

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment v 2.0

Pedro Haworth
April 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Executive Summary

1. Security Architecture
1.1. GIAC Enterprises Business Operations
1.2. Access Requirements
1.2.1. Customers
1.2.2. Suppliers
1.2.3. Partners
1.2.4. Onsite Employees
1.2.5. Mobile Employees
1.2.6. General Public
1.2.7. Other Requirements
1.3. Network Architecture
1.3.1. Network Diagram
1.3.2. Routers
1.3.3. Firewalls
1.3.4. IDS/IPS
1.3.5. VPNs
1.3.6. Other Security Components
1.3.7. Network Addressing Scheme

2. Security Policy and Tutorial
2.1. Router
2.1.1. Router Policy and Configuration
2.1.2. Border Router Tutorial
2.2. External Firewall Policy and Configuration
2.2.1. External Firewall Policy and Configuration
2.2.2. External Firewall Tutorial
2.3. **VPN** VPN Policy and Configuration
2.4. IDS/IPS
2.4.1. IDS/IPS Tutorial

3. Verify the Firewall Policy
3.1. Firewall Validation Plan
3.1.1. Technical Approach
3.1.2. Variable Considerations
3.1.3. Calculating Costs
3.1.4. Risk Considerations
3.2. Firewall Validation Execution

© SANS Institute 2004, Author retains full rights.

3.2.1. Tools used in Validation
3.2.2. Firewall Validation Step-by-Step
3.3. Firewall Validation Results and Analysis
3.3.1. Firewall Validation Results
3.3.2. Recommendations
4. Design Under Fire
4.1. Purpose of Exercise
4.2. Design Weakness Discussion
4.3. Perform Attack
4.3.1. Attack Design for Firewall
4.3.2. Attack Design for DoS
4.3.3. Attack Design for Compromising Internal
Appendix
Appendix A Large Network Diagram
Appendix B Router Configuration

References

© SANS Institute 2004, Author retains full rights.

Executive Summary

GIAC Enterprises, in its effort to increase its online fortune cookie saying market share, has initiated an effort to create a comprehensive, scalable and secure business infrastructure. The purpose of this study is to streamline the exchange of proprietary data with their customers, suppliers and partners, and better secure their way of doing business on the Internet. Because of budgetary constraints, GIAC is attempting to improve its infrastructure with a minimal amount of capital investment, using resources that are largely already available within the company. The burden has been placed on the shoulders of the two person security staff to come up with a strategy for securing the environment and planning for future growth.

The following pages explain GIAC Enterprises business operations with their customers, suppliers and partners, as well as their mobile and on-site employees. It also details the physical infrastructure, security policy and expansion strategies for the future.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Security Architecture

1.1 GIAC Enterprises

GIAC Enterprises is committed to maintaining itself as a market leader in the on-line fortune cookie saying industry. By maintaining a high-level of secrecy with its core business processes, GIAC Enterprises can assure its product will arrive to the end customer securely. Communications in their business processes is the key to success, and facilitating this with their customer, suppliers and partners is how GIAC Enterprises plans to expand their market share.

At the core of the company is a database that contains all of the fortune cookie sayings. This database is accessed in different ways by their customers, suppliers and partners, however, all access it via a web enabled application that resides in a DMZ zone off of the main firewall. This in-house developed web application called *FortuneDealer* communicates with the *FortuneDealer* database that resides within the internal network of the company.

Transactions between Internet-based nodes and the database are protected by a number of security measures including Access Control Lists (ACL's), firewalls, Network Intrusion Prevention Systems (NIPS) and Host Intrusion Prevention Systems (HIPS) which are all detailed herein.

Additionally, the business process is streamlined for remote and mobile users who are granted access to key internal resources via the firewall that doubles as a VPN gateway. This eliminates the need for field sales personnel to come to the office for submitting contracts established with customers, suppliers and partners, and also facilitates access for telecommuters and on-call support personnel.

1.2 Business Operations and Access Requirements

This section details how each entity interacts with the GIAC Enterprise security infrastructure.

1.2.1 Customers

There are two options for customer wishing to purchase bulk online fortune cookie sayings. If a customer chooses to commit to a single or multi-year contract, a username, password and grant number would be given to access the *FortuneDealer* web-enabled application that residing on the extranet webserver. A customer that has signed a contract is typically permitted to access our entire fortune sayings database as many times as they wish for a fixed period of time according to the terms of the contract.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A customer that has not signed a contract with us is welcome to access the same *FortuneDealer* application and purchase bulk fortunes on a per-transaction basis with a credit card. This will provide them with a fixed number of sayings (ranging from minimum of 500 sayings to a maximum of 10,000 sayings) for set price.

Being an on-line based service, the only way customers may gain access to our *FortuneDealer* application is via the Internet. A customer must use a web browser that can support 128-bit SSL encryption. They would access the *FortuneDealer* application from our main website initially through standard HTTP and subsequently through HTTPS during and after authentication. *FortuneDealer* uses MS SQL between the Webserver in the DMZ and the database server on the internal network to communicate all transactions such as customer authentication, orders, sales and fortune cookie sayings uploads to the customer.

A customer that has any issues can also contact GIAC Enterprises customer support by phone or by e-mail.

Summary of Customer Access Requirements

Who	From	To	Protocol	Port
Customer	Internet	DMZ	HTTP	80
Customer	Internet	DMZ	HTTPS	443
Customer	Internet	DMZ	SMTP	25
Customer	Internet	DMZ	DNS	53
FortuneDealer	DMZ	Inside Network	MS SQL	1433

1.2.2 Suppliers

Our suppliers keep us competitive in our industry. We have combed the world to find talented providers of insightful single sentence sayings and lucky numbers that are pertinent to the customers in the many markets to which we sell our bulk fortunes. Our suppliers vary from single person operations that supply new sayings every few weeks to larger companies that supply sayings to us on a daily basis. We therefore have two ways by which our suppliers transmit sayings into our *FortuneDealer* database.

For our smaller suppliers, we have established an interface to the *FortuneDealer* web application that allows them to log-on to *FortuneDealer* via the internet and upload their bulk sayings in a flat file they can create with any word processing application. The supplier must use a web browser that can support 128-bit SSL encryption. Communication between the Webserver in the DMZ and the database server on the internal network allows for integration of these sayings into our database via MS SQL network calls.

For our larger suppliers that cannot use this method, we have established an FTP server in our DMZ that can receive PGP encrypted files from them. These files are encrypted with the supplier's private-key and GIAC Enterprises database

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

server's public-key. Permissions on this server only allow a supplier to authenticate and perform a *put* command. *List* and *get* commands are disabled for all users except for the database process user when coming from the internal network. A process on the internal database server monitors the incoming directory of this FTP server. When a file is detected in the incoming directory of the FTP server, the database server process initiates an FTP *get* and pulls the document to the database server. The file is then automatically authenticated and decrypted with the database server's private-key using Mcafee Security E-Business Server.[1] The contained flat file is then scanned for viruses locally before its contents are automatically imported by the server-side version of *FortuneDealer*.

A supplier that has any issues can also contact GIAC Enterprises customer support by phone or by e-mail.

Summary of Supplier Access Requirements

Who	From	To	Protocol	Port
Supplier	Internet	DMZ	HTTP	80
Supplier	Internet	DMZ	HTTPS	443
Supplier	Internet	DMZ	FTP	20, 21
Supplier	Internet	DMZ	SMTP	25
Supplier	Internet	DMZ	DNS	53
FortuneDealer	DMZ	Inside Network	MS SQL	1433
FortuneDealer Database	Inside Network	DMZ	FTP	20, 21

1.2.3 Partners

We have established key partnerships with companies in markets where English is not the spoken language. These partners have signed agreements with us to provide our bulk fortunes to customers in their local countries in exchange for a small percentage of their gross sales (typically 5-15%). Much like our customers, these partners access *FortuneDealer* via the internet with a username, password and grant number in order to obtain the sayings that they will translate and sell themselves. They also require a browser that can support 128-bit SSL encryption to access the application.

Unlike our customers, our partners have access to different options within *FortuneDealer* that enable them to download only the differential of our latest sayings.

A partner that has any issues can also contact GIAC Enterprises customer support by phone or by e-mail.

[1] ***Mcafee E-Business Server 7.1 Datasheet***. Network Associates, Inc. 2002. URL: http://www.nai.com/us/_tier2/products/_media/mcafee/ds_ebusiness_server.pdf (3 Mar, 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Summary of Partner Access Requirements

Who	From	To	Protocol	Port
Partner	Internet	DMZ	HTTP	80
Partner	Internet	DMZ	HTTPS	443
Partner	Internet	DMZ	SMTP	25
Partner	Internet	DMZ	DNS	53
FortuneDealer	DMZ	Inside Network	MS SQL	1433

1.2.4 Onsite Employees

Our onsite employees serve a number of functions within the company such as sales, customer service, legal, human resources, IT and management. While they have different purposes within the organization, they have very similar requirements for their computers. Company policy states that every onsite employee requires a computer that they can use to:

- Access the *FortuneDealer* database
- Create and read documents, spreadsheets and presentations
- Access shared documents, spreadsheets and presentations on servers
- Communicate with customers, partners and suppliers via e-mail
- Access the Internet for company related research

In addition to these, the computer should have sufficient privileges for the IT department to form basic administration of the device such as (ICMP) and for it to function in a Windows based LAN environment (DHCP, DNS, NetBIOS). IT administrators require only SSH and Telnet in addition to the basic requirements and will use them for maintaining the IPS sensor and the border router. *Terminal Services* will used for communication between specific internal workstations and the firewall for configuration.

Summary of Onsite Employee Access Requirements

Who	From	To	Protocol	Port
Employee	Inside Network	Internet/DMZ	HTTP	80
Employee	Inside Network	Internet/DMZ	HTTPS	443
Employee	Inside Network	Internet/DMZ	FTP	20/21
Employee	Inside Network	Inside Network/ DMZ	SMTP	25
Employee	Inside Network	Inside Network	MS SQL	1733
Employee	Inside Network	Inside Network	DNS	53
Employee	Inside Network	Inside Network	DHCP	67/68
Employee	Inside Network	Inside Network	NetBIOS	137-139
IT Admins	Inside Network	Internet (router)	Telnet	23
IT Admins	Inside Network	Firewall	Terminal Services	3389

The standard desktop computer issued to onsite employees is as follows:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Intel P4 2.4 GHz
- 256 MB RAM
- 60 GB Hard Drive
- 10/100 Ethernet NIC

Each of these workstations is loaded with the following software:

- Microsoft Windows XP Pro SP1 (latest hotfix level)
- Microsoft Office 2003 (latest hotfix level)
- Microsoft Internet Explorer 6 SP1 (latest hotfix level)
- Mcafee ePO agent (to manage Mcafee products)
- Mcafee VirusScan Enterprise 7.1 (latest engine and virus definitions)
- Mcafee Desktop Firewall 8.0 (latest IDS signatures loaded)
- *FortuneDealer* Internal Client Software
- PuTTY (available for IT staff only)

Special consideration was made to include security related software that can be easily centrally managed and automatically updated. Such is the case with Mcafee VirusScan and Mcafee Desktop Firewall that are managed by Mcafee ePO Server.[2]

1.2.5 Mobile Employees

Our mobile employees consist primarily of the sales force, IT on call staff and management totaling no more than 30 people. The mobile staff has the same requirements as the onsite staff; however, they need to be able to perform their tasks outside of the office.

Summary of Onsite Employee Access Requirements

Who	From	To	Protocol	Port
Mobile Employee	Internet	Firewall	PPTP	1723
Mobile Employee	Internet	DMZ	DNS	53
Mobile Employee	Internet (VPN)	Inside Network	SMTP	25
Mobile Employee	Internet (VPN)	Inside Network	MS SQL	1733
Mobile Employee	Internet (VPN)	Inside Network	DNS	53
Mobile Employee	Internet (VPN)	Inside Network	NetBIOS	137-139
Mobile IT Admins	Internet (VPN)	Internet/DMZ	Telnet	23
Mobile IT Admins	Internet (VPN)	Internet/DMZ	SSH	22
Mobil IT Admins	Internet(VPN)	Internet/DMZ	Terminal Services	3389

The laptop computer issued to mobile employees is as follows:

[2] ***Mcafee ePolicy Orchestrator 3.0 DataSheet***. Network Associates, Inc. 2003. URL: http://www.nai.com/us/_tier2/products/_media/mcafee/ds_epolicy_orchestrator.pdf (Mar 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Intel Centrino 1.6 GHz
- 512 MB RAM
- 60 GB Hard Drive
- 10/100 Ethernet NIC
- Integrated WLAN NIC

Each of these computers is loaded with the following software:

- Microsoft Windows XP Pro SP1 (latest hotfix level)
- Microsoft Office 2003 (latest patch level)
- Microsoft Internet Explorer 6 SP! (latest hotfix level)
- Mcafee ePO agent (to manage Mcafee products)
- Mcafee VirusScan Enterprise 7.1 (latest engine and virus definitions)
- Mcafee Desktop Firewall 8.0 (latest IDS signatures loaded)
- *FortuneDealer* Internal Client Software
- PuTTY (available for IT staff only)

1.2.6 General Public

The general public needs only to access the website and be able to send e-mail to employees within our company.

Summary of General Public Access Requirements

Who	From	To	Protocol	Port
Customer	Internet	DMZ	HTTP	80
Customer	Internet	DMZ	SMTP	25

1.2.7 Other Requirements

Below are the access requirements for other servers.

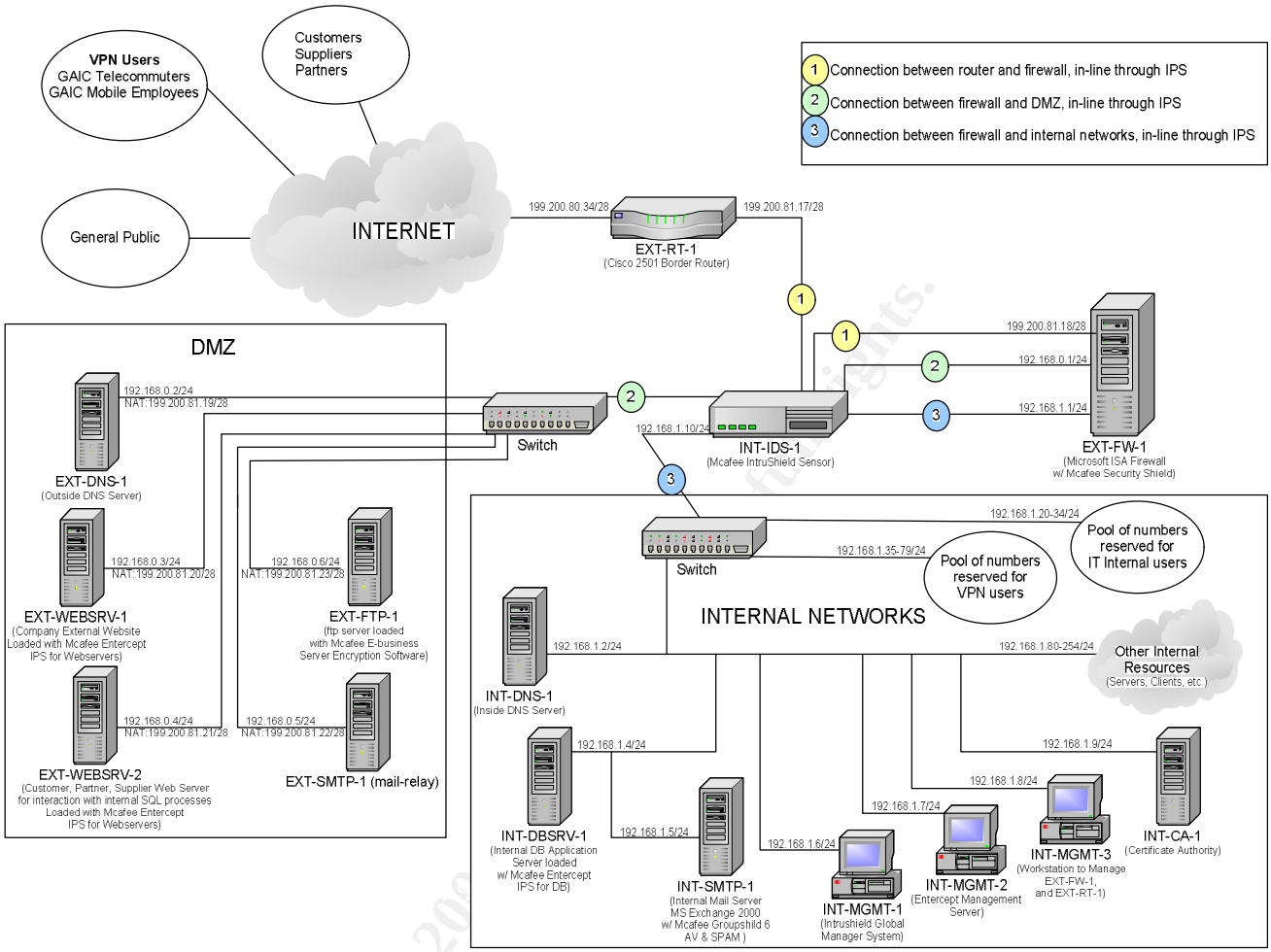
Summary of Server Access Requirements

Who	From	To	Protocol	Port
Entercept Agents	DMZ	Internal Network (INT-MGMT-2)	TCP	5005
EXT-SMTP-1	DMZ	Internal Network (INT-SMTP-1)	SMTP	25

1.3 Network Architecture

1.3.1 Network Diagram

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



A larger version of this diagram is located in Appendix A at the end of the document.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3.2 Router

A Cisco 2501 was chosen because of budgetary constraints. It is a legacy device that remains from the old network infrastructure. The router is a 2500 processor with 4096 Kbytes of main memory, running Cisco IOS 2500 version 11.2(9)P[3], release fc1. The device will be replaced within the year when IT receives funding. At that time, the architecture will be revised.

This router serves as the only connection between GIAC Enterprises' corporate network and the existing ISP. It is the true physical delineation point that distinguishes between LAN and WAN in this environment, and serves as the first line of defense when filtering traffic destined to the internal or DMZ networks. Robust ACL and protocol restrictions have been instituted for this device, and management access has been restricted to a specific address on the network.

Physical security of this device is assured by placing the router in a locked room with all other security components in this infrastructure.

1.3.3 Firewall

A Microsoft centric senior management staff has dictated that the majority of the components used in this environment be Microsoft Windows based. As a result, the use of a Microsoft Internet Security and Acceleration Server 2000 (ISA Server) was selected. This device has been loaded on a dual Pentium 4, 2 GHz server, with 2 GB of RAM with three 160 gigabyte hard-drives, using RAID 5 fault tolerance[4], running Windows Server 2000, SP4 and all the latest hotfixes for the OS. The Stand Alone server has three network interfaces; one dedicated to router, one to the DMZ environment and the last the internal networks. The ISA server is also to the most current level of hotfix.

The firewall serves as the primary means of defense when it comes to distinguishing trusted traffic from untrusted traffic. By applying a set of rules based on place of origin, destination, protocol, port and content, this device dictates whether data is permitted to proceed. Consider it the sheriff of the secure infrastructure of GIAC Enterprises. It has been placed immediately behind the router as the gateway to the internal network.

Additionally, the operating system has been hardened by removing all unnecessary services and applications such as:

---

[3] ***Release Notes for Cisco IOS Release 11.2(2)P***. Cisco Systems, Inc. 1998. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/xprn112/141503.htm (Mar 7, 2004)

[4] Shiner, Thomas and Shinder, Debra. ***Configuring ISA Server 2000.*** Rockland: Syngress Publishing, Inc. 2001. Pg 220.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

• DHCP • DNS • WINS • Certificate Services • IIS Services: WWW, SMTP, NNTP, FTP • Mail Servers, such as Exchange • Third party FTP servers • Mail clients, such as Outlook and Outlook Express • NetMeeting • Alerter • Clipbook • Computer Browser • Distributed File System • Fax Service • File Replication • Indexing Service • Internet Connection Sharing	• Intersite Messaging • Kerberos Key Distribution Center • License Logging Service • Messenger • NetMeeting Remote Desktop Sharing • Network DDE • Print Spooler • QoS RSVP • Removable Storage • RunAs • Telnet • Disabling File and Printer sharing on the external interface • Disabling Client for Microsoft Networks on the external interface • Disabling NetBIOS over TCP/IP on the external interface [5]

Keeping defense in depth as a priority in this implementation, the ISA Server has also been loaded with the Mcafee SecurityShield 1.0 software that uses ISA Server's filter extensions. When FTP, HTTP, or SMTP packets arrive at the ISA Server, ISA Server redirects them to SecurityShield, which scans the packets for viruses, spam, and other malicious content, and then passes them back to ISA Server for delivery with minimal latency.

The ISA Firewall is managed remotely with Terminal Services. INT-MGMT-3, a client device on the internal network has been designated as the management workstation for the firewall as well as the router. Access to the firewall terminal service is only permitted from this workstation.

Physical security of this device is assured by placing the ISA Firewall in a locked room with all other security components in this infrastructure.

1.3.4 IDS/IPS

If the firewall is considered the sheriff of the infrastructure, the intrusion detection system (IDS) and intrusion protection system (IPS) could be viewed as its informant and deputy. The IDS/IPS serves the function of monitoring the network for hostile activity in IDS mode, and stopping or preventing the hostile activity in IPS mode.

As a concession to the security department of GIAC Enterprises, senior management allowed the purchase of one Mcafee IntruShield 2600 IDS/IPS.[6] It

[5] Shinder, Thomas, ***ISA Server Security Checklist Part 1***. February 4, 2002. URL: http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist__Part_1_Securing_the_Operating_System_and_the_Interface.html# (March 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

being a purpose built appliance that protects against signature, anomaly and Denial of Service (DoS) attacks. The IntruShield 2600 sensor was chosen because of its ability to be put inline with minimal latency overhead and also because it can be transitioned from an IDS mode to IPS mode with minimal effort and no interference on the network. Six 10/100 Ethernet ports are used for inline connectivity between the firewall's 3 NICs and their corresponding networks. This also assures complete security of the firewall, minimizing the possibility that that the firewall will be compromised from a network based attack. In addition to the securing the firewall, the IntruShield 2600 will enhance the firewall's protection of the DMZ, internal networks and router components. The IntruShield Sensor is loaded with image 1.9.2.5 ED and signature set 1.9.6.4. The IntruShield Manager is located on the internal network and communicates through directly to the sensor's management interface facing the internal network. The IntruShield Manager is loaded with version 1.9.2.7 ED.

Physical security of this device is assured by placing the sensor and the management workstation in a locked room with all other security components in this infrastructure.

© SANS Institute 2004, Author retains full rights.

[6] ***Mcafee IntruShield Network IDS Sensor Data Sheet***. Network Associates Inc. 2004. URL: http://www.nai.com/us/_tier2/products/_media/sniffer/ds_intrushieldidssensor.pdf (April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3.5 VPN

Following the K.I.S.S. principal of design, the ISA Server doubles as the enterprise VPN for the limited pool of field staff and IT staff that may be using it. Based on historical data detailing VPN usage within the organization, concurrent connection to the VPN tend to hover around 15 during peak periods, minimizing the impact it has on the performance of the firewall. As with all purchasing, senior management has deferred the allocation of funds for a dedicated VPN unit until the time these connections become a burden to the firewall.

The VPN serves as method by which field sales, home-office workers and IT staff can connect to the internal network as if they were on-site. The primary concerns for the field sales and home-office workers were being able to access e-mail, internal file servers and use the *FortuneDealer* client software that cannot be used from the Internet. The IT staff main issue was being able to connect to all the servers on the DMZ, the management servers on the internal network and as an internal client in order to manage the firewall and router.

The VPN client is built into all of our Windows XP workstation laptops and a Certificate-Based PPTP EAP-TLS Authentication[7] method has been established for better security when using PPTP. PPTP was selected over L2TP so that users would not have any issues when connecting from a location where the IP address of their laptops was NAT'ed such as from home offices with firewall router appliances. An internal installation of Microsoft Enterprise CA on a Windows 2003 server was used to create the certificates that are to be installed on the VPN client devices.

1.3.6 Other Security Components

Defense in depth is the objective of this design. Key enterprise components have several steps to their security as evidenced by the Border Router ACL's, the firewall and the NIDS/NIPS devices. In order to further secure the most critical outward facing components of GIAC Enterprises, we have taken steps to further secure the outward facing webservers.

Mcafee Entercept is a host-based IDS/IPS program that uses signatures and behavior analysis to prevent the exploitation of known and unknown vulnerabilities in Microsoft Windows based servers. It does so by intercepting calls made to applications at the kernel level and comparing these calls to what is considered normal or accepted behavior based on the purpose of the device.[8]

Mcafee Entercept 4.0 Webserver Edition has been installed on EXT-WEBSRV-1, our main internet presence server. EXT-WEBSRV-2, our *FortuneDealer*

---

[7] Shinder, Thomas. ***Configuring the VPN Client and Server to Support Certificate-Based PPTP EAP-TLS Authentication - Part 1***. ISAserver.org [Online], June 22, 2003. URL: http://www.isaserver.org/tutorials/pptpeaptlspart1.html (April 2004).

[8] ***Mcafee Entercept Web Server Edition Data Sheet***. Network Associates Inc. 2004. URL: http://www.nai.com/us/_tier2/products/_media/mcafee/ds_entercept_webserver.pdf (Feb 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

webserver, has been loaded with Mcafee Entercept 4.0 Webserver and Database edition. Security is further enhanced with this version by being honed for web-based database exploitation attacks.

1.3.7 Network Addressing Scheme

Routable addresses have been assigned by the ISP to GIAC Enterprises' external interfaces. These addresses are located in the 199.200.81.16/28 subnet and are listed below. Non routable, RFC 1918[9] compliant addresses have been assigned to all DMZ and Internal resources. These addresses fall in the 192.168.0.0/24 subnet for the DMZ and 192.168.1.0/24 subnet for internal resources. The network addressing scheme is as follows:

EXTERNAL/DMZ	**Host**	**Public IP**	**Private IP via NAT**	**Firewall Interface**
Outfacing from Router	EXT-RT-1	199.200.80.32/28	None	Serial Interface
In-facing from Router	EXT-RT-1	199.200.81.17/28	None	Firewall External Interface
Firewall External	EXT-FW-1	199.200.81.18/28	None	Firewall External Interface
Firewall DMZ	EXT-FW-1	None	192.168.0.1/24	Firewall DMZ Interface
DNS 1 External	EXT-DNS-1	199.200.81.19/28	192.168.0.2/24	Firewall DMZ Interface
Webserver 1 External	EXT-WEBSRV-1	199.200.81.20/28	192.168.0.3/24	Firewall DMZ Interface
Webserver 2 External	EXT-WEBSRV-2	199.200.81.21/28	192.168.0.4/24	Firewall DMZ Interface
Mail Server 1 External	EXT-SMTP-1	199.200.81.22/28	192.168.0.5/24	Firewall DMZ Interface
FTP Server 1 External	EXT-FTP-1	199.200.81.23/28	192.168.0.6/24	Firewall DMZ Interface
INTERNAL	**Host**		**Private IP**	**Firewall Interface**
Internal DNS 1	INT-DNS-1		192.168.1.2/24	Firewall Internal Interface
Internal IDS 1 Management Interface	INT-IDS-1		192.168.1.3/24	Firewall Internal Interface
Internal DB Server 1	INT-DBSRV-1		192.168.1.4/24	Firewall Internal Interface
Internal Mail Server 1	INT-SMTP-1		192.168.1.5/24	Firewall Internal Interface
IntruShield Management Server	INT-MGMT-1		192.168.1.6/24	Firewall Internal Interface
Entercept Management Server	INT-MGMT-2		192.168.1.7/24	Firewall Internal Interface
Firewall and Router Management Server	INT-MGMT-3		192.168.1.8/24	Firewall Internal Interface
Certificate Authority	INT-CA-1		192.168.1.9/24	Firewall Internal Interface

[9] Rekhter, Y et al. ***RFC 1918 Address Allocation for Private Internets***. Internet RFC/STD/FYI/BCP Archives. February 1996. URL: http://www.faqs.org/rfcs/rfc1918.html (Nov 2003).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Addresses Reserved for IT	IT Workstations		192.168.1.20 – 192.168.1.34	Firewall Internal Interface
Addresses Reserved for VPN Users	VPN Internal Addresses		192.168.1.35 – 192.168.1.79	Firewall Internal Interface
Addresses Reserved for Other Internal Resources	Other Internal Resources (Servers, Clients)		192.168.1.80 – 192.168.1.254	Firewall Internal Interface

2 Security Policies

2.1 Border Router

The security policy and configuration have been developed using guidelines presented in the "Router Security Configuration Guide" by the NSA.[10]

2.1.1 Border Router Policy and Configuration

The underlying objective in the security policy for the router is to keep the router isolated and secure, both physically and logically, permit limited access to it for management, and configure it so that it filters all unwanted inbound and outbound traffic, thus lessening the firewall's burden.

To achieve physical isolation and security, the router has been placed in a locked network component closet located in a locked room with restricted access. Power to router is supplied via a UPS also located in said closet.

Logical isolation was performed at the Cisco IOS level by following the steps to harden the device:

1. Enabling a secure password, enable secret during initial configuration.
2. ***no cdp run*** command was added to the configuration to disable the Cisco Discovery Protocol since this is being run as an external resource.
3. ***no service udp-small-servers*** and ***no service tcp-small-servers*** lines were added to disable these unnecessary services.
4. ***finger*** and ***http server*** services were not part of this IOS, so there was no need to disable these services.
5. Loading of the IOS over the network using bootp was disabled with the ***no ip bootp server*** and ***no boot network*** commands.
6. By adding the command ***no ip source-route*** to the configuration, we disable the ability of packets to direct their own route.
7. ***no ip proxy-arp*** command on the Ethernet interface is used to disable sending arps across multiple interfaces. This service is not needed in this environment.
8. Since NTP is not used in this environment, the command ***ntp disable*** is used to disable this service on the Ethernet interface.

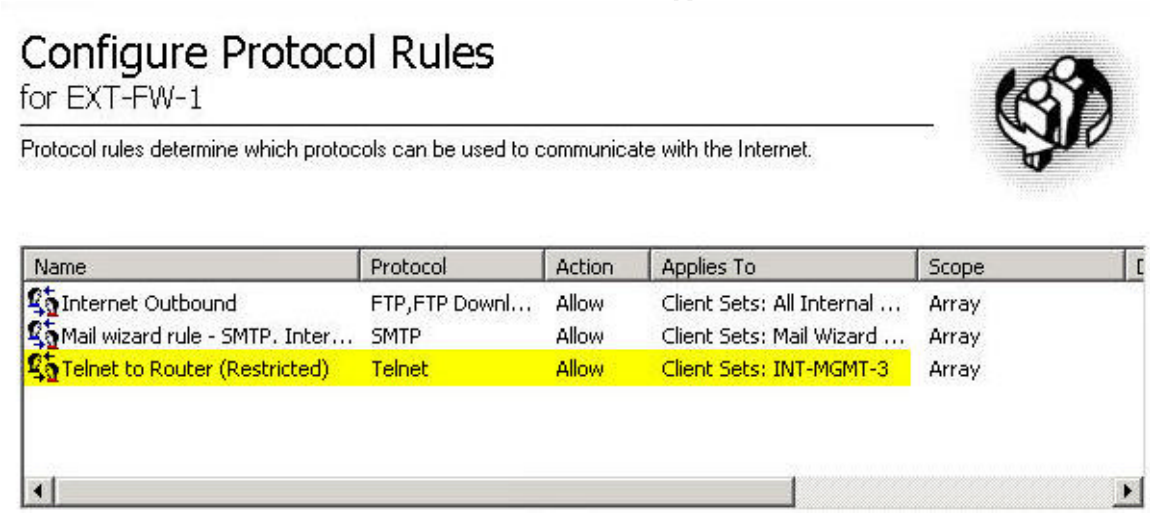
[10] National Security Agency, ***Router Security Configuration Guide*****.** NSA [online], 2002. URL: http://www.nsa.gov/snac/cisco/guides/cis-2.pdf. (Feb 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

9. SNMP is disabled since we are not using it in this environment. This is achieved using the following command: ***no snmp-server***
10. The unused serial interface was disabled using the ***shutdown*** command.

Further logical security is achieved by using the Mcafee IntruShield IDS/IPS sensor in an inline configuration between the firewall and the router. The current signature set has the ability to identify and prevent all known Cisco router, network based attacks. However, in the case of this design, the sensor is limited to monitoring attacks originating solely from the Ethernet Interface side.

Management of this device is restricted to the physical device via a terminal connection or via telnet through the firewall. In the case of the physical connection, the administrator must first gain physical access to the room and then physical access to the network component closet – both of which are restricted. Telnet access is possible only by one logging on to INT-MGMT-3 and performing a telnet from this device. Internal network to external network outbound telnet is restricted at the firewall to only this device.



This router itself prevents access to it via telnet with the following ACL entry which allows only the external interface of the firewall to access the router with telnet:

access-list 110 permit tcp host 199.200.81.18 any eq telnet log

To further improve the security of the environment, an extensive ACL list has been created and applied to the border router. Below is a summary of the key components of the ACL's applied to the router. The full configuration is contained within Appendix A.

Inbound Rules (Internet Side) Listed in order of appearance	**Purpose**
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log access-list 100 deny ip 172.16.0.0 0.15.255.255 any log access-list 100 deny ip 10.0.0.0 0.255.255.255 any log access-list 100 deny ip 127.0.0.0 0.255.255.255 any log	These rules prevent the transmission of packets that do not belong on the WAN. They are also important because they will prevent certain exploits

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access-list 100 deny ip 255.0.0.0 0.255.255.255 any log access-list 100 deny ip 224.0.0.0 7.255.255.255 any log access-list 100 deny ip 169.254.0.0 0.0.255.255 any log access-list 100 deny ip host 0.0.0.0 any log	
access-list 100 deny ip 199.200.81.16 0.0.0.240 any log	This rule prevents the transmission of packets with the LAN interface address from originating from the WAN side. Important because it prevents spoofing of internal router address
access-list 100 deny ip host 199.200.80.34 any log	This rules prevents attackers from using the IP address of the external router interface to gain access. It prevents spoofing of external router address
access-list 100 permit tcp any 199.200.81.16 0.0.0.240 established	A key component of some DoS attacks is the use of packets that have only the 'SYN' flag set. This rule Denies packets that have this characteristic
access-list 100 deny ip any host 199.200.81.16 log access-list 100 deny ip any host 199.200.81.31 log	Another type of DoS uses internal network and broadcast addresses for an exploit. This rule prevents this attack
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 199.200.81.16 0.0.0.240	Allows limited ICMP and this is done to inhibit related DoS attacks
access-list 100 deny udp any any range 33400 34400 log	Denies inbound tracert and this is done to prevent the discovery of internal addresses
access-list 100 permit tcp any host 199.200.81.19 eq 53 access-list 100 permit udp any host 199.200.81.19 eq 53	Allows access to EXT-DNS-1 only with DNS service. It limits the port that can be used with this server.
access-list 100 permit tcp any host 199.200.81.20 eq www access-list 100 permit tcp any host 199.200.81.21 eq www access-list 100 permit tcp any host 199.200.81.21 eq 443	Access to EXT-WEBSRV-1 and EXT-WEBSRV-2 limited to http and https These rules limit the ports that can be used with these server.
access-list 100 permit tcp any host 199.200.81.22 eq smtp	Access to EX-SMTP-1 limited to SMTP. It limits the port that can be used with this server.
access-list 100 permit tcp any host 199.200.81.23 eq ftp	Access to EX-FTP-1 limited to FTP. It limits the port that can be used with this server.
access-list 100 permit tcp any host 199.200.81.18 eq 1723 access-list 100 permit udp any host 199.200.81.18 eq 47 access-list 100 permit tcp any host 199.200.81.18 eq 47	Access to Firewall VPN gateway for VPN users using PPTP. These limit the ports that can directly address the firewall.
access-list 100 deny ip any any log	Deny everything else. Placed in the last spot to catch anything we may have not explicitly denied
Outbound Rules (Firewall Side) Listed in order of appearance	**Purpose**
access-list 110 permit tcp host 199.200.81.18 any eq telnet log	Telnet access to router from firewall
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log access-list 110 deny ip 172.16.0.0 0.15.255.255 any log access-list 110 deny ip 10.0.0.0 0.255.255.255 any log access-list 110 deny ip 127.0.0.0 0.255.255.255 any log access-list 110 deny ip 255.0.0.0 0.255.255.255 any log access-list 110 deny ip 224.0.0.0 7.255.255.255 any log access-list 110 deny ip 169.254.0.0 0.0.255.255 any log access-list 110 deny ip host 0.0.0.0 any log	These rules prevent the transmission of packets that do not belong on the WAN. They are also important because they will prevent certain exploits
access-list 110 permit ip 199.200.81.16 0.0.0.240 any	Allows only packets from internal network to this interface.
access-list 110 permit icmp any any echo access-list 110 permit icmp any any parameter-problem access-list 110 permit icmp any any packet-too-big access-list 110 permit icmp any any source-quench access-list 110 deny icmp any any log	Permits outbound ping.
access-list 110 deny ip host 199.200.81.17 host 199.200.81.17 log	Prevents spoofing internal interface
access-list 110 deny tcp any any range 1 19 log access-list 110 deny tcp any any eq 43 log access-list 110 deny tcp any any eq 93 log access-list 110 deny tcp any any range 135 139 log access-list 110 deny tcp any any eq 445 log access-list 110 deny tcp any any range 512 518 log access-list 110 deny tcp any any eq 540 log	Prevents other unwanted port activity such as whois, dcp, uucp, windows networking, UNIX lan activity
access-list 110 deny ip any any log	Deny everything else. Placed in the last spot to catch anything we may have not explicitly denied

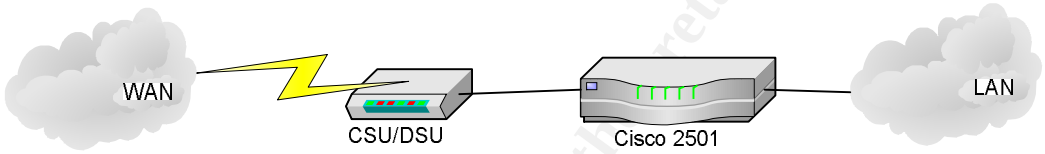
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.1.2 Border Router Tutorial

Adding a Border Router to an Infrastructure

A router is placed in an environment when there are at least two distinct networks that need to communicate with each other. In the case of GIAC Enterprises, we are discussing the placement of a Cisco 2501 Router that can connect 2 T1 connections between a WAN and a LAN environment.

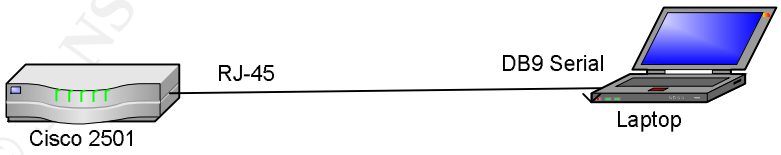
When up-linking a LAN environment to WAN, a service provider (i.e. AT&T, MCI, Sprint) must provide a channel by which data is communicated to their backbone. This is accomplished by providing physical connection and a piece of equipment to the customer's environment called a Channel Service Unit/Data Service Unit (CSU/DSU). This CSU/DSU translates the data from a connection such as a T1 or T3, down to a format that is understood by a router. The CSU/DSU is connected to the router via a V.35 serial cable.



On the LAN side of the router, the connection is limited to a physical CAT-5 cable that transmits Ethernet to the firewall.

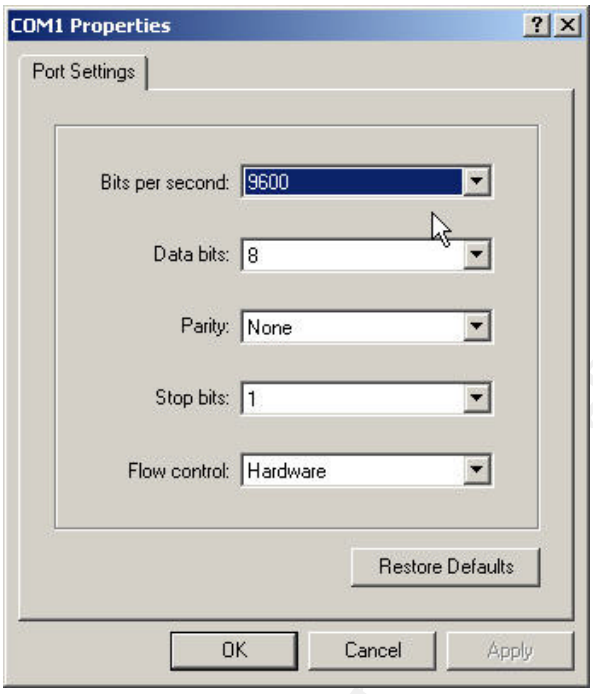
The following configuration procedures were performed using a Microsoft Windows 2000 Professional workstation. To configure the router perform the following steps:

1. With the Cisco provided DB9 to RJ-45 connector, connect the DB9 plug to the serial interface of the workstation and plug the RJ-45 connection in to the port labeled "console" on the back of the router.



2. Using HyperTerminal, configure a session to initiate communication from the workstation to router's terminal interface. Select communications for COM1 and configure as follows (9600, 8, none, 1, Hardware):

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



3. Power on the router and you will see data scrolling on the screen that details the router's build information. Wait until you see the following prompt and then press return to select the default:

```
Would you like to enter the initial configuration dialog? [yes]: yes
```

4. You will then be asked a series of questions which you should answer as shown below. Questions are highlighted in **blue** and responses are highlighted in **red**:

```
Configuring global parameters:

  Enter host name [Router]: EXT-RT-1

The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

  Enter enable secret: g00dpassword1

The enable password is used when there is no enable secret
and when using older software and some boot images.

  Enter enable password: g00dpassword2
  Enter virtual terminal password: g00dpassword3
  Configure SNMP Network Management? [yes]: no
  Configure IP? [yes]: yes
    Configure IGRP routing? [yes]: yes
      Your IGRP autonomous system number [1]: yes
  Configure bridging? [no]: no

Configuring interface parameters:

Configuring interface Ethernet0:
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  Is this interface in use? [yes]: yes
Configure IP on this interface? [yes]: yes
    IP address for this interface: 199.200.81.17
    Number of bits in subnet field [0]: 4
    Class C network is 199.200.81.0, 4 subnet bits; mask is /28

Configuring interface Serial0:
  Is this interface in use? [yes]: yes
  Configure IP on this interface? [yes]: yes
  Configure IP unnumbered on this interface? [no]: no
    IP address for this interface: 199.200.80.34
    Number of bits in subnet field [0]: 4
    Class C network is 199.200.80.0, 4 subnet bits; mask is /28

Configuring interface Serial1:
  Is this interface in use? [yes]: no
```

This query will end with a summary of your settings and this last question:

```
Use this configuration? [yes/no]: yes
```

The enable secret is the password that you will initially have to remember to configure the device. This password is encrypted in the configuration file and is the one that permits you to modify the configuration.

5. You will now be at the following prompt that indicates you are connected to router:

```
EXT-RT-1>
```

Take this time to understand the CLI by typing "**?**". This will display all the commands that are available to a minimum privileged user. The only one you are interested in using for the moment is the `enable` command. This will escalate your privileges to the level that will permit you to modify the configuration file.

TIP: You do not have to type out the entire command as long as you type in enough letters to distinguish this command from any other command. So typing `en` is sufficient to distinguish this command from `exit` and thus the command is executed as follows:

```
EXT-RT-1>en
Password:g00dpassword1
```

6. Having been escalated to the privileged user account, you will see more commands that will permit you to perform other configuration activities. Type "**?**" at the CLI to see the additional commands.

The router's configuration is stored in two locations: 1) Memory (which is cleared after powering down the router and 2) NVRAM which remains after power is recycled. When you want to see the current configuration, you would type the command `show running-config` (`sh run` for short). As follows:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
EXT-RT-1#sh run
Building configuration...

Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname EXT-RT-1
!
enable secret 5 $1$zL5E$cBzkX9oja54pzVkd2AP3f.
enable password g00dpassword2
!
!
!
interface Ethernet0
 ip address 199.200.81.17 255.255.255.240
!
interface Serial0
 ip address 199.200.80.34 255.255.255.240
!
interface Serial1
 no ip address
 shutdown
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
 password g00dpassword3
 login
!
end

EXT-RT-1#
```

If the router were to be rebooted, this configuration would be lost since it is stored in volatile memory. To prevent this, one must write the running configuration to what is referred to as the startup-configuration as follows:

```
EXT-RT-1#copy running-config startup-config
```

This command assures that the next time the router boots, it will boot with the most recent configuration. The abbreviated version of this command would look something like this: `cop run star`.

7. The full configuration of the router is listed in **Appendix B** of this document. The simple way of configuring the router to secure operational status, is to copy key components from the configuration to the terminal session. This is done as follows.

© SANS Institute 2004, Author retains full rights.

To enter configuration mode, one would type **configure** at the prompt and then select **terminal** as the configuration method. The short way of doing this would be to type **conf t**. This will enable a different prompt which indicates that the router is ready to receive commands for configuration. This prompt looks like this:

```
EXT-RT-1(config)#
```

8. Configuration parameters are generally applied to a particular interface or to the router as a whole. If one were to want to apply an ACL to the router, one would have to begin by creating the ACL list at the configuration prompt. ACL's have to be grouped initially by an access list number and subsequently, that access list number is applied to a particular interface.

```
EXT-RT-1(config)# access-list 110 permit tcp host 199.200.81.18 any eq telnet log
EXT-RT-1(config)# access-list 110 permit ip 199.200.81.0 0.0.0.240 any
```

The above access list contains two very simple controls. The first line permits the access of the router from a particular host using telnet, the second permits ip traffic from a particular subnet to any other location. If we break down the first line even further, one can begin to understand the structure of the command, which is as follows:

access-list	Defines the type of configuration parameter
110	Defines the unique ACL grouping. For our purposes, an ACL grouping number should be between 100-199. These numbers are reserved specifically for IP extended access lists.[11]
permit	Defines the action (deny or dynamic being the alternatives)
tcp	Defines the protocol (others include udp, ip, icmp, etc.)
host (followed by IP address)	This is the "source" field. "Host" indicates that the IP address belongs to a unique entity on the network
any	This is the "destination" field. "Any" indicates that it is applying the rule to any destination
eq	Matches the following parameter for the rule
telnet	Defines the protocol that needs to be matched
log	States that when this rule is matched, it should be logged.

TIP: If you reach a point during writing the ACL where you need to see what options you can enter, type "**?**" and a list of parameters will be shown. For example:

```
EXT-RT-1(config)#access-list 110 deny ?
  <0-255>  An IP protocol number
  eigrp    Cisco's EIGRP routing protocol
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  igrp     Cisco's IGRP routing protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
```

[11] CCNA Study Guide, pg 356.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  ospf      OSPF routing protocol
  tcp       Transmission Control Protocol
  udp       User Datagram Protocol

EXT-RT-1(config)#
```

9. Applying the ACL to an interface is simple. From the configuration prompt, the user would need to specify a particular interface to which ACL will be applied and then select which ACL is to be applied as follows:

```
EXT-RT-1(config)#interface ethernet0
EXT-RT-1(config-if)#ip access-group 110 in
```

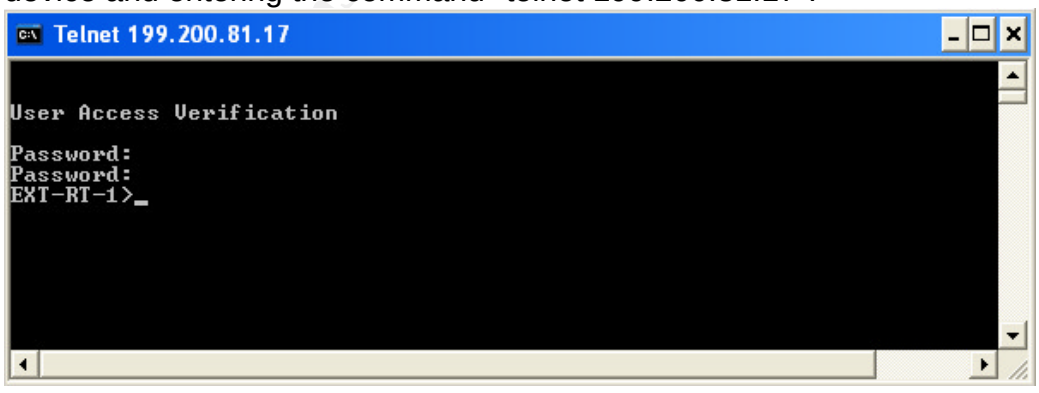
The first command above sets the terminal configuration mode so that it only manages the ethernet0 interface. The second command applies the access-list created in step 8, to this interface in the incoming direction. In other words, the router is to apply access list 110 to interface ethernet0 as packets reach the router on this interface.

To exit the configuration mode enter the following commands:

```
EXT-RT-1(config)#end
EXT-RT-1#copy running-config startup-config
```

As good practice, we have saved the configuration from volatile to non-volatile memory with the second command.

10. The router is now ready to configure from the device with the ip address of 199.200.81.18, which would be the firewall's external interface. So having already set rules on the firewall that only permit the outbound telnet from a particular workstation on the internal network, we can connect from this workstation to the router by opening up a command line window on the client device and entering the command "telnet 199.200.81.17".



The above password prompt appears and you need to enter the password that was created for terminal access (***g00dpassword3***). From the `EXT-RT-1>` prompt, you can enter all the same commands as if you were at the terminal, so an `enable` command is the next advised step.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SECURITY TIP: Using telnet over an Ethernet network is insecure because telnet transmits username and passwords in clear text that can be captured by protocol analyzers (a.k.a. Sniffers). The solution would be to setup an SSH encrypted connection to the router. This is likely a future solution for this environment when a newer router is purchased.

TIME SAVER TIP: By saving all your ACL's in a text file you can save time by cutting and pasting them directly to the `EXT-RT-1(config)#` prompt in bulk.

2.2 External Firewall Policy and Configuration

This installation of ISA Server is configured with the Local Address Tables listing the 192.168.0.0 and 192.168.1.0 networks. This means that these two networks are considered local to each other and are limited in their restrictions between each. In the architecture diagram, the DMZ labeled area, which is the 192.168.0.0, has direct communication with all the devices in the 192.168.1.0 network, so most rules created at the firewall are built with the intent of segregating these two internal networks from the external un-trusted network on the outward facing interface of the EXT-FW-1. With this in mind, only the rules that communicate between the external network and the two internal networks are discussed. It is assumed that communication between the two local networks mentioned above flow freely because the ISA Server behaves like a router between them. In this design, we have tried to isolate communications initiated between the un-trusted external networks and the GIAC servers exclusively to the 192.168.0.0 network.

In Microsoft ISA's Enterprise server, policy elements must be created to establish what are referred to *Destination Sets* and *Client Address Sets*.[12] These represent policy elements much like source and destination groups used in other types of firewalls. *Destination Sets* are most typically servers that other users wish to get to and have to go through the firewall to do so. Below are the *Destination Sets* and the *Client Address Sets* created on EXT-FW-1 (External Firewall):

[12] Shiner, Thomas and Shinder, Debra. ***Configuring ISA Server 2000.*** Rockland: Syngress Publishing, Inc. 2001. Pg 109.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Destination Sets

Name	Description	Destinations
EXT-DNS-1	GIAC External DNS Server Access	199.200.81.19, dns.GIAC.com
EXT-FTP-1	External FTP Server	199.200.81.23, ftp.GIAC.com
INT-IDS-1	Mcafee IntruShield IDS/IPS	192.168.1.10
EXT-SMTP-1	External SMTP mail server relay	199.200.81.22, mail.GIAC.com
EXT-WEBSRV-1	External Company Webserver for Web presence	199.200.81.20, www.GIAC.com
EXT-WEBSRV-2	Fortunedealer.GIAC.com	199.200.81.21, fortunedealer.GIAC.com
INT-DBSRV-1	Internal Database Server	192.168.1.4
INT-SMTP-1	Internal Mail Server	192.168.1.5
EXT-RT-1	Router's Ethernet Interface	199.200.81.17, ext-rt-1.GIAC.com
Entercept DMZ Agents	HIPS Agents on EXT-WBSRV-1 and 2	192.168.0.3 - 192.168.0.4
INT-MGMT-2	Internal Entercept Management Server	192.168.1.7

Client Address Sets

Name	Description	Clients
All Internal Addresses	192.168.1.0	192.168.1.2 - 192.168.1.254
All Internal Management Servers	INT-DNS-1, INT-DBSRV-1, INT-SMTP-1, INT-MGMT-1, INT-MGMT-2, INT-MGMT-3	192.168.1.2,192.168.1.4 - 192.168.1.8
INT-CA-1	Internal Certificate Authority	192.168.1.9
INT-DBSRV-1	Internal FortuneDealer Database Server	192.168.1.4
INT-DNS-1	Internal DNS Server	192.168.1.2
INT-MGMT-1	Management Workstation for Intrushield IDS/IPS	192.168.1.6
INT-MGMT-2	Management Workstation for Entercept Agents	192.168.1.7
INT-MGMT-3	Management Workstation for Firewall and Router	192.168.1.8
INT-SMTP-1	Internal Mail Server	192.168.1.5
IT Admins	IT Admins	192.168.1.20 - 192.168.1.34
Mail Wizard set: 192.168.0.5	EXT-SMTP-1 DMZ Mail Server	192.168.0.5
Other Internal Resources	Internal Clients and Servers	192.168.1.80 - 192.168.1.254
VPN Users	Addresses reserved for VPN Users	192.168.1.35 - 192.168.1.79
DMZ Entercept Agents	External Webservers 1 and 2 with Entercept Agents	192.168.0.3 - 192.168.0.4

Note: Not all listed Destination and Client Address sets will be used in the configuration. Identifying these entities now will simplify future rule implementations.

The most important task is to give the Internet secure access to our DMZ for the appropriate functions. In order to do this in ISA, servers must be "published" to the Internet. By publishing certain parts of a server to the Internet, one assures that the firewall controls access to these servers on specific ports and using specific protocols that are properly monitored by ISA's protocol filters. In addition to this access control, the servers are accessed via SecureNAT, a Microsoft term that assures improved privacy of the servers, putting them in an RFC 1918 non-routable subnet and then assigning them routable addresses via the firewall's external interface. Below is a summary of the published servers via the firewall:

Published Web Servers

Order	Name	Description	Action	Applies to	Destination
1	EXT-WEBSRV-1	Publishes Main Webserver to outside as www.GIAC.com	Route to specified site	Any request	EXT-WEBSRV-1
2	EXT-WEBSRV-2	Publishes Fortunedealer.GIAC.com to Internet	Route to specified site	Any request	EXT-WEBSRV-2
Last	Default rule	Deny	Deny	Any Request	All destinations

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The default ports that are opened for these servers are 80, 443 and 21. These servers will not respond on 21, and the router ACL's prevent the 21 port from being accessed on these servers from the Internet.

Published DMZ Servers

Name	Description	Protocol	Internal IP	External IP	Applies to
EXT-DNS-1	Allows DNS Query to DMZ	DNS Query Server	192.168.0.2	199.200.81.19	Any request
EXT-FTP-1	Allows FTP service to DMZ	FTP Server	192.168.0.6	199.200.81.23	Any request
Mail wizard rule - SMTP Server Published	IP: 199.200.81.22	SMTP Server	192.168.0.5	199.200.81.22	Any request

By publishing the above servers to the internet, the following access requirements are fulfilled:

Requirements Fulfilled by Above Rules

Who	From	To	Protocol	Port
Customer, Supplier, Partner	Internet	DMZ	HTTP, HTTPS, SMTP	80, 443, 25
Customer, Supplier, Partner, Mobile Employees	Internet	DMZ	DNS	53
Supplier	Internet	DMZ	FTP	21

In ISA Server, *Protocol Rules* work in conjunction with *Site and Content Rules* to establish the security policy. While *Protocol rules* define which protocols a client can use to access another network through the ISA Server, *Site and Content Rules* explicitly permit or deny access to particular sites. These rules are not enforced in a particular order according Microsoft, however, a rule that denies an action will always supersede a permit rule if there is ever a conflict, and by default, it is not explicitly permitted, then it is denied. This is not the most intuitive approach; however, it does offer additional configurability over traditional firewall rules in other types of firewalls.

The following *Protocol Rules* and *Site and Content Rules* are created to fulfill access requirements for the internal users to access external http, https and ftp, as well as for granting access to the management station to telnet to the router. The key rules are highlighted in yellow.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Site and Content Rules

Name	Description	Action	Applies To	Destination	Content
Internet Outbound	Allows Internal Clients to Internet/DMZ FTP, HTTP, HTTPS	Allow	Client Sets: All Internal Addresses	All destinations	All
INT-DBSRV-1 to EXT-WEBSRV-2	Allows FortuneDealer MS-SQL Communications	Allow	Client Sets: INT-DBSRV-1	EXT-WEBSRV-2	All
EXT-WEBSRV-2 to INT-DBSRV-1	FortuneDealer MS-SQL Query	Allow	Client Sets: EXT-WEBSRV-2	INT-DBSRV-1	All
IN-MGMT-3 to EXT-RT-1	Allows Telnet for Router Management	Allow	Client Sets: INT-MGMT-3	EXT-RT-1	All
EXT-SMTP-1 to INT-SMTP-1	Allows e-mail delivery internal	Allow	Client Sets: INT-SMTP-1	INT-SMTP-1	All
Entercept DMZ Agents	Access to Entercept HIPS Agents from Management Server	Allow	Client Sets: INT-MGMT-2	Entercept DMZ Agents	All
Entercept Reporting to INT-MGMT-2	Entercept Agents Reporting to INT-MGMT-2	Allow	DMZ Entercept Agents	INT-MGMT-2	All

Protocol Rules

Name	Description	Protocol	Action	Applies to
FortuneDealer MS-SQL	Communications between EXT-WEBSRV-2 and INT-DBSRV-1	Microsoft SQL Server	Allow	Client Sets: EXT-WEBSRV-2,INT-DBSRV-1
Internet Outbound	All internal users access to the internet with the following protocols	FTP,FTP Download only,HTTP,HTTPS	Allow	Client Sets: All Internal Addresses
Mail wizard rule - SMTP. Internal IP: 192.168.0.5	This rule associated with publishing of Mail server using the SMTP Wizard	SMTP	Allow	Client Sets: EXT-SMTP-1
Telnet to Router (Restricted)	Allows Telnet for Router Management	Telnet	Allow	Client Sets: INT-MGMT-3
Entercept Communications	Allows communications between Entercept Agents and Server	Entercept:5005 Inbound, Entercept 5005 Outbound	Allow	Client Sets: Entercept DMZ Agents, INT-MGMT-2

Packet Filtering enables the administrator to control the flow of traffic from an un-trusted network to the trusted network. When *Packet Filtering* is enabled on an ISA Server as it is in this environment, all incoming packets are dropped unless there is a specific rule that permits them, thus taking the approach of denying everything and permitting only exceptions to this rule. By enabling *Packet Filtering*, all ports are disabled on the external interface of the firewall. "Only ports that you explicitly open through a static packet filter, through a publishing rule, or dynamically will be available."[13]

By entering a packet filter rule in the *Packet Filtering* page, one is creating a static filter that will always apply. A more secure method is creating a dynamic packet filter as is done when one creates a rule in the *Protocol Rules* page. These rules open the ports for access as needed.[14]

[13] Shiner, Thomas and Shinder, Debra. ***Configuring ISA Server 2000.*** Rockland: Syngress Publishing, Inc. 2001. pg 559.

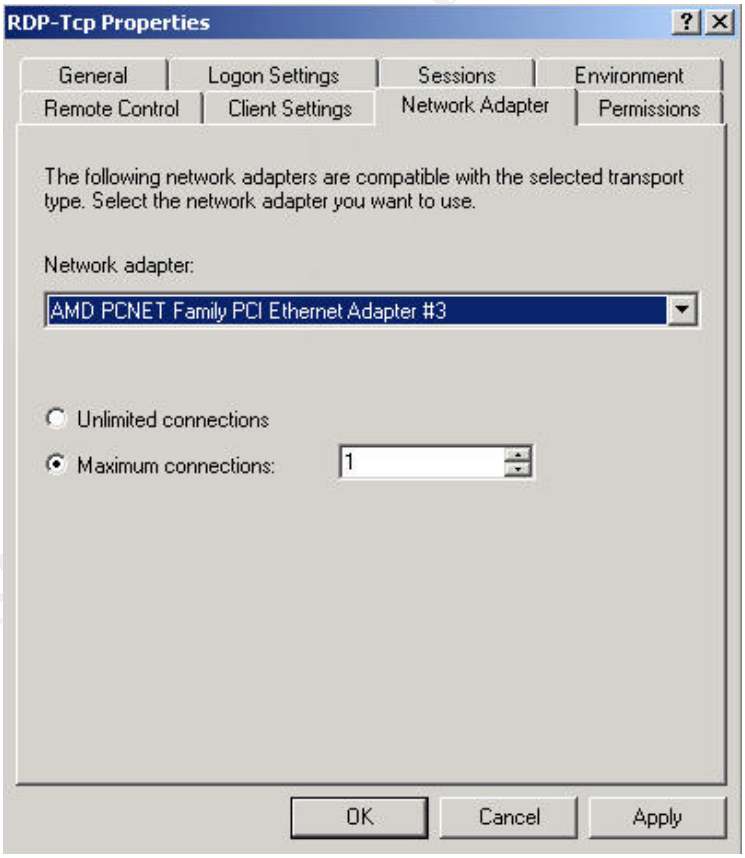
[14] Ibid, pg 560.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following filters are used for facilitating analysis more than for security purposes. More filters are listed in the VPN Policy and Configuration section of this document.

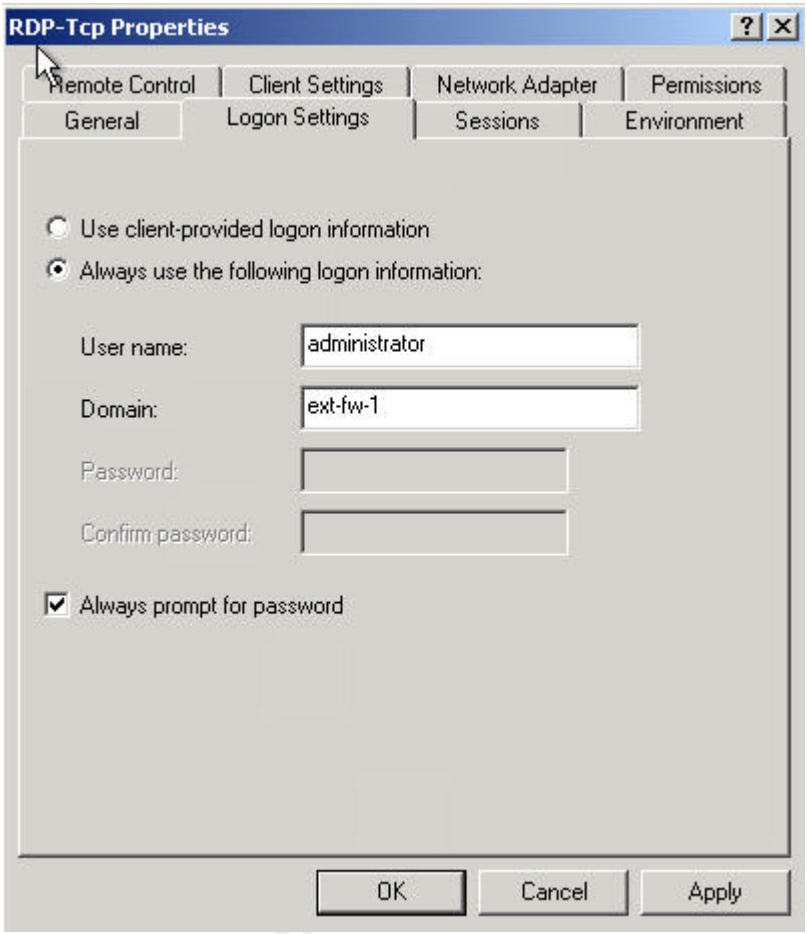
Name	Mode	Filter type	Protocol	Direction	Local Computer	Remote Computer
DNS filter	Allow	DNS Lookup	UDP	Both	Default External IP	Any
ICMP outbound	Allow	ICMP All Outbound	ICMP	Outbound	Default External IP	Any
ICMP ping response (in)	Allow	ICMP Ping Response	ICMP	Inbound	Default External IP	Any
ICMP source quench	Allow	ICMP Source Quench	ICMP	Inbound	Default External IP	Any
ICMP timeout in	Allow	ICMP Timeout	ICMP	Inbound	Default External IP	Any
ICMP unreachable	Allow	ICMP Unreachable	ICMP	Inbound	Default External IP	Any

Administration of the firewall will take place via Terminal Services. The Terminal Services Manager connection has been configured to limit connections to the firewall through the internal interface only.



To further enhance the management of the firewall, authentication has been limited to the administrator log on account. If the user attempting to log onto the terminal service is not using the administrator account, the connection will be rejected.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



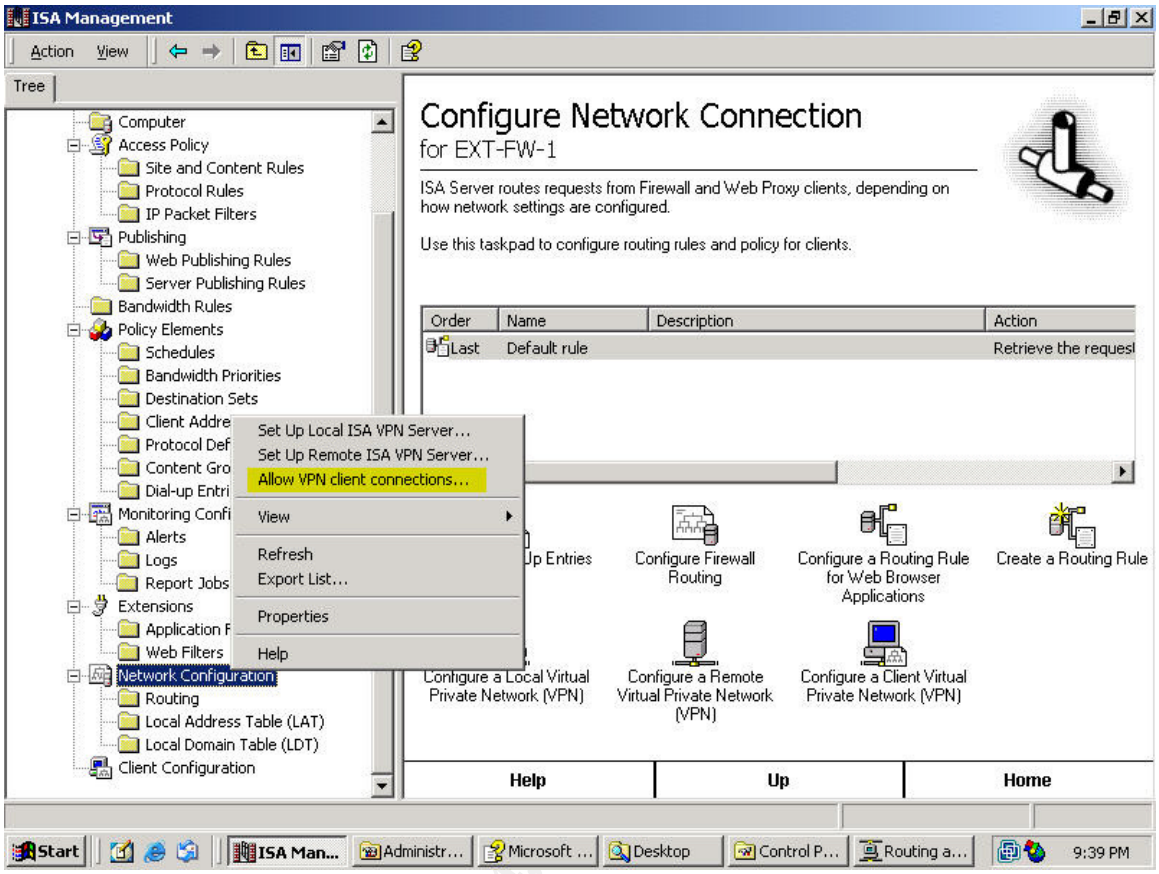
2.3 VPN Policy and Configuration

PPTP with EAP-TLS authentication using 128-bit MPPE encryption was selected as the method for creating a VPN connection because of the ease with which it could be implemented and for the ability of the client to traverse a router with out breaking IPSec. L2TP, although more secure, is not sufficiently flexible as a protocol for our mobile workforce that may be attempting to access the VPN gateway from behind another firewall. The ISA Server's ability to easily integrate with a Radius server for certificate based authentication made selecting VPN clients on our Microsoft Windows XP-based mobile platform a natural choice.

The implementation procedure was borrowed from an article posted by Thomas Shinder at http://www.isaserver.org/.[15]
The first part of setting up the VPN entailed enabling the *Remote ISA VPN Server* on the exterior interface of our EXT-FW-1 and then selecting the *Allow VPN client connections* option as follows:

[15] Shinder, Thomas, **Configuring the VPN Client and Server to Support Certificate-Based PPTP EAP-TLS Authentication - Part 1**. ISAserver.org [Online], June 22, 2003. Available at: http://www.isaserver.org/tutorials/Configuring_the_VPN_Client_and_Server_to_Support_Certificate-Based_PPTP_EAP-TLS_Authentication_-_Part_1.html# (cited April 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



By doing so, Routing and Remote Access Service (RRAS) was started, and the following filter rules were added to permit the establishment of the connection to the external interface of the firewall:

Name	Mode	Filter type	Protocol	Direction	Local Computer	Remote Computer
Allow PPTP protocol packets (client)	Allow	PPTP Call	47	Both	Default External IP	Any
Allow PPTP protocol packets (server)	Allow	PPTP Receive	47	Both	Default External IP	Any

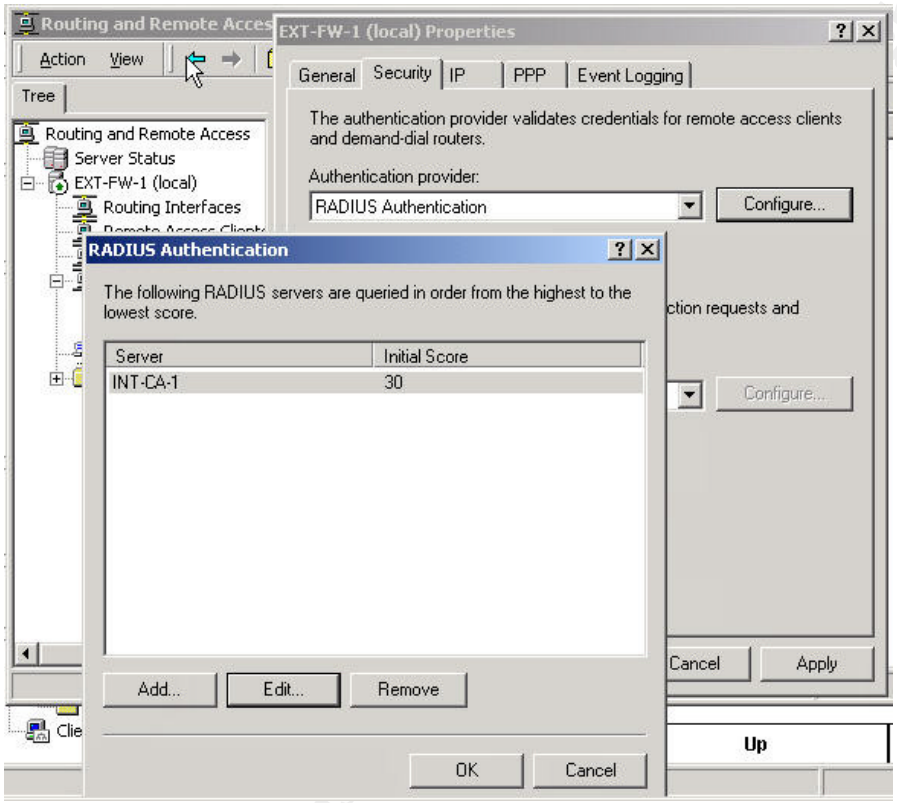
INT-CA-1 is an internal Windows 2003 server running Enterprise CA and configured as an Internet Authentication Server (IAS). The IAS service is integrated with Active Directory and leverages Microsoft's Active Directory model that is used inside GIAC Enterprises for user authentication. Each user that is granted permissions to be a mobile user, is issued a digital certificate from INT-CA-1, and has that certificate associated with their Active Directory user name.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The IAS Access Policy for remote users is as follows:

Access Method	Grant Access Permissions	Mode	Authentication	Encryption	EAP Method
VPN Access	By user	Allow	EAP/TLS	128-bit MPPE	Smartcard or other certificate

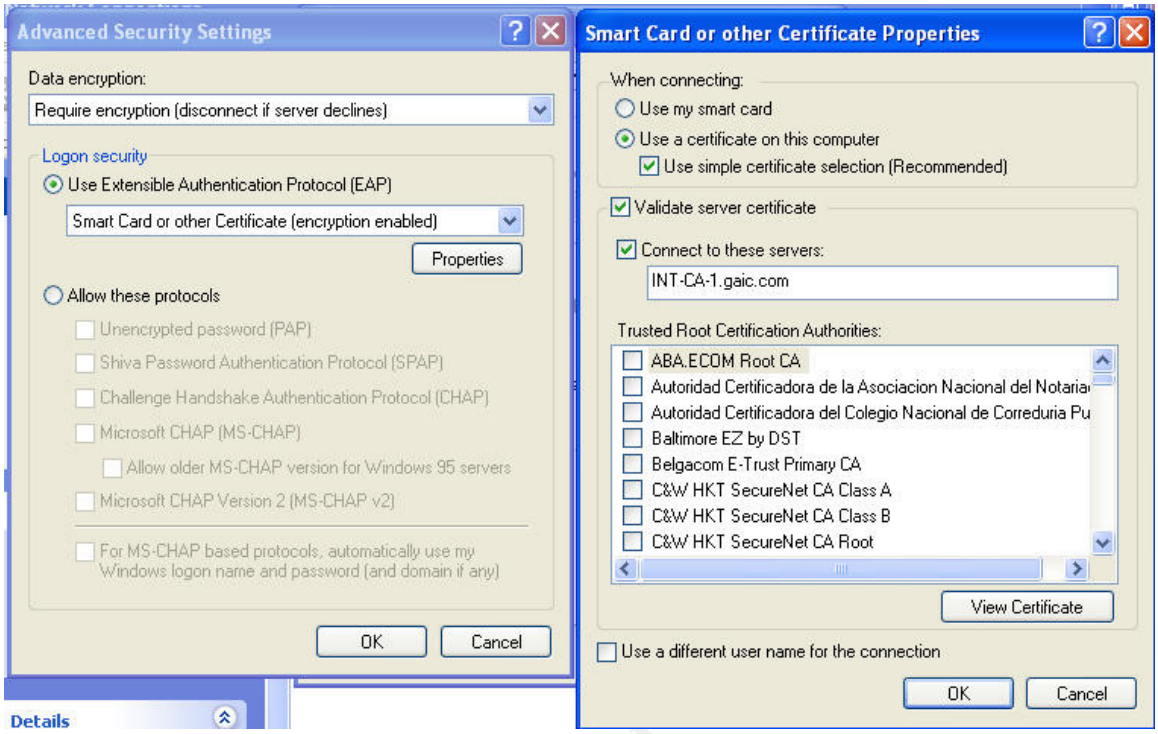
EXT-FW-1 is configured through the Routing and Remote Access (RRA) management interface to pass Radius authentication requests off to INT-CA-1. The following image shows the configuration for RRA.



The RRA is also configured to receive inbound VPN connections on the firewall's primary external interface 199.200.81.18.

The certificates are loaded directly to the Microsoft XP VPN client which is configured to communicate directly with the EXT-FW-1's external interface mentioned above. When the connection is established, the client presents this digital certificate to the RRAS service, which in turn attempts to establish the validity and read the connection policy for this user. Each client is unique from the perspective of the IAS, however, all the clients are configured as follows:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Future considerations for this environment's VPN should include investing in a stand-alone VPN gateway for the purpose of offloading VPN gateway responsibility from the main firewall and also for moving away from PPTP which has a limited lifespan. An ideal solution would be an IPSec based solution integrated with token and/or certificate authentication, but the IT department must do with what is provided and make the most secure solution available for the GIAC Enterprises infrastructure.

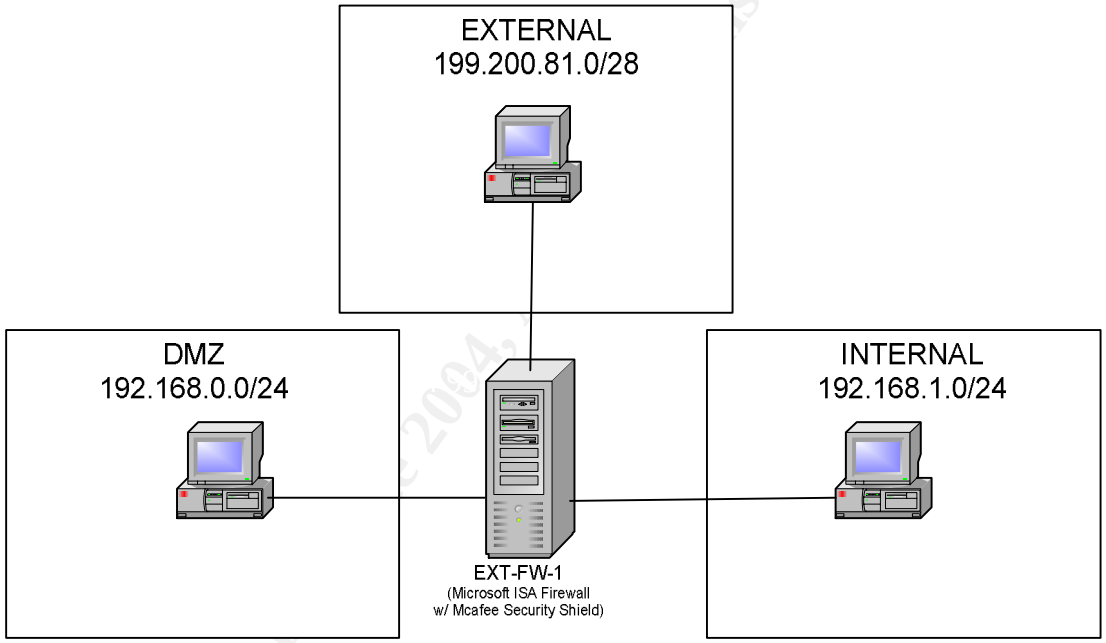
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.1 Verify the Firewall Policy

Validation of the firewall policy involves understanding the policy in place. Identifying how these policies can be tested, assigning resources to the effort and performing the evaluation.

3.1.1 Technical Approach

For validating the configuration of the firewall, client devices will be placed in networks of each of the three interfaces that the firewall serves. These client devices will have varying configurations depending on the policy which is being tested. Changes will include modifying their IP addresses and emulating services such as SMTP, HTTP and FTP.



3.1.2 Calculating Costs & Risk Considerations

To accomplish this task it will require approximately 56 man hours by mid-level security engineers, employees of GIAC Enterprise that will perform this task during off hours in order to minimize the impact on transactions. These 56 hours are assigned 8 to one engineer over a period of 1 day to develop the test plan, 16 each to two engineers over a period of two days for testing and 8 each to two engineers over a period of 1 day to write the results. The days selected for the execution of the testing task are over a weekend as follows and total costs are included herein:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Day	Engineers Used	Hourly Rate per Engineer	Begin time	End Time	Hours Used/Day	Total Cost Per Day	Total Cost Aggregate
1	1	$50	Thu 9:00 AM	Thu 5:00 PM	8	$400	$400
2	2	$75 (rate x 1.5 for overtime)	Fri 10:00 PM	Sat 6:00 AM	16	$1200	$2000
3	2	$75 (rate x 1.5 for overtime)	Sat 10:00 PM	Sun 6:00 AM	16	$1200	$3200
4	2	$50	Tue 9:00 AM	Tue 5:00 PM	16	$800	$4000

The total labor cost for this effort will be $4000.00.

Risk considerations taken into account include the possibility that the firewall server may fail during this testing. Additional time between the scheduled completion of this effort and beginning of the next work week totals 26 hours. This time can be used to recover the server in case of failure. Test devices have been allocated from GIAC Enterprises' internal pool of workstations and all testing tools and licenses are owned by the company.

3.2 Firewall Validation Execution

3.2.1 Tools used in Validation

The following tools will be used to execute the test plan:

3 Workstations, each loaded with:

- Microsoft Windows XP
- ArGoSoft FTP Server 1.01,
- Apache 2.0.49 Web Server
- WorkGroupMail SMTP server 7.5.1 Enterprise Edition

The external test workstation located on the 199.200.81.0 subnet will have the following programs in addition:

- GFI LANguard Network Security Scanner 5

3.2.2 Firewall Validation Step-by-Step

Here are some example test scenarios that should be performed by the analysis team. A thorough firewall validation will include more than just the tests listed below.

© SANS Institute 2004, Author retains full rights.

Sample Test Case 1 – Scanning Firewall External Interface

Scanning with GFILANGaurd NSS 5.0. This scanner will scan for open UDP and TCP ports, DNS, FTP, SMTP and RPC vulnerabilities. [16] Any responses are logged for follow-up analysis. The following external IP addresses were scanned: 199.200.81.18-199.200.81.23. All scans concluded with the following message:

```
==========================================================================
STARTING SECURITY SCAN FOR MACHINE/RANGE: 199.200.81.18-199.200.81.23
Profile: Default
==========================================================================
Validating targets...
    Building computers list...
    Resolving hosts...
    Check if a valid range of addresses was specified...
    Netbios discovery...
    SNMP discovery...
        Community string: public
    ICMP sweep ... (PING!)
    Resolving host names...
No computers found.
==========================================================================
COMPLETED SECURITY SCAN FOR MACHINE/RANGE: 199.200.81.18-199.200.81.23
Scan Start Time: 11:04:41 AM
Scan Duration: 5 seconds
==========================================================================
```

This would indicate the filters are working on the firewall to prevent inbound scanning. The firewall's log confirms this assessment, and read as follows during this scan:

2004-04-15	15:06:48	199.200.81.24	199.200.81.18	Udp	1207	137	BLOCKED 199.200.81.18
2004-04-15	15:06:48	199.200.81.24	199.200.81.19	Udp	1207	137	BLOCKED 199.200.81.18
2004-04-15	15:06:49	199.200.81.24	199.200.81.20	Udp	1207	137	BLOCKED 199.200.81.18
2004-04-15	15:06:49	199.200.81.24	199.200.81.21	Udp	1207	137	BLOCKED 199.200.81.18
2004-04-15	15:06:49	199.200.81.24	199.200.81.22	Udp	1207	137	BLOCKED 199.200.81.18
2004-04-15	15:06:49	199.200.81.24	199.200.81.23	Udp	1207	137	BLOCKED 199.200.81.18
2004-04-15	15:06:50	199.200.81.24	199.200.81.18	Udp	1208	161	BLOCKED 199.200.81.18
2004-04-15	15:06:50	199.200.81.24	199.200.81.19	Udp	1208	161	BLOCKED 199.200.81.18
2004-04-15	15:06:50	199.200.81.24	199.200.81.20	Udp	1208	161	BLOCKED 199.200.81.18
2004-04-15	15:06:50	199.200.81.24	199.200.81.21	Udp	1208	161	BLOCKED 199.200.81.18
2004-04-15	15:06:50	199.200.81.24	199.200.81.22	Udp	1208	161	BLOCKED 199.200.81.18
2004-04-15	15:06:50	199.200.81.24	199.200.81.23	Udp	1208	161	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.18	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.18	ICMP	17	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.18	ICMP	13	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.18	ICMP	15	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.18	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.18	Udp	1209	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.19	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.19	ICMP	17	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.19	ICMP	13	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.19	ICMP	15	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.19	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.19	Udp	1209	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.20	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.20	ICMP	17	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.20	ICMP	13	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.20	ICMP	15	0	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.20	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:51	199.200.81.24	199.200.81.20	Udp	1209	0	BLOCKED 199.200.81.18
2004-04-15	15:06:52	199.200.81.24	199.200.81.21	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15	15:06:52	199.200.81.24	199.200.81.21	ICMP	17	0	BLOCKED 199.200.81.18
2004-04-15	15:06:52	199.200.81.24	199.200.81.21	ICMP	13	0	BLOCKED 199.200.81.18
2004-04-15	15:06:52	199.200.81.24	199.200.81.21	ICMP	15	0	BLOCKED 199.200.81.18
2004-04-15	15:06:52	199.200.81.24	199.200.81.21	ICMP	8	19	BLOCKED 199.200.81.18

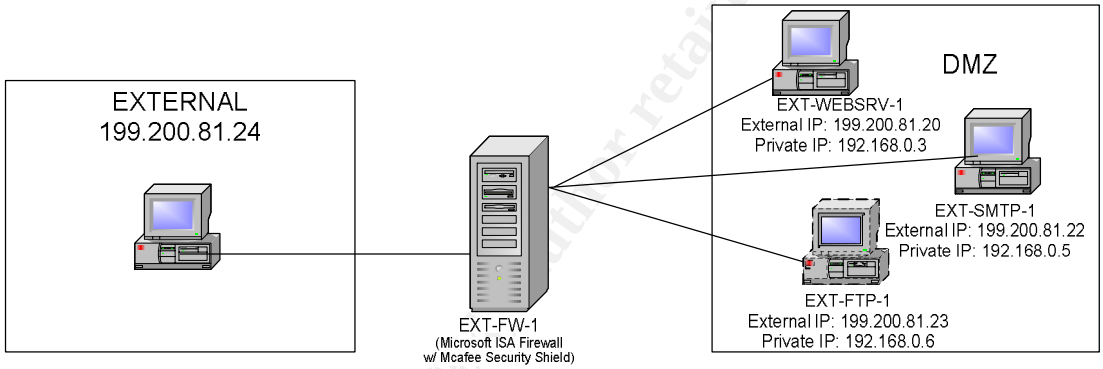
[16] ***GFI NSS***. April 2004. GFI Online. URL: http://www.gfi.com/downloads/mirrors.asp?pid=8&vid=100&lid=1 (April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2004-04-15 15:06:52	199.200.81.24	199.200.81.21	Udp	1209	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.22	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.22	ICMP	17	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.22	ICMP	13	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.22	ICMP	15	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.22	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.22	Udp	1209	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.23	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.23	ICMP	17	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.23	ICMP	13	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.23	ICMP	15	0	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.23	ICMP	8	19	BLOCKED 199.200.81.18
2004-04-15 15:06:52	199.200.81.24	199.200.81.23	Udp	1209	0	BLOCKED 199.200.81.18

Sample Test Case 2 – Accessing Services through the Firewall

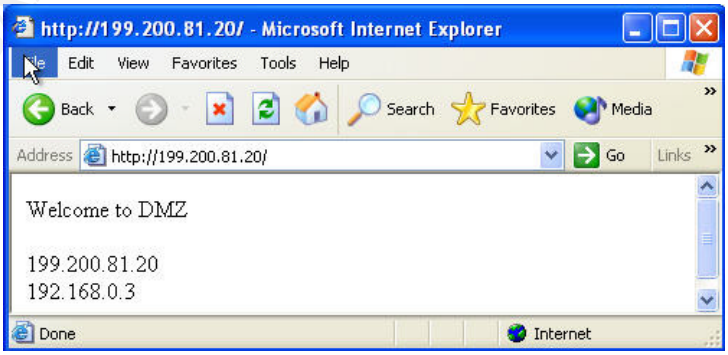
This test entails accessing FTP, HTTP and SMTP services through the firewall by configuring the DMZ workstation to emulate several different servers in the DMZ environment. These services will be accessed via the External Interface of the firewall from the device configured with the IP address 199.200.81.24.



For validating the following published server rule:

Order	Name	Description	Action	Applies to	Destination
1	EXT-WEBSRV-1	Publishes Main Webserver to outside as www.GIAC.com	Route to specified site	Any request	EXT-WEBSRV-1

A browser window is opened on the external client and is pointed to the address http://199.200.81.20. The following window is displayed indicating a successful connection:



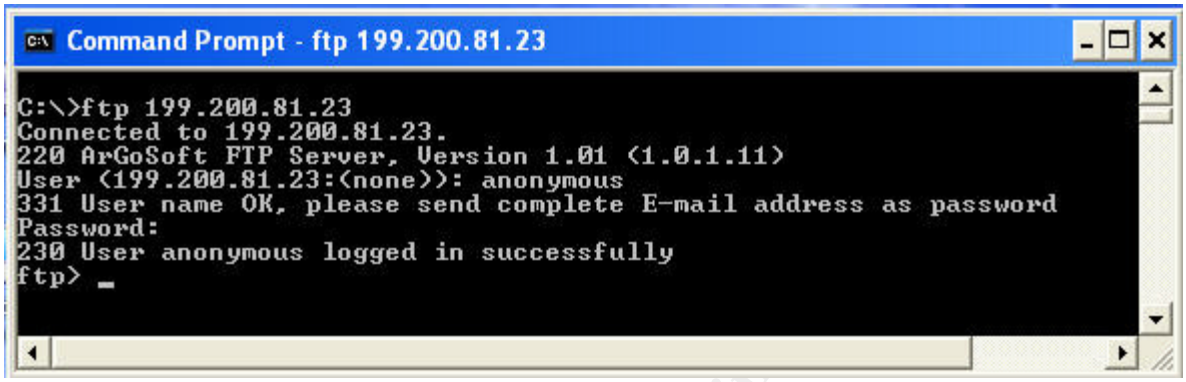
For validating the following published server rule:

Name	Description	Protocol	Internal IP	External IP	Applies to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

EXT-FTP-1	Allows FTP service to DMZ	FTP Server	192.168.0.6	199.200.81.23	Any request

A command line window is opened on the external client machine and the following ftp command is issued: ftp 199.200.81.23 . The following window is displayed indicating a successful connection:



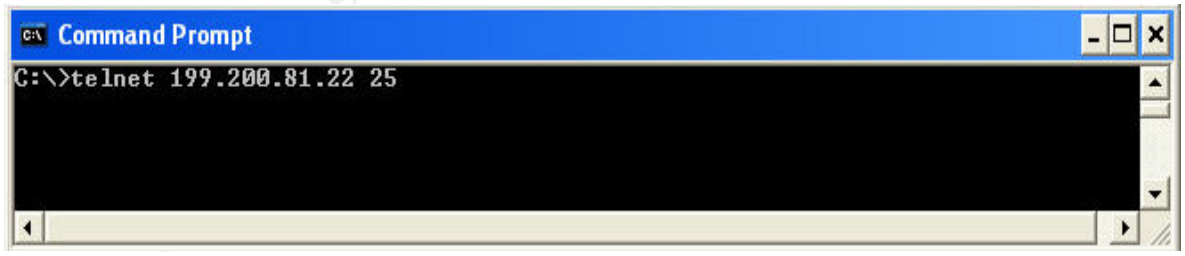
The firewall log records the establishment of this connection with the following entry:

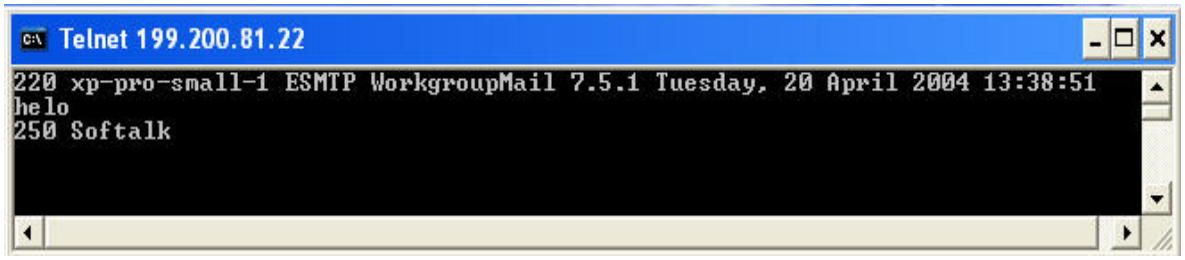
192.168.0.6 2004-04-15 17:24:29 EXT-FW-1 199.200.81.241478 310141 21 TCP Accept 20000 2 1

For validating the following published server rule:

Name	Description	Protocol	Internal IP	External IP	Applies to
Mail wizard rule - SMTP Server Published	IP: 199.200.81.22	SMTP Server	192.168.0.5	199.200.81.22	Any request

A connection is initiated via telnet to port 25 of the external mail server's IP address to simulate an SMTP connection to the WorkGroupMail SMTP server.





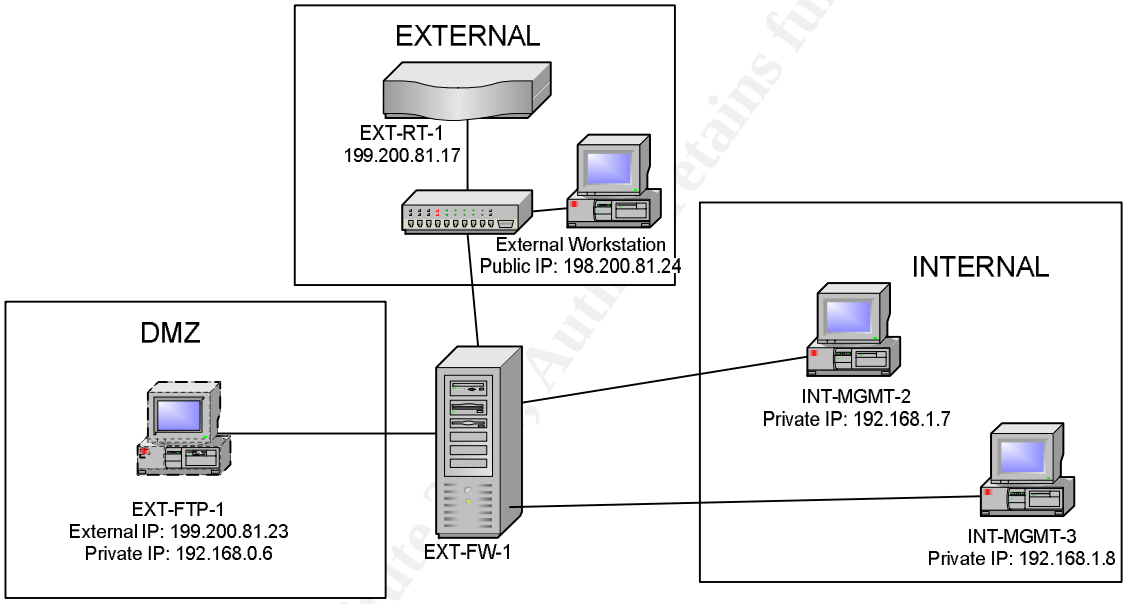
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The server SMTP server responds with a connection banner as shown above and the user types in “helo” to verify server interaction. This rule is verified the firewall places the following entry in the connection log:

```
192.168.0.5  2004-04-15 17:38:26 EXT-FW-1 199.200.81.24 1481 25  TCP Accept 0  3  3
```

Sample Test Case 3 – Accessing the Router from the Internal Network

In this test case scenario, router accessibility and restrictions are tested by attempting to connect to the router via Telnet from four different workstations. One located on the External network, one on the DMZ and two located on the Internal network as follows:

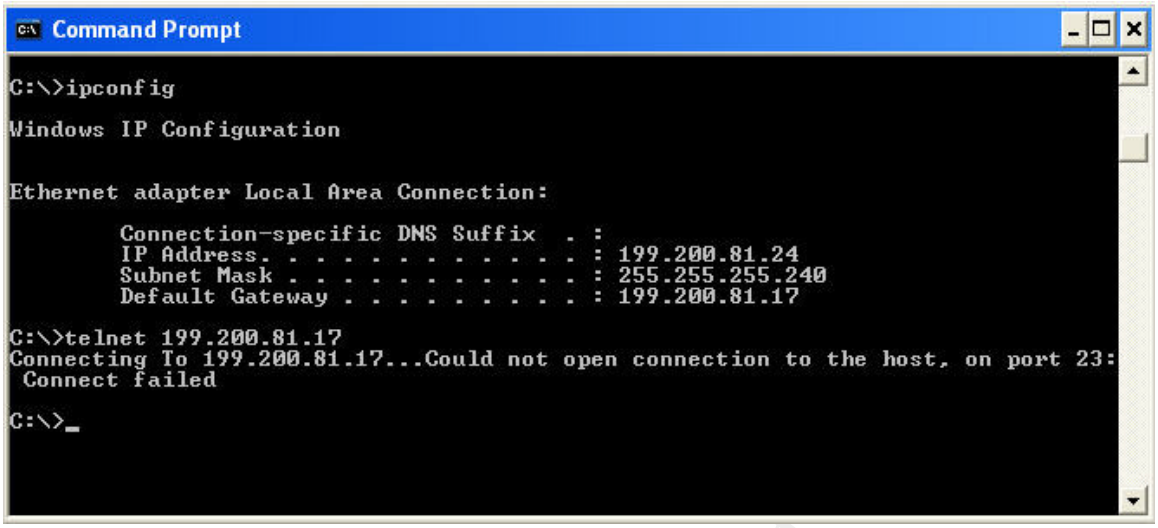


This test is attempting to validate the following firewall rule that permits access to the Router’s internal interface by enforcing a restriction on outbound Telnet to only the device called INT-MGMT-3:

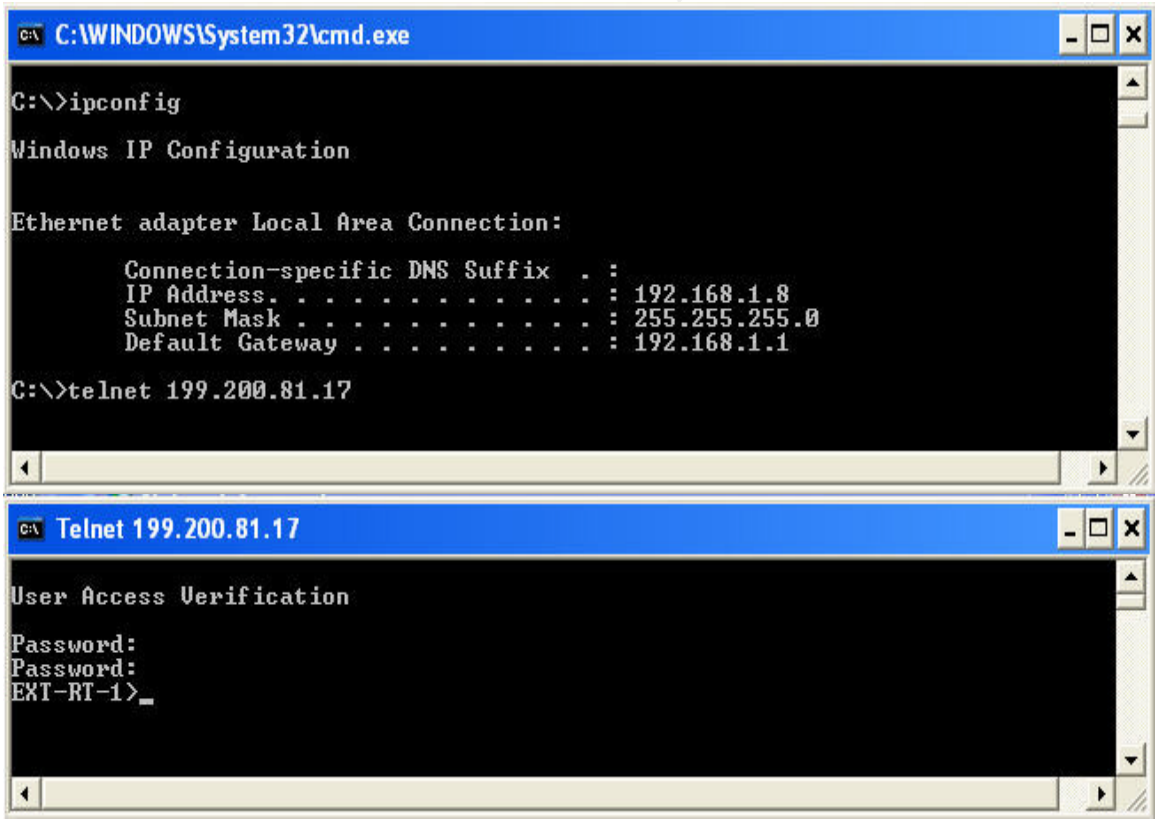
Name	Description	Protocol	Action	Applies to
Telnet to Router (Restricted)	Allows Telnet for Router Management	Telnet	Allow	Client Sets: INT-MGMT-3

The first connection attempted is from the External workstation (199.200.81.24) to the router. This connection by-passes firewall rules all together, but is unsuccessful because of the ACL’s implemented on the router. The attempt is recorded as follows:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



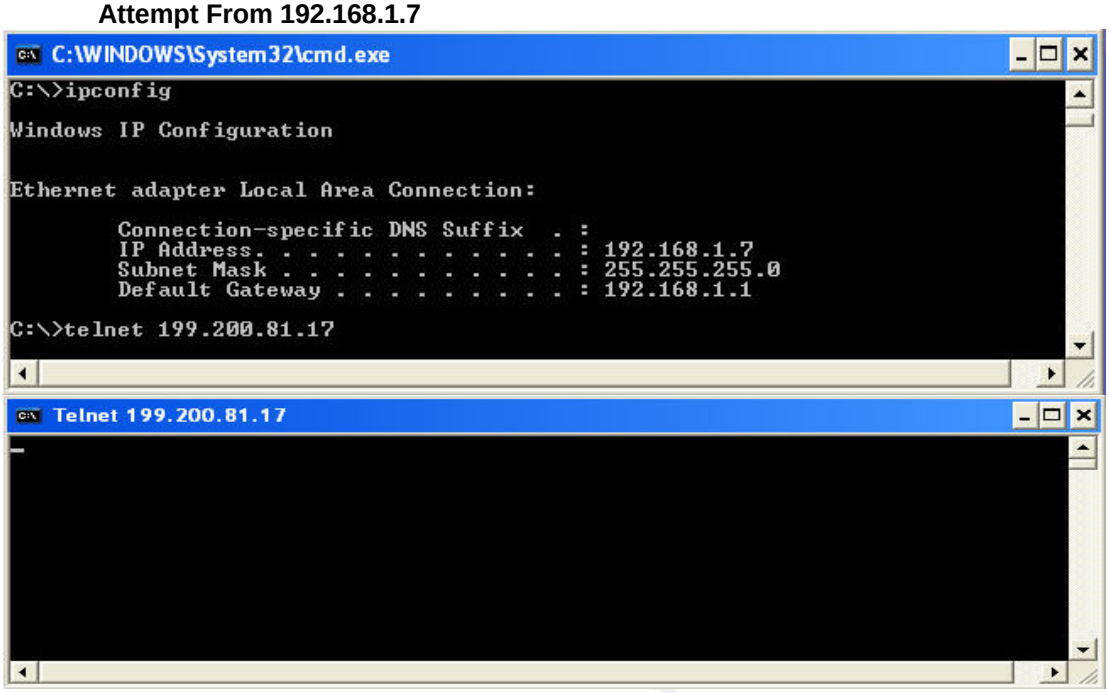
The second attempt at a Telnet connection is made by the only authorized workstation to do so, INT-MGMT-3 (192.168.1.8). This connection is successful and is shown as follows:



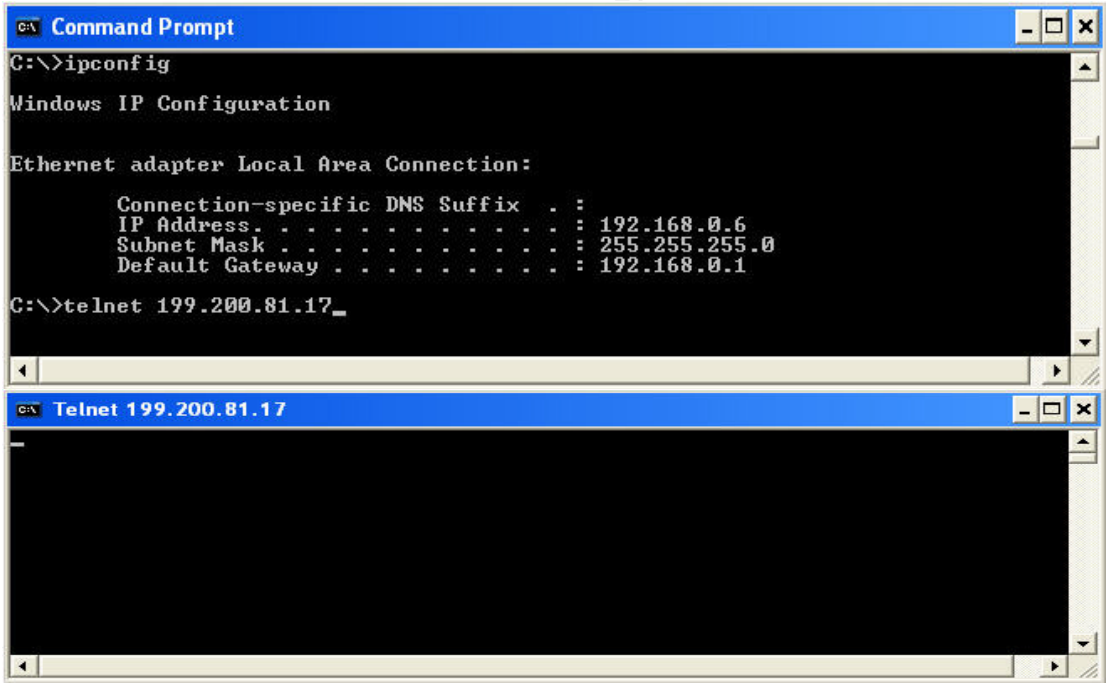
The third connection is attempted by INT-MGMT-2 (192.168.1.7), which is not authorized to use telnet outbound according to the firewall's policy. This connection attempt hangs and subsequently disconnects. The same result is recorded for the attempt made from EXT-FTP-1 (192.168.0.6). Here are the captured attempts:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Attempt From 192.168.1.7



Attempt From 192.168.0.6



3.3 Firewall Analysis & Recommendations

The objective of the firewall is to segregate un-trusted traffic from trusted traffic. This firewall implementation does so. This, however, would not be the best approach for securing an internet based company that serves fortune cookie sayings to the public. There are many factors that have influenced the evolution of this secure infrastructure implementation for GIAC Enterprises. These factors

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

include budgetary constraints and directives from upper management to maintain a Microsoft based infrastructure.

Setting these limiting factors aside there are several key areas that could be use improvement for creating a true secure e-business environment for GIAC Enterprises. These are:

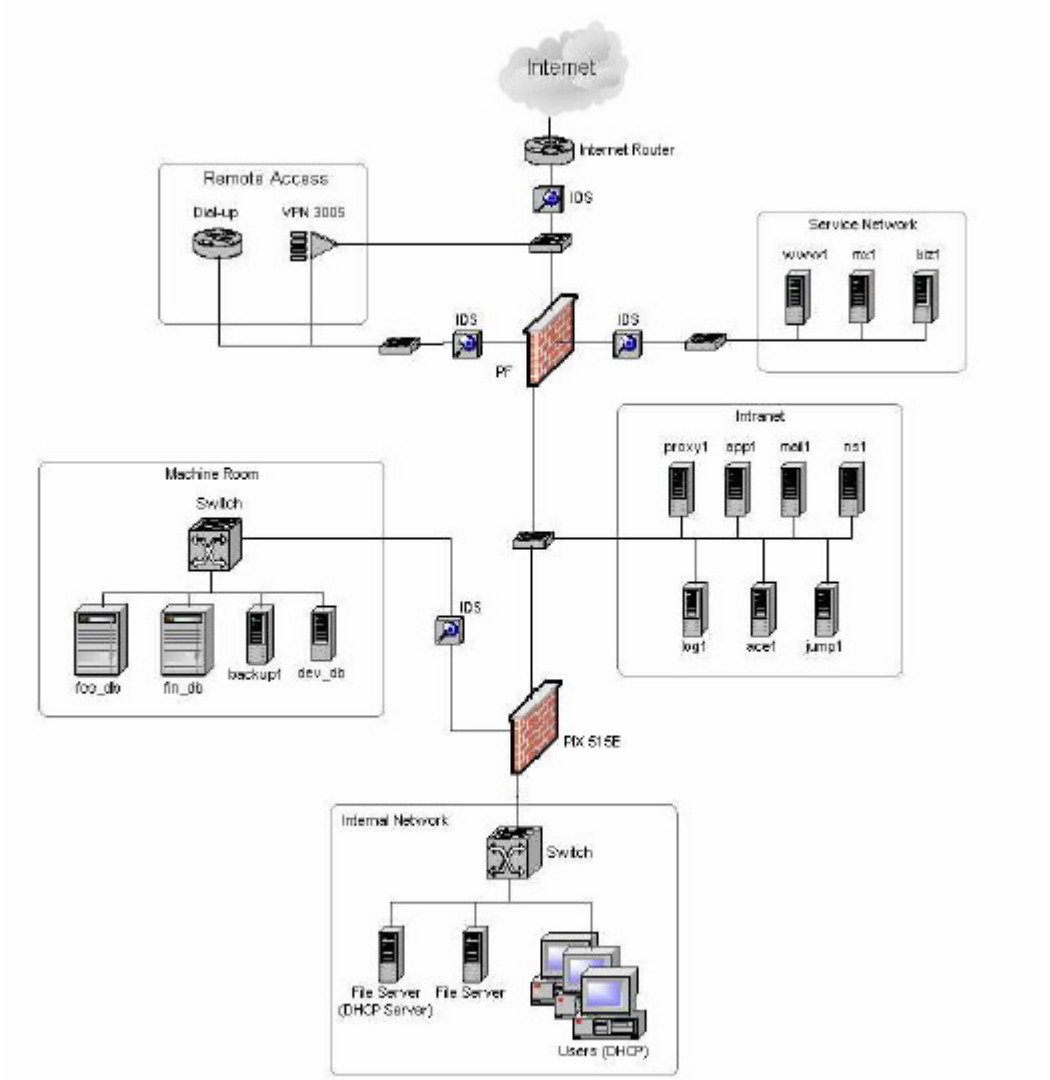
1. Invest in 2 new border routers to replace the legacy 2501 router that has limited functionality. By having two routers in place, the single point of failure can be minimized at this level. By having newer routers, security vulnerabilities that are present with the 2501 IOS can be minimized.
2. Invest in 2 appliance based firewalls tuned for large volume throughput for the purpose of maintaining traffic flowing to and from our customers, partners and suppliers. Redundancy with this gateway firewall is a key to uptime. This current design requires that all communications with the Internet cease if a patch or an update is performed to the single ISA firewall. This is a key single point of failure and that would be difficult to explain to investors when we are knocked offline for several hours due to a "glitch" in the firewall. This type of firewall is probably better suited for protection of key internal resources compared to enterprise serving of data.
3. Separate the VPN gateway from the firewall in order to offload the processing of connections from the firewall and on to a dedicated device. This would be another step towards maintaining the high availability of the key resources such as webservers, mail servers and the like.
4. If the plan is to grow the company, a more robust internal infrastructure needs to be developed. Active Directory is already being used, but its functionality is greatly being wasted on this flat network design. By segregating key resources and putting those on separate networks with routers in between, more control can be gained over these resources by defining clear ACL's at each transition point in the network in order to keep data secure and data flow at its highest efficiency. Having a shared collision domain for the entire internal network is inefficient.

In an ideal environment, the company would have sufficient money to create this secure infrastructure discussed, but in reality, the "bottom line" speaks more that sound practice. Knowing that one should sacrifice a little money now in order to not sacrifice a lot more when your systems finally get compromised is a difficult decision to make, but it is one that should be encouraged by every security professional in this industry as well as those working for GIAC Enterprises. Unfortunately, GIAC Enterprises has chosen to wait for the investment and continue growing a little at a time versus investing a large amount now.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.1 Design Under Fire

I've selected Michael Hotaling's design for this exercise. Michael used an OpenBSD Packet Filter 3.3 as his firewall.[17]



18

4.1.1 Design Weakness Discussion

The firewall that he selected is a solid performer that gets an "Excellent" rating for it's capabilities by eWeek online.[19] Merits to an open source approach to firewall security include cheapness and configurability. Problems may arise if a firewall is not maintained as improvements or weaknesses arise, or if the firewall

[17] Hotaling, Miichael ***SANS GIAC Certified Firewall Analyst Practical Assignment Version 2.0, GIAC Firewall Implemetation***. GIAC [online], 2003. URL: http://www.giac.org/practical/GCFW/Michael_Hotaling_GCFW.pdf (April 2004).
[18] Ibid.
[19] Dyck, Timothy. ***OpenBSD Gets Harder to Crack***. Eweek online.June 2003. URL: http://www.eweek.com/article2/0,3959,1111894,00.asp 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

administrator leaves the company and the knowledge of how this firewall has been customized for the environment leaves with him or her.

While researching this firewall, I came across Bugtraq vulnerability 9362[20] which describes an issue which allows spoofing of the firewall's other interface(s) address(es) through the use of a malformed packet when stateful-inspection is turned on, thus bypassing packet filtering rules on the device. In other words, if there are two interfaces that have the same stateful inspection policy bound to them, PF will match the access rule to all packets regardless of the interface they come in on, just as long as these packets have the same source, destination and protocol and port number information.[21] This is a very serious vulnerability by all accounts. For this attack to be successful, an attacker must have knowledge of commonly bound stateful inspection rules.

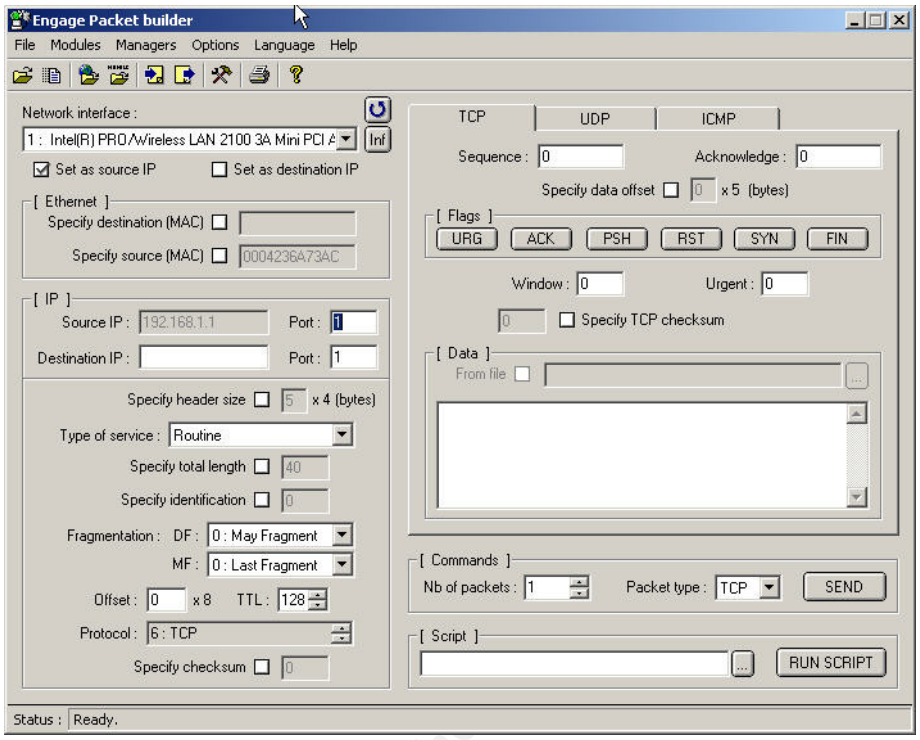
4.1.2 Design the Attack & Discussion of Potential Results

Using a document on spoofing techniques obtained at Online Documentation Server[22], I have chosen to exploit this vulnerability by causing a Denial of Service (Dos) attack on GIAC Enterprises' database server by claiming to be a resource from the DMZ interface. The attack would entail generating packets claiming to be from the DMZ interface of the OpenBSD PF using a freeware product called Packet Builder by Engage Security[23]. Packet Builder will enable the design of custom packets matching the exact format of packets coming from the DMZ's webserver and entering the database area of the design. By sending sufficient packets of data, I can in essence initiate a non existent conversation between the GIAC's main webserver and the database server internally, thus making both servers either partially or fully unavailable to access from the outside. Exploiting this for obtaining confidential information is slightly more difficult because one needs to understand more details about the actual communications between servers internally. This attack is more of a "flying blind" effort that can succeed by knowing the NAT'ed address of the Webserver, the internal address of the database server and the port numbers with which they communicate. This attack would be invisible to monitor because it is bypassing rules, thus not triggering an alert.

[20] ***OpenBSD PF State Tracking Spoofed Packet Vulnerability*.** Security Focus Online. Jan 2004. URL: http://www.securityfocus.com/bid/9362/info/ April 2004.
[21] Reed, Darron***. [Full-Disclosure] firewall security bug?*** Jan 2004. URL: http://archives.neohapsis.com/archives/fulldisclosure/2004-01/0059.html April 2004.
[22] ***Spoofing Attacks. Online*** Doucmentation Server. http://www.ods.com.ua/win/eng/security/Max_Security/ch28/ch28.phtml. April 2004
[23] **Engage Security Online**. April 2004. URL: http://www.engagesecurity.com/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Packet Builder Interface



4.1.3 Preventing this Attack

The simplest solution to this type of attack would be to avoid bounding stateful packet inspection rules to more than a single interface at a time. Create separate rules for each interface even if they seem redundant and then bind these rules individually. Additionally, an administrator could enter an ACL on the router preventing packets of data containing invalid IP addresses based on the direction that they are flowing through the router.

4.2.1 Attack Design for DoS on Cable/DSL

Despite vast media coverage of blended threat attacks, those attacks that use multiple methods of propagation to exploit vulnerabilities in various systems, there is a great number of personal DSL or Cable modem users that remain vulnerable to exploitation because they have either not updated their systems, don't have virus protection, don't have personal firewalls or all three. I have chosen to design this attack around propagating an internet worm through known Microsoft RPC vulnerabilities such as those detailed in MS03-026[24].

[24] ***Microsoft Security Bulletin MS03-026***. Microsoft Online. Sept 10, 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx (April 2004)

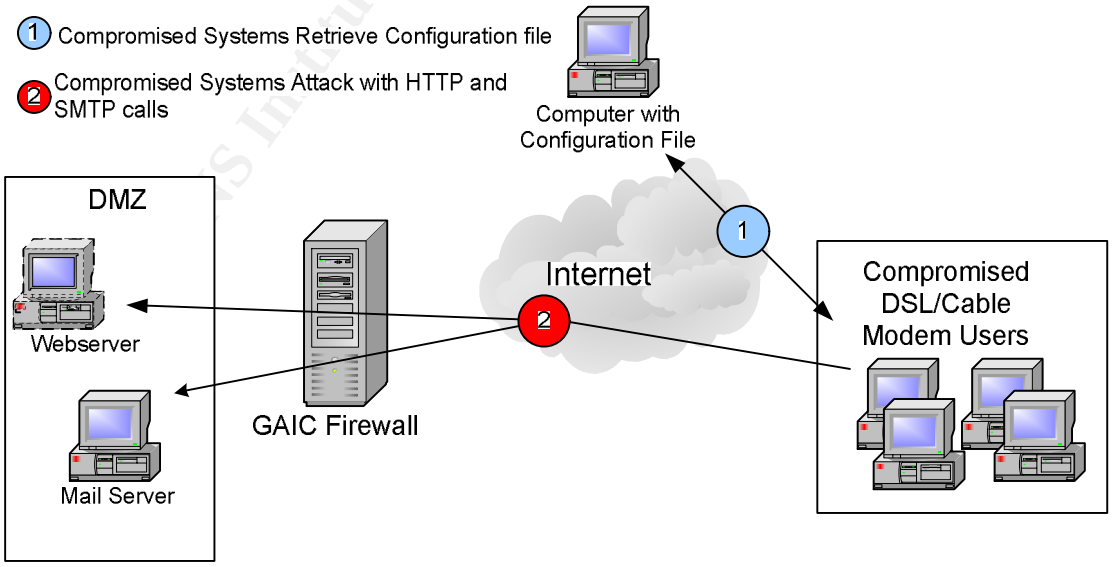
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The first step would be to design a program that will do four things:

1. Scan a specified IP address for a configuration file
2. Scan randomly generated IP addresses within a given range for port 135[25] being open. This would indicate that a particular system is likely vulnerable to attack
3. Be able to copy itself to a computer that has port 135 open
4. Using the configuration file, it could perform a DoS attack on a specified range of addresses through HTTP and SMTP

To complete the attack, I would identify networks pertaining to DSL or Cable Modem users for a particular ISP. Once these networks are identified, I would configure the aforementioned program to start scanning these ranges and finding open ports to which it could copy itself. Once a port is identified as being open, the program would send a Buffer Overflow attack to the RPC interface by sending a TCP packet with the exploit payload and program binary for installation on the system.[26] Once compromised, the system would check this configuration file on the Internet and begin to check the designated IP address range provided in the configuration file. I believe that this propagation would generate a healthy number of "zombies" with which phase two could be initiated.

The second phase of this attack would involve modifying the configuration file on the Internet to target specifically the Webserver and mail server of GIAC Enterprises. The configuration file would contain basic information such as the IP address(es) of the devices to be attacked, and the type of attack to be sent, such as SMTP messages, Telnet calls to port 25 or great numbers of HTTP "get" calls to the webservers.



[25] ***CERT® Advisory CA-2003-19 Exploitation of Vulnerabilities in Microsoft RPC Interface***. CERT Online. July 10, 2003. URL: http://www.cert.org/advisories/CA-2003-19.html (April 2003)
[26] ***W32/Mydoom@MM***. NAI Online. Jan 26, 2004. URL: http://vil-origin.nai.com/vil/content/v_100983.htm (April 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.2.2 Countermeasures for DoS Attack

By placing an IntruShield NIPS Sensor in line with inbound traffic to the webserver and mail servers, this attack would not succeed. A DoS detection engine on the sensor would identify this traffic as an attack and drop the packets before they reach their destinations.

4.3 Attack Design for Compromising Internal System

Not knowing the internal configuration of the network, I would modify the program created for the DoS attack so that it silently installs itself through html code, automatically executed just by opening the message – similar to **W32/Bagle@MM** virus.[27] This being a customized virus, there would not be a signature yet that would catch this at the gateway scanner or on locally installed anti-virus scanners. This program would have the same method for retrieving a configuration file via an http get command as the DoS program describe above. This program would differ from the previous one by being able to scan networks on which is installed and send user name, IP address and open port information via an e-mail to a specified anonymous account on the Internet or via an http "put" to the IP address from where it downloads the configuration file.

By minimizing network traffic activity used for pings and sweeps of the network so as to lower to probability of alerting any NIDS, the program will slowly send the attacker bits of information with which to build a comprehensive map of the internal environment. After sufficient information has been gathered, the configuration file on the Internet will be modified to instruct the compromised devices to target the internal database at a specific. The rules for internal access of the database are undoubtedly more flexible than those that are used for external users. By performing a concentrated targeted attack on this system, the potential exists that the server will be brought down through a DoS on open ports, and thus stopping GIAC Enterprises from transacting business – at least for a little while. As the attack unfolds, parts of the internal network will become unavailable; the IDS will begin registering the attacks, but will be able to do nothing. The only solution would be to shut down access to the database server or alter the firewall rules to prevent this attack leaving the user network. Cleanup of this attack will be costly, and productivity on local users will grind to a halt. Eventually firewall logs would reveal this slow-motion conspiracy and trace it back to a single device on the Internet, but that single device would also have been a compromised system, not the true source of the attack.

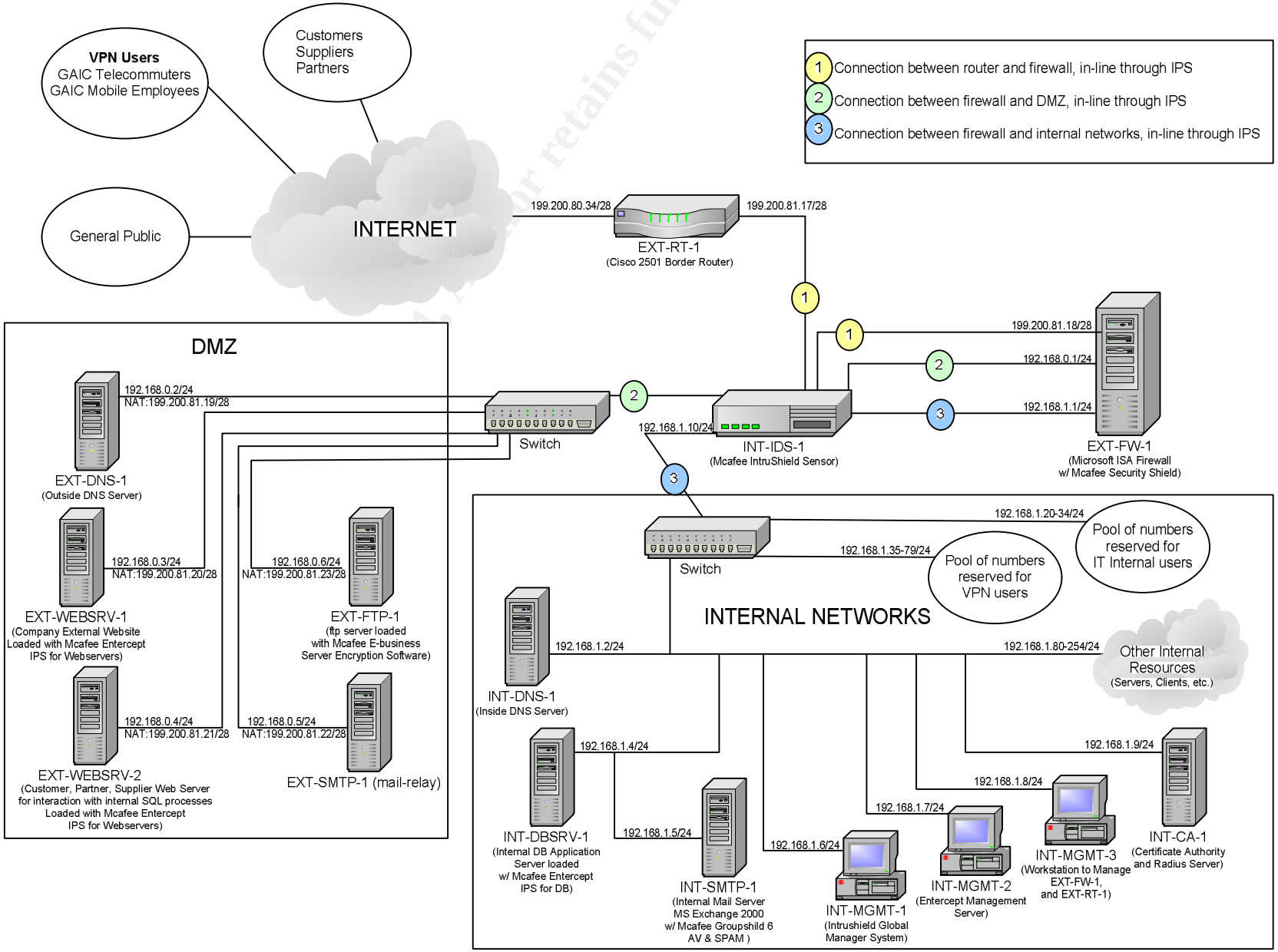
An IntruShield NIPS Sensor placed in inline mode between the database server and all other networks would prevent his attack. The DoS detection engine on the sensor would immediately drop the packets before the reach the database server.

---

[27] ***W32/Bagle@MM***. NAI Online. Jan 18, 2004. URL: http://vil.nai.com/vil/content/v_100965.htm. (April 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A: Large Network Diagram



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix B: Router Configuration

```
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname EXT-RT-1
!
enable secret 5 ****************************
enable password ******
!
no ip source-route
no ip bootp server
no ip domain-lookup
!
!
interface Ethernet0
 description Internal Ethernet Interface
 ip address 199.200.81.17 255.255.255.240
 ip access-group 110 in
 no ip proxy-arp
 ntp disable
!
interface Serial0
 description External Serial Interface Facing Internet
 ip address 199.200.80.33 255.255.255.240
 ip access-group 100 in
!
interface Serial1
 no ip address
 shutdown
!
no ip classless
access-list 100 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 100 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 100 deny   ip 169.254.0.0 0.0.255.255 any log
access-list 100 deny   ip host 0.0.0.0 any log
access-list 100 deny   ip 199.200.81.0 0.0.0.240 any log
access-list 100 deny   ip host 199.200.80.33 any log
access-list 100 permit tcp any 199.200.81.0 0.0.0.240 established
access-list 100 deny   ip any host 199.200.81.16 log
access-list 100 deny   ip any host 199.200.81.31 log
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 199.200.81.0 0.0.0.240
access-list 100 deny   udp any any range 33400 34400 log
access-list 100 permit tcp any host 199.200.81.19 eq domain
access-list 100 permit udp any host 199.200.81.19 eq domain
access-list 100 permit tcp any host 199.200.81.20 eq www
access-list 100 permit tcp any host 199.200.81.21 eq www
access-list 100 permit tcp any host 199.200.81.21 eq 443
```

© SANS Institute 2004, Author retains full rights.

```
access-list 100 permit tcp any host 199.200.81.22 eq smtp
access-list 100 permit tcp any host 199.200.81.23 eq ftp
access-list 100 permit tcp any host 199.200.81.18 eq 1723
access-list 100 permit udp any host 199.200.81.18 eq 47
access-list 100 permit tcp any host 199.200.81.18 eq 47
access-list 100 deny   ip any any log
access-list 110 permit tcp host 199.200.81.18 any eq telnet log
access-list 110 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 110 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 110 deny   ip 169.254.0.0 0.0.255.255 any log
access-list 110 deny   ip host 0.0.0.0 any log
access-list 110 permit ip 199.200.81.0 0.0.0.240 any
access-list 110 permit icmp any any echo
access-list 110 permit icmp any any parameter-problem
access-list 110 permit icmp any any packet-too-big
access-list 110 permit icmp any any source-quench
access-list 110 deny   icmp any any log
access-list 110 permit udp any any range 33400 34400 log
access-list 110 deny   ip host 199.200.81.17 host 199.200.81.17 log
access-list 110 deny   tcp any any range 1 chargen log
access-list 110 deny   tcp any any eq whois log
access-list 110 deny   tcp any any eq 93 log
access-list 110 deny   tcp any any range 135 139 log
access-list 110 deny   tcp any any eq 445 log
access-list 110 deny   tcp any any range exec 518 log
access-list 110 deny   tcp any any eq uucp log
access-list 110 deny   ip any any log
no cdp run
!
line con 0
line aux 0
line vty 0 4
 password ******
 login
!
end
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. ***Mcafee E-Business Server 7.1 Datasheet***. Network Associates, Inc. 2002. URL: http://www.nai.com/us/_tier2/products/_media/mcafee/ds_ebusiness_server.pdf (3 Mar, 2004).
2. ***Mcafee ePolicy Orchestrator 3.0 DataSheet***. Network Associates, Inc. 2003. URL: http://www.nai.com/us/_tier2/products/_media/mcafee/ds_epolicy_orchestrator.pdf (Mar 2004)
3. ***Release Notes for Cisco IOS Release 11.2(2)P***. Cisco Systems, Inc. 1998. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/xprn112/141503.htm (Mar 7, 2004)
4. Shiner, Thomas and Shinder, Debra. ***Configuring ISA Server 2000.*** Rockland: Syngress Publishing, Inc. 2001.
5. Shinder, Thomas, ***ISA Server Security Checklist Part 1***. February 4, 2002. URL: http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist__Part_1_Securing_the_Operating_System_and_the_Interface.html# (March 2004).
6. ***Mcafee IntruShield Network IDS Sensor Data Sheet***. Network Associates Inc. 2004. URL: http://www.nai.com/us/_tier2/products/_media/sniffer/ds_intrushieldidssensor.pdf (April 2004)
7. Shinder, Thomas. ***Configuring the VPN Client and Server to Support Certificate-Based PPTP EAP-TLS Authentication - Part 1***. ISAserver.org. June 22, 2003. URL: http://www.isaserver.org/tutorials/pptpeaptlspart1.html (Mar 2004)
8. ***Mcafee Entercept Web Server Edition Data Sheet***. Network Associates Inc. 2004. URL: http://www.nai.com/us/_tier2/products/_media/mcafee/ds_entercept_webserver.pdf (Feb 2004)
9. National Security Agency, ***Router Security Configuration Guide.*** NSA [online], 2002. URL: http://www.nsa.gov/snac/cisco/guides/cis-2.pdf. (Feb 2004).
10. Rekhter, Y et al. ***RFC 1918 Address Allocation for Private Internets***. Internet RFC/STD/FYI/BCP Archives. February 1996. URL: http://www.faqs.org/rfcs/rfc1918.html (Nov 2003).
11. SANS Institute, ***2.1 TCP/IP for Firewalls and Intrusion Detection***. SANS Press, 2001.
12. SANS Institute, ***2.2 Firewalls 101: Perimeter Protection with Firewalls***. SANS Press, 2001.
13. SANS Institute, ***2.3 Firewalls 102: Perimeter Protection and Defense in-Depth***. SANS Press, 2001.
14. SANS Institute, ***2.4 VPNs and Remote Access.*** SANS Press, 2001.
15. SANS Institute, ***2.5 Networking Design and Performance***. SANS Press, 2001.
16. Eu Jin, Justin Ng, ***SANS GIAC Certified Firewall Analyst Practical Assignment Version 2.0 Protecting Internet Fortune Cookies, 24 October 2003.*** GIAC [online], 2003. URL: http://www.giac.org/practical/GCFW/EuJin_JustinNg_GCFW.pdf (December 24,2003).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

17. Stadler, Philipp, ***SANS GIAC Certified Firewall Analyst Practical Assignment Version 1.9, Scalable Network for Expanding Company***. GIAC [online], 2003. URL: http://www.giac.org/practical/GCFW/Philipp_Stadler_GCFW.pdf (December 24,2003).

18. Hotaling, Miichael ***SANS GIAC Certified Firewall Analyst Practical Assignment Version 2.0, GIAC Firewall Implemetation***. GIAC [online], 2003. URL: http://www.giac.org/practical/GCFW/Michael_Hotaling_GCFW.pdf (April 2004).

19. Chapman, D. Brent and Zwicky, Elizabeth D., ***Building Internet Firewalls***. O'Reilly & Associates, Inc, 1997.

20. National Security Agency, ***Router Security Configuration Guide*****.** NSA [online], 2002. URL: http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (Feb,2004).

21. IntruVert Networks, ***IntruShield IDS System, Manager Administrator's Guide, Version 1.9***, Network Associates Inc., 2004.

22. Hunt, Craig, ***TCP/IP Network Administration, Second Edition***. O'Reilly & Associates, Inc, 1998.

23. Wright, Gary R., ***TCP/IP Illustrated, Volume 2, The Implementation***. Addision Wesley Longman, Inc, 1999.

24. ***Configuring Remote Access Policy*** (for IAS). Microsoft. 2004. URL: http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_nap_condition.asp (April 2004)

25. Dyck, Timothy. ***OpenBSD Gets Harder to Crack***. Eweek online.June 2003. URL: http://www.eweek.com/article2/0,3959,1111894,00.asp 2003.

26. ***OpenBSD PF State Tracking Spoofed Packet Vulnerability*****.** Security Focus Online. Jan 2004. URL: http://www.securityfocus.com/bid/9362/info/ April 2004.

27. ***Microsoft Security Bulletin MS03-026***. Microsoft Online. Sept 10, 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx (April 2004)

28. ***CERT® Advisory CA-2003-19 Exploitation of Vulnerabilities in Microsoft RPC Interface***. CERT Online. July 10, 2003. URL: http://www.cert.org/advisories/CA-2003-19.html (April 2003)

29. ***W32/Mydoom@MM***. NAI Online. Jan 26, 2004. URL: http://vil-origin.nai.com/vil/content/v_100983.htm (April 2004).

30. Lammle, Todd, et al. ***CCNA Study Guide (Exam 640-407)***. Sybex Press. 1999.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

31. Reed, Darron***. [Full-Disclosure] firewall security bug?*** Jan 2004. URL: http://archives.neohapsis.com/archives/fulldisclosure/2004-01/0059.html April 2004.

32. ***Spoofing Attacks. Online*** Doucmentation Server. http://www.ods.com.ua/win/eng/security/Max_Security/ch28/ch28.phtml. April 2004

33. **Engage Security Online**. April 2004. URL: http://www.engagesecurity.com/

© SANS Institute 2004, Author retains full rights.