Global Information Assurance Certification Paper

(GCFW)

Track II - Firewall and Perimeter Protection Practical Assignment

CAPITOL SANS 2000 – WASHINGTON, DC
Alexandre Freire

Document created on February, 2001

GENERAL INDEX

Preface

In the past, the strength of countries and organizations were measured in terms of production, with tons of steel, barrels of oil, and similar metrics used to gauge their place among contemporaries. Today, the strength of countries and organizations is more dependent upon their capacity to transfer information. That information can range in scope from satellite images of terrorists´ base camps in the village of Afghanistan, which are used to wage reliatory strikes to countries, to the flow of financial information between organizations and the use of ATM machines by consumers. If this information flow is disrupted or altered, the effect on countries, organizations and individuals can be severe or even disastrous. Just imagine if a person could intercept the flow of financial information and reroute the flow of funds into an account in Switzerland or in the Bahamas? Depending on whose accound was diverted, countries, business or individuals might become candidates for national bankruptcy.

The key to securing networks is obtained through the use of appropriate equipment and policies that govern the use of such equipment. In today´s environment, companies must protect their data, both inside and outside their corporate networks. To protect themselves from inside, companies rely on internal audits, password security etc. For a company to protect itself from the outside, it must use special technology. This special technology is a firewall, wich protects and internal network from the outside world and only permits those protocols and services allowed in through a corporate security policy. Firewalls today have many other useful features, such as authentication, virus checking, intrusion detection but their main goal is protection.

Firewalls are designed to keep unwanted and unauthorized traffic from an unprotected network like the Internet off limits to a private network like a LAN or WAN. At the same time they allow users of the local network to access the Internet services and permit Internet services, such as SMTP and DNS, to enter internal networks.

Some Firewalls are merely routers, filtering incoming datagrams based on the informaton contained in the datagram e.g., source address, destination address, higherlevel protocol, or other criteria specified by the private networks´ security manager of security policy. Some corporations use routers as if the were firewalls, to filter security policy. This is accomplished by applying access lists on routers.

Some Firewalls employ proxy servers, also called *bastion hosts*. The bastion hosts prevents direct access, white filtering out unauthorized incoming Internet traffic.

A Firewall acts like a security gate, providing security to those components inside the gate, controlling who (or what) is allowd to get into this protected environment. It also controls what is allowd to go out. It works like a security guardian at a front door, controlling and authenticating who can or cannot have access to the site.

It is set up yo provide controllable filtering of network traffic, allowing restricted access to certain Internet port numbers and blocking access to almost everything else. In order to do that, it must function as a single point of entry. That is why many times Firewalls are integrated with routers.

One of the basic features of a firewall should be to protect the site against hackers, but they cannot protect against connections that bypass firewalls (authorized connections / users). Therefore, be careful with back doors, such as modem connections to a LAN. Even front doors are vulnerable to attack. When a firewall is configured, holes are created to allow inbound services. When a corporation receives e-mail from others on the Internet, it is because the firewall has been set up to allow the SMTP protocol (port 25) to enter the network.. This service is needed for receiving Internet mail, but is also allows hackers to attempt to telnet to the mail server (via port 25). In addition to the security policy that is installed on firewall, it must consider

any inbound access and take steps to tighten the security on those machines that make use of such services.

Neverthless, a firewall is to enhance security, not to guarantee it! If there is very valuable information in a LAN, the Web server should not be connected to it in the first place. Also, if the Web server is inside the internal LAN, watch for internal attacks there as well as those on corporate servers. There is nothing a firewall can do about threats from inside the organization. An upset employee, could pull the plug of a corporate server, and shut it down, and there is nothing a firewall could do!

Welcome to Firewall and Perimeter Protection Practical Assignment for Capitol SANS GCFW!

1. Introduction to Capitol SANS Practical Assignment

The SANS Institute requests students to complete a Practical Assignment that is needed to demonstrate the understanding of the course material before being authorized to take exams. It is impossible for SANS to fully test the knowledge of the course material using exams alone; therefore it is imperative demonstrating knowledge of the subject matter in the practical assignment.

The Capitol SANS Practical Assignment requests four Assignments as follows ;

1.1 Assignment 1 - Security Architecture (25 Points)

Define a security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

Customers (the companies that purchase bulk online fortunes);

Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);

Partners (the international partners that translate and resell fortunes).

Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component.

1.2 Assignment 2 – Security Policy (25 Points)

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

- Border Router
- Firewalls
- VPN

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

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

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

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

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.

2. Any relevant information about the behavior of the service or protocol on the network.

3. The syntax of the ACL, filter, rule, etc.

4. A description of each of the parts of the filter.

5. An explanation of how to apply the filter.

6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)

7. Explain how to test the ACL/filter/rule.

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

1.3 Assignment 3 – Audit Your Security Architecture (25 Points)

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

8. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

9. Implement the assessment. Validate that the Border Router and Firewalls are actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

10. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

1.4 Assignment 4 – Design Under Fire (25 Points)

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

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

11. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.

12. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose. ´

13. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

2 Security Architecture (25 Points)

2.1 Network Topology – Security Architecture Defined

2.1.1 Routers

Two Cisco 3640 acts as our filtering/screening firewall (***Internet#1*** and ***Internet#2***). It´s the first line of network defense. The routers provide an important role as being a front line defense mechanism. While not representing the core of security platform, the screening router provides an important role in being a front line defense

Both routers are running IOS version 12.0. Beginning with IOS 11.3, Cisco routers support three different types of access-lists: standard, extended, and reflexive (added in IOS 11.3). Extended access- lists were used for this practical.

Company has two Internet links. The first one is the Inbound Link (inbound connections to Protected Subnet). It´s a T1 providing 1.54Mbps bandwidth to our ISP. The second one is a 512 Kbps to same ISP but it´s used for outbound traffic only (connections started from LAN Subnet to outside – Internet).

Another router, Cisco 2501 Access Server provide dial-in connections and allow 8 users simultaneously.

2.1.2 Firewalls

Two CheckPoint firewalls (***Firewall-1_FW1*** and ***Firewall-1_FW2)*** *are* providing network security. Both of the firewalls are running in a Dual Pentium III 700 processor with 1GB Ram Intel system. The firewalls are running CheckPoint Firewall-1 version 4.1 with the latest Service Pack (Service Pack 3). They are running under Windows NT Server 4 / Service Pack 6a.

Firewall-1_FW1 is configured with 3 10/100 3COM interface cards (NICS) The external NIC is connected to the DMZ Subnet 1.1.1.0 and its IP address is 1.1.1.2. The Protected Subnet NIC (Screened Network) is connected to a 3COM switch 1000 an its IP address is 1.1.2.1. The last NIC is connected to a 3Com Corebuilder 5000 on the core network segment (Core Subnet 1.1.5.0) and its IP address is 1.1.5.1

Firewall-1_FW2 is also configured with 3 10/100 3COM interface cards (NICS). The external NIC is connected to the DMZ Subnet 1.1.3.0 and its IP address is 1.1.3.2. The Lan Subnet NIC is connected to a 3COM switch 1000 and its IP address is 1.1.4.1. The last NIC is connected to a 3COM Corebuilder 500 on the core network segment (Core Subnet) amd its IP addresss is 1.1.5.2.

2.1.3 Secure Remote VPN (Remote Access)

Remote access to business partners and suppliers is provided and authentication is required. The proposed

architecture relies on Firewall-1 SecuRemote (VPN-1 Secure Remote Version 4.1 – Service Pack 2 3DES) to establish VPN services that are available on FW-1. Access is authenticated using Firewall-1 password which identifies the user, and authenticates access based on polices enforced by FireWall-1.

2.1.4 Protected Subnet (Screened Network)

Our screened network contains 9 servers,.the web server (IP address 1.1.2.2), the Customer Web Server (IP address 1.1.2.3), the Suppliers Web Server (IP address 1.1.2.4), the Partners Web Server (IP address 1.1.2.5), the Mail Server (IP address 1.1.2.6), the Primary Domain Name Server (IP 1.1.2.7), the Syslog Server (IP address 1.1.2.9) and the Intrusion Detection System server (IP address 1.1.2.10). The secondary external DNS is hosted by our ISP.

All servers are running RedHat Linux 7.0 and they were screened using the ***Securing Linux*** book ***(Published from SANS Institute)*** and with the ***Bastille Linux Scrippts (scripts to secure Linux).***

Any sensitive data accessed via our external Web servers is to be done via https utilizing SSL and our digital certificate purchased from VeriSign. All electronic commerce transactions are to be performed via this method.

Primary Domain Name Server has been updated to ***bind 9.1.0*** due recent buffer overflow problems. Web Servers are running the latest Apache release (1.3.17) and MailServer is running the latest Sendmail release (8.11.2)

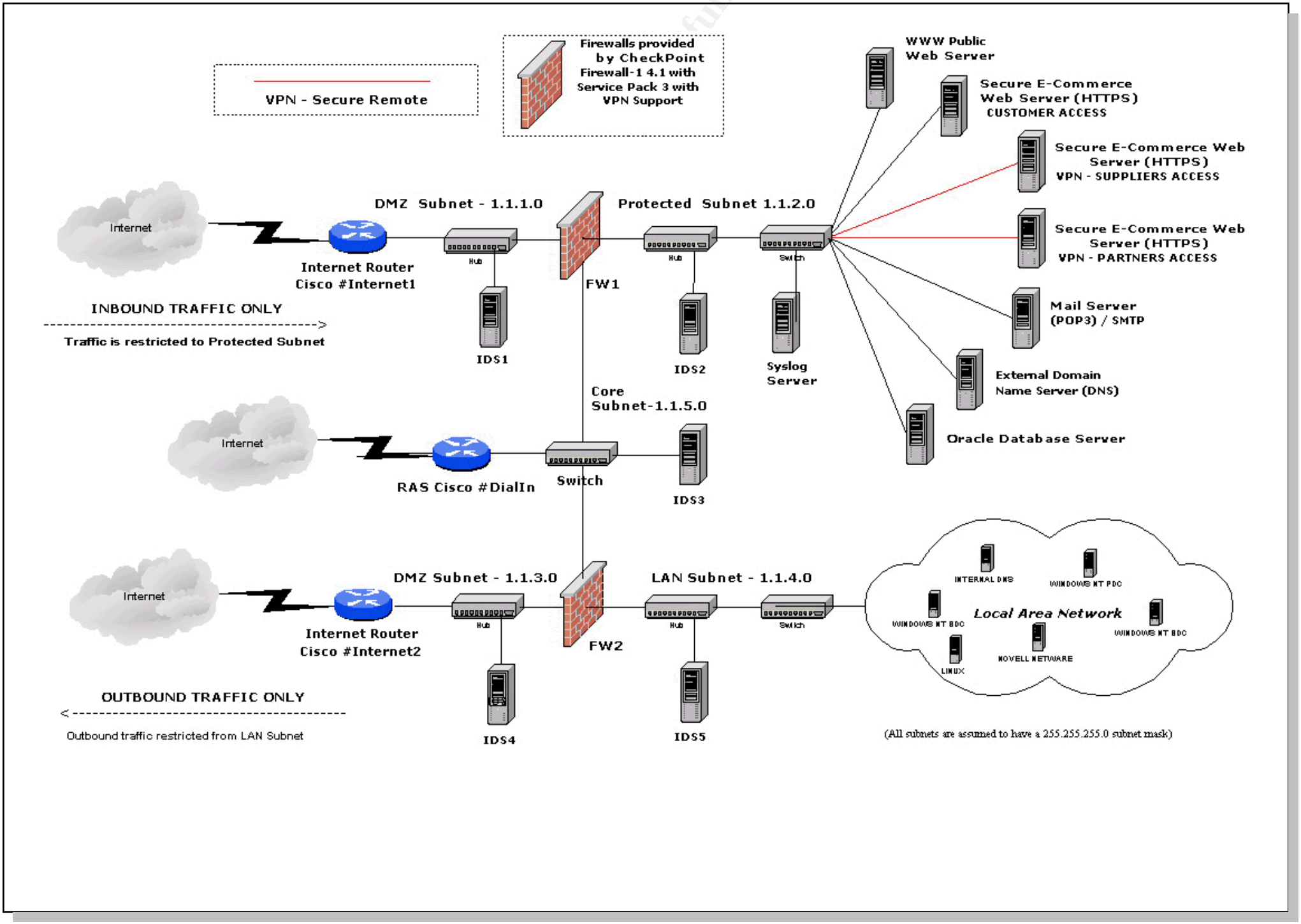
*** Alert: BIND DNS Buffer Overflow –** Posted: 22:00 January 29, 2001

The ISC has recently released Bind 8.2.3, which fixes multiple high-risk security concerns which would allow a remote attacker to execute arbitrary code on your server. All Bind 8.2.x versions are vulnerable, as well as Bind 8.2.3 T1A through T9B. The buffer overflow is in the processing of transaction signatures (TSIG), which leads to both recursive and non-recursive DNS servers being vulnerable.

There are also two security problems (one buffer overflow and one format string vulnerability) in Bind 4.9.x versions (up to and including 4.9.7). The newer Bind 9.1.x series is not vulnerable to any of the these vulnerabilities. We suggest you upgrade to Bind 8.2.3, 4.9.8, or 9.1.0 immediately.

2.1.5 Intrusion Detection System

Each subnet has it own Intrution Detection System that runs in promiscuous mode analyzing packets on the hire. The Intrusion Detection System chosen was the SNORT one and critical messages are logged and sent to Syslog Server on Protected Subnet (Screened Subnet). The SNORT version running is the 1.7 one.



3 Security Policy (25 Points)

3.1 Security Policy Defined - Base Security Policy Recommendations from SANS Top Ten Document

When you connect your network to the Internet, securing your network against intrusion is of critical importance. The most effective way to secure the Internet link is to put a firewall system between the local network and the Internet.

The firewall ensures that all communication between an enterprise's network and the Internet conforms to the enterprise's Security Policy.

In order to effectively provide real security, a firewall must track and control the flow of communication passing through it. To reach control decisions for TCP/IP based services (for example, whether to pass, reject, encrypt or log communication attempts), a firewall must obtain, store, retrieve and manipulate information derived from all communication layers and from other applications.

A security policy is vital when a firewall is set up at any company, since it outlines what assets are worth protecting and what actions or risk management procedures must be undertaken to protect corporate assets. Network security policies must often integrate security issues from previous policies.

As a requirement of any good security policy, a basic set of policy rules is required. For the purposes of this paper the SANS Top Ten Filtering Recommendations are assumed to be implemented on Firewalls and routers *

Warning : It is not recommended to mirror rules (same rules on routers and Firewalls). The main reason for a router operating is to route packets. Do not have the router replicate every firewall rule, intead work together. As a recommendation from SANS Institute, when you have a router / Firewall combination, make sure the router is not replicating the entire firewall rulebase. In general a router allows everything, then denies only specific services or IPs. In contrast,a firewall denies everything, then allows only specific services or IPs.

The Base Security Policy contains the filtering recommendations from Appendix B of the SANS Top Ten document located at http://www.sans.org/topten.htm.

In this section, we list the Base Security Policy so you know what additional services to recommend blocking. This Policy lists ports that are commonly probed and attacked.

Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts.

A warning is also in order: blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

1) Block "spoofed" addresses

Packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.

2) Login services
telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)

3) RPC and NFS
Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

4) NetBIOS in Windows NT
135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

5) X Windows
6000/tcp through 6255/tcp

6) Naming services
DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)

7) Mail
SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

8) Web
HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

9) "Small Services"
ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

10) Miscellaneous
TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

11) ICMP
block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded,

and unreachable messages.

3.2 Security Policy Implementations on Border Routers and Firewalls – Addressing Security Policy Recommendations from SANS Top Ten Document

As requested for the Practical Assignment, It is needed to provide a tutorial explaining how to implement each ACL, rule, or policy measure on specific components. It´s requested to provide information about services or protocols addressed by the Access Control Lists or Firewall rules and the reason these services might be considered a vulnerability.

In this section, the SANS Top Ten Document was used as a reference on how to develop a secure policy. It shows the recommentations, associated vulnerabilities and make reference to access control lists or rules implemented on components (Cisco router or CheckPoint Firewall-1) and how to accomplish them.

Important Notes :

The syntax of the Access Control Lists, filters and rules, description of each of the parts of the filters, explanation on how to apply the filters can be found on next sections : ***(Section 3.4 - Perimeter Security – Security Policy on Border Routers and Section 3.5 – Perimeter Security – Security Policy on Firewalls).***

Explanation on how to test the ACLs/filters/rules, including output of tools like Snort IDS and CheckPoint Log Viewer can be found on ***Section 4 – Security Audit***

Recommentations, associated vulnerabilities and reference on implemented security :

3.2.1 Spoofed Addresses :

Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.

- ***Vulnerability:***

Three address ranges fall into the category of Private IP address ranges, they are:

10.0.0.0/8 172.16.0.0/12 192.168.0.0/16

Packets addressed with Private IP's coming from the Internet would not be accepted. As described in RFC 1918d evices with a Destination IP address in one of these ranges cannot be routed to and should be rejected. Hence, the response to any traffic entering a Publicly addressed network with a Private IP address in the SRC field cannot be routed back to. Therefore, this kind of traffic coming from or going to the Internet should not be considered valid traffic and should be dropped.

Source routed packets should also be blocked at the firewall in order to prevent hostile hosts from pretending to be trusted hosts.

Blocking inbound packets using internal address, private address, or the loopback address as the source address will help to protect the network from inbound spoofed packets.

- ***Filtering Rule - Routers***

Refer to ***Section 3.4 - Perimeter Security – Security Policy on Border Routers.*** Extended access list was created in the INBOUND direction on the External interface on both two routers denying inbound traffic with invalid SRC address and the command "*no ip source-route"* was placed on router in order to prevent source routed packets from entering the network.

- ***How to Test :***

One of the best ways in order to test these filter rules is to try sending crafted packets from the Internet through the router to the protected network (traveling inbound to the external interface of the router). The log option is set in order to view whether or not the packets were blocked at the router.

3.2.2 Login Services

Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)

TELNET (23/tcp) .

- ***Vulnerability:***

Telnet is a remote access protocol that enables bi-directional communications between a "user" host and a "server" host who both appear to the other to be a network virtual terminal.Telnet is used for remote terminal access, where all the session information (login, passwords, data) is presented in clear text across the network. Once a session is established and a valid user name and password has been submitted, keystrokes entered at the "user" host are sent to the "server" host, and output from the "server" host appear on the screen of the "user" host.

Data, including the username and password, are sent in clear text. The information being passed is susceptible to interception and exposure. Telnet is also vulnerable to session hijacking. Telnet could allow remote users full command line access to systems, allowing for a full system compromise.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Login_Services*** contains and blocks telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), and the r-services rlogin et al (512/tcp through 514/tcp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a **telnet** session with an internal host. The log option is set in order to view whether or not the packets were blocked at the router or Firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump) can be used for packet capture verification.

SSH (22/tcp)

- ***Vulnerability:***

Secure shell (SSH) can be thought of as "encrypted telnet" and it´s intended to be a replacement for the Unix "r" commands (rlogin, rsh, rcp, and rdist). In a SSH session, login, password, and data are all encrypted. Since the traffic is encrypted, it is difficult for network administrators to monitor traffic being sent and received. SSH also enables the forwarding of TCP connections through the encrypted channel and It can be exploited to send possibly malicious traffic across the channel.

It also allow remote users full command line access to systems, because It can be used for remote logons, remote execution of commands, and remote copy.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Login_Services*** contains and blocks telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), and the r-services rlogin et al (512/tcp through 514/tcp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a **ssh** session with an internal host. The log option is set in order to view whether or not the packets were blocked at the router or Firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump) can be used for packet capture verification.

FTP (21/tcp)

- ***Vulnerability:***

File Transfer Protocol is used in order to allow file transfers from one system to another one. It allows remote copying of data. If permissions on the FTP enabled system are not carefully set, users might modify files to exploit the r-services (rsh, rexec) or upload password files to crack and exploit, storing various warez or undesirable files on corporate systems.

The FTP session may be susceptible to session hijacking and the information, sent in clear text, may be susceptible to sniffing.If the attacker has or gains write access, malicious code can be placed on the server.

The user can use either an account with a specific username and password, or if supported, the user name "anonymous", to login to the server.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Login_Services*** contains and blocks telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), and the r-services rlogin et al (512/tcp through 514/tcp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a **ftp** session with an internal host. The log option is set in order to view whether or not the packets were blocked at the router or Firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump) can be used for packet capture verification.

For NETBIOS services please, refer to Section 3.3.4 – NetBIOS in Windows NT

Rlogin et al

- ***Vulnerability:***

TCP ports 512-514 (exec 512/tcp, login 513/tcp, and shell 514/tcp) are based upon a trust model which can provide access simply based upon the address of the host that is communicating with it. These three services can pose a significant security risk to UNIX systems because they are used for logging into systems across the network and executing commands on remote systems.

Since data is transmitted in clear text, traffic is susceptible to sniffing. Vulnerable to unauthorized access. The r-services vulnerability ties in with an unsecured FTP server and the possibility of manipulating the .rhosts and /etc/hosts.equiv files to gain access.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Login_Services*** contains and blocks telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), and the r-services rlogin et al (512/tcp through 514/tcp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **inbound r-services (rsh, etc)** on an internal host. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.3 RPC and NFS

Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

Portmap/Rpcbind (111/tcp and 111/udp)

- ***Vulnerability:***

The portmap service is used to keep track of Remote Procedure Call services. Rpcbind is the name of the portmapper on systems using TI-RPC. RPC server program that acts as a registrar that keeps track of which RPC programs are using which ephemeral ports. Servers use RPCs to register themselves with the portmapper. Clients use RPCs in order to query the portmapper.

These RPC's notify portmap as to which high ports that service is going to be using. By being able to connect to port 111, users can discern which RPC's are running on which ports. This information can then be exploited as the situation permits.

An attacker can use rpcinfo, which is a program that calls PMAPPROC_DUMP, to gather information about which port numbers are being used by which RPC program. Also, earlier versions of portmapper permitted any program to register itself.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***RPC_NFS _Services*** contains and blocks Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a inbound connection to **TCP port 111 and UDP port 111** on an internal host. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

NFS (2049/tcp and 2049/udp)

- ***Vulnerability:***

Network File Systems allows a remote machine to mount local file systems. It´s a is a client-server application based on Sun RPC. NFS enables clients to access files and file systems on a server. The NFS client is able to access files on an NFS server by transmitting RPC requests to the NFS server.

NFS is vulnerable to IP spoofing attacks because it uses IP addresses for access control. Certain versions of NFS that place limits on the access control list may be susceptible to the disabling of access controls when the limit is surpassed. Misconfiguring mount permissions can unintentionally permit unauthorized machines to mount the drive and access data.

It may also be vulnerable to attackers placing malicious programs on the system.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***RPC_NFS _Services*** contains and blocks Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a inbound connection to **TCP port 2049 and UDP port 2049** on an internal host.The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

Lockd (4045/tcp and 4045/udp)

- ***Vulnerability:***

Lockd is an RPC program that is used with NFS to handle file lock requests either locally from the kernel or remotely from another lock daemon. It process relates to NFS in that it is responsible for managing locks on NFS files. Since Internet hosts should not be so openly trusted, these protocols should be blocked.

Lockd may be susceptible to a remote denial of service attack. client is able to access files on an NFS server by transmitting RPC requests to the NFS server.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***RPC_NFS _Services*** contains and blocks Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) services on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a inbound connection to **TCP port 4045 and UDP port 4045** on an internal host.The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.4 NetBIOS in Windows NT

NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

- ***Vulnerability:***

NetBIOS is an application programming interface that uses three types of services: the name service uses port 137 to send UDP broadcast packets; the datagram service uses port 138 to send UDP broadcast or directed broadcasts; and the session service uses port 139 to send TCP segments. The WINS manager uses tcp port 135 and the Common Internet File System (CIFS) uses tcp and udp ports 445. NetBIOS is mainly used in the Microsoft Windows environment. The default NetBIOS setting for Windows 95 and 98 is enabled.

An attacker sending spoofed "Name Release" or "Name Conflict" messages to a victim host could force the victim to remove its own name from its name table; this would result in a denial-of-service attack because the victim host would be unable to initiate NetBIOS requests or respond to NetBIOS requests. User name and password traffic on a Windows NT network is vulnerable to sniffers and crackers. Also, the "one account/one login" scheme places multiple resources at risk when one account has been compromised. Trust relationships existing in a Microsoft network are susceptible to exploitation.

"For Windows NT systems, prevent anonymous enumeration of users, groups, system configuration and registry keys via the "null session" connection. Block inbound connections to the NetBIOS Session Service

(tcp 139) at the router or the NT host."

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Netbios_Services*** contains and blocks 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 earlier ports plus 445 (tcp and udp) on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

Warning : CheckPoint Firewall-1 NBT group does not contain all of these ports or that all of these services. Some service objects have to be created.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 135, UDP port 135, UDP port 137, UDP port 138, TCP port 139, TCP port 445, and UDP port 445** on an internal host. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.5 X-Windows Services

X Windows -- 6000/tcp through 6255/tcp

- ***Vulnerability:***

X-Windows systems provides a UNIX user with an attractive GUI interface to a system. It's a client-server application that can support multiple virtual user windows on a single display that is managed by a server.

In this architecture, the client is an application that runs on either the same host as the server or on a different host. The server is responsible for managing the display, mouse, and keyboard. There are two basic protection functions used in the X Window System: xhost and xauth. Xhost uses specified host IP addresses to restrict which activities are allowed. Xauth provides a similar protection service through the use of a "magic cookie" text string.

There are a number of things an attacker can do with access to an X11 server, including getting screen dumps, redirect window displays and keyboard and mouse entries in order to execute commands on the victim's host. An attacker may also be able to establish a remote window session in order to execute commands on the victim's host. Certain versions are also vulnerable to buffer overflow attacks allowing an Internet user to have a root session on a UNIX server which is nothing short of full system compromise.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service ***Xwindows_Range*** contains and blocks port 6000-6250/tcp on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

Warning : CheckPoint Firewall-1 default X11 service does only spans 6000 – 6063, so it is needed to create a new service.

- ***How to Test :***

Follow the same testing methodology to ensure that X-Windows traffic is blocked correctly. Use an external host to attempt to establish a connection to **TCP port range 6000-6250** on an internal host. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.6 Naming Services

Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)

DNS (53/UDP and 53 TCP)

- ***Vulnerability:***

The Domain Name System is a distributed database that is used to translate a host name to an IP address as well as an IP Address to a host name. It also provides electronic mail routing information. UDP port 53 is used for DNS queries and replies. TCP port 53 is used for zone transfers and for when the UDP DNS response is greater than 512 bytes.

DNS traffic needs to be controlled for several reasons, including: hosts, other than the DNS server, that are running a DNS implementation, such as BIND, may be exploited using vulnerabilities within that particular implementation. DNS may also be vulnerable to cache poisoning. An attacker could a remote DNS server to place erroneous DNS records into the cache of the victim DNS server. Zone transfers must be controlled in order to prevent unauthorized disclosure of the internal network.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**.Service group ***Naming_Services*** contains and blocks 53 (tcp and udp), 389 (tcp and udp) on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 53 and UDP port 53.** The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

LDAP (389/tcp and 389/udp)

- ***Vulnerability:***

The Lightweight Directory Access Protocol is set of protocols used to access the X.500 Directory. It´s used with Microsoft's Windows 2000 Active Directory architecture and other systems. Since Active Directory represents a unified object repository, significant user information can be quickly obtained by queries to this system.

Directories implementing LDAP may contain private individual and organizational information. An attacker may attempt to exploit LDAP vulnerabilities that may provide unauthorized access to this information. There is also the concern of denial of service attacks and modification of records.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**.Service group ***Naming_Services***

contains and blocks 53 (tcp and udp), 389 (tcp and udp) on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Once again, use an external host to attempt to establish a connection to **TCP port 389 and UDP port 389.** . The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.7 Mail Services

SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

SMTP (25/tcp)

- ***Vulnerability:***

The Simple Mail Transfer Protocol specifies how two Message Transfer Agents (MTAs) exchange electronic mail over a TCP connection. There is no need to allow SMTP traffic to any device other than the site's appropriate mail server(s). This is probably one of the most common services offered by an organization with an internet presence. Because of the prevalence of the protocol it is naturally one of the most commonly scanned for protocols

SMTP does not provide confidentiality and authentication. SMTP is therefore vulnerable to sniffing and modification of host and user name. SMTP is also susceptible to denial of service attacks. An attacker may also be able to Telnet to port 25 and execute commands as root.

Sendmail has a long and sordid history of security vulnerabilities.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Sservice group ***Mail_Services*** contains and blocks 25/TCP, 109/TCP and 110/TCP ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Once again, use an external host to attempt to establish a connection to **TCP port 25.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

POP (109/tcp and 110/tcp)

- ***Vulnerability:***

The Post Office Protocol enables users to download e-mail messages stored on a mail server. POP3 uses TCP port 110. POP2 and older versions use TCP port 109.

POP should not be allowed to any system if these remote mail services are not permitted by the corporate security policy. It´s vulnerable to spoofing and denial of service attacks. Since POP transmits passwords in clear text, an attacker would be able to sniff the wire and capture information. POP also does not provide server authentication; therefore, an attacker would be able to transmit data to the client and the client would think this information was originating from the mail server.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Sservice group ***Mail_Services*** contains and blocks 25/TCP, 109/TCP and 110/TCP ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 109 and TCP port 110.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

IMAP (143/tcp)

- ***Vulnerability:***

The Internet Message Access Protocol enables users to access e-mail messages stored on a mail server. The service is vulnerable to network sniffing.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Mail_Services***

contains and blocks 25/TCP, 109/TCP and 110/TCP ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 109 and TCP port 110.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.8 Web

HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

HTTP (80/tcp)

- ***Vulnerability:***

The Hypertext Transfer Protocol is used for distributed, hypermedia information systems and resides at the application layer. Often organizations have confidential information on their organizational web servers, so it's a good idea to have a few network controls protecting them. Although HTTP's well-known port is TCP port 80, it can be configured to other ports. HTTP over SSL uses TCP port 443. HTTP can also use other ports such as TCP port 8080.

Limiting access to the correct Web servers prevents remote users from accessing un-intentional web servers (i.e.: those systems running IIS or Apache type servers without their knowledge). Further, eliminating the other common high ports and limiting web services to ports 80 or 443 would prevent having to open holes in the firewall on any tcp-high ports. Limiting port and destination access to just the web servers does not prevent exploiting the web server applications. It can still be exploited by techniques, such as cgi script exploit as the dissemination of malicious mobile code or the use of HTTP to tunnel other types of services.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Web_Services*** contains and blocks 80/TCP, 443/TCP, 8000/TCP, 8080/TCP and 8888/TCP ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP ports 80, 443, 8000, 8080 and 8888.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.9 Small Services

Ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

- ***Vulnerability:***

Many of the small services can lead to a denial of service (DoS) attack. TCP Small Services include echo, chargen, discard, and daytime. Echo - server replies back with whatever is typed. Chargen - server generates a stream of ASCII data. Discard - server drops whatever is typed. Daytime - server returns system date and time. UDP Small Services include echo, discard, and chargen. Echo - server replies back with the payload of the datagram that was sent. Discard - server drops the datagram that was sent. Chargen - server discards the datagram that was sent and responds with a 72-character string of ASCII characters.

Time protocol should not be accepted from an untrusted source, such as an Internet host. If time synching of devices is required, it should be provided as an internal service.

One the of small services (chargen, tcp/19) will generate character responses to your network request. Echo (tcp/7) will echo back the characters received on a connection to it. This means that if you spoof an chargen service connection to an echo service, you can get the two in a never ending conversation which can slow or crash a machine. The bottom line with small services is that no one ever really uses them, and they simply give an attacker some more information or an additional exploit opportunity.

- ***Filtering Rule - Routers***

Refer to ***Section 3.4 - Perimeter Security – Security Policy on Border Routers.*** The following global configuration commands should be used too avoid Small Servers

no service tcp-small-servers / no service udp-small-servers

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Group ***Smalls_Services*** contains and blocks all the TCP and UDP services below 20 and ports 37/tcp and 37/udp on ***Firewall1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP/UDP ports below 20 and 37 TCP/UDP.** The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.10 Miscellaneous

TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), **LPD** (515/tcp), syslog (514/udp), SNMP

(161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

TFTP (69/udp)

- ***Vulnerability:***

Trivial File Transfer Protocol is a less secure version of FTP that was developed for use when bootstrapping diskless systems. TFTP should be blocked for much the same reasons as FTP, plus TFTP is even less secure as no authentication is needed to transfer data.

It uses UDP instead of TCP in order to make it smaller and simpler. If not properly implemented, TFTP will allow a user to download any file from the host. It also does not support authentication.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **UDP port 69.** The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

FINGER (79/tcp)

- **Vulnerability:**

The finger service can provide quite a lot of information to outsiders such as Real names and phone numbers of users, user home directory and login shell, amount of time a user has been idle, when a user last read e-mail and the remote host that a user is logged in from.

In addition to revealing possibly private or sensitive information, some of the information finger provides may be used by an attacker to make inferences about trust relationships between hosts on your network, collect usernames for password guessing attempts, obtain phone numbers for "social engineering" attacks, and to monitor the activity on your system.

An attacker can use this information to help plan an attack. For example, what period of the day would be the most opportune time to attack or perhaps to identify rarely used accounts. Information from finger could be used as a starting point to guessing account login/password combinations and contact information would be useful for "social engineering" type attacks.

- ***Filtering Rule - Routers***

Refer to ***Section 3.4 - Perimeter Security – Security Policy on Border Routers.*** The following global configuration commands was used to avoid finger service:

```
no service finger
```

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Once again, use an external host to attempt to establish a connection to **TCP port 79.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

NNTP (119/tcp)

- **Vulnerability:**

Network News Transport Protocol is used to transfer Usenet news across the Internet. Open news servers allow posting and reading from anybody, and are used to access newsgroups blocked by someone's ISP, to post anonymously, or to post spam.

NNTP uses access control lists that are based on hostnames. This protocol is vulnerable to IP spoofing. An attacker may be able to gain access to an NNTP server and view private information. The other issue with NNTP is the shear volume of traffic.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 119.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

NTP (123/tcp)

- **Vulnerability:**

The Network Time Protocol is used to synchronize system times across the network. NTP across the firewall should be blocked for the same reason as TIME. NTP traffic can be spoofed. Spoofed NTP traffic could be used to change the time on a system prior to attempting to break in so that it's logs could not be compared to other logs.

It can take into account the network delay and the existence of different servers with different clocks.
NTP was not designed to resist attack and several versions of ntpd can be fooled in making changes to system's clock.

A replay attack could be used to modify system clocks. This would have an affect on services such as time-based authentication and time stamps. Log files will no longer accurately inicate the correct time at which events took place and batch jobs run from cron daemon may not be executed if the system's clock jumps over the time specified in the crontab.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 123.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

LPD (515/tcp)

- ***Vulnerability:***

LPD is a Unix printing protocol. LPD is used to provide network printing services and Its access control is based IP addresses.

LPD is susceptible to buffer overflow problems similar to just about every other service that uses the TCP/IP stack, IP spoofing and denial of service attacks through the use of false print requests.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 515.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

SYSLOG (514/udp)

- ***Vulnerability:***

Syslog is a service that allows multiple machines to log system messages to a central host. It provides generic logging services for system events and makes easy the task of review logs from a single point of reception.

Since most syslog servers accept unauthenticated traffic, it would be easy for a hacker to add numerous bogus entries. For example, false messages can be used to generate a denial of service attack. Information about the network's hosts can be obtained from the syslog.

Older versions may be vulnerable to buffer overflows. For example, versions of Solaris syslogd will crash when they receive a syslog message off the network from a host without inverse DNS entries. This allows an attacker to disable security auditing before attacking a host, avoiding detection by programs like TCP wrappers. If the host is vulnerable, it's syslogd will be disabled, and must be re-started via administrative intervention. Obtain the Solaris patch for this problem.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **UDP port 514.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

SNMP
(161/tcp and 161/udp, 162/tcp and 162/udp)

- ***Vulnerability:***

Simple Network Management Protocol is used to is used to centrally manage network elements. It´s a very common port that intruders probe for. SNMP allows for remote management of devices. It is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. All the configuration and performance information is stored in a database that can be retrieved or set via SNMP

It provides reading and writing to a network device's MIB (Management Information Base). Management stations can be used to gather information about interfaces as well as control particular functions on those interfaces. Port 161 is used for commands and port 162 is used for network device alarms.

SNMP is primarily used for monitoring of a network. Once one of these packages are installed, you tell it what subnets to monitor and the package will go out and discover the devices that have SNMP enabled. The discovery process works by trying a default community string such as public. The community string is the primary means of authentication used by the SNMP service. Once it performs the discovery process, the software can display and alarm on any information that is contained in that device's MIB.

SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption is bad enough, but the default community string used by the vast majority of SNMP devices is "public". Many managers leave this available on the Internet. Crackers can use the passwords "public" and "private" to access the system.. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Follow the same testing methodology to ensure that SNMP traffic is blocked correctly. Use an external host to attempt to establish a connection to **TCP port range 161-162 and UDP port range 161-162** on an internal host. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

BGP (179/tcp)

- ***Vulnerability:***

The Border Gateway Protocol is an Exterior Gateway Protocol that connects distinct Autonomous Systems and forms a single network. This routing protocol is used on the Internet backbone. Since our perimeter router is not connected to the backbone of the Internet, it should not need to receive BGP packets.

The BGP server is vulnerable to SYN flooding attacks, session hijacking, and RST attacks that attempt to tear down the connection to the server.

- ***Filtering Rule - Firewalls***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 179.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

SOCKS (1080/tcp)

- ***Vulnerability:***

Secure Sockets is a protocol that is used to support TCP traffic through a proxy server. It is used to Proxy different kinds of data (FTP, Telnet, etc). If the site is not running any SOCKS servers, the service should be denied as it serves no legitimate business need. If SOCKS proxies are being used, the firewall rules should be tightened down to specify the source and destination systems as explicitly as possible.

SOCKS may be vulnerable to denial of service attacks as well as buffer overflow attacks.

- ***Filtering Rule – Firewalls :***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. Service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp ports on ***Firewall-1_FW1*** and ***Firewall-1_FW2***.

- ***How to Test :***

Use an external host to attempt to establish a connection to **TCP port 1080.**. The log option is set in order to view whether or not the packets were blocked at the router / firewall. Nmap scan of these ports in combination with logs checking is a nice test to ensure packets were dropped. A sniffer program like tcpdump/windump can be used for packet capture verification.

3.2.11 ICMP Services

ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages

- ***Vulnerability :***

Internet Control Message Protocol is often used to assist with network mapping, It is used to transmit status and error messages. Some of the message types include: host unreachable, redirect, and time exceeded.

It can be used by intruders to learn information about the network. ICMP is a lightweight set of application that were originally created for network troubleshooting. The purpose is to report errors rather than transferring information. And the most well known ICMP application is certainly the echo request/echo reply or ping. The ICMP echo request is one of the most common mapping technique. Therefore you should block incoming echo request. The "Ping of Death fragmentation attack' uses fragmented icmp packets for denial of service which created an IP packet that exceeds the maximum 65,535 bytes of data allowed by IP specification. This will cause the victim host to crash or freeze.

With the possible exception of outbound echo requests, used for troubleshooting network connectivity, and inbound echo replies, in response to the authorized outbound echo requests, ICMP traffic (incoming pings) as well as responses to traceroute (time exceeded), echo replies (possible covert channel), and unreachable messages (provides port/service information) should be blocked whenever possible. An attacker can obtain valuable information about the internal network from ICMP messages. ICMP can be used in a denial of service attack such as a Smurf attack. ICMP can also be used as a covert channel, such as in Loki.

- ***Filtering Rule – Firewalls :***

Refer to **Section 3.5 – Perimeter Security – Security Policy on Firewalls**. The Firewall does not accept ICMP packets as configured on default properties (Pseudo Rules). It blocks all the ICMP traffic on ***Firewall-***

1_FW1 and ***Firewall-1_FW2***.

- ***How to Test :***

The ICMP blocking can be tested by using ping and traceroute (tracert) from an Internet device against protected devices. The Internet device can also try to connect to a service on a protected device that is known to not be supported and then verify that the response was blocked by the Firewall. Tools can be used to craft packets to generate and test icmp-reply packets.

3.3 Perimeter Security – Security Policy on Border Routers

3.3.1 Introduction

From a operational perspective, the major function of a router is to transfer packets from one network to another. Routers operate at the network layer that represents the third layer of the OSI Reference Model. By examining the network address of packets, routers are programmed to make decisions concerning the flow of packets.

Another function that goes hand-in-hand with routing packets between networks is the creation and maintenance of routing tables. Such protocols as RIO, OSPF and BGP represent only three of more than 50 routing protocols that have been developed over the past 20 years. With respect o security, the router represents the first line of protection for a network. That protection in in the form of access lists, which are created to enable or deny the flow of information through one or more router interfaces.

There are many facets to security and one of the most important is the capability to control the flow of data packets within a network. Specifically, preventing packets from entering a network by examining information withinthe packet header is critical. This capability is typically termed “packet filtering” and is one of the most important uses of Cisco access lists although, it´s not the only use.

Packet filtering allows control data flows in network based on source and destination IP addresses and the type of application used.For example, packet filtering allows preventing packets from entering the network if the packets are part of a telnet session that originated from certain address ranges. Additionally, It is possible to prevent all packets from a certain IP address range from entering the network, regardless of the apllication used. These kinds of functions are especially usefil when applied to routers.

In many cases, routers serve as a boundary between administrative domains. The term "administrative domains" is used to indicate a general grouping of network devices such as workstations, servers, routers and network links that are maintained by a single administrative group. Different administrative domains normally have different security policies, and there is usually limited access between data networks in separate administative domains. In most cases, an administrative domain makes up a company´s corporate network, although some large companies may have many administrative domains.

One of the functions served by routers is to tie these separate administrative domains together. Routers serve this function, for example, as a connection point between a corporate LAN and the Internet or between two or more corporate networks. In these situations, routers are uniquely suited to filter packets because every packet between the two administrative domains must pass through the router. All the functionality for creating a complex security perimeter solution is contained within the Cisco IOS.

Cisco uses the term *Internetwork Operating System (IOS)* to designate the operatign system used by Cisco routers. The operating system on Cisco routers provides many of the same features of more traditional operating systems, lke Unix and Windows, but it also provides many especialized features. It controls the system hardware such as memory and interfaces, and also takes care of executing necessary system tasks like moving packets and building dynamic information suc as the routing and ARP tables.

One of the most powerfuls features of a Cisco router IOS is its capability to intelligently filter packets flowing between data networks. This capability is provided through the creation and application of access lists.

3.3.2 Cisco Access List Technology

An access list is an ordered list of statements denying of permitting packets based on matching criteria contained within the packet. An access list is an ordered list. In order words, the order in which the statements are created in an access list is very important. One of the most common mistakes made when creating access lists is entering the access list statements in an incorrect order.

Access list statements can either permit or deny packets. Additionally, it should be pointed out now that there is always an implicit "Deny All" statement at the end of a Cisco access list. A packet that is not explicitly permitted will be rejected by the implicit Deny All statement at the end of the access list. Another common mistake when creatign access lists is forgetting this fact.

Access-lists are processed sequentially starting from the top and working down. Each packet arriving at an interface with an access-list applied is checked against each line (rule) in the list until a match is made. Once a packet matches a rule it is either denied (dropped) or permitted in which case it will be routed to the next interface where it may be subject to a new access-list. Only one access-list may be applied to an interface in each direction for a total of two per interface.

An extended access list enables the flow of information to be controlled by both network address and the type of data being transferred within a packet. Extended access-lists are capable of filtering packets based on IP source and destination address, protocol, and protocol options.

Description of the Filter Syntax

access-list	Literal statement
access-list number	For extended access-lists, numbers 100-199 (inclusively) must be used. The configuration parser uses this number to determine how the information in the filter rule should be interpreted.
deny/permit	Specifies what action to take if the packet matches the stated criteria.
Protocol	Name or number of protocol
Source	Source IP address
Source-wildcard	32-bit quantity number in four-part, dotted-decimal format. This number is used to determine what part of the source IP address is used for matching. A "binary 1 bit" in a bit field indicates that the corresponding bit in the IP address is **not** tested for a match. For example, wildcard 255.255.255.255 doesn't care about any of the bits in the IP address. Wildcard 0.0.0.0, however, indicates that all bits in the IP address need to be matched.
destination	Destination IP address
destination-wildcard	Performs the same function as the source-wildcard, with the exception that it corresponds to the destination IP address.
protocol-option	Optional. Allows you to add criteria that is specific to the identified protocol. For example, when using TCP/UDP, an operator such as eq (equal), gt (greater than), range, etc. and then a port or port range can be specified. For ICMP, an example would be the specification of a particular ICMP type.
log	Optional. Enables logging to the system console when a match occurs (regardless of whether the packet was permitted or denied).

Once the access-lists have been written, they may be assigned to a specific interface. Just as with writing access-lists, applying access-lists to an interface is performed while in configuration mode. In order to apply an access-list to an interface, the following interface configuration command is used,

ip access-group *access-list-number* in/out

Description of Syntax

ip access-group	Literal statement
access-list-number	Represents the number of the access-list being applied to the interface.
in/out	Specifies whether the access-list will be applied to inbound or outbound packets (direction is in relation to the interface).

3.3.3 Screening Cisco Routers – Disabling Protocols and Services

Before developing a system policy in order to apply access lists, It will be necessary to harden Cisco routers from default services that can be exploited. The recommendations must be applied on both two Cisco routers #internet1 and #internet2.

- ***CDP – Cisco Discovery Protocol***

Cisco Discovery Protocol (CDP) is used for some network management functions, but is dangerous in that it allows any system on a directly-connected segment to learn that the router is a Cisco device, and to determine the model number and the Cisco IOS software version being run.

This information may in turn be used to design attacks against the router. CDP information is accessible only to directly connected systems.

The CDP protocol may be disabled with the global configuration command **no cdp running**. CDP may be disabled on a particular interface with **no cdp enable**.

- ***Finger Service***

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

The "finger" service may be disabled with the command:

no service finger

- ***Source Routing***

Source routing is a method of crafting a packet so that it goes through certain routers in an attempt to avoid other routers. This is typically done because a certain router may be blocking something that the initiator is trying to pass. In today's current internet environment, there is no legitimate reason that anyone would need to dictate what route a packet should take. Since we only route to and from our on private network, we should never get packets that route somewhere else via our router. Because of this, we will prevent all source routing on our router. IP source routing is disabled to prevent source-routed packets from entering the network. The loose source routing can be disabled with a single *no ip source-route* command."

no ip source-route

- ***UDP Small Servers and TCP Small Servers***

Some internetworking devices offer the "small services": echo, chargen, and discard. These services, especially their UDP versions, are infrequently used for legitimate purposes, but can be used to launch denial of service and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to some UDP echo port, the result would be the device sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

These services may be disabled using the following commands:

no service tcp-small-servers and ***no service udp-small-servers***

- ***HTTP Server***

Most recent software devices support remote configuration and monitoring using the World Wide Web's HTTP protocol. In general, HTTP access is equivalent to interactive access to the router.

The authentication protocol used for HTTP is equivalent to sending a cleartext password across the network, and, unfortunately, there is no effective provision in HTTP for challenge-based or one-time passwords. This makes HTTP a relatively risky choice for use across the public Internet.

If you choose to use HTTP for management, you should restrict access to appropriate IP addresses using the ip http access-class command. You should also configure authentication using the ip http authentication command. As with interactive logins, the best choice for HTTP authentication is probably to use a TACACS+ or RADIUS server. It's usually wisest to avoid using the "enable" password as an HTTP password.

The "http" service may be disabled with the command:

no ip http

- ***Logging***

Cisco routers can record information about a variety of events, many of which have security significance. Logs can be invaluable in characterizing and responding to security incidents. The main types of logging used by Cisco routers are:

- AAA logging, which collects information about user dial-in connections, logins, logouts, HTTP accesses, privilege level changes, commands executed, and similar events. AAA log entries are sent to authentication servers using the TACACS+ and/or RADIUS protocols, and are recorded locally by those servers, typically in disk files. If you are using a TACACS+ or RADIUS server, you may wish to enable AAA logging of various sorts; this is done using AAA configuration commands such as aaa accounting. Detailed description AAA configuration is beyond the scope of this document.

- SNMP trap logging, which sends notifications of significant changes in system status to SNMP management stations. You will probably want to use SNMP traps only if you have a preexisting SNMP management infrastructure.

- System logging, which records a large variety of events, depending on the system configuration. System logging events may be reported to a variety of destinations, including the following:

    - The system console port (logging console).
    - Servers using the UNIX "syslog" protocol (logging ip-address, logging trap).
    - Remote sessions on VTYs and local sessions on TTYs (logging monitor, terminal monitor).
    - A local logging buffer in router RAM (logging buffered).

From a security point of view, the most important events usually recorded by system logging are interface status changes, changes to the system configuration, access list matches, and events detected by the optional firewall and intrusion detection features.

Each system logging event is tagged with an urgency level. The levels range from debugging information (at the lowest urgency), to major system emergencies. Each logging destination may be configured with a "threshold" urgency, and will receive logging events only at or above that threshold.

3.3.4 #Internet1 Router Security Policy

⇨ To avoid spoof protection and provide security to Protected Subnet, filters were configured to inbond direction (Serial0) on Border Router. It´s defined as "Ingress Filters".

Spoofed Addresses / Source Routing Group of Rules (Ingress Access-List)

Rule #	Extended access-list	Permit / Deny	Protocol	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Deny	IP	1.1.1.0	0.0.0.255	Any		Log
2	Ingress	Deny	IP	1.1.2.0	0.0.0.255	Any		Log
3	Ingress	Deny	IP	1.1.3.0	0.0.0.255	Any		Log
4	Ingress	Deny	IP	1.1.4.0	0.0.0.255	Any		Log
5	Ingress	Deny	IP	1.1.5.0	0.0.0.255	Any		Log
6	Ingress	Deny	IP	10.0.0.0	0.255.255.255	Any		Log
7	Ingress	Deny	IP	172.16.0.0	0.15.255.255	Any		Log

8	Ingress	Deny	IP	192.168.0.0	0.0.255.255	Any		Log
9	Ingress	Deny	IP	127.0.0.0	0.255.255.255	Any		Log
10	Ingress	Deny	IP	224.0.0.0	31.255.255.255	Any		Log
11	Ingress	Deny	IP	240.0.0.0	15.255.255.255	Any		Log
12	Ingress	Deny	IP	serial.interface	0.0.0.0	serial.interface	0.0.0.0	Log
13	Ingress	Deny	IP	0.0.0.0	0.255.255.255	Any		Log

- Rules #1, #2, #3, #4 and #5are used to **Block "spoofed" addresses**-- packets coming from outside company sourced from internal addresses.
- Rule #6 denies access to any packet with a source address equal to the private class "A" address space.
- Rule #7 denies access to any packet with a source address equal to the private class "B" address space.
- Rule #8 denies access to any packet with a source address equal to the TEST-NET address space.
- Rule #9 denies access to any packet with a source address equal to the loop-back address space.
- Rule #10 denies access to any packet with a source address equal to the multicast address space.
- Rule #11 denies access to any packet with a source address equal to the IETF Reserved address space.
- Rule #12 prevents a *"Land Attack"* (connection established by router with itself into an infinite loop).
- Rule #13 denies access to any packet without ip address.

ICMP (Ingress Access-List)

Rule #	Extended access-list	Permit / Deny	Proto	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Deny	ICMP	Any		Any		log

- Rule #1denies ICMP traffic from entering the network.

Permit All Other Traffic (Ingress Access-List)

Rule #	Extended access-list	Permit / Deny	Proto	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Permit	IP	Any		Any		

- Rule #1 allows all other IP traffic from entering the network. It will be received by CheckPoint Firewall-1, the second line of perimeter defense.

⇨ To avoid spoof protection and control the source of packets that are leaving our network and ICMP traffic, filters were configured to inbond direction (Ethernet0) on Border Router. It´s defined as "Egress Filters".

Spoofed Addresses / Source Routing Group of Rules (Egress Access-List)

Rule #	Extented access-list	Permit / Deny	Protocol	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Egress	Permit	IP	1.1.1.0	0.0.0.255	Any		
2	Egress	Permit	IP	1.1.2.0	0.0.0.255	Any		

- Rule2 #1 and #2 are used to permit only IP traffic that has our valid address as the source address from leaving our router.

ICMP (Egress Access-List)

Rule #	Extented access-list	Permit / Deny	Protocol	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Egress	Deny	ICMP	Any		Any		Log

- Rule #1 denies all ICMP traffic from leaving the network.

Deny All Other IP Traffic (Egress Access-List)

Rule #	Extended access-list	Permit / Deny	Proto	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Deny	IP	Any		Any		Log

- Rule #1 denies all other traffic from leaving our network and generates logging of possible connection attempts.

3.3.5 #Internet2 Router Security Policy

⇨ Filters to inbond direction on Serial0 interface were defined as "Ingress Filters" and it is used to avoid spoof protection and provide security to LAN.

Spoofed Addresses / Source Routing Group of Rules (Ingress Access-List)

Rule #	Extended access-list	Permit / Deny	Protocol	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Deny	IP	1.1.1.0	0.0.0.255	Any		Log
2	Ingress	Deny	IP	1.1.2.0	0.0.0.255	Any		Log
3	Ingress	Deny	IP	1.1.3.0	0.0.0.255	Any		Log

4	Ingress	Deny	IP	1.1.4.0	0.0.0.255	Any		Log
5	Ingress	Deny	IP	1.1.5.0	0.0.0.255	Any		Log
6	Ingress	Deny	IP	10.0.0.0	0.255.255.255	Any		Log
7	Ingress	Deny	IP	172.16.0.0	0.15.255.255	Any		Log
8	Ingress	Deny	IP	192.168.0.0	0.0.255.255	Any		Log
9	Ingress	Deny	IP	127.0.0.0	0.255.255.255	Any		Log
10	Ingress	Deny	IP	224.0.0.0	31.255.255.255	Any		Log
11	Ingress	Deny	IP	240.0.0.0	15.255.255.255	Any		Log
12	Ingress	Deny	IP	serial.interface	0.0.0.0	serial.interface	0.0.0.0	Log
13	Ingress	Deny	IP	0.0.0.0	0.255.255.255	Any		Log

- Rules #1, #2, #3 and #4 are used to **Block "spoofed" addresses**-- packets coming from outside company sourced from internal addresses.
- Rule #6 denies access to any packet with a source address equal to the private class “A” address space.
- Rule #7 denies access to any packet with a source address equal to the private class “B” address space.
- Rule #8 denies access to any packet with a source address equal to the TEST-NET address space.
- Rule #9 denies access to any packet with a source address equal to the loop-back address space.
- Rule #10 denies access to any packet with a source address equal to the multicast address space.
- Rule #11 denies access to any packet with a source address equal to the IETF Reserved address space.
- Rule #12 prevents a *“Land Attack”* (connection established by router with itself into an infinite loop).
- Rule #13 denies access to any packet without ip address.

ICMP (Ingress Access-List)

Rule #	Extended access-list	Permit / Deny	Proto	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Deny	ICMP	Any		Any		log

- Rule #1denies ICMP traffic from entering the network.

Permit All Other Traffic (Ingress Access-List)

Rule #	Extended access-list	Permit / Deny	Proto	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Permit	IP	Any		Any		

- Rule #1 allows all other IP traffic from entering the network. It will be received by CheckPoint Firewall-1, the second line of perimeter defense.

⇨ To avoid spoof protection and control the source of packets that are leaving our network and ICMP traffic, filters were configured to inbond direction (Ethernet0) on Border Router. It´s defined as

"Egress Filters". This access-list is intended to filter traffic leaving network for the Internet.

Spoofed Addresses / Source Routing Group of Rules (Egress Access-List)

Rule #	Extented access-list	Permit / Deny	Protocol	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Egress	Permit	IP	1.1.3.0	0.0.0.255	Any		
2	Egress	Permit	IP	1.1.4.0	0.0.0.255	Any		

- Rules #1 and #2 are used to permit only IP traffic that has our valid address as the source address from leaving our router.

ICMP (Egress Access-List)

Rule #	Extented access-list	Permit / Deny	Protocol	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Egress	Deny	ICMP	Any		Any		Log

- Rule #1 denies all ICMP traffic from leaving the network

Deny All Other IP Traffic (Egress Access-List)

Rule #	Extended access-list	Permit / Deny	Proto	Source Address	Source Mask	Destination Address	Destination Mask	Options
1	Ingress	Deny	IP	Any		Any		Log

- Rule #1 denies all other traffic from leaving our network and generates logging of possible connection attempts.

3.3.6 Sample #Internet1 Router Config

```
version 12.0

no ip source-route
no cdp running
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip direct-broadcast
```

```
no ip unreachables
no ip http
no ip bootp

hostname #internet1

Interface Ethernet0
description CONNECTION TO DMZ
ip address 1.1.1.1 255.255.255.0
ip access-group egress in

access-list extended egress permit ip 1.1.1.0 0.0.0.255 any
access-list extended egress permit ip 1.1.2.0 0.0.0.255 any
access-list extended egress deny icmp any any log
access-list extended egress deny ip any any log

interface Serial0
 description CONNECTION TO THE INTERNET
 ip address serial interface ip
 ip access-group ingress in

access-list ingress deny ip host 0.0.0.0 any log
access-list ingress deny ip 10.0.0.0 0.255.255.255 any log
access-list ingress deny ip 172.16.0.0 0.15.255.255 any log
access-list ingress deny ip 192.168.0.0 0.0.255.255 any log
access-list ingress deny ip 1.1.1.0 0.0.0.255 any log
access-list ingress deny ip 1.1.2.0 0.0.0.255 any  log
access-list ingress deny ip 1.1.3.0 0.0.0.255 any log
access-list ingress deny ip 1.1.4.0 0.0.0.255 any log
access-list ingress deny ip 1.1.5.0 0.0.0.255 any log
access-list ingress deny ip 127.0.0.0 0.255.255.255 any log
access-list ingress deny ip 224.0.0.0 31.255.255.255 any log
access-list ingress deny ip 240.0.0.0 15.255.255.255 any log
access-list ingress deny ip serial interface mask serial interface ip mask log
access-list ingress deny icmp any any log
access-list ingress permit ip any any

logging 1.1.2.9
```


3.3.7 Sample Output of #Internet2 Router Config

```
version 12.0

no ip source-route
no cdp running
no service tcp-small-servers
no service udp-small-servers
no service finger
```

```
no ip direct-broadcast
no ip unreachables
no ip http
no ip bootp

hostname #internet1

Interface Ethernet0
description CONNECTION TO DMZ
ip address 1.1.3.1 255.255.255.0
ip access-group egress in

access-list extended egress permit ip 1.1.3.0 0.0.0.255 any
access-list extended egress permit ip 1.1.4.0 0.0.0.255 any
access-list extended egress deny icmp any any log
access-list extended egress deny ip any any log

interface Serial0
description CONNECTION TO THE INTERNET
 ip address serial interface ip
 ip access-group ingress in

access-list ingress deny ip host 0.0.0.0 any log
access-list ingress deny ip 10.0.0.0 0.255.255.255 any log
access-list ingress deny ip 172.16.0.0 0.15.255.255 any log
access-list ingress deny ip 192.168.0.0 0.0.255.255 any log
access-list ingress deny ip 1.1.1.0 0.0.0.255 any log
access-list ingress deny ip 1.1.2.0 0.0.0.255 any  log
access-list ingress deny ip 1.1.3.0 0.0.0.255 any log
access-list ingress deny ip 1.1.4.0 0.0.0.255 any log
access-list ingress deny ip 1.1.5.0 0.0.0.255 any log
access-list ingress deny ip 127.0.0.0 0.255.255.255 any log
access-list ingress deny ip 224.0.0.0 31.255.255.255 any log
access-list ingress deny ip 240.0.0.0 15.255.255.255 any log
access-list ingress deny ip serial interface mask serial interface ip mask log
access-list ingress deny icmp any any log
access-list ingress permit ip any any

logging 1.1.2.9
```


3.4 Perimeter Security – Security Policy on Firewalls

3.4.1 Introduction to CheckPoint Firewall-1 Rulebase

The Check Point Policy Editor enables an enterprise to easily define a comprehensive Security Policy. A VPN-1/FireWall-1 Security Policy is defined in terms of a Rule Base and Properties.

A Rule Base is an ordered set of rules against which each communication is checked. Each rule specifies the source, destination, service and action to be taken for each communication — for example, whether it is permitted or denied. A rule also specifies how a communication is tracked — for example, a specific event can be logged and then trigger an alert message.

VPN-1/FireWall-1's scalable, modular architecture enables an organization to define and implement a single, centrally managed Security Policy. The enterprise Security Policy is defined at a central management console and downloaded to multiple enforcement points throughout the network.

The Firewalls Security Polity is explained in details in the following sections. Although many of the deny rules could have been accounted for simply by using the "ANY, ANY, deny and log" rule, they have been explicitly stated to illustrate how they would be created.

3.4.2 Firewalls Security Policy – Implied Rules (Rule0)

Rule 0 : Implied Rules (System Properties) – Same for both Firewalls.

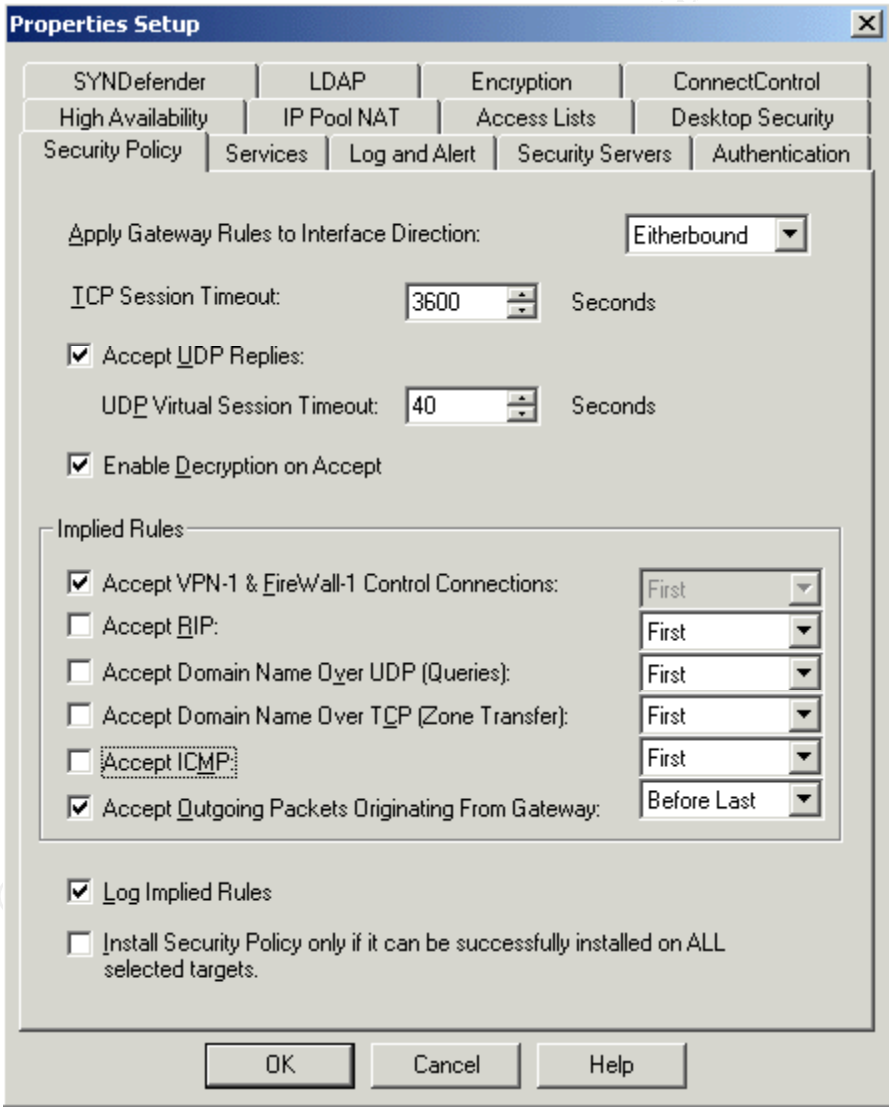
A Security Policy is defined not only by the Rule Base, but also by the properties specified in the various tabs of the Properties Setup window.

These properties enable the user to control all aspects of a communication's inspection, while at the same time freeing the user of the need to specify repetitive detail in the Rule Base.

Properties specify general aspects of communication inspection, such as authentication session timeout periods, or how VPN-1/FireWall-1 handles established TCP connections.

Properties are applied to all rules, so there is no need to specify repetitive details in the Security Policy.

Rule 0 has the same configuration for both Firewalls (Firewall-1_FW1 and Firewall-1_FW2).



- ***Apply Gateway Rules to Interface Direction***
  This property specifies the communication direction in which rules will be enforced when they are Installed.

  Eitherbound - Enforce the Security Policy on packets entering and leaving the gateway. This option gives added

protection, as packets passing through the gateway are examined twice: once on the external interface and again on the internal interface.

- ***TCP Session Timeout***
  A TCP session will be considered to have timed out after this period.

  TCP Session Timeout is configured to ***3600 seconds.***

- ***Accept UDP Replies***
  Accept reply packets in a two-way UDP communication.

  A UDP communication sets up a two-way communication between the source and the destination; that is, when the communication is established between the source and the destination, a reply channel is also created between the destination and the source.

  When a UDP communication is accepted on the destination and Accept UDP Replies is enabled, the reply channel is allowed. Only packets from the destination host going to the source host and source port are accepted as part of
  this communication.

- ***UDP Virtual Session Timeout***
  Specifies the amount of time a UDP reply channel may remain open without any packets being returned.

  Since the communication is connectionless, there is no way to inform the reply channel when the communication has finished. VPN-1/FireWall-1 creates a connection context for UDP. Once the specified time has elapsed,
  the session is assumed to have ended and the reply channel is closed.

  UDP Virtual Session Timeout is configured to ***40 seconds.***

- ***Enable Decryption on Accept***
  Decrypt incoming accepted packets even if the rule does not include encryption.

  This option is selected and if a rule allows an unencrypted incoming connection, the rule will not reject the connection if it is encrypted. The motivation for this option is that encryption adds security, and a connection that
  would be accepted if it were not encrypted should not be rejected only because its security has been improved.

- ***Accept VPN-1 & FireWall-1 Control Connections***
  VPN-1/FireWall-1 uses these connections communications between FireWall daemons on different machines, and for connecting to external servers such as RADIUS, TACACS, *et*c.

  The option has been enabled to provide control connections to Firewall-1 daemon port and the Management Server port, allowing VPN-1/FireWall-1 GUI Clients to communicate with the Management Server. I

- ***Accept RIP***
  Accept Routing Information Protocol used by the routed daemon RIP maintains information about reachable systems and the routes to those systems.

  The ACCEPT RIP option has not been selected.

- ***Accept Domain Name Over UDP (Queries)***
  Accept Domain Name Queries used by named.

  Named resolves names by associating them with their IP address. If named does not know the IP address associated with a particular host name, it issues a query to the name server on the Internet.

  This option has been disabled and should not be used as default A secure way is to create a specific rule and accept DNS queries destinated to Primary DNS Server on Protected Subnet only.

- ***Accept Domain Name Over TCP (Zone Transfer)***
  Allow uploading of domain name-resolving tables.

  Tables of Internet host names and their associated IP addresses and other data can be uploaded from designated servers on the Internet.

  This option has been disabled and should not be used as default A secure way is to create a specific rule and accept Zone Transfers from Secondary DNS Server only.

- ***Accept ICMP***
  Accept Internet Control Messages.

  ICMP (Internet Control Message Protocol) is used by IP for control messages (for example, destination unreachable, source quench, route change) between systems.

  This option has been disabled. The Firewall-1 is configured to not accept ICMP Control Messages by default.

- ***Accept Outgoing Packets Originating from Gateway***
  Accept all outgoing packets (from the FireWall, not from the internal network).

  On gateways, rules are usually enforced in the inbound direction only. When a packet passing through the gateway leaves the gateway, it will be allowed to pass only if one the Accept Outgoing Packets Originating from Gateway property is checked or if rules are enforced both directions (eitherbound), and there is a rule which allows the packet to leave the gateway.

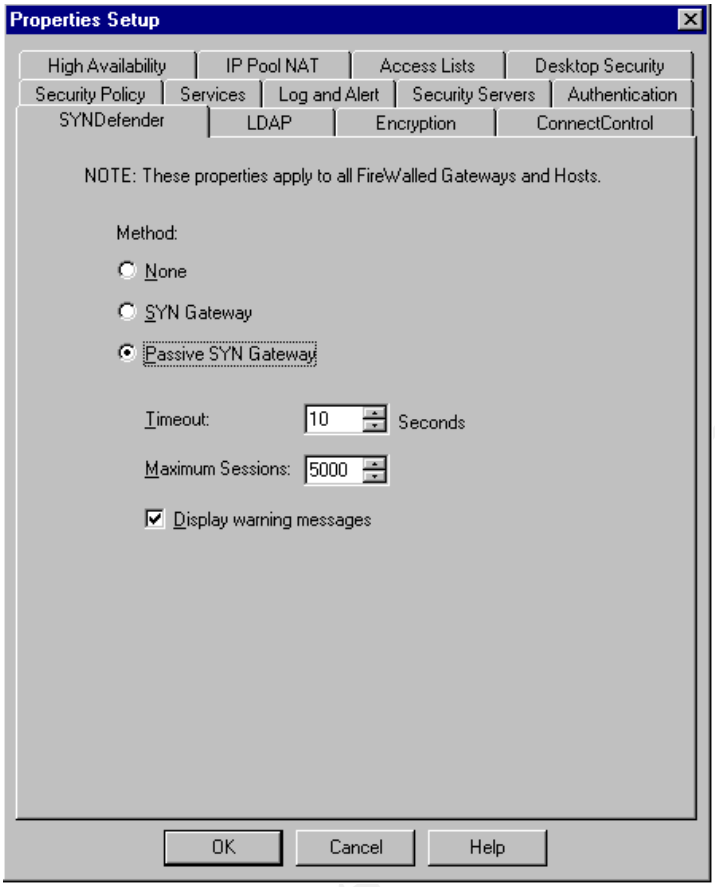
- ***Log Implied Rules***

  Log the connections to which implied rules (the rules shown when Implied Rules has been selected in the View menu) are applied. This options is checked in order to log events originated from Implied Rules.

3.4.3 Firewalls Security Policy – SYN Defender Gateway

SYN Defender Rule - Same for both Firewalls.

The SYN Defender provides approaches for defending against a SYN flooding attack. The SYN flooding atack workds by sending SYN packets with the source adress of unreachable hosts which would no reply the SYN/ACK packets.



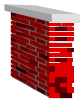
In order for resetting of SYN connection attempts to be effective against SYN flooding attack, the reset timer must be small enough to keep A´s backlog queue from filling up , while at the same time being large enough to allow users coming over slow links to connect. The SYN Defender Gateway solutions surmounts this problem by making sure that an ACK packet is sent in immediate response to A´s SYN/ACK packet. When A receives the ACK packet, the connection is moved out of the backlog queue and becomes an open connection on A.

Internet servers can typically handle hundreds or thousands of open connections, so the SYN flooding attack is no more effective in creating a denial of service condition than a hacker trying to estabilish an excessive number of valid connection to the server.

The backlog queue is effectively kept clear and it is possible to wait longer before ressetting connections which have not been completed.

Syn Gateway has been configured as Passive mode with timeout of 10 seconds

3.4.4 Firewalls Rulebase Objects Description



Description of Rulebase Objects Used by Firewall-1_FW1 and Firewall-1_FW2

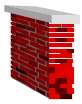
Object Name	Firewall-1 Object Type	IP Address	Description
Firewall-1_FW1	Workstation (Gateway)	1.1.1.1	CheckPoint Firewall-1 4.1 SP3 runs under Windows NT Server 4.0 on a dual Intel Pentium III 700 / 256 MB RAM system. It provides security to Protected Subnet.
Firewall-1_FW2	Workstation (Gateway)	1.14.1	CheckPoint Firewall-1 4.1 SP3 runs under Windows NT Server 4.0 on a dual Intel Pentium III 700 / 256 MB RAM system.
WebServer	Workstation (Host)	1.1.2.2	The web server provides public access to corporate web site. It's a Apache HTTP server running under RedHat Linux 7.0 on a Intel Pentium III 500 / 256 MB RAM system.
Customer_WebServer	Workstaion (Host)	1.1.2.3	The web server provides secure customers access for on-line shopping. It's a Apache 1.3.17 with SSL-enabled running under RedHat Linux 7.0 on a Intel Pentium II 500 256 MB RAM system.
Suppliers_WebServer	Workstaion (Host)	1.1.2.4	The web server provides secure suppliers access for trading. The access is provided by VPN (secure remote) and the server runs Apache 1.3.17 with SSL-enabled under RedHat Linux 7.0 on a Intel Pentium II 500 256 MB RAM system.
Partners_WebServer	Workstaion (Host)	1.1.2.5	The web server provides secure parrtners access for trading and relationship. The access is provided by VPN (secure remote) and the server runs Apache HTTP with SSL-enabled under RedHat Linux 7.0 on a Intel Pentium II 500 256 MB RAM system.
MailServer	Workstation (Host)	1.1.2.6	Corporate mail server. The server provides POP3 access through SSL (Secure POP3) and It's responsible to receive and send Internet mail (SMTP). It's a RedHat Linux running Sendmail 8.11.2 on a Intel Pentium II 500 256 MB RAM system
SyslogServer	Workstation (Host)	1.1.2.9	RedHat Linux 7.0 that centralizes all critical logging from other Unix Servers, border routers and IPChains Firewall (used to provide security from dialin users). It´s powered by Intel Pentium II 500 256 MB RAM system.
Primary_DNS	Workstation (Host)	1.1.2.7	Primary corporate Domain Name Server. It's a RedHat Linux 7.0 running **Bind 9.1.0 *** on a Intel Pentium II 500 256 MB RAM system.
Internal_DNS	Workstation (Host)	1.1.4.4	Internal Domain Name Server. It's a RedHat Linux 7.0 running **Bind 9.1.0 *** on a Intel Pentium II 500 256 MB RAM system.
IDS1	Worskstation (Host)	1.1.1.3	The Intrusion Detection System is a SNORT 1.6.3 running under RedHat Linux 7. It listens on Subnet 1.1.1.0. The hardware is powered by Pentium II 500 256 MB RAM system.

IDS2	Workstaion (Host)	1.1.2.10	The Intrusion Detection System is a SNORT 1.6.3 running under RedHat Linux 7. It listens on Subnet 1.1.2.10. The hardware is powered by Pentium II 500 256 MB RAM system.

Object Name	Firewall-1 Object Type	IP Address	Description
IDS3	Workstaion (Host)	1.1.5.4	The Intrusion Detection System is a SNORT 1.6.3 running under RedHat Linux 7. It listens on Core Subet 1.1.5.0 and the hardware is also powered by Pentium II 500 256 MB RAM system.
IDS4	Workstaion (Host)	1.1.3.3	The Intrusion Detection System is a SNORT 1.6.3 running under RedHat Linux 7. It listens on DMZ Subnet 1.1.3.0 and the hardware is powered by Pentium II 500 256 MB RAM system.
IDS4	Workstaion (Host)	1.1.3.3	The Intrusion Detection System is a SNORT 1.6.3 running under RedHat Linux 7. It listens on DMZ Subnet 1.1.3.0 and the hardware is powered by Pentium II 500 256 MB RAM system.
IDS5	Workstaion (Host)	1.1.4.2	The Intrusion Detection System is a SNORT 1.6.3 running under RedHat Linux 7. It listens on Internal Subnet 1.1.4. and the hardware is also powered by Pentium II 500 256 MB RAM system.
Internet1	Router	1.1.1.1	Cisco 3600 router #Internet1, receives inbound traffic destinated to Protected Network.
Internet2	Router	1.1.3.1	Cisco 3600 router Internet2, receives inbond traffic from LAN destinated to Internet.
LAN_Subnet	Network	1.1.4.0	It's the corporate Local Area Network Subnet.
Protected_Subnet	Network	1.1.2.0	It's the Protected SubNet.
Core_Subnet	Network	1.1.5.0	It´s the core Subnet. It supports all traffic between Protected Subnet and Lan SubNet. It also provides dial-in access to remote users.
FWIPCHains	Workstation (Host)	1.1.5.3	RedHat Linux 7.0 running IPCHains 1.3.9 on a Intel Pentium II 500 256 MB RAM system. It provides protection from Dialin Users
Oracle_DB_Server	Workstation (Host)	1.1.2.8	Oracle database server (Oracle 8) running under Sun Solaris 8.0 on a dual Intel Pentium III 700 / 1 GB RAM system.
Network_Admins	Group	----------	Admin group contains IP address of authorized machines that will manage servers on Protected Subnet.

3.4.5 Firewall-1_FW1 Policy

This section contains general description of each rule created in Firewall-1_FW1 Rulebase. It explains the contents of each rule. The rules will be tested on section ***4.0 – System Audit.***



Rule 1 : Lockdown FW-1

No.	Source	Destination	Service	Action	Track	Install On
1	Any	Firewall-1_FW1	Any	drop	Alert	Gateways

- Deny traffic directly to the firewall. (lock-down rule). Attempts to connect to the firewall drops the packet, and alerts the operator of the connection attempt. The firewall does not provide services other than screening packets and enforcing the policy. This is positioned right at the start to ensure that no other rules would allow traffic to the firewall before this one is matched. This rule effectively notifies of any attempts to gain access to FW-1 by intruders or the curious. The attempt generates an alert to the operator.

Rule 2 : Web Server

No.	Source	Destination	Service	Action	Track	Install On
2	Any	WebServer	http	accept	Long	Gateways

- HTTP traffic from Internet, LAN Subnet and Core SubNet (Dial-In Users) will be allowed in order to provide public web access to corporate web site. This rule is the very first permit rule to try and enhance rule base performance. It generates logging (tracking) of succesfull connection attempts.

Rule 3 : E-Commerce Web Server (Customers)

No.	Source	Destination	Service	Action	Track	Install On
3	Any	Customer_WebServer	http https	accept	Long	Gateways

- HTTP and HTTPS traffic from Internet, LAN Subnet and Core SubNet (Dial-In Users) will be allowed in order to provide public web access to customers for on-line shopping. It generates logging (tracking) of succesfull connection attempts.

Rule 4 : VPN To E-Commerce Web Server (Suppliers)

No.	Source	Destination	Service	Action	Track	Install On
4	Suppliers@Any	Suppliers_WebServer	http https	Client Encrypt	Long	Gateways

- This rule provides VPN access to Suppliers. Once connection is established, It will provide HTTP and HTTPS traffic from anywhere to Suppliers Web Server for trading. Suppliers must use Secure Remote Client in order to exchange keys and authenticate for Secure Remote access. The Firewall has a database of users/passwords that will be used in order to provide user authentication It generates logging (tracking) of succesfull connection attempts.

Refer to section 3.4.7 – VPN Policy. It contains complete information about VIRTUAL PRIVATE NETWORK Technology with explanations about crypto schemes, rules and Secure Remote Software operation.

Rule 5 : VPN To E-Commerce Web Server (Suppliers)

No.	Source	Destination	Service	Action	Track	Install On
5	Partners@Any	Partners_WebServer	http https	Client Encrypt	Long	Gateways

- This rule provides VPN access to Partners. Once connection is established, It will provide HTTP and HTTPS traffic from anywhere to Partners Web Server for trading and relationship. Parnets must use Secure Remote Client in order to exchange keys and authenticate for Secure Remote access. The Firewall has a database of users/passwords that will be used in order to provide user authentication. It generates logging (tracking) of succesfull connection attempts.

Refer to section 3.4.7 – VPN Policy. It contains complete information about VIRTUAL PRIVATE NETWORK Technology with explanations about crypto schemes, rules and Secure Remote Software operation.

Rule 6 : Mail Server Inbound

No.	Source	Destination	Service	Action	Track	Install On
6	Any	MailServer	smtp SecurePOP3	accept	Long	Gateways

- Rule allows mail delivery to corporate mail server. It also allows employees to check mail from outside company (Internet) or from company´s LAN. The POP3 connection is safe because It avoids clear POP3 traffic. The mail is received under a secure SSL POP connection (port 995) and there is no risk of password discovery. It generates logging (tracking) of succesfull connection attempts.

Rule 7 : Mail Server Outbound

No.	Source	Destination	Service	Action	Track	Install On
7	MailServer	Any	smtp	accept	Long	Gateways

- Mail server is allowed to start connections from inside Protected Subnet to deliver mail on Internet. It provides Sendmail mail delivery to outside MX servers in order to exchange mail. It´s the only server allowed to start connections to outside Protected Subnet. It generates logging (tracking) of succesfull connection attempts.

Rule 8 : DNS Zone Transfer

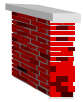
No.	Source	Destination	Service	Action	Track	Install On
8	Secondary_DNS	Primary_DNS	domain-tcp	accept	Long	Gateways

- Secondary DNS is allowed to send TCP PORT 53 packets to Primary DNS on Protected Subnet in order to process DNS zone transfers. It´s the only server allowed to transfer zone maps. It generates logging (tracking) of succesfull connection attempts.

Rule 9 : DNS Queries

No.	Source	Destination	Service	Action	Track	Install On
9	Any	Primary_DNS	domain-udp	accept	Long	Gateways

- The rule allows inbound *DNS traffic to Primary Name Server on UDP port 53* for domain queries. It generates logging (tracking) of succesfull connection attempts.



Rule 10 : LAN SubNet To Oracle Database Server

No.	Source	Destination	Service	Action	Track	Install On
10	LAN_Subnet	Oracle_DB_Server	SSH sqlnet1	accept	Long	Gateways

- Users on Local Area Network subnet are allowed to connect Oracle Database Server on Protected Subnet in order to secure telnet (SSH) Unix server for terminal emulation and to retrieve informations from database using SQLNET Oracle protocol. The rule also generates logging (tracking) of succesfull connection attempts.

Rule 11 : Network Admin – Management of Unix Servers

No.	Source	Destination	Service	Action	Track	Install On
11	Network_Admin	Customer_WebServer MailServer Partners_WebServer Primary_DNS Suppliers_WebServer WebServer SyslogServer IDS1 IDS2	SSH	accept	Long	Gateways

- Group of Network Administrators can connect to Unix Servers from Local Area Network Subnet (1.1.4.0) to DMZ Subnet (1.1.1.0) and Protected Subnet (1.1.2.0) through secure telnet (SSH) in order to provide system management and maintenance. The rule generates logging (tracking) of succesfull connection attempts.

Rule 12 : Network Admin – Management of #INTERNET1 Router

No.	Source	Destination	Service	Action	Track	Install On
12	Network_Admin	Internet1_Cisco	telnet	accept	Long	Gateways

- Group of Network Administrators can connect to router #Internet1 in order to provide router management and maintenance. The rule also generates logging (tracking) of succesfull connection attempts.

Rule 13 : Logging – Syslog Server

No.	Source	Destination	Service	Action	Track	Install On
13	FWIpchains IDS1 IDS3 IDS4 IDS5 Internet1_Cisco Internet2_Cisco	SyslogServer	syslog	accept	Long	Gateways

- The rule allows Syslog traffic to Syslog server on Protected Subnet in order to centralize information about a variety of events that have security significance. The events are generated by the Intrusion Detection Systems (Snort), Cisco router devices and Ipchains firewall.

Rule 14 : DROP Login Services

No.	Source	Destination	Service	Action	Track	Install On
14	Any	Protected_Subnet	Login_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Login_Services*** contains and blocks telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), and the r-services rlogin et al (512/tcp through 514/tcp) traffic destinated to Protected Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 15 : DROP RPC and NFS Services

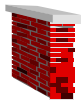
No.	Source	Destination	Service	Action	Track	Install On
15	Any	Protected_Subnet	RPC_NFS_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***RPC_NFS_Services*** contains and blocks Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) traffic destinated to Protected Subnet from anywhere The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 16 : DROP Netbios Services

No.	Source	Destination	Service	Action	Track	Install On
16	Any	Protected_Subnet	Netbios_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Netbios_Services*** contains and blocks 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 earlier ports plus 445 (tcp and udp) traffic destinated to Protected Subnet from anywhere The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.



Rule 17 : DROP Xwindows Range

No.	Source	Destination	Service	Action	Track	Install On
17	Any	Protected_Subnet	XWindows_Range	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service ***Xwindows_Range*** contains and blocks 6000-6250/tcp traffic destinated to Protected Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 18 : DROP Naming Services

No.	Source	Destination	Service	Action	Track	Install On
18	Any	Protected_Subnet	Naming_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Naming_Services*** contains and blocks 53 (tcp and udp), 389 (tcp and udp) traffic destinated to Protected Subnet from anywhere . The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 19 : DROP Mail Services

No.	Source	Destination	Service	Action	Track	Install On
19	Any	Protected_Subnet	Mail_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service ***Mail_Services*** contains and blocks 25/TCP, 109/TCP and 110/TCP traffic destinated to Protected Subnet from anywhere . The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 20 : DROP Web Services

No.	Source	Destination	Service	Action	Track	Install On
20	Any	Protected_Subnet	Web_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Web_Services*** contains and blocks 80/TCP, 443/TCP, 8000/TCP, 8080/TCP and 8888/TCP traffic destinated to Protected Subnet from anywhere The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 21 : DROP Small Servicess

No.	Source	Destination	Service	Action	Track	Install On
21	Any	Protected_Subnet	Small_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Small_Services*** contains and blocks all the TCP and UDP services below 20 and 37/tcp and 37/udp traffic destinated to Protected Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 22 : DROP Misc Services

No.	Source	Destination	Service	Action	Track	Install On
22	Any	Protected_Subnet	Misc_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp traffic destinated to Protected Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 23 : REJECT Traffic Between Subnets

No.	Source	Destination	Service	Action	Track	Install On
23	Protected_Subnet	LAN_Subnet	Any	reject	Alert	Gateways

- This rule explicitly denies connections from Protected Subnet to LAN (Local Area Network) Assuming the case that a intruder has compromised one of the systems on Protected Subnet, any connection attempts from Protected Subnet to Lan Subnet will be rejected. An alert is also generated to notify the security staff.

Rule 24 : REJECT Traffic Between Subnets

No.	Source	Destination	Service	Action	Track	Install On
24	LAN_Subnet	Protected_Subnet	Any	reject	Alert	Gateways

- This rule explicitly denies connections from Lan Subnet to Protected Subnet. Any connection attempts from Protected Subnet to Lan Subnet will be rejected. An alert is also generated to notify the firewall operator. Log everything so there is a audit trail.

Rule 25 : Silent Drop Rule (Broadcast)

No.	Source	Destination	Service	Action	Track	Install On
25	Any	Any	SilentServices	drop		Gateways

- As a precaution any broadcast traffic originating from any source is dropped. It is not essential or even desirable to forward any broadcast so for that reason we drop them all.

Rule 26 : Last Rule (Explicit Deny ANY-ANY)

No.	Source	Destination	Service	Action	Track	Install On
26	Any	Any	Any	drop	Alert	Gateways

- The explicit deny all and log rule. Useful to see what other kind of traffic is attempting to access resources. This rule is always the very last one. (Clean up rule). It´s important to log and generate alert to security staff because the rule can probe for weakness in our policy,

3.4.6 Firewall-1_FW1 VPN Policy

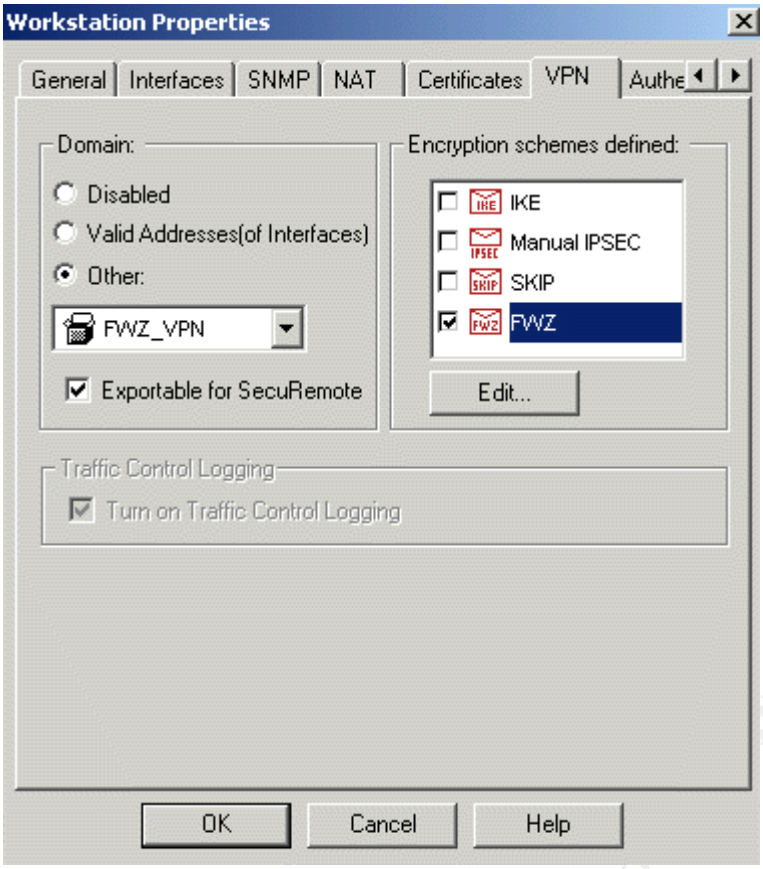
Check Point VPN-1 SecuRemote enables PC users to securely communicate sensitive and private nformation to networks and individual servers. Check Point VPN-1 SecuRemote extends the VPN to Windows 9x and Windows NT workstations and desktops, using both dial-up and LAN connections.

VPN-1 SecuRemote is based on a technology called Client Encryption. Because SecuRemote encrypts data before it leaves the computer, it offers a completely secure solution for remote connections.

VPN-1 SecuRemote can transparently encrypt any TCP/IP communication. There is no need to change any of the existing network applications on the user's PC. SecuRemote can interface with any existing adapter and TCP/IP stack. A PC on which SecuRemote is running can be connected to several different VPN-1/FireWall-1 sites.

A VPN-1/FireWall-1 security manager can enable access for SecuRemote users with the standard VPN-1/FireWall-1 Rule Base editor. After a SecuRemote user is authenticated, a completely transparent secured connection is established and the user is treated just as any user in the Virtual Private Network. The network administrator can enforce VPN-1/FireWall-1 security features, including authentication servers, logging and alerts, on SecuRemote connections (just as with any other connection).

First off all, it´s necessary to ***Specify Encryption*** that will be used to protect the environment :



- ***Who will encrypt?***
  It´s necessary to define the encrypting gateways and their encryption domains.

- ***What are the encryption keys?***
  On the Management Station, generate the Diffie-Hellman keys for the encrypting gateway and its CA or obtain the certified keys from the remote gateways or Certificate Authorities.

- ***What will be encrypted?***
  Add a rule (or rules) to the Rule Base specifying encryption.

- ***Which encryption scheme will be used?***
  Specify the encryption scheme in the rule. The scheme must be one that both parties to the encryption can implement.

For the Practical Assignment, the firewall object (***Firewall-1_FW1***) is set to ***FWZ Encryption***.

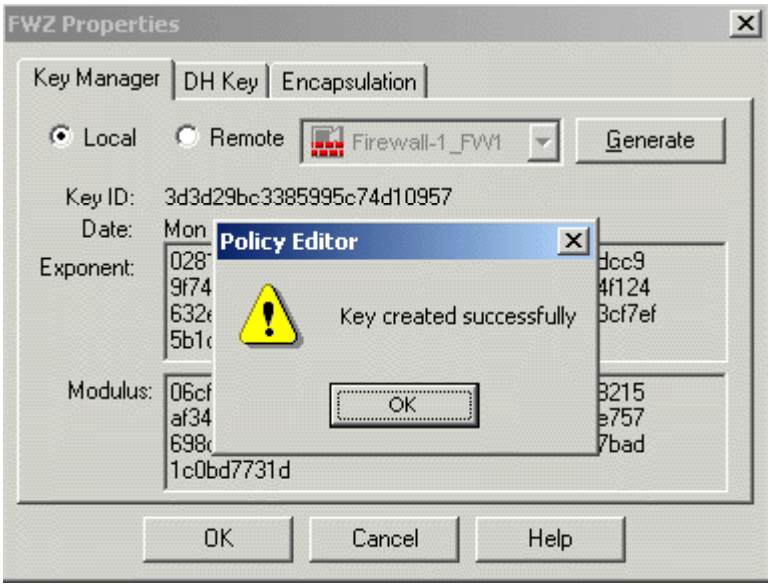
Under the VPN-1/FireWall-1 encryption scheme (FWZ), a message is encrypted with a secret key derived in a secure manner from the correspondents' Diffie-Hellman keys. The Diffie-Hellman keys are authenticated by a Certificate Authority.
Under this scheme, the number of keys that must be managed is proportional to the number of correspondents. This is in contrast to some other schemes, in which the number of keys to be managed is proportional to the square of the number of correspondents.

The TCP/IP packet headers are not encrypted, to ensure that the protocol software will correctly handle and deliver the packets. The cleartext TCP/IP header is combined with the session key to encrypt the data portion of each packet, so that no two packets are encrypted with the same key.

A cryptographic checksum is embedded in each packet (utilizing otherwise unused bits in the header) to ensure its data integrity.

Encryption is in–place. A packet's length remains unchanged, so the MTU remains valid and efficiency is not compromised.

FWZ Encryption will be used to secure communications to *Encryption Domain* ***FWZ_VPN.*** The group ***FWZ_VPN*** has been created in order to specify servers for which the gateway performs encryption.

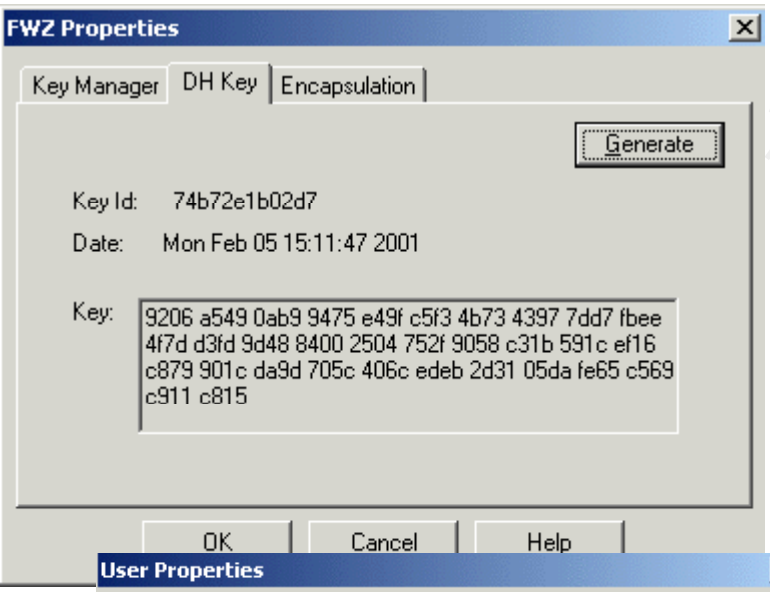


Group ***FWZ_VPN*** has the two servers that will be avaiable for ***Secure Remote*** access (***Parnets_WebServer*** and ***Suppliers_WebServer***)

The next step will be the Certificate Authority and key management specifications. Two keys must be generated. The Firewall-1 CA is being used to generate the new management sign key and the ***DH KEY.***

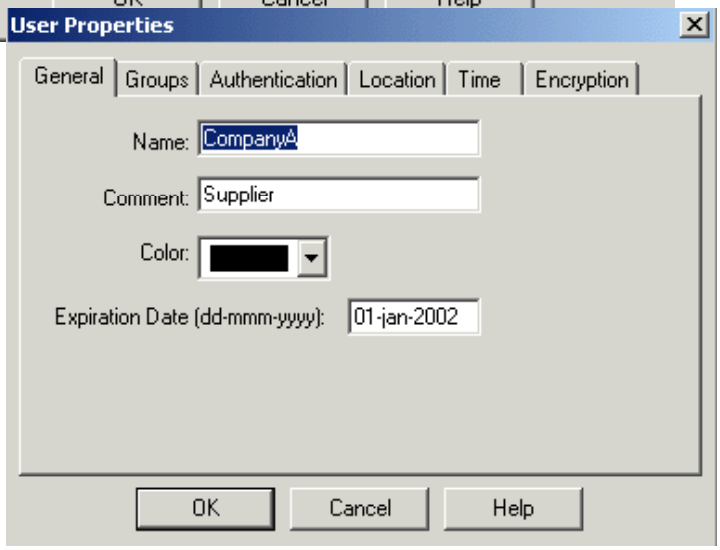
A ***Diffie-Hellman*** public-private key pair is used for calculating a secret key, which is in turn used for encrypting and decrypting messages.

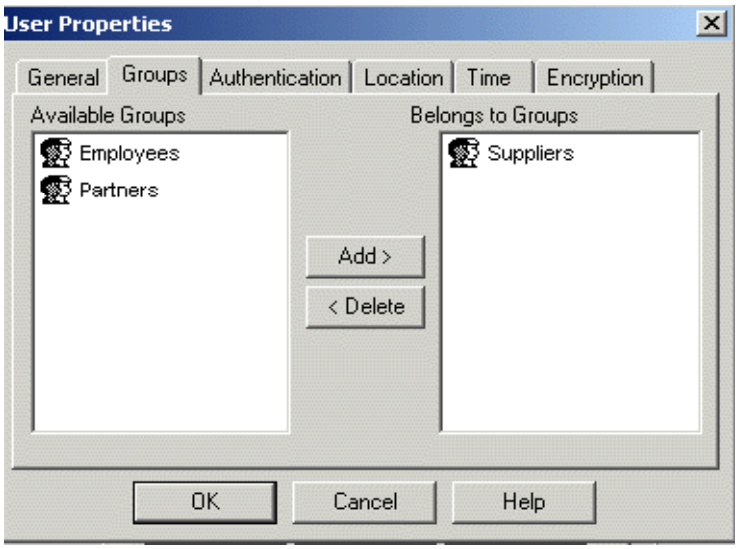
No secret information is communicated during the key exchange, so it does not require a secure channel.



Only one key pair needs to be managed for each correspondent (instead of one key for each pair of correspondents). The correspondents compute a shared secret key, which they use to encrypt and decrypt messages between them.

After creating the keys it will be necessary to create the users that will be used to authenticate on Firewall in order to establish de VPN.

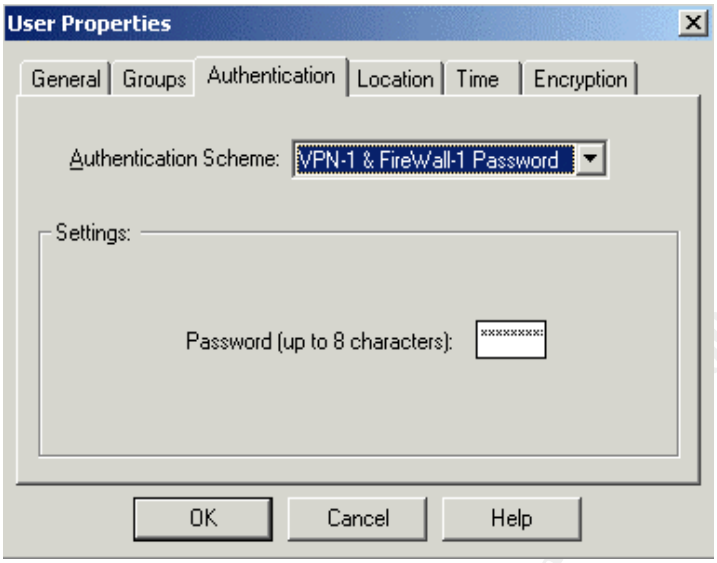


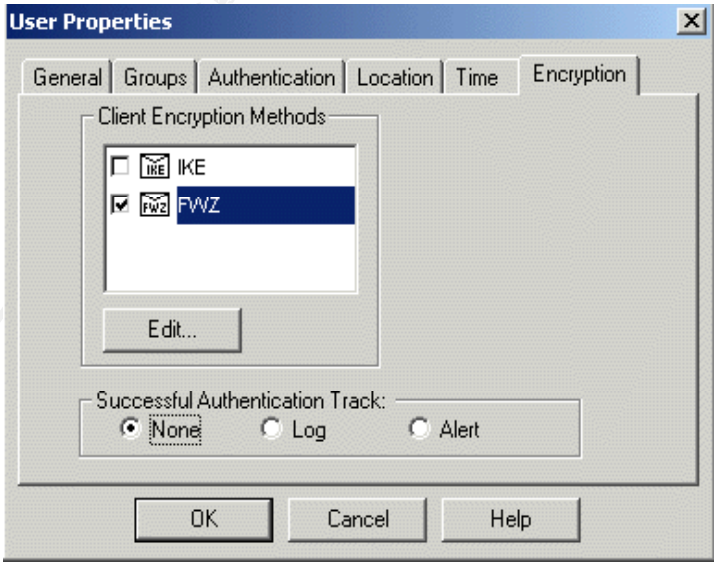


User *CompanyA* is a user that has been created in Firewall-1 user database and supports VPN/Firewall-1 OS authentication scheme.

The *General tab* of user properties provides fields to identify user name, comments and expiration date of account. The expiration date is the date after which the user will be denied access.

User CompanyA has an expiration date of 01jan-2002 and has been added to *Suppliers* group and the *authentication scheme is* FireWall-1 Password – (The user is challenged to enter his or her internal FireWall-1 password on the gateway) was chosen.





The Encryption tab of the User Properties window defines the Client Encryption properties for the user. The IKE and FWZ are schemes are supported for Client Encryption.

FWZ Encryption Scheme has been chosen.

FWZ means any of the authentication schemes supported on the server side. In the password window, the user enters user name an password, in accordance with the authentication scheme specified in the Authentication tab of the User Properties Windows.

Rule #4 allows any user that belongs to group *Suppliers* to provide username and password in order to authenticate on Firewall. The password must be provided when initiating a communication with *Suppliers_WebServer.* On the user´s first attempt to connect to *Suppliers_WebServer*, the password windows will appear, as shown in the above picture. When user name and password is entered, the *Secure Remote daemon* will remember them and use them next time it initiates a connection with the host.

When user *CompanyA* tries to connect to Suppliers_WebServer on Protected Subnet for web access (HTTP port 80 or HTTPS port 443) ***Secure Remote Client*** requests user name and password in order to authenticate for access.

As soon as the user provides its user name and password, the connection will be established and ***Secure Remote Client*** will confirm the success of authentication procedure. The same procedure is applied to rule #5, when users that are in *Partners* group exchange keys with Firewall host and provide username and password, the access will be authenticated and HTTP/HTTPS connection to *Partners Web Server* will be established.

Rule #	Source	Destination	Service	Action	Track
4	SUPPLIERS@ANY	SUPPLIERS_WEBSERVER	HTTP HTTPS	CLIENT ENCRYPT	LONG
Rule #	Source	Destination	Service	Action	Track
5	PARTNERS@ANY	PARTNERS_WEBSERVER	HTTP HTTPS	CLIENT ENCRYPT	LONG

Firewall-1_FW1 Security Policy will allow only users that are members of groups *Suppliers* or *Partners* coming from anyplace to access the web servers for trading and e-commerce. Only authenticated users will be able to connect to the web servers that are in these two rules. It´s a ***Secure VPN tunnel.***

3.4.7 Firewall-1_FW2 Policy

This section contains general description of each rule created in Firewall-1_FW2 Rulebase. It explains the contents of each rule. The rules will be tested on next section, ***4.0 – System Audit.***

Rule 1 : Lockdown FW-1

No.	Source	Destination	Service	Action	Track	Install On
1	Any	Firewall-1_FW2	Any	drop	Alert	Gateways

- Deny traffic directly to the firewall. (lock-down rule). Attempts to connect to the firewall drops the packet, and alerts the operator of the connection attempt. The firewall does not provide services other than screening packets and enforcing the policy. This is positioned right at the start to ensure that no other rules would allow traffic to the firewall before this one is matched. This rule effectively notifies of any attempts to gain access to FW-1 by intruders or the curious. The attempt generates an alert to the operator.

Rule 2 : Web Server Access on Protected Subnet

No.	Source	Destination	Service	Action	Track	Install On
1	Any	Firewall-1_FW2	Any	drop	Alert	Gateways

- Employees can access corporate web site on Protected Subnet from Local Area Network. It generates logging (tracking) of succesfull connection attempts.

Rule 3 : E-Commerce Web Server Access (Customers) on Protected Subnet

No.	Source	Destination	Service	Action	Track	Install On
3	LAN_Subnet	Customer_WebServer	http https	accept	Long	Gateways

- HTTP and HTTPS traffic from LAN Subnet to Customer Web Server on Protected Subnet will be allowed. It generates logging (tracking) of succesfull connection attempts.

Rule 4 : Mail retrieve from Mail Server

No.	Source	Destination	Service	Action	Track	Install On
4	LAN_Subnet	MailServer	SecurePOP3	accept	Long	Gateways

- Rule allows employees to check mail on Protected Subnet from Local Area Network Subnet. The POP3 connection is safe because It avoids clear POP3 traffic. The mail is received under a secure SSL POP connection (port 995) and there is no risk of password discovery. It generates logging (tracking) of succesfull connection attempts.

Rule 5 : DNS Queries

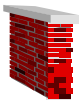
No.	Source	Destination	Service	Action	Track	Install On
5	Internal_DNS	Primary_DNS	domain-udp	accept	Long	Gateways

- Internal DNS provides name resolution from employees on Local Area Network. The rule allows outbound *DNS traffic to Primary Name Server on UDP port 53* for domain queries. It generates logging (tracking) of succesfull connection attempts.

Rule 6 : LAN SubNet To Oracle Database Server

No.	Source	Destination	Service	Action	Track	Install On
6	LAN_Subnet	Oracle_DB_Server	SSH sqlnet1	accept	Long	Gateways

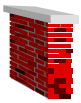
- Users on Local Area Network subnet are allowed to connect Oracle Database Server on Protected Subnet in order to secure telnet (SSH) Unix server for terminal emulation and to retrieve informations from database using SQLNET Oracle protocol. The rule also generates logging (tracking) of succesfull connection attempts.



Rule 7 : Internet Access from Local Area Network

No.	Source	Destination	Service	Action	Track	Install On
7	All Users@LAN_Subnet	Any	http https	Client Auth	Long	Gateways

- Users on Local Area Network can browse the Internet. Outside access is allowed only from Local Area Network and users must authenticate on firewall in order to surf outside.



Rule 8 : Network Admin – Management of Unix Servers

No.	Source	Destination	Service	Action	Track	Install On
8	Network_Admin	Customer_WebServer MailServer Partners_WebServer Primary_DNS Suppliers_WebServer WebServer SyslogServer IDS1 IDS2	SSH	accept	Long	Gateways

- Group of Network Administrators can connect to Unix Servers from Local Area Network Subnet (1.1.4.0) to DMZ Subnet (1.1.1.0) , DMZ Subnet (1.1.3.0) and Protected Subnet (1.1.2.0) through secure telnet (SSH) in order to provide system management and maintenance. The rule generates logging (tracking) of succesfull connection attempts.

Rule 9 : Network Admin – Management of Internet1 and Internet2 Routers

No.	Source	Destination	Service	Action	Track	Install On
9	Network_Admin	Attacker_Host Internet2_Cisco	telnet	accept	Long	Gateways

- Group of Network Administrators can connect to router Internet1 and Internet2 in order to provide router management and maintenance. The rule also generates logging (tracking) of succesfull connection attempts.

Rule 10 : DROP Login Services

No.	Source	Destination	Service	Action	Track	Install On
10	Any	LAN_Subnet	Login_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Login_Services*** contains and blocks telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), and the r-services rlogin et al (512/tcp through 514/tcp) traffic destinated to Local Area Network Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 11 : DROP RPC and NFS Services

No.	Source	Destination	Service	Action	Track	Install On
11	Any	LAN_Subnet	RPC_NFS_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***RPC_NFS_Services*** contains and blocks Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) traffic destinated to Local Area Network Subnet from anywhere The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 12 : DROP Netbios Services

No.	Source	Destination	Service	Action	Track	Install On
12	Any	LAN_Subnet	Netbios_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Netbios_Services*** contains and blocks 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 earlier ports plus 445 (tcp and udp) traffic destinated to Local Area Network Subnet from anywhere The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 13 : DROP Xwindows Range

No.	Source	Destination	Service	Action	Track	Install On
13	Any	LAN_Subnet	XWindows_Range	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service ***Xwindows_Range*** contains and blocks 6000-6250/tcp traffic destinated to Local Area Network Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 14 : DROP Naming Services

No.	Source	Destination	Service	Action	Track	Install On
14	Any	LAN_Subnet	Naming_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Naming_Services*** contains and blocks 53 (tcp and udp), 389 (tcp and udp) traffic destinated to Local Area Network Subnet from anywhere . The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 14 : DROP Naming Services

No.	Source	Destination	Service	Action	Track	Install On
15	Any	LAN_Subnet	Mail_Services	drop	Alert	Gateways

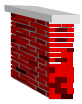
- According to recommentations from SANS Top Ten Document, service ***Mail_Services*** contains and blocks 25/TCP, 109/TCP and 110/TCP traffic destinated to Local Area Network Subnet from anywhere . The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 16 : DROP Web Services

No.	Source	Destination	Service	Action	Track	Install On
16	Any	LAN_Subnet	Web_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Web_Services*** contains and blocks 80/TCP, 443/TCP, 8000/TCP, 8080/TCP and 8888/TCP traffic destinated to Local Area Network Subnet

from anywhere . The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.



Rule 17 : DROP Small Servicess

No.	Source	Destination	Service	Action	Track	Install On
17	Any	LAN_Subnet	Small_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Small_Services*** contains and blocks all the TCP and UDP services below 20 and 37/tcp and 37/udp traffic destinated to Local Area Network Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 18 : DROP Misc Services

No.	Source	Destination	Service	Action	Track	Install On
18	Any	LAN_Subnet	Misc_Services	drop	Alert	Gateways

- According to recommentations from SANS Top Ten Document, service group ***Misc_Services*** contains and blocks 69/UDP, 79/TCP, 119/TCP, 123/TCP, 155/TCP, 514/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, 179/TCP and 1080/tcp traffic destinated to Local Area Network Subnet from anywhere. The rule also generates altert to security staff in order to advise unsuccesfull connection attempts.

Rule 19 : REJECT Traffic Between Subnets

No.	Source	Destination	Service	Action	Track	Install On
19	Protected_Subnet	LAN_Subnet	Any	reject	Alert	Gateways

- This rule explicitly denies connections from Protected Subnet to LAN (Local Area Network) Assuming the case that a intruder has compromised one of the systems on Protected Subnet, any connection attempts from Protected Subnet to Lan Subnet will be rejected. An alert is also generated to notify the security staff.

Rule 20 : REJECT Traffic Between Subnets

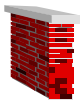
No.	Source	Destination	Service	Action	Track	Install On
20	LAN_Subnet	Protected_Subnet	Any	reject	Alert	Gateways

- This rule explicitly denies connections from Lan Subnet to Protected Subnet. Any connection attempts from Protected Subnet to Lan Subnet will be rejected. An alert is also generated to notify the firewall operator. Log everything so there is a audit trail.

Rule 21 : Silent Drop Rule (Broadcast)

No.	Source	Destination	Service	Action	Track	Install On
21	Any	Any	SilentServices	drop		Gateways

- As a precaution any broadcast traffic originating from any source is dropped. It is not essential or even desirable to forward any broadcast so for that reason we drop them all.

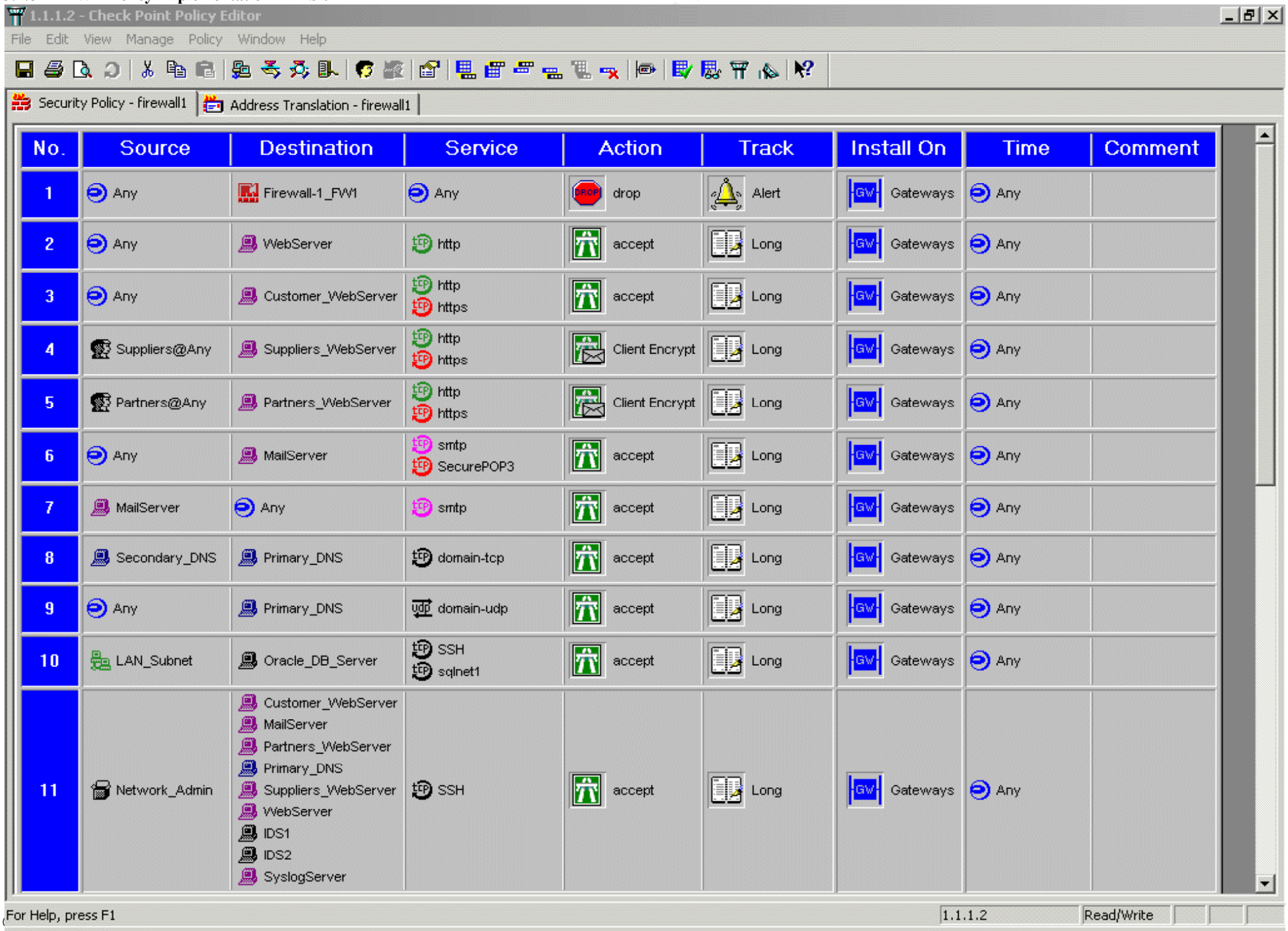


Rule 22 : Last Rule (Explicit Deny ANY-ANY)

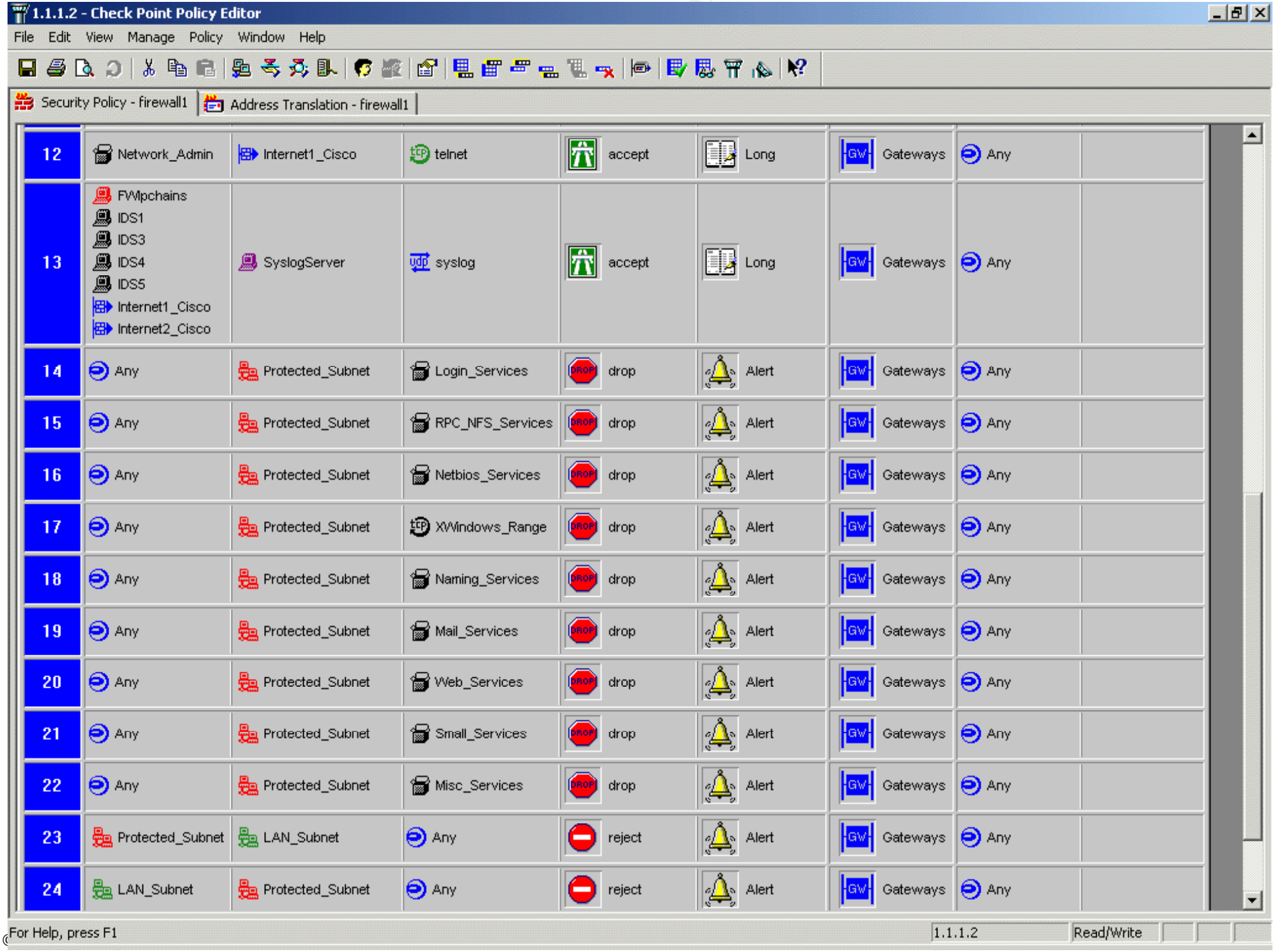
No.	Source	Destination	Service	Action	Track	Install On
22	Any	Any	Any	drop	Alert	Gateways

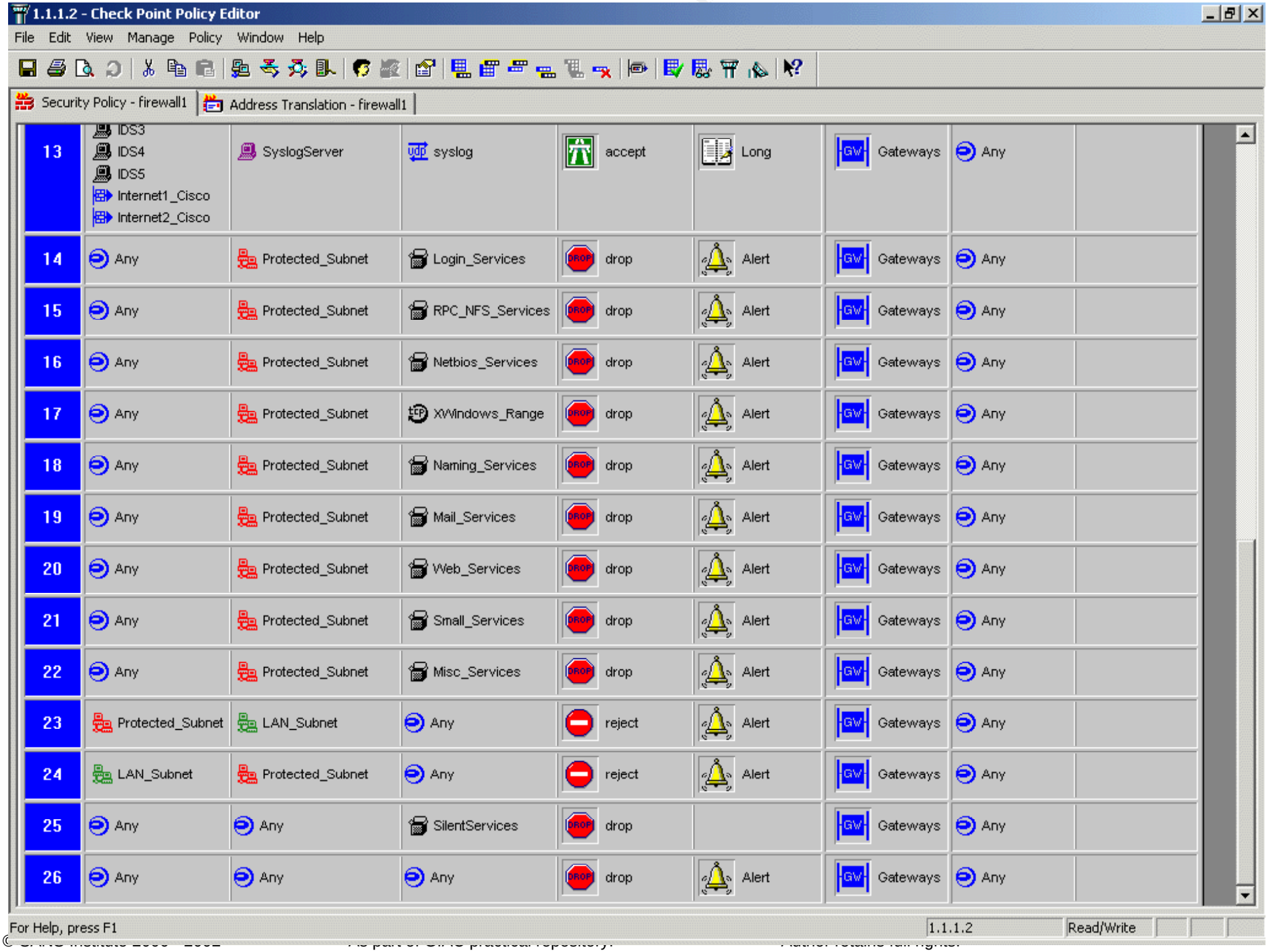
- The explicit deny all and log rule. Useful to see what other kind of traffic is attempting to access resources. This rule is always the very last one. (Clean up rule). It´s important to log and generate alert to security staff because the rule can probe for weakness in our policy,

3.4.8 FW-1 Policy Implementation Exhibit

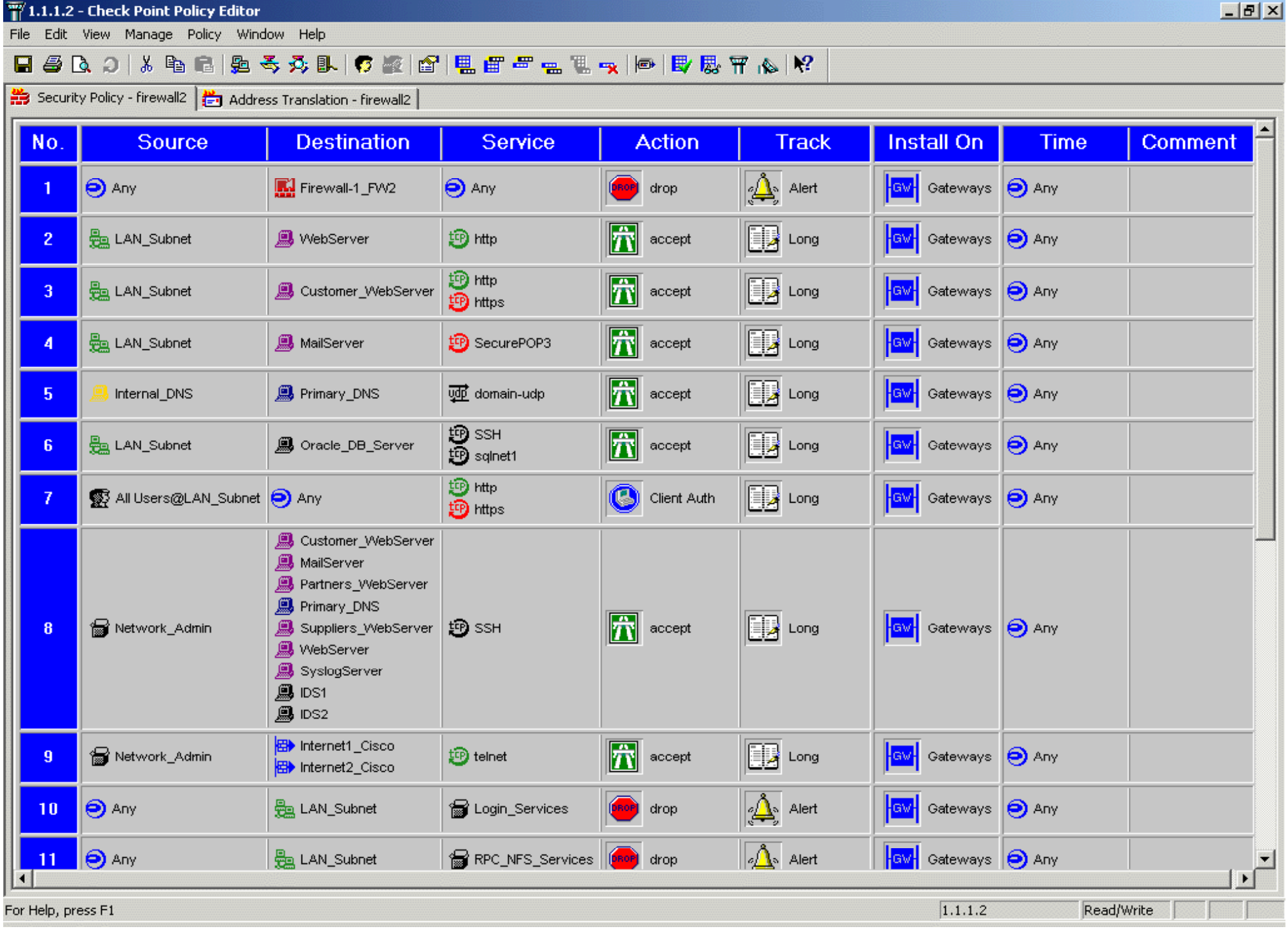


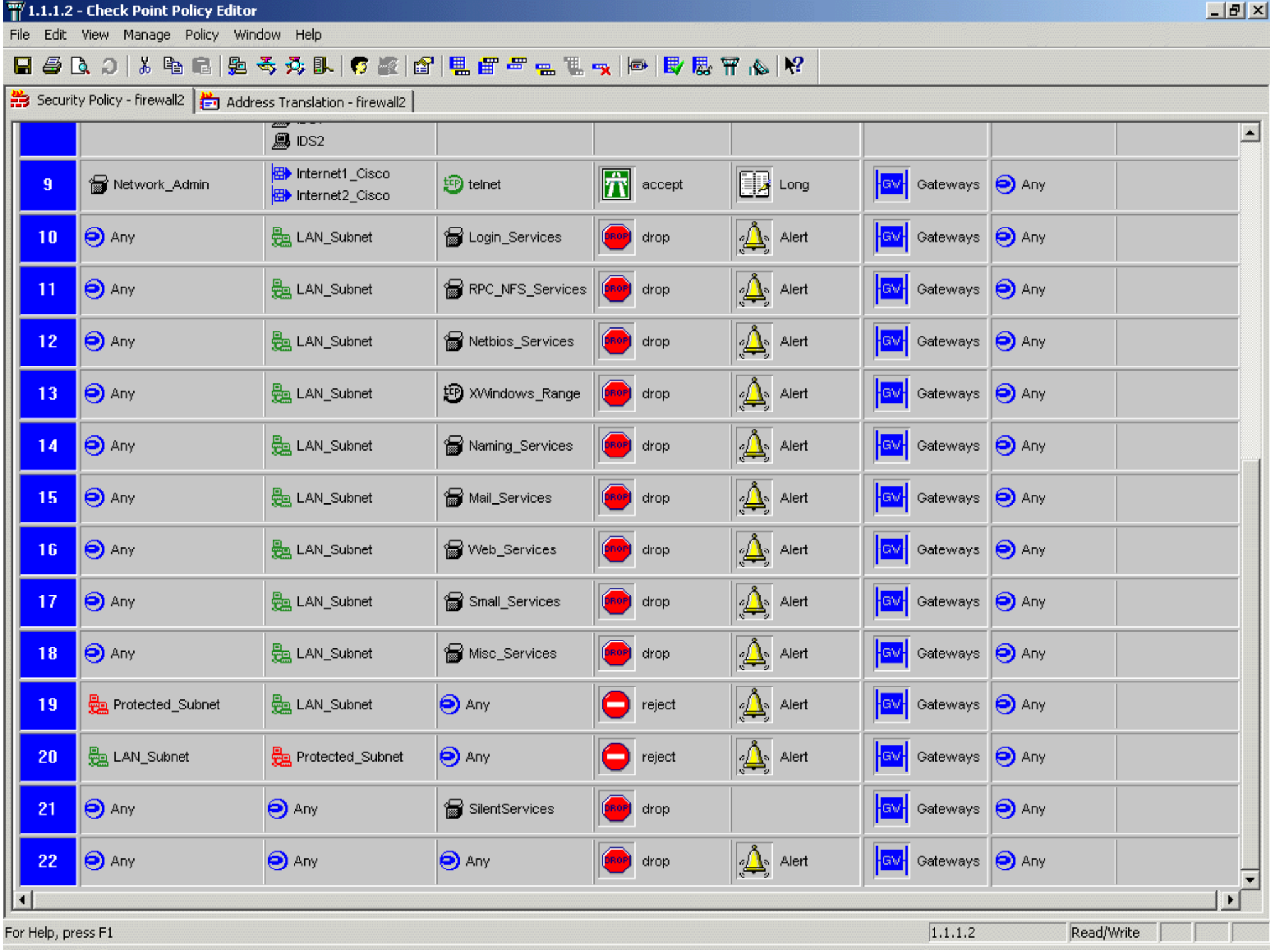
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	Firewall-1_FW1	Any	drop	Alert	Gateways	Any	
2	Any	WebServer	http	accept	Long	Gateways	Any	
3	Any	Customer_WebServer	http https	accept	Long	Gateways	Any	
4	Suppliers@Any	Suppliers_WebServer	http https	Client Encrypt	Long	Gateways	Any	
5	Partners@Any	Partners_WebServer	http https	Client Encrypt	Long	Gateways	Any	
6	Any	MailServer	smtp SecurePOP3	accept	Long	Gateways	Any	
7	MailServer	Any	smtp	accept	Long	Gateways	Any	
8	Secondary_DNS	Primary_DNS	domain-tcp	accept	Long	Gateways	Any	
9	Any	Primary_DNS	domain-udp	accept	Long	Gateways	Any	
10	LAN_Subnet	Oracle_DB_Server	SSH sqlnet1	accept	Long	Gateways	Any	
11	Network_Admin	Customer_WebServer MailServer Partners_WebServer Primary_DNS Suppliers_WebServer WebServer IDS1 IDS2 SyslogServer	SSH	accept	Long	Gateways	Any	


1.1.1.2 - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - firewall1
Address Translation - firewall1
12 Network_Admin Internet1_Cisco telnet accept Long Gateways Any
13 FWIpchains IDS1 IDS3 IDS4 IDS5 Internet1_Cisco Internet2_Cisco SyslogServer syslog accept Long Gateways Any
14 Any Protected_Subnet Login_Services drop Alert Gateways Any
15 Any Protected_Subnet RPC_NFS_Services drop Alert Gateways Any
16 Any Protected_Subnet Netbios_Services drop Alert Gateways Any
17 Any Protected_Subnet XWindows_Range drop Alert Gateways Any
18 Any Protected_Subnet Naming_Services drop Alert Gateways Any
19 Any Protected_Subnet Mail_Services drop Alert Gateways Any
20 Any Protected_Subnet Web_Services drop Alert Gateways Any
21 Any Protected_Subnet Small_Services drop Alert Gateways Any
22 Any Protected_Subnet Misc_Services drop Alert Gateways Any
23 Protected_Subnet LAN_Subnet Any reject Alert Gateways Any
24 LAN_Subnet Protected_Subnet Any reject Alert Gateways Any
For Help, press F1
1.1.1.2
Read/Write


1.1.1.2 - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - firewall1
Address Translation - firewall1
13 IDS3 IDS4 IDS5 Internet1_Cisco Internet2_Cisco SyslogServer syslog accept Long Gateways Any
14 Any Protected_Subnet Login_Services drop Alert Gateways Any
15 Any Protected_Subnet RPC_NFS_Services drop Alert Gateways Any
16 Any Protected_Subnet Netbios_Services drop Alert Gateways Any
17 Any Protected_Subnet XWindows_Range drop Alert Gateways Any
18 Any Protected_Subnet Naming_Services drop Alert Gateways Any
19 Any Protected_Subnet Mail_Services drop Alert Gateways Any
20 Any Protected_Subnet Web_Services drop Alert Gateways Any
21 Any Protected_Subnet Small_Services drop Alert Gateways Any
22 Any Protected_Subnet Misc_Services drop Alert Gateways Any
23 Protected_Subnet LAN_Subnet Any reject Alert Gateways Any
24 LAN_Subnet Protected_Subnet Any reject Alert Gateways Any
25 Any Any SilentServices drop Gateways Any
26 Any Any Any drop Alert Gateways Any
For Help, press F1
1.1.1.2
Read/Write

3.4.9 FW-2 Policy Implementation Exhibit





4 Security Architecture Audit (25 Points)

4.1 Audit Plan

Audit Plan will execute tests on the security policy installed on ***Firewall-1_FW1*** and border router ***Internet#1.*** To achieve this will require a LAB configuration with appropriate tools.

To verify firewall policy rules will require that stimulus is applied, and the response measured to determine if the policy is behaving as designed, and to verify the audit trail. Following are actual results taken by executing each of the test cases in the lab. The primary tool for generating stimulus was nmap, and the command line options for each test are included in the table for each test case. Expected and actual responses are recorded to determine if the test passed or failed and to make note of any abnormalities.
NMAP is used to scan the network for unnecessary services and to generate traffic patterns to exercise the network, and measure response using the log facility of firewall , and a packet sniffer attached to each segment to determine if traffic is forward or not.

User accounts should be reviewed and accounts with weak passwords should be identified. Access logs to servers, routers and firewalls should be analyzed to ensure only authorized access attempts have occurred..
Tools like L0PHTCRACK or CRACK should be used to check for weak passwords and logfiles should be manually scanned. Logfiles from routers are sent to ***Syslog Server*** on the Protected Subnet and logfiles from the two CheckPoint Firewalls should be removed from all systems frequently by the security administrators and stored for future reference. Scans of the entire network should be performed from each subnet to identify services that should be disabled and to check that the IDS systems are functional

The log analysis should occur daily, to ensure intrusion attempts are being identified but is important to notice that audit tasks should consume approximately 50% of one of the security team member's time.

All updates to the external firewall and routers should be review with at least one other member of the security group.

Important Notes about AUDIT Tests

It was requested to audit **the Border Router and Firewalls described in Assignments 1 and 2. As the network topology has two border routers (one is used to outbound traffic and another is used for inbound traffic) the inbound router will be used for auditing tests.**

Due to not having available sufficient hardware on hand to create the entire lab configuration testing regarding Firewall-1_FW2 it was not possible to perform the tests.

5 Security Architecture Audit (25 Points)

5.1 Audit Plan

Audit Plan will execute tests on the security policy installed on ***Firewall-1_FW1*** and border router ***Internet#1.*** To achieve this will require a LAB configuration with appropriate tools.

To verify firewall policy rules will require that stimulus is applied, and the response measured to determine if the policy is behaving as designed, and to verify the audit trail. Following are actual results taken by executing each of the test cases in the lab. The primary tool for generating stimulus was nmap, and the command line options for each test are included in the table for each test case. Expected and actual responses are recorded to determine if the test passed or failed and to make note of any abnormalities.
NMAP is used to scan the network for unnecessary services and to generate traffic patterns to exercise the network, and measure response using the log facility of firewall , and a packet sniffer attached to each segment to determine if traffic is forward or not.

User accounts should be reviewed and accounts with weak passwords should be identified. Access logs to servers, routers and firewalls should be analyzed to ensure only authorized access attempts have occurred..
Tools like L0PHTCRACK or CRACK should be used to check for weak passwords and logfiles should be manually scanned. Logfiles from routers are sent to ***Syslog Server*** on the Protected Subnet and logfiles from the two CheckPoint Firewalls should be removed from all systems frequently by the security administrators and stored for future reference. Scans of the entire network should be performed from each subnet to identify services that should be disabled and to check that the IDS systems are functional

The log analysis should occur daily, to ensure intrusion attempts are being identified but is important to notice that audit tasks should consume approximately 50% of one of the security team member's time.

All updates to the external firewall and routers should be review with at least one other member of the security group.

Important Notes about AUDIT Tests

It was requested to audit **the Border Router and Firewalls described in Assignments 1 and 2. As the network topology has two border routers (one is used to outbound traffic and another is used for inbound traffic) the inbound router will be used for auditing tests.**

Due to not having available sufficient hardware on hand to create the entire lab configuration testing regarding Firewall-1, it was not possible to audit FW2.

5.2 Firewall-1_FW1 Audit

Audit Test #1 – Checking TCP Port 80 Access (Web Server)	
A) Stimulus	***B) Expected Result***
From Attacker Host (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to port 80/TCP on WebServer. (nmap -sT –p 80 1.1.2.2)	Stimulus will confirm that inbound connections to Public Web Server (1.1.2.2) on TCP port 80 are accepted from any source. Rule #2 should allow inbound traffic and track connection session

C) Result

Test works as expected. Due rule #2, Firewall-1 accepts and logs the successful connection

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	log	accept	http	Audit_Machine	WebServer	tcp	2	1087

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows connection being established. First, remote host sends a SYN packet to ***WebServer*** on TCP port 80. ***WebServer*** sends a packet with SYNand ACK flags set to source ephemerous port and finally, the remote host sends the ACK flag telling ***WebServer*** that the connection has been established and they are ready to send/receive data.

```
02/06-19:41:51.917511 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1101 -> 1.1.2.2:80 TCP TTL:64 TOS:0x0 ID:29727  DF
******S* Seq: 0xD2AA002C   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 36920792 0 NOP WS: 0

02/06-19:41:51.918607 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x4E
1.1.2.2:80 -> 172.16.5.3:1101 TCP TTL:127 TOS:0x0 ID:7468  DF
***A**S* Seq: 0xBD31781A   Ack: 0xD2AA002D   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

02/06-19:41:51.918747 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x42
172.16.5.3:1101 -> 1.1.2.2:80 TCP TTL:64 TOS:0x0 ID:29728  DF
***A**** Seq: 0xD2AA002D   Ack: 0xBD31781B   Win: 0x7D78
TCP Options => NOP NOP TS: 36920792 0
```

Audit Test #2 – Searching for interesting ports on Web Server

A) Stimulus	*B) Expected Result*
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN in order to verify what services are accessible on ***WebServer.*** ***(nmap -sT –P0 -F 1.1.2.2)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to any other port unlike TCP port 80 should be dropped , logged and altert must be sent to Security staff.

C) Result

Test works as expected. Connections to ports unlike TCP 80 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	747	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	1445	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	482	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	120	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	244	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	457	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	1476	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	1374	Attacker_Host	WebServer	tcp	26	58416
Firewall-1_FW1	alert	drop	435	Attacker_Host	WebServer	tcp	26	58416

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows attacker trying to establish connection in a portscan attack by sending SYN and waiting for SYN/ACK replies.

```
02/06-20:00:51.439374 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1574 -> 1.1.2.2:1475 TCP TTL:64 TOS:0x0 ID:36534  DF
******S* Seq: 0x1A8469C3   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 37034745 0 NOP WS: 0

02/06-20:00:51.439477 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1575 -> 1.1.2.2:360 TCP TTL:64 TOS:0x0 ID:36535  DF
******S* Seq: 0x19E3EAB4   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 3703474d5 0 NOP WS: 0

02/06-20:00:51.439573 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1576 -> 1.1.2.2:6147 TCP TTL:64 TOS:0x0 ID:36536  DF
******S* Seq: 0x1A43445E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 37034745 0 NOP WS: 0
```

Audit Test #3 – Checking TCP Port 80/443 Access (Customer Web Server)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN in order to connect to ports 80/TCP and 443/TCP on **Customer Web Server** ***(nmap –sT –p 80,443 1.1.2.3).***	Stimulus will confirm that inbound connections to Customer Web Server (1.1.2.3) on TCP ports 80/443 are accepted from any source. Rule #3 should allow inbound traffic and track connection session.

C) Result

Test works as expected. Due rule #3, Firewall-1 accepts and logs the successful connection.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	log	accept	http	Attacker_Host	Customer_WebServer	tcp	3	1298
Firewall-1_FW1	log	accept	https	Attacker_Host	Customer_WebServer	tcp	3	1299

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows connection being established from ***Audit Machine*** to ***Customer WebServer*** on TCP Ports 80 and 443 (SYN from Audit Machine, SYN/ACK from Customer Web Server and finally ACK from Audit Machine).

```
02/08-11:19:42.720359 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2949 -> 1.1.2.3:443 TCP TTL:64 TOS:0x0 ID:22906  DF
******S* Seq: 0xE68B8411   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 2979471 0 NOP WS: 0

02/08-11:19:42.721410 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2950 -> 1.1.2.3:80 TCP TTL:64 TOS:0x0 ID:22907  DF
******S* Seq: 0xE5E6F056   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 2979471 0 NOP WS: 0

02/08-11:19:42.721664 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x4E
1.1.2.3:443 -> 172.16.5.3:2949 TCP TTL:127 TOS:0x0 ID:157  DF
***A**S* Seq: 0x1CFCCFE4   Ack: 0xE68B8412   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

02/08-11:19:42.721849 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x42
172.16.5.3:2949 -> 1.1.2.3:443 TCP TTL:64 TOS:0x0 ID:22908  DF
***A**** Seq: 0xE68B8412   Ack: 0x1CFCCFE5   Win: 0x7D78
TCP Options => NOP NOP TS: 2979471 0

02/08-11:19:42.722177 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x4E
1.1.2.3:80 -> 172.16.5.3:2950 TCP TTL:127 TOS:0x0 ID:158  DF
***A**S* Seq: 0x1CFD64EC   Ack: 0xE5E6F057   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

02/08-11:19:42.722272 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x42
172.16.5.3:2950 -> 1.1.2.3:80 TCP TTL:64 TOS:0x0 ID:22909  DF
***A**** Seq: 0xE5E6F057   Ack: 0x1CFD64ED   Win: 0x7D78
TCP Options => NOP NOP TS: 2979471 0
```

Audit Test #4 – Searching for interesting ports (Customer Web Server))

A) Stimulus	*B) Expected Result*
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN in order to verify what services are accessible on ***Customer WebServer*** (1.1.2.3)***(nmap -sT -P0 -F 1.1.2.3)***	.TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to any other port unlike TCP ports 80/443 should be dropped , logged and altert must be sent to Security staff

C) Result

Test works as expected. Connections to ports unlike TCP 80/443 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	1466	Attacker_Host	Customer_WebServer	tcp	26	2262
Firewall-1_FW1	alert	drop	149	Attacker_Host	Customer_WebServer	tcp	26	2263
Firewall-1_FW1	alert	drop	744	Attacker_Host	Customer_WebServer	tcp	26	2264
Firewall-1_FW1	alert	drop	1386	Attacker_Host	Customer_WebServer	tcp	26	2265
Firewall-1_FW1	alert	drop	437	Attacker_Host	Customer_WebServer	tcp	26	2266
Firewall-1_FW1	alert	drop	uucp	Attacker_Host	Customer_WebServer	tcp	26	2267
Firewall-1_FW1	alert	drop	10083	Attacker_Host	Customer_WebServer	tcp	26	2268
Firewall-1_FW1	alert	drop	1366	Attacker_Host	Customer_WebServer	tcp	26	2269
Firewall-1_FW1	alert	drop	370	Attacker_Host	Customer_WebServer	tcp	26	2270

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows attacker trying to establish connection in a portscan attack by sending SYN and waiting for SYN/ACK replies.

```
02/08-12:15:26.517954 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:3336 -> 1.1.2.3:68 TCP TTL:64 TOS:0x0 ID:36743  DF
******S* Seq: 0xB8BF247E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 3313851 0 NOP WS: 0

02/08-12:15:26.518166 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:3337 -> 1.1.2.3:800 TCP TTL:64 TOS:0x0 ID:36744  DF
******S* Seq: 0xB8904E6A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 3313851 0 NOP WS: 0

02/08-12:15:26.518378 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:3338 -> 1.1.2.3:361 TCP TTL:64 TOS:0x0 ID:36745  DF
******S* Seq: 0xB831E38E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 3313851 0 NOP WS: 0

:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:3339 -> 1.1.2.3:759 TCP TTL:64 TOS:0x0 ID:36746  DF
******S* Seq: 0xB864734E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 3313851 0 NOP WS: 0
```

Audit Test #5 – Checking TCP Port 80/443 Access (Suppliers Web Server)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to ports 80/TCP and 443/TCP on ***Suppliers Web Server*** (1.1.2.4). ***(nmap –sT –p 80,443 1.1.2.4)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to TCP ports 80/443 should be dropped and logged. ***Acess is restriced and will be allowed only to users after authenticating with Secure Remote (VPN tunnel)***

C) Result

Test works as expected. Connections to ports TCP 80/443 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	http	Attacker_Host	Suppliers_WebServer	tcp	20	4111
Firewall-1_FW1	alert	drop	https	Attacker_Host	Suppliers_WebServer	tcp	20	4112

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows attacker trying to establish connection in a portscan attack by sending SYN and waiting for SYN/ACK replies.

```
02/08-14:13:59.237292 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:4176 -> 1.1.2.4:80 TCP TTL:64 TOS:0x0 ID:26178  DF
******S* Seq: 0x786217F9   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 4025123 0 NOP WS: 0

02/08-14:13:59.237524 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:4177 -> 1.1.2.4:443 TCP TTL:64 TOS:0x0 ID:26179  DF
******S* Seq: 0x78AFE26E   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 4025123 0 NOP WS: 0
```

Audit Test #6 – Checking TCP Port 80/443 Access (Partners Web Server)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to ports 80/TCP and 443/TCP on ***Partners Web Server*** (1.1.2.5). ***(nmap –sT –p 80,443 1.1.2.5)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to TCP ports 80/443 should be dropped and logged. ***Acess is restriced and will be allowed only to users after authenticating with Secure Remote (VPN tunnel)***

C) Result

Test works as expected. Connections to ports TCP 80/443 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	http	Attacker_Host	Partners_WebServer	tcp	20	4325
Firewall-1_FW1	alert	drop	https	Attacker_Host	Partners_WebServer	tcp	20	4326

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

```
02/08-17:09:03.503692 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:4361 -> 1.1.2.5:80 TCP TTL:64 TOS:0x0 ID:57477  DF
******S* Seq: 0xE0E29BE   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 678450 0 NOP WS: 0

02/08-17:09:03.504582 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:4362 -> 1.1.2.5:443 TCP TTL:64 TOS:0x0 ID:57478  DF
******S* Seq: 0xE0C02A3   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 678450 0 NOP WS: 0
```

Audit Test #7 – Checking TCP Port 25/995 Access (Mail Server)

A) Stimulus	*B) Expected Result*
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN in order to connect to ports 25/TCP and 995/TCP on **Mail Server** (1.1.2.6) ***(nmap –sT –p 25,995 1.1.2.6).***	Stimulus will confirm that inbound connections to Mail Server (1.1.2.6) on TCP ports 25/995 are accepted from any source. Rule #6 should allow inbound traffic and track connection session

C) Result

Test works as expected. Due rule #6, Firewall-1 accepts and logs the successful connections.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	log	accept	smtp	Attacker_Host	MailServer	tcp	6	4499
Firewall-1_FW1	log	accept	SecurePOP3	Attacker_Host	MailServer	tcp	6	4500

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows connection being established from ***Attacker Host*** to ***Mail Server*** on TCP Ports 25 and 995. (SYN from Attacker Host, SYN/ACK from Mail Server and finally ACK from Attacker Host).

```
02/08-17:26:48.420279 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:4529 -> 1.1.2.6:25 TCP TTL:64 TOS:0x0 ID:58610  DF
******S* Seq: 0x5022D5CA   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 784941 0 NOP WS: 0

02/08-17:26:48.421477 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:4530 -> 1.1.2.6:995 TCP TTL:64 TOS:0x0 ID:58611  DF
******S* Seq: 0x50311AE9   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 784941 0 NOP WS: 0

02/08-17:26:48.421575 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x4E
1.1.2.6:25 -> 172.16.5.3:4529 TCP TTL:127 TOS:0x0 ID:6231  DF
***A**S* Seq: 0x65B0B8AA   Ack: 0x5022D5CB   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

02/08-17:26:48.421748 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x42
172.16.5.3:4529 -> 1.1.2.6:25 TCP TTL:64 TOS:0x0 ID:58612  DF
***A**** Seq: 0x5022D5CB   Ack: 0x65B0B8AB   Win: 0x7D78
TCP Options => NOP NOP TS: 784941 0

02/08-17:26:48.422257 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x4E
1.1.2.6:995 -> 172.16.5.3:4530 TCP TTL:127 TOS:0x0 ID:6232  DF
***A**S* Seq: 0x65B1B4DB   Ack: 0x50311AEA   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

02/08-17:26:48.422363 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x42
172.16.5.3:4530 -> 1.1.2.6:995 TCP TTL:64 TOS:0x0 ID:58613  DF
***A**** Seq: 0x50311AEA   Ack: 0x65B1B4DC   Win: 0x7D78
TCP Options => NOP NOP TS: 784941 0
```

Audit Test #8 – Searching for interesting ports (Mail Server)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN in order to verify what services are accessible on ***Mail Server*** (1.1.2.6) ***(nmap -sT -P0 -F 1.1.2.6)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to ***Mail Server*** on port unlike TCP ports 25/993 should be dropped and logged

C) Result

Test works as expected. Connections to ports unlike TCP 25/995 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	eklogin	Attacker_Host	MailServer	tcp	26	2061
Firewall-1_FW1	alert	drop	164	Attacker_Host	MailServer	tcp	26	2062
Firewall-1_FW1	alert	drop	128	Attacker_Host	MailServer	tcp	26	2063
Firewall-1_FW1	alert	drop	1440	Attacker_Host	MailServer	tcp	26	2064
Firewall-1_FW1	alert	drop	582	Attacker_Host	MailServer	tcp	26	2065
Firewall-1_FW1	alert	drop	1350	Attacker_Host	MailServer	tcp	26	2066
Firewall-1_FW1	alert	drop	132	Attacker_Host	MailServer	tcp	26	2067
Firewall-1_FW1	alert	drop	3141	Attacker_Host	MailServer	tcp	26	2068

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows attacker trying to establish connection in a portscan attack by sending SYN and waiting for SYN/ACK replies.

```
02/08-18:18:31.898269 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2364 -> 1.1.2.6:5713 TCP TTL:64 TOS:0x0 ID:4003  DF
******S* Seq: 0x12FE5283   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1095289 0 NOP WS: 0

02/08-18:18:31.899135 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2365 -> 1.1.2.6:2106 TCP TTL:64 TOS:0x0 ID:4004  DF
******S* Seq: 0x12D71EB8   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1095289 0 NOP WS: 0

02/08-18:18:31.899995 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2366 -> 1.1.2.6:1539 TCP TTL:64 TOS:0x0 ID:4005  DF
******S* Seq: 0x12F1512A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1095289 0 NOP WS: 0

02/08-18:18:34.883567 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2357 -> 1.1.2.6:1546 TCP TTL:64 TOS:0x0 ID:4008  DF
******S* Seq: 0x1391E316   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1095588 0 NOP WS: 0
```


Audit Test #9 – Checking TCP Port 53 Access (Zone Transfers – Primary DNS Server)

A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN SCAN to port 53 /TCP on ***Primary DNS Server*** ***(nmap –sT –p 53 -P0 1.1.2.7).***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to TCP port 53 (***Zone Transfers***) should be dropped and logged. ***Access to TCP port 53 is restricted only from Secondary Domain Name Server. Only the Secondary DNS is able to connect and perform Zone Transfers***

C) Result

Test works as expected. Connections to ports unlike TCP 25/995 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	nameserver	Attacker_Host	Primary_DNS	tcp	18	2691

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows attacker trying to establish connection in a portscan attack by sending SYN and waiting for SYN/ACK replies.

```
02/08-18:39:05.843559 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2717 -> 1.1.2.7:53 TCP TTL:64 TOS:0x0 ID:5207  DF
******S* Seq: 0x613DF7D6   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1218684 0 NOP WS: 0

02/08-18:39:05.863558 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2718 -> 1.1.2.7:53 TCP TTL:64 TOS:0x0 ID:5208  DF
******S* Seq: 0x6111A7A9   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1218686 0 NOP WS: 0

02/08-18:40:24.680286 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2722 -> 1.1.2.7:53 TCP TTL:64 TOS:0x0 ID:5390  DF
******S* Seq: 0x6634610A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1226567 0 NOP WS: 0

02/08-18:40:27.673568 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:2722 -> 1.1.2.7:53 TCP TTL:64 TOS:0x0 ID:5392  DF
******S* Seq: 0x6634610A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 1226867 0 NOP WS: 0
```


Audit Test #10 – Checking TCP Port 22/1521 Access (Oracle Database Server)	
A) Stimulus	***B) Expected Result***
From any workstation on ***Lan Subnet*** (the workstation chosen was the Oracle Database Administrator one) open a connection in order to connect to TCP ports 22/1521 on ***Oracle Database Server*** ***(nmap –sT –p 21,1521 –P0 1.1.2.8)***	Connections started from Lan Subnet (in our example from Oracle Database Administrator – workstation 1.1.4.20) – should be accepted. It will confirm that inbound connections to the Oracle Database Server on TCP ports 22/1521 are accepted from any workstation that belongs to Local Area Network.
C) Result	
Test works as expected. Due rule #10, Firewall-1 accepts and logs the successful connections	
D) Output (Firewall-1 Event Log Viewer	

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	log	accept	SSH	Oracle_DBA_wkst	Oracle_DB_Server	tcp	11	1617
Firewall-1_FW1	log	accept	sqlnet1	Oracle_DBA_wkst	Oracle_DB_Server	tcp	11	1618

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)
Snort shows connection being established from ***Oracle DBA Wkst*** to ***Oracle Server*** on TCP Ports 22 and 1521 (SYN from Oracle DBA Wkst, SYN/ACK from Mail Server and finally ACK from Oracle DBA Wkst). 02/09-10:45:31.149851 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x3E 1.1.4.20:1800 -> 1.1.2.8:22 TCP TTL:127 TOS:0x0 ID:21924 DF ******S* Seq: 0xE24179E9 Ack: 0x0 Win: 0x4000 TCP Options => MSS: 1460 NOP NOP SackOK 02/09-10:45:31.150906 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x3E 1.1.2.8:22 -> 1.1.4.20:1800 TCP TTL:127 TOS:0x0 ID:3001 DF ***A**S* Seq: 0x35D67733 Ack: 0xE24179EA Win: 0x4470 TCP Options => MSS: 1460 NOP NOP SackOK 02/09-10:45:31.150991 0:0:B4:52:4B:30 -> 0:10:4B:87:1F:EB type:0x800 len:0x3E 1.1.2.8:22 -> 1.1.4.20:1800 TCP TTL:126 TOS:0x0 ID:3001 DF ***A**S* Seq: 0x35D67733 Ack: 0xE24179EA Win: 0x4470 TCP Options => MSS: 1460 NOP NOP SackOK 02/09-10:45:25.731042 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x3E 1.1.4.20:1799 -> 1.1.2.8:1521 TCP TTL:127 TOS:0x0 ID:21914 DF ******S* Seq: 0xE22BE963 Ack: 0x0 Win: 0x4000 TCP Options => MSS: 1460 NOP NOP SackOK 02/09-10:45:25.732257 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x3E 1.1.2.8:1521 -> 1.1.4.20:1799 TCP TTL:127 TOS:0x0 ID:2992 DF ***A**S* Seq: 0x35C107A0 Ack: 0xE22BE964 Win: 0x4470 TCP Options => MSS: 1460 NOP NOP SackOK 02/09-10:45:25.732803 0:10:4B:87:1F:EB -> 0:0:B4:52:4B:30 type:0x800 len:0x3C 1.1.4.20:1799 -> 1.1.2.8:1521 TCP TTL:128 TOS:0x0 ID:21915 DF ***A**** Seq: 0xE22BE964 Ack: 0x35C107A1 Win: 0x4470

Audit Test #11 – Checking TCP Port 22/1521 Access from outside (Oracle Database Server)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to TCP ports 22/1521 on ***Oracle Database Server*** ***(nmap –sT –p 22,1521 –P0 1.1.2.8)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to TCP ports 22/1521 on Oracle Database Server should be dropped and logged. Access is ***restricted only from Local Area Network.***
C) Result	
Test works as expected. Connections to port TCP 22/1521 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempt for ***SSH or SQLNet***	
D) Output (Firewall-1 Event Log Viewer	

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	sqlnet1	Attacker_Host	Oracle_DB_Server	tcp	26	1302
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	Oracle_DB_Server	tcp	14	1303

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows attacker trying to establish connection in a portscan attack by sending SYN and waiting for SYN/ACK replies.

```
02/09-12:07:22.718370 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1324 -> 1.1.2.8:1521 TCP TTL:64 TOS:0x0 ID:9659  DF
******S* Seq: 0xD855EA44   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 5814970 0 NOP WS: 0

02/09-12:07:22.719356 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1325 -> 1.1.2.8:22 TCP TTL:64 TOS:0x0 ID:9660  DF
******S* Seq: 0xD8FF2A4A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 5814970 0 NOP WS: 0

02/09-12:07:25.710897 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1324 -> 1.1.2.8:1521 TCP TTL:64 TOS:0x0 ID:9662  DF
******S* Seq: 0xD855EA44   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 5815270 0 NOP WS: 0

02/09-12:07:25.710983 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1325 -> 1.1.2.8:22 TCP TTL:64 TOS:0x0 ID:9663  DF
******S* Seq: 0xD8FF2A4A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 5815270 0 NOP WS: 0
```


Audit Test #12 – Checking TCP Port 22 (SSH) Access to specific hosts from Admin Machine (LAN)

A) Stimulus	*B) Expected Result*
From any workstation that belongs to Network Admin group (the workstation chosen was the **NetAdmin1** one) using nmap as stimulus tool, open connections to TCP port 22 on servers **Customer Web Server, MailServer, Partners Web Server, Primary DNS Server, Suppliers Web Server, Syslog Server and IDS2** ***(nmap –sT –p 22 –P0 1.1.2.2-7,9,10)***	Connections started from **NetAdmin1 machine** (1.1.4.35) or another machine that belongs to Network Admin group should be accepted. It will confirm that inbound connections to specific servers on TCP ports 22 are accepted from Network Admin group (specific workstations @Local Area Network.). Connections should be accepted and logged.

C) Result

Test works as expected. Due rule #8, Firewall-1 accepts and logs the successful connections

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	log	accept	SSH	NetAdmin1	Customer_WebServer	tcp	11	2104
Firewall-1_FW1	log	accept	SSH	NetAdmin1	MailServer	tcp	11	eklogin
Firewall-1_FW1	log	accept	SSH	NetAdmin1	Partners_WebServer	tcp	11	2106
Firewall-1_FW1	log	accept	SSH	NetAdmin1	Primary_DNS	tcp	11	2107
Firewall-1_FW1	log	accept	SSH	NetAdmin1	Suppliers_WebServer	tcp	11	2108
Firewall-1_FW1	log	accept	SSH	NetAdmin1	WebServer	tcp	11	2109
Firewall-1_FW1	log	accept	SSH	NetAdmin1	SyslogServer	tcp	11	2110
Firewall-1_FW1	log	accept	SSH	NetAdmin1	IDS2	tcp	11	2111

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows connection being established from ***Network Admin Wkst*** to ***specific servers*** on TCP Port 22 for SSH (SYN from Admin machine, SYN/ACK from other hosts and finally ACK from network admin machine).

```
02/09-13:40:45.836101 0:10:4B:87:1F:EB -> 0:0:B4:52:4B:30 type:0x800 len:0x3E
1.1.4.35:2128 -> 1.1.2.3:22 TCP TTL:128 TOS:0x0 ID:26931  DF
******S* Seq: 0x7F874B12   Ack: 0x0   Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK

02/09-13:40:45.836425 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x3E
1.1.4.35:2128 -> 1.1.2.3:22 TCP TTL:127 TOS:0x0 ID:26931  DF
******S* Seq: 0x7F874B12   Ack: 0x0   Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK

02/09-13:40:45.837658 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x3E
1.1.2.3:22 -> 1.1.4.35:2128 TCP TTL:127 TOS:0x0 ID:3798  DF
***A**S* Seq: 0xD26EC634   Ack: 0x7F874B13   Win: 0x4470
TCP Options => MSS: 1460 NOP NOP SackOK

02/09-13:40:45.837755 0:0:B4:52:4B:30 -> 0:10:4B:87:1F:EB type:0x800 len:0x3E
1.1.2.3:22 -> 1.1.4.35:2128 TCP TTL:126 TOS:0x0 ID:3798  DF
***A**S* Seq: 0xD26EC634   Ack: 0x7F874B13   Win: 0x4470
TCP Options => MSS: 1460 NOP NOP SackOK

02/09-13:40:45.838192 0:10:4B:87:1F:EB -> 0:0:B4:52:4B:30 type:0x800 len:0x3C
1.1.4.35:2128 -> 1.1.2.3:22 TCP TTL:128 TOS:0x0 ID:26932  DF
***A**** Seq: 0x7F874B13   Ack: 0xD26EC635   Win: 0x4470

02/09-13:40:45.838274 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x36
1.1.4.35:2128 -> 1.1.2.3:22 TCP TTL:127 TOS:0x0 ID:26932  DF
***A**** Seq: 0x7F874B13   Ack: 0xD26EC635   Win: 0x4470
```

Audit Test #13 – Checking TCP Port 22 (SSH) Access from outside (Hosts on Screened Network)

A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to TCP port 22 on ***Customer Web Server, MailServer, Partners Web Server, Primary DNS Server, Suppliers Web Server, Syslog Server and IDS2*** ***(nmap –sT –p 22 –P0 1.1.2.3-7,9,10).***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to TCP port 22 on specific servers should be dropped and logged. ***Access is restricted only from network admin group on Local Area Network.*** SSH is not authorized from outside (Internet) to Protected Subnet

C) Result

Test works as expected. Due rule #14 Connections to port TCP 22 were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection for SSH.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	Oracle_DB_Server	tcp	14	1477
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	Customer_WebServer	tcp	14	1478
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	Suppliers_WebServer	tcp	14	1489
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	Partners_WebServer	tcp	14	1490
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	MailServer	tcp	14	1496
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	Primary_DNS	tcp	14	1507
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	SyslogServer	tcp	14	1508
Firewall-1_FW1	alert	drop	SSH	Attacker_Host	IDS2	tcp	14	1515

Audit Test #14 – Checking Hosts on Screened Network (Login Services connection attempts)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to TCP ports 21,22,23, 512,513 and 514 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sT –p 21-23,512-514 –P0 1.1.2.1-10)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to one of ***Login Services*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #10***.
C) Result	

Test works as expected. Due rule #10 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts
D) Output (Firewall-1 Event Log Viewer
No log avaiable at this time.

Audit Test #15 – Checking Hosts on Screened Network (RPC /NFS Connection attempts)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP / UDP CONNECT PORT SCAN to ports 111, 2049 and 4045 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sTU –p 111,2049,4045 –P0 1.1.2.1-10)***	TCP/UDP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP and UDP connection from Internet to one of ***RPC/NFS Services*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #15.***

C) Result

Test works as expected. Due rule #15 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	LockD-tcp	Attacker_Host	Partners_WebServer	tcp	15	3900
Firewall-1_FW1	alert	drop	sunrpc	Attacker_Host	Partners_WebServer	tcp	15	3901
Firewall-1_FW1	alert	drop	nfsd-tcp	Attacker_Host	Partners_WebServer	tcp	15	3902
Firewall-1_FW1	alert	drop	nfsd	Attacker_Host	Partners_WebServer	udp	15	55432
Firewall-1_FW1	alert	drop	Portmap-rpcbi...	Attacker_Host	Partners_WebServer	udp	15	55432
Firewall-1_FW1	alert	drop	LockD-udp	Attacker_Host	Partners_WebServer	udp	15	55432
Firewall-1_FW1	alert	drop	LockD-tcp	Attacker_Host	Suppliers_WebServer	tcp	15	3920
Firewall-1_FW1	alert	drop	nfsd-tcp	Attacker_Host	Suppliers_WebServer	tcp	15	3921
Firewall-1_FW1	alert	drop	sunrpc	Attacker_Host	Suppliers_WebServer	tcp	15	3922
Firewall-1_FW1	alert	drop	LockD-tcp	Attacker_Host	Suppliers_WebServer	tcp	15	3923
Firewall-1_FW1	alert	drop	LockD-udp	Attacker_Host	Suppliers_WebServer	udp	15	48094
Firewall-1_FW1	alert	drop	Portmap-rpcbi...	Attacker_Host	Suppliers_WebServer	udp	15	48094
Firewall-1_FW1	alert	drop	nfsd	Attacker_Host	Suppliers_WebServer	udp	15	48094

Audit Test #16 – Checking Hosts on Screened Network (Netbios Connection attempts)

A) Stimulus	***B) Expected Result***

From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a CONNECT PORT SCAN to TCP ports 135,139 445 and a UDP PORT SCAN to UDP ports 135, 137, 138 and 445 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sT –p 135,139,445 –P0 1.1.2.1-10)(*** ***nmap –sU –p135, 137,138,445 –P0 1.1.2.1-10)***	TCP/UDP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP and UDP connection from Internet to one of ***Netbios Service*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #16***.

C) Result

Test works as expected. Due rule #16 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	netbios445tcp	Attacker_Host	Primary_DNS	tcp	16	3927
Firewall-1_FW1	alert	drop	nbsession	Attacker_Host	Primary_DNS	tcp	16	3928
Firewall-1_FW1	alert	drop	netbios135tcp	Attacker_Host	Primary_DNS	tcp	16	3929
Firewall-1_FW1	alert	drop	netbios135udp	Attacker_Host	Primary_DNS	udp	16	50138
Firewall-1_FW1	alert	drop	netbios445udp	Attacker_Host	Primary_DNS	udp	16	50138
Firewall-1_FW1	alert	drop	nbdatagram	Attacker_Host	Primary_DNS	udp	16	50138
Firewall-1_FW1	alert	drop	nbname	Attacker_Host	Primary_DNS	udp	16	50138
Firewall-1_FW1	alert	drop	netbios135tcp	Attacker_Host	Oracle_DB_Server	tcp	16	3960
Firewall-1_FW1	alert	drop	nbsession	Attacker_Host	Oracle_DB_Server	tcp	16	3961
Firewall-1_FW1	alert	drop	netbios445tcp	Attacker_Host	Oracle_DB_Server	tcp	16	3962
Firewall-1_FW1	alert	drop	nbdatagram	Attacker_Host	Oracle_DB_Server	udp	16	50900
Firewall-1_FW1	alert	drop	netbios135udp	Attacker_Host	Oracle_DB_Server	udp	16	50900
Firewall-1_FW1	alert	drop	netbios445udp	Attacker_Host	Oracle_DB_Server	udp	16	50900
Firewall-1_FW1	alert	drop	nbname	Attacker_Host	Oracle_DB_Server	udp	16	50900

The output of Audit Test is not showing log entries of connections dropped for all hosts on Screened Subnet. ***To make easy for this Practical, output is showing only connections dropped to hosts 1.1.2.7 and 1.1.2.8***

Audit Test #17 – Checking Hosts on Screened Network (Xwindows Connection Attempts))

A) Stimulus	*B) Expected Result*
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to TCP ports 6000 through 6255 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sT –p 6000-6255 –P0 1.1.2.1-10)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to one of the ports in ***Xwindows port range*** on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #17***. .

C) Result

Test works as expected. Due rule #17 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	6055	Attacker_Host	Customer_WebServer	tcp	17	4031
Firewall-1_FW1	alert	drop	6092	Attacker_Host	Customer_WebServer	tcp	17	4032
Firewall-1_FW1	alert	drop	6048	Attacker_Host	Customer_WebServer	tcp	17	4033
Firewall-1_FW1	alert	drop	6038	Attacker_Host	Customer_WebServer	tcp	17	4034
Firewall-1_FW1	alert	drop	6203	Attacker_Host	Customer_WebServer	tcp	17	4035
Firewall-1_FW1	alert	drop	6143	Attacker_Host	Customer_WebServer	tcp	17	4036
Firewall-1_FW1	alert	drop	6059	Attacker_Host	Customer_WebServer	tcp	17	4037
Firewall-1_FW1	alert	drop	6216	Attacker_Host	Customer_WebServer	tcp	17	4038
Firewall-1_FW1	alert	drop	6072	Attacker_Host	Customer_WebServer	tcp	17	4039
Firewall-1_FW1	alert	drop	6018	Attacker_Host	Customer_WebServer	tcp	17	4040
Firewall-1_FW1	alert	drop	6055	Attacker_Host	Customer_WebServer	tcp	17	4041
Firewall-1_FW1	alert	drop	6092	Attacker_Host	Customer_WebServer	tcp	17	4042
Firewall-1_FW1	alert	drop	6048	Attacker_Host	Customer_WebServer	tcp	17	4043
Firewall-1_FW1	alert	drop	6038	Attacker_Host	Customer_WebServer	tcp	17	4044
Firewall-1_FW1	alert	drop	6203	Attacker_Host	Customer_WebServer	tcp	17	LockD-tcp
Firewall-1_FW1	alert	drop	6143	Attacker_Host	Customer_WebServer	tcp	17	4046
Firewall-1_FW1	alert	drop	6059	Attacker_Host	Customer_WebServer	tcp	17	4047
Firewall-1_FW1	alert	drop	6216	Attacker_Host	Customer_WebServer	tcp	17	4048
Firewall-1_FW1	alert	drop	6072	Attacker_Host	Customer_WebServer	tcp	17	4049
Firewall-1_FW1	alert	drop	6018	Attacker_Host	Customer_WebServer	tcp	17	4050

The output of Audit Test is not showing log entries of connections dropped for all hosts on Screened Subnet. ***To make easy for this Practical, output is showing only connections dropped to host 1.1.2.3***

Audit Test #18 – Checking Hosts on Screened Network (Naming Services Connection Attempts)

A) Stimulus	*B) Expected Result*
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP/UDP CONNECT PORT SCAN to TCP/UDP ports 53 and 389 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sTU –p 53,389 –P0 1.1.2.1-10)***	TCP/UDP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP/UDP connection from Internet to one of the ***NamingServices*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #18.***. **Note on accepted connection to Primary DNS :** Primary Name Server 1.1.2.3, is the only server on ***Protected Subnet*** that is allowed to accept inbound UDP port 53 – Domain Queries from any host on Internet).

C) Result

Test works as expected. Due rule #18 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts. Due rule #9, Primary DNS accepts domain queries from any host.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	ldap	Attacker_Host	Primary_DNS	tcp	18	1072
Firewall-1_FW1	alert	drop	nameserver	Attacker_Host	Primary_DNS	tcp	18	1073
Firewall-1_FW1	log	accept	domain-udp	Attacker_Host	Primary_DNS	udp	9	49494
Firewall-1_FW1	alert	drop	ldap	Attacker_Host	SyslogServer	tcp	18	1095
Firewall-1_FW1	alert	drop	nameserver	Attacker_Host	SyslogServer	tcp	18	1096
Firewall-1_FW1	alert	drop	domain-udp	Attacker_Host	SyslogServer	udp	18	34420
Firewall-1_FW1	alert	drop	ldap-udp	Attacker_Host	SyslogServer	udp	18	34420
Firewall-1_FW1	alert	drop	nameserver	Attacker_Host	IDS2	tcp	18	1107
Firewall-1_FW1	alert	drop	ldap	Attacker_Host	IDS2	tcp	18	1108
Firewall-1_FW1	alert	drop	ldap-udp	Attacker_Host	IDS2	udp	18	50734
Firewall-1_FW1	alert	drop	domain-udp	Attacker_Host	IDS2	udp	18	50734
Firewall-1_FW1	alert	drop	ldap	Attacker_Host	WebServer	tcp	18	1119
Firewall-1_FW1	alert	drop	nameserver	Attacker_Host	WebServer	tcp	18	1120
Firewall-1_FW1	alert	drop	domain-udp	Attacker_Host	WebServer	udp	18	59113
Firewall-1_FW1	alert	drop	ldap-udp	Attacker_Host	WebServer	udp	18	59113
Firewall-1_FW1	alert	drop	nameserver	Attacker_Host	Customer_WebServer	tcp	18	1130
Firewall-1_FW1	alert	drop	ldap	Attacker_Host	Customer_WebServer	tcp	18	1131
Firewall-1_FW1	alert	drop	domain-udp	Attacker_Host	Customer_WebServer	udp	18	60183
Firewall-1_FW1	alert	drop	ldap-udp	Attacker_Host	Customer_WebServer	udp	18	60183

The output of Audit Test is not showing log entries of connections dropped for all hosts on Screened Subnet. ***To make easy for this Practical, output is showing only connections dropped to hosts 1.1.2.7, 1.1.2.9,1.1.2.10,1.1.2.2 and 1.1.2.3***

Audit Test #19 – Checking Hosts on Screened Network (Mail Services Connection Attempts)

A) Stimulus

From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to TCP ports 25, 109, 110 and 143 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.*

(nmap –sT –p 25,109,110,143 –P0 1.1.2.1-10)

B) Expected Result

TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to one of the ***Mail Services*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #19.***.

Note on accepted connection to Mail Server :
Mail Server (1.1.2.6), is the only server on ***Protected Subnet*** that is allowed to accept inbound TCP port 25 connections in order to receive mail from other MX systems over the Internet).

C) Result

Test works as expected. Due rule #19 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts. Due rule #6, Mail Server accepts inbound connections to TCP port 25 .

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	pop3	Attacker_Host	Customer_WebServer	tcp	19	1157
Firewall-1_FW1	alert	drop	pop2	Attacker_Host	Customer_WebServer	tcp	19	1158
Firewall-1_FW1	alert	drop	imap	Attacker_Host	Customer_WebServer	tcp	19	1159
Firewall-1_FW1	alert	drop	smtp	Attacker_Host	Customer_WebServer	tcp	19	1160
Firewall-1_FW1	alert	drop	smtp	Attacker_Host	Suppliers_WebServer	tcp	19	1163
Firewall-1_FW1	alert	drop	pop2	Attacker_Host	Suppliers_WebServer	tcp	19	1164
Firewall-1_FW1	alert	drop	imap	Attacker_Host	Suppliers_WebServer	tcp	19	1165
Firewall-1_FW1	alert	drop	pop3	Attacker_Host	Suppliers_WebServer	tcp	19	1166
Firewall-1_FW1	alert	drop	smtp	Attacker_Host	Partners_WebServer	tcp	19	1167
Firewall-1_FW1	alert	drop	pop2	Attacker_Host	Partners_WebServer	tcp	19	1168
Firewall-1_FW1	alert	drop	imap	Attacker_Host	Partners_WebServer	tcp	19	1169
Firewall-1_FW1	alert	drop	pop3	Attacker_Host	Partners_WebServer	tcp	19	1170
Firewall-1_FW1	alert	drop	pop2	Attacker_Host	MailServer	tcp	19	1175
Firewall-1_FW1	alert	drop	pop3	Attacker_Host	MailServer	tcp	19	1176
Firewall-1_FW1	log	accept	smtp	Attacker_Host	MailServer	tcp	6	1177
Firewall-1_FW1	alert	drop	imap	Attacker_Host	MailServer	tcp	19	1178
Firewall-1_FW1	alert	drop	pop2	Attacker_Host	Primary_DNS	tcp	19	1194
Firewall-1_FW1	alert	drop	pop3	Attacker_Host	Primary_DNS	tcp	19	1195
Firewall-1_FW1	alert	drop	smtp	Attacker_Host	Primary_DNS	tcp	19	1196
Firewall-1_FW1	alert	drop	imap	Attacker_Host	Primary_DNS	tcp	19	1197

The output of Audit Test is not showing log entries of connections dropped for all hosts on Screened Subnet. ***To make easy for this Practical, output is showing only connections dropped to hosts 1.1.2.2, 1.1.2.3,1.1.2.4,1.1.2.5, 1.1.2.6 and 1.1.2.7***

Audit Test #20 – Checking Hosts on Screened Network (Web Services Connection Attempts)

A) Stimulus	*B) Expected Result*
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP CONNECT PORT SCAN to TCP ports 80, 443, 8000, 8080 and 8888 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sT –p 80,443,8000,8080,8888 –P0 1.1.2.1-10)***	TCP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP connection from Internet to one of the ***Web Services*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated ***due to Firewall rule #20.***. **Note on accepted connections to Web Server and Customer Web Server :** Web Server (1.1.2.2) and Customer Web Server (1.1.2.3) are the servers on ***Protected Subnet*** allowed to accept inbound TCP port 80 connections. Customer Web Server also accepts inbound connections to TCP port 443 (HTTPS)

C) Result

Test works as expected. Due rule #20 Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts. Due rule #2, Web Server accepts inbound connections to TCP port 80 and due to rule #3, Customer Web Server accepts inbound connections to TCP port 80 and TCP port 443.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	log	accept	http	Attacker_Host	WebServer	tcp	2	1435
Firewall-1_FW1	alert	drop	http_8080	Attacker_Host	WebServer	tcp	20	1436
Firewall-1_FW1	alert	drop	http_8000	Attacker_Host	WebServer	tcp	20	1437
Firewall-1_FW1	alert	drop	http_8888	Attacker_Host	WebServer	tcp	20	1438
Firewall-1_FW1	alert	drop	https	Attacker_Host	WebServer	tcp	20	1439
Firewall-1_FW1	log	accept	https	Attacker_Host	Customer_WebServer	tcp	3	1456
Firewall-1_FW1	log	accept	http	Attacker_Host	Customer_WebServer	tcp	3	1457
Firewall-1_FW1	alert	drop	http_8888	Attacker_Host	Customer_WebServer	tcp	20	1458
Firewall-1_FW1	alert	drop	http_8080	Attacker_Host	Customer_WebServer	tcp	20	1459
Firewall-1_FW1	alert	drop	http_8000	Attacker_Host	Customer_WebServer	tcp	20	1460
Firewall-1_FW1	alert	drop	http_8080	Attacker_Host	Suppliers_WebServer	tcp	20	1502
Firewall-1_FW1	alert	drop	http_8888	Attacker_Host	Suppliers_WebServer	tcp	20	T.120
Firewall-1_FW1	alert	drop	https	Attacker_Host	Suppliers_WebServer	tcp	20	1504
Firewall-1_FW1	alert	drop	http	Attacker_Host	Suppliers_WebServer	tcp	20	1505
Firewall-1_FW1	alert	drop	http_8000	Attacker_Host	Suppliers_WebServer	tcp	20	1506
Firewall-1_FW1	alert	drop	http_8080	Attacker_Host	Partners_WebServer	tcp	20	1507
Firewall-1_FW1	alert	drop	https	Attacker_Host	Partners_WebServer	tcp	20	1508
Firewall-1_FW1	alert	drop	http	Attacker_Host	Partners_WebServer	tcp	20	1509
Firewall-1_FW1	alert	drop	http_8000	Attacker_Host	Partners_WebServer	tcp	20	1510
Firewall-1_FW1	alert	drop	http_8888	Attacker_Host	Partners_WebServer	tcp	20	1511

The output of Audit Test is not showing log entries of connections dropped for all hosts on Screened Subnet. ***To make easy for this Practical, output is showing only connections dropped to hosts 1.1.2.2, 1.1.2.3,1.1.2.4 and 1.1.2.5***

Audit Test #21 – Checking Hosts on Screened Network (Small Services Connection Attempts)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP/UDP CONNECT PORT SCAN to TCP/UDP ports 1-20 and 37 on ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sTU –p 1-20, 37 –P0 1.1.2.1-10)***	TCP/UDP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP/UDP connection from Internet to one of the ***Misc Services*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated.

C) Result

Test works as expected. Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port
Firewall-1_FW1	alert	drop	chargen	Attacker_Host	Customer_WebServer	tcp	22	1033
Firewall-1_FW1	alert	drop	3	Attacker_Host	Customer_WebServer	tcp	22	1034
Firewall-1_FW1	alert	drop	6	Attacker_Host	Customer_WebServer	tcp	22	1035
Firewall-1_FW1	alert	drop	ftp-data	Attacker_Host	Customer_WebServer	tcp	27	1036
Firewall-1_FW1	alert	drop	5	Attacker_Host	Customer_WebServer	tcp	22	1037
Firewall-1_FW1	alert	drop	qotd	Attacker_Host	Customer_WebServer	tcp	22	1038
Firewall-1_FW1	alert	drop	echo-tcp	Attacker_Host	Customer_WebServer	tcp	22	1039
Firewall-1_FW1	alert	drop	14	Attacker_Host	Customer_WebServer	tcp	22	1040
Firewall-1_FW1	alert	drop	discard-tcp	Attacker_Host	Customer_WebServer	tcp	22	1041
Firewall-1_FW1	alert	drop	time-tcp	Attacker_Host	Customer_WebServer	tcp	22	1042
Firewall-1_FW1	alert	drop	chargen	Attacker_Host	Customer_WebServer	tcp	22	1043
Firewall-1_FW1	alert	drop	3	Attacker_Host	Customer_WebServer	tcp	22	1044
Firewall-1_FW1	alert	drop	6	Attacker_Host	Customer_WebServer	tcp	22	1045
Firewall-1_FW1	alert	drop	ftp-data	Attacker_Host	Customer_WebServer	tcp	27	1046
Firewall-1_FW1	alert	drop	5	Attacker_Host	Customer_WebServer	tcp	22	1047
Firewall-1_FW1	alert	drop	qotd	Attacker_Host	Customer_WebServer	tcp	22	1048
Firewall-1_FW1	alert	drop	echo-tcp	Attacker_Host	Customer_WebServer	tcp	22	1049
Firewall-1_FW1	alert	drop	14	Attacker_Host	Customer_WebServer	tcp	22	1050
Firewall-1_FW1	alert	drop	discard-tcp	Attacker_Host	Customer_WebServer	tcp	22	1051
Firewall-1_FW1	alert	drop	time-tcp	Attacker_Host	Customer_WebServer	tcp	22	1052
Firewall-1_FW1	alert	drop	chargen	Attacker_Host	Customer_WebServer	tcp	22	1053
Firewall-1_FW1	alert	drop	3	Attacker_Host	Customer_WebServer	tcp	22	1054

The output of Audit Test is not showing log entries of connections dropped for all hosts on Screened Subnet. ***To make easy for this Practical, output is showing only connections dropped to host 1.1.2.3***

Audit Test #22 – Checking Hosts on Screened Network (Misc Services Connection Attempts)	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, perform a TCP/UDP CONNECT PORT SCAN to TCP ports 79, 119, 123, 515, 161, 179, 1080 and UDP ports 69, 515, 161 and 162 ***Protected Subnet (Screened Subnet)*** *starting on ip address 1.1.2.1 up to 1.1.2.10.* ***(nmap –sT –p 79,119,123,515,161,179,1080 –P0 1.1.2.1-10)*** ***(nmap –sU –p 69,515,161,162 –P0 1.1.2.1-10)***	TCP/UDP CONNECT PORT SCAN must be blocked. Any attempt to establish a TCP/UDP connection from Internet to one of the ***Small Services*** ports on ***Protected Subnet*** (1.1.2.0) should be dropped, logged and alert must be generated**.**
C) Result	
Test works as expected. Connections to specific ports were dropped and logged. Alert was generated in order to advise security staff of possible malicious connection attempts.	
D) Output (Firewall-1 Event Log Viewer	
No log avaiable at this time	

Audit Test #23– Synflood Attack	
A) Stimulus	***B) Expected Result***
From Attacker Host (Internet) in a Linux shell, using nmap as stimulus tool, perform a SYN-halt-open stealth scan. (nmap -sT -F 1.1.2.2)	SynDefender Gateway must Reject connections (SYNFlood Attack).

C) Result

Test works as expected. Due Firewall-1 Syn Gateway Defender, connections were rejected.

D) Output (Firewall-1 Event Log Viewer

Origin	Type	Action	Service	Source	Destinati..	Proto.	Rule	S_Po..	Info.
Firewall-1_FW1	log	reject	http	Attacker_Host	WebServer	tcp	0	44525	message SYNDefender...
Firewall-1_FW1	log	reject	http	Attacker_Host	WebServer	tcp	0	54256	message SYNDefender...
Firewall-1_FW1	log	reject	http	Attacker_Host	WebServer	tcp	0	43449	message SYNDefender...
Firewall-1_FW1	log	reject	http	Attacker_Host	WebServer	tcp	0	44499	message SYNDefender...
Firewall-1_FW1	log	reject	http	Attacker_Host	WebServer	tcp	0	47074	message SYNDefender...
Firewall-1_FW1	log	reject	http	Attacker_Host	WebServer	tcp	0	47065	message SYNDefender...

E) Output (SNORT IDS Running in Verbose Mode – TCPDUMP)

Snort shows connection being established. First, remote host sends a SYN packet to ***WebServer*** on TCP port 80. ***WebServer*** sends a packet with SYNand ACK flags set to source ephemerous port and finally, the remote host sends the ACK flag telling ***WebServer*** that the connection has been established and they are ready to send/receive data.

b

```
02/06-19:41:51.917511 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x4A
172.16.5.3:1101 -> 1.1.2.2:80 TCP TTL:64 TOS:0x0 ID:29727  DF
******S* Seq: 0xD2AA002C   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 36920792 0 NOP WS: 0

02/06-19:41:51.918607 0:0:B4:52:4E:EC -> 0:0:B4:52:4B:30 type:0x800 len:0x4E
1.1.2.2:80 -> 172.16.5.3:1101 TCP TTL:127 TOS:0x0 ID:7468  DF
***A**S* Seq: 0xBD31781A   Ack: 0xD2AA002D   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

02/06-19:41:51.918747 0:0:B4:52:4B:30 -> 0:0:B4:52:4E:EC type:0x800 len:0x42
172.16.5.3:1101 -> 1.1.2.2:80 TCP TTL:64 TOS:0x0 ID:29728  DF
***A**** Seq: 0xD2AA002D   Ack: 0xBD31781B   Win: 0x7D78
TCP Options => NOP NOP TS: 36920792 0
```

5.3 Border Router Cisco Internet#1 Audit

Audit Test #1 - Packets coming from outside company sourced from Subnet 1.1.1.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 1.1.1.0 sourced address. ***(nmap –sS –P0 –F –e eth0 –S 1.1.1.82 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.1.14 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.1.83 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.1.31 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***Subnet 1.1.1.0*** should be dropped and logged ***due to access-list 101***: ***Access-list 101 deny ip 1.1.1.0 0.0.0.255 any log*** ***Note about NMAP –S flag :*** ***The flag -S flag is used to spoof the scan to make the targets think that someone else is scanning them.***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from internal subnet 1.1.1.0 were dropped and logged.	
D) Output (Cisco Router Log)	
Feb 11 20:27:06 1.1.1.3 21: 00:19:05: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.1.82(0) -> 1.1.2.3(0), 1 packet Feb 11 20:38:02 1.1.1.3 27: 00:30:01: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.1.14(0) -> 1.1.2.4(0), 1 packet Feb 11 20:39:41 1.1.1.3 28: 00:31:40: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.1.83(0) -> 1.1.2.8(0), 1 packet Feb 11 20:40:44 1.1.1.3 29: 00:32:43: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.1.83(0) -> 1.1.2.10(0), 1 packet	

Audit Test #2 - Packets coming from outside company sourced from Subnet 1.1.2.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 1.1.2.0 sourced address ***(nmap –sS –P0 –F –e eth0 –S 1.1.2.12 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.2.41 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.2.33 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.2.73 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***Subnet 1.1.1.0*** should be dropped and logged ***due to access-list 101:*** ***Access-list 101 deny ip 1.1.2.0 0.0.0.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from internal subnet 1.1.2.0 were dropped and logged.	
D) Output (Cisco Router Log)	

Feb 11 21:11:09 1.1.1.3 30: 01:03:07: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.2.12(0) -> 1.1.2.3(0), 1 packet
Feb 11 21:12:04 1.1.1.3 31: 01:04:02: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.2.41(0) -> 1.1.2.4(0), 1 packet
Feb 11 21:12:34 1.1.1.3 32: 01:04:32: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.2.33(0) -> 1.1.2.8(0), 1 packet
Feb 11 21:13:12 1.1.1.3 33: 01:05:10: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.2.73(0) -> 1.1.2.10(0), 1 packet

Audit Test #3 - Packets coming from outside company sourced from Subnet 1.1.3.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 1.1.3.0 sourced address. ***(nmap –sS –P0 –F –e eth0 –S 1.1.3.2 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.3.33 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.3.65 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.3.76 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***Subnet 1.1.3.0*** should be dropped and logged ***due to access-list 101:*** ***Access-list 101 deny ip 1.1.3.0 0.0.0.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from internal subnet 1.1.3.0 were dropped and logged.	
D) Output (Cisco Router Log)	
Feb 11 21:31:45 1.1.1.3 34: 01:23:43: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.3.2(0) -> 1.1.2.3(0), 1 packet Feb 11 21:32:22 1.1.1.3 35: 01:24:20: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.3.33(0) -> 1.1.2.4(0), 1 packet Feb 11 22:11:19 1.1.1.3 36: 02:03:17: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.3.65(0) -> 1.1.2.8(0), 1 packet Feb 11 22:12:06 1.1.1.3 37: 02:04:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.3.76(0) -> 1.1.2.10(0), 1 packet	

Audit Test #4 - Packets coming from outside company sourced from Subnet 1.1.4.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 1.1.4.0 sourced address ***(nmap –sS –P0 –F –e eth0 –S 1.1.4.3 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.4.21 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.4.33 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.4.65 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***Subnet 1.1.4.0*** should be dropped and logged ***due to access-list 101:*** ***Access-list 101 deny ip 1.1.4.0 0.0.0.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from internal subnet 1.1.4.0 were dropped and logged.	
D) Output (Cisco Router Log)	

Feb 11 22:14:25 1.1.1.3 38: 02:06:22: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.4.3(0) -> 1.1.2.3(0), 1 packet
Feb 11 22:15:03 1.1.1.3 39: 02:06:59: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.4.21(0) -> 1.1.2.4(0), 1 packet
Feb 11 22:15:40 1.1.1.3 40: 02:07:38: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.4.33(0) -> 1.1.2.8(0), 1 packet
Feb 11 22:16:11 1.1.1.3 41: 02:08:09: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.4.65(0) -> 1.1.2.10(0), 1 packet

Audit Test #5 – Packets coming from outside company sourced from Subnet 1.1.5.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 1.1.5.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 1.1.5.2 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.5.25 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.5.42 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 1.1.5.64 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***Subnet 1.1.5.0*** should be dropped and logged ***due to access-list 101:***: ***Access-list 101 deny ip 1.1.5.0 0.0.0.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from internal subnet 1.1.5.0 were dropped and logged.	
D) Output (Cisco Router Log)	
Feb 11 22:18:57 1.1.1.3 42: 02:10:54: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.5.2(0) -> 1.1.2.3(0), 1 packet Feb 11 22:19:28 1.1.1.3 43: 02:11:24: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.5.25(0) -> 1.1.2.4(0), 1 packet Feb 11 22:20:10 1.1.1.3 44: 02:12:08: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.5.42(0) -> 1.1.2.80), 1 packet Feb 11 22:20:33 1.1.1.3 45: 02:12:30: %SEC-6-IPACCESSLOGP: list 101 denied tcp 1.1.5.64(0) -> 1.1.2.10(0), 1 packet	

Audit Test #6 – Packets coming from outside company sourced from 10.0.0.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 10.0.0.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 10.0.0.4 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 10.1.2.4 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 10.4.3.2 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 10.20.3.1 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***10.0.0.0 (Private address space – RFC 1918)*** should be dropped and logged ***due to access-list 101*** : ***Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from internal subnet 1.1.5.0 were dropped and logged.	
D) Output (Cisco Router Log)	

Feb 11 22:38:17 1.1.1.3 46: 02:30:14: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.0.0.4(0) -> 1.1.2.3(0), 1 packet
Feb 11 22:39:08 1.1.1.3 47: 02:31:06: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.1.2.4(0) -> 1.1.2.4(0), 1 packet
Feb 11 22:40:29 1.1.1.3 48: 02:32:26: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.4.3.2(0) -> 1.1.2.8(0), 1 packet
Feb 11 22:42:39 1.1.1.3 49: 02:34:36: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.2.0.3(0) -> 1.1.2.10(0), 1 packet

Audit Test #7 – Packets coming from outside company sourced from 172.16.0.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 172.16.0.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 172. 16.0.3 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 172.16.3.33 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 172.16.54.2 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 172.16.63.3 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***172.16.0.0 (Private address space – RFC 1918)*** should be dropped and logged ***due to access-list 101*** : ***Access-list 101 deny ip 172.16.0.0 0.15.255.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from 172.16.0.0 were dropped and logged.	
D) Output (Cisco Router Log)	
Feb 12 01:24:21 1.1.1.3 50: 05:16:15: %SEC-6-IPACCESSLOGP: list 101 denied tcp 172.16.0.3(0) -> 1.1.2.3(0), 1 packet Feb 12 01:25:20 1.1.1.3 51: 05:17:15: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 172.16.3.33(0) -> 1.1.2.4(0), 1 packet Feb 12 01:26:38 1.1.1.3 52: 05:18:34: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 172.16.54.2(0) -> 1.1.2.8(0), 1 packet Feb 12 01:28:22 1.1.1.3 53: 05:20:18: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 172.16.63.3(0) -> 1.1.2.10(0), 1 packet	

Audit Test #8 – Packets coming from outside company sourced from 192.168.0.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 192.168.0.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 192.168.0.3 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 192.168.2.34 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 192.168.4.54 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 192.168.8.4 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***192.168.0.0 (Private address space – RFC 1918)*** should be dropped and logged ***due to access-list 101*** : ***Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from 192.168.0.0 were dropped and logged.	
D) Output (Cisco Router Log)	

Feb 12 02:21:16 1.1.1.3 54: 06:13:11: %SEC-6-IPACCESSLOGP: list 101 denied tcp 192.168.0.3(0) -> 1.1.2.3(0), 1 packet
Feb 12 02:21:57 1.1.1.3 55: 06:13:52: %SEC-6-IPACCESSLOGP: list 101 denied tcp 192.168.2.34(0) -> 1.1.2.4(0), 1 packet
Feb 12 02:22:19 1.1.1.3 56: 06:14:13: %SEC-6-IPACCESSLOGP: list 101 denied tcp 192.168.4.54(0) -> 1.1.2.8(0), 1 packet
Feb 12 02:23:09 1.1.1.3 57: 06:15:03: %SEC-6-IPACCESSLOGP: list 101 denied tcp 192.168.8.4(0) -> 1.1.2.10(0), 1 packet

Audit Test #9 – Packets coming from outside company sourced from 127.0.0.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 127.0.0.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 127.0.0.1 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 127.0.0.1 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 127.0.0.1 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 127.0.0.1 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***127.0.0.0 (Private address space – RFC 1918)*** should be dropped and logged ***due to access-list 101*** : ***Access-list 101 deny ip 127.0.0.0 0.255.255.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from 127.0.0.0 were dropped and logged.	
D) Output (Cisco Router Log)	
Feb 12 18:14:55 1.1.1.3 28: 00:40:54: %SEC-6-IPACCESSLOGP: list 101 denied tcp 127.0.0.1(0) -> 1.1.2.3(0), 1 packet Feb 12 18:16:12 1.1.1.3 29: 00:42:11: %SEC-6-IPACCESSLOGP: list 101 denied tcp 127.3.31.31(0) -> 1.1.2.4(0), 1 packet Feb 12 18:18:07 1.1.1.3 30: 00:44:04: %SEC-6-IPACCESSLOGP: list 101 denied tcp 127.122.2.211(0) -> 1.1.2.8(0), 1 packet Feb 12 18:18:53 1.1.1.3 31: 00:44:52: %SEC-6-IPACCESSLOGP: list 101 denied tcp 127.15.33.111(0) -> 1.1.2.10(0), 1 packet	

Audit Test #10 – Packets coming from outside company sourced from 224.0.0.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 224.0.0.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 224.0.0.45 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 224.3.21.3 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 224.8.13.1 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 224.34.1.2 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***224.0.0.0 Multicast (Class D)*** should be dropped and logged ***due to access-list 101*** : ***Access-list 101 deny ip 224.0.0.0 31.255.255.255 any log***
C) Result	

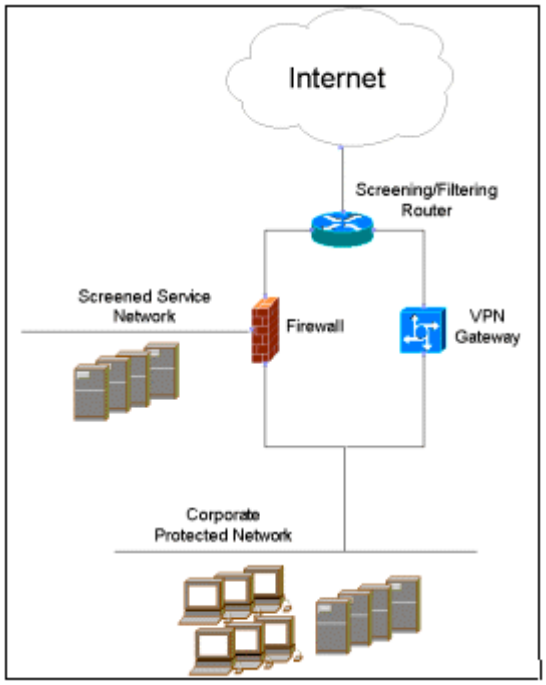
Test works as expected. Due access-list 101 connections from outside company sourced from 224.0.0.0 were dropped and logged.
D) Output (Cisco Router Log)
Feb 12 18:48:10 1.1.1.3 46: 01:14:09: %SEC-6-IPACCESSLOGP: list 101 denied tcp 224.0.0.45(0) -> 1.1.2.3(0), 1 packet Feb 12 18:52:19 1.1.1.3 47: 01:18:17: %SEC-6-IPACCESSLOGP: list 101 denied tcp 224.3.21.3(0) -> 1.1.2.4(0), 1 packet Feb 12 18:52:59 1.1.1.3 48: 01:18:57: %SEC-6-IPACCESSLOGP: list 101 denied tcp 224.8.13.1(0) -> 1.1.2.8(0), 1 packet Feb 12 18:53:39 1.1.1.3 49: 01:19:37: %SEC-6-IPACCESSLOGP: list 101 denied tcp 224.34.1.2(0) -> 1.1.2.10(0), 1 packet

Audit Test #11 – Packets coming from outside company sourced from 240.0.0.0	
A) Stimulus	***B) Expected Result***
From ***Attacker Host*** (Internet) in a Linux shell, using nmap as stimulus tool, peform a SYN-halt-open stealth scan to the protected network in order to send crafted packets (traveling inbound to the external interface of the router) with 240.0.0.0 sourced adddress. ***(nmap –sS –P0 –F –e eth0 –S 240.0.0.1 1.1.2.3)*** ***(nmap –sS –P0 –F –e eth0 –S 240.3.33.45 1.1.2.4)*** ***(nmap –sS –P0 –F –e eth0 –S 240.12.13.1 1.1.2.8)*** ***(nmap –sS –P0 –F –e eth0 –S 240.34.6.3.2 1.1.2.10)***	Connections must be blocked. Any attempt to establish a connection from outside company sourced from ***240.0.0.0 Unspecified (Class D)*** should be dropped and logged ***due to access-list 101*** : ***Access-list 101 deny ip 240.0.0.0 15.255.255.255 any log***
C) Result	
Test works as expected. Due access-list 101 connections from outside company sourced from 240.0.0.0 were dropped and logged.	
D) Output (Cisco Router Log)	
Feb 13 02:10:37 1.1.1.3 12: 00:02:08: %SEC-6-IPACCESSLOGP: list 101 denied tcp 240.0.0.1(0) -> 1.1.2.3(0), 1 packet Feb 13 02:11:29 1.1.1.3 15: 00:03:01: %SEC-6-IPACCESSLOGP: list 101 denied tcp 240.3.33.45(0) -> 1.1.2.4(0), 1 packet Feb 13 02:12:05 1.1.1.3 16: 00:03:36: %SEC-6-IPACCESSLOGP: list 101 denied tcp 240.12.13.1(0) -> 1.1.2.8(0), 1 packet Feb 13 02:12:44 1.1.1.3 17: 00:04:15: %SEC-6-IPACCESSLOGP: list 101 denied tcp 240.34.63.2(0) -> 1.1.2.10(0), 1 packet	

6 Design Under Fire (25 Points)

6.1 Network Architecture

This is the network topology choosen. It´s the **Colin Stuckless** topology from Practical Assignment (SANS Parliament Hill 2000). As requested, the Network Architecture will be target of three different attacks



An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.

A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose. ´

An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Since Colin Stuckless Practical Assignment does not show access-lists created in order to prevent anti-spoofing packets we assume that it was not used.

The next pages will describe a Pix vulnerability found in version 5.0 and how it could be possible to take the network down.

6.2 Attack Against the Firewall – Pix Vulnerability

Describe an attack against the firewall Pix Cisco and explain the results after the attack.

Phase A – Find the Cisco Device

Some cisco equipment implements a very simple identification protocol that can be used to locate devices on networks. When a TCP connection is opened to port 1999 on a Cisco router, the device returns a RST packet (normal activity) with 'cisco' in the data payload

Phase B – Attacking the Firewall

The Cisco Secure PIX Firewall cannot distinguish between a forged TCP Reset (RST) packet and a genuine TCP RST packet. Any TCP/IP connection established through the Cisco Secure PIX Firewall can be terminated by a third party from the untrusted network if the connection can be uniquely determined. This vulnerability is independent of configuration. There is no known workaround.

This vulnerability exists in all Cisco Secure PIX Firewall software releases up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1). The defect has been assigned Cisco bug ID CSCdr11711.

When the Cisco Secure PIX Firewall receives a TCP Reset (RST) packet, it evaluates that packet based on data contained in the TCP packet header: source IP address, source port, destination IP address, and destination port. If these four values match an entry in the stateful inspection table, the associated connection will be reset. This affects only TCP sessions. Data exchange based on any other protocol is not affected.

To exploit this vulnerability, an attacker would need to have or infer:

- Detailed knowledge of the source and destination IP Address and ports associated with a particular connection to be attacked, that would be found using some scanner like Nmap.

- Cisco Secure PIX Firewall that provides external access to the Internet and for which all of the preceding conditions are met is vulnerable to the disruption of individual sessions.

Cisco is offering free software upgrades to remedy this vulnerability for all affected customers.

6.3 Denial Of Service Attack – No IP Spoofing filters on Border Router

When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections--telnet, Web, email, etc.

The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server. Here is a view of this message flow:

```
Client                          Server
 ------                          ------
SYN------------>      <------------SYN-ACK
ACK------------>
```

Client and server can now send service-specific data

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection. The server has built in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the victim server system; these appear to be legitimate but in fact reference a client system that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent

to the victim server system.

The half-open connections data structure on the victim server system will eventually fill; then the system will be unable to accept any new incoming connections until the table is emptied out.

Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim server system will recover. However, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can expire the pending connections.

In most cases, the victim of such an attack will have difficulty in accepting any new incoming network connection. In these cases, the attack does not affect existing incoming connections nor the ability to originate outgoing network connections.

However, in some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

The location of the attacking system is obscured because the source addresses in the SYN packets are often implausible. When the packet arrives at the victim server system, there is no way to determine its true source.

Since the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering

Cisco 3640 border router has no anti-spoofing filters. The second line of defense is a Pix Firewall 5.0. Pix also does not have any kind of anti-spoof configuration and does not have the floodguard feature enabled <u>The network can be a target of Denial of Service Attacks.</u>

Border router is not configured with Inbound and Outbound filters in order to deny spoofed packets entering and leaving the network.

If an attack from 50 compromised cable modem/DSL systems using TCP SYN flags with spoofed reserved private networks address like 10.0.0.0, 127.0.0.0, 172.16.0.0 or 192.168.0.0 could be fired, the network will surely get down.

It is needed to provide a proper router configuration can reduce the likelihood that the site will be the source of one of these attacks. It is needed to install the filters in order to protect the network against DDOS attacks.

With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, ***steps can be taken to reduce the number of IP-spoofed packets entering and exiting the network.*** Currently, the best method is to install a filtering router that restricts the input to external interface (known as an input filter) by not allowing a packet through if it has a source address from internal network.

In addition, filter outgoing packets that have a source address different from your internal network to prevent a source IP spoofing attack from originating from the site.

The combination of these two filters would prevent outside attackers from sending packets pretending to be from internal network. It would also prevent packets originating within corporate network from pretending to be from outside. These filters will *not* stop all TCP SYN attacks, since outside attackers can spoof

packets from *any* outside network, and internal attackers can still send attacks spoofing internal addresses.

Disabling source routing at the router does not protect network from this attack, but it is still good security practice to follow. On the external interface, (that is coming from the Internet to corporate network), the followig packets should be blocked :

Broadcast Networks: The addresses to block here are network 0 (the all zeros broadcast address) and network 255.255.255.255 (the all ones broadcast network).

* Local Network(s): These are network coporate addresses

* Reserved private networks: The following networks are defined as reserved private networks and no traffic should ever be received from or transmitted to these networks through a router: 10.0.0.0 127.0.0.0 172.16.0.0 192.168.0.0

It is possible using ***nmap as stimulous tool,*** perform a TCP SYN scan: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response.

A SYN|ACK indicates the port is listening. A RST is indicative of a non-lis-tener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log

At the same time, attack from 50 compromised cable modem/DSL systems using TCP SYN flags with spoofed address as source (invalid addresses), could led network to down status due the overload of SYN Flood being received by Screened servers.

(nmap –sS –P0 –F –e eth0 –S 10.1.2.5 3.3.3.4)
TCP SYN SCAN to host 3.3.3.4 – packet spoofed (sourced from address 10.1.2.5 - Reserved Private Network)

(nmap –sS –P0 –F –e eth0 –S 172.16.5.2 3.3.3.5)
TCP SYN SCAN to host 3.3.3.5 – packet spoofed (sourced from address 172.16.5.2 - Reserved Private Network)

(nmap –sS –P0 –F –e eth0 –S 172.16.13.5 3.3.3.6)
TCP SYN SCAN to host 3.3.3.6 – packet spoofed (sourced from address 172.16.13.5 - Reserved Private Network)

(nmap –sS –P0 –F –e eth0 –S 192.168.3.5 3.3.3.7)
TCP SYN SCAN to host 3.3.3.7 – packet spoofed (sourced from address 192.168.3.5 - Reserved Private Network)

(nmap –sS –P0 –F –e eth0 –S 127.0.0.4 3.3.3.8)
TCP SYN SCAN to host 3.3.3.8 – packet spoofed (sourced from address 127.0.0.45 - Reserved Private Network)

6.4 Attack Plan to Compromise Internal Systems

There are 05 computers systems that have services that are designed to be accessible from any location on the Internet. They are doing static NAT through PIX Firewall

conduit permit tcp host 3.3.3.4 eq ftp any
conduit permit tcp host 3.3.3.5 eq http any
conduit permit tcp host 3.3.3.6 eq 443 any
conduit permit tcp host 3.3.3.7 eq 53 any
conduit permit tcp host 3.3.3.8 eq smtp any

Many attacks are successful because the content of packets are not screened at all, IDS signatures are not up to date, operating systems are not up to date, and unknown vulnerabilities that are impossible to defend against.

The web server is a good startup point. Web Servers are target of attacks due numerous reasons:

Access is to the web server application is not protected by the firewall or screening router. Web server applications are constantly under attack and a great number of exploits Poor software-programming practices could led to security problems.

To compromise an internal corporate web server the first step is to try to discover remote operating systems and such informations like web server software, web application being provided. After seeking information about remote system, It could be possible to look for vulnerabilities. These vulnerabilities can be problems with the operating system, the web server software, the applications that run the site, insecure configuration of the web server, and poor coding practices.

Once the attacker has chosen a particular vulnerability to exploit the will most likely take steps to perform the attack from a system that will make it nearly impossible to trace the origin of the attack back to the attacker. In many cases an attacker will compromise another host on the Internet and install any tools needed to compromise the web server so that at a later time the attacker can come back and perform the attack. Mail Server, Ftp Server and DNS Server also can be a good point of entry and could be used for second attempt.