.com
- Source Interface: Servicenet1
- Destination: Universe*
- Destination Interface: Externalnet
- Protocol: SMTP

Internet hosts need to be able to send e-mail to mail.giac.com

- Source: Universe*
- Source Interface: Externalnet
- Destination: Hst-mail.giacent.com
- Destination Interface: servicenet1
- Protocol: SMTP

The Internal MS Exchange Server must be able to send mail to Mailsweeper.giacent.com

- Source: Hst-exchange.giacent.com
- Source Interface: Internalnet
- Destination: Hst-mailsweeper.giacent.com
- Destination Interface: Servicenet1
- Protocol: SMTP

Mailsweeper.giacent.com needs to relay mail back to exchange.giacent.com

- Source: Hst-mailsweeper.giacent.com
- Source Interface: Servicenet1
- Destination: Hst-exchange.giacent.com
- Destination Interface: Externalnet
- Protocol: SMTP

Exchange.giacent.com needs to connects to the Ackmee.net NNTP server for Internet News

- Source: Hst-exchange.giacent.com
- Source Interface: Internalnet
- Destination: Hst-news.ackmee.net
- Destination Interface: Externalnet
- Protocol: SMTP

Allow outbound access to the Internet for the proxy server clients

- Source: Hst-proxy.giac.com
- Source Interface: Internalnet
- Destination: Universe*
- Destination Interface: Externalnet
- Protocol:
  - HTTP* (Application proxy includes support for https on ports 443 and 563 as well as FTP over an http session)
  - Ping*
- Advanced Services:
  - *ping.preserve.ttl* (to allow traceroute through the firewall

Allow special outbound FTP access for users possessing gateway password

- Source: Grp-Giacnet
- Source Interface: Internalnet
- Destination: Universe*
- Destination Interface: Externalnet
- Protocol: FTP* (GET only)
- Authentication: gwpassword
- Apply authentication to: ftpusers
- Out-of-Band Authentication: Yes

- Out-of-Band Authentication (OOBA) is utilized whenever an authentication process is required and is not support by the protocol being passed. With OOBA, the user connects to the firewall first then authenticates with the username and password supplied by the firewall administrator. Once authentication has occurred, the connection is allowed.

Customer Connections

Web-based customers need access to orders.giac.com

- Source: Universe*
- Source Interface: Externalnet
- Destination: Hst-orders.giacent.com
- Destination Interface: Servicenet1
- Protocol: HTTP* (including support for https on port 443)

Specific SSH Customers require access to ftporders.giac.com

- Source: Grp-SSHCustomers
- Source Interface: Externalnet
- Destination: Hst-ftporders.giacent.com
- Destination Interface: Servicenet1
- Protocol: ssh-customers

The Customer web server requires an ODBC connection to webdata.giacent.com in order to store customer orders

- Source: Hst-orders.giacent.com
- Source Interface: Servicenet1
- Destination: Hst-webdata.giacent.com
- Destination Interface: Servicenet0
- Protocol: customer-ssh (1984/tcp)

Supplier/Partner Connection

Web-based suppliers require SFTP access to sftp.giacent.com

- Source: Grp- SSHSuppliers-Partners
- Source Interface: Externalnet
- Destination: Hst-sftp.giacent.com
- Destination Interface: Servicenet2
- Protocol: ssh-sp (9278/tcp)

The group of RS/6000 servers on the 172.28.14.0 network needs to access the data stored on the sftp.giacent.com server

- Source: Grp-RS6000
- Source Interface: Internalnet

- Destination: Hst-sftp.giacent.com
- Destination Interface: Servicenet2
- Protocol: ssh-sp (9278/tcp)

Other Connections

All users need to access the public web servers – www.giac.com and webmail.giac.com

- Source: Universe*
- Source Interface: <ANY>
  - The <ANY> interface is specified here in order to allow access from internal network machines
- Destination: Grp-webservers
- Destination Interface: Servicenet1
- Protocol: HTTP* (includes support for https-443/tcp)

All servers in servicenet1 with logging enabled, need to send logs to syslog.giacent.com

- Source: Sub-Servicenet1
- Source Interface: Servicenet1
- Destination: Hst-syslog.giacent.com
- Destination Interface: Internalnet
- Protocol: syslog (514/udp)

All servers in servicenet2 with logging enabled, need to send logs to syslog.giacent.com

- Source: Sub-Servicenet2
- Source Interface: Servicenet2
- Destination: Hst-syslog.giacent.com
- Destination Interface: Internalnet
- Protocol: syslog (514/udp)

All servers in servicenet2 with tripwire enabled, need to send alerts via e-mail to mailsweeper.giacent.com

- Source: Sub-Servicenet2
- Source Interface: Servicenet2
- Destination: Hst-mailsweeper.giacent.com
- Destination Interface: Servicenet1
- Protocol: smtp*

Developers and administrators need access to the webdata.giacent.com server via Microsoft Terminal Services

- Source: Grp-webserveradmins
- Source Interface: Internalnet
- Destination: Hst-webdata.giacent.com

- Destination Interface: Servicenet0
- Protocol: ms-termservices_tcp (3389/tcp) & ms-termservices_udp(3389/udp)

Developers and administrators need access to the webserv.giacent.com server via Microsoft Terminal Services

- Source: Grp-webserveradmins
- Source Interface: Internalnet
- Destination: Hst-webserv.giacent.com
- Protocol: ms-termservices_tcp (3389/tcp) & ms-termservices_udp(3389/udp)

Security needs access to the siteprotector.giacent.com server via Microsoft Terminal Services and Siteprotector protocol

- Source: Sub-172.28.12.0
- Source Interface: Internalnet
- Destination: Hst-siteprotector.giacent.com
- Protocol: ms-termservices_tcp (3389/tcp), ms-termservices_udp(3389/udp), siteprotector (3998/tcp)

System administrators need access to the sftp.giacent.com server via SSH for management

- Source: Sub-172.28.10.0
- Source Interface: Internalnet2
- Destination: Hst-sftp.giacent.com
- Protocol: ssh-sp (9278/tcp)

System administrators need access to the ftporders.giacent.com server via SSH for management

- Source: Sub-172.28.10.0
- Source Interface: Internalnet2
- Destination: Hst-sftp.giacent.com
- Protocol: ssh-customers (1984/tcp)

Note: None of the rules containing Group entities contain conflict therefore rule location is not a factor in writing the ruleset.

2.3.8 – CREATING A RULE WITH THE SYMANTEC RAPTOR MANAGEMENT CONSOLE

Next, we will create a rule with the SRMC interface. Since all rules are generally created the same, I will create a rule with nearly all configuration items. We will be creating a rule that allows the custom protocol *Widgets_tcp* as well as *ping** to pass from the Subnet *Sub-172.28.1.0* on the internal network to the mailsweeper.giacent.com server on Servicenet1. The rule will allow only specified users to attach to the destination host during working day/hours. This

rule is not going to be used in our rule base as this is only an example. The valid rules in the GIACFW firewall will be created similarly.

Steps to creating a new firewall rule

1. Open SRMC and log into the console
2. Double-click *Access Controls* in the left pane of the SRMC to expand that group of objects
3. Right-click *Rules* on the left hand pane and select *New* > *Rule*
4. In the Description field, type **Allow users of the Widgets protocol access the mailsweeper.giacent.com server.**
5. In the *For Connections coming in via:* field, select Internalnet. This is the Source Interface discussed above.
6. In the *From Source* field, select Sub-172.28.1.0
7. In the *Destined For:* field, select Hst-mailsweeper.giacent.com
8. In the *Coming out via:* field, select Servicenet1

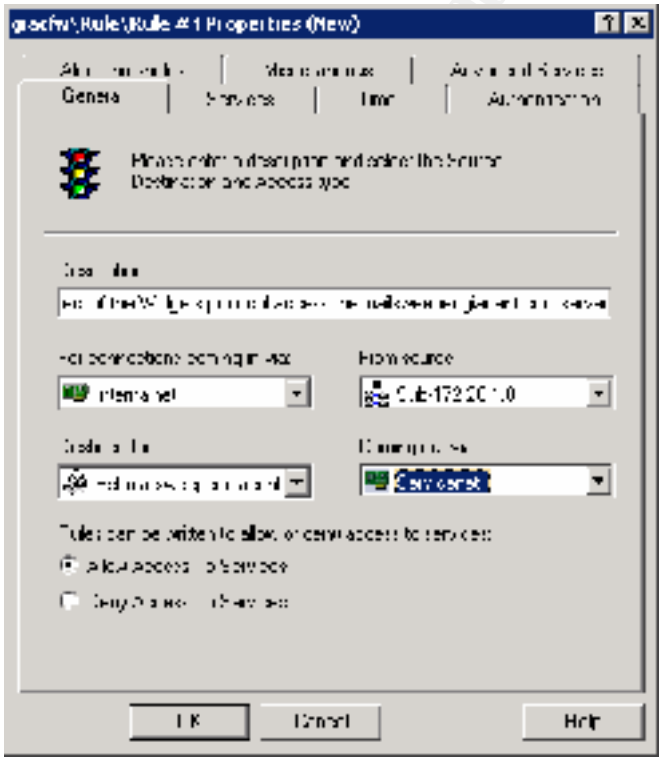


Figure 34 - New Rule

9. Click the *Services* tab. Highlight the *Widgets_tcp* protocol and click the **>>** button

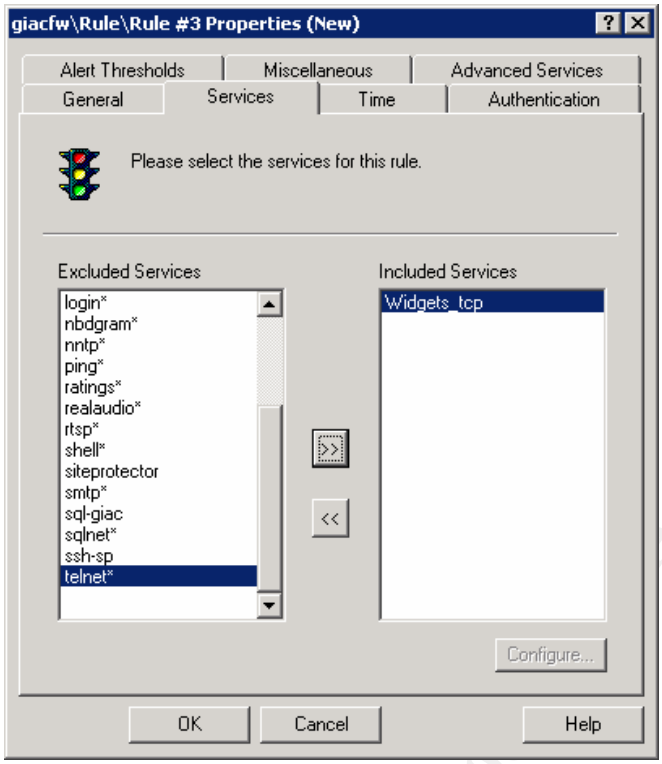


Figure 35 - Adding Services To A Rule

10. Before we click the *Time* tab, we need to set up our working hours/working days time period. Alt-tab to the SRMC.

11. Under *Base Components*, right click *Time* and select *New*

12. In the *Description* field, type **WorkingHours-Days**

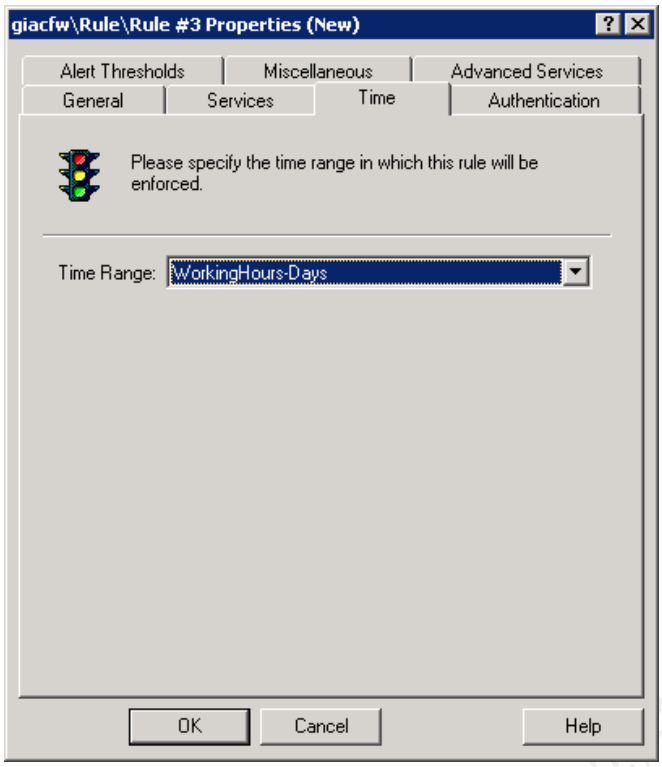


Figure 36 - Selecting Time Range

13. Check the *From box* in the *Time Range* section and type **8:00 AM**

14. Check the *Through box* in the *Time Range* section and type **5:00 PM**

15. Under *Day Range* Select ***Monday*** in the top box and **Friday** in the bottom box

16. Click OK

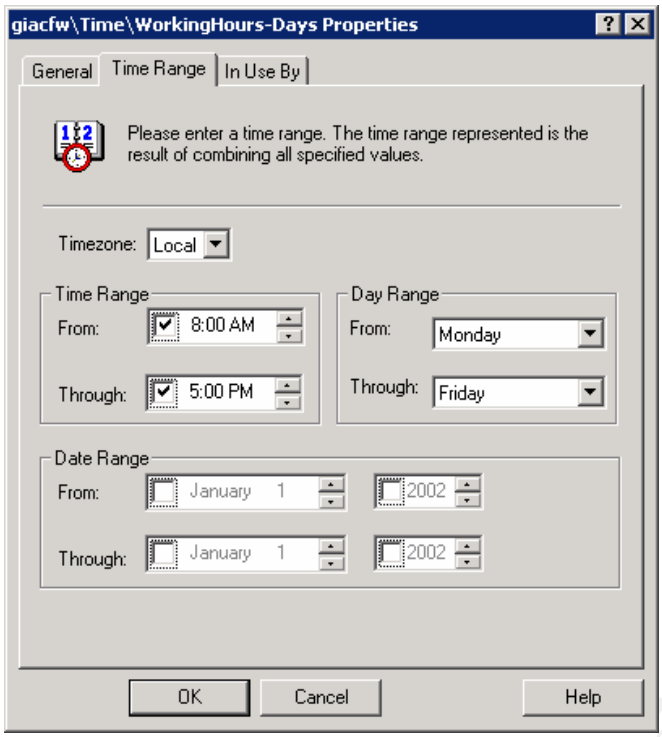


Figure 37 - New Time Range

17. Alt-tab back to your rule creation and click the Time tab

18. Select WorkingHours-Days

19. Next, we'll need to set up our users for this rule. Alt-tab back to the SRMC.

20. Under *Base Components*, right-click *User Groups* and select *New > User Group*

21. In the Name field, type **Ug-Wigets**. The *Ug* specifies that this is a user group.

22. In the description field, type **Users of the Widgets Protocol**

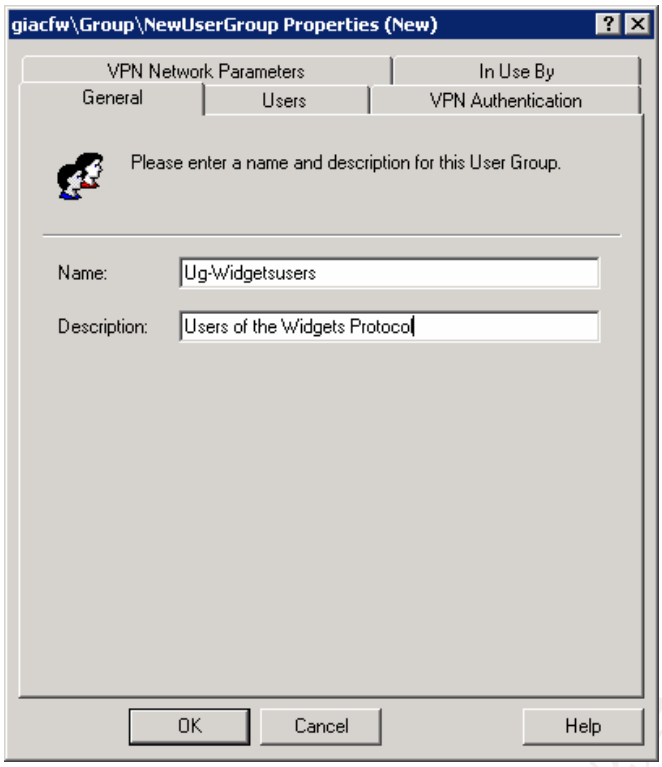


Figure 38 - New User Group

23. Click OK to exit

24. Alt-tab back to the SRMC

25. Under *Base Components*, right click *Users* and select *New* > *User*

26. In the Name field, type **Widget1**

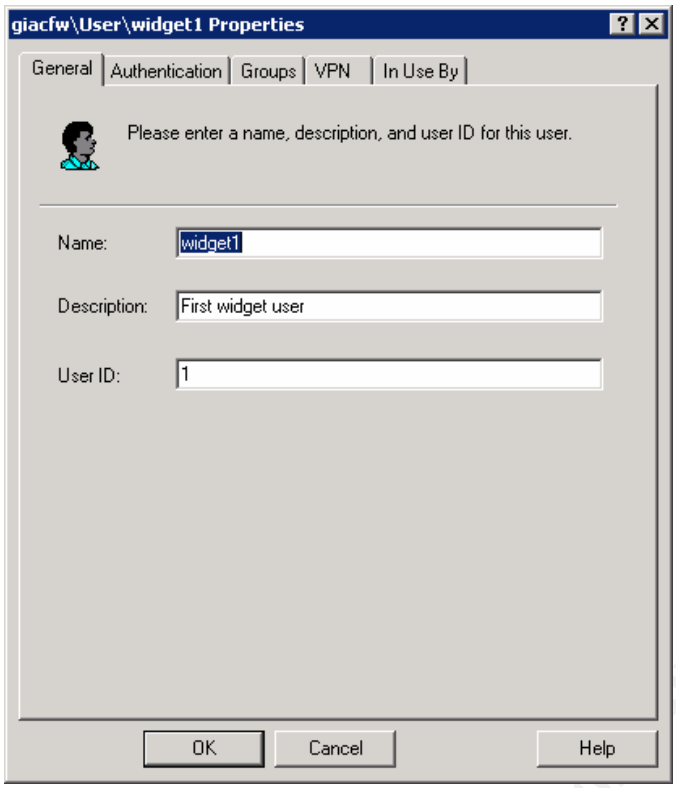


Figure 39 - New User

27. Click the *Authentication* tab
28. Type a password into the appropriate fields.
29. Click the Groups tab
30. Select *Ug-Widgets* and click the **>>** button
31. Click OK.
32. Alt-tab back to your new rule
33. Click the Authentication tab
34. Select **gwpassword** in the Authentication field
35. Click the *Use of out band authentication* box
36. In the *Apply rule to* select *Members of*
37. Click the *Edit* button and select *Ug-Widgets*

38. Since there are only supposed to be 5 users that access the widgets protocol lightly throughout the day, we want to be alerted if there are a large number of connections. In order to do this, we'll need to turn *Alert Threshold* on. We do this by first clicking the *Alert Threshold* tab.

39. Check the *Send notifications if any of these thresholds are reached* box

40. Increase the base numbers by a factor of three Type **10** in the *During 5 minutes,* 15 in the *During 15 minutes,* **30** in the *During 30 minutes* box and so on..

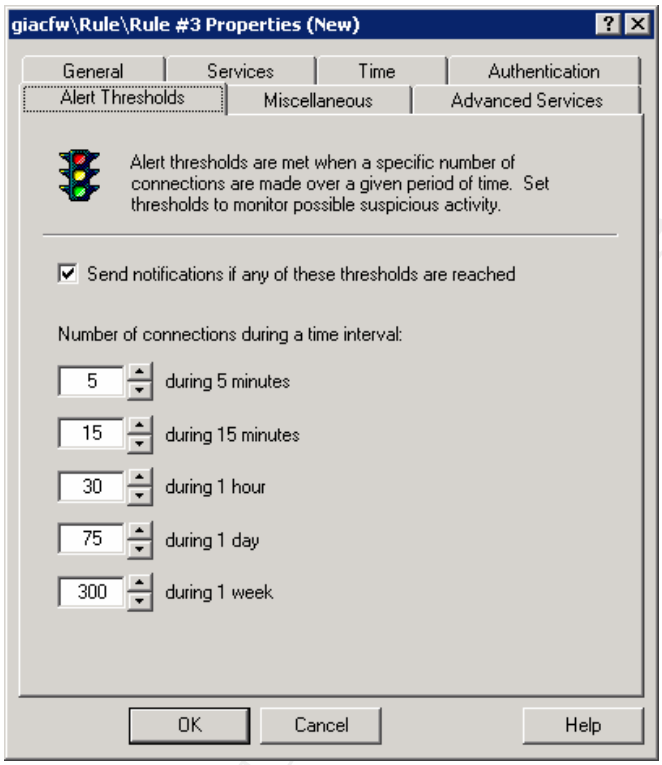


Figure 40 - Alert Thresholds

41. Click OK.

42. Click *Save and Reconfigure*

2.3.9 – ADDRESS REDIRECTION

In order for users to be able to access internal addresses, the Redirected Services section needs to be configured on the firewall. This is also known as service or port redirection. For example, the public web server, www.giac.com, is assigned the address of 10.100.2.80 by the GIAC network engineers. This

address is not accessible from the Internet so the GIAC engineers also need to assign an IP address that is publicly available from the Internet. This address is 5.10.100.46. SEF next needs to be configured to allow ports 80/tcp (http) and 443/tcp (https) to be passed to 10.100.2.80 if a machine on the Internet requests 5.10.100.46. Below lists the steps to set up Redirected Services for the www.giac.com web server.

The steps to redirecting services

1. Open SRMC and log in.
2. Right click Access Controls in the left pane and select **New > Redirected Service**
3. Under Service, select **http**
4. In the Requested Address field, type **5.10.100.46**
5. In the Address Mask field, type **255.255.255.255**
6. In the Redirected Address field, type **10.100.1.80**
7. In the Redirected Port field, type **80**
8. Click **OK**
9. Click **Save and Reconfigure**

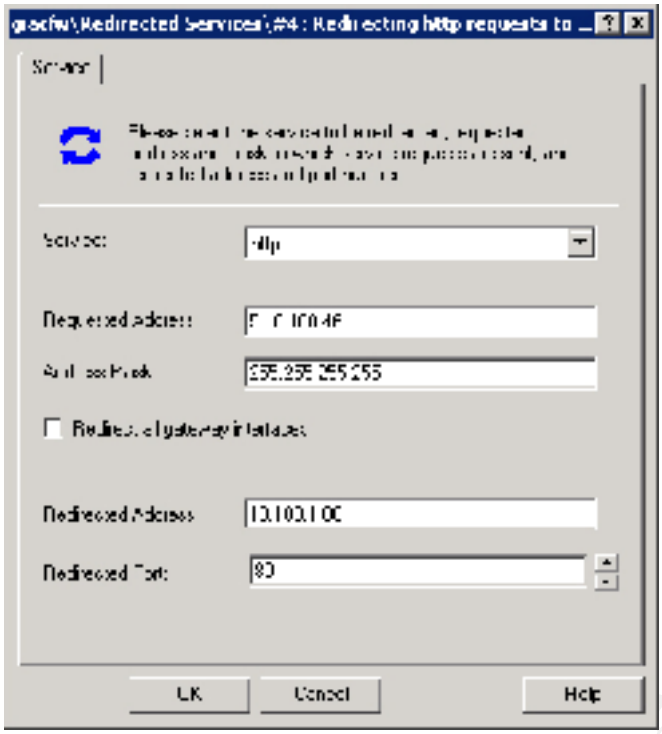


Figure 41 - Redirected Services

2.3.10 – OTHER TIPS AND TRICKS FOR THE SYMANTEC ENTERPRISE FIREWALL

Config.cf File

The config.cf file allows you to modify options in SEF that are not located in the SRMC. These options generally should not be set unless directed by Symantec Support. GIAC has configured options that have been found to be useful. The config.cf file can be opened by right clicking anywhere in the SRMC and selecting *Editor*. With the Editor program open, click *File* | *Open* and select the config.cf file.

One of the options set by GIAC is the location of the log files. By default, SEF saves the log files in the same directory location as the SEF installation. GIAC would rather save the log files on a separate partition (E:) that has been set aside mainly for the storage of the log files. In order to save these files on this partition, the config.cf variable `logdir` has been changed from `logdir=C:\Raptor\Firewall\Sg` to `E:\SEFLOGS`. The Seflogs directory needs to be created before the logs will be saved to that directory.

Login Banner

When someone opens a telnet session to the SEF, a banner appears identifying the firewall as the "Raptor Firewall Secure Gateway". Since limiting the amount of information a hacker has to use against you is important, a good idea is to either turn off the banner or change the banner to a legal notice informing any unauthorized connections to the firewall are not welcome. The legal notice is preferred over a blank banner since displaying a banner that discourages unauthorized access may help when prosecuting a hacker.

Steps performed to configure SEF to display a warning banner.

1. Open SRMC
2. Right-click anywhere on the screen and select All Tasks > Editor
3. Click File | Open
4. Type *C:\Raptor\Firewall\Sg\gateway_motd* and click OK
5. To modify the FTP banner, open *C:\Raptor\Firewall\Sg\ftp_motd*
6. Type in your new banner or delete the present banner if you do not wish to have a login banner.
7. Click File | Save
8. Exit the Editor
9. Click Save and Reconfigure in the SRMC

The GIAC SEF banners display the following:

```
This is a GIAC Enterprises Inc. system for Company official business
ONLY. System use is an express consent to being monitored and any
evidence of unauthorized activities will be used for criminal
prosecution.  All unauthorized users must disconnect NOW to avoid
prosecution.
```

2.3.11 – VULTURE.RUNTIME FILE

The Vulture service on SEF will shutdown all unauthorized services on the firewall. Vulture is used to prevent someone from running services that may compromise the security on the Symantec Enterprise Firewall. Administrators may need to run tools such as the Scheduler service in order to automate tasks on the firewall, such as copying the log files to another drive or server. In order to be able to perform this task, the SEF configuration file named *vulture.runtime* needs to be edited. What is typed into this file is the service name found in the Windows registry. For example, if you would want to run the Task Scheduler

service, you would just add the word Schedule to the vulture.runtime.

Steps to modifying the vulture.runtime file

1) Determine the name of the service you wish to allow to run on the firewall.

2) Open SRMC

3) Right-click anywhere on the screen and select All Tasks > Editor

4) Click File | Open

5) Type C:\Raptor\Firewall\Sg\vulture.runtime and click OK

6) Type in the name of the service

7) Click File | Save

8) Exit the Editor

9) Click Save and Reconfigure in the SRMC

2.4 – RAS FIREWALL

The firewall separating the RAS network (172.28.40.0) from the rest of the GIAC network is in place in order to prevent successful war-dialers from attacking the network. The configuration isn't nearly as complex as the Internet firewall as it only has to filter certain protocols from the RAS users. This firewall is also running Symantec Enterprise Firewall on Windows 2000.

The RAS firewall only permits CIFS (445/tcp) and Netbios (137-139/tcp) connections for all general users. Company officers are permitted to also browse the World Wide Web and the Firewall Administrator is permitted web traffic and the ability to connect to the border firewall for management.

Appendix B lists the entities for the RAS firewall.

2.4.1 – RAS FIREWALL RULES

Rules

Allow Windows networking access to RAS users

- Source: Sub-RasNet

- Source Interface: RasNet
- Destination: Sub-172.28.2.0
- Destination Interface: Internalnet
- Protocol: Cifs* Nbdgram*

Allow Executives Internet Browsing Access

- Source: Grp-Execs
- Source Interface: Rasnet
- Destination: Universe*
- Destination Interface: Internalnet
- Protocol: HTTP* (Includes https and ftp over http access)

Allow Firewall Admin to connect to the external firewall

- Source: Hst-FWA
- Source Interface: Rasnet
- Destination: Hst-ExternalFirewall
- Destination Interface: Internalnet
- Protocol: Readhawk (418/tcp – used by SRMC to connect to a firewall for administration)

ASSIGNMENT 3 – VERIFY THE FIREWALL POLICY (25 POINTS)

You have been asked to conduct a technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced as described in Assignments 1 and 2. To conduct the audit, you will need to:

- Plan the audit.
  - Describe the technical approach you will use to assess the firewall.
  - Be certain to include considerations such as what shift or day you would do the assessment.
  - Estimate costs and level of effort.
- Identify risks and considerations and how they are addressed.
- Using the approach you described conduct the audit.
- Demonstrate how you validated that the primary firewall is actually implementing GIAC Enterprise's security policy.
- Be certain to include the tools and commands used. Include screen shots in your report if possible.
- Evaluate the audit. Based on your assessment (and referring to data from your assessment):
- Provide an analysis of the audit results.
- Make recommendations for improvements or alternate architectures.
- Supportive diagrams are strongly recommended for this part of the assignment.

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

3.1 – PLANNING THE AUDIT

Note: Since I could not build enough machines to simulate the GIAC environment, much of this audit is based on several past audits that I have been a part of. Where possible, I used actual results from machines that closely resemble those in the GIAC environment. However, some of the auditing results were made up for the purposes of generating enough information to use in this paper.

In order to verify the GIAC security policy, an audit was ordered by the management team. The requirements set forth by company management for this audit were:

- A minimal impact on business processes. Minimal impact means that individual employees can be disrupted but business flow shall not be interfered with. Attacking the firewall with a DoS attack (or any other type of mass disruption) during business hours is grounds for the removal of any auditor(s) from the GIAC site.

- GIAC Security department initially should not be aware of the audit. This is to verify that the security department is following company procedures for handling intrusion incidents as well as auditing the IDS and logging systems.

- All aspects of the network border should be evaluated for weaknesses. This includes evaluating helpdesk personnel as well as end-users in their security consciousness. The goal is to audit the GIAC personnel as well as the machines in place for network security. If GIAC is not confident in its people, no amount of money spent on the latest security products is worth the effort if the personnel managing these systems are not properly trained.

- Any vulnerability found needs to be addressed by the security department immediately. The auditors shall notify network administrators upon discovering any gaping hole in the network perimeter. Notification via the final report is not acceptable as this leaves an open hole. A machine so easily compromised that a minimal effort is required by a hacker in order to exploit the vulnerability used defines a gaping hole.

3.2 – AUDITING THE NETWORK

3.2.1 – DISCOVERY

The first step to the audit of the GIAC network is discovery. The auditing company, Fredo Leigh and Associates (FLA) was initially not given any information about GIAC Enterprises. In order to gauge the availability of information about GIAC, the auditors needed to act as though they are like any other attacker on the Internet and gather any information they could on their own.

Armed with absolutely no information other than the words “audit GIAC Enterprises network”, the auditors ran a Google (www.google.com) search for GIAC Enterprises. This led to the knowledge that the GIAC Enterprises located in Yeehaw Junction, Florida registered the domain name of giac.com. Beginning on an early Saturday morning, the discovery process started with utilizing a program called *Sam Spade* is used to query the Whois databases at arin.net and internic.net. By initially querying internic.net, for www.giac.com, FLA discovered that the IP address for this server is 5.10.100.46. More importantly, FLA discovered that the GIAC DNS servers were ns1.ackmee.net (5.2.146.5) and ns2.ackmee.net (5.2.124.6). Next, FLA attempted to perform a DNS zone transfer for giac.com by using the *Sam Spade* program. The zone transfer would have allowed FLA to find out all machines with a DNS name assigned to it. This was unsuccessful so other steps needed to be taken in order to determine the addressing scheme of the giac.com network. Allowing zone transfers seems to be a big problem with many ISPs. While not a huge security issue, there is no reason to give up the host information so easily to those machines that don’t have a valid reason for viewing an entire DNS table for a domain. The Ackmee.net ISP scored points for not allowing zone transfers to any just host on the Internet.

The FLA auditors knew that there was a www.giac.com, a good start to finding other hosts on the GIAC domain was to determine the router address for giac.com. Running a traceroute to www.giac.com terminated at the address of 5.10.100.34 while passing through 5.10.100.33 in the process. Taking this information, FLA then ran a traceroute to 5.10.100.29, which did not pass through 5.10.100.33. Next, FLA ran a traceroute to hosts from 5.10.100.35 to 5.10.100.49 (the next potential subnet) to determine their router. On those addresses that responded, all but the .49 host passed through the 5.10.100.33 address. This told FLA that the router was most likely sitting on the address of 5.10.100.33. Since all of the hosts that did respond in the correct subnet also passed through 5.10.100.34, it was determined that this address most likely represented either a firewall, or another router. The firewall was chosen as the most likely type of host.

Now that FLA had a network to work against, a ping sweeper was deployed to attempt to discover all active hosts. A program called Super Scanner is used to scan for active hosts. Since FLA didn’t want to raise any alerts, the ping sweep was performed using the slow scan option on Super Scanner.

Running the ping sweep enabled FLA to determine that there were 8 active machines on the giac.com network, including the router. Nmap was next deployed in order to try to discover the services running on the 8 machines discovered. Unfortunately, running Nmap against the 7 machines was an exercise in futility since the Nmap port scans resulted in the exact same output.

This output is because the firewall is an application proxy and is proxying the services listed.

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Interesting ports on  (5.10.100.44):
(The 1501 ports scanned but not shown below are in state: closed)
Port       State       Service
20/tcp     open        ftp-data
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
70/tcp     open        gopher
80/tcp     open        http
101/tcp    open        hostname
110/tcp    open        pop-3
119/tcp    open        nntp
139/tcp    open        netbios-ssn
420/tcp    filtered    smpte
443/tcp    open        https
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
554/tcp    open        rtsp
700/tcp    open        unknown
1521/tcp   open        ncube-lm
3389/tcp   open        msrdp
4444/tcp   open        krb524
5631/tcp   open        pcanywheredata
8080/tcp   open        http-proxy

TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
No OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
TSeq(Class=TR)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(Resp=N)


Nmap run completed -- 1 IP address (1 host up) scanned in 37 seconds
```

Next, it was time to test the logging and the alerting function of the GIAC network. FLA launched a series of attacks that are likely to alert an

administrator. Attacks as simple as telnet connections to short term DOS attacks were launched. The idea was to not break into the network but to verify that the IDS system was working properly. It was revealed later that the GIAC security department was notified on the simple attacks but when a DOS attack was launched, the security engineer was not notified. This was because sending SMTP mail to the employee's pager is the preferred method for alerting. A recommendation to GIAC was to utilize the modem paging alerts within SEF and the IDS system.

The next step to the audit process required the assistance and knowledge of the GIAC Security Department. In order to test the security policy, FLA attempted to connect to the various services listed in the Nmap scan. The following were steps taken to verify the security policy for each of the Internet servers:

www.giac.com

FLA wanted to verify that only 80/tcp and 443/tcp were enabled for this server. They attempted to telnet to the other ports listed in the Nmap scan, only the http and https were active. In every attempt to connect, the message the following was given as the output:

```
554 5.7.1 giacfw.giac.com Connection not authorized
```

orders.giac.com

FLA again attempted the telnet sessions to the same ports listed on the nmap scan. The results were the same as www.giac.com. Next, FLA wanted to verify that the web server was sending out only secure pages were necessary. FLA logged into the web server and got to the order screen. FLA then changed the url from `https://orders.giac.com/orderbot/order.cgi` to `http://orders.giac.com/orderbot/order.cgi` and then hit the Enter key. The output was the original login screen. Since the "403.4 – https required" page is set to immediately refresh to the original login screen, the non-secure page is not displayed.

sftp.giac.com

The usual telnet to the ports that Nmap also displayed the "Connection Not Authorized" messages (from this point forward, all servers audited will be assumed to display the exact same messages for the Nmap open ports). FLA then attempted to connect to the SSH server by using port 9278/tcp. This also displayed the "Connection Not Authorized" screen. Finally, the FLA machine was then added to the Grp-SSHPartners-Suppliers group and the connection was established. No other ports were allowed.

Ftporders.giac.com

FLA performed the same steps as sftp.giac.com except using port 1984. The same result as that which occurred on sftp.giac.com was given. No other ports were open.

webmail.giac.com

FLA connected to the webmail.giac.com web site via regular http. The opening page immediately redirected to the https version of the original login page. This held true no matter where an http page was attempted. No other ports were open.

www.giac.com

This web server allowed http and https connections from anywhere. The http versions of the pages did not redirect to any other web page. No other port connections were allowed.

mail.giac.com

A connection to the SMTP mail server was made through port 25. An attempt to relay mail through this server had failed. In addition, attempts to perform an EHLO command did not work nor did any other extended smtp (ESMTP) command, (see rfc 1869 - http://www.faqs.org/rfcs/rfc1869.html). No other port connections were allowed.

VPN Connections

FLA logged via a VPN connection using the same tunnels as the employee, suppliers, and customers. Attempts were made to telnet out to other servers on the network. This did not work on any of the servers. The message received was the usual "connection not authorized".

RAS Server

FLA dialed into the RAS server and logged in. An attempted was made to try to get to other networks. This attempt failed with the "connection not authorized" message. The FLA home directory was available as well as other shares. Attempts to log into other home directories failed.

Next, a network scanner, ISS' Internet Scanner, was to be deployed to search for vulnerabilities on the Internet hosts.

Note: Since I could not build every machine in the GIAC environment, most of the vulnerabilities cited in this paper are a compilation of some of the more common vulnerabilities found while conducting audits. They are representative of what has been seen in the environments with hosts matching the operating systems used in the GIAC Enterprises Network.

SANS Top Twenty Checklist

Since the discovery process did not turn up enough information about the host machines, the GIAC Networking Department needed to supply FLA with the appropriate IP address and host information so that proper scans of the machines could be accomplished. In addition to utilizing the network scanner, FLA also audited hosts for the SANS Top Twenty Vulnerabilities on a machine prior to running a scan with Internet Scanner.

From the results of the SANS checklist, the vulnerabilities found on GIAC systems were:

Windows

1. Incomplete backups – a number of systems had multiple days in which a backup was listed as incomplete.

2. Unprotected File System Shares (W4) – Many of the servers on the GIAC network contains shares with Full Control rights for the Everyone group. It is recommended that network shares be modified to allow specific users or groups access.

3. Null Session Shares (W5) – A null session share allows anonymous users to connect to certain shares. Attackers can use null sessions to gain access to the server. This vulnerability is only present on the Windows NT 4.0 machines. The recommendation is that GIAC remove the Null Session shares by following these instructions:

```
Use Registry Editor to view the RestrictAnonymous registry
value, add the following value to this key, or modify it if
the value is already in existence:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
Value: RestrictAnonymous
Value Type: REG_DWORD
Value Data: 0x2 (Hex)
```

Unix

1. R Commands Available (U4) – Most of the AIX machines contained the rlogin, rsh, and rcp commands. It is recommended that SSH be used on these machines instead of the r commands and that the r commands be removed from those servers.

GIAC Response:
Windows

1. *Incomplete Backups* – Some backups display an *Incomplete* result because one or more files were open at the time of the backup. For the other machines showing a failed or incomplete backup result, a process will be developed to verify the backup results on a daily basis. Any backup that fails or is incomplete will immediately be run again so that there isn't more than one day without a complete backup.

2. *Unprotected Shares* – The file system shares will be modified to remove all Everyone group permissions on the share.

3. *Null Session Shares* – The recommended registry change will be made on the NT 4.0 machines.

Unix

1. *R Commands* – The r commands will be removed from the AIX servers and SSH will be enabled on the server.

ISS Internet Scanner Tests

FLA next audited various hosts on the GIAC network for vulnerabilities by utilizing the Internet Scanner tool from Internet Security Systems (ISS). This tool checks for a large number of system and network vulnerabilities. FLA audited the Internet servers as well as the servers that play a role in the security on the network.

The following are the results from ISS Internet Scanner for each computer scanned:

Orders.giac.com

Vulnerability:
lisSamplesCodebrws
Description:
Codebrws.asp sample file distributed with IIS and SiteServer could allow remote file viewing (lisSamplesCodebrws)
Risk Level:
Medium
Platforms:
Microsoft IIS: 4.0, Windows NT 4.0, Microsoft Site Server: All versions
Remedy:
Remove the codebrws.asp file from your servers. As a rule, sampe code and example applications should not be installed on productions servers
-Or-

Apply the patch for this vulnerability located at the Microsoft FTP site. See References.

Additional Information:

Internet Scanner checks /iissamples/exair/howitworks/codebrws.asp for vulnerable versions of the codebrws.asp sample file, and any additional sample files that may be vulnerable.

References:

Microsoft Security Bulletin MS99-013 - Solution Available for File Viewers Vulnerability http://www.microsoft.com/technet/security/bulletin/ms99-013.asp
Microsoft Knowledge Base Article Q231368 - Solution Available for File Viewers Vulnerability http://support.microsoft.com/support/kb/articles/q231/3/68.asp
Microsoft Knowledge Base Article Q232449 - Sample ASP Code May be Used to View Unsecured Server Files
http://support.microsoft.com/support/kb/articles/q232/4/49.asp
Microsoft FTP site - Viewcode-fix patch ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/viewcode-fix/
CVE CAN-1999-0739 - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0739

GIAC Response:

Applied patch noted in MS99-013 as well as removed the offending .asp page.

Vulnerability:

Microsoft IIS ISAPI HTR chunked encoding heap buffer overflow (

Risk Level:

High

Platforms:

Windows 2000, Microsoft IIS: 5.0, Microsoft IIS: 4.0, Windows NT

Description:

Microsoft Internet Information Server (IIS) versions 4.0 and 5.0 are vulnerable to a buffer overflow in the function that enables the chunked encoding data transfer mechanism, which is part of the ISAPI (Internet Services Application Programming Interface) extension that implements HTR functionality. Chunked encoding is a process by which a client generates a variable sized "chunk" of data and notifies the Web server of the data's size before transferring it, so that the Web server can allocate a buffer of the correct size. By sending a specially-crafted "chunk" of data that causes the incorrect buffer size to be allocated, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the IIS service to fail.

Remedy:

Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin MS02-028. See References.

References:

Microsoft Security Bulletin MS02-028 - Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise (Q321599)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-028.asp

BugTraq Mailing List, Jun 13 2002 7:32PM - VNA - .HTR HEAP OVERFLOW http://online.securityfocus.com/archive/1/276767
CERT Vulnerability Note VU#313819 - Microsoft Internet Information Server (IIS) contains remote buffer overflow in chunked encoding data transfer mechanism for HTR http://www.kb.cert.org/vuls/id/313819

GIAC's Response:

Applied patch described in Microsoft Security Bulletin MS02-28

Vulnerability:

Microsoft Internet Explorer Gopher client malformed reply buffer overflow

Risk Level:

High

Platforms:

Windows, Microsoft Proxy Server: 2.0, Microsoft ISA Server: 2000, Microsoft Internet Explorer: 5.5, Microsoft Internet Explorer: 6.0, Microsoft Internet Explorer: 5.01

Description:

The Gopher protocol, developed by the University of Minnesota in 1991, is a distributed document delivery system that displays hierarchically organized directories and files. Microsoft Internet Explorer versions 5.01 through 6.0, Microosft Proxy Server 2.0, and Microsoft Internet Security and Acceleration (ISA) Server 2000 are vulnerable to a buffer overflow in the built-in Gopher client. A remote attacker could exploit this vulnerability by creating a Web page or an HTML email that redirects a victim to a malicious Gopher server, which could be used to overflow a buffer in the code in Internet Explorer that handles Gopher replies. An attacker could use this vulnerability to execute arbitrary code and gain complete control of the victim's computer.

Remedy:

A patch is available from Microsoft Support. See http://www.microsoft.com/technet/security/bulletin/MS02-027.asp?frame=true

References:

BugTraq Mailing List, Jun 4 2002 1:07PM - Buffer overflow in MSIE gopher code http://online.securityfocus.com/archive/1/275344
Microsoft Security Bulletin MS02-027 - Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice (Q323889) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-027.asp
CERT Vulnerability Note VU#440275 - Microsoft Internet Explorer contains buffer overflow in handling of gopher replies http://www.kb.cert.org/vuls/id/440275

GIAC Response:

Applied patch as defined in the references section. Gopher (70/tcp) is not allowed through the firewall.

Vulnerability:

HTTP server with unresolvable local links

Risk Level:

Low
Platforms:
HTTP
Description:
An unresolved link was detected. Web browsers should receive an error when accessing this link. This issue does not indicate a serious vulnerability, and is only noted as a courtesy.
Remedy:
Notify your Webmaster, since this dead link represents a vulnerability in the Web page.
References:
ISS X-Force HTTP server with unresolvable local links
http://xforce.iss.net/static/144.php
GIAC Response:
Developers will scan web server for dead links and remove them.

www.giac.com

Vulnerability:
TCP sequence prediction
Risk Level:
Medium
Platforms:
Any: All versions
Description:
The TCP sequence was found to be predictable. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from a trusted computer. These forged packets can compromise services, such as rsh and rlogin, because their authentication is based on IP addresses. Attackers can also perform session hijacking to gain access to unauthorized information. Some Microsoft patches for this did not completely resolve the sequence predictability.

The following information explains the varying levels of TCP sequence predictability in Windows operating systems:

- Windows NT 4.0 pre-SP3 systems are highly predictable.
- Windows NT 4.0 SP4 through SP6 uses a different algorithm to reduce sequence predictability, but the systems remain predictable.
- Microsoft released patch MS99-046, which uses the same algorithm as Windows 2000, to fully fix the problem.
- Windows 2000 is not TCP predictable.

Remedy:
Ask your vendor for patches to correct TCP sequence prediction. Note that some patches make sequence prediction more difficult, but still possible. As a result, the host may continue to report this vulnerability.

For Windows NT 4.0:
Apply the latest Windows NT 4.0 Service Pack (SP6a or later), available from the Windows NT Service Packs Web page. Note that Windows NT system may continue to report this vulnerability. After you successfully apply the Service Pack, apply the patch listed in Microsoft Security Bulletin MS99-046. See References.
For other distributions:
Contact your vendor for upgrades or patch information.
False Positives:
Some patches make sequence prediction more difficult, but still possible. As a result, the host may continue to report this vulnerability, even after a patch has been applied.
References:
CERT Advisory CA-1995-01 - IP Spoofing Attacks and Hijacked Terminal Connections http://www.cert.org/advisories/CA-1995-01.html
CERT Vulnerability Note VU#498440 - Multiple TCP/IP implementations may use statistically predictable initial sequence numbers
http://www.kb.cert.org/vuls/id/498440
CERT Advisory CA-2001-09 - Statistical Weaknesses in TCP/IP Initial Sequence Numbers http://www.cert.org/advisories/CA-2001-09.html
CVE-2001-0751 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0751
GIAC Response:
This flaw may not be present in this server. According to Cert Advisory CA-2001-09, the Linux kernel has used a variant of RFC1948 by default since 1996. The abstract for RFC 1948 (http://www.faqs.org/rfcs/rfc1948.html) reads as follows:

IP spoofing attacks based on sequence number spoofing has become a serious threat on the Internet (CERT Advisory CA-95:01). While ubiquitous cryptographic authentication is the right answer, we propose a simple modification to TCP implementations that should be a very substantial block to the current wave of attacks.

It is GIACs opinion that this vulnerability must be a either false positive or the firewall is producing this result due to its proxying of services.

Vulnerability:
TFTP
Risk Level:
Medium
Platforms:
Red Hat Linux: 6.0, AIX: 4.0, HP-UX: 11, Solaris: 8, Red Hat Linux: 7.x, Compaq: Tru64 UNIX, Solaris: 2.5.1, TFTP, Solaris: 7, HP-UX: 10.20, Solaris: 2.6
Description:
TFTP was detected. TFTP has no authentication process for letting file transfers take place. An attacker can gain access to the password file.
Remedy:
Unix: Comment out the tftp entry in /etc/inet.conf to disable TFTP entirely, or

change the entry to restrict TFTP from accessing all world-readable files. Then restart inetd.

References:

CERT Advisory CA-1989-05 - DEC/Ultrix 3.0 Systems
http://www.cert.org/advisories/CA-1989-05.html
CERT Advisory CA-1991-18 - Active Internet tftp Attacks
http://www.cert.org/advisories/CA-1991-18.html
CIAC Information Bulletin B-44 - Automated tftp Probe Attacks on UNIX Systems Connected to the Internet http://www.ciac.org/ciac/bulletins/b-44.shtml
CIAC Information Bulletin CIAC-05 - Security Holes in UNIX Systems
http://www.ciac.org/ciac/bulletins/ciac-05.shtml
CIAC Information Bulletin A-21 - Additional Information on Current UNIX Internet Attacks http://www.ciac.org/ciac/bulletins/a-21.shtml

GIAC Response:

Removed TFTP support from the Linux services.

Mailsweeper.giac.com

Vulnerability:

SMTP daemons allow addresses to be verified using RCPT (SMTPrcpt)

Risk Level:

Low

Platforms:

Sendmail, SMTP servers

Description:

A side affect of many implementations of the RCPT command within SMTP servers is the ability to use this command to verify those addresses that are valid. Disabling the VRFY and EXPN commands is often thought to be sufficient in preventing information gathering attacks. This method is often used in email harvesting programs run by direct email marketers.

Remedy:

This issue does not directly indicate any type of vulnerability. No effective solutions have been developed to prevent this method from being exploited. Mail administrators should pay close attention to their log files and report any obvious abuses to the appropriate person(s).

References:

ISS X-Force - SMTP daemons allow addresses to be verified using RCPT
http://xforce.iss.net/static/1928.php
CVE CAN-1999-0531 - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0531

GIAC Response:

GIAC is aware of the issue and will diligently monitor and respond to unusual activity with regards to the e-mail system.

Ftporders.giac.com

TCP sequence prediction (tcppred) – Please see the entry for www.giac.com. The response from GIAC is the same.

Sftp.giac.com

TCP sequence prediction (tcppred) – Please see the entry for www.giac.com. The response from GIAC is the same.

Ras1.giacent.com

Vulnerability:
SMB share found (NetBIOS share)
Risk Level:
Low
Platforms:
Windows: 95, OS/2, Windows for Workgroups: 3.11, Samba, Windows NT, Windows 2000
Description:
An SMB share has been detected. If the share already has the proper access controls, this is a low risk vulnerability.
Remedy:
All platforms should either disable sharing or review access controls.
In Windows 2000, remove the share from a local or remote computer:

- Start the Computer Management Console (compmgmt.msc) from a command prompt. The focus is local computer by default.
- To remove a share from a local computer, skip to the next step.
  To remove a share from a remote computer, right-click the Computer Management node and select Connect to another computer, then enter the name of the remote computer where the share will be removed.
- Double-click the Shared Folders node.
- Single-click the Shares folder.
- Right-click the shared folder of interest, and select stop sharing.
- Confirm the operation.
- You may also remove a share from the command line by typing the following at a command prompt:

```
net share sharename /delete
```

References:
ISS X-Force - SMB share found
http://xforce.iss.net/static/12.php
GIAC Response:
GIAC will review the share permissions to determine if certain shares should not be accessible to general users. All “everyone accessible” shares will be removed and the proper permissions will be set on these shares.

Vulnerability:

The default Administrator account exists
Risk Level:
Low
Platforms:
Windows NT, Windows 2000
Description:
An account named Administrator was found. This default account cannot be locked out by too many incorrect logon attempts, and can be vulnerable to a brute force attack if a poor password is chosen.
Remedy:
To secure the Administrator account:
Rename the Administrator account.
Create a new Administrator account with only Guest access.
Remove network access for Administrator.
Monitor against logon attempts.
False Positives: This check looks for the words "Administrator" and "Guest" in all of the following languages: Czech, Danish, Dutch, English, Finnish, French, German, Hungarian, Italian, Norwegian, Polish, Brazilian Portuguese, European Portuguese, Slovak, Slovenian, Spanish, Swedish, and Turkish. If the Administrator or Guest accounts appear in another language, this check will report a false positive.
References:
ISS X-Force - The default Administrator account exists
http://xforce.iss.net/static/28.php
GIAC Response:
GIAC will rename the administrator account and create a bogus account to use as a trap. Account auditing is already enabled on this server.

Vulnerability:
No user profile required (No User Profile)
Risk Level:
Low
Platforms:
Windows NT, Windows 2000
Description:
No user profile is required for the user. The System Policy Editor creates user profiles that can be used to restrict user access. Profiles can be effective tools in improving your user security.
Remedy:
Assign a profile to the user account, by following the steps below appropriate for your platform.
For a Windows 2000 domain:

- Start Active Directory Users and Computers Management Console (dsa.msc) from a command prompt.
- Double-click on Users folder.
- Double-click on user object of interest.

- Click on the Profile tab.
- In Profile path enter the location of the profile you want to assign.
- Click on OK to save the settings.

For a stand-alone Windows 2000 computer:

- Start Local Users and Groups Management Console (lusrmgr.msc) from a command prompt.
- Double-click on Users folder.
- Double-click on user object of interest.
- Click on the Profile tab.
- In Profile path enter the location of the profile you want to assign.
- Click on OK to save the settings.
- To create a profile in the System Policy Editor, follow the steps below:
- Open the System Policy Editor.
- From the File menu, select New Policy to display the Default User and Default User icons.
- Set the options of the new policy:
- Double-click the Default Computer icon and select the computer policy options.
- Double-click the Default User icon and select the user policy options.
- (Optional) Add additional users, computers, or groups to the new policy.
- Click OK.
- Save the file as NTCONFIG.POL in the netlogon share of the PDC/BDC.

References:
ISS X-Force - No user profile required http://xforce.iss.net/static/1313.php
GIAC Response:
While user profiles can be useful, GIAC does not see the need to apply them to the RAS users.

Syslog.giacent.com

Vulnerability:
Syslog flood (syslogflood)
Risk Level:
Medium
Platforms:
Unix
Description:
The syslog daemon is vulnerable to a denial of service attack known as the syslog flood. An attacker can send a large number of messages to the system log daemon to exhaust disk space. This attack can lead to the syslog service terminating, or possibly a system deadlock, putting the host in an operable state.
Remedy:
If you are not using remote logging, use the -r option (or -l in BSDI) to turn remote logging off in your syslog daemon. You must then recompile the daemon.

Contact your vendor or refer to your vendor's documentation for more information.
References:
ISS X-Force - Syslog flood http://xforce.iss.net/static/136.php
CVE-1999-0566 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0566
GIAC Response:
GIAC is fully aware of this problem. GIAC will monitor disk space on the syslog server diligently. Every week, GIAC archives the log files to tape and CD-Rom. Once this is completed, only the previous week's log files are kept on the server. All earlier log files are purged from the server.

Cisco Border Router

Vulnerability:
Cisco IOS TCP port connection denial of service
Risk Level:
Medium
Platforms:
Cisco IOS: 12.1(2)T, Cisco IOS: 12.1(3)T
Description:
Cisco Internetwork Operating System Software (IOS) versions 12.1(2)T and 12.1(3)T are vulnerable to a denial of service attack. A remote attacker could attempt to make a connection to certain TCP ports to corrupt the router's memory, which causes the router to reload. An attacker could use this vulnerability to cause a denial of service attack against the affected router. This vulnerability will occur when a connection is attempted to any of the following TCP ports: 3100-3999, 5100-5999, 7100-7999 and 10100-10999.
Remedy:
Apply the appropriate patch for your system, as listed in Cisco Systems Field Notice, May 24, 2001. See References.
References:
Cisco Systems Field Notice, May 24, 2001 - IOS Reload after Scanning Vulnerability http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml
CIAC Information Bulletin L-088 - Cisco IOS Reload after Scanning Vulnerability http://www.ciac.org/ciac/bulletins/l-088.shtml
CERT Vulnerability Note VU#178024 - Cisco IOS vulnerable to deferred DoS via SYN scan to certain TCP port ranges http://www.kb.cert.org/vuls/id/178024
ISS X-Force - Cisco IOS TCP port connection denial of service http://xforce.iss.net/static/6589.php
CVE-2001-0750 - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0750
GIAC Response:
GIAC will apply the patch specified in the References section in order to defeat

this vulnerability immediately. An upgrade to the latest IOS will occur shortly thereafter.

Vulnerability:
Remote loading of configs is enabled on the router
Risk Level:
Medium
Platforms:
Cisco IOS
Description:
Remote loading (loading from the network) of configurations is enabled on the Cisco router. Remote loading of configs is insecure and should not be enabled. If a service config is enabled then a router will load its startup configuration from a remote device.
Remedy:
Disable network (remote) loading of the startup configuration. Refer to your router documentation for specific instructions.
References:
NSA Router Security Configuration Guide - Configuration Auto-Loading (page 65) http://nsa2.www.conxion.com/cisco/download.htm
ISS X-Force - Remote loading of configs is enabled on the router
http://xforce.iss.net/static/8401.php
GIAC Response:
GIAC will add the following lines to the router config to disable remote loading of config files:

```
no boot network
no service config
```

3.2.4 – OTHER FINDINGS:

pcAnywhere Connections

A large number of servers on the internal network were running pcAnywhere as a host. These services are required by GIAC for remote management of the servers. After reviewing some of the servers closely, it was discovered that many of the servers running pcAnywhere in host configuration allowed for encryption-less connections from client machines. Running pcAnywhere without encrypted communications presents a serious security risk. It is recommended that GIAC require pcAnywhere encryption level while denying lower encryption levels.

GIAC Response: GIAC understands the need for encrypted pcAnywhere connections and will modify host configurations accordingly.

Internal Modem Lines

While conducting end user interviews, it was discovered that many machines had analog phone lines connected to them. Some of these phone lines were for legitimate use such as connecting to banks for transferring funds. However, GIAC employees with laptops connect to their personal ISP in order to download their personal e-mail using these analog lines. Another use for the modems was to set up the corporate PC as a pcAnywhere host with a connection to the network so that the end user could work from home. In many cases where pcAnywhere was used on the desktop, there was no security set up on the host machine. Fredo Leigh auditors just dialed into the end user's PC and had unrestricted access to the network because the end user simply did not log off their PC in the evening. Upon further investigation, it was determined that company policy does not inhibit the use of analog phone lines on the desktop PCs.

In light of these discoveries, it is the highly recommended that GIAC change their corporate policy to limit the use of analog phone lines by internal employees.

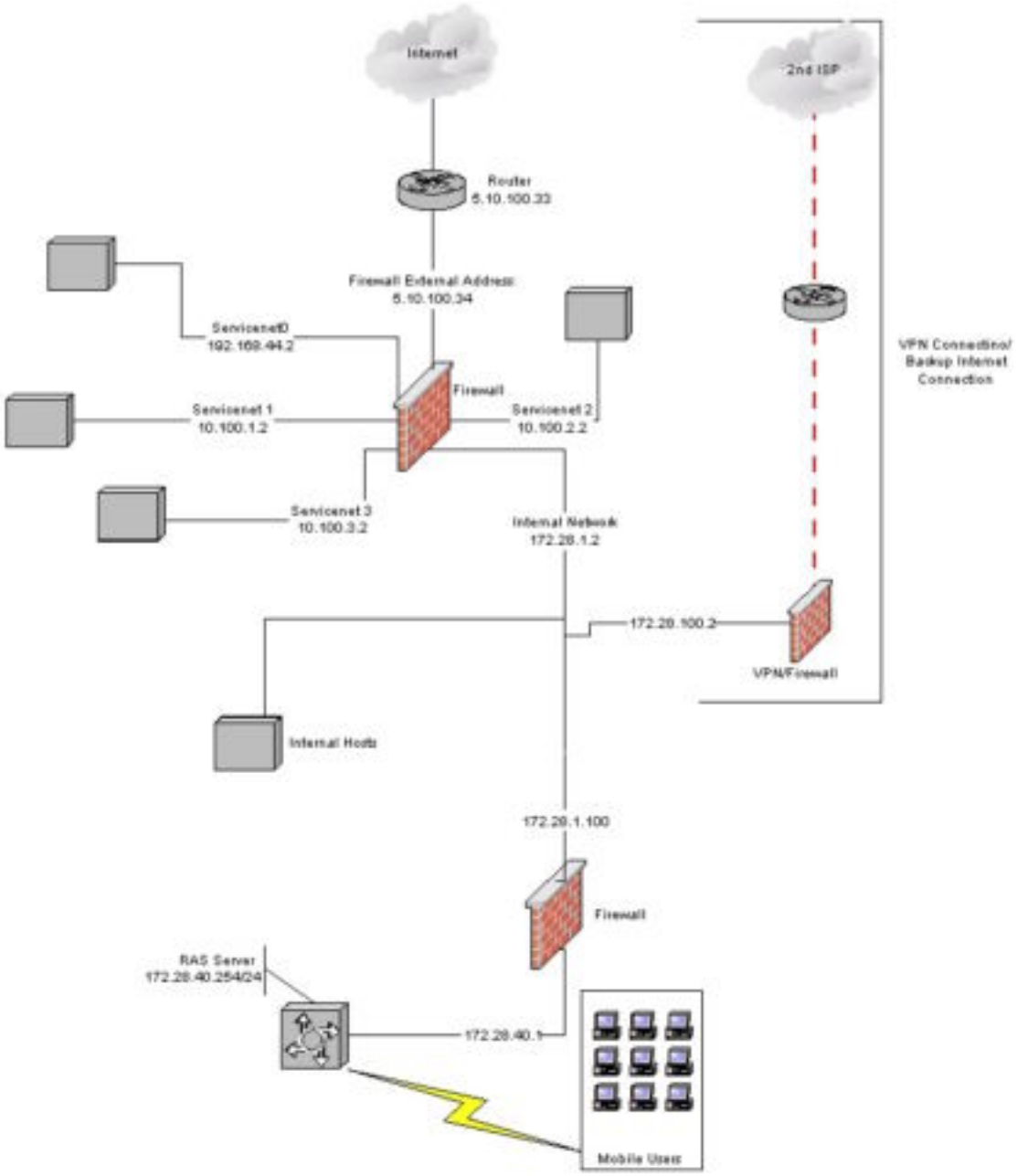
GIAC Response: The GIAC corporate policy will be reviewed and revised to limit the use of modems inside the GIAC building. Modems cannot be taken away from the laptop users but the analog lines in their offices will be removed. Only those with a legitimate business reason for having a modem sitting on their computer will be allowed to do so. Furthermore, those machines with allowed analog lines will be monitored closely by GIAC Security to verify that those machines are not connected to the GIAC network when a transmission over the analog line is committed.

VPN Connections and Redundant Internet Links

With roughly 85-100 VPN users potentially on the network at any given time, the GIAC Internet connection is most likely saturated. On average, all GIAC VPN users generally connect from 6:00 pm to 1:00 am with minimal usage during the day. While this trend is acceptable now, future growth may change this usage pattern.

Another issue with the Internet connection is there is no redundancy in the GIAC Internet connection. The mainstay of GIAC's connection to its business is connections to customers, suppliers and partners over an Internet link. Without an Internet connection, GIAC is shut down.

It is recommended that GIAC get a larger Internet connection and get a second connection through a different ISP in order to 1) route all VPN connections through the second ISP and 2) have a redundant connection to the Internet in case Ackmee.net goes down for some reason.



A second recommendation is to use a hardware-based VPN device such as the Nortel Contivity or the Cisco VPN Concentrator. By utilizing one of these devices, the encryption and compression is performed by hardware-based cards that carry out these processes in a more efficient manner. The Cisco device also has the capability to allow the user to add a second encryption card option in order to speed up this process. Both devices allow for RADIUS and SecureID authentication thereby increasing security and easing user management.

Reconfiguring the firewall to allow access to the Servicenet machines is relatively simple to accomplish in the event of an emergency. A suggestion for the configuration of the firewalls is to save the current configuration to disk then re-configure the firewalls based on the new ISPs IP addressing scheme. Once that configuration has been created and tested, back that configuration up to CD or some other location and store it for emergencies. The external DNS would need to be changed to allow the new ISP as the secondary DNS server. When Ackmee.net went down, the new ISP would need to reconfigure the DNS table for the new virtual addresses.

Note: The following response exemplifies some of the politics associated with conducting a security audit. While many companies will accept most suggestions – especially those suggestions that may prevent the loss of income, some companies feel as though the money spent isn't worth the effort. This response does not reflect my personal opinion and is only included to give insight into what some companies might say to a suggestion to spend more money on security.

GIAC Response: GIAC will review the feasibility of adding a second Internet connection. The redundancy of Internet lines is probably a good idea but the cost associated with adding the second line and the equipment to support that line is not in the I.S. budget. GIAC feels confident that if Ackmee.net was to ever go down, GIAC could afford the loss of one or two days of Internet downtime while Ackmee.net came back online. Ackmee.net has guaranteed us a 99.999% uptime and they have told us that the redundant lines in their Network Operations Center are pointing to three other upstream providers. Their guarantee is good enough for our lawyers. In addition, the VPN connection works fine for now. We will review the additional bandwidth suggestion whenever we notice that our web browsing speed is noticeably slower.

Time and Cost of the Fredo Leigh and Associates Audit: This audit was conducted over a two-week period. The actual external intrusion attempts and network scans were conducted over each Friday, Saturday and Sunday nights on both weekends. During the week, the audit was conducted by interviewing security personnel, network administrators, help desk personnel, and end users. The final report was delivered one month later at a cost to GIAC of approximately $15000.

ASSIGNMENT 4 – DESIGN UNDER FIRE (25 POINTS)

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!
Select a network design from any GCFW practical posted in the previous **6 months** and paste the graphic into your submission. Be certain to list the URL of the practical you are using.
Research and design the following three types of attacks against the architecture:
An attack against the firewall itself.

1. Research and describe a vulnerability that has been found for the type of firewall chosen for the design.
    - Design an attack based on the vulnerability.
    - Explain the results of running that attack against the firewall.

2. A denial of service attack.
    - Subject the design to an attack from 50 compromised cable modem/DSL systems.
    - Describe the countermeasures that can be put into place to mitigate the attack that you chose.

3. An attack plan to compromise an internal system through the perimeter system.
    - Select a target and explain your reasons for choosing that target.
    - Describe the process to compromise the target.

Your attack information should be detailed – include the specifics of how the attack would be carried out. Do not simply say "I would exploit the vulnerability described in Vendor Security Bulletin XXX". What commands would you use to carry out the attack? Are exploit tools or scripts available on the Internet? What additional steps would you need to take prior to conducting the attack (reconnaissance, determining internal network layout, determining valid account name…)? Would any of your methods be noticed (log files, IDS…)? What "stealth" techniques could you employ to avoid detection? What countermeasures would help prevent your attack from succeeding?

If it is possible to carry out the attack on a test system, include screen shots, log files, etc. as appropriate to illustrate your methods.

In designing your attacks, keep the following in mind:

1. The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.
2. The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should **not** assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)
3. You must supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.
4. The attack does not necessarily have to succeed. If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

During this phase, I will be examining the network implemented by Klear Sideris located at http://www.giac.org/practical/Klear_Sideris_GCFW.zip.

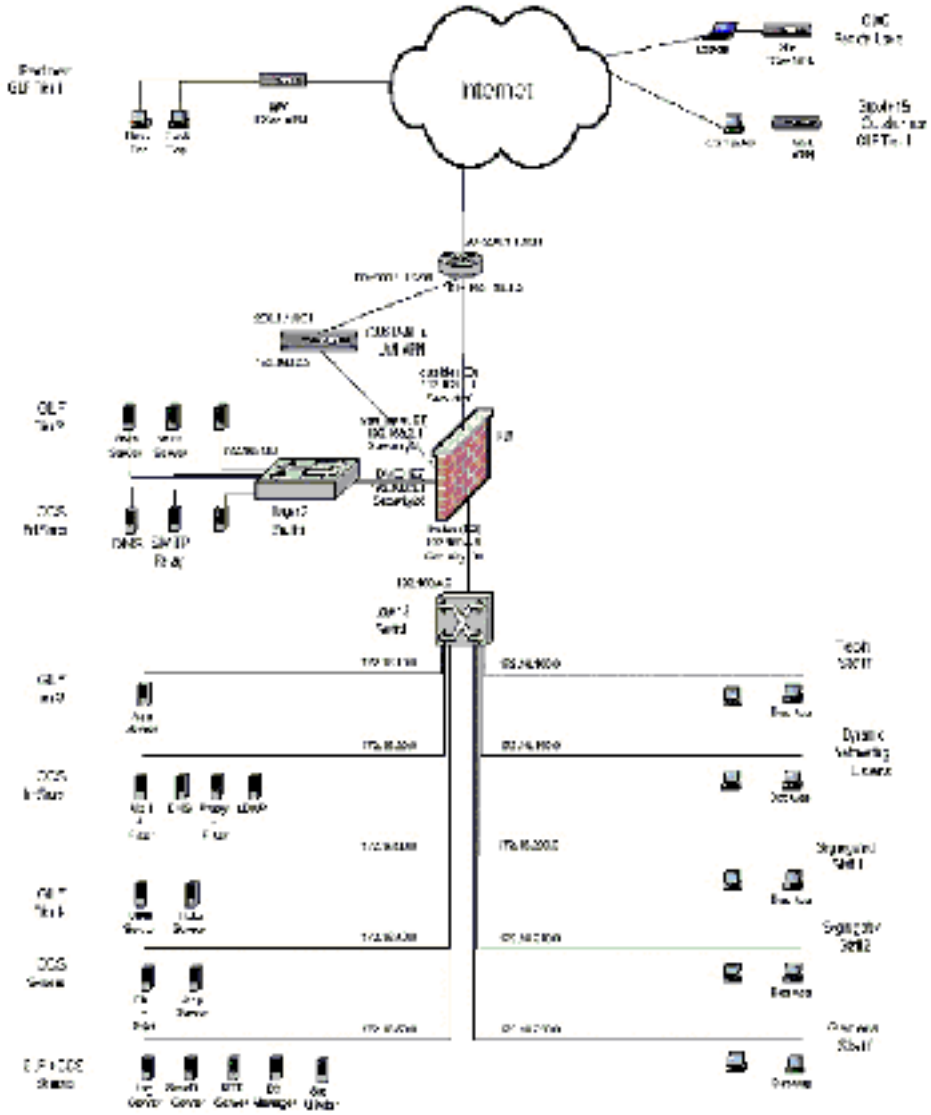


Figure 42 - Klear Sideris' GIAC Network

4.1 – ATTACK ON THE FIREWALL ITSELF

4.1.1 - Overview

There is a flaw in the Cisco PIX Firewall Manager (PFM) software that allows an attacker to gain full access to the firewall.

4.1.2 – References

Cert Vulnerability Note - http://www.kb.cert.org/vuls/id/639507
Cisco - http://www.cisco.com/warp/public/770/pixmgrfile-pub.shtml
Securiteam - http://www.securiteam.com/securitynews/6F00E1F2UM.html
Security Focus - http://www.securityfocus.com/bid/3419

4.1.3 - Explanation

Full access is gained by viewing the log file created on the PFM machine and gathering the *enable* password that is recorded in the log file in clear text. The log on the PFM machine is by default created in C:\Program Files\Cisco\PIX Firewall Manager\protect as the file PFM.LOG. An example of the log entry is as follows:

```
Jun 15 2002 06:11:18 <Receiving msg> - 9004
    172.16.1.109 0 0 0 1 5 mysupersecretpassword
```

4.1.4 – Implementation of the Attack

This attack requires access to the PIX Firewall Management workstation. While this is difficult for the Internet hacker, an internal hacker would have a relatively easy time utilizing this attack. The PIX Firewall Manager software runs on Windows 9x, NT, and 2000. Exploiting this vulnerability requires also attacking the hosting operating system. Of the three operating systems listed, the Windows 9x workstation would be the easiest to attack.. Aside from an insecure file system and no user authentication scheme, there isn't an auditing feature for the operating system. The other two operating systems are much harder to compromise but are by no means an impossible task.

In order to utilize this exploit, physical access to the machine and log on locally rights are required if the machine does not have shared directories under Windows 9x. Windows NT and Windows 2000 hosts share their hard drives as hidden shares (i.e. *C$*) by default so if the host machine is running one of these two operating systems, accessing the log files may be an easier task. The hacker will need to get an administrative account on the machine before accessing any administrative shares. Gathering the information required to begin the process of gaining access to these shares can be accomplished by running the tool *Cerberus Internet Scanner* (CIS) for Windows. CIS allows an attacker to determine the account names on Windows NT/2000 machines.

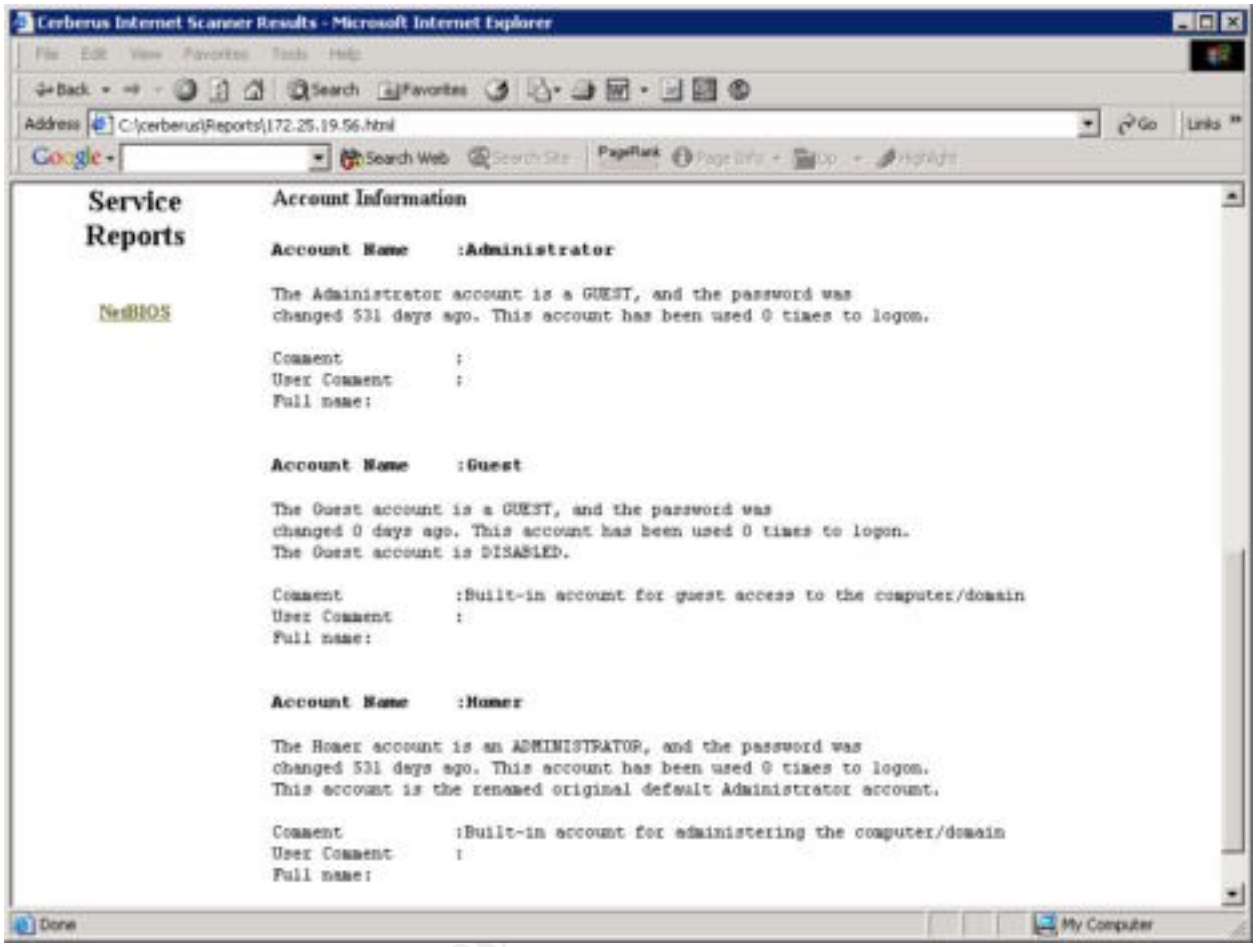


Figure 43 - The real administrator account is named Homer.

Once valid usernames are found, an attack can occur against the machine. This can be accomplished by using password crackers such as L0phtcrack, which allows for the sniffing of passwords over the network. Once the account has been cracked, accessing the PIX firewall password is as simple as running:

```
Net use r: [or some other drive letter] \\PIXMACHINE\C$
/user:administrator password
r:
cd "\program files\cisco\pix firewall manager"
type pfm.log | more
net use r: /delete
```

4.1.5 – Conclusions

This vulnerability is rather simple to exploit but information gathering prior to utilizing the exploit requires a greater level of expertise. This exploit is also only useful in environments that run PIX Firewall Manager software. A hacker will

also need to know the location of the management workstation, as the ability to access this machine remotely could be a problem. Local network security should be tight, especially on network management machines, in order to prevent this attack. Because this particular exploit is requires specific knowledge as to the whereabouts of the PFM software, it is especially attractive to potential disgruntled ex-employees or malicious vendors.

It's hard to say whether an attack such as this would be successful. With Klear's environment of over 500 employees, a fair amount of reconnaissance would need to be performed prior to attacking the firewall. It is also unclear as to whether the Cisco Firewall Manager software is in use on the management workstations. The PIX Device Manager (PDM) software, which ships with version 6.x and later firewalls, is not vulnerable. However, Klear may not wish to use the PDM software and is still able to use the PFM software with newer PIX devices.

4.2 DENIAL OF SERVICE ATTACK

Subject the design to an attack from 50 compromised cable modem/DSL systems.
Describe the countermeasures that can be put into place to mitigate the attack that you chose.

4.2.1 – Overview

In order to attack Klear Sideris' network, I have chosen the Tribe Flood Network 2000 (TFN2K) distributed denial of service attack. I have chosen this attack because it utilizes TCP, UDP, and ICMP traffic in order to "confuse" any attempts to locate TFN2K clients.

4.2.2 – References

Cert Advisory - http://www.cert.org/advisories/CA-1999-17.html
Symantec - http://securityresponse.symantec.com/avcenter/security/Content/2000_02_10_a.html
SANS Steps To Defeating Denial of Service Attacks - http://www.sans.org/dosstep/index.htm

4.2.3 – Implementation

The following terminology will be used here:

- Master - a host running the application that is used to initiate attacks by sending commands to other components.
- Slave - a host with a client that has a process running which is responsible

for receiving and carrying out commands issued by the master.
- Target - the victim of this distributed attack. Could be a host or network.

In TFN2K, the target may be hit with TCP/SYN, UDP, ICMP/PING, or BROADCAST PING (SMURF) packet flood attacks. Random patterns can also occur which utilizes all four types of attacks. The master computer can send the commands to the slave by using TCP (using random ports), UDP (using random ports), ICMP (using echo replies) or all three at random. To make matters worse when trying to stop TFN2K, these command packets are encrypted with CAST-256 with a key that is generated at compile time. In addition to the random command packet types and encryption, a TFN2K master also sends out random false packets in order to try to confuse the target's administrator.

Slaves do not respond to its master's commands so detecting the master's address is much more difficult than TFN2K's predecessor, TFN. Since the master now has no way of knowing whether the slaves have received the packets so the master sends out 20 command packets to the slave. When sniffing traffic on the suspected slave, these 20 packets can be used as a fingerprint. However, the source address on the packet sent by the master is spoofed. The source address in packets sent by the slave to the target is spoofed as well.

Prior to directing the attack to the network, I have installed the tfn2k client on ~50 computers that are cable or DSL networks. The owners of these computers helped this task because they failed to install any virus/host protection software or install a cable/DSL router on their home network. Once the clients were installed, the attack was launched on the PIX firewall in order to flood it with as much traffic as possible. Since there isn't a way to communicate with the slave once the attack begins, actively ending the attack is imperative if I do not want to get caught. Otherwise, the master will continue to send out packets to the client machines, running the risk of getting me caught.

4.2.4 – Reacting to a DDoS Attack

It's very difficult to stop a DDoS once it has begun. First, contacting local authorities and the FBI is imperative once the target and the target's ISP determine that a DDoS is occurring. The quicker this is accomplished, the better. As I stated in the previously section, the master computer will mostly likely continue to send out command packets to the slaves since a response isn't generate. Many "script kiddies" will want to see if what they're doing is actually working so they may continue the attack thinking that nothing is happening. This may help with tracking the attackers down. Another response would be to install an alternative route out to the Internet and/or changing the external IP addressing scheme.

4.2.5 – Conclusions

TFN2K is relatively easy to implement and is much harder to stop. I would have to believe that a DDoS against the PIX firewall using 50 client machines on cable and DSL networks would be successful in an attack. The ease of implementing a DoS attack is part of the reason why such attacks are frowned upon in the hacking world. Halting DoS attacks on the Internet begins with network administrators preventing these attacks from originating from their environment. By following guideline posted by SANS and other organizations, DoS attacks can be contained.

4.3 – ATTACKING INSIDE SERVICES

I will next compromise an internal system through the perimeter system. The target I chose was the IBM Web Sphere web server located in the DMZ. The reason I chose this target in particular was because:

1. My day job is considering deploying Web Sphere web servers for future web development projects. I hadn't research methods of attacking a Web Sphere web server yet and felt this was a good time to get started.
2. I hate GIAC because I was fired six months ago and I want to embarrass the company by shutting down their web servers.

4.3.1 – References

CVE-2001-0122 - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=+CVE-2001-0122
Defcom Labs Advisory - http://packetstormsecurity.nl/0101-exploits/defcom.websphere.txt
IBM - http://www-3.ibm.com/software/webservers/security.html

4.3.2 – The Attack

The method of attack I chose was based on the exploit described in CVE-2001-0122:

Kernel leak in AfpaCache module of the Fast Response Cache Accelerator (FRCA) component of IBM HTTP Server 1.3.x and Websphere 3.52 allows remote attackers to cause a denial of service via a series of malformed HTTP requests that generate a "bad request" error.

The actual attack involved sending a series "bad" GET request to the web server. An example of a bad request would be:

```
GET / HTTP/1.0\r\nuser-agent: 20000xnull\r\n\r\n
```

By running a script that contains a series of these bad requests will cause a kernel leak. The kernel leak will eventually use up all of the kernel memory and will cause the web server to not respond to any further requests.

This attack only works on Web Sphere servers that run the AfpaCache Module. The AfpaCache Module "turns Fast Response Cache Accelerator on or off"[11]. The Fast Response Cache Accelerator is a caching engine for the IBM Websphere web server[12].

4.3.3 – Conclusions

Reconnaissance and planning for this attack are minimal since the exploit requires simple commands run from the attacking workstation. Klear Sideris does not show the httpd.conf file in his design so without that information and without the version of the Websphere product that is in use, it is unknown as to whether the attack would work.

In determining whether an attacker can be discovered using this attack, if an IDS system is configured to capture `400 – Bad Request` errors coming from the server, the IDS administrator can be alerted to the possibility of this attack occurring against the web servers. Since the attack requires "a series of" malformed HTTP GET requests, it is assumed that attempting to hide the attack by slowing the rate of requests would not be a successful method of a stealthy attack.

The only solution given to this exploit is to comment out the three lines in the httpd.conf file that begins with the word **afpa**. A patch is mentioned on the IBM web site listed above but the link to the patch is dead. A search for a patch resulted in 0 hits on the IBM support web site.

[11] For more on the AfpaCache Module, consult http://www-3.ibm.com/software/webservers/httpservers/doc/v1319/9acdafpa.htm#afcache

[12] http://www-3.ibm.com/software/webservers/httpservers/doc/v51/ttun.htm#HDRDIVFRCA

Hosts

```
Hst-av.giacent.com
Description: Internal Anti-virus Server
Address: 172.28.1.65

Hst-dns1.giacent.com
Description: Internal DNS Server
Address: 172.28.1.53

Hst-dns2.giacent.com
Description: Internal DNS Server
Address: 172.28.1.54

Hst-exchange.giacent.com
Description: Internal MS Exchange Server
Address: 172.28.2.25

Hst-ftporder.giac.com
Description: Customer SSH Server (External)
Address: 5.10.100.37

Hst-ftporder.giacent.com
Description: Customer SSH Server (Internal)
Address: 10.100.2.30

Hst-IDS_Internalnet
Description: IDS Sensor for the internal network
Address: 10.100.3.28

Hst-IDS_InternetSensor
Description: IDS Sensor for the Internet
Address: 10.100.3.5

Hst-IDS_RASNetwork
Description: IDS Network Sensor Server for the RAS Subnet
Address: 10.100.3.40

Hst-IDS_Servicenet0
Description: Servicenet0 IDS Sensor Server
Address: 10.100.3.100

Hst-IDS_Servicenet1
Description: Servicenet1 IDS Sensor machine
Address: 10.100.3.80

Hst-IDS_Servicenet2
Description: Servicenet2 IDS Sensor server
Address: 10.100.3.20

Hst-IDS_Siteprotector
```

```
Description: Host machine managing the IDS sensor alerts
Address: 10.100.3.1

Hst-jack.giacent.com
Description: RS/6000 server
Address: 172.28.14.20

Hst-jill.giacent.com
Description: RS/6000 server
Address: 172.28.14.25

Hst-mail.giac.com
Description: SMTP Relay Server (External)
Address: 5.10.100.36

Hst-mailsweeper.giacent.com
Description: SMTP Relay Server (Internal)
Address: 10.100.2.25

Hst-mary.giacent.com
Description: RS/6000 server
Address: 172.28.14.40

Hst-news.ackmee.net
Description: Ackmee.net's news server
Address: news.ackmee.net

Hst-orderprocess1.giacent.com
Description: Internal Customer Order Processing Server
Address: 172.28.14.10

Hst-orderprocess2.giacent.com
Description: Internal Customer Order Processing Server
Address: 172.28.14.20

Hst-orders.giac.com
Description: Web-based orders server (External)
Address: 5.10.100.45

Hst-orders.giacent.com
Description: Web-based Orders server (Internal)
Address: 10.100.1.81

Hst-pinocchio.giacent.com
Description: RS/6000 server
Address: 172.28.14.30

Hst-proxy.giacent.com
Description: GIAC proxy server
Address: 172.28.1.80

Hst-sftp.giac.com
Description: Partner/Supplier SSH Server (External)
Address: 5.10.100.38
```

```
Hst-sftp.giacent.com
Description: Partner/Supplier SSH Server (Internal)
Address: 10.100.2.100

Hst-SFTP_Customer1
Description: SFTP Customer
Address: 7.82.44.22

Hst-SFTP_Customer10
Description: SFTP Customer
Address: 124.132.19.129

Hst-SFTP_Customer11
Description: SFTP Customer
Address: 23.49.112.77

Hst-SFTP_Customer12
Description: SFTP Customer
Address: 88.57.204.194

Hst-SFTP_Customer13
Description: SFTP Customer
Address: 79.104.63.229

Hst-SFTP_Customer14
Description: SFTP Customer
Address: 71.27.242.148

Hst-SFTP_Customer2
Description: SFTP Customer
Address: 104.127.18.201

Hst-SFTP_Customer3
Description: SFTP Customer
Address: 31.57.224.18

Hst-SFTP_Customer3b
Description: SFTP Customer
Address: 31.57.224.20

Hst-SFTP_Customer4
Description: SFTP Customer
Address: 7.55.237.124

Hst-SFTP_Customer5
Description: SFTP Customer
Address: 74.221.37.193

Hst-SFTP_Customer6
Description: SFTP Customer
Address: 50.18.12.202

Hst-SFTP_Customer7
Description: SFTP Customer
Address: 42.12.77.29
```

```
Hst-SFTP_Customer8
Description: SFTP Customer
Address: 7.92.101.226

Hst-SFTP_Customer9
Description: SFTP Customer
Address: 197.62.112.46

Hst-SP-SSH1
Description: Supplier/Partner SSH Client
Address: 197.34.201.22

Hst-SP-SSH2
Description: Supplier/Partner SSH Client
Address: 7.42.32.222

Hst-SP-SSH3
Description: Supplier/Partner SSH Client
Address: 87.49.98.51

Hst-SP-SSH4
Description: Supplier/Partner SSH Client
Address: 112.232.1.82

Hst-SP-SSH5
Description: Supplier/Partner SSH Client
Address: 2.55.237.122

Hst-SP-SSH6
Description: Supplier/Partner SSH Client
Address: 27.88.41.19

Hst-SP-SSH7
Description: Supplier/Partner SSH Client
Address: 41.56.102.65

Hst-SP-SSH8
Description: Supplier/Partner SSH Client
Address: 36.133.114.202

Hst-supplyprocess1.giacent.com
Description: Internal Supplier Processing Server
Address: 172.28.14.60

Hst-syslog.giacent.com
Description: Syslog Server
Address: 172.28.1.10

Hst-thumper.giacent.com
Description: RS/6000 server
Address: 172.28.14.35

Hst-webdata.giacent.com
Description: Web-orders Database Server
Address: 192.168.44.10
```

```
Hst-webmail.giac.com
Description: GIAC Webmail Server (External)
Address: 5.10.100.47

Hst-webmail.giacent.com
Description: GIAC Webmail Server (Internal)
Address: 10.100.1.80

Hst-webserv.giacent.com
Description: Public Web Server (Internal Address)
Address: 10.100.1.80

Hst-www.giac.com_ext
Description: GIAC Public Web server (External)
Address: 5.10.100.46

Universe*
Description:
Address: 0.0.0.0
```

Subnets

```
Sub-Servicenet0
Description: Servicenet0 Subnet - 192.168.44.0
Address: 192.168.44.0 Network Mask: 255.255.255.0

Sub-Servicenet1
Description: Servicenet1 subnet - 10.100.1.0
Address: 10.100.1.0 Network Mask: 255.255.255.0

Sub-Servicenet2
Description: Servicenet2 Subnet - 10.100.2.0
Address: 10.100.2.0 Network Mask:  255.255.255.0

Sub-Servicenet3
Description: Servicenet3 Subnet - 10.100.3.0
Address: 10.100.3.0 Network Mask: 255.255.255.0

Sub-172.28.1.0
Description: Services Network
Address: 172.28.1.0 Network Mask: 255.255.255.0

Sub-172.28.2.0
Description: Executive Offices Network
Address: 172.28.2.0 Network Mask: 255.255.255.0

Sub-172.28.3.0
Description: HR and Corporate Trainers Network
Address: 172.28.3.0 Network Mask: 255.255.255.0

Sub-172.28.4.0
Description: Sales and Marketing Network
Address: 172.28.4.0 Network Mask: 255.255.255.0

Sub-172.28.5.0
Description: Accounting Network #1
```

```
Address: 172.28.5.0 Network Mask: 255.255.255.0

Sub-172.28.6.0
Description: Accounting Network #2
Address: 172.28.6.0 Network Mask: 255.255.255.0

Sub-172.28.7.0
Description: Training Room Network
Address: 172.28.7.0 Network Mask: 255.255.255.0

Sub-172.28.8.0
Description: App Development Network
Address: 172.28.8.0 Network Mask: 255.255.255.0

Sub-172.28.9.0
Description: Helpdesk Network
Address: 172.28.9.0 Network Mask: 255.255.255.0

Sub-172.28.10.0
Description: I.S. Networking Department Network
Address: 172.28.10.0 Network Mask: 255.255.255.0

Sub-172.28.11.0
Description: Legal Department Network
Address: 172.28.11.0 Network Mask: 255.255.255.0

Sub-172.28.12.0
Description: Infosec Network
Address: 172.28.12.0 Network Mask: 255.255.255.0

Sub-172.28.13.1
Description: Networking Test Network
Address: 172.28.13.0 Network Mask: 255.255.255.0

Sub-172.28.14.0
Description: RS/6000 Server Network
Address: 172.28.14.0 Network Mask: 255.255.255.0

Sub-172.28.15.0
Description: Misc. Employee Network #1
Address: 172.28.15.0 Network Mask: 255.255.255.0

Sub-172.28.16.0
Description: Misc. Employee Network #2
Address: 172.28.16.0 Network Mask: 255.255.255.0
```


Groups

```
Grp-GiacentNet
Description: All internal subnets
Members:
      Sub-172.28.1.0
      Sub-172.28.2.0
      Sub-172.28.3.0
      Sub-172.28.4.0
      Sub-172.28.5.0
      Sub-172.28.6.0
```

```
      Sub-172.28.7.0
      Sub-172.28.8.0
      Sub-172.28.9.0
      Sub-172.28.10.0
      Sub-172.28.11.0
      Sub-172.28.12.0
      Sub-172.28.13.0
      Sub-172.28.14.0
      Sub-172.28.15.0
      Sub-172.28.16.0

Grp-IDSServers
Description: Machines running IDS Sensors or Services
Members:
            Hst-IDS_InternalNet
            Hst-IDS_InternetSensor
            Hst-IDS_RASNetwork
            Hst-IDS_Servicenet0
            Hst-IDS_Servicenet1
            Hst-IDS_Servicenet2
            Hst-IDS_Siteprotector

Grp-SSHCustomers
Description: Customers using SSH to submit orders
Members:
      Hst-SFTP_Customer1
   Hst-SFTP_Customer10
   Hst-SFTP_Customer11
   Hst-SFTP_Customer12
   Hst-SFTP_Customer13
   Hst-SFTP_Customer14
   Hst-SFTP_Customer2
            Hst-SFTP_Customer3
            Hst-SFTP_Customer3b
            Hst-SFTP_Customer4
            Hst-SFTP_Customer5
            Hst-SFTP_Customer6
            Hst-SFTP_Customer7
            Hst-SFTP_Customer8
            Hst-SFTP_Customer9

Grp-SSHPartners-Suppliers
Description: Suppliers/Partners using SSH
Members:
            Hst-SP-SSH1
            Hst-SP-SSH2
            Hst-SP-SSH3
            Hst-SP-SSH4
            Hst-SP-SSH5
            Hst-SP-SSH6
            Hst-SP-SSH7
            Hst-SP-SSH8

Grp-webservers
Description: public web servers
Members:
```

```
            Hst-webserv.giacent.com
            Hst-webmail.giacent.com

Grp-webserveradmins
Description: Subnets that will manager the web servers
Members:
```
Sub-172.28.8.0
Sub-172.28.10.0

Network Interfaces

```
RASNet
Address: 172.28.40.2

InternalNet
Address: 172.28.1.253
```

Hosts

```
Hst-CEO
Description: IP Address used by the CEO
Address: 172.28.40.10

Hst-CIO
Description: IP Address used by the CIO
Address: 172.28.40.11

Hst-CFO
Description: IP Address used by the CFO
Address: 172.28.40.12

Hst-FWA
Description: IP Address used by the Firewall Administrator
Address: 172.28.40.13

Hst-ExternalFirewall
Description: IP Address for the border Firewall
Address: 172.28.1.2
```

Subnets

```
Sub-DHCPNet
Description: IP Address Assigned by the RAS Server
Address: 172.28.40.32
Network Mask: 255.255.255.224

Sub-RasNet
Description: Entire RAS Subnet
Address: 172.28.40.0
Network Mask: 255.255.255.0

Sub-172.28.2.0
Description: Subnet used by Windows network servers
Address: 172.28.2.0
Network Mask: 255.255.255.0
```

Groups

```
Grp-Execs
Description: Corp. Executives
Members:
            Hst-CEO
            Hst-CIO
            Hst-CFO
            Hst-FWA
```

RESOURCES AND REFERENCES

"IANA Well-Known Port Assignments". 15 August 2002. URL: http://www.iana.org/assignments/port-numbers

Matt Curtin and Marcus J. Ranum. "Internet Firewalls FAQ". 3 December 2000. URL: http://www.interhack.net/pubs/fwfaq/. (29 July 2002)

Romanofski, Ernest. "A Comparison of Packet Filtering Vs Application Level Firewall Technology". 28 March 2001. URL: http://rr.sans.org/firewall/app_level.php (1 August 2002)

Maxon, Keith D. "Application Layer Firewalls vs. Network Layer Firewalls: Which Is the Better Choice?" 13 Aug 2000 URL: http://rr.sans.org/firewall/firewall.php (1 August 2002)

"SQL Security Checklist". URL: http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4. (11 August 2002)

"Snakefoot's WinNT, Win2k, WinXP Service Details P-Q-R". WINNT, WIN2K, WinXP Service Details. URL:http://snakefoot.fateback.com/tweak/winnt/service_details/service_details_pqr.html (12 August 2002)

"Q155831 - XADM: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall". URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q155831 (12 August 2002)

Mills, Dave. "Time Synchronization Server." 4 August 2002. URL: http://www.eecis.udel.edu/~ntp/ (16 August 2002)

"Overview of Cisco Secure ACS". Cisco Secure ACS 3.0 for Windows 2000/NT Servers User Guide. 13 July 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt30/user/index.htm (18 August 2002)

Bice, Brent "Building a Web Mail Server with SquirrelMail." Sys Admin - The Journal for UNIX Systems Administrators July 2002 (2002) 25-29.

United States National Security Agency "Router Security Configuration Guide" 25 March 2002 URL: http://nsa2.www.conxion.com/cisco/download.htm (10 September 2002)

United States National Security Agency "The 60 Minute Network Security Guide" 12 July 2002 URL: http://nsa2.www.conxion.com/cisco/download.htm (10 September 2002)

Symantec Corporation "How to Remove or Change the Firewall Secure Gateway Banner" Symantec Enterprise Firewall Knowledge Base Document ID: 2001111412052154 13 December 2001 URL: http://www.symantec.com/techsupp/

Computer Security Institute "Sample Warning Messages" URL: http://www.gocsi.com/sampwarn.htm 10 September 2002

Symantec Corporation "Symantec VPN Configuration Guide – Version 2.0" 7 Jan 2002 URL: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_config.pdf (10 September 2002)

Symantec Corporation “Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide” 14 January 2002 URL ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_ref.pdf (10 September 2002)

Symantec Corporation “Symantec Enterprise Firewall & Symantec Enterprise VPN - VPN Configuration Guide Version 2.0” 7 January 2002 URL: ftp://ftp.symantec.com/public/updates/sevpn_config.zip (10 September 2002)